Baptiste Lopez

Groupe Sous Mon Toit - Siège - Olivet

IUT Orléans - Dép. Informatique

Direction des Systèmes d'Information

Année universitaire 2011 - 2012

Gaël Acke - DSI (Maître de stage)

Responsable : Gérard Roszavolgyi

REMERCIEMENTS

Je tiens à remercier M. Acke, mon maître de stage, qui m'a appris beaucoup, en termes de professionnalisme avec les utilisateurs, de relationnel avec les fournisseurs, et de vision à la fois globale et affinée du SI. Il m'a apporté parfois un point de vue d'ingénieur, point de vue qui m'a été utile et que j'ai eu régulièrement l'occasion d'apprécier.

Je souhaite aussi remercier M. Rozsavolgyi, qui m'a soutenu et écouté attentivement lors de mes démarches pour obtenir mon stage, puis par la suite pour faire le point.

Enfin, je n'oublie pas les salariés des différents services et des différentes agences de la société Sous Mon Toit, ainsi que ses dirigeants, qui m'ont accueilli fort chaleureusement dès mon premier jour de stage, et que j'ai pu côtoyer depuis. Leur aide, leur convivialité et leur sympathie sont autant de points positifs de la vie d'une entité que je ne peux négliger et que je me dois d'intégrer dans mes remerciements, car cela contribue au bon déroulement du stage que j'effectue à la DSI.

SOMMAIRE

INTRODUCTION

J'ai effectué au sein de la Direction des Systèmes d'Information (DSI) du groupe Sous Mon Toit un stage de seize semaines, du 19 juin 2012 au 19 octobre de cette même année, durant lequel j'ai suivi les directives de mon maître de stage, Gaël Acke.

Le sujet principal du stage, décrit dans ce rapport, est la mise en place d'un réseau VPN[1] opérateur, qui remplace à terme l'ancien schéma de réseau.

Ces directives concernent donc la mise en œuvre, par la DSI, de dispositifs qui s'inscrivent dans le cadre de cet aménagement du système d'information du groupe. Les changements majoritaires touchent surtout les agences, la partie centralisée du SI[2] étant au siège. Il s'agit aussi de maintenir et pouvoir faire évoluer par la suite cette nouvelle architecture, que ce soit en partie ou en totalité, par des composants de régulation complémentaires.

Conseiller pour, concevoir, réaliser et mettre en œuvre ces aménagements du système d'information constituent donc les objectifs premiers de ce sujet de stage. Pour cela, une partie de mon rôle était la force de proposition, une autre a été de prendre en compte les différentes problématiques et de faire le lien avec les utilisateurs, les fournisseurs et les différents prestataires impliqués.

Dans le cadre de ce projet, sur laquelle je base ce rapport, j'ai donc mis en application des techniques diverses. Ce sont principalement les aspects d'évolution du SI sur le lieu de stage et ceux vis-à-vis des agences, surtout informatiques, que je décris dans ce document, ainsi que leurs résultats et conséquences.

Tout d'abord, j'ai pris la mesure de l'architecture déjà en place, ainsi que de la problématique associée, afin de me rendre compte de mon domaine d'intervention. Ensuite, lors de la phase préparatoire à la mise en place des éléments du réseau VPN opérateur, j'ai pu commencer à m'imprégner de la mise en place concrète du nouveau schéma concernant la partie agence.

Lors de la phase de mise en place, j'ai été à l'écoute du prestataire concernant l'installation proprement dite, tout d'abord du lien qui relie le nouveau réseau au siège, et ensuite des box. J'ai aussi participé à l'installation de ces box, en informant les utilisateurs des tâches qu'ils devaient exécuter sous mon contrôle. J'ai pu assurer la configuration de certains paramètres, tester et valider ces installations, en lien avec le prestataire et les techniciens.

Enfin, j'ai assuré de même le suivi post-installation, résolvant des problèmes de tous ordres : configuration réseau, oublis des utilisateurs par habitude de l'ancien système, améliorations, etc.

[1] **V**irtual **P**rivate **N**etwork (français : **R**éseau **P**rivé **V**irtuel). Son principe de fonctionnement, et surtout, son intérêt, sont expliqués en 3.2. Étant le thème central de ce rapport, il y est évoqué tout au long.

[2] Cf. **DSI**

1. PRÉSENTATION DE L'ENTREPRISE ET DU CADRE

Le Groupe Sous Mon Toit (GSMT) est une société dont l'activité principale est le service à la personne, allant de la garde d'enfants au maintien à domicile des personnes âgées, en passant par le ménage. Le Groupe est certifié ISO[3].

Il s'agit, dans son cadre juridique et financier, d'une holding créée en 2006, dont les parts sont détenues à hauteur de 70 % par deux actionnaires, Xavier Mura et Daniel Cremades, respectivement créateur - Directeur Général et Président du groupe, et leur associée, la Banque Populaire, pour les 30 % restants. La Banque Populaire se charge ainsi des opérations bancaires et financières du groupe.

Le groupe est composé de deux entités, n'étant distinctes quasiment que dans leur statut : Sous Mon Toit (SMT), qui est gérée totalement par le groupe, dont le siège social est Mulhouse et qui englobe environ 30 agences, et Adhéo Services (Adhéo), entité dont les responsables d'agence sont des « directeurs associés », actionnaires de leur propre structure. Ils font néanmoins l'objet de facturations directes et de l'imposition du matériel par le groupe. Ces directeurs associés, qui ne sont donc pas des franchisés, sont rémunérés en fonction de leur Chiffre d'Affaires. Ce Chiffre d'Affaires est comptabilisé en heures de prestations placées par mois, et en heures de prestations effectuées. Les sites les plus importants de cette entité sont Le Mans, Rennes, ou bien Colmar, Clermont-Ferrand, Bordeaux, Corbeil, Marseille.

Trois grands pôles d'activité se détachent, concernant le groupe, ses satellites et dépendances : la vente de prestations (Sous Mon Toit est une société de service à la personne), le recrutement des intervenant(e)s (dont le/la responsable/directeur/directrice d'agence est chargé(e)), et la gestion, pour laquelle GSMT est un relais entre les entités, leurs agences et le groupe. Le recrutement fait toutefois l'objet d'informations au niveau du groupe, le rendant assez centralisé.

Une des problématiques, liée au recrutement, est quelque peu liée aussi à la gestion, et surtout à la vente : il s'agit de trouver les clients, les fidéliser, et en assurer le suivi. Sous Mon Toit dispose d'un agrément par département pour ses activités. Avec l'administratif (documents à transférer, contrats à gérer, ...), qui échoit de même conjointement au siège, ce sont les champs d'application du modèle d'agences de Sous Mon Toit.

Tous ces pôles d'activité, toutes ces problématiques sont à la base des applications métier du groupe, utilisées à la fois par le siège et par les agences. Les utilisateurs sont à la fois les personnels des services autres que la DSI, et les personnels en agence.

[3] **I**nternational **S**tandard **O**rganization (français : **O**rganisation **I**nternationale de **N**ormalisation). L'organisme international chargé des standards et des normes.

Le siège du groupe Sous Mon Toit, c'est-à-dire GSMT dans son ensemble, se trouve à Olivet (Loiret), au 563, rue de la Juine. Les différents services y sont répartis dans un bâtiment à deux étages, le premier hébergeant la quasi-totalité des services :

- la Direction des Systèmes d'Information (DSI), dont le directeur est Gaël Acke,
- la Direction Qualité (DQ ou DQual), dont la directrice est la seule représentante, et qui gère par exemple les agréments, les audits,
- la Direction des Ressources Humaines (DRH), qui emploie deux salariées, et qui malgré son intitulé ne s'occupe pas directement du recrutement de tous les personnels, mais de l'ensemble des mille collaborateurs du groupe,
- le Secrétariat de Direction (SD ou SecDir), qui emploie deux salariées,
- la Direction Administratif et Financier (DAF), facturation du groupe et comptabilité client/fournisseur.

Le deuxième étage abrite la Cellule Support (CS). C'est le pôle dédié au support des agences, en matière de suivi des clients et de leurs rendez-vous, de la présence des ressources humaines (notamment des intervenants), et donc en matière de suivi de prestations. La Cellule Support supplée également le secrétariat de direction, en sa fonction de standard ; par ailleurs, elle est en charge de la prospection client (numéro Azur) et de la gestion partagée des plannings des responsables d'agence.

La DSI est en charge de la mise en service, de la maintenance et du cycle de vie du matériel technique (informatique, téléphonique, …). C'est elle qui définit les orientations du Système d'Information du groupe, en relation avec les fournisseurs de matériels et de prestations informatiques. Elle est composée de deux puis trois personnes (en me comptant comme stagiaire, plus un autre stagiaire développeur web arrivé en septembre), qui s'occupent de l'administration des réseaux et systèmes principalement, mais aussi de l'administration de données et web, et de certains développements logiciels et web. Mon rôle consiste donc à suppléer le DSI[4] sur les différents problèmes concrets ou plus conceptuels qui se posent à lui. La mise en place des éléments de réseau compte parmi ces problématiques.

Le service met en place des solutions logicielles et matérielles (réseau, intranet, extranet, …), entretient et maintient les postes de travail fixes ou portables (différentes types d'utilisations donc différentes marques, différentes factures, etc.) ainsi que les réseaux et communications (systèmes d'exploitation pour téléphones portables ou smartphones, ensemble de serveurs, dispositifs réseau, dispositifs d'interconnexion…).

[4] **D**irecteur des **S**ystèmes d'**I**nformation

Pour ce faire, elle est en lien avec des fournisseurs et des prestataires localisés principalement à Mulhouse et sur l'agglomération orléanaise. Cela facilite certaines interventions ou demandes locales ; les interventions sur des sites moins proches sont aussi prises en charge, éventuellement à distance, par les fournisseurs et/ou les prestataires. Il peut s'agir pour eux de se substituer directement à la DSI, ou bien de la suppléer en cas d'impossibilité pour elle de solutionner seule le problème.

Ces fournisseurs ont une grande importance dans la chaîne de décision et de mise en œuvre, car ils lui fournissent, en vertu de contrats (qu'ils ont parfois eux-mêmes passés avec d'autres fournisseurs), précédés selon les cas par des devis :

- les applications métier, développées en WLanguage (WinDev 12), et utilisées par tous les services du siège et les agences. Elles sont fournies par la société Apologic (les applications Lancelot, Perceval et Korrigan par exemple, une partie des applications métier servant à la comptabilité et à la gestion des ressources humaines, elles sont utilisées à des degrés divers par l'ensemble des personnels, y compris le DSI, qui contribue aussi personnellement à leur maintenance et leur évolution, en liaison avec Apologic) ;

- un hébergement, dit « mutualisé » (OVH), car l'offre consiste en un produit mutualisé : le domaine, le site web et les adresses emails sont regroupés au sein d'un même produit. Par exemple, la messagerie utilise le client de messagerie Outlook (pack Office), pour se connecter via les comptes de courrier électronique au serveur de messagerie OVH qui fournit les adresses de courrier électronique, et récupérer les courriers électroniques des utilisateurs ;

- le site web, dans le cas de Leadel, le fournisseur qui le conçoit ;

- des prestations de fourniture de matériel, maintenance et d'évolutivité réseau, téléphonie fixe, téléphonie mobile et internet : contrats avec Réseaux-com, filiale de SFR, à La Chapelle-St-Mesmin, dans le Loiret), parfois en lien avec d'autres filiales SFR - exemple : logiciel et système Astra de BackStage (Astreinte téléphonique) ;

- des prestations de fourniture de matériel et de maintenance réseau générale (contrats avec Atlantis, qui se trouve à Mulhouse) ;

- le nouveau réseau « opérateur » VPN, qui a fait l'objet d'une étude de projet préalable par M. Hamitouche, chef de projet Régions Ouest d'une filiale spécialisée de SFR. Cela couvre plusieurs points, qui ont conduit à la mise en place dudit réseau VPN. Ces points sont évoqués plus en détail dans ce rapport.

- du matériel (directement) : Dell

- autres fournisseurs de postes et de serveurs : IBM, Lenovo ; de matériel réseau et d'interconnexion : ZyXEL, (indirectement, par Réseaux-Com et SFR) OneAccess, TeraOptic, Cisco, Huawei ; d'équipements d'infrastructure matérielle et réseau : ESTCI

Concernant la partie logicielle, la DSI, mais aussi l'ensemble des utilisateurs selon les types de besoins, utilisent des logiciels libres mais aussi des logiciels plus connus :

- développés par Microsoft pour leur usage bureautique, comme la suite Office 2007 et 2010,
- des antivirus Kaspersky WorkStation (gérés par Atlantis), Microsoft Security Essentials (MSE), et dernièrement Avast ! 7 (en test-complément de MSE), ces deux derniers étant en licences gratuites/familiales
- des navigateurs à l'image de Google Chrome, Mozilla Firefox ou Internet Explorer,
- des systèmes d'exploitation Windows XP Professionnel, Windows Seven Professionnel et Mac OS[5] X, quasiment tous en licences OEM[6], et des systèmes d'exploitations libres et gratuits (Cent OS dans le cas de FAN[7], Linux dans le cas de ZeroShell)
- des distributions : Fully Automated Nagios est ainsi partiellement utilisée, et une distribution ZeroShell est mise en œuvre (point abordé plus en détail à la fin de ce rapport), tout cela orienté vers un usage professionnel.

Les sauvegardes et les fichiers de travail sont stockés sur différents serveurs (initialement, un serveur nommé MOON, un serveur de stockage en réseau NAS, et un serveur de stockage délocalisé en ligne) dans la salle serveurs. Dans cette même salle se trouvent le serveur AD[8], et le serveur TSE[9].

L'AD est l'annuaire informatique du groupe pour le réseau, et donc permet la gestion des droits des utilisateurs et groupes d'utilisateurs sur son arborescence de répertoires et de fichiers. Par l'intermédiaire de partages (dossiers partagés) et de lecteurs réseau (accès aux partages en connectant un lecteur virtuel dessus), il permet d'effectuer les transferts de documents, de données et d'informations entre les agences et le siège d'une part, et entre les services du siège d'autre part.

Quant au TSE, pour simplifier, il lance le service Terminal, son composant serveur écoute sur son port prédéfini, et lorsque les utilisateurs se connectent au TSE via le logiciel client Bureau à distance, ils se connectent en fait à leur session dessus, dont les identifiants, mots de passe, droits utilisateur et droits sur l'arborescence des fichiers sont régis par l'Active Directory. Cela permet l'accès aux applications métier que le TSE héberge. Un processus est lancé par ouverture d'une application, quel qu'en soit l'utilisateur qui l'a lancé.

---

[5] **O**perating **S**ystem (français : **S**ystème d'**E**xploitation)

[6] **O**riginal **M**anufacturer **E**quipment (français : **F**abricant d'**É**quipement d'**O**rigine), c'est une licence qui va avec une machine unique et donnée, et aucune autre.

[7] **F**ully **A**utomated **N**agios, distribution comprenant des outils préinstallés dédiés à la supervision de réseau, basée sur Cent OS, et pouvant se voir ajouter des « logiciels » basés aussi sur des distributions **R**ed **H**at **E**nterprise **L**inux (**RHEL**).

[8] **A**ctive **D**irectory, qui va de pair avec son Système d'Exploitation, Windows Server.

[9] **T**erminal **S**erver **E**dition, même système d'exploitation que l'Active Directory.

Ces deux machines figurent parmi les points les plus névralgiques du système d'information du groupe, et par extension, du système informatique. Elles sont dans une baie informatique « serveur », évoquée et décrite ci-après, et reliée elle-même à un coffret informatique mural. Des onduleurs[10], positionnés dans cette baie, sont également prévus en fonctionnement dans un futur proche, pour prendre le relais en douceur lors de l'extinction des matériels.

Il y a environ 85 postes informatiques à gérer sur l'ensemble du groupe (agences et siège), dont une vingtaine au siège. Ce chiffre comprend des machines dans des états de fonctionnement et d'emploi différents, le parc étant très hétéroclite. Le réseau Ethernet[11] du siège n'étant pas utilisé pour de la téléphonie/voix sur IP[12], la téléphonie du siège est composée de postes téléphoniques analogiques filaires classiques. En revanche, le siège est équipé d'un autocommutateur téléphonique privé[13], évolutif nativement vers la VoIP. Celui-ci est exploité aussi dans sa fonction de taxation : il permet d'analyser les appels téléphoniques reçus par la Cellule Support, dont on peut tirer des statistiques et des données de facturation des appels, avec des traitements paramétrables.

La prise en main à distance générique des postes (hors applications métier, dont le fonctionnement est décrit plus haut) se fait grâce à des logiciels propriétaires, avec licences pour les professionnels ou non : si TeamViewer en est un parfait exemple, d'autres sont aussi utilisés pour des raisons différentes (compatibilité avec les systèmes d'exploitation, processus différents, …). Cela permet aussi de lancer des réunions à distance. La présence d'agences du groupe sur toute la France rend nécessaire cette possibilité, utilisée notamment pour effectuer les installations de box pour le nouveau réseau VPN opérateur.

2. ANALYSE DE L'EXISTANT : AVANT

2.1. ARCHITECTURE GLOBALE

L'architecture globale du système informatique, précédant la mise en place du réseau VPN opérateur, est constituée des parties suivantes :

- l'architecture du siège
- les agences
- la centralisation, effectuée au siège

[10] Machines composées de dispositifs intégrés les uns aux autres (mis en cascade) et destinés à convertir, stocker et produire du courant, pour en éviter des coupures (prolongées ou non) ou des micro-coupures qui se produiraient sur le réseau électrique. Elles sont nommées ainsi par abus de langage, ces machines étant des **A**limentations **S**ans **I**nterruption (**ASI**), anglais : **U**ninterruptible **P**ower **S**upply (**UPS**) (source Wikipédia)

[11] Norme de réseau informatique câblé (câbles réseau RJ45 Ethernet, catégorie 5e et 6e au siège)

[12] Anglais : **T**elephone **o**n **IP** (**ToIP**) / **V**oice **o**n **IP** (**VoIP**)

[13] Anglais : **P**rivate **A**utomatic **B**ranch e**X**change (**PABX**)

2.2. FONCTIONNEMENT EN AGENCES ET CONNEXION DES AGENCES À INTERNET

Les dispositifs d'interconnexion en agence sont des box opérateurs, soit la LiveBox d'Orange, soit la NeufBox de SFR, avec des offres professionnelles de lignes téléphoniques, Internet, Internet mobile, et téléphonie mobile spécifiques, complémentaires ou de substitution.

Généralement les quatre voient leurs lignes et contrats respectifs dissociés.

L'offre Internet correspond à une liaison ADSL, la connexion en Internet mobile se fait par la 3G (une clé USB spécifique avec une carte SIM dedans, raccordée à l'ordinateur ; elle utilise les diverses connexions réseau possibles pour se connecter à Internet ; y compris par celles de téléphones portables).

Les box offrent la possibilité de s'y connecter soit en Ethernet, soit en WiFi, soit les deux. Elles sont limitées par défaut dans leur capacité à faire office de routeur VPN (ce sont des box « grand public »).

Chaque agence utilise généralement un ordinateur fixe (PC), parfois en plus, ou au lieu, un ordinateur portable. Elle dispose d'une imprimante, soit une imprimante réseau (connectée ou non à la box selon la configuration des lieux, et/ou l'utilisation qui en est faite), soit une imprimante raccordée en USB à l'ordinateur (ou un des ordinateurs, selon les dotations en câblage informatique et/ou la configuration des lieux).

La numérisation de documents, autre fonction des copieurs, s'effectue de deux manières. Via la Télécopie et numérisation Windows, qui envoie le document numérisé sur le PC relié à l'imprimante (plutôt avec un raccordement PC - imprimante en USB), et/ou via l'envoi du fichier numérisé par courrier électronique, à un ou des destinataire(s) pré-paramétré(s) sur l'imprimante, que l'utilisateur sélectionne ensuite sur le panneau de commande du copieur.

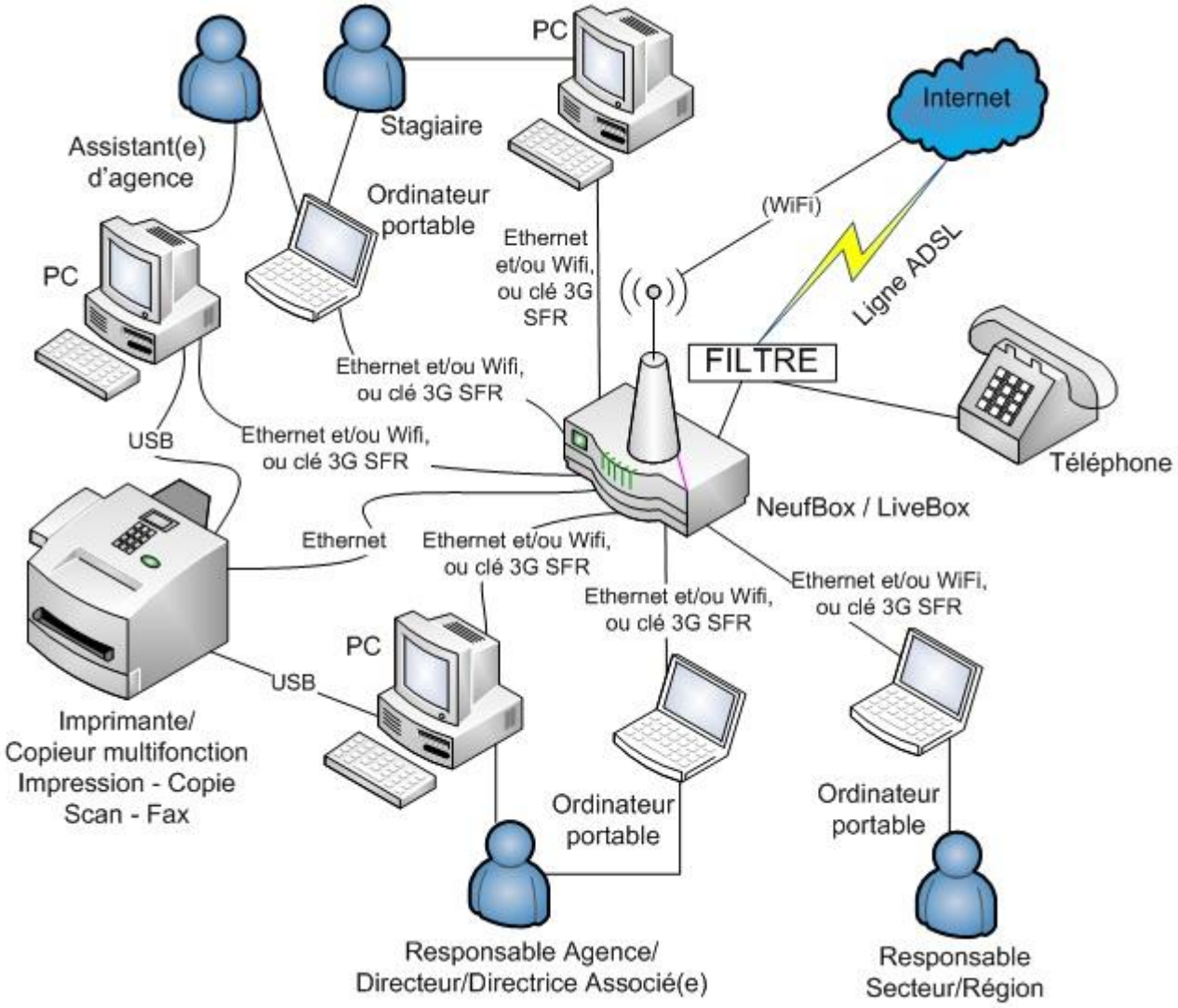


Figure 1 : Une agence.

Les responsables de secteur/région peuvent aussi être responsable d'une agence (exemple : Lille, dont la responsable d'agence est également la responsable de secteur/région).

Bien sûr, les connexions réseau entre les machines (PC et portables) et l'interconnexion (box, Internet) se font selon le matériel disponible et la disposition des lieux.

D'une manière générale, les utilisateurs du système VPN sont les personnels en agence. Le système est basé sur un client VPN ZyXEL, qui pré-paramètre son tunnel avec un fichier de configuration fourni et au lancement, l'établit avec le siège grâce au protocole IPSec. Toutes les données transitent ensuite par ce tunnel VPN jusqu'à sa fermeture. Les données sortent de l'agence encapsulées dans le tunnel VPN ZyXEL en passant par la box, encapsulant les données qui transitent par le web (WAN) ; les flux transitent dans les deux sens. Le lancement du client VPN est obligatoire (voir 3.1.1 et 3.1.2.). Chaque agence, dont les ordinateurs sont uniquement connectés sur une box, ne peut ouvrir simultanément qu'un seul tunnel VPN.

Il y a cinq agences qui font exception, ce système ne permettant pas de travailler avec les applications métier sur plusieurs machines simultanément : Grasse, Lille, Mulhouse, Nantes et Paris. Ces agences ont un routeur Netgear supplémentaire derrière la box (c'est-à-dire que le Netgear est raccordé à la box). Il permet d'ouvrir plusieurs tunnels VPN ZyXEL en même temps, et ainsi travailler sur les applications métier depuis chaque poste de l'agence (raccordé au routeur Netgear) simultanément.

En accédant à Internet, les agences reçoivent leur courrier avec leur compte Microsoft Outlook, paramétré pour le récupérer directement depuis le serveur mail d'OVH (qui héberge les adresses de courrier électronique). Un webmail (boîte de courrier électronique accessible en ligne) permet un accès décentralisé, palliatif ou complémentaire, au courrier électronique de tous les utilisateurs du groupe.

Le client VPN ZyXEL se lance aussi sur les ordinateurs portables des agences quand les utilisateurs sont en dehors de celles-ci. C'est le cas pour celles et ceux qui travaillent ou se connectent depuis chez eux, dans une forme de télétravail.

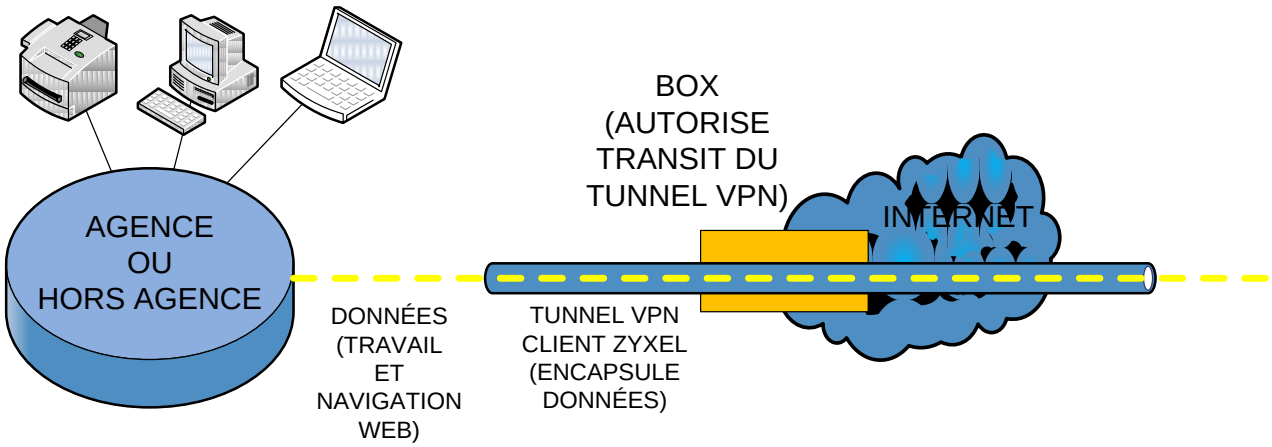


Figure 2 : Schéma de fonctionnement du VPN avant passage au réseau VPN opérateur.

La box autorise le transit VPN en tant qu'équipement réseau d'interconnexion, mais le tunnel est surtout logiciel (client VPN ZyXEL). Il encapsule lui-même les données de navigation web et de travail (acheminement des flux d'applications métier, documents et fichiers métier). Ensuite, la box passe le relais à Internet pour le transit du tunnel et de ses données.

2.3. ARCHITECTURE DU SIÈGE ET CENTRALISATION

Le serveur xxx.xxx.xx.xxx est le serveur DNS[14] et DHCP[15] du siège, en plus d'être son AD.

[14] **D**omain **N**ame **S**ystem (français : **S**ystème de **N**oms de **D**omaine). Système établissant la correspondance entre nom de domaine et adresse IP, et vice-versa. Ces correspondances s'obtiennent aussi bien par le **DNS** à l'intérieur d'un réseau local, que sur Internet pour associer une adresse IP à une URL (et inversement).

[15] **D**ynamic **H**ost **C**onfiguration **P**rotocol (français, non-officiel : **P**rotocole d'**A**llocation **D**ynamique des **H**ôtes). Allocation dynamique des configurations IP dans un réseau. Ici, les postes du réseau local du siège sont en **DHCP** ; avec le réseau VPN opérateur, le DHCP est fourni par la box VPN qui fait office de relais.

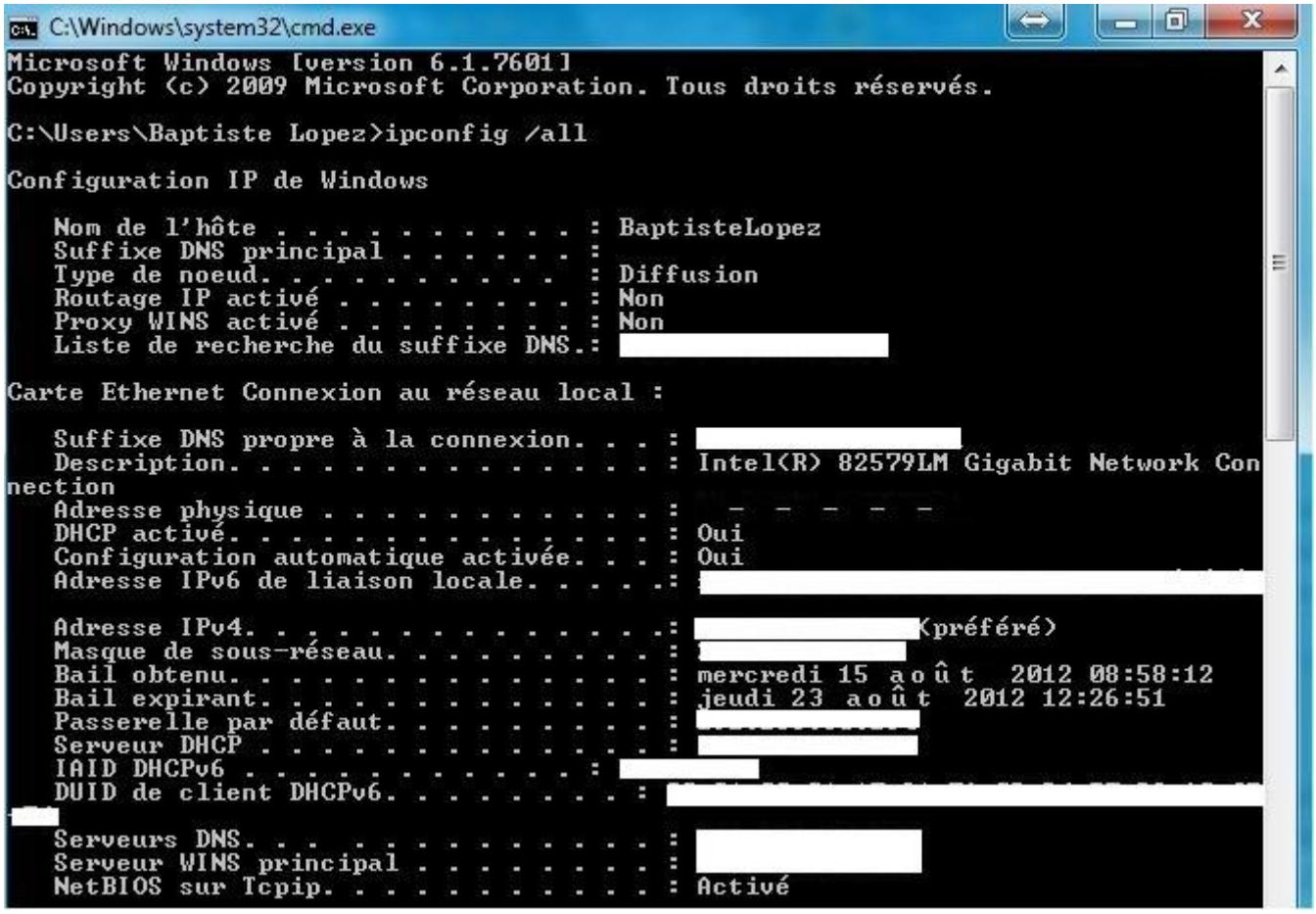


Figure 3 : Illustration de la configuration DHCP et DNS (xxx.xxx.xx.xxx) du siège.

La saisie des paramètres DNS sur les postes ne s'effectue pas, car le paramétrage du DNS est automatique (plus exactement, inclus dans la configuration offerte par le DHCP).

Les postes du siège n'ont pas besoin de se connecter en VPN, puisqu'ils sont directement dans le réseau local, que ce soit en Ethernet ou en se connectant via la WiFi du siège. Celle-ci est aussi prise en compte dans le système ZyXEL (même marque, d'où interopérabilité possible).

Néanmoins, la borne WiFi (routeur-borne WiFi ZyXEL ZyAir) du siège ne fonctionne pas très bien, ou aléatoirement, et le réseau filaire est donc sollicité au siège comme par les agences, au travers de la retransmission des données en arrivant dans le réseau local du siège.

La salle serveurs abrite, outre certains éléments décrits ci-dessus et hébergeant les applications métier cités plus haut, le cœur de réseau du groupe, l'interconnexion entre le siège et les agences. Il s'agit concrètement de l'interconnexion du réseau local du siège avec le réseau distant étendu : LAN[16] - WAN[17], dans le coffret informatique mural.

[16] **L**ocal **A**rea **N**etwork (français : **R**éseau **L**ocal - **RL**). C'est un réseau de base, taillé pour les réseaux de petite taille et/ou de faible étendue. Ici, le réseau localisé au siège (donc le réseau du siège) est un **LAN**, car sa délimitation est restreinte au bâtiment du siège.

[17] **W**ide **A**rea **N**etwork (français : **R**éseau **É**tendu). Ici, le **WAN** correspond à la sortie sur Internet, qui est considéré au même comme extérieur au siège, donc au LAN. Le WAN regroupe tout ce qui est derrière le pare-feu, du côté extérieur au siège sur le schéma, incluant le boîtier SDSL et son réseau (car adresses publiques, alors que le LAN est constitué d'adresses privées), même si une partie de ce réseau est présente au siège. De plus, de par son étendue, le WAN couvre toutes les agences, donc toute la France, de Brest/Quimper à Strasbourg/Colmar et de Lille à Cannes en passant par Olivet. C'est une étendue considérable, justifiant d'autant ce statut.

Ce coffret possède un commutateur (switch) central qui est racké dessus (c'est-à-dire fixé aux rails de bâti de la baie serveur, empilé et étagé avec d'autres), sur lequel sont raccordés et brassés plusieurs panneaux de brassage.

Sur deux de ces panneaux arrive le réseau Ethernet (raccordement des deux étages du siège, voir ci-dessous pour plus ample explication). Sur quatre autres arrivent les prises et lignes téléphoniques (connexion, par un système de brassage, des prises téléphoniques aux lignes téléphoniques, elles-mêmes reliées au PABX).

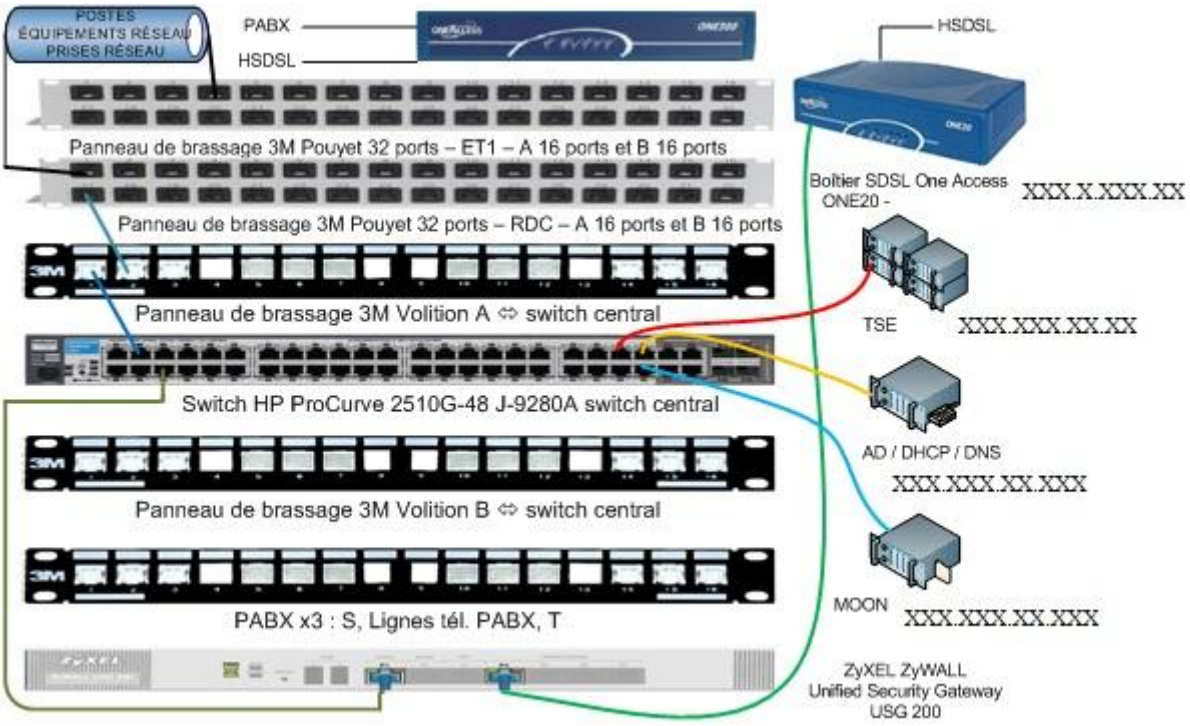


Figure 4 : La salle serveur et le cœur du réseau du siège.

Les trois panneaux PABX sont brassés de la même manière que le brassage des prises réseau sur les panneaux de brassage RDC et ETC.

Sur la figure ci-dessus :

- À droite : une partie du contenu de la baie serveur (les serveurs, le routeur SDSL)

- Sur la gauche : le coffret informatique mural

- Les trois liens obliques sur la gauche correspondent au brassage (noir, violet, bleu-vert).

- Le vert kaki est le câble reliant la patte LAN de l'USG au switch central.

- Le vert est le lien entre le routeur SDSL et l'USG 200.

- En bleu, rouge et orange, ce sont les liens directs entre les serveurs et le LAN sur le switch central.

- Le switch de brassage PABX est relié au routeur ONE300, lui-même relié au PABX et à la ligne (H)SDSL l'accompagnant.

Les différentes machines et serveurs du siège sont donc raccordés de trois façons différentes :

- brassage : les postes sont raccordées à des prises réseau, qui sont reliées aux panneaux de brassage (un pour chaque étage), les panneaux de brassage étant donc brassés sur le switch central ; ce type de raccordement de machine est assez occasionnel (par exemple, réunion),

- sur un commutateur (lui-même raccordé sur une prise réseau, brassée comme expliqué ci-dessus,

- directement sur le switch central : pour les serveurs notamment, ou certains autres postes (de test notamment).

Le réseau VPN est en fait le réseau du siège (xxx.xxx.xx.x /24). L'USG[18], dont une des fonctionnalités est le support intégré d'un dispositif de tunnel VPN, est donc le point central de tout ce système ; il est géré par le siège, en termes de localisation et d'attribution.

[18] ZyXEL ZyWALL **U**nified **S**ecurity **G**ateway (**P**asserelle de **S**écurité **U**nifiée) **USG** 200. C'est le routeur (NAT), le routeur VPN (en lien avec le client ZyXEL ZyWALL VPN des agences), le pare-feu, et le journal de log de connexion-routage LAN et WAN du siège

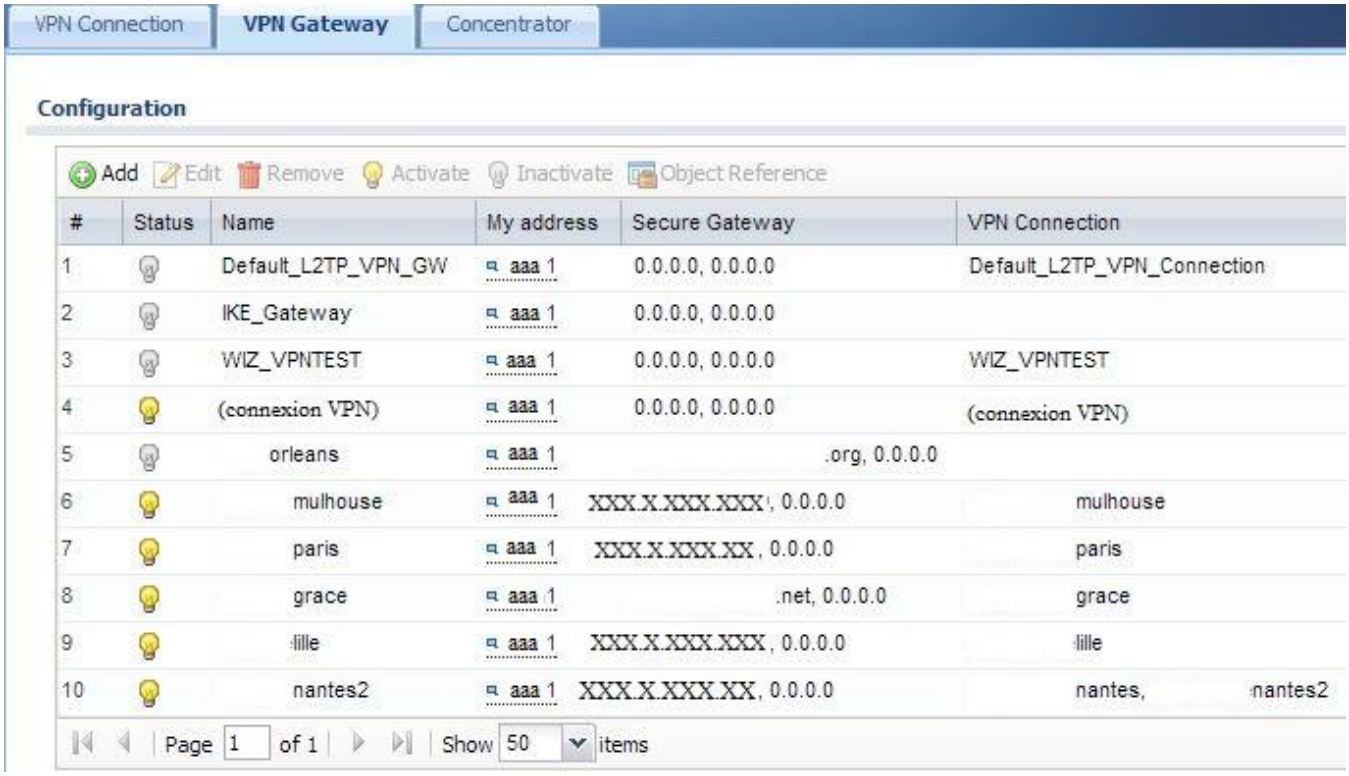


Figure 5 : Configuration des passerelles VPN ZyXEL sur l'USG 200.

Cette passerelle fait l'objet d'une configuration générale pour toutes les agences (cnxVpn, la première qui est active), hormis les cinq exceptions.

C'est la passerelle VPN des clients VPN ZyXEL des agences, pour le tunnel VPN les reliant au siège.

Les cinq exceptions sont les passerelles VPN agence[ville agence]ci-dessus.

Dans le sens Internet vers siège, les flux transitent des agences vers le siège par le WAN, puis passent du WAN au LAN du siège par le biais du routage effectué par l'USG. Ils sont redirigés depuis la « patte » du WAN (xxx.x.xxx.xx /29), vers la patte du LAN en xxx.xxx.xx.x /24 (sens inverse de la translation NAT ci-dessous).

Dans le sens siège vers Internet, le WAN est créé comme une translation (NAT[19]) d'adresse privée du LAN (xxx.xxx.xx.x /24) en une adresse publique (xxx.x.xxx.xx /29) d'un réseau fourni par Réseaux-Com, qui interconnecte le siège et Internet. Ce réseau est une plage de six adresses publiques (xxx.x.xxx.xx à xxx.x.xxx.xx incluses), certaines étant disponibles pour une utilisation par la DSI.

[19] **N**etwork **A**ddress **T**ranslation (français, non-officiel : Traduction d'Adresse Réseau). Procédé par lequel une adresse privée, non-routable à la base, est translatée puis en adresse publique, routable sur Internet, puis utilisée pour sortir effectivement sur Internet. Le **NAT** permet donc d'accéder au réseau web depuis une adresse privée.

Son adresse est xxx.x.xxx.xx, son masque de sous-réseau /29 (255.255.255.248 en notation décimale). L'une de ces adresses est utilisée par le boîtier SDSL[20] (xxx.x.xxx.xx), en tant que passerelle d'accès à Internet. Les adresses restantes, hormis celles prises (cas de l'USG avec la .xx), sont effectivement à la disposition de la DSI. Ce routeur est posé dans la baie serveur.

Le schéma VPN global consiste en une intégration du poste sur le réseau du siège via le client VPN ZyXEL. La box de l'agence, comme routeur, laisse passer les flux VPN vers Internet, pour simuler une liaison directe encapsulée (tunnel) avec l'USG, routeur VPN du siège.

Comme les agences se connectent directement à Internet, en sortant dessus grâce à leurs box, le siège ne gère pas ces flux spécifiques de navigation web des agences. En revanche, les flux de travail transitent par le tunnel VPN (seule possibilité d'accès au réseau local du siège), donc aussi par Internet (qui sert de capsule au tunnel VPN).

Le WAN peut donc se confondre avec les agences, lorsque celles-ci utilisent les applications métier, ou qu'elles télé-travaillent, le VPN changeant seulement de box pour sortir sur Internet.

La limite entre le siège et Internet se situe alors en sortie de l'USG 200. La limite géographique, elle, se situe à la sortie du bâtiment, après le routeur SDSL.

[20] **S**ymmetric **D**igital **S**uscriber **L**ine (français : Ligne d'abonné numérique à débit symétrique). Il s'agit d'une technique d'accès, permettant le transport de données à haut débit sur un réseau (jusqu'à 2 Mbit/s (megabit par seconde), avec une portée maximale de 2,4 km). Contrairement à l'**ADSL** (**A**symmetric **DSL**), pour laquelle le débit montant (upload) est plus faible que celui descendant (download), les débits montants et descendants sont égaux pour les lignes **SDSL**.

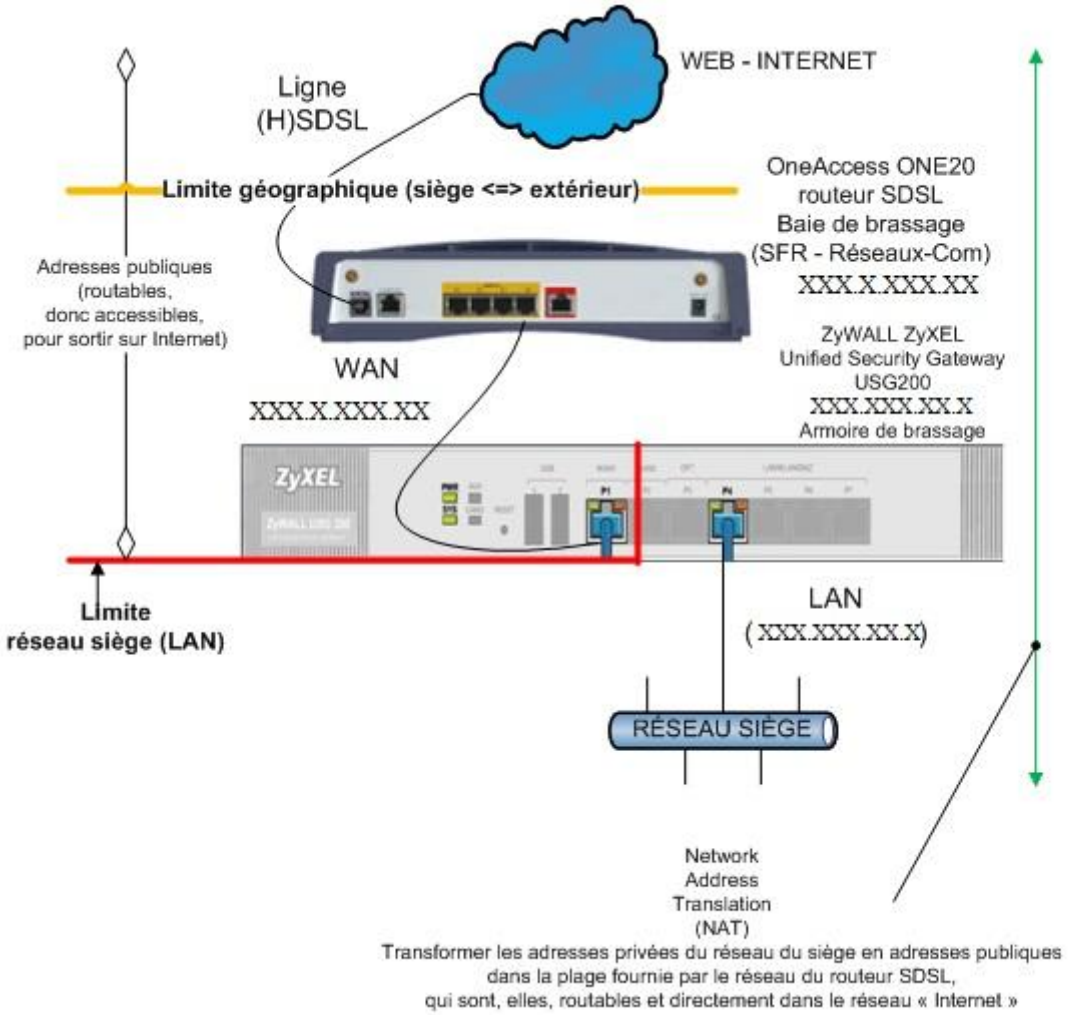


Figure 6 : LAN, WAN et accès à Internet – siège

Le siège dispose ainsi, pour ses accès à Internet, d'une liaison SDSL de débit 4 Mo (méga-octets), dont le dispositif qui permet l'arrivée des échanges au siège est le routeur SDSL.

3. ANALYSE DU PROJET : POURQUOI, POUR QUOI FAIRE

3.1. PROBLÉMATIQUE GLOBALE, ET OBJECTIF SPÉCIFIQUE DU RÉSEAU VPN

3.1.1. PROBLÉMATIQUE GLOBALE INITIALE ET DÉCLENCHEUR DU PROJET

La problématique ayant conduit à la création du projet englobant la mise en place du réseau VPN opérateur (car c'est un sous-projet, cf 3.1.2) est d'ordre technique. Un des points de cette problématique globale concerne plus particulièrement les échanges entre le siège et les agences.

En effet, il a été constaté, et remonté par les agences, mais aussi par le siège, que des utilisateurs des deux côtés ont rencontré des problèmes lors de leurs travaux nécessitant la mise à contribution du réseau local du siège (touchant notamment les serveurs). L'objectif du projet global mis en chantier par la DSI, est de fluidifier les flux entre les agences et le siège.

Les flux provenant du système existant peuvent engorger et ralentir le réseau pour trois raisons : sollicitation excessive du réseau Ethernet en lui-même (débit insuffisant) et engorgement dans le filtrage des flux (ce qui conduit à réfléchir et agir sur une des possibilités évoquées plus loin dans ce document), sollicitation excessive des applications métier en provenance du siège et/ou des agences (car le TSE est en réseau, son utilisation l'est aussi, et l'utilisation des applications métier l'est donc de même).

Il s'agit donc de pouvoir effectuer une première séparation entre les différents types de flux, ceux de travail (accès aux serveurs, applications métier, fichiers et documents métier, ...) ne dépassant pas le réseau du siège, dans lequel ils s'arrêtent.

Néanmoins, cela fait passer les flux de navigation Internet par le siège, du fait celui-ci joue en quelque sorte un rôle de fournisseur d'accès intermédiaire. Cela induit un besoin d'avoir une connexion à Internet qui soit adaptée à ce doublement de trafic, mais aussi de bien la gérer.

Cette évolution est partie intégrante des contrats passés avec les différentes organisations concernées par le projet, ou susceptibles de l'être (appel d'offres).

D'autre part, le système consistant à utiliser un logiciel client VPN est un système assez lourd. Il y a donc un autre objectif, celui de l'optimiser et de ne l'utiliser définitivement plus que pour les ordinateurs portables, lorsqu'ils sont en déplacement hors des agences, ou au domicile de leurs détenteurs/détentrices.

L'autre objectif est de substituer quasi intégralement les lignes téléphoniques et internet auparavant en service, par des lignes capables d'assurer les deux fonctions (téléphonie et données) à la fois.

3.1.2. OBJECTIFS SPÉCIFIQUES DU NOUVEAU RÉSEAU VPN

L'objectif spécifique du réseau VPN opérateur est d'éliminer les problèmes de connexion en VPN qu'induisait l'ancien système, lors de l'accès aux serveurs pour utiliser les applications métier.

C'est aussi de pouvoir faire en sorte que les utilisateurs se connectent concrètement au réseau du groupe, plutôt que de passer par Internet, pour accéder aux applications métier.

Cela facilite aussi la traçabilité des connexions, puisque tout transite par l'USG, qui inclut une possibilité de sauvegarder des journaux de connexion. Cette solution donne l'opportunité au DSI de surveiller le trafic et de prendre des décisions sur cette partie du SI en toute connaissance de cause.

Ces objectifs sont rendus permis par la mise en place de la solution réseau VPN opérateur, retenue par le DSI après étude des propositions du chef de projet de SFR, M. Hamitouche.

3.1.3. DISPOSITIF CONCERNÉ EN AGENCE : LA BOX VPN

La box retenue pour être le dispositif intégrant le support complet du VPN est la box SFR VPN NBE200. Différentes terminologies sont employées pour la désigner, « box » étant un terme générique : « routeur » est un autre exemple de terme employé.

Elle est donc nativement configurée pour agir comme un routeur, chargé de capter les flux sécurisés dans le tunnel VPN à leur arrivée sur le sous-réseau de l'agence, en provenance de l'extérieur. Ensuite elle redirige les flux de données décapsulées (ramenées à leur état initial, non-sécurisées) à l'intérieur du réseau de l'agence.

De même, elle encapsule les données provenant du sous-réseau de l'agence, avant qu'elles ne transitent sur le réseau VPN de l'opérateur, pour arriver au siège sur l'USG (qui fait lui aussi fonction de routeur VPN), qui retransmet les flux décapsulés dans le réseau local, au siège.

En outre, ce routeur est Plug and Play (raccordement à chaud possible) ; son raccordement initial est de fait facilité (hors problèmes de repérage de ligne téléphonique), y compris pour des personnes n'ayant pas beaucoup de connaissance des installations téléphoniques ou Internet.

Son manuel d'installation figure en annexe (pages 40 à 43).

3.2. FONCTIONNALITÉS ET INTÉRÊTS PARTICULIERS DU NOUVEAU SYSTÈME VPN

L'intérêt majeur du concept même du RPV est de pouvoir faire transiter des données de façon sécurisée, et somme toute, masquée.

En effet, le principe de base de fonctionnement du VPN est l'encapsulation des données d'un protocole dans un autre protocole de même couche réseau ou de couche réseau supérieure, le tout transitant de manière sécurisée et cryptée.

L'aspect de tunnel est basé dessus : les données transitent par un tunnel, et ne peuvent pas être interceptées sur cette partie bien précise de ce système, même si ce tunnel est en fait percé à travers la liaison à Internet, qui elle, est peu fiable. Toutefois, les données peuvent être récupérées aux deux extrémités du tunnel (émetteur et récepteur), raison pour laquelle des filtrages sont prévus, ou déjà existants, à ces deux extrémités.

Le but général est donc de sécuriser les flux de données, tout en les faisant transiter par le réseau du groupe et non plus Internet. C'est d'autant plus vrai pour les flux « de travail » (applications, documents et fichiers métier). C'est aussi doter les agences d'un système spécifique et dédié, qui à terme permettra d'isoler la partie la plus importante du système informatique et du réseau du groupe, qui se trouve donc au siège.

En outre, cela laisse des possibilités d'extension ou de modification des liaisons, afin de se tourner vers celles qui sont les plus appropriées d'un côté comme de l'autre des échanges.

L'évolutivité est donc aussi une fonctionnalité, car ce système possède des capacités d'intégration de composants qui permettent par exemple de le superviser. En effet, la complexité et l'étendue de ce système implique la possibilité d'avoir des moyens informatiques accolés afin de pouvoir le maîtriser dans sa globalité.

3.3. CONTRAINTES GÉNÉRALES DE LA NOUVELLE ARCHITECTURE

- Le système choisi au préalable a fait l'objet d'un contrat avec un opérateur, SFR. Des obligations contractuelles sont à respecter de part et d'autre (fournisseur, groupe, voire aussi partenaires).

- L'installation des box ne peut se faire que si la liaison existe sur ce nouveau système, entre le siège et le réseau VPN opérateur, le réseau VPN opérateur étant lui relié aux box.

- Au vu de la solution retenue pour répondre à ce besoin en VPN (remplacement de l'ancien schéma d'échanges avec le siège par le nouveau), après passage d'un appel d'offres auprès du partenaire habituel Réseaux-Com (SFR) et d'Orange, le « lien » qui permettra à ce nouveau réseau d'être relié au siège sera de la fibre optique. Les tests n'ont pu s'effectuer tant que la fibre optique n'était pas installée au siège. L'inconvénient majeur de la fibre optique est du même acabit que la nécessité de son installation, car il s'agit de sa fragilité ; toute coupure ou rupture de fibre optique cause la coupure des liaisons avec le réseau VPN opérateur, donc plus de possibilité de jonction du siège par les agences sur ce lien, et vice-versa.

- L'installation des box nécessite aussi l'installation en agence d'une ligne téléphonique dédiée par France Télécom, qui est dégroupée (séparation des parties data et voix) par SFR, la box s'installant sur cette ligne devant prendre en compte la partie data. Cette ligne est la « ligne support » VPN.

  Le processus s'effectue sur une ligne SFR dégroupée VPN par l'opérateur (c'est une contrainte, la circulation des échanges sur le VPN opérateur étant un échange de données, il faut qu'une partie de la ligne support soit affectée au transport de données).

  Il est dévolu à Réseaux-com, qui doit aussi intervenir sur les problèmes rencontrés dessus : mauvais numéro, lien avec France Télécom pour les installations physiques des lignes et des prises téléphoniques en agence, prise en charge de certains tests d'identification de lignes...

  Ce dégroupage permet de séparer la partie « data » (données) de la ligne installée par l'opérateur « historique » (France Télécom), de la partie voix des lignes.

- Les routes vers les réseaux des agences, autre préalable à l'installation des box, doivent être créées au niveau de l'USG 200. Il reste le seul dispositif de routage VPN dans le sens du siège vers le réseau VPN opérateur, qui retransmet aux box.

- Les contraintes majeures sont la disponibilité permanente et le bon fonctionnement permanent des outils pour les utilisateurs. Le bon fonctionnement des applications métier est donc un point clé, et une finalité qui ne doit pas changer par rapport à l'ancien système. Le délai accordé à la réussite d'une migration est très court. Et en cas d'échec, avant toute nouvelle tentative, l'ancien schéma doit retrouver sa place pour permettre cette continuité.

- La continuité de service et la qualité de service sont deux caractéristiques essentielles qui sont déjà possibles, et d'où peuvent découler plusieurs contraintes qui sont citées pour la plupart ci-dessous, point par point. La possibilité d'utiliser les outils dépend du fait d'être connecté au réseau du groupe.

  Pour rappel, l'AD et le TSE, dispensant les comptes et informations de sessions d'utilisateurs TSE, leur arborescence et leur droits pour l'un, et hébergeant les logiciels accessibles par sessions pour l'autre, figurent parmi les points vitaux et se trouvent au siège. Ils sont donc dans le réseau local du siège, avec l'obligation de pouvoir joindre ce dernier pour y accéder. Et ce, de quelque manière que ce soit.

- Les agences doivent pouvoir travailler à plusieurs utilisateurs, tous raccordés sur la box VPN. Le principal défaut du système existant, l'impossibilité de travailler à plusieurs en simultané, liée aux limitations du VPN des box « grand public » qui sont en service dans le système existant, est ainsi supprimé. La box VPN SFR est donc prévue pour remplacer le client VPN ZyXEL dans son rôle d'établissement du tunnel VPN, ainsi que dans celui d'encapsulation des données. Toutefois, son « interlocuteur » du et au siège, l'USG 200, est prévu pour être conservé.

- Le RPV se doit de rester imperméable aux flux totalement extérieurs aux activités des agences et du siège, donc si les agences peuvent, à la base, naviguer librement comme auparavant, il reste cependant nécessaire de garder un œil sur les flux venant complètement de l'extérieur.

- La migration s'effectue « au fil de l'eau », ce qui signifie que l'on ne migre pas tout le système d'un seul coup, comme ce serait le cas en « one shot » (voir le point ci-dessous), et on ne migre pas non plus toutes les agences en même temps.

- L'ancien système dans son ensemble est conservé dans un premier temps, jusqu'à décision contraire du DSI, afin de comparer concrètement l'efficacité des deux systèmes, de pouvoir rebasculer sur l'ancien système en cas de problème sur le nouveau, mais aussi d'avoir une vision des problèmes qui surviennent sur le nouveau système. Cette conservation, provisoire, se fait donc notamment à des fins de maintenance.

- La totalité du réseau informatique du groupe, par lequel les informations transitent, en plus d'être en toutes circonstances opérationnelle, doit aussi être adaptée au système d'information et à son schéma établi. C'est une nécessité abstraite, mais allant dans le sens de l'évolutivité, car elle y prédispose.

- Le nouveau schéma (concept théorique et schématique du nouveau réseau mis en place concrètement) doit permettre ensuite d'isoler encore plus les serveurs des éventuelles vulnérabilités, d'où qu'elles viennent (agences, siège, extérieur). Cela doit se faire dans un futur pas trop éloigné, en sus de la sécurité apportée par le nouveau réseau VPN.

- La fluidification des flux attendue ne doit pas être remise en cause, quelles que soient les évolutions futures.

4. RÉALISATION PROJET, MISE EN PLACE DU NOUVEAU RÉSEAU : PENDANT

4.1. UTILISATION DE LA FIBRE OPTIQUE

La liaison en fibre optique, d'un débit de 6 Mo, relie le siège au réseau VPN opérateur. Physiquement, cela se traduit dans la salle serveur par un boîtier spécifique, posé par un technicien mandaté par le fournisseur de la fibre, Medialys, qui délègue éventuellement cette installation à ses partenaires.

La fibre optique, qui débouche par l'arrivée France Télécom dans le siège, court jusqu'à ce boîtier, fixé dans la baie serveur, sur lequel elle est raccordée.

La qualification du lien fibre consiste à tester la continuité entre l'arrivée France Télécom, qui se trouve au dehors, et le boîtier du siège. La distance entre le POP[21] d'Orléans et le siège étant d'environ dix kilomètres, cette qualification est essentielle pour s'assurer de la non-interruption des signaux en provenance de ce POP. C'est le test qui permet de vérifier que les échanges transitant par la fibre partent du siège et arrivent bien au siège. La première étape de l'établissement de la liaison avec les agences est donc une étape physique, basée sur deux éléments : installation de la fibre, et vérification de la fibre.

Le test s'effectue donc avec une compteuse, qui est un équipement réseau portable comparable à celui que comprend un ordinateur, mais dédié aux tests de ping (test de l'envoi aller-retour de trames pour vérifier si ces trames obtiennent une réponse). Donc elle possède des témoins qui indiquent lors du test si la continuité est correcte ou non.

Dans notre cas, le technicien a raccordé sa compteuse au lien fibre sur le boîtier, et n'a pas relevé d'erreur, ce qui lui a permis de valider la qualification. Il reste alors un test de débit à faire.

Suite à cela, un switch opérateur (Huawei S5300) est fixé pour recevoir la fibre (venant de l'extérieur), et la transmettre dans le réseau au siège. Puis un autre routeur (Huawei S3300) est raccordé par un prestataire à ce switch.

Enfin, un routeur opérateur Cisco (permettant l'interconnexion du réseau VPN opérateur SFR, et donc des agences, avec le réseau local du siège) a été racké et raccordé aux deux réseaux, sur le port 25 du switch central pour le LAN, et donc sur le switch précédent, d'où la fibre repart pour faire transiter les données par le VPN opérateur.

Cette deuxième étape d'installation de la liaison par fibre optique avec le réseau VPN opérateur est primordiale, notamment pour pouvoir tester les installations des box lorsqu'elles sont faites, puisque sans liaison, pas d'échanges possibles avec les agences. Une fois validée, cette étape met fin à la première phase de lien avec les agences en passant par le VPN opérateur : mise en place du lien physique avec les agences, entre le siège et le VPN opérateur.

[21] **P**oint **O**f **P**resence (français : **P**oint **d**e **p**résence) : interface réseau entre deux entités de communication (source : Wikipédia). Une interface réseau est un point de connexion entre deux réseaux (même source).

4.2. INSTALLATION DES BOX EN AGENCE

Pour installer les box en agence, la première étape consiste à faire raccorder la box à la ligne VPN et au secteur par les utilisateurs (cf. manuel en annexe).

Pour ce faire, un test doit être effectué dans les agences, pour lesquelles un doute existe quant à la ligne sur laquelle doit être raccordée la box VPN Le branchement d'un téléphone sur une box déjà raccordée, alors que les tests pour identifier la partie données (VPN) d'une ligne fausse aussi les tests pour identifier la bonne ligne.

L'autre problème qui peut se poser, est que les utilisateurs ne savent pas toujours quelle est la bonne ligne, les configurations des locaux n'aidant pas forcément. De plus, j'ai pu constater des problèmes avec des rendez-vous pris pour des installations de lignes, qui prenaient du retard, ou pour d'autres causes.

L'organisation et le planning du personnel peuvent aussi s'en mêler, rendant parfois obligatoire le report de cette installation, le retour complet ou partiel vers le système existant, la prise d'un nouveau rendez-vous.

Ces soucis sont vus avec le responsable du projet pour la partie déploiement du réseau VPN opérateur, ainsi qu'avec le responsable Réseaux-com de la partie commande et mise en œuvre des lignes supports.

Le principal problème technique rencontré est donc la mauvaise identification de ligne téléphonique. Le test associé consiste à faire raccorder un téléphone fixe analogique par les utilisateurs, qui doit donc être seul sur la prise téléphonique à tester. Selon le type d'observations effectuées ensuite, on détermine sur quelle prise raccorder la box VPN SFR, ou s'il y a problème.

Dans ce deuxième cas, plusieurs choses sont vérifiées :

- la présence ou l'absence de tonalité, juste au décrochage (sans appeler),
- possibilité de joindre la ligne supposée et d'avoir le/la responsable d'agence ou son assistant(e) au bout du fil,
- correspondance du bon numéro à la bonne ligne

Les tests ci-dessus effectués, pour m'assurer du bon raccordement initial, je demande à la personne qui se trouve sur l'agence de vérifier les voyants de la box. Ceux-ci doivent être vert fixe pour le voyant central, et clignoter en blanc pour les deux voyants d'état trafic et accès. Ce sont des indications préalables du bon raccordement initial de la box, et qui servent à confirmer la visibilité de la box par le chef de projet SFR lorsqu'il doit configurer la box en relais DHCP.

Lorsque cette première étape est validée et vérifiée, je demande au chef de projet par mail ou au téléphone si la configuration du DHCP est effectuée et correcte, et je vérifie avec lui. Je suis son interlocuteur préférentiel en cas de problème dessus.

4.3. VÉRIFICATION DE LA CONFIGURATION, CONTINUITÉ D'ACCÈS ET FINALISATION

4.3.1. DHCP

J'essaie par la suite de prendre la main par TeamViewer, en laissant l'ancien système en parallèle, de façon à vérifier en direct. Un éventuel problème est vite détecté, la reconnexion à TeamViewer nécessitant Internet. Les postes connectés à la box sont sensés se connecter au nouveau réseau en très peu de temps. Si la reprise de contrôle n'est plus possible après la coupure de l'ancien système, le problème doit remonter au chef de projet SFR pour traitement.

Ensuite je regarde si le nouveau réseau remonte bien dans le Centre Réseaux et partage ou son équivalent sur Windows XP, Connexions réseau, et dans la liste des réseaux (Windows 7). Si c'est le cas, les paramètres sont *a priori* corrects puisque le réseau de l'agence est trouvé et joint par la machine.

J'effectue ensuite un ipconfig (ou un ipconfig /all) pour vérifier les paramètres réseau, qui doivent être corrects vis-à-vis des plages prévues dans le projet, ainsi que de la configuration du DHCP. Il doit être activé, et donc fournir les bonnes adresses dans la bonne plage, à savoir XXX.XXX.x.y, où x est le numéro du sous-réseau de l'agence, et y, le numéro de l'hôte. y doit être dans la plage attribuée par le DHCP, configurée entre XX et XXX, .XXX étant l'imprimante (voir plus bas). Les serveurs DNS paramétrés sont ceux de SFR (xxx.xx.xx.xxx et xxx.xxx.xxx.xxx).

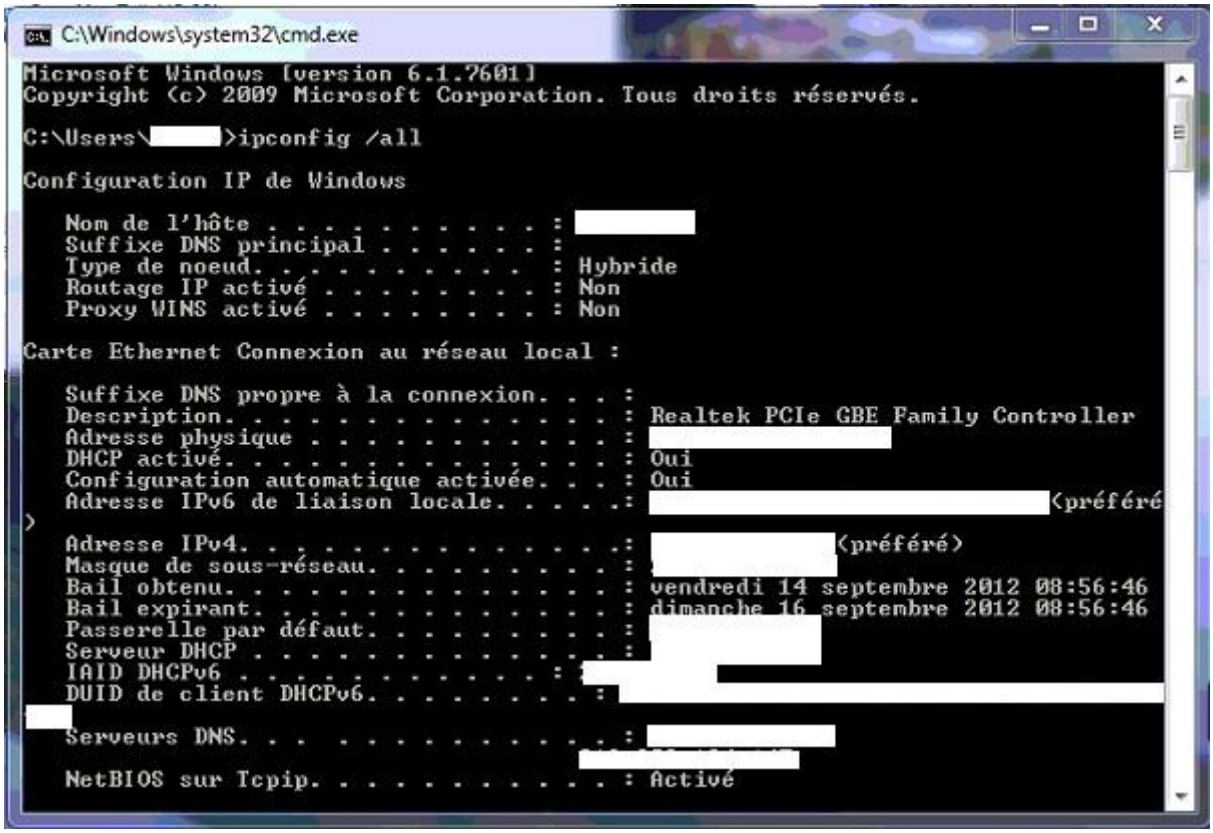


Figure 7 : Configuration réseau des agences avec le réseau VPN opérateur

Ici, un des postes en agence, certainement une agence possédant plusieurs postes, et donc raccordé probablement sur le port eth1 de la box VPN.

Dans le cas d'un DHCP qui connaitrait un dysfonctionnement, celui-ci est traité conjointement avec le chef de projet, qui identifie le problème, le traite si c'est de son ressort (mauvaise configuration), ou nous dirige vers la hotline des box VPN en déploiement du service client, ou le service client directement (incidents sur les offres données SFR) qui nous prend en charge. Selon le type d'incident, SFR fait intervenir France Télécom, ou intervient avec eux.

Il peut s'agir aussi d'un problème de route statique qui n'est pas paramétrée sur l'USG. Ce tout premier problème, rencontré lors de l'installation de l'agence d'Orléans, nous a permis de constater l'insuffisance de la configuration existante en matière de routage, car le système existant est basé sur des sous-réseaux avec un adressage commun à toutes les agences, XXX.XXX.X.x, et la gestion des échanges est basée sur le seul routage VPN.

Avec le nouveau réseau VPN opérateur, à chaque agence correspond maintenant un sous-réseau, et chaque sous-réseau nécessite donc l'ajout d'une route statique pour le joindre.

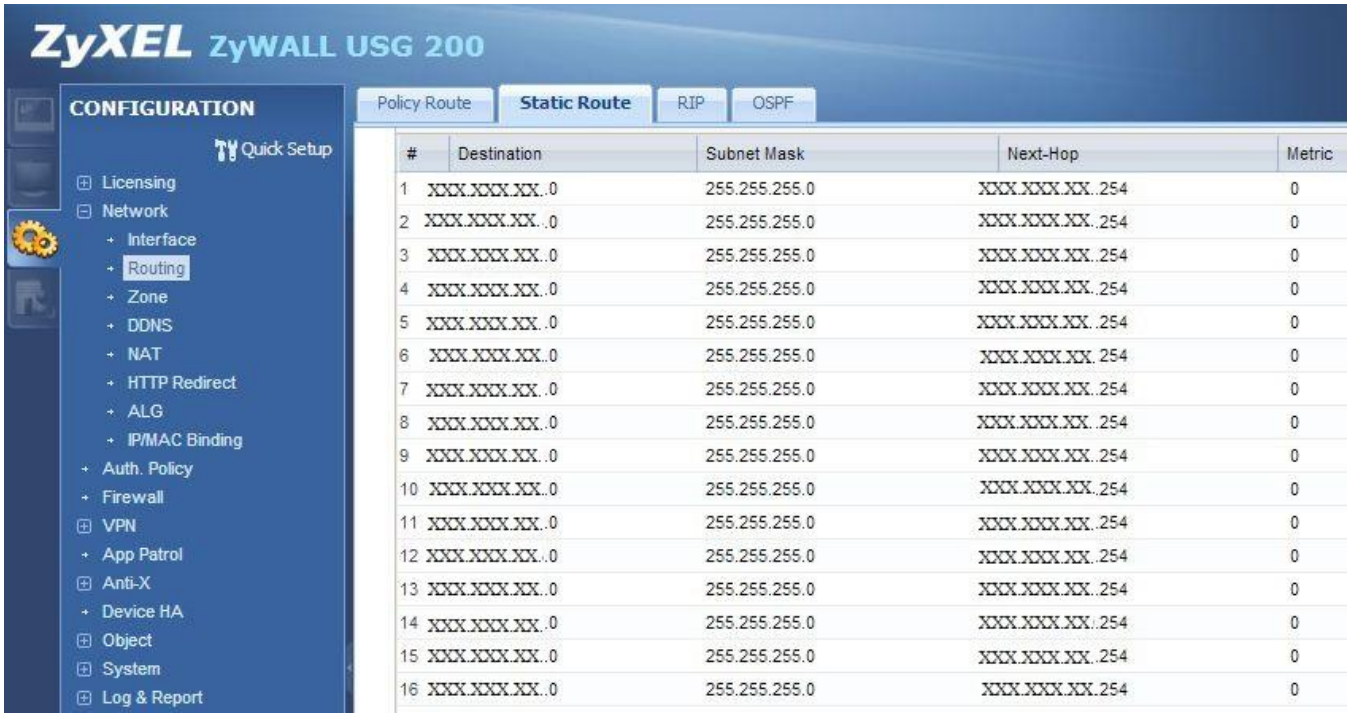


Figure 8 : Un extrait des lignes de routage statiques configurées sur l'USG200.

Par ailleurs, le RIP et l'OSPF (routage « intelligent » / automatique) ne sont pas activés.

Tout autre problème qu'un dysfonctionnement de la configuration du DHCP doit se régler avec le support activation des Modems et Routeurs Plug & Play SFR, dont le numéro de téléphone figure dans le manuel de la box, en annexe.

Une fois que cette vérification est effectuée, je peux commencer à tester l'accès à Internet. Cet accès signifie que la messagerie Outlook est également disponible.

Lorsque le processus d'installation complet d'une box est terminé, M. Hamitouche envoie les fiches de recette des opérations au DSI, et les problèmes rencontrés par la suite doivent être signalés à la hotline SFR qui gère le service technique client, dont le numéro de téléphone figure dans le manuel. M. Hamitouche ne s'occupe que de la phase de déploiement.

Les agences, dont l'ensemble des flux transitent désormais par le VPN opérateur en sortant de leur box, ont maintenant accès à Internet par l'intermédiaire de celui du siège, tandis que leurs flux dits de travail « s'arrêtent » dans le réseau du siège.

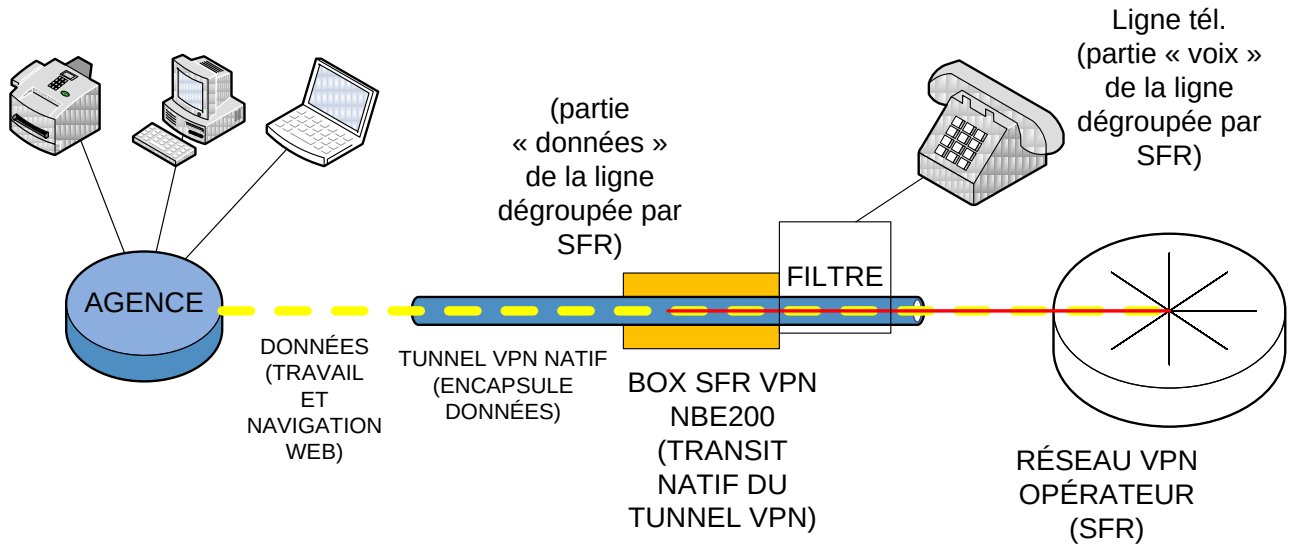


Figure 9 : Schéma après l'installation des box VPN en agences.

En rouge, le trait symbolise le trajet suivi par les données sur la ligne ADSL depuis la box, qui sont séparées de la voix par le filtre, puis sortent par la « boucle locale » vers le répartiteur téléphonique. Cela passe ensuite par le DSLAM (multiplexeur des lignes xDSL de la boucle locale qui lui viennent du répartiteur).

Le DSLAM les multiplexe (transforme) en Ethernet vers le BRAS, qui le retransmet dans le réseau VPN opérateur (SFR).

4.3.2. CONTINUITÉ D'ACCÈS ET SCHÉMA FINAL VPN

Dès lors qu'elles ont accès à Internet, les agences doivent avoir aussi accès aux applications métier et aux serveurs. C'est ce que je vérifie ensuite, afin de permettre aux agences de travailler dans la foulée de l'installation.

Le schéma VPN est finalisé avec cette deuxième étape. Les box permettent l'établissement de la jonction avec le siège, supprimant la nécessité d'ouvrir le tunnel VPN via le client ZyXEL lorsque les machines sont connectées aux box VPN, et permettant aux utilisateurs d'accéder à plusieurs en même temps sur le TSE pour travailler.

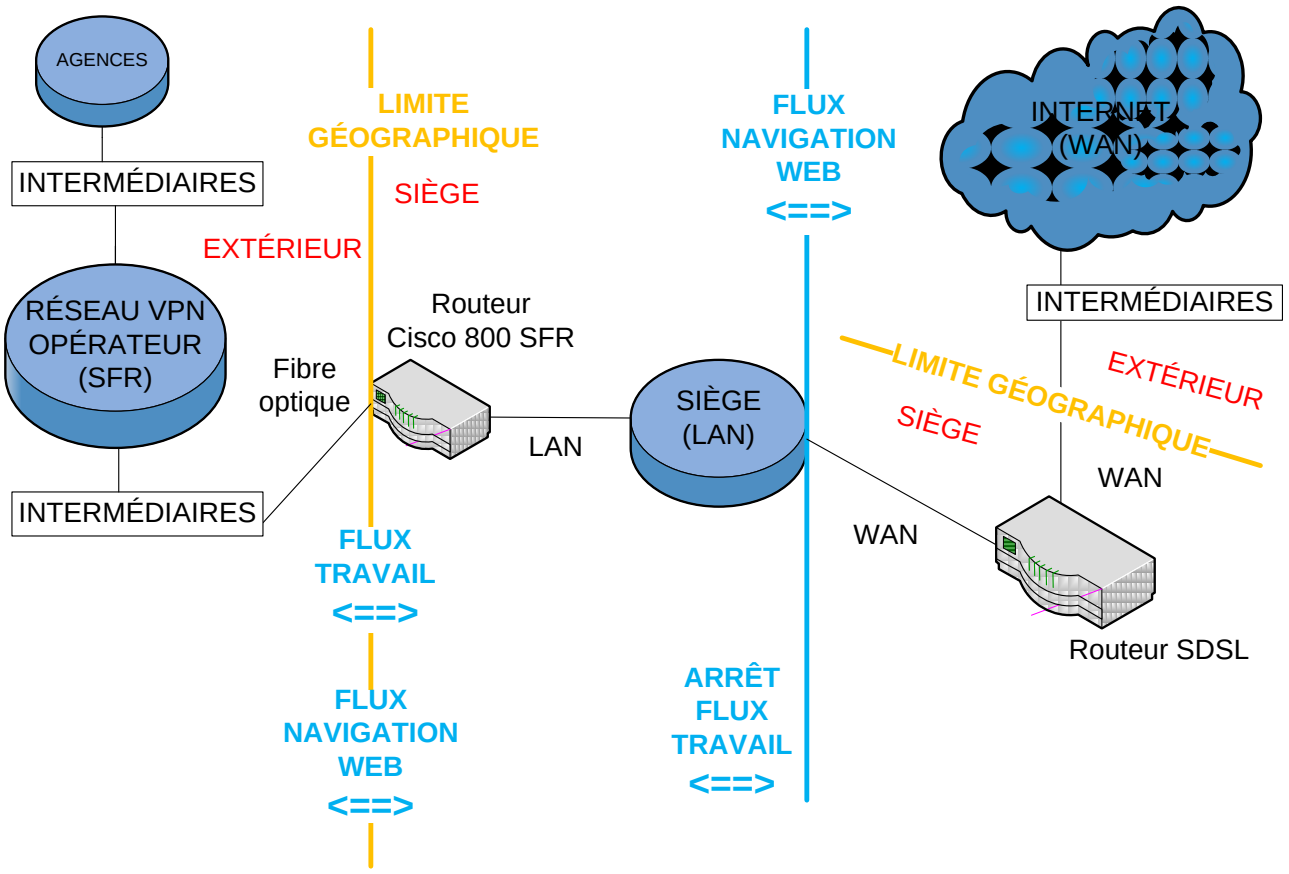


Figure 10 : Schéma final des liaisons VPN et des flux agence - siège avec les limites géographiques.

Toute la partie des agences jusqu'à la limite d'arrêt des flux de travail (qui est l'USG 200, dans les faits) est constituée de tunnel VPN.

4.4. MIGRATION DES IMPRIMANTES

Après la vérification de l'accès réseau des postes, il faut configurer les imprimantes. Je configure les paramètres d'adressage fixe de l'imprimante via les interfaces web (adresses IP, DNS), lorsque les paramètres existants ne correspondent plus aux nouveaux paramètres à adopter.

Je peux aussi faire appel à un technicien envoyé par le fabricant du copieur, soit pour paramétrer de nouveau la machine, soit pour l'initialiser (cas des agences nouvellement installées dans leurs locaux, ou venant de recevoir leur copieur). Pour certaines agences, je l'ai fait faire directement par le ou la responsable d'agence, ou par son assistante, en leur indiquant les manipulations à effectuer sur le panneau de commande du copieur.

L'adressage des copieurs est fixe, toutes les imprimantes ayant une adresse en XXX.XXX.x.XXX, où x est le sous-réseau propre à chaque agence.

À terme, l'objectif quant aux imprimantes des agences est de les raccorder en Ethernet, pour qu'elles soient toutes présentes sur le réseau. Une autre optimisation optionnelle, à laquelle j'ai contribué, est leur configuration sur le serveur TSE, afin de les mutualiser dessus (par partage et mappage), une fois leur adresse IP attribuée, la liaison réseau établie et les droits attribués.

Ce mappage causant des dysfonctionnements en agence, lorsqu'on essaie de connecter les imprimantes partagées sur le TSE depuis les sessions Windows des postes, les imprimantes locales sont paramétrées telles quelles sur ces sessions (sans se connecter sur le partage du serveur TSE et connecter les imprimantes). Il est donc utilisé seulement pour les applications métier sous session TSE. Le raccordement en USB reste possible, mais uniquement en cas d'absence d'autres solutions suite à un problème.

La partie scan est configurée de pair avec la partie email des paramètres si nécessaire (certains copieurs Canon), autrement seuls les paramètres d'email nécessaires au scan vers mail sont configurés (Konica, autres Canon, Toshiba).

5. AVENIR DU SYSTÈME, OPTIMISATIONS ET UTILISATIONS : APRÈS

5.1. DIFFÉRENCIATION DES FLUX DE NAVIGATION ET D'ACCÈS

Il s'agit ici de séparer les flux de navigation des agences, qui représentent 20 % du total du trafic régulièrement observé, et ceux qui correspondent à des accès réseau pour les applications métier (80 %).

Plusieurs solutions sont envisageables pour mettre en place cette priorisation de flux. L'une d'elles est d'utiliser celle offerte par ZeroShell (**Q**uality **o**f **S**ervice **QoS**). Éventuellement, pour renforcer l'affectation des flux et leur répartition, et ne pas trop modifier le schéma en place à la suite de la mise en œuvre du filtrage sur ZeroShell, l'installation d'une nouvelle liaison ADSL, qui sera dédiée spécifiquement aux flux de navigation des agences, peut être étudiée.

J'ai donc commencé à me renseigner sur la possibilité d'utiliser une des adresses IP disponibles sur le boîtier SDSL, pour que cette partie du système qui subsiste arrive dessus.

Ces deux parties, la priorisation de flux et le filtrage associé au siège, concerneront donc le réseau du siège et sa liaison directe avec le réseau VPN opérateur.

5.2. FILTRAGE ASSOCIÉ

Suite à la différenciation évoquée ci-dessus, il sera nécessaire de filtrer les flux pour atteindre l'objectif de contrôle du trafic.

Cela se fera derrière le boîtier SDSL, c'est-à-dire dans le réseau du siège. Un système ZeroShell est mis en œuvre pour répondre à cette problématique, étant la meilleure solution trouvée qui corresponde aux critères et aux fonctions requises par le DSI (simplicité d'utilisation, simplicité d'insertion dans le réseau, matériel pouvant prendre cette fonction en charge, …).

De plus, ZeroShell prenant en charge le SSH, on dispose d'un moyen d'accès aux journaux du système et du filtrage. Cela peut se faire par l'interface web (comme pour l'USG), ainsi que par des logiciels et services complémentaires chargés de les récupérer (KiwiSyslog, NTSyslog et WinSCP, pour ne citer qu'eux), ou offrant la possibilité de les visionner depuis la machine physique.

Ce système peut être mis en place de deux façons : la première en lançant la distribution ZeroShell comme une machine virtuelle avec le logiciel VMWare, et la deuxième en l'installant sur une machine physique, en utilisant directement les cartes réseau de cette machine pour ZeroShell.

Le transfert de partages de fichiers du serveur de fichier Moon vers le serveur AD a permis de libérer Moon et de le rendre disponible pour tenter cette deuxième solution.

Cela s'est fait en parallèle à la migration et la mutualisation par mappage des imprimantes du siège et des agences (configuration des imprimantes sur le serveur TSE, en les partageant dessus ; les agences se connectent sur ces imprimantes mutualisées, configurées par défaut pour l'impression des documents d'applications métier).

Néanmoins, l'option retenue n'a pu être validée, visiblement à cause d'un problème de configuration matérielle : la configuration IRQ de la machine physique (serveur rackable IBM System x3650) pose problème à Linux, dont ZeroShell est une distribution.

Car les pilotes de cartes Ethernet et SCSI ne peuvent gérer des interruptions, occasionnant des conflits IRQ[22], et une erreur SIOCSIFFLAGS « No such device » à l'affichage des cartes réseau sur l'interface de démarrage, et « No such file or directory » lorsque l'on essaie de localiser précisément l'erreur dans les répertoires correspondants de la distribution.

Une solution éventuelle était de paramétrer les périphériques posant problème comme « used by an ISA[23] device » (utilisé par un périphérique ISA) dans le BIOS[24].

Mais les tentatives effectuées en recherchant ce paramètre dans le BIOS du serveur IBM se sont soldées par des échecs.

Je me suis donc tourné vers IBM pour leur demander la manipulation exacte du BIOS à effectuer, mais le serveur n'étant plus sous garantie, toute question devait faire l'objet d'un devis puis d'une réponse, ainsi payante. J'ai abandonné cette option, un serveur Dell devant être commandé en urgence pour sortir de cette impasse. Il est prévu d'éviter cet écueil sur ce serveur.

---

[22] **I**nterruption **R**e**Q**uest (français : Interruption matérielle, ou Demande d'interruption) : demande d'interruption (arrêt temporaire d'un programme informatique par le microprocesseur pour en exécuter un autre), déclenchée par une ligne d'entrée-sortie matérielle d'un microprocesseur (source : Wikipédia, http://fr.wikipedia.org/wiki/Interruption_matérielle http://fr.wikipedia.org/wiki/Interruption_(informatique))

[23] **I**ndustry **S**tandard **A**rchitecture : standard de bus informatique interne utilisé pour connecter des cartes d'extension à la carte mère d'un ordinateur, remplacé par le **P**eripheral **C**omponant **I**nterconnect (**PCI**) depuis. Si les connecteurs **ISA** ont disparu des cartes mères, les bus ont subsisté. (source : Wikipédia http://fr.wikipedia.org/wiki/Industry_standard_architecture).

[24] **B**asic **I**nput-**O**utput **S**ystem (français : Système Élémentaire d'Entrée/Sortie) : ensemble de fonctionnalités lancées à l'amorçage d'une machine (mise en tension), qui permettent notamment l'initialisation, l'identification et la mise en ordre de lancement des périphériques et du Système d'Exploitation. Le **BIOS** a généralement une interface graphique épurée permettant de le configurer, avant le lancement effectif du SE.

Faute de temps disponible, je me suis replié vers l'installation d'une machine virtuelle sur la machine physique, avec VMWare Player (version gratuite du logiciel d'émulation, pour une machine virtuelle utilisable à la fois). Cette solution de virtualisation pose toutefois un autre problème, évoqué un peu plus loin.

Lors de l'installation de VMWare Player, il faut copier le dossier network.cab depuis le répertoire temporaire de l'utilisateur, et le décompresser dans le répertoire d'installation du logiciel une fois l'installation terminée. Ceci est nécessaire pour pouvoir configurer par la suite le mappage (affectation) des cartes réseau virtuelles sur les cartes réseau de la machine physique. Cette fonction n'est pas activée par défaut lors de l'installation sinon.

Ensuite, la dernière machine virtuelle ZeroShell sous image iso disponible, la version 1.0.beta16, se lance à partir de VMWare. J'ajoute une carte réseau virtuelle (émulée par VMWare elle aussi) dans la configuration de la machine virtuelle, paramétrée en « bridge » (c'est-à-dire connectée directement au réseau local) comme la première.

Les deux cartes réseau physiques de la machine sont elles paramétrées en adresses IP fixes :

- carte Ethernet Broadcom BCM5708C NetXtreme II GigE (nom : Interne) :
    - adresse IP : xxx.xxx.xx.xxx (adresse précédemment attribuée par le DHCP du siège à Moon)
    - masque de sous-réseau (celui du réseau LAN du siège) : 255.255.255.0 (= /24)
    - passerelle (l'USG 200, sur sa patte LAN) : xxx.xxx.xx.x
    - adresse serveur DNS (celui du siège) : xxx.xxx.xx.xxx
- carte Ethernet Broadcom BCM5708C NetXtreme II GigE 2 (nom : SDSL) :
    - adresse IP : xxx.x.xxx.xx (idem que celle de ZeroShell sur ETH01, même fonctionnement, mais sans passerelle dans le réseau WAN)
    - masque de sous-réseau (celui du réseau d'adresses publiques, donc le réseau WAN) : 255.255.255.248 (= /29)
    - passerelle (le routeur SDSL, puisqu'on doit le traverser en NAT pour sortir sur Internet) : xxx.x.xxx.xx
    - adresses serveur DNS : les deux adresses de serveur DNS SFR (xxx.xx.xx.xxx et xxx.xxx.xxx.xxx)

Les deux cartes réseau virtuelles sont ensuite mappées, avec le programme de configuration réseau VMWare mentionné ci-dessus (VM Network Config), sur les deux cartes réseau de la machine physique, avec deux adaptateurs (VMNet Adapter 0 et 1). La première, ETH00, est mappée avec VMNet Adapter 0 sur la carte Ethernet « Interne ». La deuxième est mappée de la même manière avec VMNet Adapter 1 sur la carte Ethernet « SDSL ».

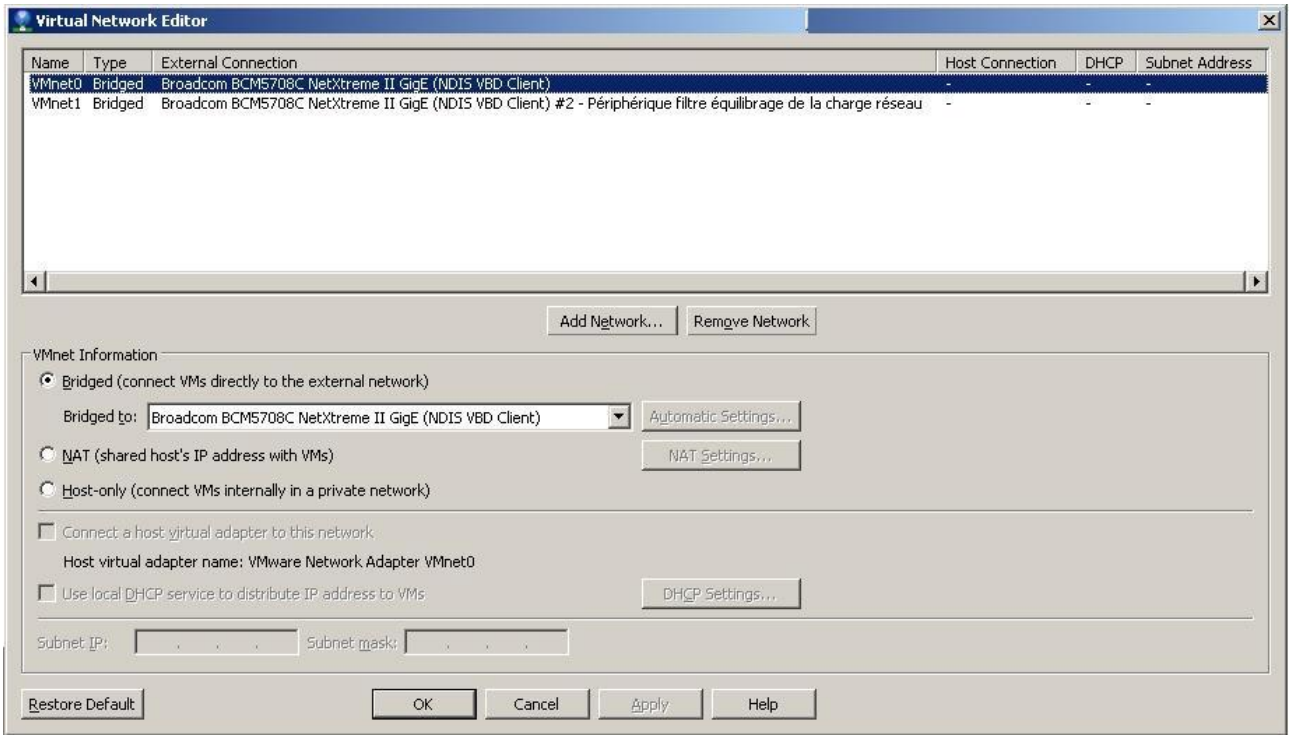


Figure 11 : Le « mappage » en bridge des deux cartes réseau virtuelles, par les adaptateurs VMNet, sur les deux cartes réseau physiques.

Ceci entérine leur propre configuration IP dans le réseau local, comme machines indépendantes sur le réseau : elles sont mappées sur les deux cartes (elles les utilisent physiquement), mais sont indépendantes du point de vue de la présence sur le réseau.

Une fois cette machine virtuelle-support de distribution lancée, ZeroShell se voit donc affecter deux cartes réseau virtuelles, ETH00 et ETH01.

ZeroShell possède une configuration initiale en xxx.xxx.x.xx. On l'attaque (on y accède) par l'interface web sur cette adresse, pour une configuration plus aisée du reste.

Ensuite on fixe cette configuration par la création d'un profil avec les cartes réseau ETH00 et ETH01, configurées respectivement en xxx.xxx.xx.xxx, et xxx.x.xxx.xx plus xxx.x.xxx.xx. La première sert à placer ZeroShell dans le réseau du siège (comme prévu dans le schéma définitif), les deux adresses IP de la deuxième servent à placer ZeroShell comme passerelle dans le réseau d'adresses publiques, et à disposer d'une adresse propre dans ce réseau, pour faire du NAT directement sur ZeroShell.

Le NAT intégré à ZeroShell, que l'on peut configurer pour traduire les adresses une par une, ou par plusieurs à la fois, est activable sur une ou plusieurs de ses cartes réseau ETH. On ne l'utilise pas dans le schéma mis en place pour les raisons déjà évoquées ci-dessus.

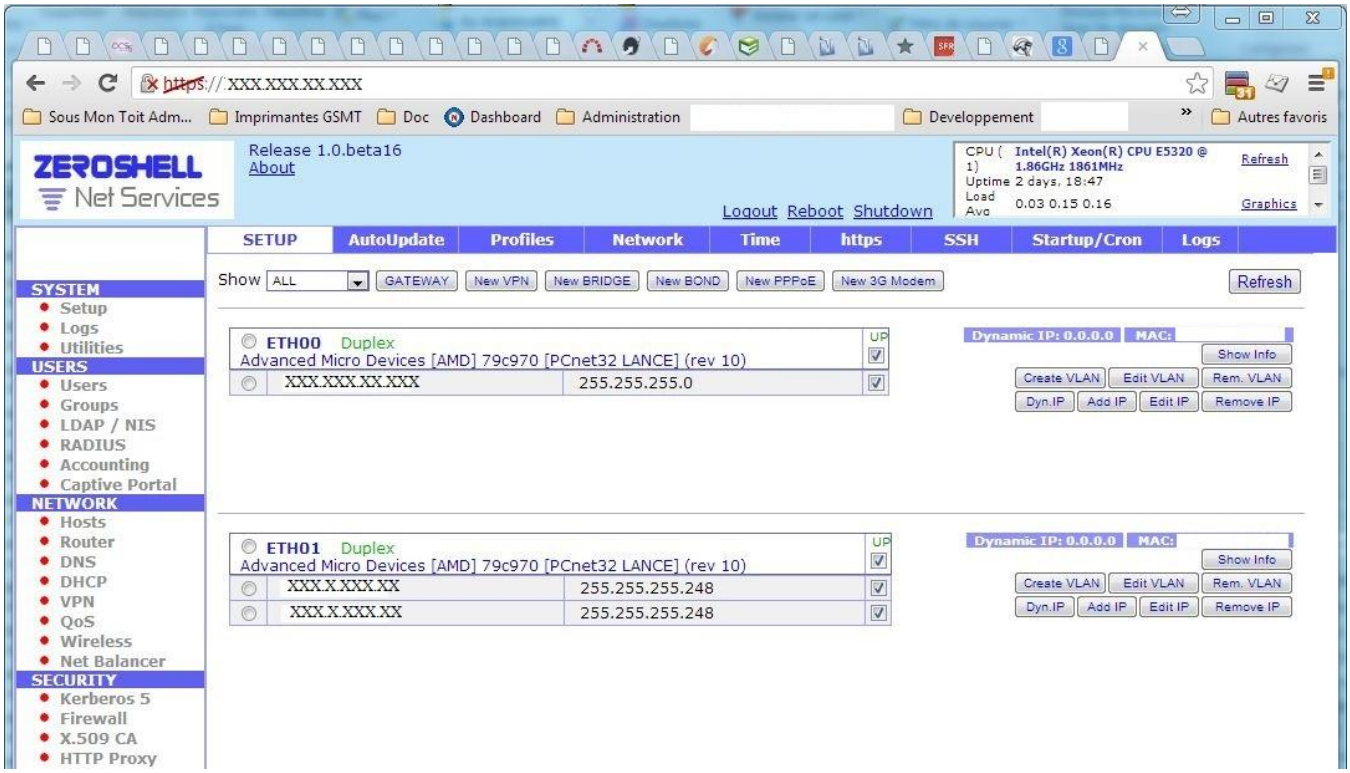


Figure 12 : Configuration réseau initiale de ZeroShell.

Étant « bridgées », les deux cartes ETH00 et ETH01 représentent chacune une machine virtuellement indépendante sur le réseau, même si pour cette présence elles utilisent les cartes physiques sur lesquelles elles sont mappées.

Ce système propose, une fois la configuration initiale effectuée, un dispositif de pare-feu, de routage et de filtrage web (proxy transparent avec antivirus), qui sont ajoutés à l'utilisation de l'USG 200, et ajustables en tenant compte de la configuration de l'USG.

Le pare-feu est utilisé en redirection et en régulation d'entrée sur ZeroShell, depuis le réseau du siège et depuis l'extérieur, qui lui parvient de l'USG par le routage, « rudimentaire » : une ligne de routage pour définir la route automatique par défaut en xxx.xxx.xx.x.

Cela se fait via la configuration de la passerelle par défaut de ZeroShell (faisable aussi depuis la configuration du routeur). Une fois configurée, un redémarrage s'impose pour la prise en compte. ZeroShell route depuis et vers le LAN, tout en routant depuis et vers l'USG, car ils sont tous les deux dans le LAN. Le routeur filtrant que constitue ZeroShell officie ainsi directement pour le siège.

Il utilise par ailleurs le NAT de l'USG 200 pour sortir sur Internet. Cette sortie fait partie des conditions requises pour que le proxy de ZeroShell, HAVP, soit effectivement « transparent ».

Un proxy est dit « transparent », lorsqu'il n'a pas besoin d'être paramétré sur les postes cibles du filtrage (dans les navigateurs notamment, pour lesquels les paramètres de proxy se trouvent dans les Options Internet de Windows). Cela permet d'éviter que les utilisateurs soient tentés de le contourner, ou de ne pas l'utiliser (le paramétrage cité ci-dessus étant à la portée de l'utilisateur qui aurait envie de le modifier).

Le paramétrage de ZeroShell comme routeur et/ou passerelle (selon le schéma adopté) est une autre de ces conditions. Ici, il est utilisé simplement comme routeur intermédiaire, le routeur final avant Internet étant l'USG 200.

Initialement, le routeur Cisco SFR est paramétré avec l'USG 200 comme passerelle.

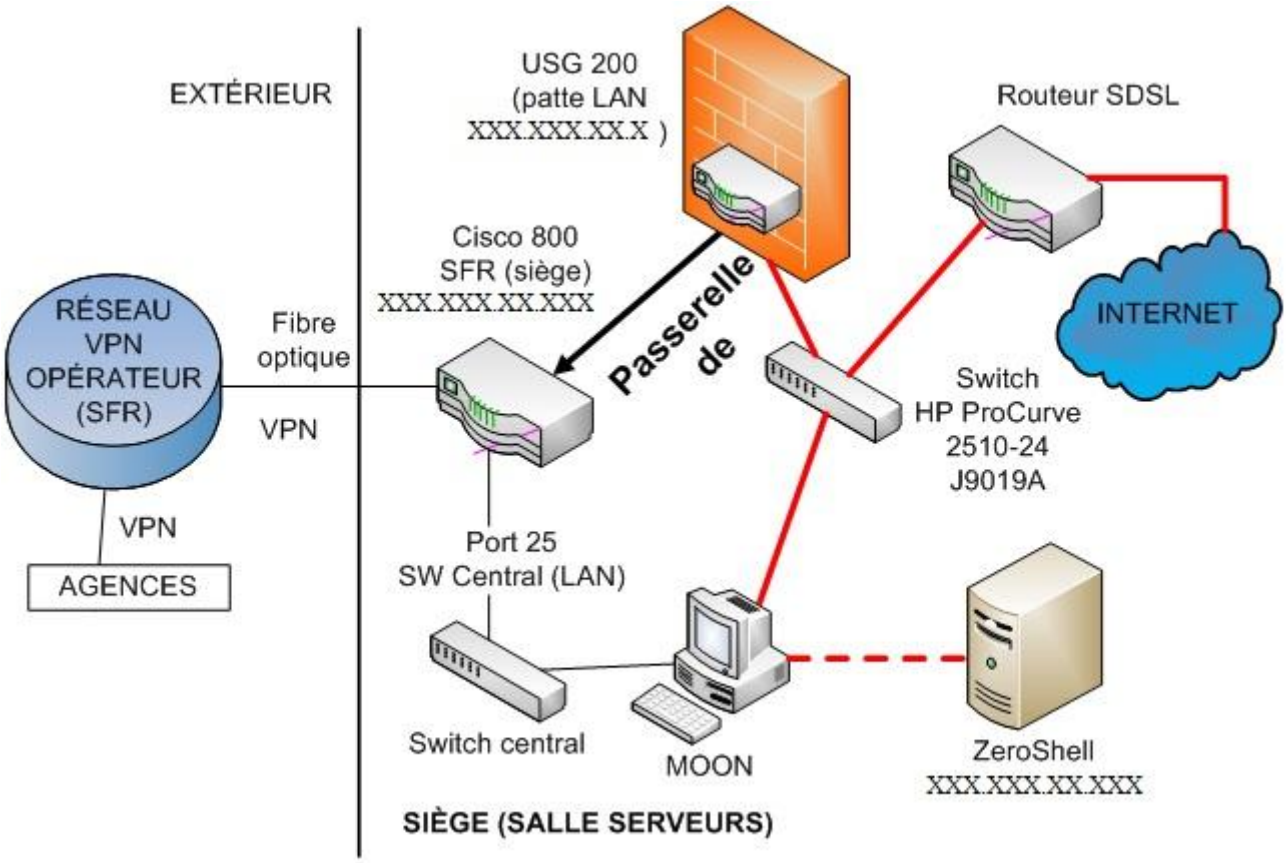


Figure 13 : Après la mise en place de ZeroShell, avant le changement de passerelle du switch Cisco SFR.

Les traits pleins et en pointillés en rouge indiquent le NAT.

Afin de capturer directement les flux des agences, sans nécessairement passer par l'USG 200, une demande est effectuée auprès de SFR, pour que la passerelle de leur routeur Cisco au siège soit ZeroShell. Ce routeur avait l'USG 200 comme passerelle depuis la mise en place du VPN opérateur, pour l'accès au réseau du siège depuis les agences, il se référait donc à celui-ci pour l'accès à Internet des agences.

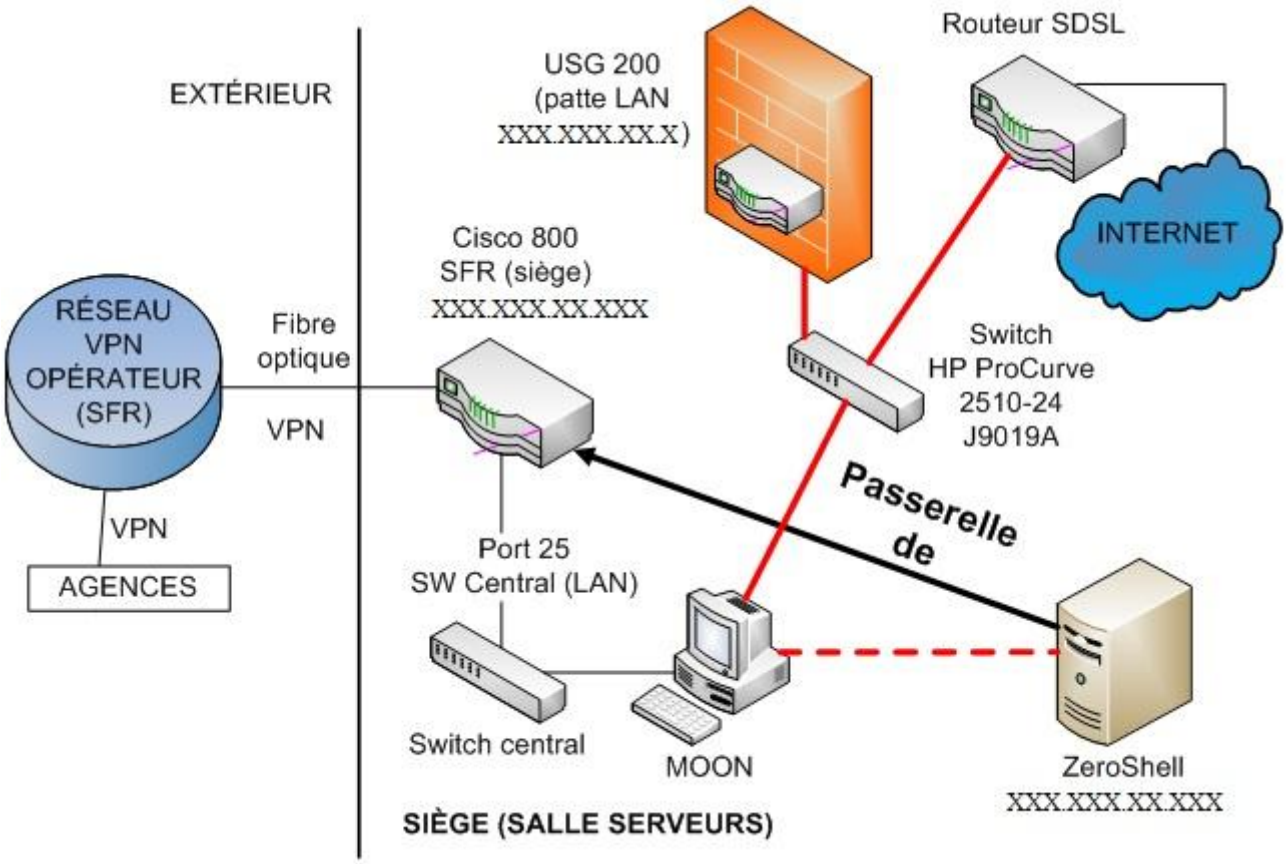


Figure 14 : Après le changement de passerelle du switch Cisco SFR.

Les traits pleins et en pointillés en rouge indiquent toujours le NAT.

ZeroShell route depuis le routeur Cisco 800 SFR vers l'USG 200 tout en filtrant ce qui passe par ses interfaces.

Un tandem est créé, qui permettra aussi d'en faire un relais, sur lequel l'on pourra basculer en cas de problèmes avec l'USG, tout en gardant la possibilité de repasser uniquement sur l'USG si c'est uniquement ZeroShell qui dysfonctionne.

Cela nécessiterait toutefois une demande au service client SFR, pour reconfigurer la passerelle par défaut du routeur Cisco de xxx.xxx.xx.xxx à xxx.xxx.xx.x.

Pour la partie filtrage, on commence par définir des listes d'URL à placer dans la blacklist (liste noire, sites à interdire) à partir de catégories de sites reconnus dangereux ou ne rentrant pas dans le cadre de l'activité professionnelle ou l'usage professionnel.

La whitelist (liste blanche) comporte les sites qui ne seront pas bloqués. On sauvegarde à chaque fois avant de quitter la fenêtre du paramètre ajouté ou changé.

Le filtrage proprement dit se fait sur la base des flux capturés, pour lesquels on peut configurer l'interface concernée, l'adresse IP ou la plage d'adresses IP émettrice, l'adresse IP ou la plage d'adresses IP de destination. On peut, de même, ne pas capturer depuis ou vers certaines sources ou destinations.

Dans le cas présent, on filtre les deux interfaces ETH00 et ETH01 (ce qui filtre tout par défaut). Ensuite on définit des adresses IP du siège, dont les flux ne sont pas à capturer, et qui échappent donc au filtrage. Il est prévu que seules les adresses IP des machines de la DSI et celle du DG ne soient pas capturées, mais en phase de test des exceptions ont pu être accordées.

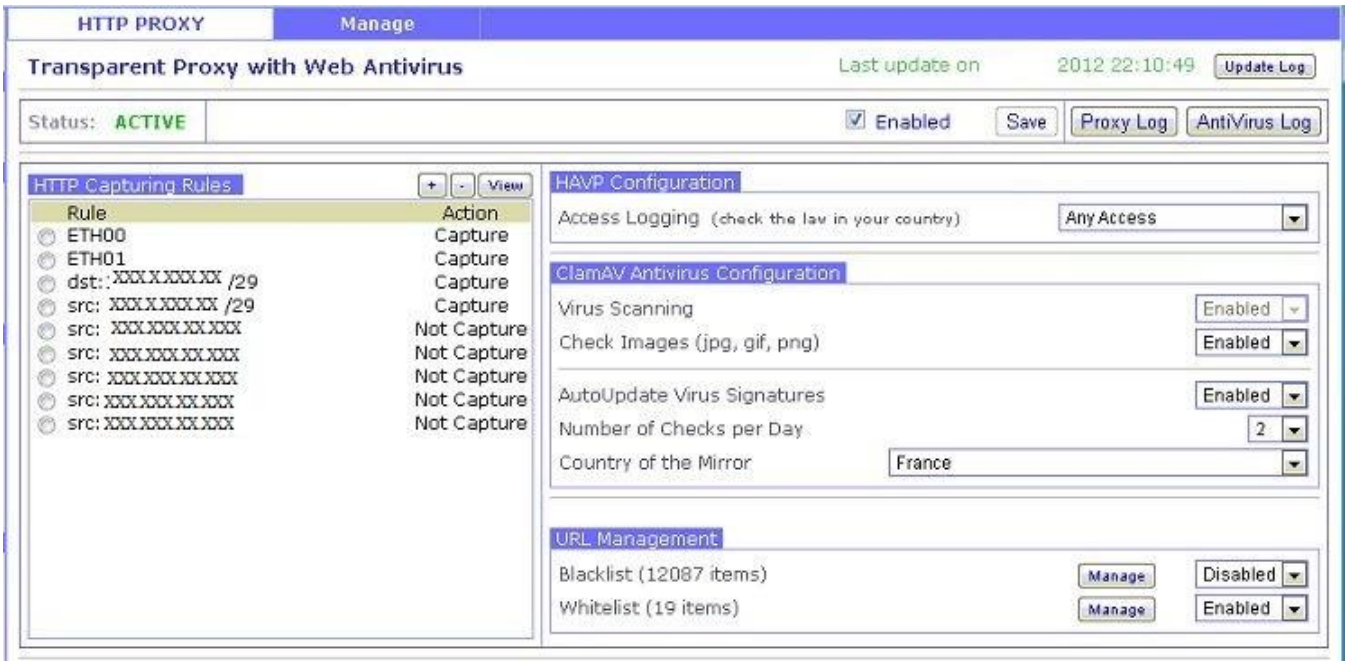


Figure 15 : Le filtrage ZeroShell activé.

On voit les deux interfaces qui sont filtrées par défaut, le sous-réseau public qui l'est aussi, et la liste des adresses IP exclues du filtrage (Not capture).

La blacklist est désactivée pour ne laisser que les sites autorisés.

Les logs HAVP enregistrent tous les accès, pas seulement les URL suspectées de contenir des virus. Les contrôles de l'antivirus sont limités à deux par jour, avec un miroir en France, pour limiter l'impact sur le débit.

Une fois les listes et les machines concernées définies, on active le tout, la prise d'effet étant immédiate.

Un des défauts du filtrage est de ralentir les accès aux pages web demandées, aussi bien au siège qu'en agences. Face à ça, on ne peut guère que réduire le nombre de contrôles de l'antivirus couplé au proxy, ainsi que configurer HAVP pour que le filtrage n'enregistre dans les logs que les URL[25] contenant des virus.

[25] **U**niform **R**esource **L**ocator (français : adresse réticulaire, ou adresse universelle). Adresses des pages web, comportant diverses informations sur le protocole employé, la localisation de la ressource (page), le nom de domaine concerné, etc.

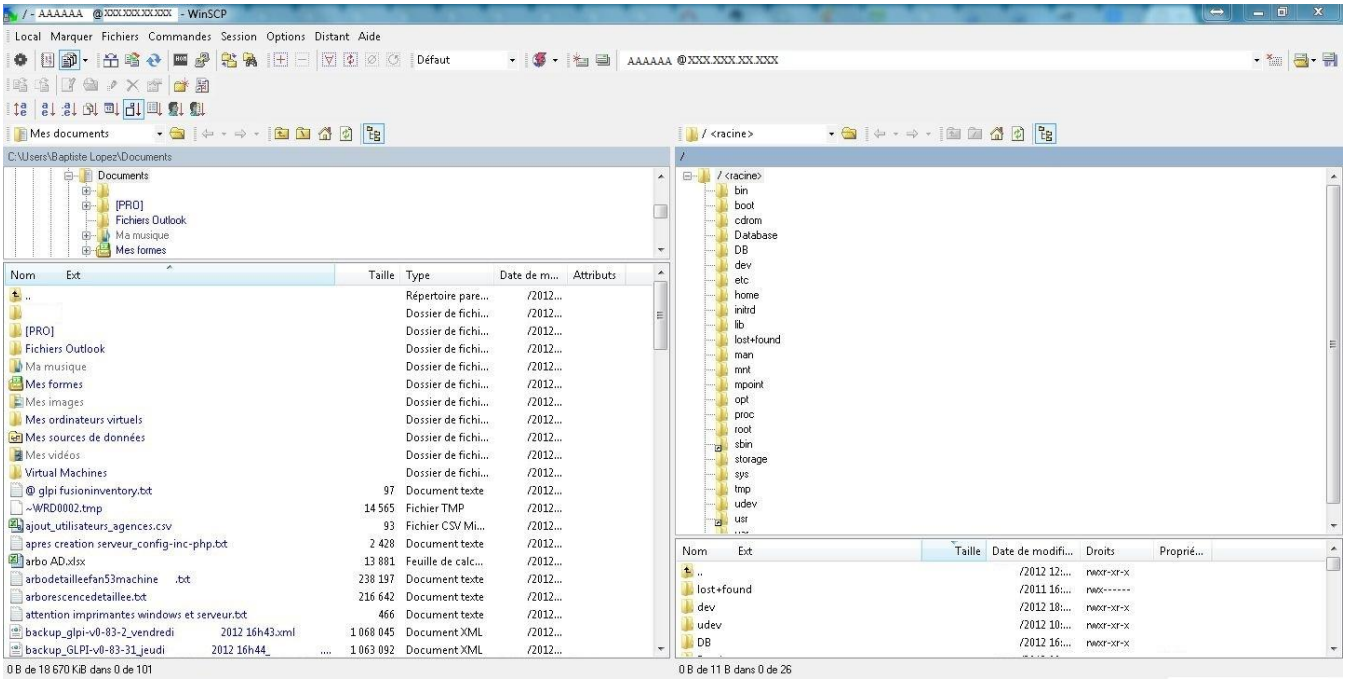


Figure 16 : Accès aux répertoires et fichiers de ZeroShell par WinSCP.

Comme ZeroShell est une machine virtuelle, et bien qu'une partition lui soit affectée (sur laquelle les profils sont), les fichiers de configuration, notamment ceux de HAVP, sont bien souvent en lecture seule générale.

5.3. MEILLEURE ISOLATION DU RÉSEAU DU SIÈGE FACE À L'EXTÉRIEUR

Le réseau du siège, qui est prévu pour évoluer vers l'ajout de différents serveurs, aura besoin d'une meilleure isolation des machines et serveurs importants.

En effet, il est plus encore l'élément central que lorsqu'il cohabitait seulement avec le système existant, car il faut rappeler que dorénavant, les utilisateurs passent directement par le réseau du siège via le réseau VPN opérateur pour les applications métier. Il est donc « pris entre deux feux », celui provenant des agences, et celui venant d'Internet.

C'est pourquoi je me suis penché sur la possibilité d'une DMZ, évoquée par le DSI comme solution pour une meilleure protection des points névralgiques présents et à venir du siège. Il s'agit aussi, dans le même temps, de leur assurer une meilleure disponibilité, en les débarrassant d'éventuels flux parasites. Cela offre la possibilité de faciliter un accès partiel aux éléments qui seront placés dedans, tout en contrôlant les accès en question par le biais de pare-feux.

BILAN

J'ai appris beaucoup de ce stage. Tout d'abord, sur moi-même et mon rapport aux utilisateurs, qu'il a fallu adapter, car il y a un certain nombre d'utilisateurs, qui n'ont pas le même niveau de connaissance informatique. La communication avec les utilisateurs et les gestionnaires, majoritairement mon maître de stage, fut donc un aspect de travail pour moi. Cela s'est vu notamment lorsque les utilisateurs ont été impactés par les différents changements apportés à l'architecture.

Les prises de contacts avec les partenaires techniques ont été une découverte, qui s'est révélée instructive, tant sur les points de gestion de la relation client - prestataire, que sur les points et avancées techniques dont nous étions amenés à discuter ensemble.

Les quelques retards de la part des prestataires dans certaines étapes importantes ont été traités, en ce qui me concerne, dans le respect du principe de « référé hiérarchique », qui appelait celui d' « escalade » auprès des fournisseurs et de leurs sous-traitants.

Ensuite, j'ai également eu la possibilité de m'informer sur des concepts et des schémas que je ne connaissais pas, tels l'installation de la fibre optique, l'architecture en LAN combinée avec un WAN.

J'ai également acquis des connaissances sur des éléments plus techniques et matériels, comme les serveurs dans leur cadre d'utilisation dans les structures développées, l'utilisation d'applications métier pour un regroupement de services.

Sur le plan des connaissances réseau et systèmes d'exploitation, j'ai pu réviser des éléments de base au travers de leur mise en œuvre concrète, comme les interconnexions, les commandes réseau et organisation de fichier des mondes Windows et Linux.

Le fait de tester des intégrations dans des schémas existants en production m'a beaucoup amené à surmonter l'appréhension que j'avais de le faire, étant habitué à tester dans un environnement spécialement dédié, hors production.

J'ai donc pu m'imprégner de principes ayant largement cours dans les organisations privées, qui sont différents de mes précédents stages, au cours desquels je n'avais pas une vision aussi étendue et globale.

Durant ces quatre mois, l'immersion a été totale. C'est la conclusion majeure, et qui constitue comme un point d'orgue de ce stage.

ANNEXES

Annexe 1 : Manuel d'installation de la NBE200

9IPnet - Prise Eco Fédélan - Accès ADSL Light - Page 1

Manuel d'installation du NBE200

L'envoi des équipements est effectué par SFR soit :

- Sur chaque site, suite à l'activation de la ligne ADSL ;
- Par lot en un point centralisé, charge au Client de les envoyer ou de les installer sur site.

Si, durant l'installation, une difficulté se présente (les lumières du CPE ne s'allument pas, il manque des cordons, etc.), le support activation des Modems et Routeurs Plug & Play SFR est disponible au :

0805.02.01.02

Ouverture du lundi au jeudi : 9h - 17h30
Et le vendredi de 9h - 16h

9IPnet - Prise Eco Fédélan - Accès ADSL Light - Page 2

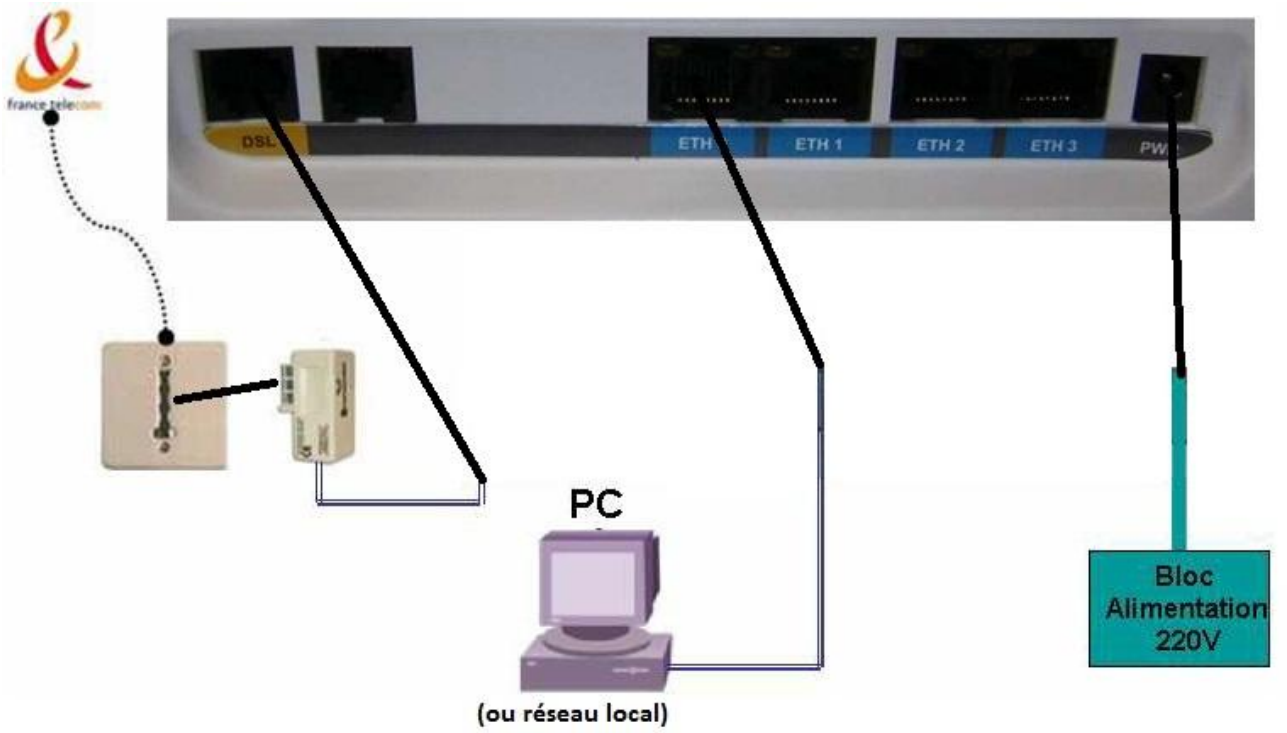
1. PACKAGE DU MODEM ROUTEUR NBE200

Le pack routeur NBE200 comprend les éléments suivants :

Désignation	Quantité	Commentaires
Modem routeur NBE200	1	
Câble téléphonique RJ11/RJ11	1	Câble de raccordement à la ligne FT
Câble Ethernet	1	Câble de raccordement au PC / câble droit
Bloc alimentation 220V	1	
Filtres ADSL	2	
Document d'installation Plug&Play	1	Le présent document

1.1 Raccordement

Le raccordement du NBE200 est visualisé par la figure suivante :



9IPnet - Prise Eco Fédélan - Accès ADSL Light - Page 3

1.2 Etapes de la connexion

1) Mise en place de l'alimentation

- Branchez la prise du bloc d'alimentation sur la face arrière du routeur
- Branchez le bloc d'alimentation dans une prise secteur 220V

2) Mise en place de la connexion ADSL

- Branchez une extrémité du câble téléphonique dans la prise ADSL du routeur
- branchez l'autre extrémité dans le filtre ADSL (filtre en forme de prise Gigogne)
- Enlevez toutes les prises de la prise téléphonique murale de la ligne
- Enfichez le filtre ADSL dans la prise téléphonique murale
- Enfichez toutes les prises téléphoniques, fax, modem, … dans le filtre ADSL (attention : 2 appareils au maximum).

Si d'autres appareils y compris alarme sont branchés sur d'autres prises de la même ligne, mettre un filtre à chaque prise murale.

3) Mise en place de la connexion au réseau local

- Branchez une extrémité du câble réseau RJ45 sur un port Fast Ethernet « Eth 0 » du routeur ADSL.
- Branchez l'autre extrémité sur la carte réseau de votre ordinateur.

2. INDICATEURS LUMINEUX DU NBE200

Les Leds de la face avant permettent de suivre le statut du NBE200 et permettent de réaliser un premier diagnostic en cas de dysfonctionnement.

Les voyants disponibles sur le dessus sont les suivants :

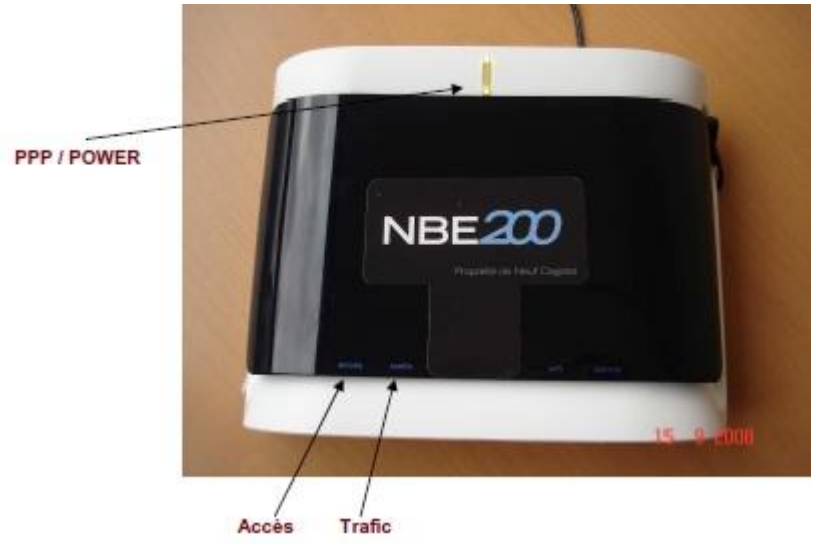


Fig1 – Vue de dessus du NBE200

Fig2 – Vue latérale du NBE200

Label	Couleur	Fonction
Accès DSL	Bleu	**Clignote** lorsque le modem se synchronise **Allumé** fixe si le lien ADSL est synchronisé
PPP/Power	Allumé Vert foncé Bleu Jaune Rouge	si le modem est **alimenté** la connexion **PPP** à l'ISP est établie Firmware en mode **rescue** La connexion PPP est DOWN **Bootloader** ou **flash** d'un firmware.
Trafic	Bleu	**clignote** s'il y a transmission de trafic DSL
ETHERNET (2 LEDS)	LED Verte LED orange	**Allumé** si la connexion est établie Clignote s'il y a une activité réseau (transmission du data)

3. PRE-REQUIS NECESSAIRE AVANT DE FAIRE APPEL A LA HOTLINE

Une fois le routeur raccordé sur la ligne dégroupée, si la connexion ne fonctionne pas :

♉ Vérification du routeur :

- faire un arrêt/marche
- état des voyants : PPP/Power, Accès DSL, Trafic, Ethernet (2 Leds)

L'état des voyants sera demandé par le technicien de la Hotline.

Si pas de synchronisation de la ligne sur le routeur, il faut :

♉ Vérifier le câblage entre le routeur et le conjoncteur téléphonique. Un filtre est obligatoire et tout équipement téléphonique (téléphone, fax, etc.) doit être raccordé sur le filtre.

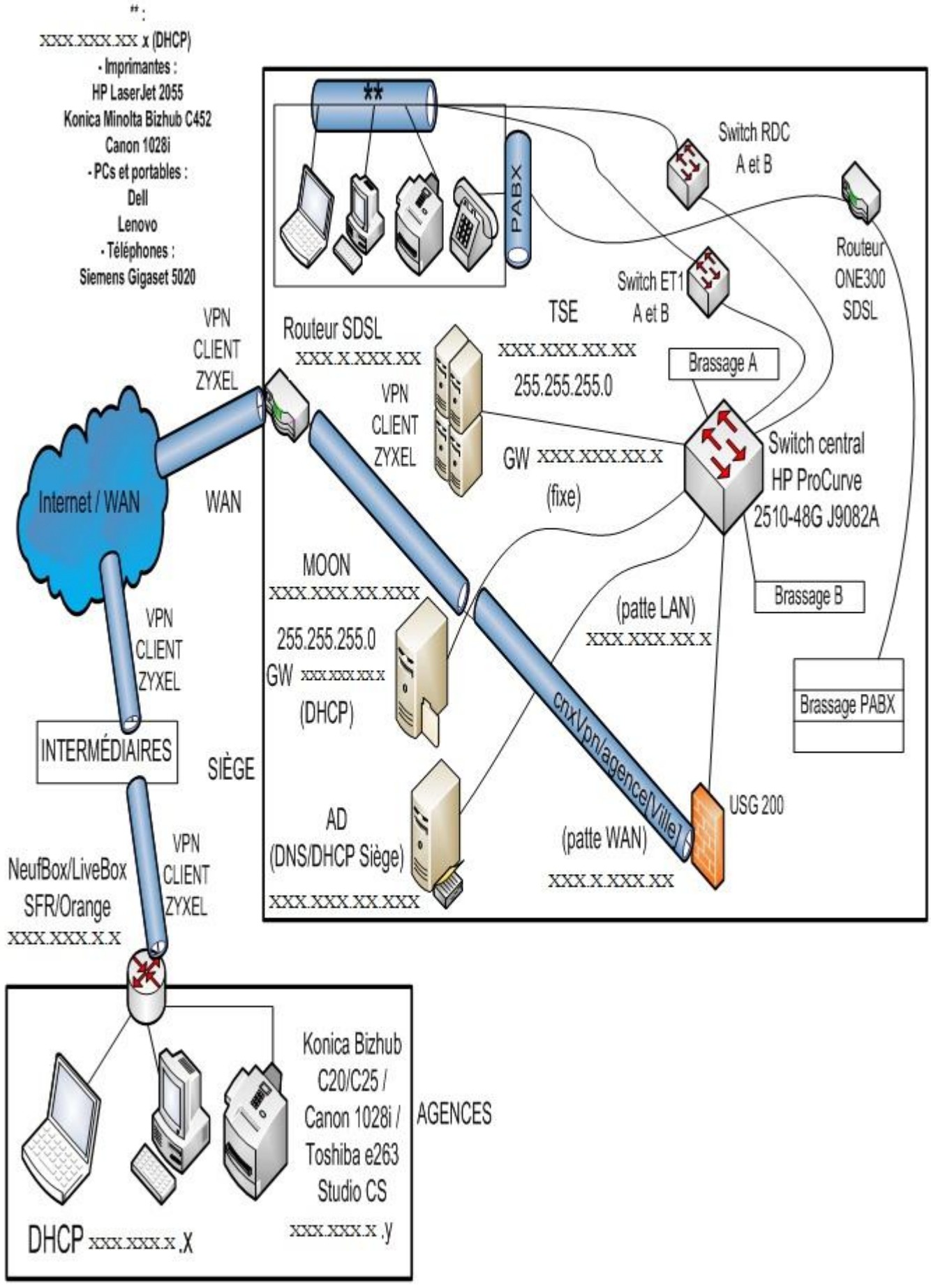
♉ Vérifier qu'un filtre est installé sur toutes les prises en parallèle de votre ligne téléphonique si des équipements y sont raccordés.

♉ Démonter chaque conjoncteur de votre ligne téléphonique et y supprimer les condensateurs. Ces derniers ont été installés par France Telecom pour pouvoir procéder à des mesures à distance. Avec leur propre équipement ADSL, ces condensateurs ne posaient pas de problèmes, mais sur nos propres équipements, ils peuvent perturber le fonctionnement du service de SFR.

♉ Vérifier le bon fonctionnement de la ligne téléphonique. L'abonnement aux services téléphoniques est à votre charge et une dégradation du signal téléphonique ou son non fonctionnement perturbe le bon fonctionnement du service SFR. Le test consiste à faire un appel sortant et constater la qualité de la conversation. En cas de dysfonctionnement ou de fonctionnement dégradé de la ligne appelez le 1013.

♉ Vérifier votre desserte interne qui correspond au câblage après le point de livraison de la ligne téléphonique par France Télécom (normalement une tête de câble pour un immeuble) la première prise téléphonique dans une maison individuelle) et qui est de votre responsabilité.

Annexe 2 : Schéma d'ensemble (ancien système informatique)



Annexe 3 : Schéma d'ensemble (nouveau système informatique)

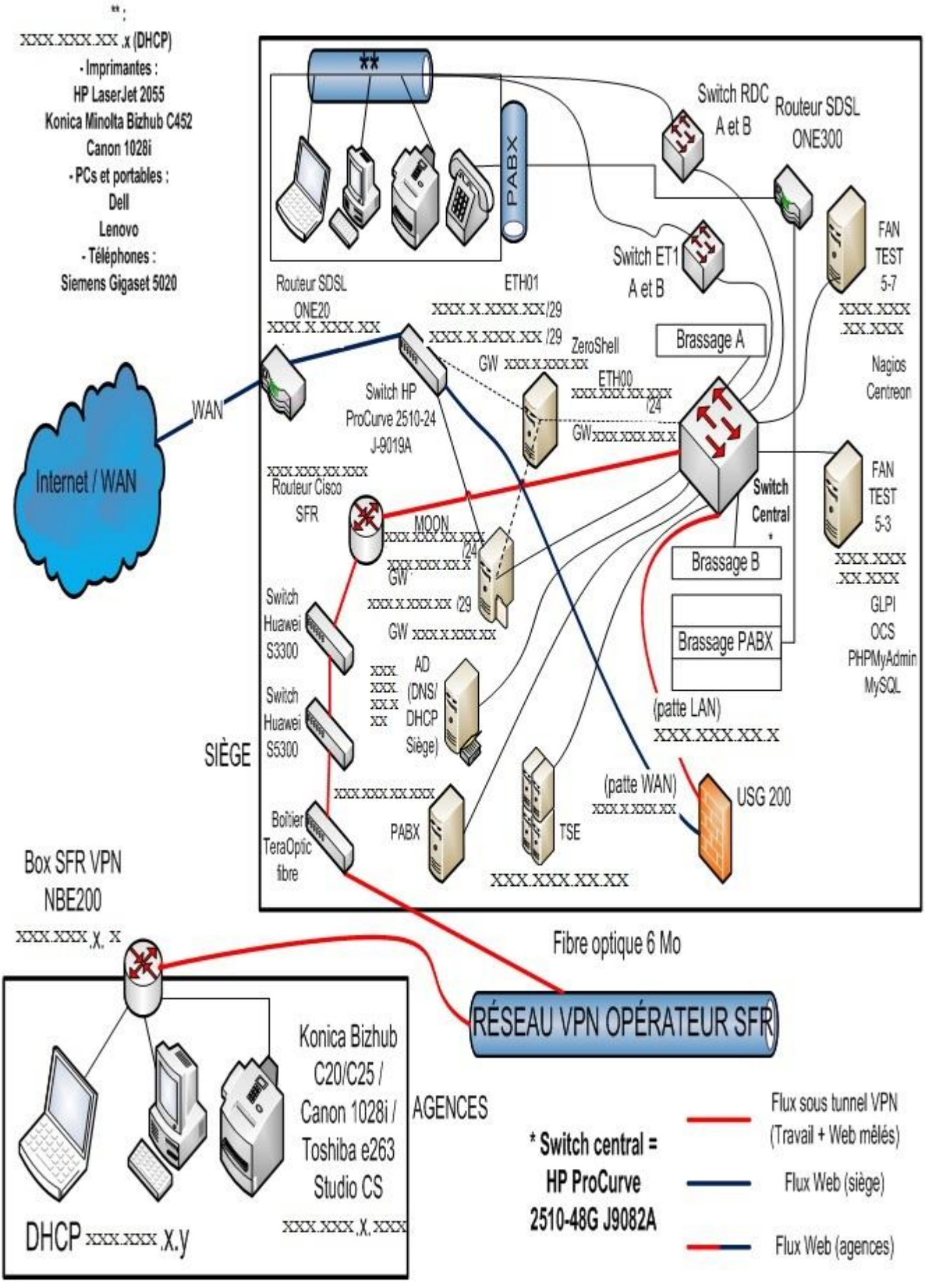


TABLE DES ILLUSTRATIONS