DESCRIPTION DE L'ENTREPRISE GSB ET DE SES BESOINS INFORMATIQUES

Sommaire

Description du laboratoire GSB

Le secteur d'activité

L'industrie pharmaceutique est un secteur très lucratif dans lequel le mouvement de fusion acquisition est très fort. Les regroupements de laboratoires ces dernières années ont donné naissance à des entités gigantesques au sein desquelles le travail est longtemps resté organisé selon les anciennes structures. Des déboires divers récents autour de médicaments ou molécules ayant entraîné des complications médicales ont fait s'élever des voix contre une partie de l'activité des laboratoires : la visite médicale, réputée être le lieu d'arrangements entre l'industrie et les praticiens, et tout du moins un terrain d'influence opaque.

L'entreprise

Le laboratoire Galaxy Swiss Bourdin (GSB) est issu de la fusion entre le géant américain Galaxy (spécialisé dans le secteur des maladies virales dont le SIDA et les hépatites) et le conglomérat européen Swiss Bourdin (travaillant sur des médicaments plus conventionnels), lui-même déjà union de trois petits laboratoires.

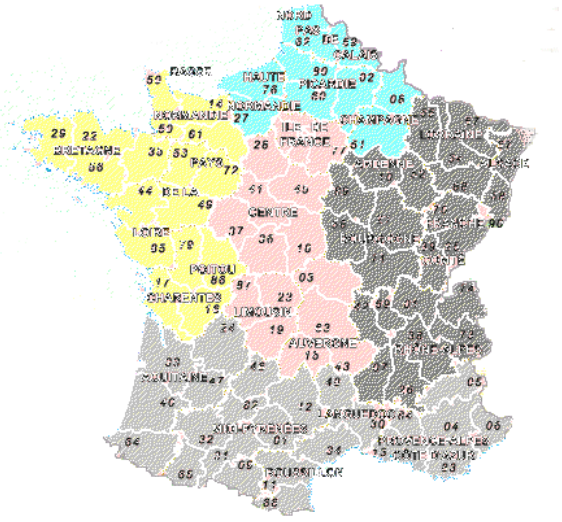
En 2009, les deux géants pharmaceutiques ont uni leurs forces pour créer un leader de ce secteur industriel. L'entité Galaxy Swiss Bourdin Europe a établi son siège administratif à Paris. Le siège social de la multinationale est situé à Philadelphie, Pennsylvanie, aux Etats-Unis.

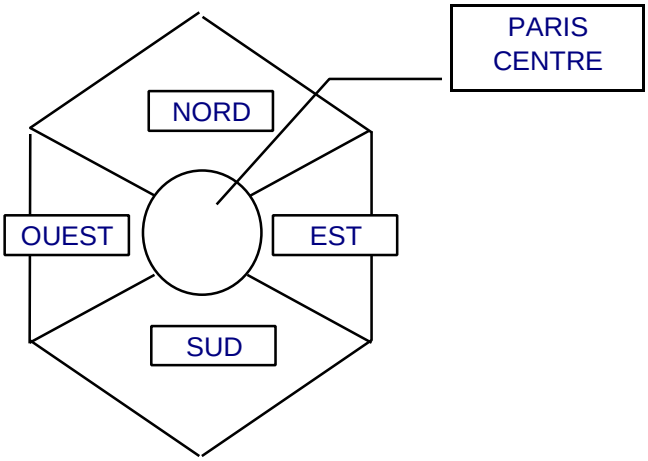
La France a été choisie comme témoin pour la restructuration et la mutualisation des agences du territoire.

Réorganisation

Une conséquence de cette fusion, est la recherche d'une optimisation de l'activité du groupe ainsi constitué en réalisant des économies d'échelle dans la production et la distribution des médicaments (en passant par une nécessaire restructuration et vague de licenciement), tout en prenant le meilleur des deux laboratoires sur les produits concurrents.

L'entreprise compte 480 visiteurs médicaux en France métropolitaine (Corse comprise), et 60 dans les départements et territoires d'outre-mer. Les territoires sont répartis en 6 secteurs géographiques (Paris-Centre, Sud, Nord, Ouest, Est, DTOM Caraïbes-Amériques, DTOM Asie-Afrique). Une vision partielle de cette organisation est présentée ci-dessous.





Après deux années de réorganisations internes, tant au niveau du personnel que du fonctionnement administratif, l'entreprise GSB souhaite restructurer certaines agences en testant la restructuration sur 3 zones géographiques majeures comportant chacunes trois agences spécialisées et complémentaires. Les villes concernées sont Lyon, Toulouse et Lille

Description du Système Informatique

Le système informatique

Sur le site parisien, toutes les fonctions administratives (gestion des ressources humaines, comptabilité, direction, commerciale, etc.) sont présentes. On trouve en outre un service *laborecherche*, le service juridique et le service communication.

La salle serveur occupe le 6ème étage du bâtiment et les accès y sont restreints (étage accessible par ascenseur à l'aide d'une clé sécurisée, portes d'accès par escalier munies d'un lecteur de badge, sas d'entrée avec gardien présent 24h/24).

Les serveurs assurent les fonctions de base du réseau (DHCP, DNS, Annuaire et gestion centralisée des environnements) et les fonctions de communication (Intranet, Messagerie, Agenda partagé, etc.). On trouve aussi de nombreuses applications métier (base d'information pharmaceutique, serveurs dédiés à la recherche, base de données des produits du laboratoire, base de données des licences d'exploitation pharmaceutique, etc.) et les fonctions plus génériques de toute entreprise (Progiciel de Gestion Intégré avec ses modules RH, GRC, etc.).
Une réflexion est à l'étude sur la mise en place de la virtualisation d'une majorité de serveurs.

Constitué autour de VLAN, le réseau segmente les services de manière à fluidifier le trafic.

Les données de l'entreprises sont considérées comme stratégiques et ne peuvent tolérer ni fuite, ni destruction. L'ensemble des informations est répliqué quotidiennement aux Etats-Unis par un lien dédié. Toutes les fonctions de redondances (RAID, alimentation, lien réseau redondant, Spanningtree, clustering, etc.) sont mises en œuvre pour assurer une tolérance aux pannes maximale.

La gestion informatique

La DSI (Direction des Services Informatiques) est une entité importante de la structure Europe qui participe aux choix stratégiques.
Pour Swiss-Bourdin, qui occupait le siège parisien avant la fusion, l'outil informatique et l'utilisation d'outils décisionnels pour améliorer la vision et la planification de l'activité ont toujours fait partie de la politique maison, en particulier pour ce qui concerne la partie recherche, production, communication et juridique.
La partie commerciale a été le parent pauvre de cette informatisation, les visiteurs étant vus comme des acteurs distants autonomes. La DSI a convaincu l'entreprise que l'intégration des données fournies par cette partie aura un impact important sur l'ensemble de l'activité.

L'équipement

L'informatique est fortement répandue sur le site. Chaque employé est équipé d'un poste fixe relié au système central. On dénombre ainsi plus de 350 équipements terminaux et un nombre de serveurs physiques conséquent (45 en 2012).

On trouve aussi des stations de travail plus puissantes dans la partie *labo-recherche*, et une multitude d'ordinateurs portables (personnels de direction, service informatique, services commerciaux, etc).

Les visiteurs médicaux reçoivent une indemnité bisannuelle pour s'équiper en informatique (politique Swiss-Bourdin) ou une dotation en équipement (politique Galaxy). Il n'y a pas à l'heure actuelle d'uniformisation des machines ni du mode de fonctionnement

Organisation du réseau du siège social parisien

Répartition des services

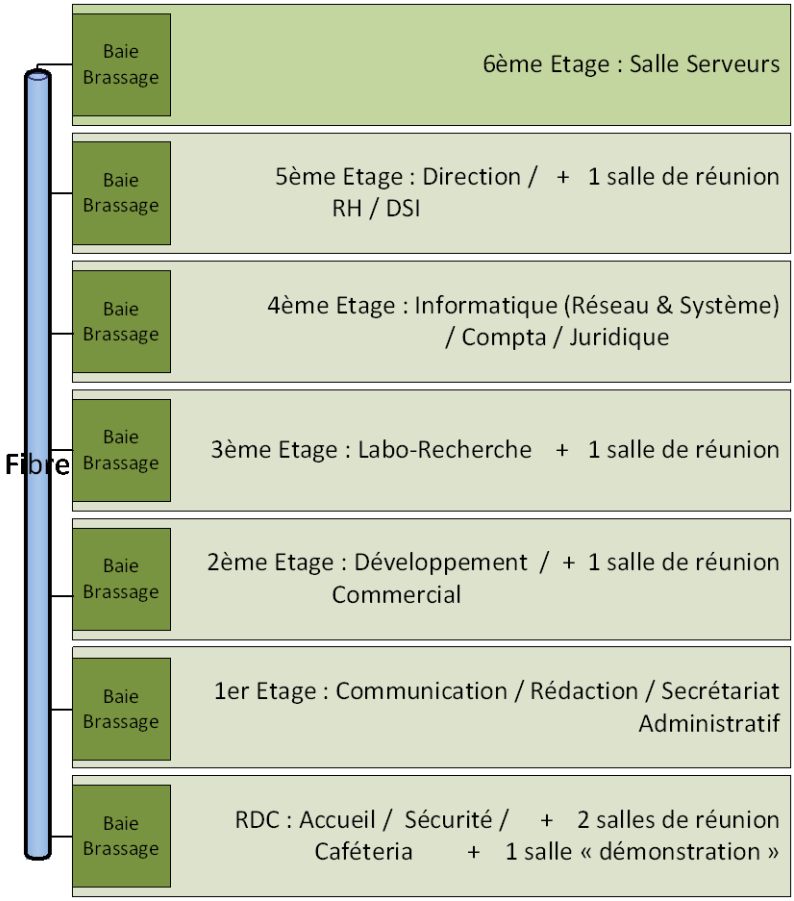
Chaque étage dispose d'une baie de brassage qui le relie par une fibre à la baie centrale de la salle serveurs.

Toutes les salles de réunion sont équipées d'un point d'accès Wifi positionné par défaut dans le VLAN "Visiteurs" qui autorise uniquement un accès Internet.
Les portables connectés en wifi à ce point d'accès reçoivent ainsi une adresse IP et n'ont, par conséquent accès qu'aux services DHCP et DNS.

Le point d'accès peut être configuré à la demande pour être raccordé à un VLAN présent au niveau de l'étage.

Chaque salle de réunion dispose d'un vidéoprojecteur, d'enceintes et d'un tableau numérique interactif.

La salle "Démonstration" est destinée à l'accueil des organismes de santé (AFSSAPS notamment) et des partenaires scientifiques. Elle dispose de paillasses et d'équipements de laboratoire, en plus d'une salle de réunion.



Segmentation

L'organisation des VLAN et de l'adressage IP n'a pas encore été publiée aux responsables techniques (vous) des agences car le directeur technique est en pleine restructuration du plan d'adressage et des vlans. Si vous devez intervenir au siège social, il vous sera communiqué les informations nécessaires à vos interventions.

Salle serveur et connexion internet au siège social

L'organisation des serveurs vous sera communiquer au long de vos missions dans l'organisation. Actuellement la direction ne vous a communiqué aucune information certainement en raison de la restructuration menée par le directeur technique du siège.

Domaine d'étude

L'entreprise souhaite porter une attention nouvelle à sa force commerciale dans un double objectif : obtenir une vision plus régulière et efficace de l'activité menée sur le terrain auprès des praticiens, mais aussi redonner confiance aux équipes malmenées par les fusions récentes.

Les visiteurs

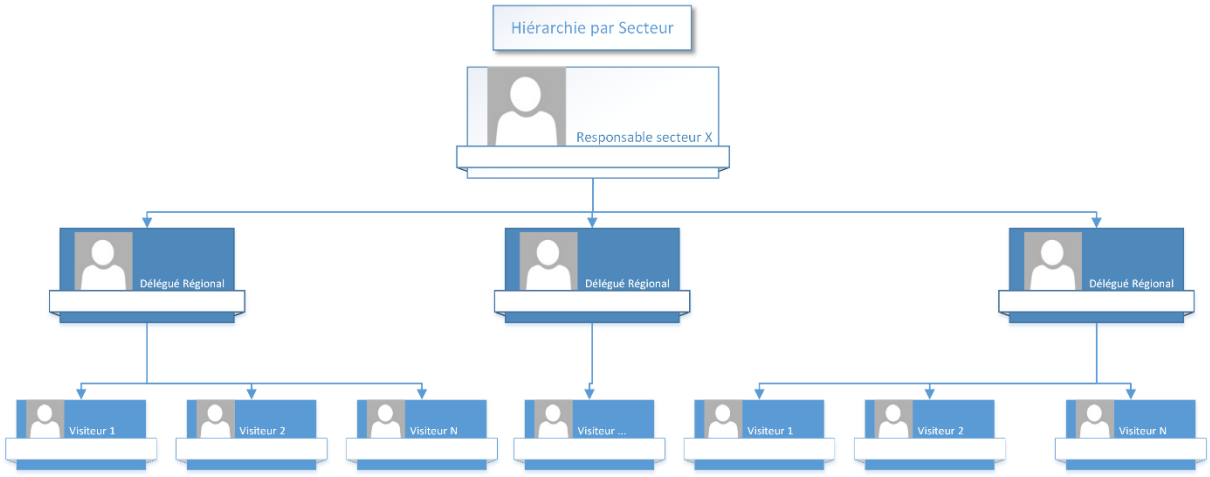
La force commerciale d'un laboratoire pharmaceutique est assurée par un travail de conseil et d'information auprès des prescripteurs. Les *visiteurs médicaux* (ou *délégués*) démarchent les médecins,

pharmaciens, infirmières et autres métiers de santé susceptibles de prescrire aux patients les produits du laboratoire.

L'objectif d'une visite est d'actualiser et rafraîchir la connaissance des professionnels de santé sur les produits de l'entreprise. Les visiteurs ne font pas de vente, mais leurs interventions ont un impact certain sur la prescription de la pharmacopée du laboratoire.

Pour donner une organisation commune aux délégués médicaux, l'entreprise a adopté l'organisation de la flotte de visiteurs existant chez Galaxy, selon un système hiérarchique par région et, à un niveau supérieur, par secteur géographique (Sud, Nord, Paris-Centre, Antilles-Guyane, etc).

Il n'y a pas eu d'harmonisation de la relation entre les personnels de terrain (Visiteurs et Délégués régionaux) et les responsables de secteur. Les habitudes en cours avant la fusion ont été adaptées sans que soient données des directives au niveau local.



On souhaite améliorer le contact entre ces acteurs mobiles autonomes et les différents services du siège parisien de l'entité Europe. Il s'agit d'uniformiser la gestion du suivi des visites.

Les visiteurs et les autres services

Les déplacements et actions de terrain menées par les visiteurs engendrent des frais qui doivent être pris en charge par la comptabilité. On cherche à agir au plus juste de manière à limiter les excès sans pour autant diminuer les frais de représentation qui font partie de l'image de marque d'un laboratoire. Chez Galaxy, le principe d'engagement des frais est celui de la carte bancaire au nom de l'entreprise. Chez Swiss-Bourdin, une gestion forfaitaire des principaux frais permet de limiter les justificatifs. Pour tout le reste, le remboursement est fait après retour des pièces justificatives.
Une gestion unique de ces frais et remboursement pour l'ensemble de la flotte visite est souhaitée.

Les visiteurs récupèrent une information directe sur le terrain. Ceci concerne aussi bien le niveau de la confiance qu'inspire le laboratoire que la lisibilité des notices d'utilisation des médicaments ou encore les éventuels problèmes rencontrés lors de leur utilisation, etc.
Ces informations ne sont actuellement pas systématiquement remontées au siège, ou elles le sont dans des délais jugés trop longs. Le service *rédaction* qui produit les notices souhaite avoir des remontées plus régulières et directes. Ceci permettra également au service *labo-recherche* d'engager des évaluations complémentaires.

Le *turn-over* des visiteurs est de plus en plus important. Pour un délégué régional et plus encore un responsable de secteur, le suivi des équipes devient une véritable activité : obtenir les coordonnées auprès des services RH lors de l'arrivée d'un nouveau personnel, réaliser un suivi personnalisé et former les recrues, etc.
Un accès plus direct aux données de personnel est nécessaire.

Responsabilités

Les **équipes du service développement** auront notamment à produire puis à fournir les éléments applicatifs permettant :

- l'enregistrement d'informations en provenance des visiteurs
- la gestion des frais de déplacement

Les **équipes du service Réseau et système** fourniront les équipements et configuration réseau, ainsi que les ressources serveur nécessaires à héberger les applications mises à disposition de la flotte visite.

Informations complémentaires sur le paramétrage obligatoire des agences lyonnaises

Agence	*GSB-LYON-C*	*GSB-LYON-F*	*GSB-LYON-D*
Responsables techniques			
vlan LAN1	201	202	204
vlan LAN2	203	207	208
vlan DMZ	1001	1002	1003
vlan Ext.(internet)	298	298	298
Réseau IP LAN1	192.168.224.0	192.168.224.16	192.168.224.48
Masque CIDR LAN1	/28	/28	/28
Réseau IP LAN2	192.168.224.32	192.168.224.96	192.168.224.112
Masque CIDR LAN2	/28	/28	/28
Réseau DMZ	10.69.1.0	10.69.2.0	10.69.3.0
Masque CIDR DMZ	/24	/24	/24
DNS	GSB-LYON-C.cool	GSB-LYON-F.cool	GSB-LYON-D.cool
DOMAINE AD	GSB-LYON-C.cool	GSB-LYON-F.cool	GSB-LYON-D.cool
NB d'@IP dyn max.	4	4	4
PLAGE DHCP	192.168.224.[5-8]	192.168.224.[21-24]	192.168.224.[53-56]
Adr. IP IPFIRE (LAN)	192.168.224.13	192.168.224.29	192.168.224.61
Adr. IP IPFIRE (DMZ)	10.69.1.254	10.69.2.254	10.69.3.254
Adr. IP IPFIRE (WAN)	100.64.1.101	100.64.1.102	100.64.1.103
Adr. IP srv 2K8R2E	192.168.224.1	192.168.224.17	192.168.224.49
Mot de passe de l'administrateur du domaine	P@ssw0rdadmin1	P@ssw0rdadmin2	P@ssw0rdadmin3

L'adresse IP publique d'IPFIRE sera distribuée dynamiquement par un FAI via le réseau **RVLAN298**.

Remarques : Les stations clientes Windows des agences auront comme mot de passe pour l'administrateur locale **P@ssw0rdGSB**. Les serveurs/clients linux auront comme mot de passe pour root **P@ssw0rdGSB**. Pour le compte admin (pas root) d'IPFIRE : vous prendrez comme mot de passe : **P@ssw0rdIPF**

Informations complémentaires sur le paramétrage obligatoire des agences toulousaines

Agence	*GSB-TOUL-C*	*GSB-TOUL-F*	*GSB-TOUL-D*
Responsables techniques			
vlan LAN1	205	206	210
vlan LAN2	209	214	212
vlan DMZ	1004	1005	1006
vlan Ext.(internet)	298	298	298
Réseau IP LAN1	192.168.224.64	192.168.224.80	192.168.224.144
Masque CIDR LAN1	/28	/28	/28
Réseau IP LAN2	192.168.224.128	192.168.224.208	192.168.224.176
Masque CIDR LAN2	/28	/28	/28
Réseau DMZ	10.31.1.0	10.31.2.0	10.31.3.0
Masque CIDR DMZ	/24	/24	/24
DNS	GSB-TOUL-C.cool	GSB-TOUL-F.cool	GSB-TOUL-D.cool
DOMAINE AD	GSB-TOUL-C.cool	GSB-TOUL-F.cool	GSB-TOUL-D.cool
NB d'@IP dyn max.	4	4	4
PLAGE DHCP	192.168.224.[69-72]	192.168.224.[85-88]	192.168.224.[149-152]
Adr. IP IPFIRE (LAN)	192.168.224.77	192.168.224.93	192.168.224.157
Adr. IP IPFIRE (DMZ)	10.31.1.254	10.31.2.254	10.31.3.254
Adr. IP IPFIRE (WAN)	100.64.1.104	100.64.1.105	100.64.1.106
Adr. IP srv 2K8R2E	192.168.224.65	192.168.224.81	192.168.224.145
Mot de passe de l'administrateur du domaine	P@ssw0rdadmin4	P@ssw0rdadmin5	P@ssw0rdadmin6

L'adresse IP publique d'IPFIRE sera distribuée dynamiquement par un FAI via le réseau **RVLAN298**.

Remarques : Les stations clientes Windows des agences auront comme mot de passe pour l'administrateur locale **P@ssw0rdGSB**. Les serveurs/clients linux auront comme mot de passe pour root **P@ssw0rdGSB**. Pour le compte admin (pas root) d'IPFIRE : vous prendrez comme mot de passe : **P@ssw0rdIPF**

Informations complémentaires sur le paramétrage obligatoire des agences lilloises

Agence	*GSB-LILL-C*	*GSB-LILL-F*	*GSB-LILL-D*
Responsables techniques			
vlan LAN1	211	215	217
vlan LAN2	213	216	218
vlan DMZ	1007	1008	1009
vlan Ext.(internet)	298	298	298
Réseau IP LAN1	192.168.224.160	192.168.224.224	192.168.225.0
Masque CIDR LAN1	/28	/28	/28
Réseau IP LAN2	192.168.224.192	192.168.224.240	192.168.225.16
Masque CIDR LAN2	/28	/28	/28
Réseau DMZ	10.59.1.0	10.59.2.0	10.59.3.0
Masque CIDR DMZ	/24	/24	/24
DNS	GSB-LILL-C.cool	GSB-LILL-F.cool	GSB-LILL-D.cool
DOMAINE AD	GSB-LILL-C.cool	GSB-LILL-F.cool	GSB-LILL-D.cool
NB d'@IP dyn max.	4	4	4
PLAGE DHCP	192.168.224.[165-168]	192.168.224.[229-232]	192.168.225.[5-8]
Adr. IP IPFIRE (LAN)	192.168.224.173	192.168.224.237	192.168.225.13
Adr. IP IPFIRE (DMZ)	10.59.1.254	10.59.2.254	10.59.3.254
Adr. IP IPFIRE (WAN)	100.64.1.107	100.64.1.108	100.64.1.109
Adr. IP srv 2K8R2E	192.168.224.161	192.168.224.225	192.168.225.1
Mot de passe de l'administrateur du domaine	P@ssw0rdadmin7	P@ssw0rdadmin8	P@ssw0rdadmin9

L'adresse IP publique d'IPFIRE sera distribuée dynamiquement par un « FAI » via le réseau **RVLAN298**.

Remarques : Les stations clientes Windows des agences auront comme mot de passe pour l'administrateur locale **P@ssw0rdGSB**. Les serveurs/clients linux auront comme mot de passe pour root **P@ssw0rdGSB**. Pour le compte admin (pas root) d'IPFIRE : vous prendrez comme mot de passe : **P@ssw0rdIPF**

Compte rendu de la direction technique sur l'installation des services DNS, Active Directory et DHCP

Suite à l'entretien avec le directeur technique, il est demandé aux technicien régionaux, situés à Lyon, Lille et Toulouse de mettre en place un serveur multiservices proposant un service Active Directory, un service DNS et un service DHCP.
Différentes informations se trouvent en annexes (voir sur les pages précédentes les documents intitulés « Informations complémentaires sur le paramétrage obligatoire des agences *lilloises/toulousaines/lyonnaises* ».

Des informations complémentaires sont nécessaires, vous les trouverez dans les prochaines lignes, si vous estimez qu'il vous manque une information bloquante dans votre installation, vous avez toujours la possibilité d'essayer de contacter votre directeur technique parisien actuellement en convalescence (sur son téléphone portable ;-) votre téléphone sera autorisé en séance de PPE uniquement pour contacter votre responsable technique et uniquement à titre professionnel.

Pour ce qui concerne l'Active Directory et le DNS : Chaque agence doit être vue comme un nouveau domaine dans une nouvelle forêt, la direction a choisi cette solution de manière à rendre les agences autonomes donc sans hiérarchie autant au niveau de l'Active Directory que du DNS. Pour le niveau fonctionnel, les serveurs de ces domaines seront au minimum des serveurs 2008 R2, il n'est donc pas nécessaire de choisir un niveau inférieur.

En cas de restauration de services d'annuaire dans une des agences du groupe GSB, nous demandons à nos techniciens de saisir le même mot de passe : **P@ssw0rdrestauration** de manière à unifier la procédure de restauration de ce service.

Pour ce qui concerne le DHCP : Le bail ne devra pas dépasser 1 jour car il faut libérer assez rapidement les adresses IP de la plage restreinte pour chaque agence à 4 adresses IP. L'étendue sera nommée EtendueLAN1 dans toutes les agences. Les agences ne gèreront pas pour l'instant l'adressage IPv6.

Mission 1 pour les équipes du service Réseau et système

Les objectifs du groupe de se rapprocher du terrain ont provoqué l'implantation de l'organisation dans trois grandes villes sur le territoire français : Lyon, Toulouse et Lille.

Cette implantation dans ces trois villes a provoqué la création de plusieurs agences. La spécificité des activités du groupe a obligé la direction à créer des agences spécialisées dans l'un des domaines suivants : commercial (pour la partie vente auprès des prescripteurs), formation (pour la partie conseilactualisation des produits pharmaceutique du groupe auprès des prescripteurs) et direction (pour la partie management et décisionnelle).

L'objectif des dirigeants était d'implanter une agence de chaque spécialité dans chaque ville de manière à couvrir via ces 9 agences une grande partie du territoire français.

De manière à augmenter la proximité géographique des agences d'une même ville donc les coûts, le groupe GSB avait axé sa recherche d'acquisition immobilière sur des locaux disposant de plusieurs bureaux tout en gardant l'aspect autonome de chaque agence. Cette notion est très importante pour la direction surtout d'un point de vue indépendance dans le fonctionnement d'une agence.

Les partenaires immobiliers ont retenu et réalisé trois transactions répondant aux exigences de la direction de GSB. Pour la région lyonnaise, les locaux des trois agences se situeront dans le centre d'affaires Lyon la Part Dieu, cet immeuble est situé à proximité de la gare SNCF, les trois agences se trouveront à trois étages différents (1er pour l'agence commerciale, 2ème pour la formation et 3ème pour la direction). Pour Toulouse, les agences ont pu être regroupées dans le centre d'affaires Ixion situé à 4 minutes du centre-ville et à 10 minutes de l'aéroport. Les trois agences toulousaines seront également sur des étages différents (7er pour l'agence commerciale, 8ème pour la formation et 9ème pour la direction).

Pour la dernière ville, la demande immobilière pour des locaux professionnels a été plus longue mais une solution similaire aux deux autres villes a été trouvée au centre d'affaires I.B.S. (Integral Business Services) situé sur le grand boulevard, axe majeur de la métropole lilloise, cette zone géographique se situe à 7 minutes des deux gares lilloises et se trouve desservie par le tramway.

Vous faites partie des équipes du service Réseau et Système, vous travaillerez en binôme et serez responsable d'une de ces nouvelles agences. Vos missions s'effectueront en majorité au sein de votre agence mais vous pourrez être amené à aider, à distance ou surplace, vos collègues d'autres agences ou du siège social.

Votre direction technique a décidé des solutions informatiques à mettre en place dans ses agences. Largement inspiré de l'existant au siège social parisien, la partie authentification des comptes utilisateurs se fera à l'aide d'un contrôleur de domaine Windows 2008 R2 entreprise, ce même serveur proposera les services réseaux DNS et DHCP et donc Active Directory. Pour la partie Pare-feu, les responsables ont testé un grand nombre de solution, matérielle comme logicielle, libre et commercial. La solution retenue mais peut-être pas définitive sera IPFIRE (base Linux From Scratch en 64 bits), solution libre mais à priori robuste. Cette solution devra permettre de créer une liste noire (donc non accessible) de sites web ainsi que la possibilité de gérer une DMZ.

Suite à un entretien avec votre responsable technique du siège, vous prendrez connaissance de l'adressage IP à utiliser pour les parties DMZ et LAN (lire les tableaux des pages suivantes : Informations complémentaires sur le paramétrage obligatoire des agences).

Votre objectif dans un premier temps sera de mettre en place une solution minimaliste composée d'une station Windows 7 Pro, d'un serveur 2008 R2 entreprise et d'un pare-feu utilisant la solution IPFIRE. Il faudra que la station Windows 7 membre du domaine du serveur 2008R2E fasse son authentification Windows sur ce dernier et que ces deux équipements puissent accéder à Internet sans restriction à l'aide de l'IPFIRE.

A la fin de votre mission, vous devrez réaliser différentes documentations dont voici la liste :

- Procédure d'installation et de paramétrage des services DNS / DHCP et Active Directory - Procédure d'installation d'IPFIRE
- Schéma format visio du réseau de l'agence indiquant les vlans, les adresses IP/MAC, le nommage des équipements. Ce schéma sera tenu à jour au fur et à mesure de vos installations et /ou modifications (tout au long de l'année).

ATTENTION, les mots de passe diffusés par votre responsable parisien devront être respectés de manière à ce que ce dernier ou un de vos collègues puisse accéder à vos équipements en cas d'absences de votre part (congé, maladie, démission, licenciement, formation, …)

Remarque : les MV que vous créerez n'utiliseront qu'un seul socket virtuel et un seul noyau par socket.

Mission 2 Filtrage de contenu Web et prise en main à distance

Votre mission consiste, que vous l'acceptiez ou non ;-) à mettre en place des solutions pour que les directives des notes de services du 25/09/2013 puisse être appliqué dans votre agence.
Remarque : L'agence du domaine GSB-LILLE-F.cool a déjà réalisé le travail, malheureusement les techniciens en responsabilité ont du partir au siège social pour une intervention et n'ont pas pu rédiger de procédure pour vous aider.

De votre côté, la direction technique vous demande de garder une trace numérique de vos paramétrages et cela de manière professionnelle (sous forme de procédure utilisant un maximum d'impression d'écran mais pas seulement), c'est-à-dire réutilisable par un autre technicien.

Mission 2 Documents : Notes de services et Charte informatique de l’entreprise

Voir pages suivantes

NOTE DE SERVICE DU 23/03/2015

DESTINATAIRES : L'ensemble du personnel de l'entreprise GSB (au siège et en agence)
OBJET : Mise en place d'une solution informatique restrictive face à l'utilisation Internet

Chères collaboratrices, chers collaborateurs,

Suite à une recrudescence d'**utilisations abusives de la connexion Internet**, la direction se voit dans l'obligation de restreindre l'utilisation Internet, essentiellement l'utilisation à but non professionnelle.

La Direction rappelle également que l'ensemble du personnel a signé, mi-septembre 2013, une charte Informatique dans laquelle **chaque employé s'est engagé à respecter le contenu de cette charte**, cette dernière rappelle également les risques encourus par son non-respect.

La Direction a demandé, de manière urgente, à son directeur technique, monsieur PERRIN, la mise en place **d'un filtrage de contenu** sous forme d'une liste noire (black list) ainsi qu'un suivi des logs (fichiers contenant l'historique des différentes utilisations faites de l'outil informatique).

Si certains sites se retrouvent bloqués par cette solution, nous invitons le collaborateur concerné à écrire à son technicien de proximité pour lui indiquer le site bloqué ainsi que l'intérêt professionnel que ce dernier peut lui apporter. Après vérification et autorisation, le service informatique s'engage à **débloquer le site concerné sous 72h ouvrables**.

La Direction déplore de devoir en arriver à de telles actions mais **n'hésitera pas à appliquer les sanctions spécifiées** dans la charte Internet si certains de ses collaborateurs ne lui en laissent pas le choix.

Cordialement.

Fait à PARIS le 23 Mars 2015

Pascal MOIRE
Directeur Général de GSB

NOTE DE SERVICE DU 23/03/2015

DESTINATAIRES : Les techniciens informatiques d'agence
OBJET : Mise en place d'une solution informatique restrictive face à l'utilisation Internet

Chers collaborateurs,

Suite à la note de service du 23 Mars 2015 écrite par la Direction générale à destination de tous les employés de la société GSB. Je demande à tous les techniciens d'agence de mettre en place les éléments suivants et au plus vite.

Il faudrait mettre en place sur IPFIRE la black list utilisée par l'université de Toulouse (la direction technique vous la mise à disposition sur le partage traditionnelle sous le nom : blacklists.tar). Il faudra activer les listes suivantes : drogue / malware / proxy / strong-redirector / warez / adult / drugs / gambling / phishing / social networks / aggressive / dangerous materials / filehosting / games / marketing ware / porn / radio / sect / tricheur / agressif / hacking / mixed-adult / sexual-education / violence.

Ces blocages de contenu renverront vers une page web indiquant en français la situation de blocage.
Il faudrait également bloquer le site www.lequipe.fr ainsi que celui de facebook. La station PAEXX7PRO64-01, station du technicien/administrateur ne sera pas concernée par ce filtrage de contenu sauf peut être pour facebook (à voir en dernier ressort : pas d'urgence)

Nous souhaiterions une mise en place de proxy sans intervention sur les équipements terminaux.

Cordialement.

Fait à PARIS le 25 Mars 2015

Laurent PERRIN
Directeur technique GSB du siège à PARIS

NOTE DE SERVICE DU 23/03/2015

DESTINATAIRES : Les techniciens informatiques d'agence
OBJET : Prise en main à distance de l'administration d'une agence

Chers collaborateurs,

Suite à certaines absences de techniciens d'agence pour diverses raisons (maladies, formations, R.T.T. (Réduction du Temps de Travail) et face à la nécessité d'avoir une maintenance plus réactive, je vous demande de mettre en place certaines prises en main à distance. L'objectif est de pouvoir confier certaines tâches d'administration réseau à un de vos collègues d'une autre agence en cas d'absence de votre part. Cela aura également l'objectif de créer une entre-aide entre les techniciens d'agence.

Mon souhait n'est pas de diminuer les effectifs mais simplement d'avoir des agences maintenues en fonctionnement (dans notre domaine : celui du Réseau et Système) même sans spécialistes sur place.

L'administrateur distant utilisera le compte de l'administrateur de l'agence visée. Depuis cette semaine les agences bénéficient d'une adresse IP publique FIXE. J'ai demandé cela à notre FAI. Cette modification devrait être efficace depuis le lundi 23/09/2013. Vous trouverez les adresses IP publiques des agences dans le document modifié nommé « Informations complémentaires sur le paramétrage obligatoire des agences … »

Pour la partie prise en main à distance, vous devrez mettre en place les actions suivantes :

- Lorsqu'une requête en SSH arrivera sur l'interface extérieure de votre IPFIRE, elle devra être transférée au serveur Debian
- Lorsqu'une requête lancée par le bureau à distance Windows arrivera sur l'interface extérieure de votre IPFIRE, elle devra être transférée à la station locale PAEXX-7PRO64-01.
- Lorsqu'une requête lancée par le réseau 100.64.1.100/28 (uniquement celui-ci) pour une prise en main à distance sur le port 3390 (TCP) arrivera sur l'interface extérieure de votre IPFIRE, elle devra être transférée au serveur PAEXX-2K8R2E-01

Nous profiterons de ces paramétrages pour rajouter celle qui permettra de rendre votre serveur Web disponible depuis l'extérieur sur le port http (cela permettra d'arriver sur la page d'accueil du site par défaut).

Vous rédigerez les procédures liées à ces différents travaux de manière à garder une trace de votre travail.

Fait à PARIS le 25 Mars 2015

Laurent PERRIN
Directeur technique GSB du siège à PARIS

Charte informatique de l'entreprise

D'une manière générale, l'utilisateur doit s'imposer le respect des lois et, notamment, celles relatives aux publications à caractère injurieux, raciste, pornographique, diffamatoire, sur le harcèlement sexuel/moral.

1) Sécuriser l'accès au compte

Le contrôle d'accès logique permet d'identifier toute personne utilisant un ordinateur.

Cette identification permet, à chaque connexion, l'attribution de droits et privilèges propres à chaque utilisateur sur les ressources du système dont il a besoin pour son activité.

Une identification (login + mot de passe) unique est confiée à chaque utilisateur. Ce dernier est personnellement responsable de l'utilisation qui peut en être faite, et ne doit en aucun cas la communiquer.

Chaque mot de passe doit obligatoirement être modifié selon la fréquence suivante : 1 an. Un mot de passe doit, pour être efficace, comporter 8 caractères alphanumériques. Il ne doit pas être, notamment, identique au login, même en inversant les caractères, comporter le nom et/ou prénom de l'utilisateur ou de membres de sa famille, le numéro de téléphone, la marque de la voiture ou toute référence à quelque chose appartenant à l'utilisateur, être un mot ou une liste de mots du dictionnaire ou un nom propre, nom de lieu, être écrit sur un document et être communiqué à un tiers.

2) Courrier électronique

Les éléments de fonctionnement de la messagerie à considérer sont les suivants.

Un message envoyé par Internet peut potentiellement être intercepté, même illégalement, et lu par n'importe qui.

En conséquence, aucune information stratégique ne doit circuler de cette manière, sauf à la crypter.

Il est interdit d'utiliser des services d'un site web spécialisé dans la messagerie.
Lors du départ d'un collaborateur, il doit être indiqué au responsable de l'administration du système ce qu'il sera fait des fichiers et courriers électroniques de l'utilisateur.

Les messages électroniques sont conservés sur le serveur de messagerie pendant une période de 365 jours et il existe des copies de sauvegarde pendant une période de 730 jours.

Ces copies de sauvegarde conservent tous les messages au moment où ils passent sur le serveur de messagerie, même s'ils ont été supprimés ensuite par leur destinataire.

2.1 Utilisation privée de la messagerie

L'utilisation du courrier électronique à des fins personnelles est autorisée dans des proportions raisonnables et à la condition de ne pas affecter le trafic normal des messages professionnels. À ce titre, les salariés devront identifier leurs messages et fichiers personnels de façon à ne pas les confondre avec les messages reçus à titre professionnel : qualification par l'objet, création d'un répertoire spécifique dédié au contenu privé.

2.2 Contrôle de l'usage

Dans l'hypothèse la plus courante, le contrôle éventuellement mis en œuvre porte sur :
- le nombre des messages échangés par utilisateur ;
- la taille des messages échangés ; - le format des pièces jointes.

3) Utilisation d'Internet

Chaque utilisateur doit prendre conscience qu'il est dangereux pour l'entreprise :
- de communiquer à des tiers des informations techniques concernant son matériel ;
- de connecter un micro à Internet via un modem (sauf autorisation spécifique) ;
- de diffuser des informations sur l'entreprise via des sites Internet ; - de participer à des forums (même professionnels) ;
- de participer à des conversations en ligne (« chat »).

3.1 Utilisation d'Internet à des fins privées

L'utilisation d'Internet à des fins privées est tolérée dans des limites raisonnables et à condition que la navigation n'entrave pas l'accès professionnel.

3.2 Contrôles de l'usage

Dans l'hypothèse la plus courante, les contrôles portent sur :
- les durées des connexions par utilisateur ; - les sites les plus visités de façon globale.

La politique et les modalités des contrôles font l'objet de discussions avec les représentants du personnel.

4) Pare-feu

Le (les) pare-feu vérifie(nt) tout le trafic sortant de l'entreprise, aussi bien local que distant. Il vérifie également le trafic entrant constitué de la messagerie électronique, de l'échange de fichiers ainsi que de la navigation sur Internet.

Il détient toutes les traces de l'activité qui transite par lui s'agissant :

- de la navigation sur Internet : sites visités, heures des visites, éléments téléchargés et leur nature (textes, images, vidéos ou logiciels) ;
- des messages envoyés et reçus : expéditeur, destinataire(s), objet, nature de la pièce jointe (et éventuellement texte du message).

Il filtre les URL des sites non autorisés par le principe de la liste noire. Les catégories des sites visés sont les sites diffusant des données de nature pornographique, pédophile, raciste ou incitant à la haine raciale, révisionniste ou contenant des données jugées comme offensantes.

5) Sauvegardes

La mise en œuvre du système de sécurité comporte des dispositifs de sauvegarde des informations en cas de défaillance.

Ceci implique, entre autres, que la suppression par un utilisateur d'un fichier de son disque dur n'est pas absolue et qu'il en reste une copie : - sur le dispositif de sauvegarde;
- sur le serveur ;
- sur le proxy ;
- sur le firewall (pare-feu) ;
- chez le fournisseur d'accès.

Fait à PARIS le 02 Septembre 2013

Pascal MOIRE
Directeur Général de GSB

Lettre de décharge liée à la charte informatique de l'entreprise

Madame, Monsieur,

Nous vous rappelons qu'en tant que salarié de la société GSB, vous êtes tenu de respecter les règles en vigueur dans l'entreprise.

Nous vous invitons à vous conformer aux bonnes pratiques d'utilisation de la messagerie électronique , d'Internet et des outils informatiques exposées dans la charte informatique.

Par cette présente lettre, vous déclarez avoir pris connaissance de cette Charte informatique et vous vous engagez à respecter les règles qui y sont notifiées.

Société : **GSB**

Nom du salarié :

Date :

Signature :

Nb : Veuillez retourner cette note signée et datée au service informatique de votre agence de rattachement.

Mission 3 Déploiement de masse de Windows 7 dans les agences

Cette mission consiste à mettre en place le service **Windows Deployment Services** sur un nouveau serveur **PAEXX-2K8R2E-02**, ce serveur sera membre du domaine de l'agence concernée. Une station **PAEXX-7PRO64-03** sera utilisée comme modèle (master).

Ce système de déploiement devra être automatisé via un fichier réponse permettant une installation dite « zéro touch » (ou presque). La direction technique de GSB attend donc un minimum d'interventions humaines sur les stations bénéficiant de ce type de déploiement. Le déploiement se fera sur au moins deux stations vierges de toutes installations en simultanée (multi-diffusion), ces stations se nommeront au final **PAEXX-7PRO64-04** et **PAEXX-7PRO64-05**

Lorsque la solution « zéro touch » sera opérationnelle, la direction souhaiterait pouvoir déployer **Windows 7 32 bits** sur d'anciennes stations de travail (**type Maxdata**) achetées d'occasion à un organisme nommé M2L.

Mission 3 Ressources

Les ressources mis à votre disposition pour cette mission sont :

- Document pdf nommé « Installation et configuration de WDS tuto de A à Z »
- Document pdf nommé « Analyse du fonctionnement de WDS tuto de A à Z »
- Document pdf nommé « Deploiement automatise de Seven via le WAIK tuto de A à Z »
- Fichier au format iso nommé « fr_windows_7_professional_with_sp1_x64_dvd_u_678724 »
- Fichier au format iso nommé « fr_windows_7_professional_with_sp1_x86_dvd_u_677092 »
- Fichier au format iso nommé « fr_windows_automated_installation_kit_for_windows_7_and_windows_server_2008_r2_sp1_x86_x64_ia64_dvd_619627(1) »

Les documentations à votre disposition ne sont pas prévues pour le déploiement dans les agences GSB, il faudra donc adapter ces ressources et produire vos propres procédures d'installation, de configuration et d'utilisation du service WDS.

La direction technique a demandé aux techniciens de proximité d'augmenter la plage DHCP, elle comptera deux adresses IP supplémentaires. Le début de la plage DHCP ne changera pas.