VPN

Principes, mise en oeuvre et outils open source

SMILE

I.T IS OPEN

Préambule

SMILE

Smile est une société d'ingénieurs experts dans la mise en œuvre de solutions open source et l'intégration de systèmes appuyés sur l'open source. Smile est membre de l'APRIL, l'association pour la promotion et la défense du logiciel libre, du PLOSS – le réseau des entreprises du Logiciel Libre en Ile-de-France et du CNLL – le conseil national du logiciel libre.

Smile compte plus de 1200 collaborateurs dans le monde ce qui en fait le premier intégrateur français et européen de solutions open source.

Depuis 2000, environ, Smile mène une action active de veille technologique qui lui permet de découvrir les produits les plus prometteurs de l'open source, de les qualifier et de les évaluer, de manière à proposer à ses clients les produits les plus aboutis, les plus robustes et les plus pérennes.

Cette démarche a donné lieu à toute une gamme de *livres blancs* couvrant différents domaines d'application. La gestion de contenus (2004), les portails (2005), la business intelligence (2006), la virtualisation (2007), la gestion électronique de documents (2008), les PGIs/ERPs (2008), les VPN open source (2009), les Firewall et Contrôle de flux (2009), les Middleware orientés messages (2009), l'ecommerce et les Réseaux Sociaux d'Entreprise (2010), le Guide de l'open source et NoSQL (2011), et plus récemment Mobile et Recensement et audit (2012). Chacun de ces ouvrages présente une sélection des meilleures solutions open source dans le domaine considéré, leurs qualités respectives, ainsi que des retours d'expérience opérationnels.

Au fur et à mesure que des solutions open source solides gagnent de nouveaux domaines, Smile sera présent pour proposer à ses clients d'en bénéficier sans risque. Smile apparaît dans le paysage informatique français comme le prestataire intégrateur de choix pour accompagner les plus grandes entreprises dans l'adoption des meilleures solutions open source.

Ces dernières années, Smile a également étendu la gamme des services proposés. Depuis 2005, un département consulting accompagne nos clients, tant dans les phases d'avant-projet, en recherche de solutions, qu'en accompagnement de projet. Depuis 2000, Smile dispose d'un studio graphique, devenu en 2007 Smile Digital – agence interactive, proposant outre la création graphique, une expertise e-marketing, éditoriale, et interfaces riches. Smile dispose aussi d'une agence spécialisée dans la TMA (support et l'exploitation des applications) et d'un centre de formation complet, Smile Training. Enfin, Smile est implanté à Paris, Lille, Lyon, Grenoble, Nantes, Bordeaux, Marseille et Montpellier. Et présent également en Espagne, en Suisse, au Benelux, en Ukraine et au Maroc.

Quelques références

Intranets et Extranets

Société Générale - Caisse d'Épargne - Bureau Veritas - Commissariat à l'Energie Atomique - Visual - CIRAD - Camif - Lynxial - RATP - Sonacotra - Faceo - CNRS - AmecSpie - INRA - CTIFL - Château de Versailles - Banque PSA Finance - Groupe Moniteur - Vega Finance - Ministère de l'Environnement - Arjowiggins - JCDecaux - Ministère du Tourisme - DIREN PACA - SAS - CIDJ - Institut National de l'Audiovisuel - Cogedim - Diagnostica Stago Ecureuil Gestion - Prolea - IRP-Auto - Conseil Régional Ile de France - Verspieren - Conseil Général de la Côte d'Or - Ipsos - Bouygues Telecom - Prisma Presse - Zodiac - SANEF - ETS Europe - Conseil Régional d'Ile de France - AON Assurances & Courtage - IONIS - Structis (Bouygues Construction) - Degrémont Suez - GS1-France - DxO - Conseil Régional du Centre - Beauté Prestige International - HEC - Veolia

Internet, Portails et e-Commerce

Cadremploi.fr - chocolat.nestle.fr - creditlyonnais.fr - explorimmo.com - meilleurtaux.com - cogedim.fr - capem.fr - Editions-cigale.com - hotels-exclusive.com - souriau.com - pci.fr - odit-france.fr - dsv-cea.fr - egide.asso.fr - Osmoz.com - spie.fr - nec.fr - vizzavi.fr - sogeposte.fr - ecofi.fr - idtgv.com - metro.fr - stein-heurtey-services.fr - bipm.org - buitoni.fr - aviation-register.com - cci.fr - eaufrance.fr - schneider-electric.com - calypso.tm.fr - inra.fr - cnil.fr - longchamp.com - aesn.fr - bloom.com - Dassault Systemes 3ds.com - croix-rouge.fr - worldwatercouncil.org - Projectif - credit-cooperatif.fr - editionsbussiere.com - glamour.com - nmmedical.fr - medistore.fr - fratel.org - tiru.fr - faurecia.com - cidil.fr - prolea.fr - bsv-tourisme.fr - yves.rocher.fr - jcdecaux.com - cg21.fr - veristar.com - Voyages-sncf.com - prismapub.com - eurostar.com - nationalgeographic.fr - eau-seine-normandie.fr - ETS Europe - LPG Systèmes - cnous.fr - meddispar.com - Amnesty International - pompiers.fr - Femme Actuelle - Stanhome-Kiotis - Gîtes de France Bouygues Immobilier - GPdis - DeDietrich - OSEO - AEP - Lagardère Active Média - Comexpo - Reed Midem - UCCIFE - Pagesjaunes Annonces - 1001 listes - UDF - Air Pays de Loire - Jaccede.com - ECE Zodiac - Polytech Savoie - Institut Français du Pétrole - Jeulin - Atoobi.com - Notaires de France - Conseil Régional d'Ile-de-France - AMUE

Applications métier

Renault - Le Figaro - Sucden - Capri - Libération - Société Générale - Ministère de l'Emploi - CNOUS - Neopost - Industries - ARC - Laboratoires Merck - Egide - ATEL-Hotels - Exclusive Hotels - CFRT - Ministère du Tourisme - Groupe Moniteur - Verspieren - Caisse d'Epargne - AFNOR - Souriau - MTV - Capem - Institut Mutualiste Montsouris - Dassault Systèmes - Gaz de France - CAPRI Immobilier - Croix-Rouge Française - Groupama - Crédit Agricole - Groupe Accueil - Eurordis - CDC Arkhineo

Applications décisionnelles

IEDOM – Yves Rocher - Bureau Veritas - Mindscape – Horus Finance – Lafarge – Optimus – CecimObs – ETS Europe – Auchan Ukraine – CDiscount – Maison de la France – Skyrock – Institut National de l'Audiovisuel – Pierre Audouin Consultant – Armée de l'air – Jardiland – Saint-Gobain Recherche – Xinek – Projectif – Companeo – MeilleurMobile.com – CG72 – CoachClub

Ce livre blanc

Ce livre blanc, consacré aux principes et outils des VPN, les réseaux virtuels privés, appartient à une collection traitant des outils d'infrastructure, dans laquelle on peut ranger également le livre blanc intitulé « Plateformes web Hautes Performances - Principes d'architecture et outils open source », paru début 2009, et le livre blanc consacré aux firewalls.

Selon le schéma habituel de nos livres blancs, nous présentons ici à la fois les concepts fondamentaux, et une sélection des meilleurs outils.

Nous exposons les caractéristiques de chacun, les possibilités et outils de leur mise en œuvre et configuration, afin d'aider le lecteur dans la sélection d'outils adaptés à chaque contexte d'utilisation.

Table des matières

2 Introduction

2.1 Le réseau d'entreprise

Le réseau est au cœur de la productivité d'une entreprise, et évolue en même temps qu'elle, au fil de sa croissance, d'acquisitions, de partenariats, de ses besoins de mobilité. Le réseau qui relie l'ensemble des équipements au sein d'un même site géographique est généralement la propriété de l'entreprise, tandis que les interconnexions entre ces sites empruntent le plus souvent des infrastructures publiques ou du moins non sécurisées.

On appelle *Réseau Privé Virtuel,* en anglais *Virtual Private Network ou donc « VPN »,* l'ensemble des techniques permettant d'étendre le *Réseau* de l'entreprise en préservant la confidentialité des données (*Privé*) et en traversant les barrières physiques des réseaux traditionnels (*Virtuel*).

Certaines entreprises n'ont pas les moyens, ni parfois même l'intérêt, d'avoir des liens d'interconnexion dédiés. La mise en place d'une interconnexion par VPN leur permet alors de connecter leurs propres réseaux au travers d'un réseau public, en particulier Internet, à des coûts beaucoup plus faibles tout en conservant les garanties de sécurité nécessaires.

Les solutions VPN apportent généralement les bénéfices suivants :

- Authentification par clé publique (bien plus sécurisée qu'un mot de passe)
- Confidentialité des échanges (chiffrement)
- Confidentialité a posteriori en cas de compromission des secrets cryptographiques
- Transport de paquets à destination d'un réseau privé via un réseau public (encapsulation)

Le principal inconvénient à l'utilisation d'un VPN porte sur les performances, puisque le réseau Internet que l'on emprunte ne possède pas les garanties de qualité de service d'un réseau dédié. Nous verrons plus loin que l'encapsulation et le chiffrement ont également un coût en matière de performances.

2.2 Principes

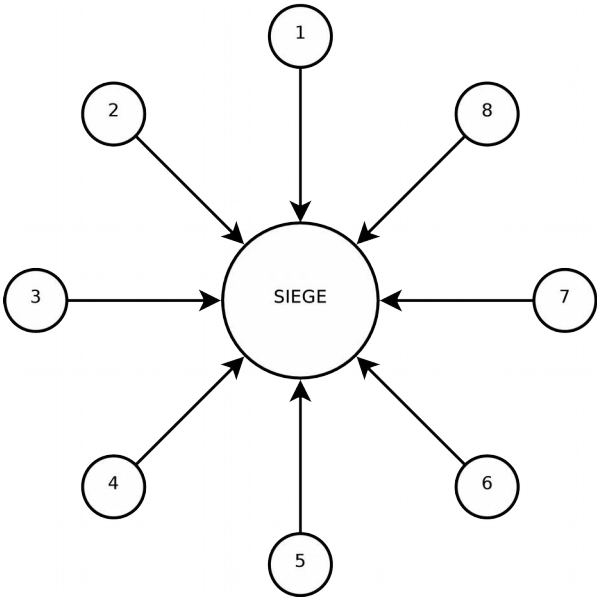
On distingue généralement deux types de besoins pour les connexions au réseau d'entreprise :

- Les connexions d'un employé au réseau

- L'interconnexion entre deux branches de l'entreprise

En effet, si l'objectif est similaire, et si les moyens techniques mis en jeu sont souvent les mêmes, les différences conceptuelles entre ces deux types d'accès font qu'on utilisera le plus souvent des solutions différentes pour gérer ces deux cas.

La connexion d'un employé au réseau relève d'une approche de type client-serveur. Le serveur est un concentrateur VPN central sur lequel chaque employé se connecte, obtenant ainsi, après authentification, l'accès aux ressources de l'entreprise. Bien souvent, les clients de ce VPN ne peuvent communiquer entre eux, hormis via une ressource du réseau (serveur de messagerie, etc.). La connexion du réseau d'une filiale au siège de l'entreprise peut parfois s'effectuer suivant le même principe. Par exemple, de grandes entreprises très centralisées, peuvent reposer sur un modèle en étoile :



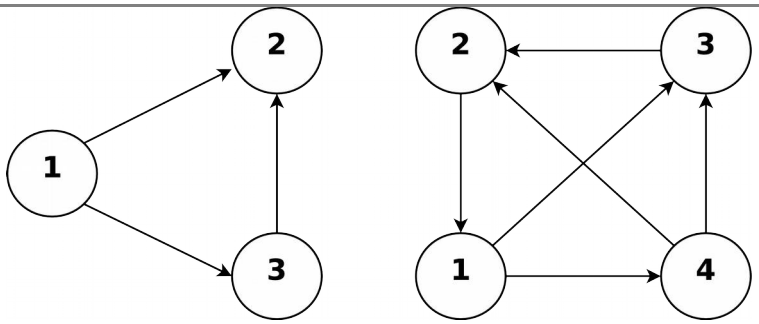
Cela ressemble beaucoup à la connexion d'employés au réseau central, mais à double sens : le réseau central peut à son tour accéder au réseau auxiliaire, permettant par exemple l'administration des postes de travail à distance.

En revanche ce modèle est très peu performant dès lors que les réseaux périphériques essaient de communiquer entre eux, puisque tout le trafic passe alors par un goulot d'étranglement central.

2.2.1 Interconnexion

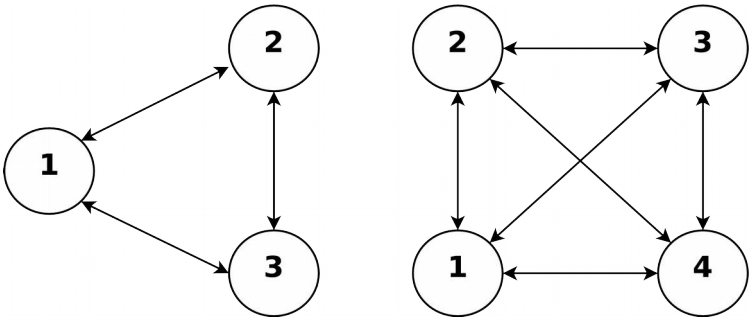
Dans d'autres entreprises, ce modèle n'est pas pertinent. Par exemple, une entreprise structurée en agences indépendantes de taille identique échangeant fréquemment des données ne peut pas fonctionner sur un modèle en étoile. Dans ce cas, il n'est pas possible non plus de définir un "serveur" autrement que de façon arbitraire.

La connexion entre plusieurs entités peut poser de véritables casse-têtes d'administration :



Dès que l'on dépasse 3 entités, l'égalité entre les nœuds n'est pas retranscrite dans la topologie réseau : certains d'entre eux doivent être arbitrairement désignés comme des serveurs.

Heureusement, nous verrons que certaines protocoles de VPN ne fonctionnent pas selon le modèle client-serveur, mais suivant un principe décentralisé. Dans ce cas la configuration se fait de façon identique sur chaque équipement.



On retrouve alors un meilleur équilibre entre les nœuds.

L'interconnexion entre *n* nœuds nécessite $\frac{n(n-1)}{2}$ liens.

Dans tout les cas, il est important que la topologie du VPN d'interconnexion reflète le fonctionnement de l'entreprise.

2.2.2 Tunnel

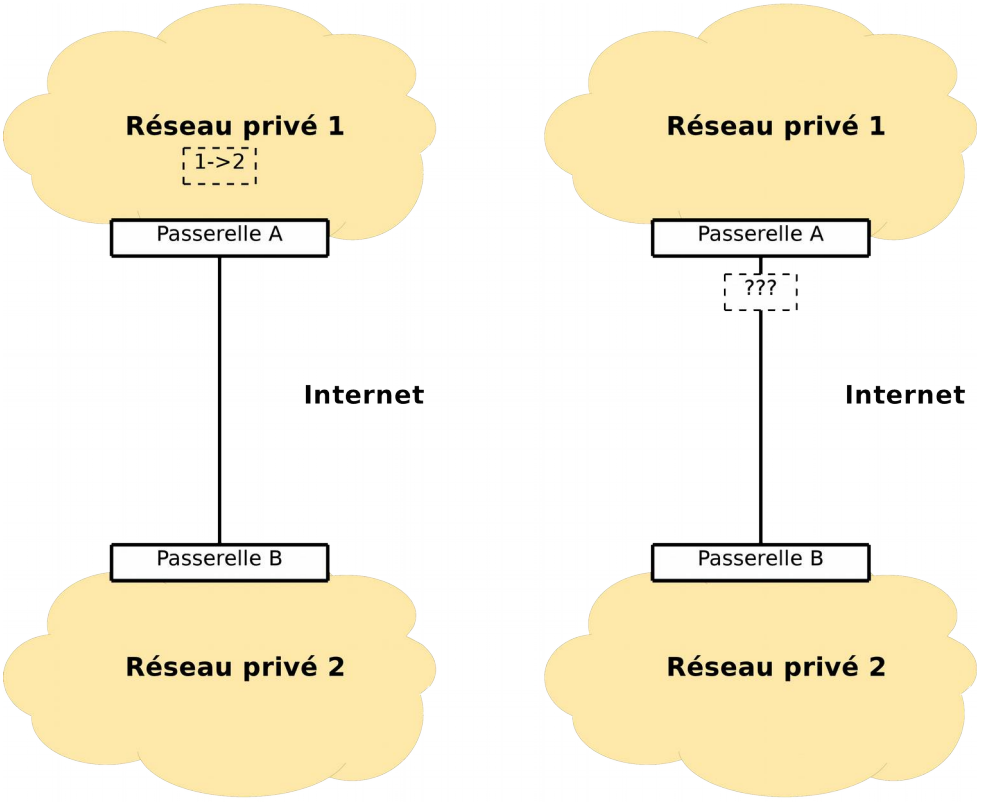
Dans chacun des cas cités, le VPN permettra d'établir un « *tunnel* », soit entre un poste et un réseau, soit entre deux réseaux.

Un tunnel est une connexion réseau virtuelle, dont le trafic est en réalité dirigé vers une autre interface réseau après avoir subi un traitement, généralement une encapsulation et le chiffrement des informations contenues dans la trame.

L'encapsulation permet, comme mentionné plus haut, de masquer la véritable destination d'une trame réseau dans le cas où celle-ci serait à destination d'une IP privée. En effet, la plupart des réseaux d'entreprise utilisent des adresses privées, car l'obtention d'adresses publiques pour un usage interne pose de lourds problèmes administratifs et est devenue impossible en raison de la pénurie d'adresse Ipv4. Elle est

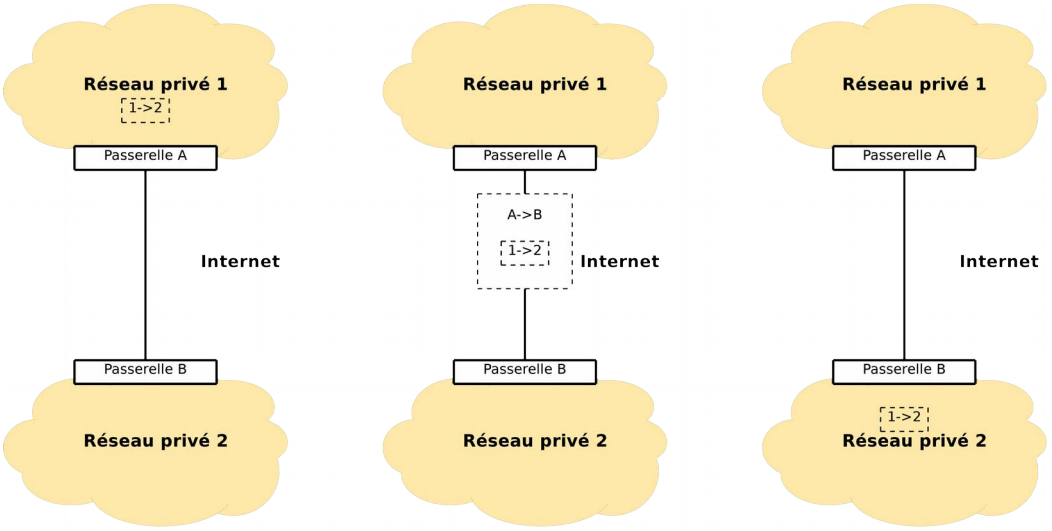
de ce fait réservée aux pionniers d'Internet (militaires, universités, entreprises de télécom...).

Sans un VPN, une trame à destination d'un réseau privé ne peut pas circuler sur Internet :



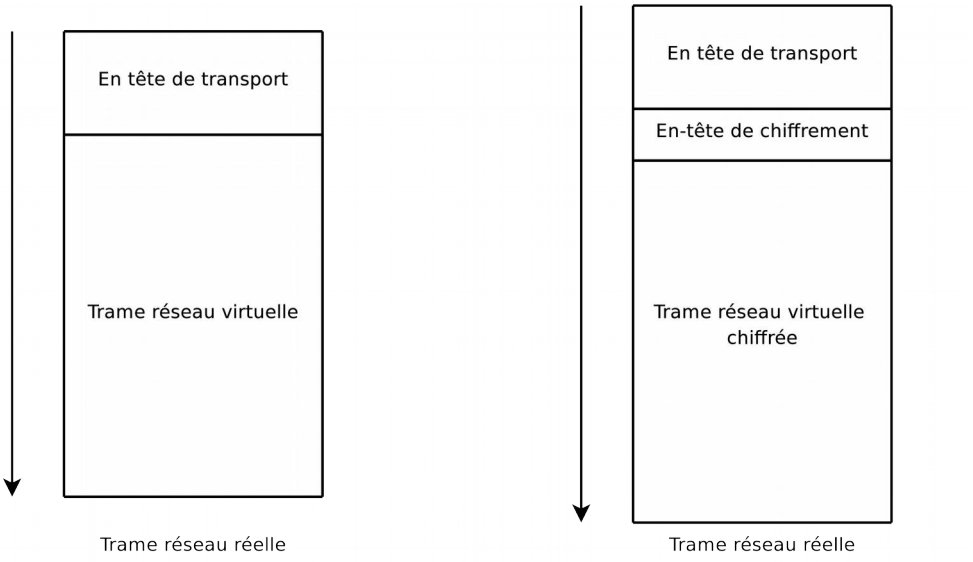
Pas de VPN : lorsqu'il quitte le réseau 1, le paquet n'est plus routable

En revanche, via l'encapsulation, on embarque cette trame dans une trame routable sur Internet, et voici ce que devient le schéma précédant :



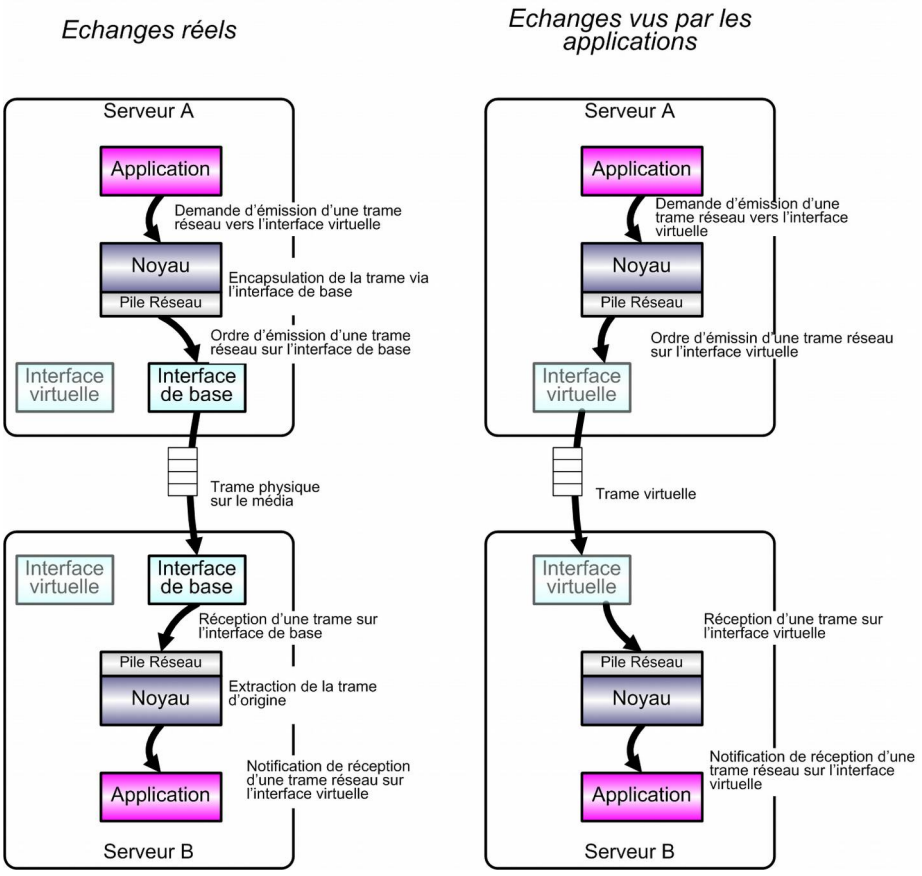
Avec un VPN : le paquet est encapsulé dans un paquet routable sur Internet

Une trame encapsulée ressemble à ceci :



Encapsulation simple **Encapsulation + chiffrement**

Au niveau du système d'exploitation, une interface virtuelle sert à rendre transparent le traitement de la trame. Ainsi n'importe quelle application peut fonctionner sans avoir connaissance du VPN :



Il est bien sûr possible d'enchaîner les tunnels, si l'interface de base est une interface virtuelle, le même processus se répète sur cette interface, encapsulant une nouvelle fois le trafic, et ce jusqu'à retomber sur une interface physique de la machine, qui enverra réellement la trame sur le fil.

Dimensionnement

L'encapsulation, en particulier lorsqu'elle est complétée par le chiffrement des échanges, présente un coût non négligeable. C'est pourquoi les équipements VPN sont souvent dédiés, ou cohabitent avec des firewalls réseau qui consomment peu de ressources. Le coût de l'encapsulation est rarement limitant pour peu que l'on utilise des serveurs récents. Un serveur bas de gamme encaissera sans problèmes 10 Mbps de trafic chiffré, un serveur un peu plus performant et équipé de cartes réseau haut de gamme pourra assurer des connexions entre réseaux plus rapides (au dessus de 100 Mbps). Ces limites apparaissent en revanche beaucoup plus vite sur des équipements dédiés possédant des processeurs de faible puissance.

Il est également utile de noter que certains serveurs ou équipements spécialisés peuvent être équipés de puces d'accélération cryptographique, qui assurent le support d'un ou plusieurs mécanismes de chiffrement. Pour peu que l'on configure un mécanisme supporté au niveau du logiciel qui assure le chiffrement, et que le système d'exploitation supporte cette fonctionnalité, le processeur sera considérablement déchargé.

3 Les VPN Open Source

L'open source étant un mouvement pionnier en matière de technologies réseau, l'offre en matière de VPN est très fournie. Nous avons cependant choisi de présenter les produits les plus matures, qui sont des références dans leur domaine.

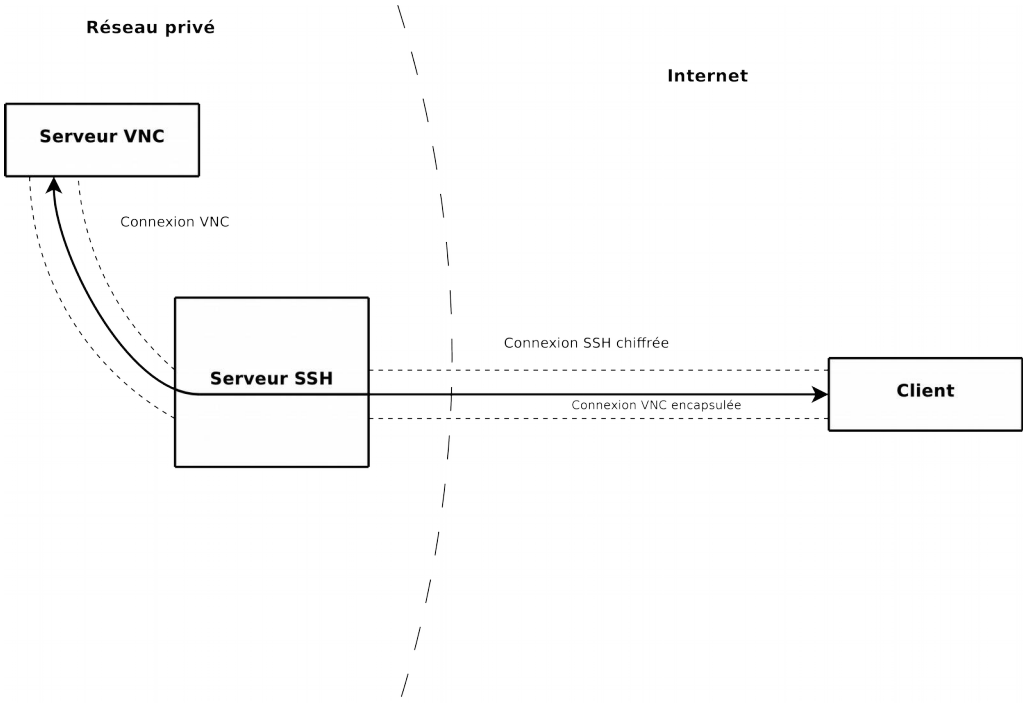
3.1 OpenSSH

OpenSSH est le logiciel le plus utilisé pour l'export de console, il est utilisé sur près de 90% des serveurs de type UNIX dans le monde, pour les tâches d'administration. Au fil des années, *OpenSSH* s'est étoffé de nombreuses fonctionnalités qui permettent de l'utiliser bien au delà de la classique « console réseau » que tous les administrateurs UNIX connaissent bien. Précisons qu'il ne s'agit pas à proprement parler d'une solution de VPN « traditionnelle », mais elle fournit les mêmes services à plus petite échelle.

3.1.1 Redirection de port

La fonctionnalité « alternative » la plus connue de SSH est la redirection de ports.

Une fois connecté à un serveur via une connexion SSH, un client peut demander à ce que le serveur lui « transmette » des connexions vers d'autres machines, à la manière d'un proxy via une encapsulation du trafic. L'une des principales applications de cette technique est de sécuriser un protocole qui initialement ne l'est pas, par exemple VNC :



Ici, le serveur de destination n'est pas accessible depuis Internet car VNC n'est pas un protocole sûr. En revanche, il est accessible depuis le serveur passerelle SSH, lui-même accessible depuis Internet. Le client va donc s'authentifier auprès du serveur SSH, puis ouvrira une connexion VNC qui sera en clair entre le serveur et la passerelle SSH, puis chiffrée de la passerelle à l'utilisateur.

Une autre possibilité est l'ouverture d'un proxy dynamique. Une fois connecté, le client peut utiliser le serveur SSH comme un proxy SOCKS, et s'en servir pour relayer les connexions vers la plupart des services réseau, notamment les mails, la navigation web, etc.

Cette possibilité n'étant pas limitée à un seul serveur à la fois, elle se rapproche d'une configuration VPN.

Ces applications de *OpenSSH* sont utiles dans certaines circonstances, et offrent certains avantages du VPN pour un coût de mise en place extrêmement faible. Cependant elles sont vite limitées, et réservées aux utilisateurs avertis, par exemple des administrateurs réseau.

3.1.2 Tunnel sécurisé

Les techniques de la partie précédente sont généralement utilisées pour des accès au réseau par un utilisateur. *OpenSSH* propose aussi une solution d'interconnexion entre réseaux plus robuste : la redirection d'interface.

Elle permet de « partager » une carte réseau virtuelle entre deux machines? Il s'agit d'une solution plus souple car l'ensemble des capacités réseau de Linux sont accessibles (routage, filtrage, haute disponibilité, etc.). L'ensemble des trames réseau envoyées sur cette carte virtuelle, dans un sens comme dans l'autre, réapparait sur l'autre machine, après avoir été chiffré et transmis au travers la connexion SSH.

Cette technique permet de monter rapidement un VPN entre deux machines UNIX pour un besoin ponctuel, elle est cependant peu utilisée pour de l'interconnexion définitive, au profit de solutions plus interopérables et configurables.

OpenSSH offre donc des possibilités de VPN réduites, pratiques pour une mise en place d'accès rapide. Cependant l'absence de connexion avec un annuaire ou d'intégration dans une PKI rend le déploiement de *OpenSSH* à grande échelle difficile.

3.2 *OpenVPN*

OpenVPN est le fer de lance d'une catégorie de VPN assez récente : les VPN SSL. Ces derniers réutilisent les mécanismes du chiffrement SSL pour authentifier et chiffrer les connexions.

OpenVPN est basé sur le produit *OpenSSL*, la principale implémentation libre du protocole SSL, tant en terme de qualité que d'adoption, et s'appuie sur ses routines de chiffrement et de vérification d'identité pour assurer une très bonne sécurisation des données.

L'utilisation de *OpenVPN* requiert une PKI X509, comme tout système basé sur SSL. L'avantage est bien sûr de pouvoir réutiliser une PKI existante, le certificat personnel d'un utilisateur lui permettant de s'authentifier auprès du VPN.

3.2.1 Principe

OpenVPN est une solution relativement complète qui permet plusieurs modes de fonctionnement, plusieurs modes d'encapsulation et plusieurs méthodes d'authentification. Le point fort d'*OpenVPN* est sa capacité à fonctionner presque sans configuration dès lors que l'on possède une PKI. Ce qui le rend très attractif pour la mise en place d'une solution de connexion à distance pour les employés d'une entreprise.

3.2.2 Poste à réseau

Les avantages de *OpenVPN* en mode poste à réseau sont multiples, citons :

- Intégration immédiate dans une PKI X509
- Ne nécessite qu'un flux réseau sur le port 1194 (TCP/UDP au choix) : les clients peuvent donc sans aucun problème se situer derrière un équipement faisant des translations d'adresse.
- Possibilité de traverser les proxies HTTPS, par exemple pour une utilisation depuis un réseau d'entreprise.
- Possibilité de configurer le serveur pour tester la validité des certificats selon n'importe quel critère (LDAP, Active Directory, RADIUS, etc.)
- Disponible sous Windows, Mac, et UNIX

3.2.3 Réseau à réseau

OpenVPN est particulièrement adapté aux configurations poste à réseau, mais il est également utilisable en interconnexion de réseaux.

Dans ce cas de figure, son principal problème est sa dissymétrie, comme évoqué en début de ce livre blanc : il est indispensable de désigner une machine « cliente » et une machine « serveur » ce qui n'a pas vraiment de sens dans une interconnexion un pour un. Cette dissymétrie se retrouve aussi bien au niveau de la connexion proprement dire (si TCP est utilisé) que au niveau de l'authentification (le serveur vérifie l'identité du client). De plus l'administration est considérablement alourdie car il est nécessaire d'écrire un fichier de configuration par serveur distant sur chaque nœud, et d'ouvrir un port du firewall pour chaque connexion côté serveur. Par exemple pour interconnecter complètement 6 nœuds il y a 15 connexions, donc 15 ouvertures de port à faire, et ainsi de suite.

OpenVPN en mode réseau à réseau n'est donc adapté qu'à de petites infrastructures, et on lui préférera *IPsec* dès que le nombre de réseaux à interconnecter dépassera 4 ou 5.

3.3 IPsec

3.3.1 Introduction

Contrairement à *OpenVPN*, les VPN de type *IPsec* n'utilisent pas SSL, mais des protocoles de niveau 3 dédiés : *ESP* et *AH.*

ESP est un protocole qui permet d'assurer la confidentialité et l'intégrité des trames. Il est donc plus utilisé que *AH* qui lui n'assure que l'intégrité. Cependant, contrairement à *AH*, ce protocole ne garantit pas l'intégrité du niveau 3, ce qui permet de l'utiliser dans des situations de type NAT (où le niveau 3 du paquet est modifié pendant le trajet). En pratique, la plupart des solutions *IPsec* en mode client à réseau implémentent le NAT-T (traversée de NAT), qui encapsule le trafic ESP dans des paquets UDP, leur permettant ainsi de traverser plus facilement les passerelles réseau.

Il existe deux modes d'utilisation de *IPsec* : le mode transport, et le mode tunnel.

Le mode transport est celui qui nous intéresse le moins: il permet simplement de chiffrer le trafic entre deux machines à partir du niveau 4. Ce mode est donc idéal lorsque le routage est fait en amont et que les échanges réseaux ont lieu sur un canal de communication non sécurisé. Une utilisation typique de cette utilisation est la protection d'un réseau Wifi.

Voici le fonctionnement détaillé du mode transport :

- Un paquet a été routé à destination d'une machine protégée par *IPsec*
- Les données (niveau 4) du paquet sont chiffrées et encapsulées dans un nouveau paquet ESP
- Le paquet ESP est envoyé à la destination
- La destination reçoit le paquet en provenance d'une source protégée par *IPsec*
- La destination déchiffre le paquet et le traite.

L'autre mode d'utilisation de *IPsec* est le mode tunnel, qui permet une encapsulation de toute la trame à partir du niveau 3. Chaque tunnel possède une adresse « de sortie » vers laquelle est envoyé l'ensemble du trafic.

Voici le fonctionnement détaillé du mode tunnel :

- Un paquet arrive à l'entrée du tunnel, à destination du réseau de sortie.
- La destination et les données (niveau 3) du paquet sont chiffrés et encapsulés dans un nouveau paquet ESP
- Le paquet ESP est envoyé à l'autre extrémité du tunnel.
- Cette dernière reçoit le paquet en provenance de l'entrée du tunnel *IPsec*

- La sortie du tunnel déchiffre le paquet, et l'envoie à sa destination d'origine.

On voit bien que le mode tunnel permet de "coller" virtuellement deux réseaux initialement disjoints, alors que le mode transport ne fait qu'assurer la sécurité des données transmises. On est bien dans un cas de réseau privé virtuel.

Il existe une idée préconçue selon laquelle *IPsec* est exclusivement un protocole de VPN. En réalité *IPsec* est simplement un protocole de sécurisation des échanges réseau qui permet, dans un de ses modes de fonctionnement, de mettre en place un VPN.

3.3.2 Généralités

IPsec est un protocole complexe, qui nécessite l'utilisation de multiples secrets cryptographiques dont la configuration est bien trop lourde pour être gérée facilement par un administrateur : il faudrait qu'il intervienne à chaque établissement de session. C'est pourquoi on utilise généralement un troisième protocole, *IKE*, pour automatiser une grande partie de la négociation. *IKE* permet de négocier l'établissement de tous les paramètres du tunnel en se basant sur :

- Un mot de passe partagé
- Un certificat X509
- Une clé publique DSA (similaires à l'authentification SSH)
- D'autres critères selon les implémentations (mot de passe, etc.)

IPsec possède quelques sérieux avantages par rapport aux autres solutions présentées ici :

- Le protocole est un standard industriel, il est implémenté dans de nombreux équipements réseaux de différentes constructeurs. Le choix de *IPsec* est donc un gage d'interopérabilité y compris avec des solutions propriétaires.
- Le protocole est mature et très répandu, ses implémentations sont éprouvées.
- En termes réseau, le protocole fonctionne sur un port bien défini quel que soit le nombre de clients, il suffit d'ouvrir le firewall une seule fois pour supporter tout les futurs tunnels. *IPsec* se prête très bien à de gros équipements centraux supportant des centaines de tunnels.

En revanche :

- La configuration d'un VPN *IPsec* est complexe, même avec le système IKE.
- Au sein d'une même implémentation, la configuration est souvent simplifiée. En revanche dès que l'on souhaite se connecter à une implémentation différente il faut configurer tous les paramètres explicitement.
- Certaines implémentations proposent des fonctionnalités avancées qui ne sont pas disponibles dans d'autres (notamment pour l'authentification).

3.3.3 IPsec sous Linux et *FreeBSD*

FreeBSD a été l'un des premiers systèmes dotés d'une implémentation *IPsec*. Cette implémentation à été initiée par le projet KAME, un conglomérat d'universités et de sociétés de télécommunications japonaises. *KAME* s'est rendu célèbre pour avoir été un pionnier d'IPv6, dont les fonctions de sécurité ont été récupérées pour devenir *IPsec*.

Nous mentionnerons par la suite *FreeBSD* car c'est l'OS de la famille BSD le plus connu, mais *NetBSD* et *DragonflyBSD* fonctionnent exactement de la même façon, ayant eux-aussi hérité des travaux de KAME. Seul *OpenBSD,* qui sera détaillé plus loin, possède une implémentation différente.

IPsec est un protocole fortement intégré dans les noyaux de *Linux* et de *FreeBSD*, presque transparent, contrairement à *OpenVPN* qui lui est beaucoup plus « haut niveau » : il utilise sa propre interface virtuelle et est presque entièrement géré par un processus au lieu de fonctions noyau.

L'implémentation du protocole *IPsec* sous ces deux systèmes est en deux parties. D'une part on retrouve l'implémentation coté noyau des protocoles de chiffrement et d'encapsulation, et d'autre part les outils permettant l'administration et le démon IKE pour l'échange des clés. Ces outils sont la partie visible de l'implémentation et sont communs à Linux et *FreeBSD* : leur nom officiel est « *IPsec Tools* ». Notons à titre de curiosité que si Linux et *FreeBSD* utilisent une implémentation noyau différente, tout deux partagent ces mêmes outils, issus du projet KAME.

La configuration de ces outils se fait en deux temps :

- Configuration côté noyau
- Configuration de l'échange de clés

Il est possible de ne configurer que le noyau si on spécifie tous les paramètres de la session *IPsec* manuellement, à des fins de test. À l'inverse, il est possible d'utiliser le démon d'échange de clés pour mettre en place les réglages du noyau si il fonctionne en mode passif, c'est à dire s'il ne fait qu'attendre les connexions de clients.

La configuration est assez peu intuitive. Voici une règle qui définit un tunnel entre deux réseaux (10.0.1.0/24 et 10.0.2.0/24), dont les passerelles respectives sont 192.168.1.1 et 192.168.2.1 (on se place sur la passerelle 192.168.1.1, les règles sont naturellement inversées sur l'autre passerelle) :

```
spdadd 10.0.1.0/24 10.0.2.0/24 any -P out ipsec
        esp/tunnel/192.168.1.1-192.168.2.1/require ;
spdadd 10.0.2.0/24 10.0.1.0/24 any -P in ipsec
        esp/tunnel/192.168.2.1-192.168.1.1/require ;
```

Et la configuration associée au niveau du démon IKE (*racoon*) :

```
# Phase 1 : connexion  la passerelle distante et établissement d'une session
# chiffre au moyen d'un mot de passe partagé
```

```
remote 192.168.2.1 {
        exchange_mode main;
        proposal {
                encryption_algorithm 3des;
                hash_algorithm md5;
                authentication_method pre_shared_key;
                dh_group modp1024;
        }
}

# Phase 2 : négociation du tunnel

sainfo address 10.0.1.0/24 any address 10.0.2.0/24 any {
        encryption_algorithm 3des;
        authentication_algorithm hmac_md5;
        compression_algorithm deflate ;
}
```

3.3.4 IPsec sous *OpenBSD*

OpenBSD utilise une implémentation et des outils d'administration similaires à *FreeBSD* et Linux, ses principales différences sont :

- Un seul fichier de configuration pour le noyau et le démon *IKE*
- Syntaxe beaucoup plus accessible que *IPsec Tools*
- Présence d'un démon de synchronisation des associations de sécurité pour assurer la redondance de la passerelle *IPsec* et la bascule sans interruption de service en cas de panne ou d'arrêt de maintenance.

La configuration de *IPsec* sous *OpenBSD* est particulièrement simplifiée. Voici le fichier de configuration établissant un tunnel entre les deux passerelles de l'exemple précédent sous *OpenBSD* :

```
ike esp from 10.0.1.0/24 to 10.0.2.0/24 peer 192.168.2.1
```

Contrairement à l'exemple précédent, il n'y a aucune redondance, le tunnel et l'échange de clés sont configurés au même endroit. Bien entendu cette simplicité de la syntaxe cache une grande part d'implicite: dès lors qu'on voudra établir un tunnel avec un autre système que *OpenBSD*, il faudra préciser les paramètres comme l'algorithme de chiffrement utilisé, la durée des sessions, etc. De même si l'on souhaite mettre en place une politique *IPsec* plus complexe qu'un simple tunnel.

3.4 Openswan

Openswan est une implémentation *IPsec* pour Linux, descendante du projet *FreeS/WAN* qui fût la première implémentation complète de *IPsec* sous Linux avant d'être abandonné pour une implémentation officielle couplée à *IPsec Tools*.

En comparaison à *IPsec Tools*, *Openswan* présente l'avantage d'une configuration plus simple, centralisée dans un seul fichier :

```
conn net-to-net
  left=192.168.1.1
  leftsubnet=10.0.1.0/24
  leftid=192.168.1.1
  leftnexthop=%defaultroute     # correct in many situations
  right=192.168.2.1
  rightsubnet=10.0.2.0/24
  rightid=192.168.2.1
  rightnexthop=%defaultroute    # correct in many situations
  auto=add
```

4 Outils d'administration

Comme pour les firewalls, il existe des outils intégrés permettant d'administrer plus facilement des VPN.

La plupart des distributions « firewall » comme *IPCop* ou *pfSense*, proposent une interface pour la mise en place de VPN via plusieurs protocoles, le plus souvent *OpenVPN* et *IPsec*. Ces outils permettent de faciliter l'administration au quotidien et de mettre facilement en place un VPN pour un administrateur qui ne maîtrise pas toutes les subtilités d'un protocole comme *IPsec*. En revanche, pour des gros sites comportant des centaines de tunnels, l'utilisation de scripts ou de fichiers de macros pour générer les configurations s'avèrera souvent plus efficace qu'une interface cliquable.

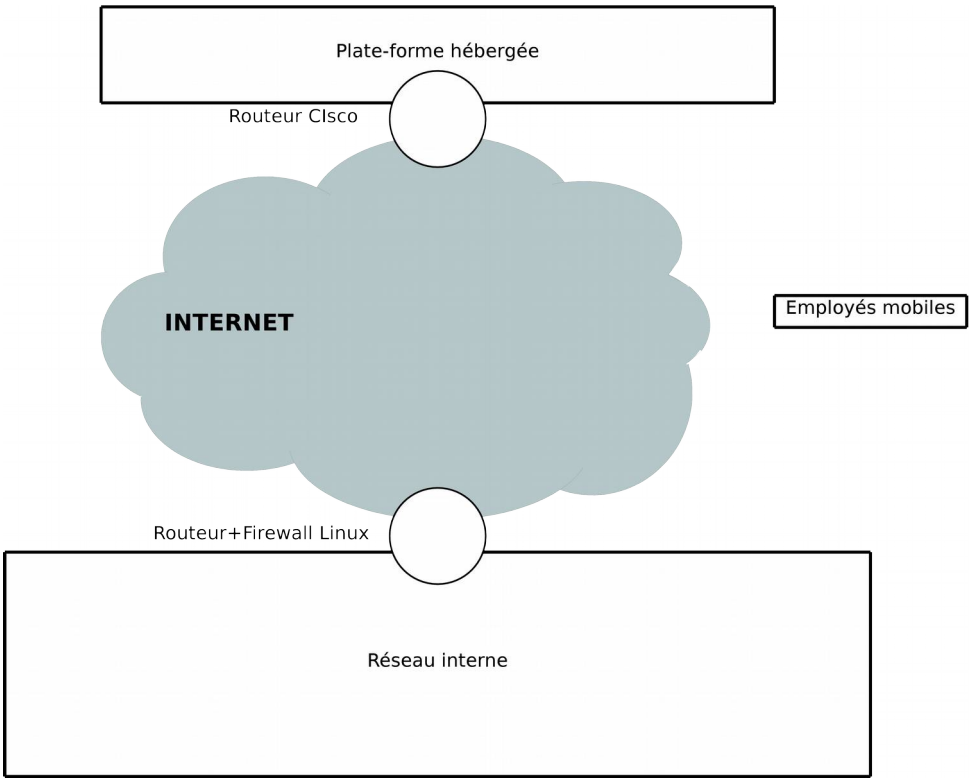
5 Exemples d'architectures et retours d'expérience

Après cette présentation des outils et principes, nous allons maintenant présenter quelques cas d'utilisation courants de solutions VPN.

5.1 PME

Le premier exemple sera une petite entreprise disposant d'une seule implantation. L'entreprise a externalisé une partie de ses ressources informatiques dans un datacenter, mais n'a pas les moyens d'un lien d'interconnexion dédié. De plus, l'entreprise souhaite permettre à certains de ses employés de travailler à distance.

Voici le schéma de la situation :



Côté hébergeur, le seul équipement de routage disponible est un routeur Cisco, compatible IPsec. Côté local, l'entreprise utilise une passerelle Linux servant de routeur et pare-feu. Le choix de *IPsec* pour l'interconnexion entre les deux réseaux est donc naturel. Cependant, il aurait été possible d'utiliser un des serveurs hébergés pour servir de passerelle pour une autre solution de VPN, telle que *OpenVPN*. Mais cette solution compliquerait légèrement le routage.

Pour la connexion des employés mobiles au réseau, il est également possible d'utiliser un client Cisco pour se connecter directement à la plate-forme hébergée, et mettre en place une deuxième solution de VPN pour la connexion au réseau interne.

Cependant, pour une plus grande souplesse, l'entreprise a choisi *OpenVPN*, et ce pour plusieurs raisons :

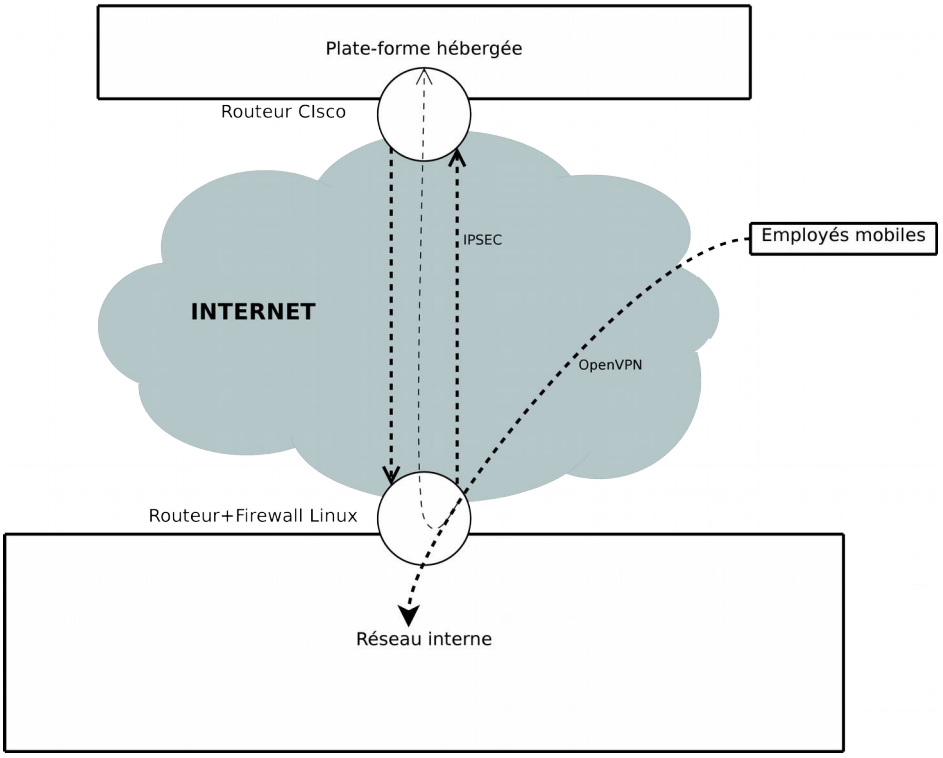
- Les employés n'ont qu'un logiciel client à gérer
- *OpenVPN* permet de gérer finement les droits d'accès en consultant l'annuaire de l'entreprise.
- *OpenVPN* permet de router le trafic aussi bien vers le réseau interne que vers le réseau hébergé à travers le tunnel *IPsec* d'interconnexion.

En revanche, cette solution présente quelques inconvénients :

- Elle est dépendante de l'état de la connexion de l'entreprise à Internet
- Si le client accède à la plate forme hébergée, les trames réseau font un allez-retour entre Internet et le routeur, ce qui est consommateur de bande passante.

Cette solution part bien sûr du principe que les clients nomades sont intéressés avant tout par les ressources présentes sur le réseau interne et non sur le réseau hébergé. En effet, si les connexions des clients nomades se font en majorité vers le réseau hébergé, il sera plus efficace de les y connecter directement. De même, si elles représentent la moitié de l'utilisation du VPN, une connexion double aux deux réseaux est envisageable. Dans notre exemple, cependant, cette possibilité n'est laissée qu'a titre de commodité, et représente une petite partie du trafic.

Voici la situation finale :



Cette solution nous permet de constater deux choses :

- Elle montre qu'on peut mettre en place, sur le même équipement, des fonctions de filtrage, de routage et de VPN. C'est un cas relativement classique surtout dans les petites entreprises où une seule machine fait office de passerelle. Des produits intégrés comme *IPCop* ou *pfSense* se prêtent très bien à ce rôle.

- Elle montre que deux technologies de VPN peuvent cohabiter sur une même machine.

Le dernier point mérite quelques éclaircissements : toutes les solutions de VPN ne sont pas par nature cumulables sur un même équipement réseau. Selon que l'encapsulation est effectuée à telle ou telle étape du traitement des trames, il peut y avoir des conflits. Dans la pratique, les solutions essayent de limiter leur impact et de se reposer sur des infrastructures standard (interfaces virtuelles, routage, etc.) de manière à être aussi transparentes que possible.

Dans la pratique, *IPsec* et *OpenVPN* peuvent cohabiter sur un même serveur, mais le routage des trames provenant de *OpenVPN* directement dans un tunnel *IPsec* établi sur la même machine nécessite une configuration particulièrement subtile.

5.2 Grande entreprise

Dans ce deuxième exemple, on s'intéresse à une entreprise plus importante possédant :

- Un siège hébergeant des applications métier.
- Plusieurs agences, dont certaines hébergent leurs propres applications.
- Une filiale à l'étranger qui ne permet pas la mise en place d'un lien réseau dédié.
- Des employés en déplacement ou en télétravail susceptibles de se connecter au réseau (leur poste, les applications, etc.).
- Un prestataire qui assure la maintenance de certaines applications.
- Un réseau Wifi au siège, pour les visiteurs et les employés en réunion.

La mise en place de différents VPN permet de répondre aux besoins suivants :

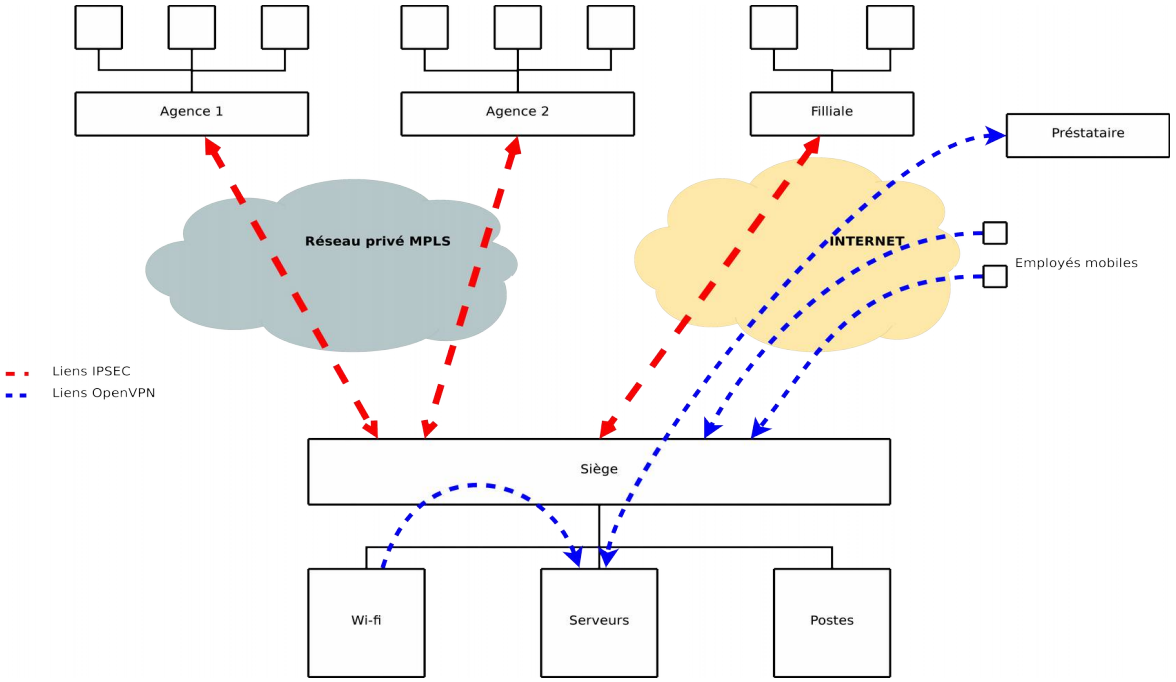
- VPN 1 : Interconnecter les réseaux d'agence en garantissant la sécurité des transmissions.
- VPN 2 : Connecter la filiale au réseau à travers Internet
- VPN 3 : Permettre aux employés de se connecter au réseau
- VPN 4 : Permettre au prestataire de se connecter aux serveurs dont il a la charge
- VPN 5 : Permettre aux utilisateurs du Wifi de se connecter aux applications internes de façon sécurisée.

Chacun de ces VPN a des objectifs différents :

	Authentifier les utilisateurs	**Assurer la confidentialité**	**Permettre l'accès à un réseau non-routable**
VPN 1		x	
VPN 2		x	x
VPN 3	x	x	x
VPN 4		x	x

VPN 5	x	x	

La solution suivante a été retenue :



Voyons à présent les détails.

5.2.1 VPN 1 : Interconnexion d'agences sur un lien dédié

Il s'agit plus d'un cas d'école que d'un réel besoin, la présence d'un lien dédié permet d'éliminer la plupart des problèmes d'interconnexion, en particulier de routage, que l'on peut rencontrer habituellement sur Internet.

Cependant, par sécurité, il est préférable de protéger par un VPN les données qui circulent entre les filiales, afin d'être certain que les échanges ne sont pas espionnés ou pire, altérés, par une personne s'étant introduite dans un local technique avec un analyseur de trames par exemple.

Le besoin est donc relativement facile à satisfaire, il s'agit d'un candidat désigné pour *IPsec* en mode transport : pas de modification des adresses réseau puisqu'on reste sur le réseau privé de l'entreprise, et pas de problématique d'authentification complexe.

5.2.2 VPN 2 : Interconnexion d'agences via Internet

Il s'agit cette fois d'un cas courant : la protection des données circulant sur Internet est une nécessité, et il est indispensable d'utiliser de l'encapsulation de paquets pour pouvoir router entre deux réseaux privés.

Ici encore, le choix est rapide : *IPsec* en mode tunnel est tout désigné. De plus l'interopérabilité de *IPsec* fait que si la filiale provient d'un rachat, les chances de s'interconnecter facilement avec les équipements existants sont très élevées.

5.2.3 VPN 3 : Connexion des employés mobiles

Comme nous l'avons déjà évoqué, ce type de VPN est assez différent des deux premiers : en effet les clients n'ont pas d'IP fixe, et souhaitent seulement accéder à des ressources et non rendre leurs propres ressources accessibles. D'autre part, il doit être possible d'authentifier chaque connexion bien qu'elles proviennent d'IP inconnues à l'avance, et il faut pouvoir anticiper les problèmes tels que le vol de matériel.

OpenVPN permet de répondre à ces besoins, en s'intégrant facilement dans la PKI de l'entreprise (ou en fournissant les outils pour créer une PKI s'il n'en existe pas), et en permettant une authentification forte : le client devra d'une part posséder un certificat valide, et d'autre part fournir son login et son mot de passe au moment de la connexion pour être accepté. De plus, des contrôles au niveau de l'annuaire permettront de restreindre l'accès aux membres d'un groupe prédéterminé.

Tous ces mécanismes sont présents dans *OpenVPN* et ne demandent que très peu de configuration : il suffit d'écrire quelques courts scripts pour mettre en place les contrôles côté serveur. Cette architecture permet de changer facilement le mode d'authentification en fonction des besoins, par exemple en cas de changement d'annuaire, ou si l'on souhaite intégrer la notion de plage horaire.

Cette solution présente cependant un inconvénient : *OpenVPN* nécessite un logiciel installé sur les postes client (il est cependant multi-plateformes et léger), et n'est pas toujours disponible sur les équipements tels que les PDA.

5.2.4 VPN 4 : Connexion temporaire avec un prestataire de services

Ce cas est similaire au VPN 3 : on souhaite permettre l'accès à des ressources internes depuis l'extérieur. La courte durée de vie de cet accès, et la relation entre les deux intervenants font qu'un système client-serveur est adapté. On a choisi *OpenVPN* car la configuration réseau est plus simple : il n'y a qu'un port à ouvrir en entrée pour l'entreprise, et un port à ouvrir en sortie pour le prestataire. De plus le prestataire peut garder son certificat X.509 et le réutiliser pour une future intervention sur un autre serveur.

On notera qu'un tunnel SSH est parfois suffisant pour ce type d'utilisation, et partage les avantages de *OpenVPN* en termes de facilité de mise en place, mais est plus compliqué à manipuler pour le prestataire.

5.2.5 VPN 5 : Wifi sécurisé

On oublie trop souvent que les réseaux Wifi sont par nature très difficiles à sécuriser : l'ensemble du trafic peut être intercepté par n'importe quelle station, et les protocoles de sécurité les plus répandus (WEP et WAP) souffrent de failles qui les rendent pratiquement inutiles et créent l'illusion de la sécurité. Les protocoles de sécurisation plus sérieux, comme WPA-Entreprise sont pour leur part difficiles à mettre en place.

Un VPN permet de protéger efficacement le trafic sur un réseau Wifi. Il s'agit d'une méthode alternative peu employée mais très robuste. En effet alors que les solutions telles que WEP tentent de sécuriser les couches inférieures de la transmission (1 et 2), un VPN se place légèrement plus haut (généralement la couche 3 voire 4 pour *IPsec* en mode transport). De plus, au plan cryptographique, les algorithmes des VPN sont beaucoup plus fiables et la phase d'authentification, qui est le talon d'Achille de la sécurité Wifi, est beaucoup plus sûre.

Ce cas de figure reprend donc à l'identique les principes du VPN 3, à la différence que le réseau intermédiaire n'est plus Internet mais le réseau Wifi de l'entreprise, et que le point de sortie du VPN n'est plus au cœur du réseau mais limité aux serveurs d'application.

On notera que cette solution est celle utilisée dans certaines salons sur la sécurité informatique pour protéger les réseaux Wifi contre la curiosité des participants.

6 Conclusion

D'une manière générale, la sécurité est l'un des domaines de prédilection de l'open source, d'une part parce que l'ouverture du code est un prérequis à l'assurance d'intégrité et l'absence de back-doors, et d'autre part parce que le *peer-review* que permet la libre diffusion est la condition nécessaire d'un code de qualité.

En matière de VPN, les solutions open source sont particulièrement matures et robustes, et couramment utilisées. OpenVPN et les diverses implémentations IPsec sont au coude à coude en matière de fonctionnalité, et le choix final se fera bien souvent sur la facilité de mise en place de telle ou telle solution ou sur la nécessité d'interagir avec des équipements propriétaires qui souvent éliminent OpenVPN de l'équation.

Si ce petit avant-goût vous a semblé pertinent, n'hésitez pas à faire appel à l'expertise de Smile pour déployer vos solutions de sécurité et d'infrastructure.