Le Livre Blanc du VPN

Les enjeux et les bénéfices du VPN pour les Entreprises

Partie Conseil réalisée par le cabinet CESMO

Le Livre Blanc du VPN

édité à l'initiative d'isdnet

Textes

Pour CESMO : Raùl Rojas
Emmanuel Richard

Pour isdnet : Mylène Veillet
Ismaïl Diedhiou

SOMMAIRE

Les Enjeux et les bénéfices du VPN pour les Entreprises

L'offre IP-VPN isdnet

I. Comprendre les enjeux : de l'entreprise à la communauté d'intérêt

I.1 Nouvelle Économie, Nouvelles Exigences

L'entreprise doit aujourd'hui faire face à une véritable révolution. Plus que jamais, elle doit faire preuve de réactivité et de flexibilité face aux attentes de ses clients et aux menaces de la concurrence. Dans ces conditions, il est primordial de développer les échanges et le travail collaboratif au sein de l'entreprise, certes, mais également entre l'entreprise et ses partenaires privilégiés que sont les fournisseurs, les sous-traitants et bien sûr les clients. L'efficacité des échanges, qu'ils soient internes ou entre l'entreprise et ses partenaires, passe par la mise en œuvre d'une solution de communication globale, rapide et fiable.

L'enjeu est d'autant plus important que le personnel des entreprises se doit d'être de plus en plus mobile et que le télétravail s'affirme chaque jour davantage dans le monde professionnel.

Les commerciaux, les dirigeants ou responsables opérationnels qui réalisent de nombreux déplacements, les experts et les techniciens en mission chez vos clients, les employés qui souhaitent pouvoir travailler depuis leur domicile,... tous ces employés ont besoin d'accéder aux ressources de l'entreprise et de communiquer avec leurs collaborateurs, où qu'ils se trouvent.

Prenons l'exemple d'un commercial, qui doit s'absenter fréquemment de son bureau pour démarcher de nouveaux clients : il est vital pour son activité qu'il soit informé en temps et en heure des évolutions de produits et de prix, et qu'il puisse transmettre des contrats à sa direction pour validation, …

L'enjeu est aujourd'hui de garantir à tous ces employés des conditions d'accès à l'information et de communication optimales, pour leur permettre de réaliser, à distance, les mêmes objectifs que n'importe quel autre employé à l'intérieur de l'entreprise.

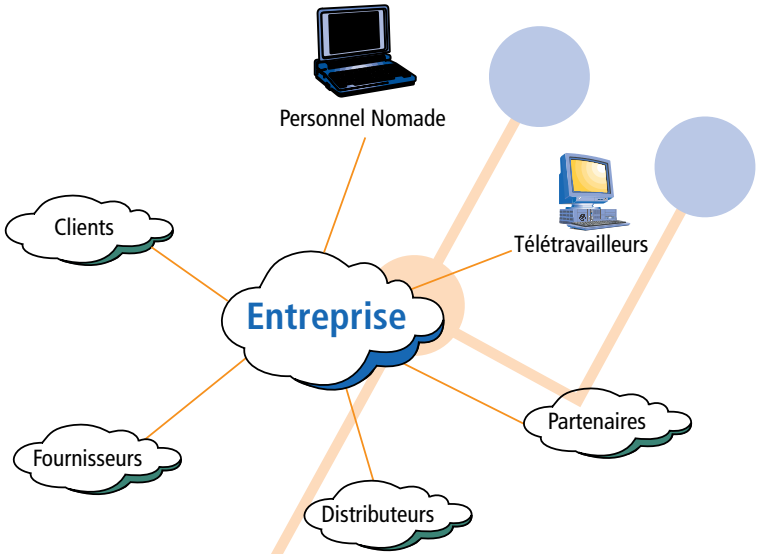
Pour répondre à ces défis, l'entreprise doit se doter de moyens de communication adaptés, qui doivent répondre en particulier aux objectifs suivants :

- Permettre à un employé d'accéder au système d'information de l'entreprise indépendamment du lieu où il se trouve;
- Rendre possible l'accès au système d'information pour des personnes extérieures à l'entreprise, et ce, de manière sécurisée;
- Fournir une grande richesse de fonctionnalités et une excellente qualité de transmission pour réaliser à distance des échanges aussi performants que ceux réalisés en local .

I.2 L'entreprise au cœur d'une communauté d'intérêt

Dans un univers où la réactivité s'affirme comme un élément-clé de la réussite, l'entreprise a besoin de s'ouvrir et de communiquer de manière efficace avec ses partenaires. L'enjeu pour elle est de constituer une véritable **communauté d'intérêt,** regroupant les fournisseurs, les partenaires, les distributeurs et bien sûr, les clients.

Bref, la communauté d'intérêt est engendrée par la présence de différents acteurs économiques sur un même business, à des positions différentes dans la chaîne de valeur, et animés d'une volonté commune de développer ce business par le développement de synergies plus grandes entre eux.



Au sein de cette communauté, votre entreprise doit jouer un rôle déterminant : posséder une vision complète des activités présentes sur l'ensemble de la chaîne de valeur et tout mettre en œuvre pour développer les synergies entre elles.

Prenons l'exemple d'un constructeur automobile. Autour de lui gravite un grand nombre d'entités ayant des métiers différents mais connexes. Ces entités interviennent dans l'activité du constructeur à différents niveaux : la recherche et développement, les études de marché, la conception du produit, le maquettage, la fourniture de matières premières, la fabrication de pièces détachées, la réalisation de tests, le marketing et la publicité, la mise en place des usines d'assemblage, le transport des automobiles et leur stockage, la distribution et la vente, la maintenance et réparation et d'autres services d'après-vente, l'assistance juridique… Chacun d'entre eux interagit avec le constructeur et

s'intègre à sa communauté d'intérêt de manière différente. Pour sa part, le constructeur est responsable de la définition, de la coordination et de l'optimisation des interventions de chaque acteur.

I.3 Les communications, un élément clé

Les objectifs à atteindre par la communauté d'intérêt dépendent du contexte propre à votre entreprise et à votre métier. Toutefois, il est important que votre entreprise soit consciente que la réalisation de ces objectifs passe par une organisation efficace des échanges à l'intérieur de la communauté. Si l'on va encore plus loin dans cette réflexion, force est de constater que la communauté d'intérêt ne peut exister que si elle met en place les outils permettant à tous ses membres d'accéder à des ressources partagées, de communiquer et de travailler ensemble indépendamment de leur localisation.

En effet, le partage de l'information est un facteur de productivité essentiel tant à l'intérieur de l'entreprise que dans le cadre d'une collaboration avec vos partenaires. Mais il ne permet pas de diriger tous les efforts de la communauté d'intérêt vers un objectif commun. La coordination des activités est également un facteur d'efficacité important. Ceci implique la mise en place d'une solution de communication globale, intégrant des outils de travail collaboratifs, et permettant de maximiser l'efficacité des échanges au sein de la communauté.

Forte de cette organisation, votre communauté d'intérêt acquiert une plus grande réactivité face aux attentes de vos clients, en perpétuelle évolution. Il devient alors possible de diminuer le «time to market» de vos produits et de mieux réagir face à la concurrence.

Ainsi, votre entreprise se doit d'être communicante et de s'ouvrir à l'extérieur pour assurer sa compétitivité. Grâce aux technologies de la communication, vous pouvez désormais mettre en œuvre une solution de communication performante pour votre entreprise et votre communauté d'intérêt.

Mais attention, le partage d'informations doit être contrôlé et maîtrisé. Des règles d'accès et d'usage de l'information doivent être établies: au sein de la communauté d'intérêt, le rôle de l'entreprise est également de décider qui accède à quoi, et comment.

I.4 Les pré-requis pour votre solution de communication

Votre entreprise doit s'assurer que la solution de communication qu'elle choisit de mettre en œuvre répond à des exigences fondamentales :

- **Rapidité de déploiement** : la solution doit pouvoir être déployée rapidement et donc permettre une interopérabilité avec les applications métiers et les protocoles de communication existants.
- **Accès pour tous** : votre solution de communication doit permettre à tout utilisateur – fixe ou nomade – d'accéder aux ressources du système d'information.
- **Partage d'information contrôlé** : l'accès aux ressources du système d'information doit être sécurisé. Cela nécessite en particulier la définition préalable de profils d'utilisateurs avec les autorisations d'accès associées et l'authentification des personnes à la connexion.

- **Fiabilité** : votre solution doit garantir une disponibilité maximale de l'information et des services. Ceci peut se traduire, par exemple, par une sécurisation physique des artères de communication et des plates-formes de services.
- **Evolutivité** : la solution doit s'adapter au développement de votre business en permettant, en particulier, une augmentation rapide des capacités de transit.
- **Facilité de gestion** : il est très important que la solution de communication soit simple à gérer. Par exemple, l'ajout ou le retrait d'un utilisateur nomade doit pouvoir être réalisé à la demande, dans des délais très courts.
- **Maîtrise des dépenses** : la solution doit vous garantir une maîtrise totale de vos dépenses en communications.

I.5 Les tendances du marché

Les entreprises ont pris conscience de l'importance des communications tant en interne que pour leur communauté d'intérêt. L'effet le plus spectaculaire de cette évolution est l'essor des Intranets – les réseaux internes aux entreprises utilisant les technologies de l'Internet et du Web – et des Extranets – les Intranets ouverts vers l'extérieur.

Les Intranets et les Extranets sont la réponse technologique actuelle aux besoins des entreprises communicantes. Selon l'étude «Panorama des opérateurs de services Internet/Intranet en France» publiée par Cesmo, le marché français des services basés sur les technologies de l'Internet est arrivé à 5,3 milliards de francs en 1999, dont 1 milliard pour des services liés aux Intranets

et plus de 600 millions pour des applications de commerce électronique. Ce marché a presque doublé par rapport à 1998 et cette tendance devrait se maintenir pendant l'année 2000.

II. Répondre aux enjeux : les solutions VPN

II.1 L'approche traditionnelle : les réseaux privés

Une des solutions envisageables pour mettre en œuvre une solution de communication à l'usage d'une communauté d'intérêt est de construire et de gérer un réseau privé avec des moyens propres à l'entreprise.

Dans le cas d'un **réseau privé**, l'entreprise choisit d'investir dans des infrastructures propres et privilégie le fait de pouvoir disposer de ressources qui lui sont totalement dédiées. L'entreprise doit alors développer les compétences techniques en interne pour l'exploitation, la maintenance mais aussi l'évolution de la solution.

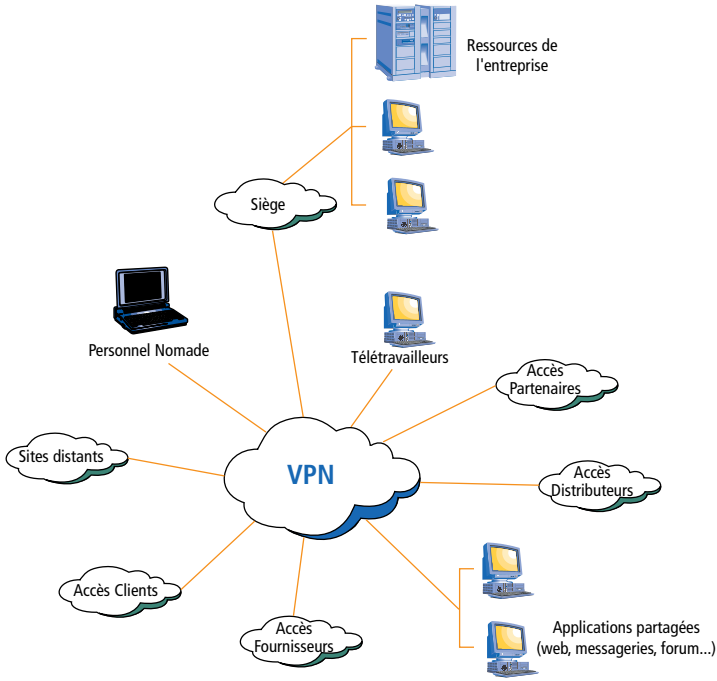
Si l'avantage majeur de cette approche est une maîtrise complète des infrastructures de télécommunications, elle implique cependant la mobilisation de ressources humaines et financières importantes dans une activité assez éloignée du cœur de métier de l'entreprise.

Cette approche se justifie de moins en moins avec le développement de services de télécommunications plus flexibles et moins chers sur des infrastructures mutualisées : les *réseaux privés virtuels*.

II.2 Une nouvelle voie : les Réseaux Privés Virtuels

Un **réseau privé virtuel** (VPN, *Virtual Private Network*) est une solution de communication pour laquelle les

infrastructures de transport sont partagées entre plusieurs communautés d'intérêt, et dont la gestion relève d'une société tierce.



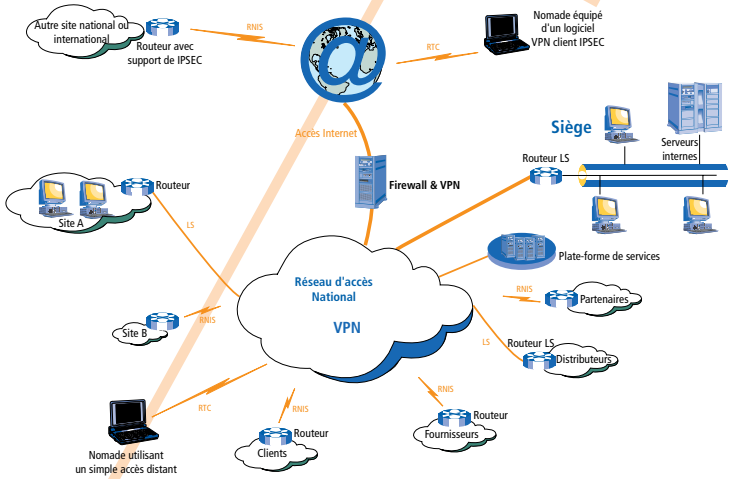
La notion de «virtuel» est simple à comprendre : vous disposez d'un service équivalent à celui fourni par un réseau privé, construit sur une infrastructure qui est gérée par un tiers, et qui mutualise les trafics de plusieurs entreprises ou communautés tout en garantissant zéro interférence entre ces trafics.

Un VPN peut s'appuyer sur les infrastructures réseaux d'un opérateur de télécommunications traditionnel. C'est le cas des services utilisant les technologies de type Frame Relay ou ATM, qui permettent d'isoler et de gérer de manière indépendante, sur une même infra-

structure physique, des flux générés par des entités différentes. Le VPN peut également être mis en œuvre sur un réseau totalement public comme l'Internet.

II.3 Les composantes d'un VPN

Comme tout réseau de transmission de données, un VPN est composé d'équipements de communications et de liaisons de transmission. A la différence des réseaux privés, la plupart des équipements et des liaisons appartiennent à un prestataire qui assure leur maintenance et leur évolution.



Parmi ces éléments, on peut identifier :

- **Le réseau de transport** : le réseau de transport, ou backbone, est une infrastructure de communication partagée qui transporte les flux de données entre vos sites et qui concentre et transporte les flux en provenance de votre personnel nomade. Il peut s'appuyer sur des infrastructures d'opérateurs ou sur Internet.

- **Des moyens d'accès** : il s'agit d'équipements d'extrémité (CPE, Customer Premises Equipment), dans la plupart des cas, des routeurs installés sur chaque site et des modems téléphoniques pour les utilisateurs nomades. Ces équipements constituent normalement la frontière entre l'infrastructure de communication propre à l'entreprise (réseau local) et l'infrastructure de communication du VPN. Ces équipements sont souvent fournis et gérés par votre prestataire, mais dans certains cas vous préférerez le faire vous-même. Les CPE sont connectés au réseau de transport par liaison louée, RTC, Numéris, ADSL, boucle locale radio, ...
- **Des moyens de sécurisation** : le service VPN permet de sécuriser les échanges et de protéger les ressources au sein d'une communauté grâce à la mise en œuvre de technologies propres au réseau de transport qui permettent d'isoler les flux – par exemple, des circuits virtuels Frame Relay – mais surtout grâce au déploiement d'équipements et de logiciels spécifiquement conçus pour protéger le VPN de toute intrusion – des pare-feux, des serveurs d'authentification/ autorisation
- **Une plate-forme de services** : le prestataire VPN peut également assurer l'hébergement et l'infogérance de services applicatifs, tels que la messagerie ou le Web. Il peut même, dans certains cas, faire appel à des partenaires technologiques pour la mise en œuvre de solutions avancées.
- **Des moyens de supervision** : une solution VPN est délivrée avec les outils qui vous permettent

de visualiser l'état de votre réseau et de contrôler la qualité du service.

II.4 Le VPN, une solution «tout en souplesse»

Une solution VPN présente plusieurs avantages pour votre entreprise :

- **Un accès pour tous** : les VPN permettent non seulement les communications entre des sites localisés n'importe où sur le territoire français, et dans certains cas à l'étranger, mais aussi l'intégration de tous les utilisateurs distants, nomades, télétravailleurs …
- **Des délais de déploiement plus courts** : parce qu'un service VPN s'appuie sur une infrastructure physique déjà opérationnelle (réseau opérateur, Internet), son déploiement mais aussi ses évolutions futures (comme l'intégration d'un nouveau site) peuvent être réalisés dans des délais très courts par rapport à ceux qui seraient nécessaires à la construction d'un réseau privé en partant de zéro. Un service VPN se révèle la solution idéale pour prendre en compte les évolutions d'une entreprise (restructurations, déménagements, nouvelles applications, nouvelles architectures…).
- **Des investissements réduits** : votre entreprise n'a pas besoin d'investir dans des équipements de communication, car ils sont fournis par le prestataire VPN.
- **La maîtrise des coûts** : l'approche forfaitaire associée au service VPN vous permet de contrôler parfaitement vos dépenses. De plus, vous n'avez pas besoin de développer des compétences internes pour anticiper et gérer les évolutions technologiques du service VPN.

- **Des solutions de sécurisation** : l'ouverture de votre entreprise vers les autres membres de votre communauté et vers les utilisateurs nomades nécessite la mise en place de solutions de sécurisation performantes. Le prestataire VPN vous accompagnera dans la définition de votre politique de sécurité et gèrera sa mise en œuvre.
- **Des services à forte valeur ajoutée** : le service VPN peut être étendu à des prestations d'hébergement ou d'infogérance d'applications Internet/Intranet, et pour lesquelles le prestataire pourra éventuellement faire appel à des partenaires ayant développé une expertise sur certaines technologies.

Certaines objections peuvent être faites quant au choix d'un service VPN :

- **Moins de sécurisation ?** : le problème de la sécurité des échanges est souvent associé aux services VPN qui utilisent l'Internet comme support de transmission. Cependant, des techniques de sécurisation telles que le «tunneling» et le chiffrement IPsec permettent d'assurer l'authentification des utilisateurs et des données, ainsi que l'intégrité et la confidentialité des échanges.
- **Perte de la maîtrise technique du réseau ?** : le service VPN induit effectivement une perte de contrôle sur les infrastructures qui sont gérées par un prestataire alors qu'un réseau privé est administré dans son intégralité par l'entreprise elle-même. Cependant, l'intérêt d'un service VPN est justement de permettre à l'entreprise de sous-traiter la gestion de votre solution de

communication. Non seulement vous profitez de l'expertise de votre prestataire dans ce domaine, mais vous disposez également d'outils qui vous permettent de superviser les ressources VPN et de contrôler la qualité de service aux utilisateurs.

- **Une qualité de service moindre ?** : si la qualité de service ne peut pas aujourd'hui être garantie sur Internet, en revanche, elle doit l'être forcément sur le réseau opérateur. Vous devrez obtenir de la part du prestataire des engagements en termes de qualité de service pour vous assurer qu'elle répond bien aux exigences de fonctionnement de vos applications .

II.5 Les avantages additionnels d'un VPN IP

A l'heure actuelle, le protocole IP est le protocole dominant dans les réseaux d'entreprise et il le sera de plus en plus, prévision confortée par le nombre croissant des nouveaux Intranets et Extranets sur le marché français et mondial.

Les techniques de tunneling IP permettent aussi de conserver des applications basées sur des protocoles propriétaires (SNA d'IBM, IPX de Novell…) et d'assurer le transport des flux par encapsulation.

De plus, les développements récents autour du protocole IP permettent d'envisager le transport de la voix.

Pour toutes ces raisons, le VPN IP s'affirme comme la solution idéale pour transporter l'ensemble des flux multimedia de l'entreprise et de sa communauté d'intérêt.

D'après le cabinet Cesmo, le marché actuel des services de transport IP a dépassé le milliard de francs en 1999, mais ce marché a été porté jusqu'à maintenant par les

plus gros clients des opérateurs que sont les ISP. Depuis 1999, on assiste, dans les entreprises, à l'accélération du remplacement des réseaux X.25 ou Frame Relay par des VPN IP. Ces estimations coïncident avec celles du cabinet d'études IDC, qui estime que le marché des VPN IP pour les entreprises passera de 21 millions de francs en 1999 à plus d'un milliard en 2002.

Dans la section suivante, vous trouverez une description plus détaillée des VPN IP et de l'impact de leur mise en place sur votre entreprise et sa communauté.

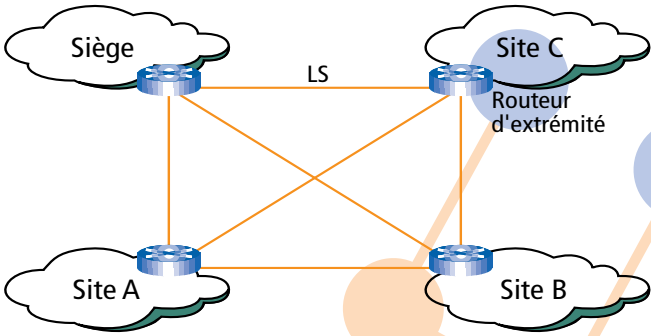
III. Mettre en place un VPN IP

III.1 Migrer du réseau actuel vers un VPN IP

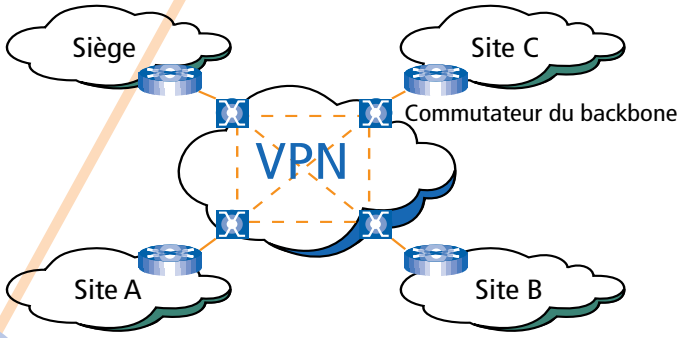
La migration d'une solution de communication existante vers une solution VPN IP est d'autant plus simple à réaliser que la solution finale permet d'assurer le transport de l'ensemble des flux de l'entreprise et de sa communauté d'intérêt, indépendamment des protocoles utilisés. L'architecture des réseaux locaux d'entreprise et les applications qu'elle supporte restent inchangées.

Les figures suivantes représentent deux scénarios de migration.

Dans le premier cas, la solution de communication de départ est un réseau privé à base de liaisons spécialisées, permettant l'interconnexion de plusieurs sites d'entreprise. La migration vers une solution VPN IP permet d'externaliser la gestion des flux et de la qualité de service. Dans certains cas, la prestation peut intégrer la gestion des équipements d'extrémité, augmentant encore le périmètre d'externalisation.

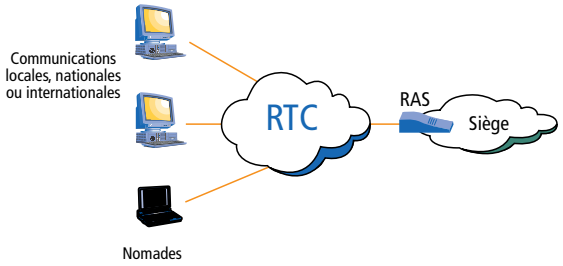


- Réseau privé géré par l'entreprise :
  - location de liaisons spécialisées à un opérateur ;
  - gestion des flux et de la qualité de service par l'entreprise.

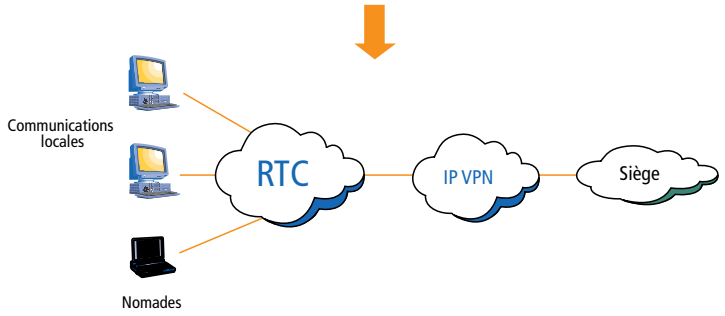


- L'infrastructure réseau local des sites ne change pas.
- Gestion des flux et de la qualité de service par l'opérateur VPN.

Dans le deuxième cas, la solution de communication de départ consiste à concentrer les connexions des utilisateurs distants sur une plate-forme mise en œuvre et gérée par l'entreprise au niveau du siège. La migration vers une solution VPN IP permet de bénéficier de la couverture géographique du réseau d'accès de l'opérateur et ainsi d'optimiser le coût des communications : initialement à hauteur d'un tarif national, celui-ci est ramené à un tarif local.



- Gestion des serveurs d'accès distant par l'entreprise.
- Communications au tarif local, national, voire international.



- Connexion des nomades via l'infrastructure d'accès du prestataire
- Communications au tarif local

III.2 Les compétences requises

La décision de développer un réseau privé avec des moyens propres ou de faire appel à un prestataire VPN

pour lui sous-traiter tout ou partie de la gestion de vos communications est fortement influencée par les compétences qui existent ou que vous souhaitez développer au sein de vos équipes techniques.

La mise en œuvre d'une solution de communication nécessite de multiples compétences et dans des domaines très différents : infrastructures physiques, sécurité logique, services applicatifs … De plus, l'évolution constante des technologies nécessite de la part des équipes techniques d'acquérir de nouvelles compétences.

Dans ces conditions, il devient de plus en plus difficile de ne pas faire appel à des prestataires spécialisés.

IV. Choisir son prestataire : les acteurs du marché VPN

La logique de la sous-traitance, même si elle permet de s'appuyer sur les compétences d'un tiers, nécessite de la part de l'entreprise qu'elle ait une bonne connaissance des prestataires présents sur le marché et des critères qui permettent d'apprécier l'adéquation de leurs compétences avec la solution de communication que l'on cherche à développer.

IV.1 Le panorama des acteurs du VPN

Plusieurs catégories de fournisseurs sont en mesure de proposer des solutions VPN IP. Ils peuvent être classifiés de la manière suivante :

- **Opérateurs IP**

  Les opérateurs IP disposent de leurs propres infrastructures de backbone et d'hébergement d'applications et fournissent des services de transmission de données IP – y compris l'accès

à Internet – et des services IP à plus forte valeur ajoutée que ceux offerts par les opérateurs généralistes (hébergement Web, messagerie internet/intranet …). Ils peuvent aussi compléter leurs offres avec des partenaires spécialisés sur des services spécifiques.

- **Opérateurs généralistes**

  Ces acteurs disposent de leurs propres infrastructures tant au niveau du backbone qu'au niveau de l'accès – ce qu'on appelle communément la boucle locale. Ils fournissent une large gamme de services de télécommunications comprenant des services de transmission de données (IP, mais aussi Frame Relay ou ATM) et des services de téléphonie. Par ailleurs, de par leur positionnement d'opérateur généraliste, leur degré de spécialisation sur les services IP est moindre.

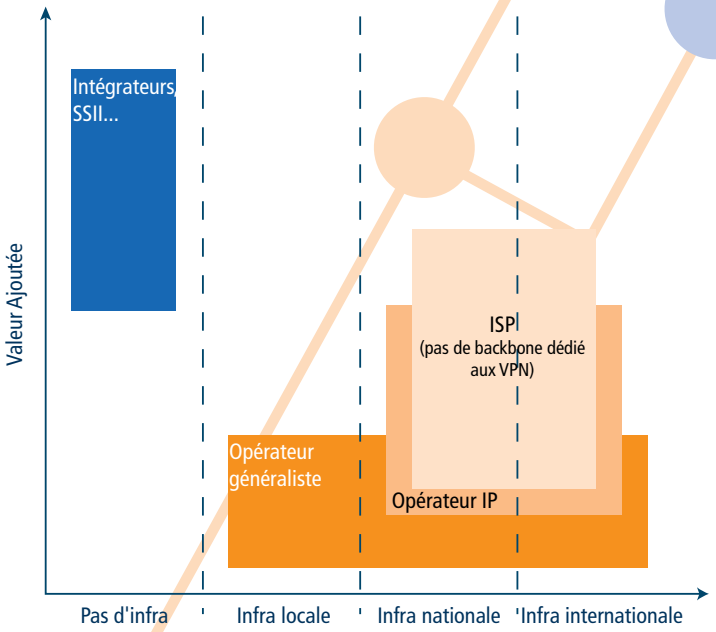
- **ISP**

  Les ISP – fournisseurs d'accès à Internet – offrent un ensemble relativement riche de services IP sur la base de leurs plates-formes de services. A l'inverse des opérateurs IP et généralistes, ils n'ont pas d'infrastructure de transmission dédiée au trafic des VPN IP de leurs clients. Ainsi, les VPN IP offerts par les ISP sont presque exclusivement des VPN Internet.

- **Intégrateurs et SSII**

  Ces acteurs ne disposent pas d'infrastructure de transport. Ils possèdent une expertise forte dans des domaines spécifiques et sont donc en mesure d'apporter des services à forte valeur ajoutée. Ils peuvent fournir des solutions VPN

IP en direct en s'appuyant sur les services des opérateurs généralistes, IP et ISP, mais ils s'intègrent aussi en tant que partenaires dans les offres des autres acteurs du marché.



Le positionnement des acteurs sur le marché VPN dépend donc de la valeur ajoutée de leurs offres de services et de la disponibilité d'une infrastructure de communication propre.

IV.2 Les critères de choix

Deux critères déterminent le choix du type de prestataire à qui s'adresser pour la mise en place d'une solution VPN IP : les besoins et les compétences internes de votre entreprise et les compétences du prestataire. Pour guider cette décision, les critères de choix suivants peuvent être utilisés :

- **L'offre réseau**

Deux aspects sont à prendre en compte concernant l'offre réseau du prestataire :

- La maîtrise de l'infrastructure réseau

Le premier point que vous devez prendre en compte est le degré de maîtrise du prestataire sur les infrastructures de télécommunications utilisées pour le service VPN.

Dans la plupart des cas, le prestataire VPN n'a pas de maîtrise sur la boucle locale (réseau de téléphonie analogique et numérique, liaisons louées), mais intègre les engagements de qualité de service de l'opérateur de boucle locale dans ses engagements propres. La maîtrise de la boucle locale n'est donc pas un élément fortement différenciateur dans le choix de votre prestataire.

Par contre, la **maîtrise du cœur de réseau VPN** est d'une importance cruciale. Elle permet au prestataire de contrôler la qualité du service et son évolution (en termes de débit) en réponse aux besoins des clients.

- Les services d'accès offerts

Le prestataire doit pouvoir vous offrir des services d'accès adaptés à vos besoins : accès permanents sur des liaisons louées à des débits pouvant évoluer de manière souple et rapide, accès commutés analogiques ou numériques (RNIS), voire accès ADSL.

- **La sécurité**

De par leur nature complexe et leur importance capitale, les services de sécurisation méritent une mention spéciale. A mi-chemin entre les services de communications et les services applicatifs, ils comprennent :

- **la sécurisation physique** des accès et du backbone du prestataire (redondance des liaisons, des équipements…),
- **la sécurisation logicielle** des communications IP (authentification/autorisation des accès, chiffrement des communications, fourniture et configuration de pare-feux, support IPsec…)

Ces services sont d'autant plus importants que les entreprises mettent en place des Extranets et s'ouvrent vers Internet. Seules des solutions de sécurité globales assurent une ouverture maîtrisée du système d'information de votre entreprise. Par conséquent, elles sont une composante clé dans l'offre du prestataire.

- **L'offre de services applicatifs**

Deux types de services sont envisageables :

- Les services de base

Un VPN IP doit être envisagé dans la plupart des cas comme le support de communication d'un Intranet ou d'un Extranet. Selon les compétences internes de l'entreprise, l'externalisation de certaines applications de l'Intranet pourrait être souhaitable. L'offre de services applicatifs peut comprendre la messagerie électronique, l'hébergement Web, des forums privés, etc. .

- **Les services évolués**

  Vous pouvez également envisager des services applicatifs évolués, caractérisés par une plus grande complexité et des compétences requises plus pointues. Par exemple, vous pourriez mettre en œuvre un portail d'entreprise pour vos utilisateurs et vos partenaires, ou des applications de commerce électronique… Vous pourriez aussi souhaiter mettre en œuvre des applications de travail collaboratif. La capacité de votre prestataire de services à vous fournir une prestation d'hébergement et d'infogérance de solutions applicatives évoluées est donc un critère de choix important.

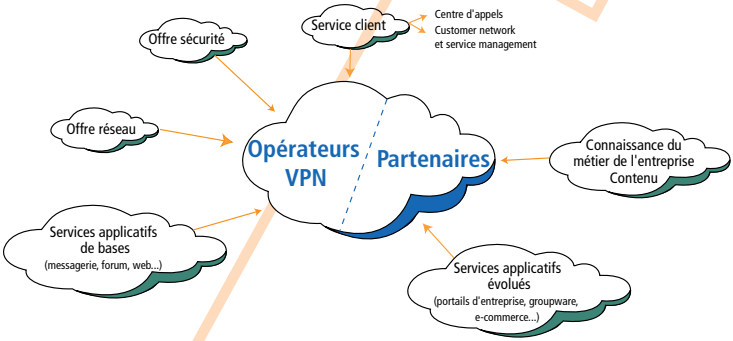
- **Le service client**

  Opter pour un service VPN IP implique un certain degré de délégation de la maîtrise technique du réseau sur le prestataire. Par conséquent, le prestataire doit pouvoir offrir à l'équipe technique de votre entreprise des outils pour la supervision de l'état du VPN IP, voire même, pour la maintenance des équipements installés sur les sites de l'entreprise (customer network and service management). Dans la plupart des cas, grâce aux économies d'échelle et à l'expérience du prestataire, le rapport qualité/prix de ces prestations est meilleur que celui qu'on pourrait atteindre par des développements en interne.

  De même, le prestataire doit pouvoir mettre à votre disposition un support technique téléphonique (hotline ou call centre), pouvant prendre en compte vos demandes d'informations ou vos signalements d'incidents.

- **L'expertise marché**

  Enfin, la connaissance du métier de votre entreprise peut s'avérer un facteur clé pour la réussite de la mise en place d'un VPN IP. C'est par exemple le cas des prestations à forte valeur ajoutée incorporant des applications sur mesure. Un prestataire habitué à traiter des problématiques proches de celle de votre entreprise est plus à même de répondre à ce type de besoin.



IV.3 Votre prestataire est aussi au centre d'une communauté d'intérêt

L'étendue et la complexité des services que vous attendez sont telles que peu d'acteurs présents sur le marché pourraient satisfaire à eux seuls tous ces besoins. Il est donc logique que, comme vous, ils travaillent souvent en partenariat avec des prestataires spécialisés dans la fourniture de certains services pour apporter une solution globale à vos besoins de communications.

Le recours à la sous-traitance ou au partenariat va de pair avec le degré de complexité et de valeur ajoutée des services que vous demandez. Ce sera souvent le cas

dans le cadre de la fourniture de solutions applicatives évoluées, du développement d'applications sur mesure ou encore de l'élaboration de contenus pour un portail d'entreprise, etc .., prestations sur lesquelles une expertise métier est indispensable.

Ainsi, le choix d'un prestataire pour votre solution VPN IP est donc déterminé aussi par sa capacité à fédérer des partenaires autour de votre projet d'entreprise et de construire une équipe de projet rassemblant toutes les compétences requises pour son développement.

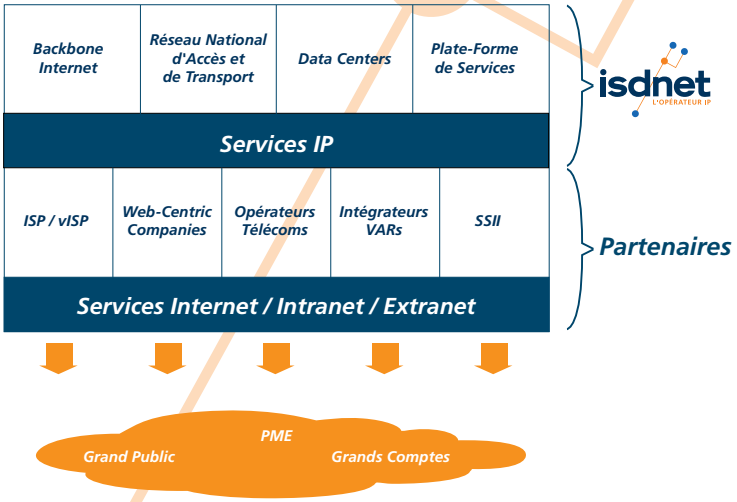
L'offre IP-VPN

L'offre IP-VPN isdnet

V. Pourquoi une offre de services IP-VPN chez isdnet

V.1 isdnet, l'opérateur IP

Opérateur licencié L33.1 et filiale de Cable & Wireless plc, isdnet est le premier opérateur IP alternatif en France. Depuis sa création en 1995, isdnet s'est donné pour mission d'être l'opérateur IP partenaire des sociétés proposant des services Internet, Intranet et Extranet.



isdnet – Positionnement et Stratégie

Pour remplir cette mission, isdnet fournit à ses clients une gamme complète de services IP de très haute qualité …

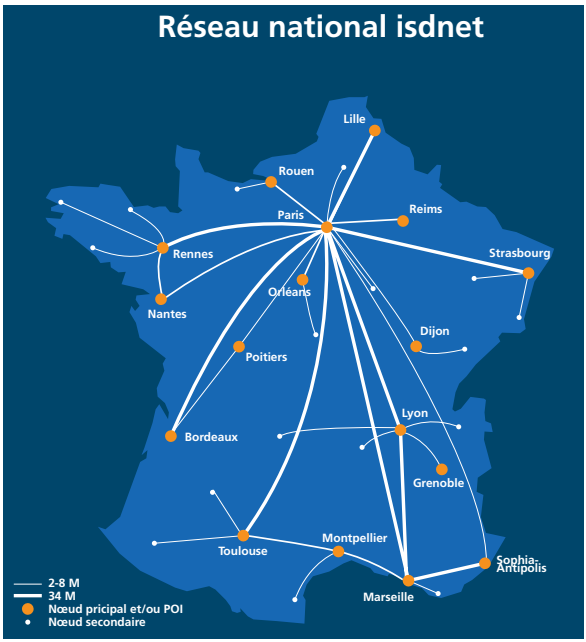
- Les Services de Connectivité Internet de 64 Kbps à 155 Mbps : trafics garantis et évolutifs, routage statique et dynamique pour plus de vitesse d'accès à l'ensemble de l'Internet
- Les Services d'Accès et de Concentration de Trafic IP / Frame Relay : à partir des 50 POPs du

réseau national isdnet, ports d'accès commutés RTC et RNIS, concentration de Liaisons Louées, Circuits Virtuels Privés

- Les Services d'Hébergement et de Connexion à Internet de Serveurs et d'Equipements Télécoms
- Les Services d'Accès Internet Clé en Main pour démarrer une activité de Fournisseur d'Accès

.. et s'appuie sur des infrastructures d'exception :

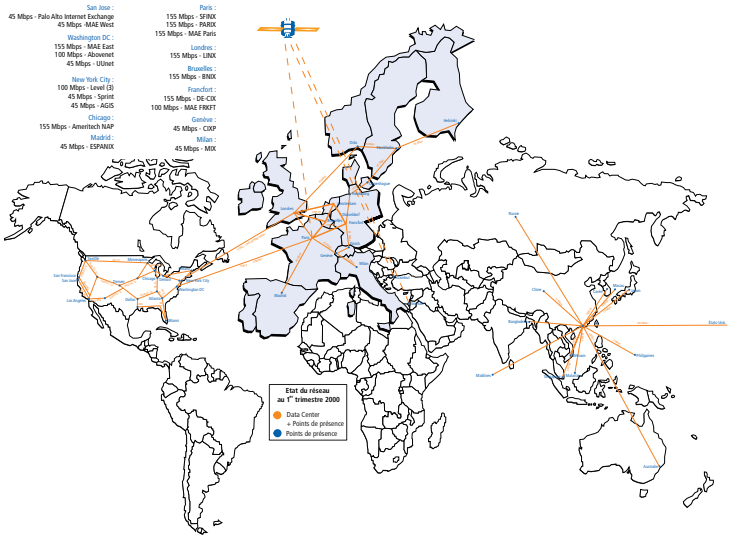
- un réseau national Frame Relay comptant 50 Points de Présence Opérationnels, spécifiquement conçu pour supporter un trafic IP de qualité professionnelle. Quotidiennement utilisé par plusieurs millions d'usagers, il a totalisé 200 millions de minutes de connexion commutées en Janvier 2000.



- des salles d'hébergement sécurisées, conçues et opérées selon les normes de sécurité les plus élevées, pour héberger les équipements des clients isdnet.

- une plate-forme de services Internet industrielle permettant à isdnet de fournir à ses clients des services applicatifs fiables : messagerie, forums de discussion, espace de stockage et diffusion multimédia, Firewall, etc.
- un backbone Internet mondial full IP, qui s'appuie sur une infrastructure optique paneuropéenne à 2,4 Gbit/s (STM-16), une boucle transatlantique à 2 x 155 Mbit/s (OC-3), et une boucle trans-américaine à 155 Mbit/s (OC-3). Ce Backbone est interconnecté aux principaux nœuds Internet en Europe et aux Etats-Unis : Londres, Frankfort, Amsterdam, Bruxelles, Genève, New-York, Washington, Chicago,

San Jose, etc. Intégralement conçu en IP natif et intégrant la technologie MPLS, ce réseau est un des Backbones Internet les plus importants centré sur l'Europe et est optimisé pour servir préférentiellement les audiences française et européennes.



V.2 Les services IP-VPN: une diversification naturelle pour isdnet

isdnet met traditionnellement à la disposition de ses partenaires son expertise dans la conception et l'exploitation d'infrastructures et de services IP, pour leur permettre de construire sur cette base des solutions à valeur ajoutée qui requièrent un niveau de disponibilité et de fiabilité élevé.

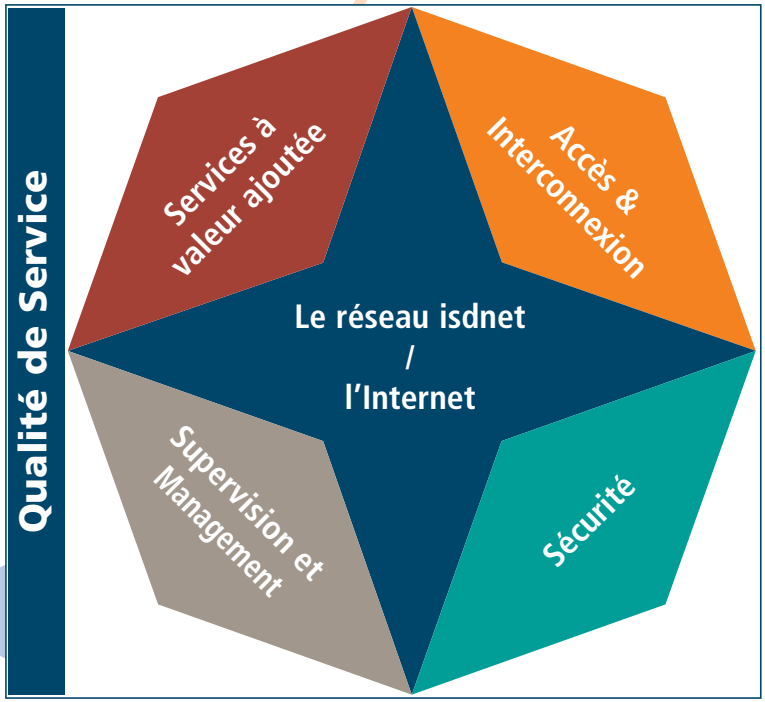
isdnet a donc naturellement développé des compétences dans la mise en œuvre des services IP-VPN, services sur lesquels les partenaires pourront s'appuyer

afin de se positionner comme des fournisseurs de solutions Internet / Intranet / Extranet globales.

VI. les services IP-VPN isdnet: la modularité

VI.1 Introduction aux modules IP-VPN isdnet

Privilégiant cette approche de partenariat, isdnet a défini une offre de services résolument modulaire. Chacun des partenaires peut ainsi choisir d'intégrer telle ou telle composante de l'offre IP-VPN isdnet pour construire ou compléter ses propres offres de services.



Plus précisément, l'offre de Services IP-VPN isdnet se compose des modules suivants :

- **Les Services Réseaux** : c'est le module de base de l'ensemble de l'offre isdnet. Associant Services d'Interconnexion et Services d'Accès, ils permettent de construire le cœur du Réseau Privé de l'Entreprise ainsi que les artères permanentes ou établies à la demande qui le desservent.
- **La Sécurité** : ce module permet de conférer un caractère réellement privatif au réseau client par des mécanismes de contrôle d'accès et de protection des données.
- **Les Services à Valeur Ajoutée** : ce module permet aux entreprises clientes de bénéficier d'une solution de communication globale pour augmenter l'efficacité et la performance des échanges entre les collaborateurs de l'entreprise, mais aussi entre l'entreprise et ses partenaires privilégiés (clients, fournisseurs …)
- **Supervision et Management** : ce module permet au partenaire et/ou au client final de bénéficier d'un niveau avancé de contrôle et de visibilité sur les ressources réseaux, systèmes et applications qui lui sont dédiées au sein des infrastructures isdnet, et ainsi de s'appuyer sur un système de supervision aussi fiable que celui qui pourrait être mis en œuvre dans le cadre d'un réseau privé.

La Qualité de Service représente la pierre angulaire de l'ensemble des Services VPN isdnet. Quel que soit le module choisi, les partenaires isdnet bénéficient d'une qualité de service optimale, sur laquelle ils peuvent asseoir des services Internet / Intranet performants. D'une part, isdnet s'engage sur les performances de son réseau et de ses Services VPN. D'autre part, isdnet

est à même de proposer des classes de services différenciées, permettant ainsi à ses partenaires et leurs clients de déterminer et gérer avec précision les priorités au sein des flux de données qui sont les leurs.

VI.2 Les services réseaux

• VI.2.a Les services d'interconnexion

Pour chacune des entreprises clientes, **isdnet** alloue au sein de son Backbone des **ressources réseaux dédiées** qui ont en charge d'**isoler**, de **fédérer** et d'**aiguiller** l'ensemble des flux de son Réseau Privé Virtuel.

Ces services permettent de construire le cœur du VPN de l'entreprise cliente. Le dimensionnement et les fonctionnalités de ce cœur de réseau varient, selon les besoins de l'entreprise cliente, en fonction de 3 paramètres :

- Le nombre de sites à interconnecter
- Le volume total de trafic à gérer
- La nature du trafic à gérer : flux montants exclusivement (des sites secondaires vers le site central), flux descendants (du site central vers les sites secondaires), flux montants et descendants

• VI.2.b Les services d'accès

Le Backbone National **isdnet** dispose sur l'ensemble du territoire français de 50 POPs (Points de Présence), qui sont autant de portes d'accès aux VPN des Entreprises Clientes.

Les Services d'Accès couvrent une gamme complète de débits (de 28,8 Kbps à 128 Kbps pour les accès commutés ; de 64 Kbps aux multiples de 2 Mbps pour les accès permanents) quelque soit la technologie employée (RTC/RNIS, xDSL, liaisons louées, Boucle Optique, …) :

- Les **Services d'Accès Permanent** : ces services sont adaptés aux sites disposant de gros réseaux locaux, ainsi qu'aux sites hébergeant des applications importantes comme le site central.
- Les **Services d'Accès Commuté** : ces services sont adaptés aux petits réseaux locaux ne justifiant pas la mise en service d'un raccordement permanent, ou les postes nomades des itinérants et des télétravailleurs.

Les services d'accès commuté sont également mis en oeuvre sur les POPs du réseau paneuropéen **isdnet**.

Par ailleurs, l'offre IP-VPN **isdnet** a été conçue pour permettre d'établir des accès sécurisés sur le VPN entreprise avec n'importe quelle connexion Internet, et sans restriction géographique.

VI.3 La sécurité selon isdnet

Les VPN doivent offrir les mêmes garanties de sécurité que les réseaux privés point à point. C'est la raison pour laquelle **isdnet** propose une **sécurité intégrale** dans le cadre de ses solutions IP-VPN.

La sécurité est mise en œuvre à plusieurs niveaux :

- Tout d'abord **au niveau physique** : la sécurité est assurée par la fiabilité des infrastructures réseaux ainsi que le maillage du réseau de transport Frame Relay et la redondance physique de l'infrastructure d'accès, qui offrent toutes les garanties de reroutage de trafic en cas de défaillance d'un lien physique ou d'un point d'accès.
- L'usage de **circuits dédiés Frame Relay CVP** permet de gérer de manière totalement indépen-

dante les flux des différents VPN et leur qualité de service associée.

- L'usage d'un **plan d'adressage privé** (RFC1918) sur le backbone **isdnet** permet de masquer et isoler le VPN et ses ressources depuis des réseaux externes comme l'Internet.
- La gestion des accès au VPN s'appuie sur les mécanismes d'**authentification** des utilisateurs et les **autorisations** associées à chacun d'eux, qui sont implémentés au travers du **serveur RADIUS isdnet**.
- L'utilisation des techniques de **Tunneling (ATMP/L2TP/IPsec)** et, dans certains cas, de **Chiffrement IPsec** permet de garantir l'authentification des données et des interlocuteurs, ainsi que l'intégrité et la confidentialité des échanges.
- L'ouverture sécurisée sur l'Internet est mise en œuvre à travers des **Firewalls** fournis et gérés par **isdnet**, en central ou en local.

VI.4 Les services à valeur ajoutée

Les solutions IP-VPN **isdnet** permettent également aux entreprises de bénéficier d'une solution de communication globale clé en main, qui intègre les prestations suivantes :

- Site Web Internet / Intranet ;
- Service de Messagerie sécurisée (anti-virus intégré) ;
- Service de messagerie unifiée permettant aux utilisateurs de recevoir des messages téléphoniques ou des fax par le biais de leur boîte aux lettres électronique ;

- Serveur FTP ;
- Forums privés et publics ;
- Annuaire Intranet ;

Mais aussi …

- **Diffusion de contenus multimédias : isdcast**

  Ce dernier service s'affirme comme le plus novateur parmi ceux proposés par **isdnet** dans le cadre des services IP-VPN. Il permet à toute entreprise d'utiliser les technologies IP pour diffuser des contenus multimedia. Cette diffusion peut être envisagée aussi bien sur Internet, que sur un Intranet / Extranet pour un contenu à destination des seuls employés et/ou partenaires de l'entreprise.

L'ensemble de ces services est mis en œuvre, supervisé et géré pour le compte des entreprises sur une plate-forme d'hébergement industrielle, qui offre toutes les garanties en termes de disponibilité et de sécurité.

Afin de concilier les impératifs d'adaptabilité et de montée en charge, cette plate-forme et organisée selon une architecture hiérarchique à trois niveaux : systèmes d'équilibrage de charge («Load Balancing»), serveurs frontaux NT ou UNIX et serveurs de fichiers à très haute disponibilité.

Les systèmes sont fédérés à travers une architecture LAN Fast Ethernet, qui dispose d'une connexion redondante haut débit au réseau national **isdnet**.

La plate-forme est intégrée à une «zone démilitarisée» (DMZ), accessible de l'Internet uniquement dans le respect des règles de sécurité implémentées sur le Firewall dédié à l'entreprise.

VI.5 Supervision et management

Les Services IP-VPN doivent être envisagés comme une solution d'externalisation partielle ou totale de services réseaux et applicatifs, permettant à l'entreprise de réaliser des économies substantielles et de rester concentrée sur son cœur d'activité. Pourtant, il s'agit de services et de ressources qui restent souvent trop stratégiques pour que l'Entreprise Cliente n'en conserve pas un contrôle total.

C'est pourquoi **isdnet** attache la plus grande importance, non seulement à la supervision qu'elle opère sur ses Services VPN, mais également aux outils de supervision et de management qu'elle met à la disposition de ses partenaires et de leurs clients.

Dans le cadre des Services VPN, une **assistance téléphonique 24 h/24, 7 j/7**, garantit des réponses et des interventions rapides. Des **procédures d'escalades** auprès d'experts Sécurité, Services et Réseaux sont en place pour assurer un fonctionnement continu.

En outre, un **Système Proactif de Qualification des Incidents et d'Alertes 24x7**, informe le partenaire et son client en temps réel de l'ensemble des événements qui pourraient avoir un impact sur le service.

Enfin, un **service Web d'administration** (**isdnet** Web VPN Manager) permet au partenaire et à son client de visualiser en temps réel l'état des équipements distants, des liaisons et des raccordements sur les points d'accès, ainsi que des éventuels changements d'état de circuits internes. Ce service permet par ailleurs de gérer au quotidien les services souscrits : gérer son parc d'utilisateurs distants, obtenir des statistiques sur l'utilisation de son VPN, visualiser des rapports sur les services hébergés (pare-feu, serveurs Intranet, serveurs publics, …).

VI.6 La qualité de service

- **VI.6.a Les engagements isdnet**

Ce sont l'ensemble des indicateurs de performance réseau sur lesquels isdnet s'engage pour l'ensemble de ses Services VPN. Ce sont les engagements de base d'isdnet dans le cadre de ces services :

- Disponibilité du réseau, des ports commutés, de la boucle locale ;
- Temps de réponse sur le réseau ;
- Taux de perte de paquets ;
- GTR, fenêtres de maintenance.

- **VI.6.b Les classes de services**

Les Classes de Service : permettent de fixer, au-delà des performances intrinsèques du réseau, le niveau de service attendu par les partenaires et leurs clients pour les différents flux de données qu'ils ont à gérer.

Pour ce qui est des accès permanents au VPN d'Entreprise, isdnet permet à ses partenaires et leurs clients de définir eux-mêmes les débits maximums et minimums qu'ils veulent attribuer à leurs différents types de trafic. Le Backbone isdnet, reposant sur une solution de transport Frame Relay, permet en effet de faire jouer des mécanismes de CVP (Circuits Virtuels Permanents) et de CIR (Commited Information Rate). L'Entreprise Cliente peut ainsi définir sur la même liaison d'accès plusieurs CVPs pour distinguer différents types de trafics (le trafic Internet et le trafic Intranet par exemple) avec des CIRs associés distincts (en donnant une priorité supérieure au trafic Intranet par exemple).

Pour ce qui est des accès commutés au VPN d'Entreprise, isdnet assure, de par le dimensionnement même de son Backbone, une qualité de service minimale à chacun des VPN d'Entreprise (de l'ordre de 8 Ko). Cependant, pour les Entreprises Clientes qui le désireraient, des mécanismes de CVP / CIR peuvent également être mis en œuvre pour les trafics issus des sites commutés, dans des conditions spécifiques (le plan d'adressage notamment, devra être défini avec isdnet).

VII Les offres IP-VPN isdnet

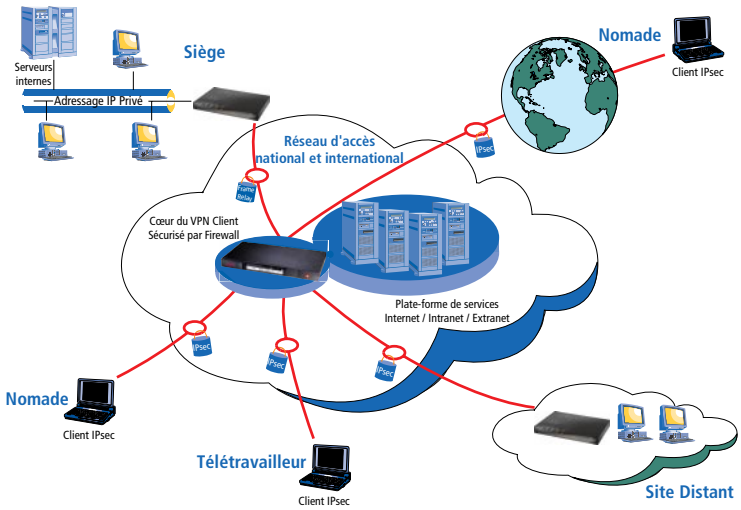
Pour répondre à l'intégralité des demandes de solutions IP-VPN qui émanent de ses partenaires, isdnet a conçu deux offres, qui permettent de répondre à des problématiques d'utilisateurs et de services différentes.

VII.1 L'offre IP-VPN Premium

L'offre IP-VPN Premium a été conçue pour permettre aux partenaires isdnet d'adresser, à travers des solutions clé en main, les besoins Internet /Intranet /Extranet des petites et moyennes entreprises, à savoir :

- Permettre aux collaborateurs (nomades, télétravailleurs, petits sites) de naviguer sur Internet, et d'accéder aux application métiers de l'entreprise en toute sécurité ;
- Sous-traiter la sécurité, ainsi que l'hébergement des sites Web Internet / Intranet, des boîtes aux lettres et plus généralement de toutes les applications Internet / Intranet ;
- Maîtriser son budget de transmission de données grâce à une approche forfaitaire, qui prend en compte l'évolution des besoins de l'entreprise dans le temps.

L'offre IP-VPN Premium, c'est aussi la garantie d'un service performant, livré clé en main et géré par isdnet pour le compte de l'entreprise 24 h/24, pour lui permettre de rester concentrée sur le cœur de son activité.



VII.2 L'offre IP-VPN Optimium

L'offre IP-VPN Optimium a été conçue pour permettre aux partenaires isdnet de répondre à des besoins clients spécifiques, qu'il s'agisse d'un service de réseau privé virtuel de grande échelle (interconnexion de plusieurs dizaines de sites), de la mise en œuvre d'une politique de sécurité complexe (filtrages applicatifs), de l'hébergement d'applications Internet/Intranet de dernière génération (datamining, one-to-one, e-commerce, diffusion multimedia..).

A travers les offres IP-VPN Premium, isdnet met à la disposition de ses partenaires toute son expertise dans les technologies IP pour les accompagner dans la réalisation de solutions sur mesure.

VIII En résumé, pourquoi choisir une solution IP-VPN isdnet ?

- **Une solution pérenne** déployée et administrée par des experts des technologies IP
- **Une solution globale**, qui répond non seulement à la problématique d'interconnexion sécurisée des sites et des employés nomades de l'entreprise, mais aussi à des besoins d'applications partagées
- **Une sécurité intégrale**, qui se décline depuis la fiabilité des infrastructures physiques jusqu'au chiffrement IPsec des données
- **Une qualité de service optimale**, qu'il s'agisse de délai de transit sur l'intranet, de disponibilité d'applications ou encore de réactivité du support technique
- **Un budget maîtrisé** grâce à une approche forfaitaire, qui prend en compte l'évolution des besoins de l'entreprise dans le temps.

Livre Blanc réalisé à l'initiative d'isdnet

A CABLE & WIRELESS COMPANY

www.isdnet.net

Siège :
5-7, rue Dareau 75014 Paris
Tél : +33 (0)1 43 13 68 00
Fax : +33 (0)1 43 13 68 68

Agence Lyon :
20, boulevard Eugène Deruelle
69432 Lyon Cedex 03

Agence Sophia-Antipolis :
WTC entrée B7 - 1300, route des Crêtes
Parc Sophia-Antipolis - 06560 Valbonne

info@isdnet.net