Pratique des Solutions VPN sur les réseaux WiFi

LIVRE BLANC

Contributeurs

Les opérateurs membres de l'association Wireless Link ont apporté leur contribution à la rédaction de ce livre blanc. Fortes de leurs expériences dans le domaine des réseaux et services à valeur ajoutée, elles ont identifié les enjeux de la mise en œuvre de solutions complémentaires au WiFi pour en assurer la sécurité.

Bouygues Telecom

orange™

SFR

Cegetel

hub télécom

meteor NETWORKS

naxos

Sanef idées en route

VISACOM

WIFIRST

Ipelium, partenaire, a apporté son expertise dans la sécurité des systèmes d'information et son retour d'expérience sur les solutions de mobilité. Ipelium a animé les débats au sein de l'association et assuré la rédaction du livre blanc.

IPELIUM
access whatever wherever whenever securely

Pratique des Solutions VPN sur les réseaux WiFi

LIVRE BLANC

Wireless Link
55, rue Sainte Anne
75002 PARIS
Directeur de la publication : Joël Gaget
Email : contact@wirelesslink.fr

Première édition
Dépôt légal 4ème trimestre 2005
Valeur marchande équivalente : 30 €

Préface

Depuis sa création il y a deux ans, l'association Wireless Link œuvre pour développer l'usage du WiFi sur les hotspots publics.

Les opérateurs membres de Wireless Link représentent plus de 90% des hotspots installés en France et contribuent largement au déploiement de cette technologie dans notre pays.

Le travail réalisé par ses membres a d'ores et déjà permis de rendre la majorité des réseaux interopérables et un parcours client simplifié et homogène a considérablement simplifié l'accès aux réseaux.
Le développement de l'usage, qui a été multiplié par 7 en l'espace d'un an, témoigne du succès de cette initiative.

Aujourd'hui, la sécurité reste cependant un frein pour les utilisateurs professionnels : comment garantir que les données que mes collaborateurs ou moi-même échangerons lors de nos déplacements ne feront pas l'objet d'une intrusion et resteront confidentielles ?

L'objet de ce Livre Blanc est de montrer que des technologies existent pour répondre à cette question : les solutions VPN sont rodées et existent depuis que l'on transmet des données sur des réseaux publics, ce qui a justifié la mise en place d'une politique de sécurisation des échanges.

Elles apportent une réponse au besoin de respect de la confidentialité et d'intégrité des données échangées.

Pour s'adapter à ce besoin, les membres de Wireless Link ont réalisé les aménagements nécessaires sur leurs infrastructures pour rendre les technologies VPN utilisables sur leurs réseaux WiFi.

Dans ce Livre Blanc, nous proposons une méthodologie de choix et de déploiement qui intègre les paramètres propres à chaque entreprise. Chacun y trouvera les éléments pour l'aider à mettre en place la solution la mieux adaptée à ses contraintes spécifiques, à l'architecture de son réseau et à ses objectifs.

En montrant que les réseaux WiFi peuvent servir à l'échange de données en complète sécurité, nous voulons contribuer au développement d'une nouvelle image :
un WiFi sûr, au service des professionnels.

Sommaire

Références des images

1

WiFi, VPN ET PRODUCTIVITE SONT INDISSOCIABLES

1.1 WiFi, UN ATOUT DE COMPÉTITIVITÉ

L'adoption des nouvelles technologies telles que le WiFi et les VPN (Virtual Private Network) par les entreprises n'est pas fortuite. Certaines sociétés y verront une réponse à un besoin, d'autres, un avantage concurrentiel.
Avec l'arrivée du téléphone portable, les notions de disponibilité ont été bouleversées. Etre joignable à tout instant était exceptionnel. Aujourd'hui, ne pas l'être est difficilement imaginable.

Voix et données constituent aujourd'hui l'essentiel des échanges internes et externes d'une entreprise. Avec ces modes de communication apparaît le besoin d'instantanéité. Bénéficier d'un moyen de communication performant ne suffit plus, il faut en élargir les modes d'accès dans l'espace et le temps. Là où être joignable par téléphone était un minimum, il faut désormais pouvoir consulter et traiter des mails, accéder à des applications métier où et quand on le souhaite.

La mobilité appuyée sur les technologies WiFi ne se résume pas aux seules problématiques de messagerie. De la synchronisation de base de données à la consultation de sites Internet en passant par le travail collaboratif ou les téléconférences, tout est réuni de nos jours pour travailler sur le terrain dans des conditions proches de celles du bureau.
Les opérateurs ont déployé des réseaux performants, les équipementiers ont développé des terminaux ergonomiques et adaptés, et les éditeurs d'applications ont pris le virage de ces modes d'échanges d'informations de toutes natures (images, vidéo, SMS …).
La question de la sécurité des informations transportées se posait clairement. Les entreprises ont tranché en faveur des moyens de sécurité déjà massivement utilisés pour les échanges sur Internet : Les VPN.

1.2 VPN, LA COMPOSANTE SÉCURITÉ DE WiFi

Les techniques de VPN ont été conçues pour sécuriser les échanges entre différentes entités d'une même entreprise sur Internet. Elles se sont ensuite diversifiées pour sécuriser les communications d'utilisateurs mobiles. Les VPN présentent des avantages qui rassureront l'entreprise candidate à l'utilisation de WiFi : ils sont simples à mettre en œuvre, extrêmement

fiables et quasiment « incassables ». Ils sont facilement conciliables avec les infrastructures en place dans les entreprises et peuvent être rendus complètement transparents pour l'utilisateur nomade.

Loin de constituer une mode ou un gadget pour technophiles, l'utilisation des technologies WiFi et VPN associées pour l'accès distant au système d'information représente un réel bénéfice et gagne les grandes comme les petites entreprises. Garantir la sécurité des données devient un enjeu majeur lors de l'ouverture contrôlée du système d'information. Les entreprises y voient l'amélioration de leur réactivité et un atout précieux dans leur quête de compétitivité.

En résumé…

L'utilisation des applications « métiers » devient pour l'entreprise un besoin fondamental. Les technologies sont aujourd'hui disponibles ; réseaux WiFi publics, terminaux, applications adaptées sont autant d'outils d'amélioration de la productivité.
La technologie VPN est la composante sécurité nécessaire à l'utilisation des applications sur les réseaux WiFi publics.

2

IMPACTS DU WiFi SUR LA SECURITE ET LE S.I

2.1 Le WiFi : un media banalisé

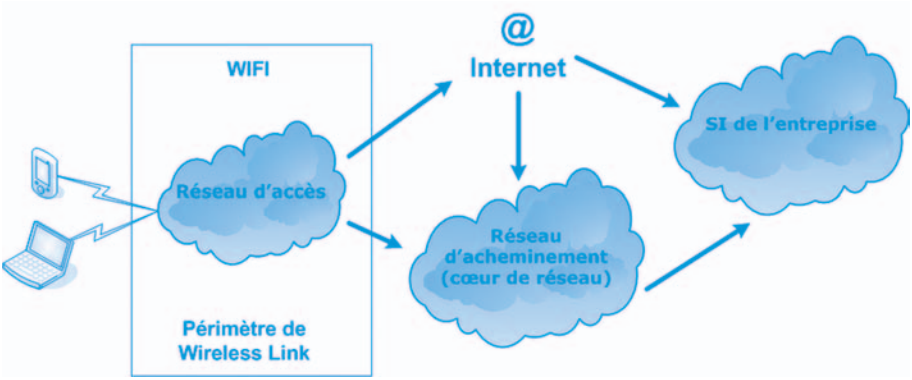
La technologie WiFi n'est pas nouvelle. Le positionnement de la technologie dans le panorama des solutions d'accès mobiles a conduit de nombreuses entreprises ou particuliers à s'approprier le WiFi devenu aujourd'hui un mode d'accès à part entière, simple, éprouvé, bref… banal.
Déployé avant tout en réseau d'accès dont les performances le classent au premier rang des réseaux mobiles, WiFi doit être considéré comme un moyen supplémentaire d'accéder à Internet d'abord puis à l'entreprise et ses ressources informatiques.

Si ce mode de transport est banalisé, il ne met pas moins en scène une multitude d'intervenants opérateurs, fournisseurs d'accès à internet, hébergeurs,...
Les plus représentatifs d'entre eux se sont regroupés dans l'association Wireless Link pour unifier les règles d'utilisation de leurs différents points d'accès WiFi et simplifier ainsi grandement la tâche aux entreprises clientes.

Revenons un instant sur la notion de réseau de transport. Nous avons décrit le WiFi comme un moyen d'accès à internet. Le point d'accès (ou Hot Spot) en matérialise la porte d'entrée.

Le rôle de « l'opérateur WiFi » au sens strict du terme est donc de fournir un accès à Internet d'où il est ensuite possible de se connecter à son entreprise.

Fig 1 : Parcours des données du terminal nomade vers le SI



Le schéma présenté ci-dessus décrit le chemin parcouru par les données transportées entre un utilisateur nomade (terminal) et le système d'information de son entreprise.

L'acheminement des données sur Internet repose sur l'utilisation de nombreux réseaux interconnectés. Si chacun des opérateurs intervenants se concentre sur son domaine de responsabilité pour atteindre ses propres objectifs de sécurité, il n'est toutefois pas réaliste de proposer une sécurité globale et maîtrisée sur l'ensemble du chemin parcouru.

Les adhérents de Wireless Link se sont fixés des objectifs communs et ont décrits des règles homogènes concernant la gestion et la sécurité :

- *Définition des caractéristiques techniques minimales du service WiFi rendu aux entreprises clientes (sécurité, authentification, QoS) en France métropolitaine*

- *Interopérabilité des services WiFi publics sur les points d'accès WiFi en France métropolitaine dans le respect de règles établies et applicables (formats des tickets de taxation, authentification …)*

- *Simplicité et homogénéité du parcours client*

Le bon fonctionnement des différentes technologies (VPN SSL, IPSEC, PPTP, …) nécessite une configuration adaptée des équipements traversés.

Afin de se prémunir face à ces désagréments potentiels, les opérateurs de l'Association Wireless Link ont apporté des modifications et adaptations à la façon dont ils opèrent leurs réseaux. L'harmonisation des règles d'ingénierie des réseaux entre les opérateurs membres de Wireless Link constitue l'un des axes de travail majeurs de l'Association.

Les principales contraintes de gestion des connexions VPN adoptées par les opérateurs membres de Wireless Link sont :

- *Autoriser sur tous les équipements traversés support des flux suivants: IKE, UDP/4500 (encapsulation UDP pour IPSec), TCP/443, ports spécifiques à certains constructeurs (TCP/264, TCP/1723, TCP/10000), etc.*
- *Autoriser les protocoles standards: IP 51, IP 50 et IP 47 (GRE).*
- *La configuration des équipements réseau des opérateurs traversés évite de fragmenter les datagrammes IP ; certains équipements d'extrémité client ne supportent pas toujours les paquets IP fragmentés.*
- *Dans le cas d'une encapsulation VPN IPSEC, l'opérateur gère un plan d'adressage IP cohérent pour l'encapsulation des clients. Il s'agit d'éviter des recouvrements d'adresses avec les réseaux IP des clients.*
- *L'authentification d'accès au réseau WiFi proposée par l'opérateur est compatible avec l'utilisation de la solution VPN. Pour cela, l'utilisateur devra s'authentifier sur le portail WiFi avant de lancer son client VPN.*

2.3 Comment identifier le besoin de sécurité ?

2.3.1 Les risques liés à l'usage du WiFi

L'utilisation du « média éther » induit naturellement une présentation et une accessibilité des données échangées dans l'espace public. Cette caractéristique rend possible l'interception des informations par un tiers non identifié.

L'absence de mécanisme de sécurité expose l'utilisateur dès lors qu'il est confronté à une volonté de nuisance. La manifestation de cet état revêt deux dimensions. D'une part, un utilisateur accède en toute bonne fois à une infrastructure WiFi se substituant à celle de son opérateur. Le risque pour l'utilisateur étant de divulguer des informations, confidentielles ou non. D'autre part, il est concevable qu'une personne malveillante s'introduise sur le poste de l'utilisateur. Le risque serait alors d'observer une modification, une destruction ou un vol des données.

Ce bref exposé des risques liés à l'utilisation du WiFi dans un contexte public ne saurait être exhaustif. Il représente toutefois l'essentiel des menaces pesant sur l'utilisateur dans cet environnement.

2.3.2 Sécurité : l'opérateur se sécurise et vous informe

La multiplication des intervenants dans la fourniture des services implique une définition claire des rôles de chacun, pierre angulaire de tout projet de sécurité. Le rôle de l'opérateur WiFi par exemple, est assimilable à un simple transport de données où les contraintes induites par la simplification des accès et leur homogénéité conduisent à une gestion minimaliste de la sécurité.

Concrètement, il s'agit pour l'opérateur de garantir un accès sécurisé à son portail d'authentification et sur ses points d'accès WiFi. Dans cette logique, il protégera l'accès à son réseau et identifiera ses abonnés.

Il revient donc à l'entreprise cliente de répondre à son propre besoin de sécurité que nul autre ne pourra assumer à sa place. Cette prise en charge de la sécurité par l'entreprise n'exonère pas les acteurs du WiFi de leur responsabilité d'information sur la technologie et les risques éventuels de son usage. C'est dans cette optique qu'est rédigé ce Livre Blanc par Wireless Link pour assister les entreprises lors du déploiement de VPN sur WiFi.

2.3.3 Sécurité : l'entreprise intervient

Si le service de connexion aux réseaux WiFi est simple pour l'utilisateur, la mise en œuvre d'applications sur les technologies WiFi dans un mode de fonctionnement optimal ne laisse pas de place à l'improvisation.

Cette mise en œuvre respectera les deux postulats suivants:

- *L'entreprise dispose d'une politique de sécurité formalisée et respectée.*
- *Le système d'information de l'entreprise est adapté.*

Le respect de ces deux points ne doit évidemment pas conduire à la remise en question de l'utilisation du WiFi dictée par des considérations dogmatiques autour de la sécurité « sacro-sainte » ou de l'architecture « idéale » du réseau. Il s'agit simplement de décrire ce que l'on va mettre en œuvre en termes de sécurité et d'architecture de réseau et de respecter certains usages pour écarter les risques et éviter les désillusions.

2.3.3.1 Une politique de sécurité formalisée et respectée

Nous venons de le voir, il appartient à l'entreprise d'assurer la sécurité des échanges de ses utilisateurs nomades. Analyser les risques et positionner à une juste valeur les niveaux de sécurité requis, constituent l'enjeu d'une stratégie de sécurité de l'information.

La méthodologie conduit alors à l'évaluer au moyen de cinq critères dits DIC-P :

- *Disponibilité : Elle permet d'évaluer la permanence de l'accès aux données ou aux processus.*
- *Intégrité : Elle qualifie le contrôle de toute création, modification ou destruction des données ou des processus.*
- *Confidentialité : Elle permet de connaître et maîtriser la visibilité et la capacité d'accès à l'information.*
- *Conformité : Elle établit les bases légales dans lesquelles l'entreprise exerce son métier. Il s'agit pour l'essentiel du respect des législations nationales et internationales.*
- *Preuve : Elle permet de mesurer et de mettre en évidence tout changement intervenu sur des données ou des processus.*

L'évaluation des critères par l'entreprise ne doit pas exclure les risques liés aux pratiques des utilisateurs nomades.

2.3.4 Un Système d'Information adapté

Parmi les différents constituants inclus dans le périmètre informatique, le maillon faible ne doit pas être le poste nomade. Il conviendra de le doter d'outils afin de garantir son intégrité et la confidentialité d'accès aux informations qu'il contient, par exemple :

- *Contrôle d'accès par mot de passe :*
  Les mots de passe seront « complexes », renouvelés fréquemment de façon automatique (éviter les mots de passe perpétuels).
- *Sauvegarde des données :*
  Penser à la synchronisation automatique des fichiers du poste de travail lors du retour de l'utilisateur nomade en entreprise.
- *Chiffrement des fichiers :*
  La sécurité du poste de travail pour les utilisateurs nomades s'entend aussi en terme de vol ou de « casse » de matériel.

Par ailleurs, le transport des données sur des réseaux publics n'est pas accompagné de protection globale. Il est donc impératif d'envisager l'utilisation d'une protection de bout en bout.
Les solutions VPN répondent parfaitement aux exigences d'intégrité et de confidentialité.

2.4.1 La sécurité du WiFi

Arrêtons nous un instant sur les éléments techniques intrinsèques à la technologie WiFi qui permettent une mise en œuvre de la sécurité.

Le WiFi est entré dans le cercle vertueux de la sécurisation depuis le début de son développement. Le groupe de travail 802.11 de l'IEEE a intégré depuis l'origine des éléments de sécurité dans les réseaux sans-fil.

Les évolutions implémentées ont pour conséquence une amélioration de la sécurité sur 2 axes principaux :

Année de ratification	*1999-2000*	*2001*	*2003*	*2004*
	Évolution de la sécurité WIFI			
Norme/standard de sécurité	WEP	802.1x	WPA (TKIP, WEP2)	802.11i
Bénéfices	Chiffrement des échanges sur la partie radio	Authentification de l'accès à l'infrastructure WIFI	Amélioration de la gestion des clés de chiffrement	Normalisation des évolutions. Gestion des clés de chiffrement et algorithmes (AES)

Fig 2 : Evolution de la normalisation de la sécurité du WiFi

- *Renforcement de la sécurité des échanges sur l'interface radio du WiFi (WPA2, TKIP, 802.11i). Le décryptage des échanges est rendu plus difficile, voire impossible.*
- *Limitation des intrusions sur les accès WiFi (802.1x).*

Pour conclure ce survol de la standardisation de la sécurité sur WiFi, on notera que l'utilisation - même pertinente - de ces seuls éléments de sécurité ne peut suffire pour garantir le niveau de sécurité attendu.

2.4.2 Qui implémente cette sécurité ?

Pour comprendre les enjeux, il est intéressant de se poser la question de la destination de ces éléments de sécurité :

- *A quoi servent-ils ?*
  Ils permettent de diminuer les risques d'intrusion sur les réseaux WiFi (802.1x par exemple).
- *Sur quel périmètre agissent-ils ?*
  Ils apportent un premier niveau de sécurité sur le transport des flux entre le poste de travail WiFi et le point d'accès WiFi mais jamais au-delà (WPA par exemple).

Le déploiement de réseaux WiFi internes à l'entreprise (salles de réunion, bureaux ouverts, espaces d'accueil…) s'accompagnera d'une mise en œuvre aisée de tous les mécanismes de sécurité cités précédemment. L'entreprise maîtrise en effet pleinement son périmètre interne et peut configurer « facilement » ces paramètres de sécurité WiFi sur son infrastructure (postes de travail et points d'accès).

Les opérateurs ne peuvent pas travailler la sécurité (notamment sur WiFi) dans cette même logique. S'ils ont la possibilité de mettre en œuvre des éléments de sécurité WiFi existants et robustes sur leurs réseaux, des questions se posent pour leurs clients : les opérateurs doivent se plier à loi du nombre et à l'hétérogénéité des configurations rencontrées sur le terrain :

- *Comment garantir le support de 802.11i ou de 802.1x, par exemple, sur le poste de travail d'un utilisateur ?*
- *Comment offrir un service d'accès simple et universel (tous types de terminaux), pour des utilisateurs a priori sans compétences techniques ?*

En guise de conclusion, on conviendra qu'il n'y a pas de plus petit dénominateur commun possible, en matière de sécurité WiFi, qui puisse être mis en œuvre facilement par l'opérateur pour répondre à toutes les problématiques spécifiques des entreprises clientes. Cette impossibilité pour les opérateurs de mettre en place des solutions de communication fortement sécurisées impose donc à l'entreprise le déploiement d'outils VPN.

Note :

Dans un autre domaine de l'implémentation du WiFi, et pour faire le parallèle avec les aspects de sécurité, on constate que les opérateurs proposent des accès sur la bande de fréquence et de débit 802.11b. Cette contrainte s'est naturellement imposée à eux car tous les terminaux ne supportent pas la norme 802.11a ou la nouvelle norme 802.11g.

2.4.3 La notion de VPN en pratique

2.4.3.1 Quelques définitions

La notion de VPN existe depuis l'utilisation de réseaux publics mutualisant des connexions à caractère privé (notion de groupe fermé d'abonné). Cette notion a pris une toute autre dimension avec l'arrivée de l'Internet et de son cortège de préoccupations sécuritaires. Aujourd'hui l'approche VPN est associée à la notion de chiffrement des échanges entre deux points d'Internet. Dans ce contexte, la technologie VPN IPSec prédominait jusqu'à ce jour en terme de part de marché. Ce développement et cet usage illustre plus le besoin de confidentialité que le besoin de sécurité « communautaire ». Beaucoup d'entreprises l'ont néanmoins adoptée et l'utilisent dans le cadre de sa définition initiale : Internet est le réseau de transport public et IPSec l'élément « virtualisant » du réseau de l'entreprise.

Nous parlerons dans ce cas d'un « VPN de sécurité » lorsque cette notion matérialise un réseau privé respectant les hypothèses suivantes :

- *Le transport chiffré des données d'un point à un autre du réseau garantit une confidentialité des données. Les clés de chiffrement appartiennent à l'entreprise*
- *Les accès logiques à l'entreprise ne sont possibles que dans la mesure où les clés présentées (mots de passe statiques ou dynamiques, certificats, etc.) sont reconnues comme valides et non compromises par l'entreprise.*

L'accès au SI depuis un point d'accès WiFi s'inscrit dans une démarche globale d'accès à distance au système d'information. La préoccupation de l'entreprise est de donner un accès élargi et contrôlé au SI.

Cet élargissement sous-tend en fait deux modes d'accès :

- *L'accès distant :*
  Les moyens techniques sont maîtrisés par l'entreprise : le poste de travail et les solutions de sécurité (l'utilisateur dispose de son PC portable et son client VPN par exemple). Le réseau de transport, s'il n'est pas maîtrisé par l'entreprise, est au minimum connu.

- *L'accès nomade banalisé :*
  Les moyens techniques ne sont pas maîtrisés par l'entreprise : le poste de travail dit banalisé peut être un kiosque Internet, un PC en salle de conférences,… Les moyens de sécurité locaux peuvent être très aléatoires. Ce mode d'accès (même s'il a tendance à se développer) concerne moins les utilisateurs d'accès WiFi, abonnés à un service opérateur.

D'un point de vue sécurité du SI, il apparaît que dans le premier cas une certaine maîtrise existe (sécurité du poste de travail, accès à l'entreprise). Dans le second cas, seule l'interface avec le SI propose des éléments de sécurité.

En résumé…

Technologie éprouvée, le WiFi public met en scène de nombreux acteurs du transport de l'information regroupés au sein de l'association Wireless Link pour unifier les règles d'utilisation. Les opérateurs adhérents de Wireless Link définissent les mécanismes d'interopérabilité destinés à faciliter l'accès banalisé pour les usagers. La sécurité apportée par les opérateurs porte uniquement sur la protection des réseaux et l'identification de l'usager. Toutes les autres composantes de la sécurité modélisée (Disponibilité, Intégrité, Confidentialité, Conformité et Preuve) doivent être gérées par l'entreprise. La mise en œuvre des techniques VPN prend en charge les dimensions Intégrité, Confidentialité et Conformité de ce modèle.

3

LA MISE EN ŒUVRE CONCRETE DE VPN SUR WIFI

3.1 Les éléments à prendre en compte

Dans la logique de déploiement d'une solution VPN, les points importants sur lesquels les préoccupations des entreprises vont se porter sont liés aux techniques utilisées, aux usages ainsi qu'à l'ergonomie de la solution. La capacité d'assister les utilisateurs peut aussi conditionner des choix techniques ou organisationnels. Pour intégrer ces inconnues dans l'équation, et, avoir une maîtrise du résultat, il est important d'opérer des choix en tenant compte d'éléments techniques.

Sans être exhaustif, voici les questions auxquelles tente de répondre un décideur informatique lorsqu'il doit choisir une solution technique :

• La solution technique de VPN à déployer existe-t-elle déjà l'entreprise ?

Si oui, répond-elle partiellement ou totalement au besoin ? Doit-elle être mise à jour ou complétée pour assurer ses nouvelles fonctions ?
Dans la négative, les éléments à déployer répondront-ils totalement à la problématique d'accès distant ?

• Quels risques seront couverts par une mise en œuvre de VPN ?

La mise en œuvre de VPN doit couvrir tous les risques liés à la problématique d'accès et de transport sur WiFi (confidentialité et intégrité des données échangées).

• Le choix du réseau est-il générateur de limitations ?

Non, l'utilisation de réseau de transport WiFi ne conditionne pas le choix d'une solution VPN propre à tel ou tel éditeur ou équipementier, par ailleurs, la solution VPN déployée peut être agnostique du type de réseau traversé et se comporter efficacement sur d'autres moyens de télécommunications (UMTS, GPRS, EDGE, xDSL …).

3.1.1 Partir d'une solution existante ?

La pénétration d'Internet comme moyen principal d'échange dans le tissu économique global (partenaires, clients et employés…) a d'ores et déjà amené les entreprises à utiliser des solutions techniques sur lesquelles il est possible de capitaliser.

Pour l'essentiel, il s'agit de plateformes de sécurité :

- *Les pare-feux (ou firewalls) :*
  Leur fonction initiale les destine au filtrage de flux. Ils peuvent toutefois être utilisés pour fournir des services VPN. Ils concentreront dans ce cas les connexions VPN.

- *Les passerelles VPN/IPSec :*
  Leur vocation première les positionne en tant que système d'interconnexion VPN avec les sites distants. Il s'agit dans ce cas de connexions permanentes. Par extension, elles peuvent supporter les connexions distantes des utilisateurs distants WiFi.

- *Les passerelles VPN/SSL :*
  Il s'agit de l'évolution technologique la plus novatrice dans le domaine de l'accès à distance aux systèmes d'information. Bâties sur la base de la technologie SSL, ces plateformes permettent un accès depuis tous types de postes de travail, qu'ils soient maîtrisés ou non par l'entreprise pour tous types d'applications.

- *Les serveurs d'accès distants :*
  Ils sont nativement utilisés pour concentrer les connexions d'utilisateurs distants et disposent pour la plupart de modems RNIS ou RTC. Leur conception et leur positionnement dans l'architecture du SI ne leur permettent pas d'intégrer des fonctions VPN suffisamment évoluées (ex : pas de chiffrement).

- *Les serveurs Web (Extranet):*
  Disposés en première ligne sur Internet pour fournir de l'information en ligne aux collaborateurs ou partenaires de l'entreprise, ils peuvent, le cas échéant accueillir des applications avec un niveau de sécurité satisfaisant (HTTPS).

3.1.2 Comment assurer une juste couverture des risques ?

Le déploiement de solutions VPN doit être l'occasion de mener une réflexion pragmatique autour de la sécurité du système d'information, notamment autour de deux notions jugées essentielles :

- *La sécurité du poste de travail :*
  - → *Protection des données brutes: chiffrement des données des disques durs et des médias amovibles,*
  - → *Protection contre les vulnérabilités du système d'exploitation et des applications du poste de travail : Pare-Feu personnel,*
  - → *Le maintien en conformité du poste de travail (outils de sécurité présents, mises à jour logiciels, etc.),*
  - → *Neutralisation des codes malicieux (virus, vers, spywares, …) : anti-virus, anti-spyware.*

- *La sécurité d'accès :*
  - → *Protection de l'accès au SI : système d'authentification basée sur le couple identifiant /mot de passe ou sur une authentification forte.*
  - → *Gestion des autorisations (offrir un accès restreint aux utilisateurs lors d'accès en mode nomade) : pare-feu périmétrique, serveur Extranet limité, passerelle VPN filtrante.*

3.1.3 Quelles solutions déployer pour les nomades ?

Les solutions qui s'offrent au DSI pour fournir des services d'accès au système d'information de l'entreprise se déclinent en deux technologies largement développées :

- *VPN IPSec :*

Nativement conçu pour sécuriser IPv6, IPSec a été repris par l'IETF pour sécuriser les architectures IP (V4, c'est-à-dire l'IP utilisé actuellement sur Internet) dans les années 90.

IPSec intègre deux modes de paramétrage :

→ Mode AH: authentification et intégrité des données échangées uniquement.

→ Mode ESP : Authentification, intégrité et chiffrement des données.

L'utilisation d'IPSec n'a pas d'incidence sur les applications transportées (IP, TCP, UDP).

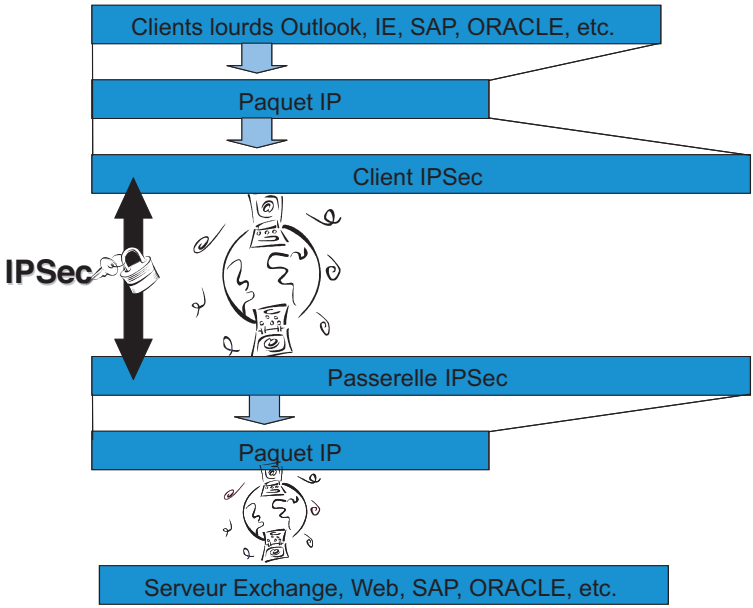


Fig 3 : Applications communicantes sécurisées par IPSec

• VPN SSL :
Développé par Netscape™ puis repris par l'IETF , SSL permettait à l'origine de répondre à la problématique de sécurité des sites Web.

Plusieurs sessions de protocoles sont établies lors de l'établissement de la connexion SSL :

→ Authentification du serveur,
→ Validation du certificat X509 du serveur,
→ Demande de certificat au client distant pour authentification réciproque (ce paramétrage est optionnel),
→ Négociation des clés symétriques de chiffrement.

La technologie SSL autorise la traversée transparente des pare-feu et permet une interface naturelle avec les applications « webisées » (agnostique vis-à-vis du navigateur et du poste de travail utilisé).

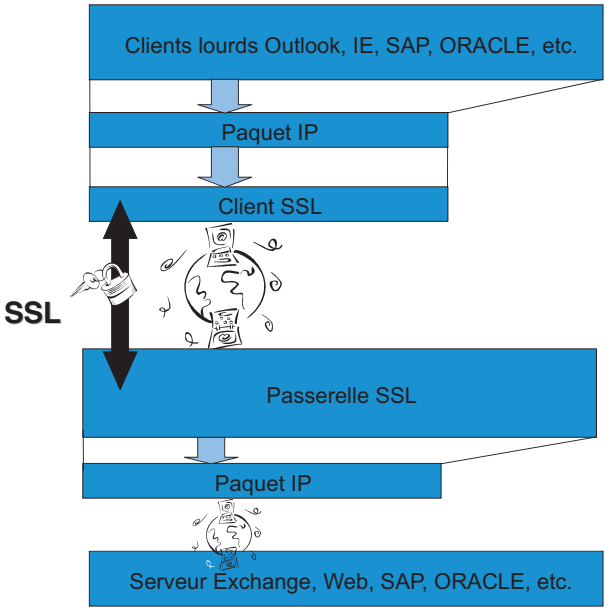


Fig 4 : Applications communicantes sécurisées par SSL

3.2.1 Guide de déploiement

3.2.1.1 Démarche de mise en œuvre de la solution

Il s'agit ici d'identifier les phases techniques et organisationnelles du déploiement.

- *Décrire la matrice des flux :*
  - → *Procéder à l'identification de la qualité des flux en provenance des postes nomades (ERP, Web, Messagerie, …)*
  - → *Etablir la cartographie de ces flux : machines de destination et sens de communication (adresse(s) IP, adresse(s) des sous-réseaux, …)*

- *Mettre en œuvre les règles afférentes sur les équipements :*
  - → *La passerelle VPN est préalablement installée dans la zone de sécurité logique adéquate (DMZ).*
  - → *Les règles du pare-feu sont adaptées :*
    - ◗ *ouverture des ports TCP/UDP en provenance des adresses IP du VPN vers les serveurs internes,*
    - ◗ *mise en œuvre des fonctions de prévention d'intrusion pour analyser les flux entrants.*
  - →*Les serveurs applicatifs sont configurés pour accepter les connexions des nomades :*
    - ◗ *Routage IP cohérent pour les paquets IP retour,*
    - ◗ *Configuration des éléments de sécurité du serveur pour autoriser les connexions nomades (TCPWRAPPER, compte de connexion, journaux d'événements, …).*

- *Configurer la gestion des identités et des droits pour les utilisateurs distants :*
  - → *Gestion des authentifications :*
    - ◗ *Basée sur l'annuaire de l'entreprise (Active Directory®, NDS®, LDAP, RADIUS, …).*
    - ◗ *Association du moyen d'authentification dans ce mode d'usage (authentification forte par calculette ou certificat).*
  - → *Gestion des autorisations :*
    - ◗ *Positionnement de l'utilisateur dans le groupe des utilisateurs nomades.*
    - ◗ *Affectation des droits sur les applications et les ressources*

• *Configurer la passerelle VPN IPSec ou SSL :*

→ *Mettre en œuvre les fonctions nécessaires au support des équipements qui translatent les adresses IP d'origine (encapsulation du trafic dans un trafic TCP ou UDP).*

→ *Configurer les services DNS pour les postes des utilisateurs distants (capacité de résoudre des noms de domaine internes).*

→ *Pour simplifier le routage IP de l'entreprise, attribuer une adresse IP interne au flux IP entrant (les paquets IP sortants de la passerelle VPN obtiennent une adresse IP locale à l'entreprise).*

→ *Mise en œuvre des filtres IP ou applicatifs (réduire la vision du système d'information pour le poste de l'utilisateur distant).*

→ *Définir les règles de sécurité respectées par le poste de travail de l'utilisateur distant avant l'établissement de la connexion (test de la mise à jour de l'anti-virus, test de la présence d'un pare-feu personnel, présence d'un spyware, …).*

→ *Définir la granularité des événements système et de sécurité à journaliser (localement sur le disque ou vers un serveur SYSLOG/SNMP).*

3.2.2 Parenthèse technique, fenêtre ouverte sur la technologie

Il est important pour les hommes de l'art d'avoir une vue globale des divers aspects que recouvrent le choix d'une solution VPN (IPSEC, SSL, L2TP, …).

Nous présentons ci-après un descriptif des aspects à ne pas négliger avant, pendant ou après le déploiement.

3.2.2.1 Problématique d'authentification

Le moyen d'authentification des utilisateurs distants dépend du niveau de sécurité que l'entreprise exige. Il est, par exemple, recommandé d'utiliser une authentification forte de type carte à puce avec certificat, biométrie, calculette (pour rappel : une authentification forte est une authentification à deux facteurs basée sur la combinaison d'un élément connu et d'un élément détenu par l'utilisateur). L'authentification forte poursuit donc un double but : s'assurer que la personne qui se connecte est bien celle qu'elle prétend être et effectuer un mode d'authentification qui satisfasse un critère minium de sécurité.
L'authentification certificat requiert que la solution VPN soit au moins compatible avec PKCS#12 (interface d'accès au certificat et à la clé privée d'un utilisateur) dans le cadre d'utilisation de carte à puce, y compris sur le port USB.

3.2.2.2 Gestion des utilisateurs

Avant tout déploiement, on se pose souvent la question de savoir quels profils d'utilisateurs sont présents dans l'entreprise. Ces profils conditionneront les droits d'accès des utilisateurs (commercial, informatique, VIP, …). Ces profils sont souvent statiques. Il convient de définir une politique d'accès qui ne soit pas figée (lorsque la technologie le permet) : en effet, un même utilisateur qui se connecte depuis son accès Internet sur une machine sans antivirus ne doit pas avoir les mêmes droits que lorsqu'il se connecte depuis une machine qui est conforme à la politique de sécurité du système d'informations. De même, si cet utilisateur se connecte avec une authentification forte, il aura accès à tout le système d'informations. S'il utilise un simple mot de passe il ne pourra voir que certains serveurs non critiques.

Associée à l'authentification des utilisateurs, la gestion des profils détermine leurs autorisations d'accès. Ces dernières définissent les droits de l'utilisateur sur le système d'information. L'entreprise équipée d'une base d'utilisateurs structurée (annuaire LDAP, Active Directory™, Radius, …) dispo-

sera d'une solution de gestion des identités complète et performante si le produit VPN retenu l'exploite efficacement.

3.2.2.3 Problématique des clients nomades

La plupart des pare-feux dits «stateful» créent une session virtuelle pour les paquets UDP, donc pour les connexions VPN. Cette session UDP n'a qu'une durée limitée. En absence de trafic entre le client et la passerelle durant un laps de temps important, les paquets échangés risquent d'être arrêtés par le pare-feu. Il est donc important d'utiliser les fonctionnalités de la passerelle et du client qui permettent d'effectuer un « keep alive » entre eux. De la même manière, le trafic depuis les clients est généralement translaté (modification de l'adresse réseau d'origine). Afin de garder la même translation tout au long de la session VPN, il est nécessaire d'envoyer régulièrement des paquets pour maintenir la connexion. DPD (Dead Peer Detection) est une fonctionnalité implémentée par certains clients VPN qui permet de s'assurer que chaque partie est toujours active.

3.2.2.4 Sécurité des postes

Dans le cas du VPN SSL, il est impératif de ne laisser aucune trace sur le poste utilisateur (mot de passe, fichier temporaire, cookie, …). Il convient implémenter une fonction d'effacement des fichiers temporaires. Cet outil fourni par les éditeurs de passerelle VPN SSL assure la confidentialité des informations, l'absence de keylogger, le chiffrement des fichiers téléchargés et la suppression des fichiers temporaires, pour l'essentiel.

Les solutions des éditeurs VPN permettent actuellement d'interagir fortement avec le poste. L'intégration de la notion de mobilité et des problèmes qu'elle induit doit amener l'entreprise à utiliser toutes les fonctionnalités assurant la conformité du poste de ses utilisateurs (anti-virus, processus, clé de registres …)

3.3.1 Comment se connecter à son SI ?

Il est intéressant d'accompagner la présentation des solutions VPN d'accès distants par une étude de la démarche pragmatique à suivre dans leur mise en œuvre.
Parce que chaque situation est particulière, nous évoquerons les quatre cas les plus représentatifs des infrastructures informatiques ou encore des exigences d'une PME :

- *Cas d'une entreprise mono-site possédant un accès à Internet.*
- *Cas de l'entreprise multi-sites interconnectés par un VPN IPSec au travers d'accès Internet.*
- *Cas de l'entreprise multi-sites reliés entre eux par un réseau privé virtuel (VPN de type MPLS par exemple) avec un accès commun à Internet.*
- *Cas d'un groupe composé de multi-entités (type franchisés, filiales ou adhérents) dont chaque site est relié sur Internet.*

3.3.1.1 Entreprise mono-site avec accès Internet

Abordons ces cas d'étude concrets par l'exemple d'une entreprise type PME située sur un site unique. Pour nombre de ces structures, l'informatique ne représente pas une priorité d'investissement mais un outil de travail comme un autre. L'architecture réseau interne est simplement reliée à un accès Internet fourni par un opérateur pouvant lui proposer également des services hébergés d'anti-virus et de pare-feux.

L'enjeu principal pour l'entreprise est d'offrir à ses collaborateurs itinérants un accès à ses ressources sans bouleverser son architecture technique (réseau et postes) et sans imposer des contraintes d'administration élevées. L'autre exigence imposée par la faible maîtrise en interne est la simplicité de mise en œuvre et d'utilisation.

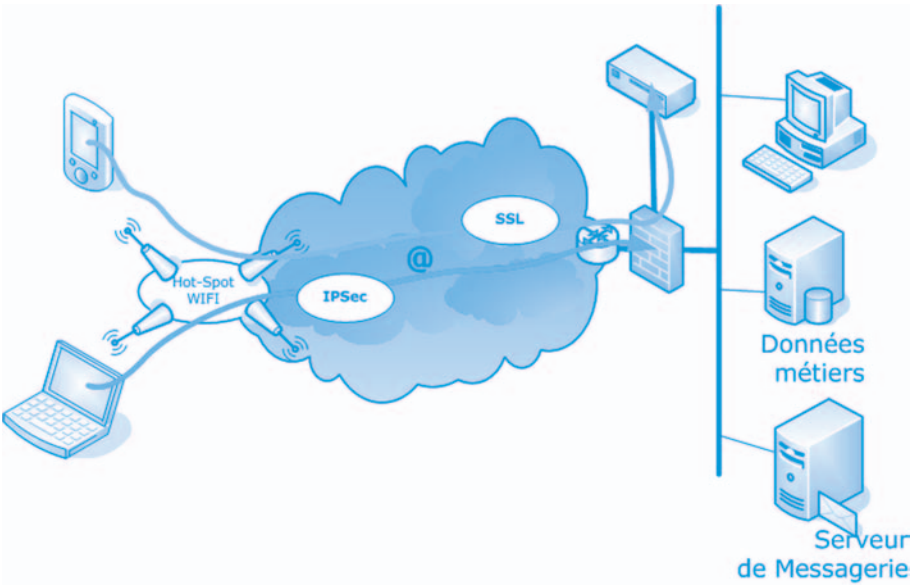


Fig 5 : Connexion depuis un Hot-Spot pour une entreprise mono-site

Cas 1 : Entreprise mono-site avec accès Internet

Périmètre existant, contraintes associées :
- Un accès Internet
- Une sécurité déléguée (pare-feux hébergé ou administré par un tiers)
- Nombre d'itinérants WiFi
- Architecture non dédiée
- Pas de responsable sécurité informatique

Enjeux :
- Intégrer la fonctionnalité VPN avec peu ou pas de maîtrise en interne
- Connexion depuis des postes pas toujours maîtrisés

Pré-requis :
- Définition des usages (bureautique, applications métier, …)
- Implication de l'entité responsable du pare-feu (opérateur, prestataire, …)
- Recours éventuel d'assistance technique (création de nom(s) de domaine(s), paramétrages.

Le choix d'une solution de type SSL plutôt qu'IPSec dans ce cas de figure repose sur les critères suivants :

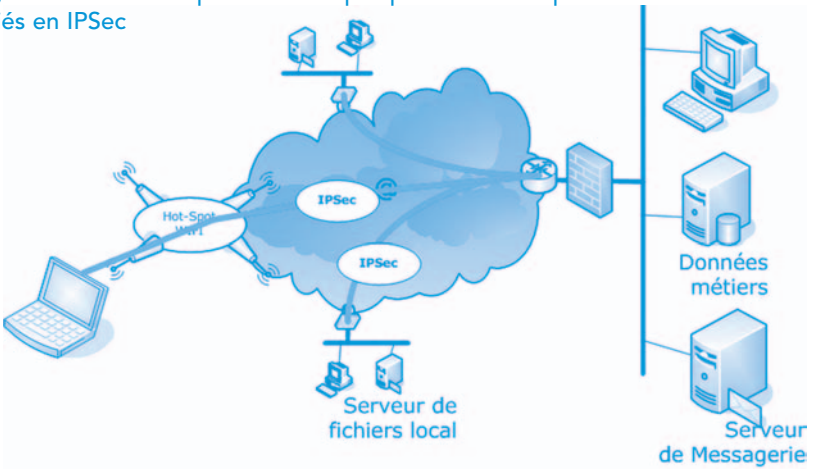
- *Pratique : la forte proportion de connexions depuis des postes non maîtrisés ou en libre service.*
- *Fonctionnel : existence ou usage plus fréquent d'applications « webisées ».*

Le choix d'une solution de type IPSec plutôt que SSL dans ce cas de figure reposera quant à lui sur les critères suivants :
- *Technique : le pare-feu installé supporte la fonction VPN IPSec*
- *Positionnement de marché : antériorité des solutions IPSec*

3.3.1.2 Entreprise multi-sites reliés en IPSEC

Ce second cas d'étude présente l'exemple d'une entreprise répartie sur plusieurs sites reliés entre eux par un réseau VPN de type IPSec.
L'enjeu dans ce cas est relativement simple : réutiliser l'architecture sécurisée déjà en place et l'étendre aux utilisateurs itinérants WiFi.

Fig 6 : Connexion depuis un Hot-Spot pour une entreprise multi-sites reliés en IPSec



CAS 2 : ENTREPRISE MULTI-SITES RELIÉS EN IPSEC

Périmètre existant, contraintes associées :
- Un réseau IPSec existant
- Une sécurité maîtrisée (pare-feux gérés par l'entreprise)
- Nombre d'itinérants WiFi
- Architecture dédiée et matrice de connexion (liens entre sites) connue
- Compétence sécurité informatique interne ou externe à l'entreprise

Enjeux :
- Capitalisation sur l'expérience acquise
- Mutualisation / optimisation des coûts

Pré-requis :
- Infrastructure IPSec existante et maîtrisée
- Définition des usages (bureautique, applications métier, …)
- Maîtrise de la configuration des postes de travail.

C'est naturellement une solution IPSec qui est envisagée. L'existence de passerelles reposant sur cette technologie avec le système d'informations permet de s'affranchir de la mise en place «d'ouvertures » supplémentaires.

3.3.1.3 Entreprise multi-sites reliés par VPN MPLS

Ce troisième cas illustre la problématique d'une entreprise qui souhaite relier les utilisateurs itinérants WiFi avec les ressources du système d'informations réparties sur les différents sites. L'interconnexion des sites peut être réalisée au moyen de réseau VPN MPLS, technologie couramment utilisée sur les WANs (Wide Area Networks).

Selon les options de déploiements et d'implémentation, nous avons identifié deux architectures MPLS rencontrées chez les clients.
La première architecture proposée repose sur l'hypothèse de l'exploitation la plus simple du réseau MPLS avec un accès large (type Any to Any dans le jargon opérateur) à l'Internet pour tous les sites. La sécurité étant gérée par l'opérateur et les ressources du Client sur tous les sites.

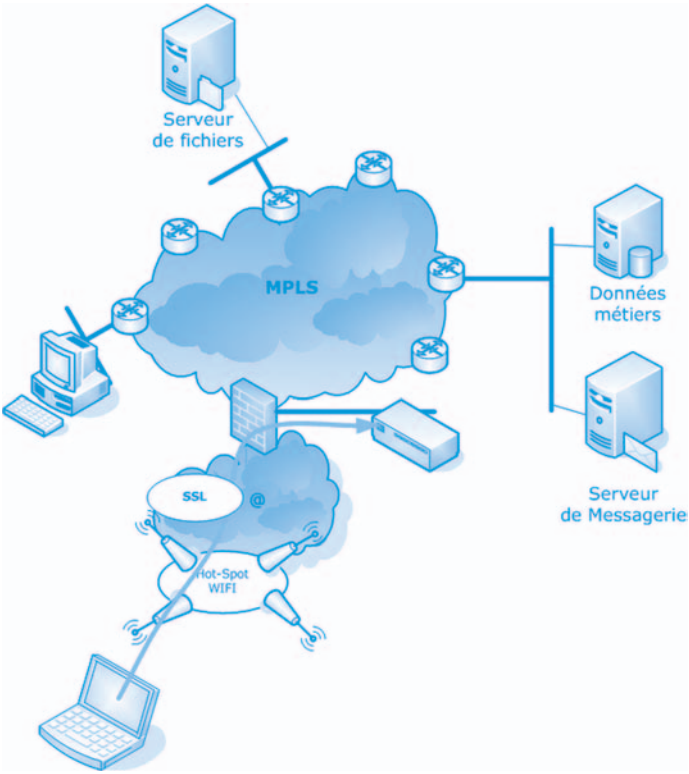


Fig 7 : Connexion depuis un Hot-Spot pour une entreprise multi-sites reliés par VPN MPLS, scénario « Any-to-Any »

La seconde architecture proposée repose sur l'hypothèse que le seul point de contact entre le client et Internet est son site central. Le client gère la sécurité et ses applications sont centralisées sur le site d'accès.

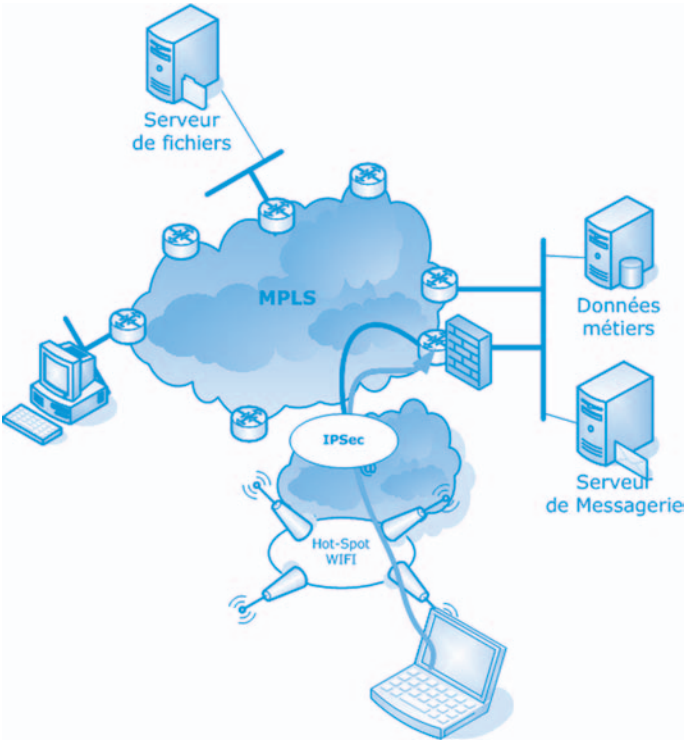


Fig 8 : Connexion depuis un Hot-Spot pour une entreprise multi-sites reliés par VPN MPLS, scénario « Hub and Spoke »

Ce type d'architecture se caractérise par un niveau de sécurisation optimal qu'il convient de préserver lors du déploiement d'accès distants pour les utilisateurs itinérants WiFi.
L'enjeu de ce type de déploiement est simplement de traiter la sécurisation de la connexion du poste itinérant WiFi de l'utilisateur jusqu'au réseau VPN MPLS. Cette sécurisation nécessite la mise en œuvre – au niveau du réseau MPLS- d'une passerelle d'accès (IPSec ou SSL).
Cette passerelle collectera les flux provenant des utilisateurs itinérants WiFi et les acheminera vers le réseau MPLS. On peut ensuite quasiment considérer ce réseau comme un LAN multi-sites disposant les ressources pour l'utilisateur itinérant.

Cas 3 : Entreprise multi-sites reliés par VPN MPLS

Périmètre existant, contraintes associées :
- Un réseau MPLS (Any to any, Hub & Spoke, …)
- Une sécurité optimale (réseau étanche, accès internet centralisé et contrôlé)
- Pare-feux hébergé(s) et administré(s) par l'entreprise ou par un tiers
- Nombre d'itinérants WiFi
- Compétence sécurité informatique interne ou externe à l'entreprise
- Compétence en architecture réseau interne ou externe à l'entreprise

Enjeux :
- Maintien du niveau de sécurité initial,
- Mutualisation / optimisation des coûts

Pré-requis :
- Connaissance du plan de routage IP du réseau VPN MPLS
- Connaissance du modèle de QoS du réseau VPN MPLS
- Définition des usages (bureautique, applications métier, …)
- Maîtrise de la configuration des postes de travail.

3.3.1.4 Entreprise multi-entités reliées à Internet

Ce dernier cas décrit l'exemple d'une entreprise constituée d'entités distinctes (franchisés, filiales, adhérents ….). Chaque entité est reliée à Internet et dispose d'une autonomie dans ses choix techniques et/ou financiers. Les utilisateurs distants de ces entités ont vocation à se connecter avec chacune d'entre elles avec les mêmes outils. La caractéristique représentative de ce type de cas est la grande hétérogénéité des solutions de sécurisation ou de filtrage qui peuvent être employées pour garantir la confidentialité et l'intégrité des flux de communication de chaque entité.

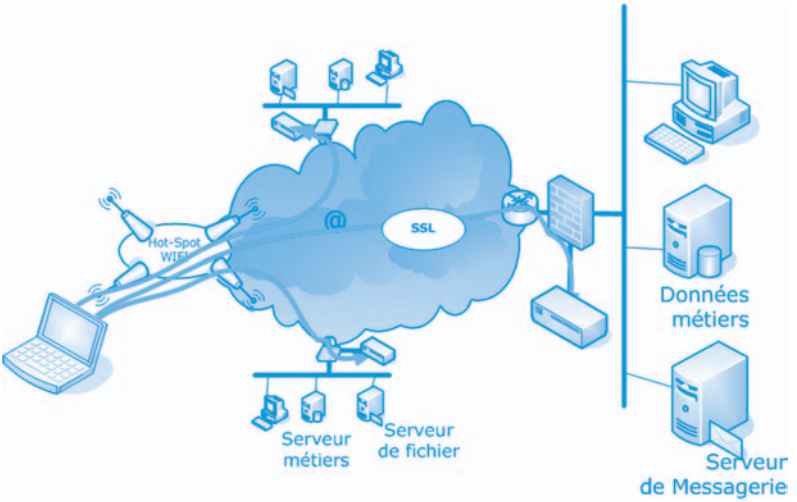


Fig 9 : Connexion depuis un Hot-Spot pour une entreprise multi-entités reliées à Internet

L'enjeu dans ce cas consiste en la mise en œuvre d'un système d'information ouvert permettant l'échange sécurisé de données entre les utilisateurs itinérants WiFi et les sites des différentes entités.
Le caractère universel du mode de distribution et de la mise à disposition des informations conduit naturellement à orienter le choix vers une architecture SSL. On imagine en effet aisément qu'un ensemble d'entreprises désirant fournir des informations de façon structurée à des utilisateurs distants privilégie des outils de communications de masse (portail banalisé, présentation « webisée » des applications) associés à des moyens de sécurité performants, simples à déployer et à utiliser.

Cas 4 : Entreprise multi-entités reliées à INTERNET

Périmètre existant, contraintes associées :
- Un accès à Internet par entité
- Une sécurité maîtrisée par chacune des entités
- Nombre d'itinérants WiFi par entité
- Compétence sécurité informatique interne ou externe à l'entreprise

Enjeux :
- Ouverture des systèmes et partage des informations
- Identification des utilisateurs distants

Pré-requis :
- Présentation d'applications « webisées »
- Système d'authentification des utilisateurs pour chaque entité
- Création de noms de domaine appropriés (un ou plusieurs par entités)
- Achat de certificats d'authentification X509 (un par entité)

Etapes du projet de mise en œuvre :
- Intégration d'une passerelle VPN SSL par entité :
  - → Installation d'une passerelle SSL
  - → Interfaçage avec la base d'authentification des utilisateurs (certificats)
  - → Paramétrage de l'accès aux applications
- Mise à jour si nécessaire des navigateurs sur les postes utilisateurs distants
- Accompagnement de l'utilisateur (au moins un guide d'utilisation commun, une liste des noms et URL des portails, …).

3.3.2 Prendre en compte l'architecture dans la configuration de la solution

Nous venons d'étudier 4 cas d'architecture possibles. En les rapprochant des éléments présentés lors du paragraphe « 3.2.1 Guide de déploiement », voici quelle pourrait être la méthode de déploiement dans chacun des cas :

- Cas 1 : Entreprise mono-site avec un accès Internet :
  - → Intégration d'une passerelle VPN :
    - ◗ Paramétrage IPSec du pare-feu (attention aux offres et aux délais de réalisation du prestataire)
    - ◗ Ou installation d'une passerelle SSL
    - ◗ Paramétrage de l'accès aux applications
  - → Mise à jour si nécessaire des navigateurs sur les postes nomades
  - → Installation des clients (si IPSec) sur les postes nomades
  - → Accompagnement de l'utilisateur (au moins un guide d'utilisation)

- Cas 2 : Entreprise multi-sites reliés en IPSEC
  - → Installation du client VPN IPSec sur les postes
  - → Mise en œuvre de moyens d'authentification :
    - ◗ certificats utilisateurs X509
    - ◗ fourniture de calculette d'authentification (token)
  - → Paramétrage du ou des pare-feux :
    - ◗ Client à site(s),
    - ◗ Configuration selon la matrice de connexion définie
    - ◗ Paramétrage de l'accès aux applications
    - ◗ Accompagnement de l'utilisateur (au moins un guide d'utilisation)

- Cas 3 : Entreprise multi-sites reliés en MPLS
  - → Intégration d'une passerelle VPN (IPSec ou SSL)
  - → Mise à jour si nécessaire des navigateurs sur les postes nomades
  - → Installation des clients (si IPSec) sur les postes nomades
  - → Adaptation éventuelle du plan de routage du VPN MPLS
  - → Intégration des flux des utilisateurs distants dans le modèle de QoS
  - → Accompagnement de l'utilisateur (au moins un guide d'utilisation)

La mise en œuvre de moyens d'authentification forte n'est pas contraignante dans ce type d'architecture (comptabilité des offres IPSec, SSL et MPLS avérée)

- Cas 4 : Entreprise multi-entités reliées à Internet

  → Intégration d'une passerelle VPN SSL par entité :

  - Installation d'une passerelle SSL
  - Interfaçage avec la base d'authentification des utilisateurs (certificats)
  - Paramétrage de l'accès aux applications

  → Mise à jour si nécessaire des navigateurs sur les postes utilisateurs distants

  → Accompagnement de l'utilisateur (au moins un guide d'utilisation commun, liste des noms et URL des portails, …)

3.3.3 Choisir une solution VPN : les pièges à éviter

Le déploiement d'une solution VPN requiert du tact et une bonne procédure de la méthode. Tant dans le processus de choix que dans celui de l'implémentation, le décideur doit tenter de répondre à plusieurs questions.

3.3.3.1 Quels critères techniques de choix ?

1. Quelle interaction du client VPN avec d'autres outils de sécurité du poste de travail ?

L'entreprise est ouverte sur le monde, elle permet aux collaborateurs en situation de mobilité d'accéder à ses ressources. Dans ce contexte, le SI doit savoir si l'on peut faire confiance à la personne et au poste qui se connecte. Il faut donc vérifier différents paramètres avant l'établissement de la connexion VPN avec le site de l'entreprise. Ces éléments sont tels que :

- L'antivirus : installé, actif et à jour,
- Quels processus sont actifs,
- Vérifier l'existence de certaines clés de registre,
- Quel niveau de mise à jour du système d'exploitation,
- Quelle version d'une application,
- etc.

La solution VPN peut vérifier ces éléments et en fonction, autoriser un plein accès aux ressources, ou positionner le poste de l'utilisateur dans une zone dite de quarantaine afin de remédier au(x) défaut(s) constaté(s).

2. Quelle support de l'Internet public ou d'autres réseaux privés ?

Comme nous l'avons vu précédemment, le support de la fonction « NAT traversal » est primordial. Sans son support par la solution VPN la connexion depuis des réseaux publics ou d'autres réseaux privés est impossible.

3. Quelle garantie de l'identité de la personne derrière la connexion VPN ?

Si la solution VPN s'assure de la sécurité du transport, elle ne permet pas à elle seule de garantir l'identité de la personne qui l'utilise. Le support de différents modes d'authentification est donc un point important. La solution VPN retenue doit s'appuyer au moins sur un support pour l'authentification forte :

- PKCS#11 et 12 pour l'usage de moyens externes d'authentification (i.e. carte à puce par exemple),
- Des mots de passe dynamiques (ou hard-token).

4. Quelle gestion technique efficace de la connexion VPN dans un contexte de mobilité ?

L'usage de la connexion pouvant être très sporadique en fonction de l'activité de l'utilisateur et du réseau de connexion, il est donc primordial que la solution VPN propose une gestion technique des connexions. Le support d'un mécanisme tel que DPD (Dead Peer Detection) peut notamment servir :

- Lorsque la connexion VPN de l'utilisateur utilise une adresse IP dynamique,
- Pour maintenir la session VPN dans le cas où le client est « NATé »,
- Afin de conserver une session VPN à travers les pare-feux lorsque le trafic de l'utilisateur est épars,
- Afin de maintenir un tunnel en état ou pour détecter que la passerelle distante est inopérante.

Afin d'offrir une résilience forte des accès au SI, certains clients VPN peuvent basculer vers une nouvelle passerelle VPN pour offrir une forme de redondance des tunnels VPN. D'autres solutions fonctionnent avec leur propre mécanisme dit de « Keep Alive » : Messages IKE vides, ping chiffrés dans le tunnel, …

5. Quelle interopérabilité des solutions VPN entre elles ?

Le choix d'une solution VPN entraîne l'acquisition d'une solution fournissant la partie cliente, installée sur le poste de travail, et une partie serveur/passerelle installée dans le SI. Pour les entreprises multi-sites ou avec des filiales, il est impératif que la solution retenue soit la plus homogène possible pour garantir la connexion des clients vers les différents points d'accès.

3.3.3.2 Comment déployer et maintenir sa solution ?

Déployer un client VPN sur 5 PCs nomades peut se résumer à refaire 5 fois la même installation. Lorsqu'il s'agit d'un parc utilisateur plus important, la question de l'industrialisation du déploiement se pose tout naturellement.

Plusieurs méthodes sont utilisables :

- l'utilisation d'un outil de distribution de logiciel,
- un CDROM,
- la publication sur le site de l'entreprise

Du choix de la méthode dépend la réussite du projet car les utilisateurs ne sont pas toujours coutumiers de l'utilisation d'un client VPN. Il faut donc que l'installation soit facile et qu'un minimum de configuration soit requis. Le mieux est donc d'avoir à disposition un outil permettant autant que possible de simplifier et standardiser l'installation. Ce dernier est fourni par l'éditeur de la solution et permet de réaliser un programme d'installation comprenant déjà tous les paramétrages.

Par ailleurs, nous conseillons aux sociétés utilisatrices de ces solutions VPN d'accompagner le déploiement d'un guide utilisateur. Il est important, pour ne pas dire essentiel, que les utilisateurs itinérants bénéficient d'une forme de support technique.

Le dépannage de la solution doit être aisé tant au niveau du poste de travail que sur la passerelle. Le niveau de détail dans les journaux d'événements et leurs clartés sont donc importants.

En résumé …

L'utilisation de VPN en association avec les réseaux WiFi publics constitue la meilleure garantie de sécurité disponible dans l'état actuel des technologies disponibles. Il ne s'agit pas d'une technique née d'une génération « spontanée », le VPN est déjà adopté par nombre d'entreprises de toutes tailles qui utilisent des accès distants. Si cette technologie est mature, elle continue néanmoins son évolution. Le cortège des solutions de VPN est aujourd'hui tracté par les offres de VPN/SSL. Néanmoins, réduire la vision de la sécurité à la seule protection du « média de transport » réduirait la portée de cette analyse à imposer une amélioration de la sécurité de l'ensemble de la chaîne cinématique en incluant dans cette démarche le traitement des postes de travail de façon globale. L'identification de l'usage, l'évaluation des coûts et la bonne connaissance des capacités de l'entreprise à déployer et exploiter les moyens de sécurité détermineront les choix du décideur en matière de solution et de technologie.

4

GLOSSAIRE

802.11b/g : Norme de communication pour réseaux sans fil. La norme 802.11b autorise des débits de 2.4 Mbits/s dans une bande de fréquence de 2.4 GHz. La norme 802.11g permet d'atteindre un débit de 54 Mbits/s.

802.11i : Standard visant à assurer la sécurité du Wi-Fi en définissant l'usage d'algorithmes de chiffrement (comme AES ou TKIP) pour l'échange des données.

802.1x : Norme permettant d'authentifier un utilisateur souhaitant accéder à un réseau grâce à un serveur d'authentification.

Active Directory : Service d'annuaire de Microsoft. Active Directory permet de gérer les ressources du réseau (données utilisateur, imprimantes, serveurs, base de données, groupe, ordinateurs et stratégies de sécurité.

AES (Advanced Encryption Standard) : Algorithme de chiffrement à clé symétrique, où la clé est la même pour le codage et le décodage. Les longueurs de clé utilisées sont 128, 192 ou 256 bits.

Aggressive Mode : Un des mode utilisé par IKE pour établir des échanges sécurisés entre deux parties. Ce mode permet de réduire le nombre d'échanges lors de l'initialisation.

Any to Any : Architecture VPN où tous les sites peuvent communiquer entre eux.

Cache Cleaner : Logiciel supprimant les informations utilisées par le navigateur web tel que les cookies, les mots de passes, les fichiers temporaires. Il est notamment utilisé lors de l'utilisation d'un VPN SSL.

Cookie : Fichier texte enregistré par un site web sur le disque dur de l'utilisateur, permettant de l'authentifier lors de futures visites.
Les informations que recèle ce fichier servent généralement à personnaliser l'accès au site.

Datagramme : Unité de transmission utilisée par le protocole TCP/IP au niveau IP.

DMZ (Demilitarized Zone / Zone démilitarisée) : Zone tampon d'un réseau d'entreprise, située entre le monde extérieur (Internet) et le réseau interne. On y place généralement des systèmes destinés à échanger avec le monde extérieur, tel que les serveurs http, ftp, smtp ou les systèmes anti-virus.

DNS (Domain Name System) : Service de résolution de noms, adresses et services. Il permet de faire la corrélation entre un nom (exemple: www.wirelesslink.fr) et son adresse IP.

DPD (Dead Peer Detection) : Permet la renégociation des tunnels VPN mal montés ou mal terminés.

EDGE (Enhanced Datarate for GSM Evolution) : Evolution du GPRS permettant des débits utiles de l'ordre de 128 Kb/s.

ERP (Entreprise Resource Planning) : Logiciel de gestion d'entreprise permettant de gérer l'ensemble des processus d'une entreprise, en intégrant l'ensemble des fonctions de cette dernière comme la gestion des ressources humaines, la gestion comptable et financière, l'aide à la décision, mais aussi la vente, la distribution, l'approvisionnement et le commerce électronique.

Firewall, Pare-feu : Système qui permet le passage sélectif des flux de données entre un ordinateur personnel et un réseau, et la neutralisation des tentatives d'intrusion en provenance du réseau public.

GPRS (General Packet Radio Service) : Seconde génération de téléphonie mobile. Elle introduit un routage de l'information par paquets et des usages "data. Les débits utiles sont de 56 Kb/s.

GRE (Generic Routing Encapsulation) : Protocole permettant d'encapsuler d'autre protocole dans IP.

Hot Spot : Point d'accès public Wi-Fi

Https (HyperText Transport Protocol) : Protocole pour l´échange sécurisé de données sur Internet.

Hub & Spoke : Architecture VPN dans laquelle tous les trafics entre différents sites effectuent un rebond sur un site central (Hub) qui analyse le trafic avant de le renvoyer vers sa destination (Spoke).

IETF (Internet Engineering Task Force) : Organisation, sous l´égide de l´IAB, qui définit les protocoles Internet, notamment TCP/IP et HTTP.

IKE (Internet Key Exchange) : Procédure d'échange de clé lors de l'établissement d'un tunnel VPN.

IP, IPv6 (Internet Protocol) : Protocole de transmission de paquets d'information sur les réseaux. IPv6 est le nouveau protocole IP en développement, Les adresses IP sont codées sur 128 bits au lieu de 32 actuellement (IPv4).

IPSEC (Internet Protocol Security) : IPSEC permet de protéger les données sensibles circulant sur un réseau TCP/IP en assurant la confidentialité, l'intégrité et l'authentification de chaque paquet IP circulant sur le réseau.

Keylogger : Programme permettant d'enregistrer dans un journal les séquences de touches frappées au clavier.

L2TP (Layer 2 Tunneling Protocol) : Norme de VPN mise au point par l'IETF en prenant le meilleur de L2F et de PPTP.

LDAP (Lightweight Directory Access Protocol) : Protocole d'accès aux annuaires, ce standard est une version allégée (d'où son nom) du protocole d'accès à l'annuaire X500 pour le monde Internet. Il permet de partager une liste d'adresses au niveau du serveur, une sorte d'annuaire simplifié. C'est le dénominateur commun des principaux éditeurs d'annuaires.

MPLS (MultiProtocol Label Switch) : Protocole utilisant une technique de routage basée sur l'attribution d'un "tag" (ou label) à chaque paquet. Il permet de router les paquets plus rapidement, les routeurs commutateurs n'utilisant que le tag comme information de routage. Ce protocole est totalement indépendant des niveaux supérieurs et inférieurs.

NAT (Network Address Translation) : Système de traduction d´adresses IP entre différents réseaux (en général, entre des réseaux locaux et Internet). Cela permet de masquer des machines ou de traduire des adresses IP non routables en adresses routables.

NAT Transversal : Méthode permettant de palier au problème d'incompatibilité entre le NAT et les VPN en encapsulant les paquets IPSEC dans des paquets UDP.

NDS (Novell Directory Services) : Service d'annuaire de Novell.

OTP (One Time Password) : Mot de passe à usage unique.

OWA (Outlook Web Access) : Extension du serveur Exchange permettant aux utilisateurs d'Outlook d'accéder à leur courrier via un navigateur.

PKCS#11 : Interface type API fourni par un système d'exploitation pour dialoguer avec des éléments de sécurité (i.e. carte à puce) afin de stocker ou d'exploiter les données cryptographiques. PKCS pour Public-Key Cryptography Standards, défini par la société RSA Security Inc.

PKCS#12 : Format de stockage de certificats et de clés privées.

PPTP (Point to Point Tunneling Protocol) : Protocole d'encapsulation PPP sur IP conçu par Microsoft, permettant la mise en place de réseaux privés virtuels (VPN) au-dessus d'un réseau public.

QoS (Quality of Service) : Ensemble d'indicateurs permettant de mesurer la performance d'un réseau.

RADIUS (Remote Authentication Dial-In User Service) : Protocole d'authentification pouvant utiliser de manière décentralisé un serveur d'authentification central.

RNIS (Réseau Numérique à Intégration de Services) : Lignes spécialisées qui autorisent des débits de 64 Kb/s à plusieurs mégabits par seconde.

RTC (Réseau Téléphonique Commuté) : Réseau téléphonique traditionnel. Connexion à une vitesse maximale de 56 Kb/s.

SMS (Short Message System) : Système de messages électroniques instantanés sur téléphones portables.

SNMP (Simple Network Management Protocol) : Protocole de contrôle et gestion d'équipements réseaux.

Spyware : Logiciel qui installe un espion fourni par une société de marketing afin d'analyser vos habitudes. Les informations recueillies sont expédiées sans que vous le réalisiez.

Syslog : Protocole de transmission de messages de notification d'événement.

TCP (Transmission Control Protocol) : Protocole de la couche de transport TCP/IP. TCP fonctionne en mode connecté.

TCP WRAPPER : Outil permettant de contrôler les tentatives de connexion sur une machine.

TKIP (Temporal Key Integrity Protocol) : Protocole de chiffrement de données qui génère régulièrement de nouvelles clés dynamiques. Le protocole TKIP effectue également un contrôle de l'intégrité des données échangées.

Token, soft token, hard token : Système fournissant un mot de passe dynamique. Ce système peut être matériel (hard token) ou logiciel (soft token).

UDP (User Datagram Protocol) : Protocole de la couche de transport TCP/IP. UDP fonctionne en mode déconnecté. Il n'assure pas la délivrance des paquets à leur destinataire.

UMTS (Universal Mobile Telecommunications System) : Troisième génération de téléphonie mobile. Permet d'atteindre des débits de 2 Mb/s.

VPN (Virtual Private Network ou Réseau Privé Virtuel) : Technologie recréant au travers d'Internet une connexion sécurisée au réseau d'entreprise.

VPN SSL : VPN basé sur la technologie SSL (Secure Socket Layer). SSL est un protocole destiné à négocier un échange de clé entre un serveur et un client afin de mettre en place un tunnel chiffré via un algorithme symétrique.

WEP, WEP2 (Wired Equivalent Privacy) : Protocole développé pour le chiffrement des trames 802.11, censé fournir aux réseaux sans fil une protection comparable aux réseaux câblés. Le WEP2 est le successeur du WEP qui a montré de nombreuses failles.

WiFi (Wireless Fidelity) : Non commercial pour la technologie IEEE 802.11b de réseau local Ethernet sans fil (WLAN), basé sur la fréquence 2.4 Ghz. Les constructeurs informatiques intègrent de plus en plus cette tech-

nologie sans fil dans leurs produits pour des utilisations chaque jour plus nombreuses (communication, réseau, pda…).

WPA (Wireless Protect Access) : Norme WiFi améliorant la sécurité sur les réseaux sans fil par une modification des techniques de chiffrement et la mise en oeuvre de changements dynamiques de clé lors des Sessions.

X509 : Format des certificats d'identité recommandé par l'Union Internationale des Télécommunications (UIT).

xDSL (Digital Subscriber Line) : Technologie permettant de transmettre de données à haut débit sur des réseaux en cuivre. Il existe différentes variantes de DSL, d'où le sigle xDSL pour désigner l'ensemble de ces technologies comme l'ADSL (A pour Asymetric).

Wireless Link
55, rue Sainte Anne
75002 PARIS

www.wirelesslink.fr

Demandes d'informations :
contact@wirelesslink.fr

Tél. 01 42 44 44 74

Fax. 01 42 44 44 75