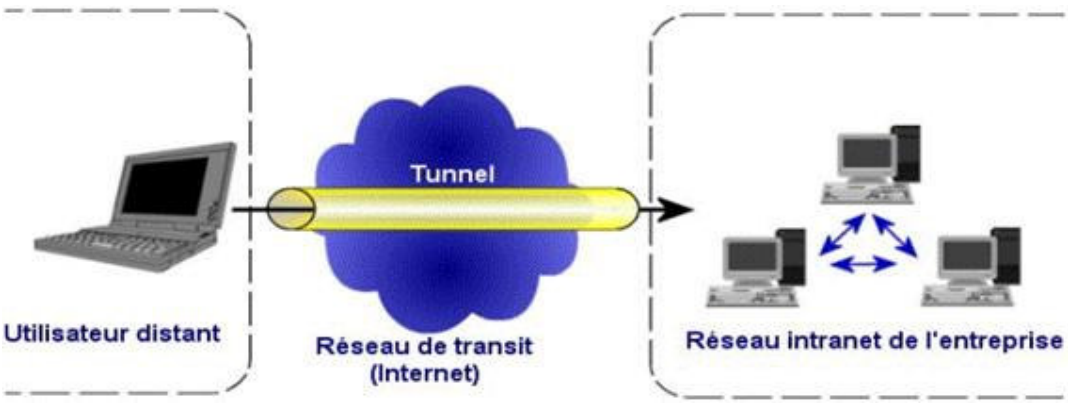
Sommaire

1 Introduction

VPN : Virtual Private Network ou RPV (réseau privé virtuel) en français est une technique permettant à un ou plusieurs postes distants de communiquer de manière sure, tout en empruntant les infrastructures publiques. Ce type de liaison est apparu suite à un besoin croissant des entreprises de relier les différents sites, et ce de façon simple et économique. Jusqu'à l'avènement des VPN, les sociétés devaient utiliser des liaisons Transpac, ou des lignes louées. Les VPN ont permis de démocratiser ce type de liaison.

Schéma d'un accés VPN :



2 Principe de fonctionnement d'un VPN

Un réseau VPN repose sur un protocole appelé "protocole de tunneling". Ce protocole permet de faire circuler les informations de l'entreprise de façon cryptée d'un bout à l'autre du tunnel. Ainsi, les utilisateurs ont l'impression de se connecter directement sur le réseau de leur entreprise.

Le principe de tunneling consiste à construire un chemin virtuel après avoir identifié l'émetteur et le destinataire. Par la suite, la source chiffre les données et les achemine en empruntant ce chemin virtuel. Afin d'assurer un accès aisé et peu coûteux aux intranets ou aux extranets d'entreprise, les réseaux privés virtuels d'accès simulent un réseau privé, alors qu'ils utilisent en réalité une infrastructure d'accès partagée, comme Internet.

Les données à transmettre peuvent être prises en charge par un protocole différent d'IP. Dans Ce cas, le protocole de tunneling encapsule les données en ajoutant une en-tête. Le tunneling est l'ensemble des processus d'encapsulation, de transmission et de désencapsulation.

Les principaux avantages d'un VPN :

- **Sécurité :** assure des communications sécurisées et chiffrées.
- **Simplicité :** utilise les circuits de télécommunication classiques.
- **Économie :** utilise Internet en tant que média principal de transport, ce qui évite les coûts liés à une ligne dédiée.

3 Les contraintes d'un VPN

Le principe d'un VPN est d'être transparent pour les utilisateurs et pour les applications y ayant accés. Il doit être capable de mettre en oeuvre les fonctionnalités suivantes :

- Authentification d'utilisateur : seuls les utilisateurs autorisés doivent avoir accés au canal VPN.

- Cryptage des données : lors de leur transport sur le réseau public, les données doivent être protégées par un cryptage efficace.

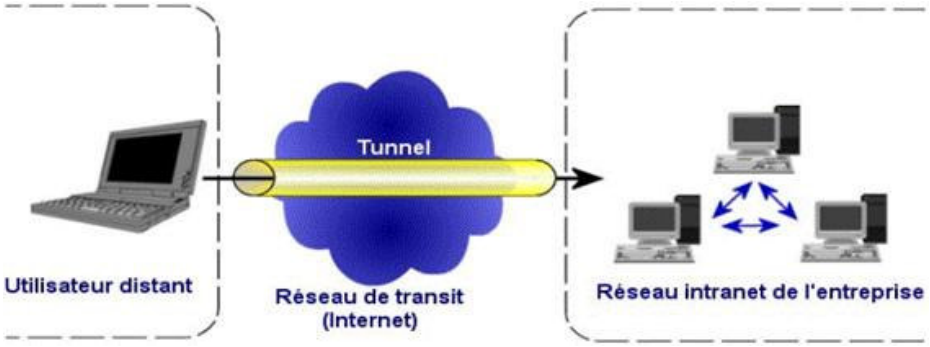
- Gestion de clés : les clés de cryptage pour le client et le serveur doivent pouvoir être générées et régénérées.

- Prise en charge multi protocole : la solution VPN doit supporter les protocoles les plus utilisés sur les réseaux publics en particulier IP.

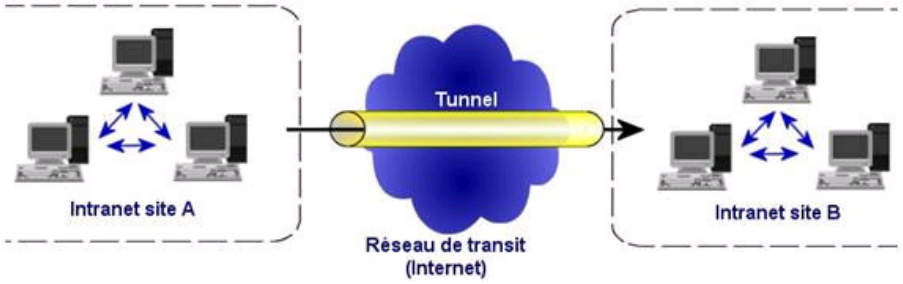
4 les différents types de VPN

Suivant les besoins, on référence 3 types de VPN :

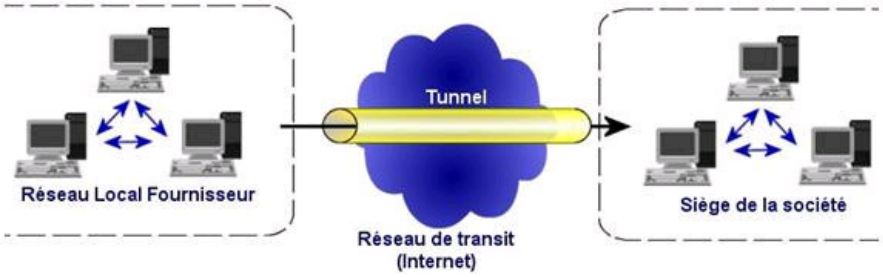
- Le VPN d'accès : il est utilisé pour permettre à des utilisateurs itinérants d'accéder au réseau de leur entreprise. L'utilisateur se sert d'une connexion Internet afin d'établir une liaison sécurisée.



- L'intranet VPN : il est utilisé pour relier deux ou plusieurs intranets d'uen même entreprise entre eux. Ce type de réseau est particulièrement utile au sein d'une entreprise possédant plusieurs sites distants. Cette technique est également utilisée pour relier des réseaux d'entreprise, sans qu'il soit question d'intranet (partage de données, de ressources, exploitation de serveurs distants …



- L'extranet VPN : une entreprise peut utiliser le VPN pour communiquer avec ses clients et ses partenaires. Elle ouvre alors son réseau local à ces derniers. Dans ce cas, il est nécessaire d'avoir une authentification forte des utilisateurs, ainsi qu'une trace des différents accés. De plus, seul une partie des ressources sera partagée, ce qui nécessite une gestion rigoureuse des espaces d'échange.



5 Les protocoles utilisés

Les protocoles utilisés dans le cadre d'un VPN sont de 2 types, suivant le niveau de la couche OSI auquel ils travaillent :

- Les protocoles de niveau 2 comme PPTP ou L2TP.
- Les protocoles de niveau 3 comme IPsec ou MLPS

5.1 le protocole PPP

PPP (Point to Point Protocol) est un protocole qui permet de transférer des données sur un lien synchrone ou asynchrone. Il est full duplex et garantit l'ordre d'arrivée des paquets. Il encapsule les paquets Ip, Ipx et Netbeui dans des trames PPP, puis transmet ces paquets encapsulés au travers de la liaison point à point. PPP est employé généralement entre un client d'accès à distance et un serveur d'accès réseau
Ce protocole n'est pas un protocole sécurisé mais sert de support aux protocoles PPTP ou L2TP.

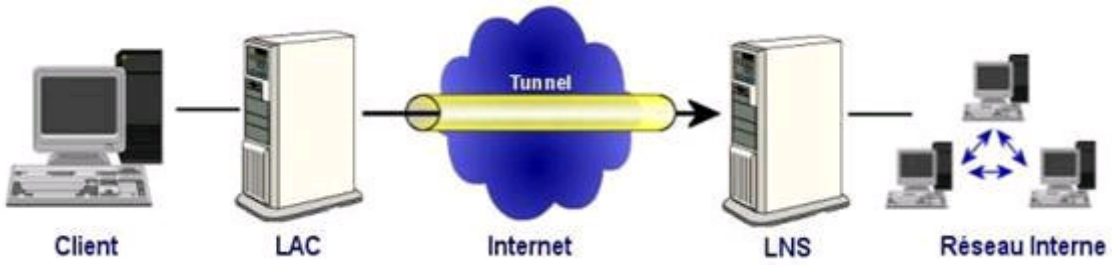
5.2 Le protocole PPTP

PPTP (Point to Point Tuneling Protocol , définit par la Rfc 2637, est un protocole qui utilise une connexion PPP à travers un réseau Ip en créant un réseau privé virtuel (VPN). Microsoft a implémenté ses propres algorithmes afin de l'intégrer dans ses versions de windows. Ainsi, PPTP est une solution très employée dans les produits VPN commerciaux à cause de son intégration au sein des systèmes d'exploitation Windows. PPTP est un protocole de niveau 2 qui permet l'encryptage des données ainsi que leur compression. L'authentification se fait grâce au protocole Ms-Chap

Le principe du protocole PPTP est de créer des paquets sous le protocole PPP et de les encapsuler dans des datagrammes IP.
Le tunnel PPTP se caractérise par une initialisation du client, une connexion de contrôle entre le client et le serveur ainsi que par la clôture du tunnel par le serveur.
Lors de l'établissement de la connexion, le client effectue d'abord une connexion avec son fournisseur d'accès Internet. Cette première connexion établit une connexion de type PPP et permet de faire circuler des données sur Internet.
Par la suite, une deuxième connexion est établie. Elle permet d'encapsuler les paquets PPP dans des datagrammes IP. C'est cette deuxième connexion qui forme le tunnel PPTP.

5.3 Le protocole L2TP

L2TP (Layer Two Tuneling Protocol), définit par la Rfc 2661, est issu de la convergence des protocoles PPTP et L2F (Layer Two Forwarding). Il est actuellement développé et évalué conjointement par Cisco , Microsoft, 3Com ainsi que d'autres acteurs du marché des réseaux. Il permet l'encapsulation des paquets PPP au niveau des couches 2 (Frame Relay et Atm) et 3 (Ip). Lorsqu'il est configuré pour transporter les données sur IP, L2TP peut être utilisé pour faire du tunnelling sur Internet. L2TP repose sur deux concepts : les concentrateurs d'accès L2TP (Lac : L2TP Access Concentrator) et les serveurs réseau L2TP (Lns : L2TP Network Server). L2TP n'intègre pas directement de protocole pour le chiffrement des données. C'est pourquoi L'IETF préconise l'utilisation conjointe d'Ipsec et L2TP



5.4 Le protocole Ipsec

Ipsec, définit par la Rfc 2401, est un protocole qui vise à sécuriser l'échange de données au niveau de la couche réseau. Le réseau Ipv4 étant largement déployé et la migration vers Ipv6 étant inévitable, mais néanmoins longue, il est apparu intéressant de développer des techniques de protection des données communes à Ipv4 et Ipv6. Ces mécanismes sont couramment désignés par le terme Ipsec pour Ip Security Protocols. Ipsec est basé sur deux mécanismes. Le premier, AH, pour Authentification Header vise à assurer l'intégrité et l'authenticité des datagrammes IP. Il ne fournit par contre aucune confidentialité : les données fournies et transmises par ce "protocole" ne sont pas encodées. Le second, Esp, pour Encapsulating Security Payload peut aussi permettre l'authentification des données mais est principalement utilisé pour le cryptage des informations. Bien qu'indépendants ces deux mécanismes sont presque toujours utilisés conjointement..

5.5 Les mécanismes de cryptage

Les protocoles sécurisés ont recours à des algorithmes de cryptage, et ont donc besoin de clefs. Un des problèmes principal dans ce cas est la gestion de ces clefs. Par gestion, on entend la génération, la distribution, le stockage et la suppression de ces clefs. Ces différentes tâches sont dévolues à des protocoles spécifiques de gestion de ces cléfs, à savoir :

- Isakmp (Internet Security Association and Key Management Protocol)
- Ike (Internet Key Exchange)

5.6 Le protocole SSL

Ssl (Secure Socket Layer) est un protocole de couche 4 (niveau transport) utilisé par une application pour établir un canal de communication sécurisé avec une autre application.

Ssl a deux grandes fonctionnalités : l'authentification du serveur et du client à l'établissement de la connexion et le chiffrement des données durant la connexion.

SSL est le dernier arrivé dans le monde des Vpn, mais il présente un gros avantages dans la mesure ou coté client, il ne nécessite qu'un navigateur Internet standard. Ce protocole est celui qui est utilisé en standard pour les transactions sécurisées sur Internet

L'inconvénient néanmoins de ce type de protocole est qu'il se limite au protocole https, ce qui n'est pas le seul besoin de connexion des entreprises.

6 La mise en œuvre d'un VPN

La mise en œuvre d'un VPN, et donc les moyens utilisés dépendent étroitement du type de VPN dont il s'agit, ainsi que de la fréquence d'utilisation.

La mise en œuvre d'un VPN nécessite systématiquement l'utilisation d'un serveur qui aura en charge la partie authentification, cryptage et décryptage et d'un client assurant la partie cryptage / décryptage et qui assurera la partie connexion vers un serveur. De plus, le client aura souvent la charge d'initialiser la connexion, sauf en cas de connexion permanente.

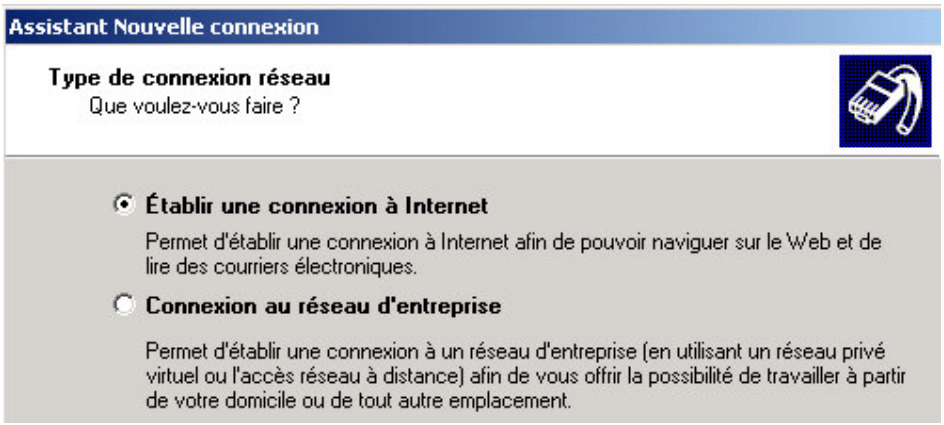
6.1 Utilisation de logiciels

6.1.1 Windows et les VPN

Windows a été un des instigateurs de PPTP et à intégrer très tôt dans ses plateformes les outils permettant de mettre en œuvre les VPN.

Coté serveur, Windows 2000 ou 2003 intégre les outils permettant de mettre en œuvre un VPN.

Coté client, Windows XP intégre de façon native à travers un assistant la création d'un réseau privé VPN



l'encryptage et l'authentification des utilisateurs est réalisée grâce à la couche MSCHAP

6.1.2 Linux et les VPN

De la même façon que sous Windows, Linux dispose des outils permettant de créer un VPN :

PPTPD coté serveur
PPTP coté client

Ce sont de part et d'autre des daemons (services sous Linux) qu'il faut paramétrer et lancer.

6.1.3 Navigateur Internet

Les navigateurs Internet prennent tous en compte le cryptage et l'authentification vers un serveur à travers le protocole https.

6.1.4 Liaison mixte

Linux, Windows, Unix, Solaris … Tous ces OS ont la possibilité de gérer des connexions VPN, puisque ces connexions font appel à des protocoles standards définit dans des RFC. La mise en œuvre en est néanmoins plus complexe puisqu'elle fait appel à un empilage de couches, la partie la plus complexe étant l'authentification et l'accés ensuite aux ressources partagées une fois le canal établit.

Microsoft offre une bibliothèque d composants permettant l'interconnexion entre monde hétérogène, les SFU (Services for Unix).

Windows Services for UNIX v3.5 offre aux informaticiens et aux développeurs les outils et l'environnement dont ils ont besoin pour une interopérabilité entre les environnements Windows et UNIX/Linux et la migration des applications UNIX vers Windows (référence : Microsoft).

6.1.5 Conclusion sur cette partie

La mise en œuvre peut être simple dans le cas de déploiement en environnement homogène, et dans le cas d'un VPN d'accés. Dans le cas de liaison d'Intranet, il est souvent fait appel à des prestataires de service qui réalisent cette partie de façon transparente pour les utilisateurs.

6.2 Utilisation de matériel

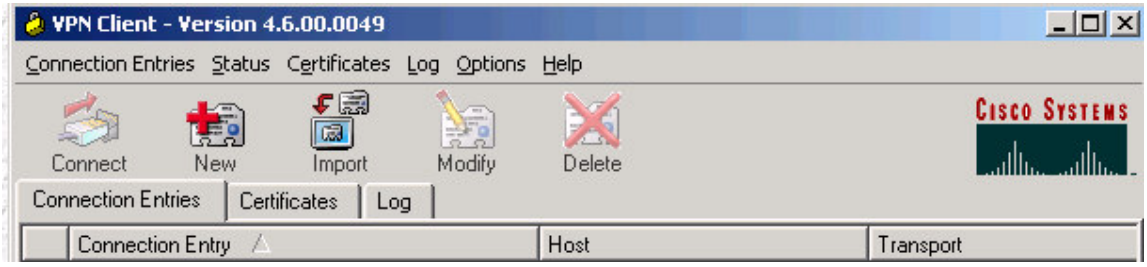
6.2.1 Présentation

l'Utilisation de matériel consiste en fait à déléguer le tuneling au matériel mis en place en sortie d'entreprise, à savoir les routeurs. La plupart des routeurs offrent des possibilités de création de VPN.

- l'avantage de cette solution est qu'elle est totalement transparente pour les utilisateurs, puisqu'ils ont l'impression d'avoir un réseau en continu avec une simple gestion des accés classique.
- Pour les administrateurs, de la même façon, ils gèrent les autorisations aux ressources sans s'occuper du VPN puisqu'il est prise en charge par les routeurs.

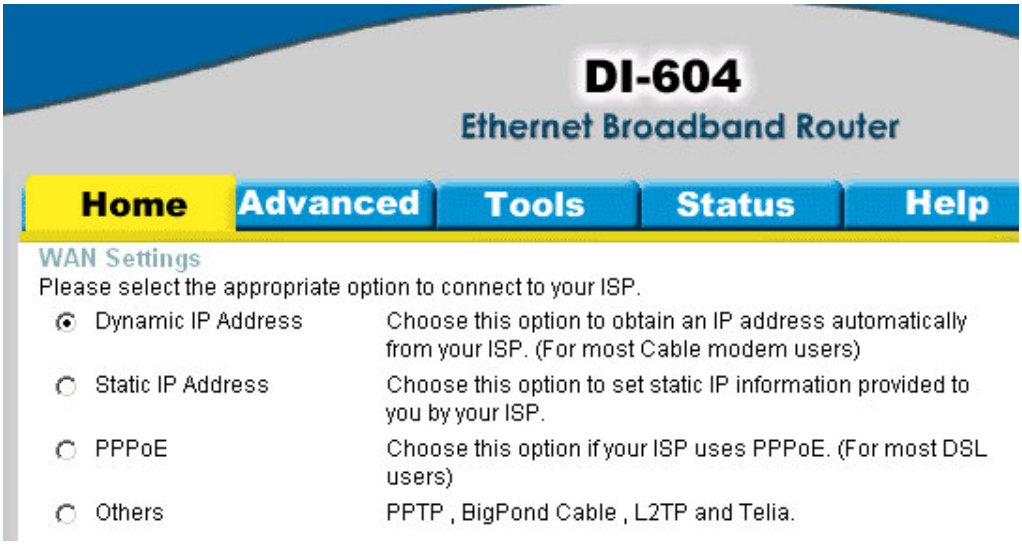
Cette solution est celle qui est de plus en plus utilisée par les entreprises, voire même externalisée vers des prestataires tiers (France telecom, cegetel, word on line, olenane …)qui prennent en charge la fourniture et le paramétrage des routeurs, la mise à disposition des infrastructures, les interventions en cas de panne ?

De la même façon, les grands des routeurs fournissent également des logiciels clients afin de prendre en compte le VPN d'accés pour des clients itinérants.



6.2.2 paramétrage de routeurs

Exemple DLINK :

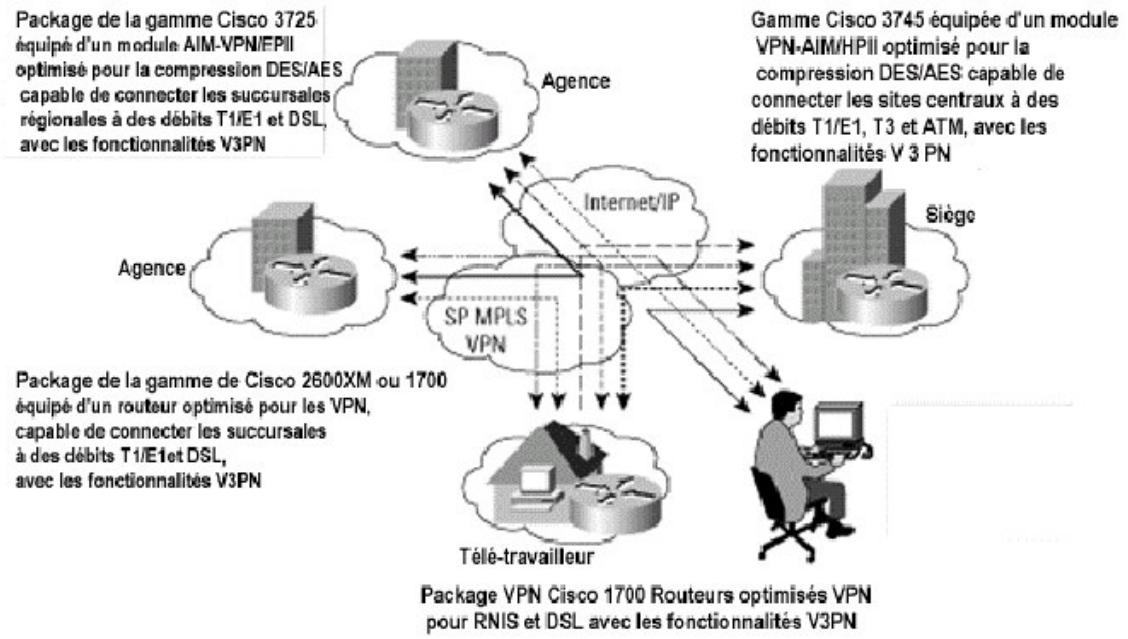


Des outils chez CISCO (référence CISCO) :

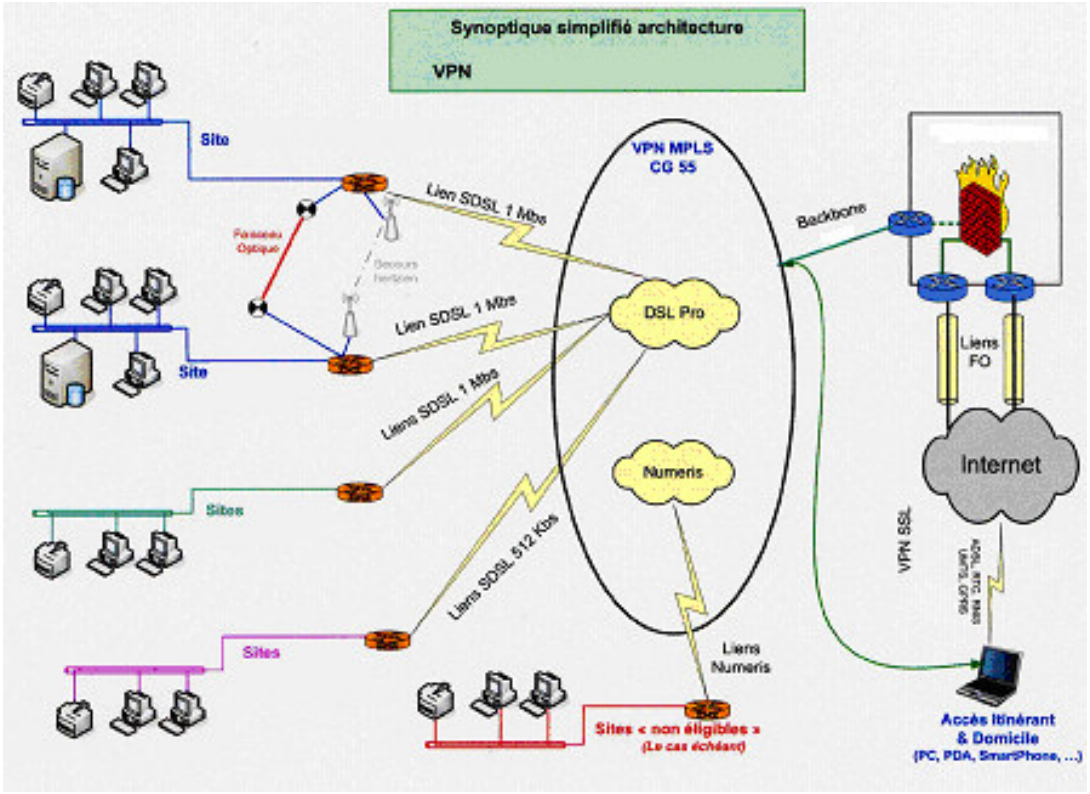
Cisco Easy VPN

Cisco Easy VPN est une extension logicielle pour les routeurs et les dispositifs de sécurité Cisco qui simplifie considérablement le déploiement des VPN pour les bureaux distants et les télétravailleurs.
Cisco Easy VPN s'articule autour de Cisco Unified Client Framework. Il centralise toute la gestion des clés et des politiques, et réduit la complexité du déploiement des VPN.
Les deux composants de Cisco Easy VPN sont Cisco Easy VPN Remote et Cisco Easy VPN Server Cisco Easy VPN Remote permet aux routeurs et aux dispositifs de sécurité Cisco d'établir et de gérer automatiquement un tunnel VPN vers un équipement sous Cisco Easy VPN Server en faisant l'économie des complications d'une configuration à distance. Cisco Easy VPN Server accepte les appels entrants des équipements sous Cisco Easy VPN Remote ou des clients logiciels VPN et garantit la mise à jour de leurs politiques de sécurité avant l' établissement de ces connextions. Cisco Easy VPN fournit une méthode de gestion cohérente des politiques et des clés des connexions et offre un multiple choix d'équipements VPN

distants – routeurs, clients hardware ou clients logiciels – lors d'un même déploiement vers n'importe quelle plateforme sous Cisco Easy VPN Server.



6.3 Exemple d'infrastructure



7 Pour aller plus loin

Quelques références de sites internet, d'où sont extrait certaines parties de ce cours ainsi que certains schémas :

http://www.frameip.com/vpn/

http://www.formation.ssi.gouv.fr/stages/documentation/architecture_securisee/vpn.html

Installation d'un VPN sous Windows XP
http://www.commentcamarche.net/pratique/vpn-xp.php3

Mise en place d'un VPN Linux
http://dambrain.homelinux.net/Dominique/VPN.htm

un howto Linux sur les VPN
http://www.linuxsecurity.com/docs/LDP/VPN-HOWTO/index.html

http://www.microsoft.com/windows2000/fr/server/help/default.asp?url=/windows2000/fr/server/help/Conn_VPN.htm

Windows services for Unix
http://www.microsoft.com/france/windows/sfu/default.mspx

Client VPN Cisco
http://www.cisco.com/en/US/products/sw/secursw/ps2308/index.html
http://www.utc.fr/~5000/vpn/