Nom : Fresneau

Prénom : Yohan

Classe : 801 – BTS SIO

Date de stage

Du 22/05/2017 Au 30/06/2017

Maitre de Stage :	*Tuteur de Stage :*
Mr Olivier Murzeau	**Mr David Balny**
Responsable Exploitation	**Professeur Economie Gestion (Option informatique)**

Sommaire

1. Introduction 3
2. Présentation du candidat 3
3. Présentation de l'entreprise 3
   a. Situation géographique 3
   b. Historique 5
   c. Activité 6
   d. Evolution économique 6
   e. Aspects Juridiques 6
   f. Organigramme du service informatique 7
   g. Activité du service informatique 7
4. Schémas réseaux logique du service informatique George Sand 7
5. Problématique 7
6. Pourquoi sécuriser une connexion 7
7. Quels sont les moyens de sécuriser une connexion 8
8. Pourquoi un VPN 9
9. Qu'est-ce qu'un VPN 9
10. Encapsulation et Protocole utilisé par le VPN 9
11. Quel VPN choisir 11
12. Différents moyens d'authentification VPN 11
13. Quels sont les deux modèles de connexion VPN 13
14. Quelle solution a été choisie par l'entreprise 15
15. Mise en place d'un VPN 16
16. Conclusion 16
17. Remerciements 17
18. Annexes 17
   a. Schémas Réseaux 17
   b. Procédure d'installation VPN 19

1. Introduction

J'ai effectué un stage de 6 semaines au service informatique du centre hospitalier George Sand, qui se situe 77, rue Louis Mallet à Bourges, dans le département du Cher. J'ai choisi ce stage pour connaitre la façon dont on peut mettre en relation la médecine et l'informatique.

2. Présentation du candidat

Je m'appelle Yohan Fresneau, je suis étudiant au lycée Paul Louis Courier à Tours. Je suis en classe de 1ère année de BTS SIO (Service informatique aux organisations) Option SISR (Solutions d'infrastructures, systèmes et réseaux).

3. Présentation de l'entreprise

a. Situation géographique

L'hôpital George Sand a 3 gros sites : Bourges, Dun sur Auron et Chezal-Benoît ainsi que plusieurs annexes.

Le site de Bourges se situe : 77, rue Louis Mallet - 18024 Bourges :

Le site de Dun sur Auron se situe : 8, rue de l'Ermitage – 18130 Dun sur Auron :

Le site de Chezal-Benoît se situe Rue de l'église – 18160 Chezal-Benoît :

b. Historique

Historique Bourges :

C'est en 1865 que Le département fit donc l'acquisition d'une propriété Route de Marmagne, au lieu-dit les « Beaux Regards » car L'inspecteur général estima que « les aliénés » avaient besoin d'air et devaient s'occuper en travaillant.

Il exposa la nécessité de trouver un terrain pour la construction d'un asile.

A cette époque les malades mentaux se trouvaient à l'hospice de St Fulgent, mêlés aux autres pensionnaires.

En 1874 fut édifié le premier pavillon destiné à recevoir les malades tranquilles (123 hommes).

Entre 1885 et 1895, de nombreuses constructions prirent forme comme le pavillon destiné aux « agités », la chapelle ou encore deux pavillons pour les femmes gâteuses et épileptiques.

En 1975, l'hôpital psychiatrique devient centre hospitalier spécialisé.

Le département du Cher a pour particularité, en matière de psychiatrie, de disposer de trois Centres Hospitaliers :

- Le Centre Hospitalier de Beauregard à Bourges
- Le Centre Hospitalier de Chezal-Benoît
- Le Centre Hospitalier de Dun-sur-Auron

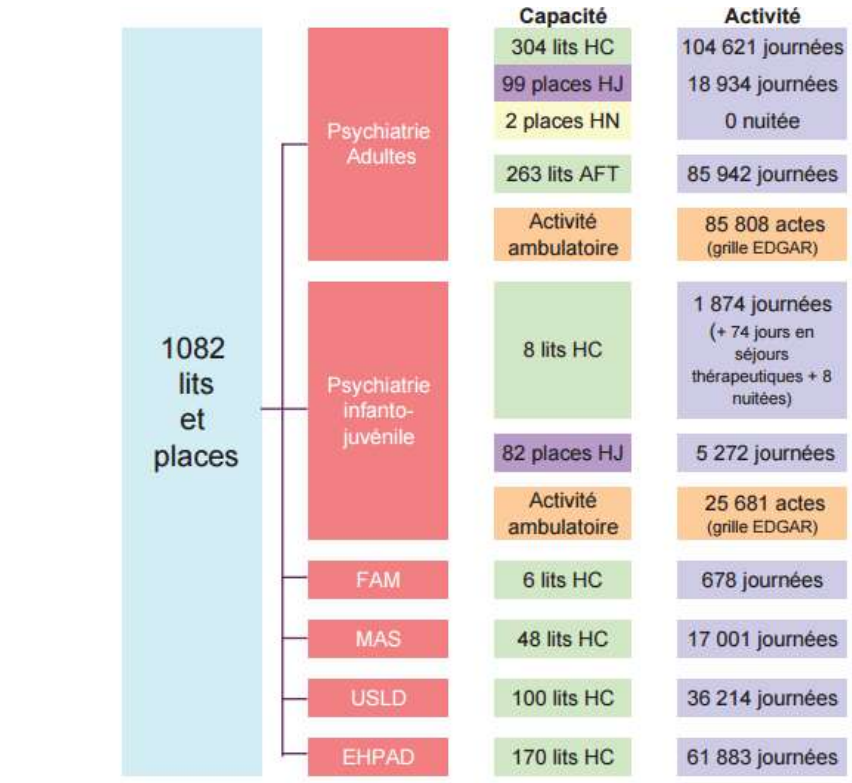
Le SIH, créé le 1er janvier 1998, a engagé un certain nombre d'actions, dans un premier temps dans trois domaines : la formation, l'informatique et l'accueil d'urgence par la création d'un Centre d'Accueil et d'Orientation Départemental (CAOD), qui a ouvert en janvier 2002 à Bourges.

Un courrier du 13/03/2000 a été adressé aux trois Présidents de Conseil d'Administration par le Directeur de l'Agence Régionale de l'Hospitalisation du Centre. Il demande aux trois établissements de créer un établissement unique intercommunal par regroupement des trois CHS existants.

L'objectif étant d'aboutir à la mise en place du nouvel établissement en 2003. Le Centre Hospitalier George Sand a vu juridiquement le jour le 1er janvier 2003, date à laquelle la suppression des trois établissements ainsi que celle du SIH ont été prononcées.

c. Activité

L'hôpital George Sand est un hôpital de santé mental pour tout âge, qui va des infanto-juvénile en passant par les adolescents jusqu'aux adultes puis les personnes âgées. L'hôpital George Sand accueille également des personnes à mobilité réduite. Il dispose de 1082 lits.



FAM : Foyer d'Accueil Médicalisé
MAS : Maison d'Accueil Spécialisée
USLD : Unité de Soins de Longue Durée
EHPAD : Établissement d'Hébergement pour Personnes Âgées Dépendantes

HC : hospitalisation complète
HJ : hôpital de jour
HN : hospitalisation de nuit
AFT : Accueil Familial Thérapeutique
EDGAR : Entretien Démarche Groupe Accompagnement Réunion

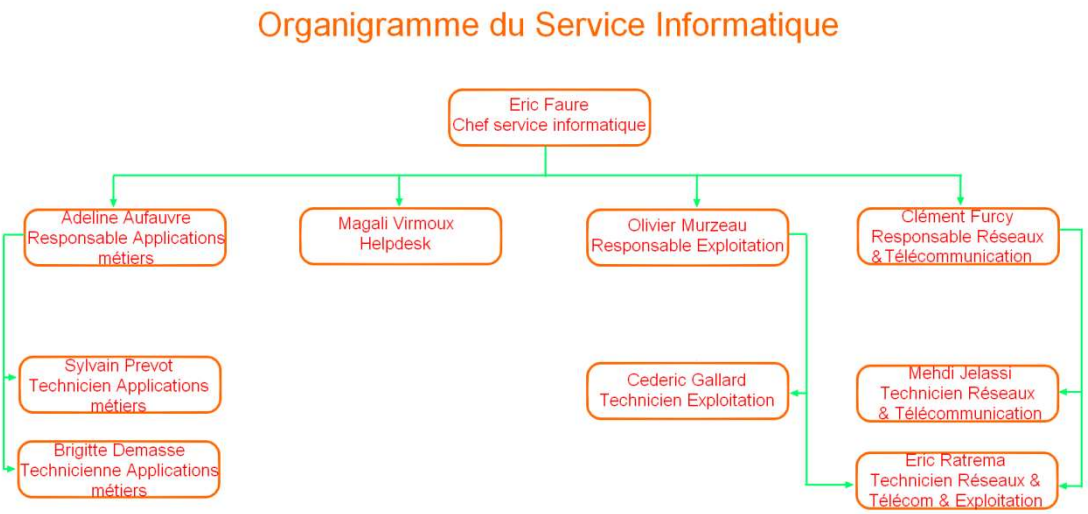
d. Evolution économique

L'hôpital George Sand est un établissement public qui n'a donc pas de chiffre d'affaire.

e. Aspects Juridiques

L'Hôpital George Sand est un hôpital de santé mental public. Il soigne et accompagne toute personne qui a besoin de soins psychiatrique. C'est un établissement public de santé il est dirigé par un directeur Mr. Jean-Paul Servier qui préside un directoire. Le conseil de surveillance délibère ou donne son avis sur un domaine d'attribution.

f. Organigramme du service informatique



g. Activité du service informatique

Le service informatique s'occupe : des serveurs d'applications, des serveurs de partage de fichiers, du réseau, des applications médicales et métier. Il forme le personnel pour les nouveaux outils et logiciels mis en place. Il s'occupe du parc informatique, dépanne les ordinateurs si nécessaires et dans la mesure du possible.

4. Schémas réseaux logique du service informatique George Sand

Schémas Réseaux en annexes

5. Problématique

Comment les médecins d'astreinte peuvent se connecter sur leurs bureaux Citrix pour avoir accès à cariatide, depuis chez eux, tout en ayant une connexion sécurisée et sans avoir besoin de faire des modifications sur les postes ou même sur leur réseau personnel (Domicile).

6. Pourquoi sécuriser une connexion

Pour une entreprise sécuriser une connexion, ou transite des données sensibles est primordiale. Les données pour une entreprise sont très importantes, elle dépende de leur

survie et de leurs images, qui peuvent avoir de grosses répercutions, comme la perte d'argent ou la notoriété. Il n'y a pas que les données qui doivent être sécurisées, mais aussi la liaison entre le client (Médecin d'astreinte) et le serveur (Serveurs Citrix CHGS), pour éviter qu'un pirate informatique se positionne entre le client et le serveur, pour faire du « man in the middle » qui a pour but d'être entre le client et serveur afin d'intercepter les communications et ou données qui sont échangées. Pour cela, il existe plusieurs moyens de mettre en place une connexion sécurisée. Voici les différents protocoles sécurisés qui existe selon les utilisations : (Les plus connus et les plus utiliser)

Transfert de fichier **:** FTPS (File Transfer Protocol Secure) utilise les protocoles TLS ou SSL, SFTP (SSH File Transfer Protocol) utilise le protocole SSH pour sécuriser les échanges.

Service Web **:** Https (HyperText Transfer Protocol Secure) utilise le chiffrement TLS ou SSL

Protocole de Transfert **:** TLS (Transport Layer Security), SSL (Secure Sockets Layer), SSH (Secure Shell) qui est à la fois un protocole de transfert sécurisé, mais aussi un programme informatique. Ces trois protocoles de communication sécuriser, ce sont les plus utilisés et les plus rependus.

Tous les protocoles n'existent pas forcement en version sécurisée, ce qui veut dire qu'avec un logiciel pour « sniffer » le réseau, on peut donc savoir ce que l'utilisateur fait et ce qu'il a transfère en clair, comme par exemple : une connexion à un serveur ftp non sécurisé, on voit en clair le nom d'utilisateur et le mot de passe.

Pour cela nous devons nous interroger, pour savoir quels sont les moyens qui existent, et qui permettent de sécuriser la connexion.

7. Quels sont les moyens de sécuriser une connexion

Comme vu précédemment, il existe des protocoles qui permettent, de sécuriser les communications et ou les échanges de données. Si seulement tous étaient sécurisés, cette question ne se poserait pas. Malheureusement, il y'a beaucoup de protocoles qui ne sont pas sécurisés, à cause de leurs anciennetés et ne sont plus mis à jour. Pour pallier à ceci, il existe des moyens de faire passer des informations dans des tunnels sécurisés. Les plus connu sont le SSH (Secure Shell), qui permettent d'échanger des données entre un client et un serveur, comme la connexion à un « Shell » pour le quelle SSH est le plus utilisé sous Linux et Unix, mais le protocole SSH est aussi utilisé pour le transfert de fichiers, en utilisant le protocole SFTP (SSH File Transfer Protocol). L'inconvénient du SSH, il ne permet pas de sécuriser tous les protocoles, car celui-ci contrairement au VPN, il vient se greffer sur le protocole existant créant un nouveau comme le SFTP, qui est à la base un protocole FTP avec un tunnel SSH pour le transfert de données sécurisées.

8. Pourquoi un VPN

Nous pouvons nous questionner : Pourquoi utiliser un VPN ? Qu'est-ce qu'un VPN ? Quelle est son utilité, son utilisation et ses avantages ?

9. Qu'est-ce qu'un VPN

Un VPN est un « Virtual Private Network », qui veut dire « Réseau virtuel privé » en français. Un VPN permet de créer un lien direct entre des ordinateurs distants. On peut donc relier un ordinateur distant à un réseau privé grâce à cela, on peut faire, comme s'il était situé dans le même lieu, tout en étant à un endroit différent et cela en utilisant le réseau public internet. Il permet aussi de relier deux sites entre eux, il suffit pour cela d'utiliser un serveur VPN sur chaque site, à l'inverse d'un utilisateur, qui doit juste être connecté au réseau et avoir un client VPN.

10. Encapsulation et Protocole utilisé par le VPN

Les technologies VPN utilisées pour encapsuler les données et informations, qui transitent dans le tunnel VPN les plus utiliser et les plus connus sont :

VPN SSL :

Il se nomme aussi « clientless », il ne nécessite pas d'installation logiciel client, seul un navigateur internet compatible avec l'ouverture des sessions HTTPS SSL/TLS est requiers .Un tunnel VPN SSL ne permet pas de faire circuler différents protocoles de communication comme le VPN IP Sec, Il existe des alternative, comme par exemple pour le protocole RDP, il existe (RD Web Access) qui permet d'accéder aux programmes RemoteApp et aux services Bureau à distance grâce à un navigateur web.

VPN IPsec :

L'installation d'un logiciel client est nécessaire afin d'établir un tunnel vers un serveur VPN. Un Tunnel VPN IPsec permet de faire transiter différents protocoles de communication comme que SSH, RDP, SMB, SMTP, IMAP, etc. Tous les protocoles sont compatibles avec ce genre de VPN.

PPTP :

Signifie « Point-to-point tunneling protocole » ou « protocole d'encapsulation ». Ce protocole PPTP crée un tunnel privé pour envoyer des données vers et depuis un ordinateur ou un appareil mobile. Les périphériques sont authentifiés à l'aide d'un mot de passe, donc pas de matériel supplémentaire nécessaire. PPTP ne fournit aucun cryptage de données ou aucune mesure de sécurité supplémentaire. Les connexions PPTP sont également faciles à bloquer pour les fournisseurs de services Internet. Cependant, il existe des avantages à utiliser un VPN

PPTP – c'est le protocole le plus facile à configurer et à utiliser, et il peut aussi vous offrir une performance stable et une vitesse fiable.

L2TP sur IPSec:

Signifie « Layer 2 Tunneling Protocol (L2TP) over Internet Protocol Security (IPSec) ». Ce protocole fonctionne d'une manière similaire à PPTP, mais il offre la confidentialité et l'intégrité des données supplémentaires grâce à un processus de multi-authentification. Comme PPTP, L2TP sur IP Sec peut être installé facilement sur tout appareil Apple, Windows ou Android. En raison des caractéristiques de sécurité supplémentaires qu'il contient, l'utilisation de ce protocole peut être plus lente lors du transfert d'un volume élevé d'information.

OpenVPN:

Comme son nom l'indique, OpenVPN ou PPTP est un protocole VPN open source qui utilisent « Secure Socket Layer (SSL) » pour créer une authentification pour une connexion Internet cryptée. Dans l'ensemble, le protocole OpenVPN offre l'une des meilleures combinaisons de performance et de sécurité, et il peut être utilisé pour contourner facilement les pare-feu ainsi que les restrictions des FAI.

HybridVPN:

Le VPN fait partie d'une nouvelle génération de fournisseurs de services qui offre un HybridVPN combinant à la fois une connexion VPN de niveau SSL et un proxy SmartDNS. Un proxy SmartDNS est un service optionnel qui simplifie le processus pour un utilisateur, afin de lui permettre d'accéder à des contenus géographiquement limités. Les utilisateurs bénéficient de la sécurité, de la fiabilité et de l'anonymat d'un VPN, avec l'avantage d'un Smart DNS. Vous pourrez également profiter d'une vitesse et d'une fiabilité exceptionnelle pour regarder des médias ou des vidéos ou des sites graphiques longs à télécharger.

Comparaison des différentes technologies VPN qui existe :

	PPTP	L2TP/ IPsec	OpenVPN ™
Cryptage VPN	128-bit	256 bits	160 bit 256 bits
Configuration manuelle possible	Windows Mac OS X Linux iOS Android DD-WRT	Windows Mac OS X Linux iOS Android	Windows Mac OS X Linux Android
Sécurité VPN	Encryptage de base	Le chiffrement le plus élevé. Vérifie l'intégrité des données et les encapsule deux fois.	Le chiffrement le plus élevé. Authentifie les données à l'aide de certificats numériques.
Vitesse VPN	Rapide grâce à un plus bas cryptage.	Nécessite plus de processeur pour la double encapsulation de données.	Le protocole le plus performant. Débits rapides, même sur les connexions à latence élevée et sur des grandes distances.

Stabilité	Fonctionne bien sur la plupart des hotspots Wifi, très stable.	Stable sur les appareils supportant le NAT	Plus fiable et plus stable sur les réseaux moins protégés et sur les hotspots Wi-Fi, même derrière des routeurs sans fil.
Compatibilité	Intégré dans la plupart des systèmes d'exploitation pour PC, périphériques mobiles et tablettes.	Intégré dans la plupart des systèmes d'exploitation pour PC, périphériques mobiles et tablettes.	Compatible avec la plupart des systèmes d'exploitation d'ordinateurs de bureau, mobiles Android et tablettes.
Conclusion	Le PPTP est un protocole rapide et simple d'utilisation. Il est un choix judicieux si OpenVPN n'est pas pris en charge par votre appareil.	Le L2TP/IPsec est un bon choix si OpenVPN n'est pas pris en charge par votre appareil et si la sécurité est votre priorité absolue.	OpenVPN est le protocole recommandé pour les ordinateurs de bureau équipés avec Windows, Mac OS X et Linux. La meilleure performance : rapide, sûre et fiable.

Conclusion des technologies VPN qui existe :

PPTP :

PPTP est un protocole rapide & facile à utiliser, avec un processus de configuration simple. C'est un bon choix si OpenVPN n'est pas pris en charge par votre appareil.

L2TP/IPsec :

L2TP/IPsec est un protocole intégré à la plupart des ordinateurs, téléphones et tablettes. C'est un bon choix si OpenVPN n'est pas pris en charge par votre appareil, et si la sécurité est votre priorité principale.

OpenVPN ™ :

OpenVPN est le protocole recommandé pour les ordinateurs de bureau équipés avec Windows, Mac OS X et Linux. La meilleure performance : rapide, sûre et fiable.

11. Quel VPN choisir

Le plus recommander est OpenVPN, qui a La meilleure performance, il est rapide, sûre et fiable. De plus il est gratuit, ce qui n'est pas négligeable quand on veut, installer un VPN à moindre coût pour les particuliers, ou bien même les petites entreprises ou startup.

12. Différents moyens d'authentification VPN

On peut se connecter à un serveur VPN, mais pour ne pas avoir des individus étrangers (inconnu ou pirate informatique) au réseau, il existe des moyens d'authentification :

- mot de passe (simple, pas besoin d'équipement appart, niveau de sécurité : faible)
- Certificat (moyen, besoin d'un certificat, niveau de sécurité : moyen)

- Connexion avec utilisateur LDAP (Lightweight Directory Access Protocol)(élever, besoin d'un nom de domaine et d'un active directory, niveau de sécurité : élever)

Quel est le meilleur moyen de s'authentifier ?

Chaque moyen d'authentification, à ses des avantages et ses inconvénients.

	Mot de passe	Certificat	LDAP
Niveau de Sécurité			
Difficulté de mise en place			
Flexibilité (autoriser un utilisateur ou non de se connecter)			
Coût de mise en place			
Equipement spécial			
Quel équipement	Aucun	Certificat et ou Serveur d'autorité de certification	Serveur DNS et Serveur LDAP
Avantages	-Aucun équipement spécial -Coût faible	-Permet d'être sûr de la provenance de la connexion	-Permet une gestion dynamique des autorisations et des utilisateurs -Avantages du domaine
Inconvénients	-Un mot de passe unique	-Devoir changer le certificat après expiration -Possible de vol de certificat -Coût élever d'un certificat certifier au prêt d'une autorité reconnu	-besoin de serveur LDAP et DNS -Coût des serveurs LDAP et DNS -Permet en plus d'être déjà authentifié et permet de changer de mot de passe facilement en cas de diffusion de mot de passe par erreur
Quel est le meilleur ?			
Conclusion sécurité authentification			

Conclusion : L'authentification la plus sécurisée mais aussi l'une des plus onéreuse est l'authentification LDAP.

13. Quels sont les deux modèles de connexion VPN

Un VPN Serveur peut être soit intégrer dans un équipement actif réseau comme un routeur ou firewall. Ou bien il peut être indépendant et être directement installer sur un serveur physique ou virtuel.

Relier 2 sites distants entre eux (serveur – serveur) :

Grace à un serveur VPN sur chaque site, on peut les liés pour qu'il soit possible, d'envoyer et de recevoir sans avoir besoin d'installer un client VPN sur chaque poste. Cela rend le VPN invisible pour les utilisateurs car ils n'ont pas besoin de lancer le tunnel, il ne se situe pas en local mais sur le serveur VPN qui fait office de client et serveur, normalement derrière le routeur ou DMZ(Zone démilitarisée). On peut donc faire passer n'importe quel flux et ou données, car aucun client VPN, n'a besoin d'être installé ce qui est avantageux quand on a des machines sur lesquelles on ne peut pas installer de client VPN.

Exemple :

- Téléphonie
- Machines réseaux (autres OS)
- Etc…

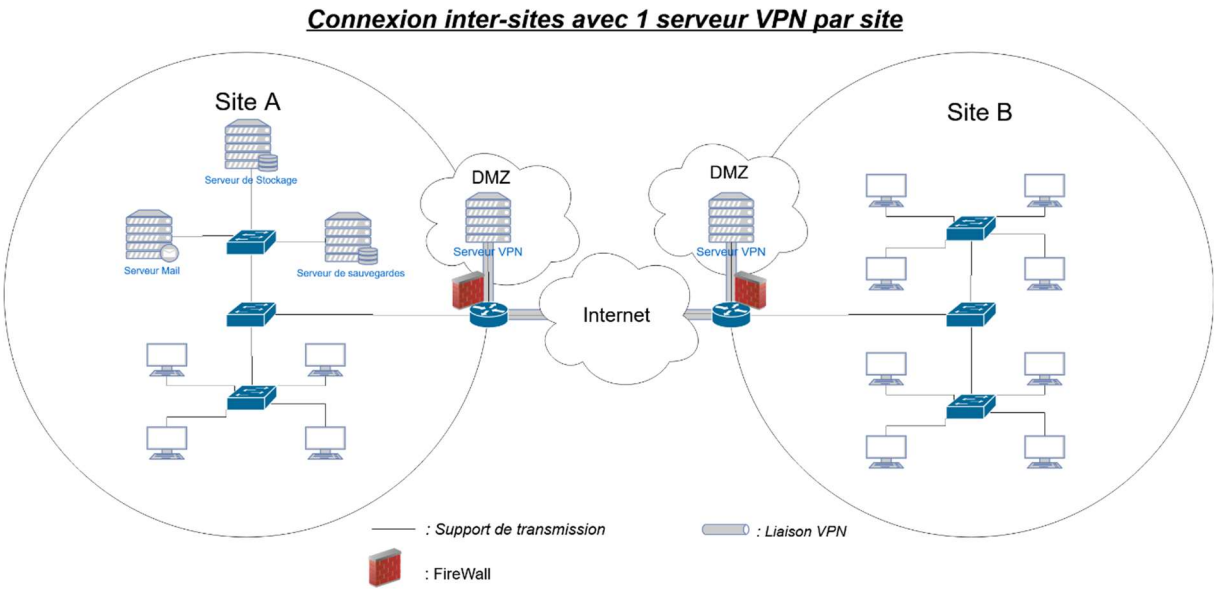
Avantage :

- Pas besoin d'avoir un client VPN par Hôte
- Permet de faire passer les flux de machines ou d'hôtes, où il est impossible d'installer un client VPN
- Pas besoin de gérer les comptes utilisateurs et les autorisations des clients VPN
- Gestion Centraliser et analyse de flux en entré et sorti du VPN
- Permet de crypter tous les informations et données échanger peut importe leur nature et protocole

Inconvénient :

- Nécessite un serveur par site, ce qui augmente le coût financier
- En cas de disfonctionnement du VPN, la liaison ne se fait plus
- On peut savoir ce qui circule entre le client et le serveur VPN dans la partie du réseau local
- Sécuriser uniquement entre les deux serveurs VPN
- Besoin de configurer les deux serveurs

Schéma réseau :



Relier 1 client au réseau grâce au VPN (client – serveur) :

On peut relier un ordinateur, grâce à un client VPN à un réseau sans que celui-ci soit directement connecté à celui-ci, pour cela il faut installer le client VPN, sur le client, ce qui est un désavantage, car chaque poste doit en être équipé et donc avoir chacun un identifiant VPN.

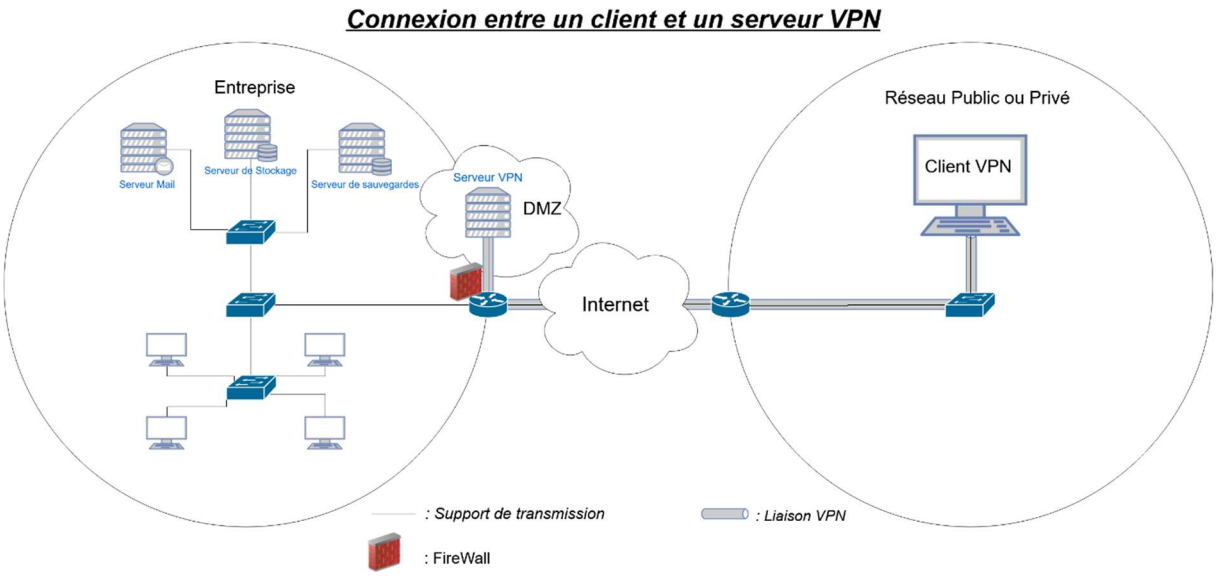
Avantage :

- Permet d'être utilisé dans n'importe quels lieux
- Permet de sécuriser l'échange sur un réseau local non sécurisé, comme les réseaux publics
- Liaison sécurisée entre le client et le serveur VPN
- Pas besoin d'avoir une configuration réseau spécial, juste besoin d'avoir accès à internet
- Control d'accès au réseau de l'entreprise, possible de désactiver l'accès d'une personne au VPN

Inconvénient :

- Nécessite un client VPN sur chaque poste
- Devoir configurer 1 à 1 les postes clients
- Visibilité du VPN
- Obliger d'activer le VPN (Si non activer au démarrage)

Schéma réseau :



Quel moyen choisir selon l'utilisation :

Chaque moyen VPN à son utilisation, si on souhaite relier plusieurs personnes, qui ne sont pas sur le même réseau local, la 2émè option est la plus adaptée.

A l'inverse si on veut relier par exemple 100 personnes qui sont sur le même réseau local, la 1ère option est la plus adaptée.

14. Quelle solution a été choisie par l'entreprise

L'entreprise a choisi d'utiliser le firewall avec une de ces fonctionnalités serveur VPN, ce qui permet de ne pas avoir de serveur VPN dédié pour cette tâche. La marque du firewall est Stormshield anciennement Netasq. Ce sont des Stormshield SN2000, ils sont au nombre de deux pour la redondance, ce sont des boitiers physiques configurés en actif/passif, ce qui leurs permet en cas de défaillance du firewall principal(actif), le firewall de secours(passif) prend le relais, ce qui permet en cas de panne, d'avoir un firewall de secours et donc une continuité de service en attendant le rétablissement fonctionnel complet du firewall principal.

On parle de firewall, mais qu'est ce qu'un firewall ?

Un firewall est un équipement réseau qui a pour but de faire respecter la politique de sécurité du réseau. En informatique, l'usage du terme « pare-feu » est une image, il évoque une porte empêchant les flammes d'Internet d'entrer chez soi et/ou de « contaminer » un réseau informatique. On peut mettre des règles d'entées et de sorties.

Pour une entreprise un firewall est important, c'est même devenu obligatoire d'en avoir un pour savoir qui a fait quoi. En cas de problèmes avec un employé ou autres, le firewall est le seul moyen qui prouve et qui permet donc de tracer les gestes et trafic des utilisateurs.

Quelle est la méthode d'authentification utiliser ?

La méthode utiliser est l'authentification LDAP. Le firewall est interfacé à l'active directory du CHGS. Chaque utilisateur autoriser à se connecter au VPN, à une adresse email et une clé partager ce qui fait l'équivalent d'un nom d'utilisateur et mot de passe. Ces utilisateurs sont dans un « OU(Unité d'organisation en français) » dédié pour le serveur VPN, ce qui permet d'affecter certains utilisateurs, pour que tous les utilisateurs du CHGS, n'ai pas l'autorisation de se connecter au VPN. Seul les utilisateurs dans OU dédier sont autoriser à se connecter au VPN. Grace à l'active directory, on peut donc avoir une gestion dynamique des utilisateurs, sans avoir besoin de passer sur chaque postes ou toutes autres moyens par le quelle l'action est fastidieuse et redondante sur chaque poste.

Quel est le modèle VPN utilisé pour la connexion ?

Le CHGS utilise le VPN, pour relier ses médecins d'astreinte au réseau du CHGS, depuis chez eux. C'est donc un modèle client-serveur, qui est donc utiliser. Un client VPN est installé sur le client léger portable, qui permet de crypter les données grâce au tunnel VPN, entre le poste et le firewall du CHGS. Cette méthode permet donc de se connecter, sur n'importe quel réseau, du moment qu'il y'a un accès internet. La connexion est possible sur les réseaux publics, qui ne sont pas sécurisés.

Quel protocole est utilisé par le serveur VPN ?

Le protocole utilisé est IPsec qui permet donc d'avoir une sécurité maximale avec, une vérification des données et une encryptions des données qui transitent, de plus la double encapsulation. On a vu que OpenVPN été le meilleur des protocoles pour les VPN.

Pourquoi ne pas avoir utilisé OpenVPN ?

Le protocole OpenVPN n'a pas été utilisé, car le firewall utiliser pas le protocole OpenVPN, mais le protocole IPsec. Le protocole IPsec et lui aussi très bien, il a la double encapsulation, mais le débit est réduit lors d'échange de données élever.

15. Mise en place d'un VPN

Procédure d'installation en annexes

16. Conclusion

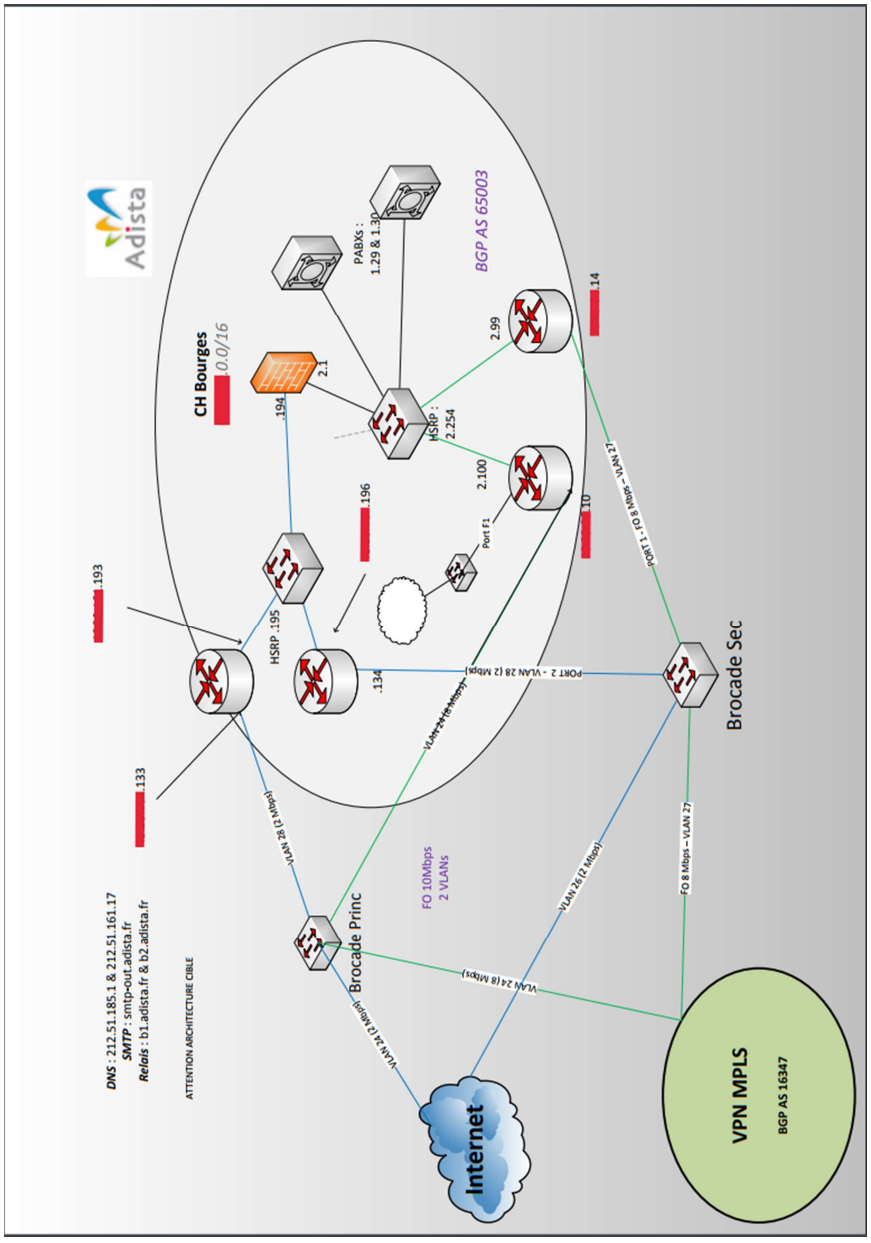
J'ai appris beaucoup de chose durent ce stage. J'ai appris comment les médecins d'astreinte pouvaient se connecter depuis chez eux, au réseau du CHGS. J'ai aussi vu comment était gérer les bureaux Citrix, documents, et les déploiements d'imprimantes sur les sessions en fonction du lieu de l'utilisateur. J'ai vu comment était gérer la partie bureau des utilisateurs ce qui m'a permis de voir les avantages et inconvénients financiers et de continuité de service dont les serveurs Citrix doivent faire preuve.

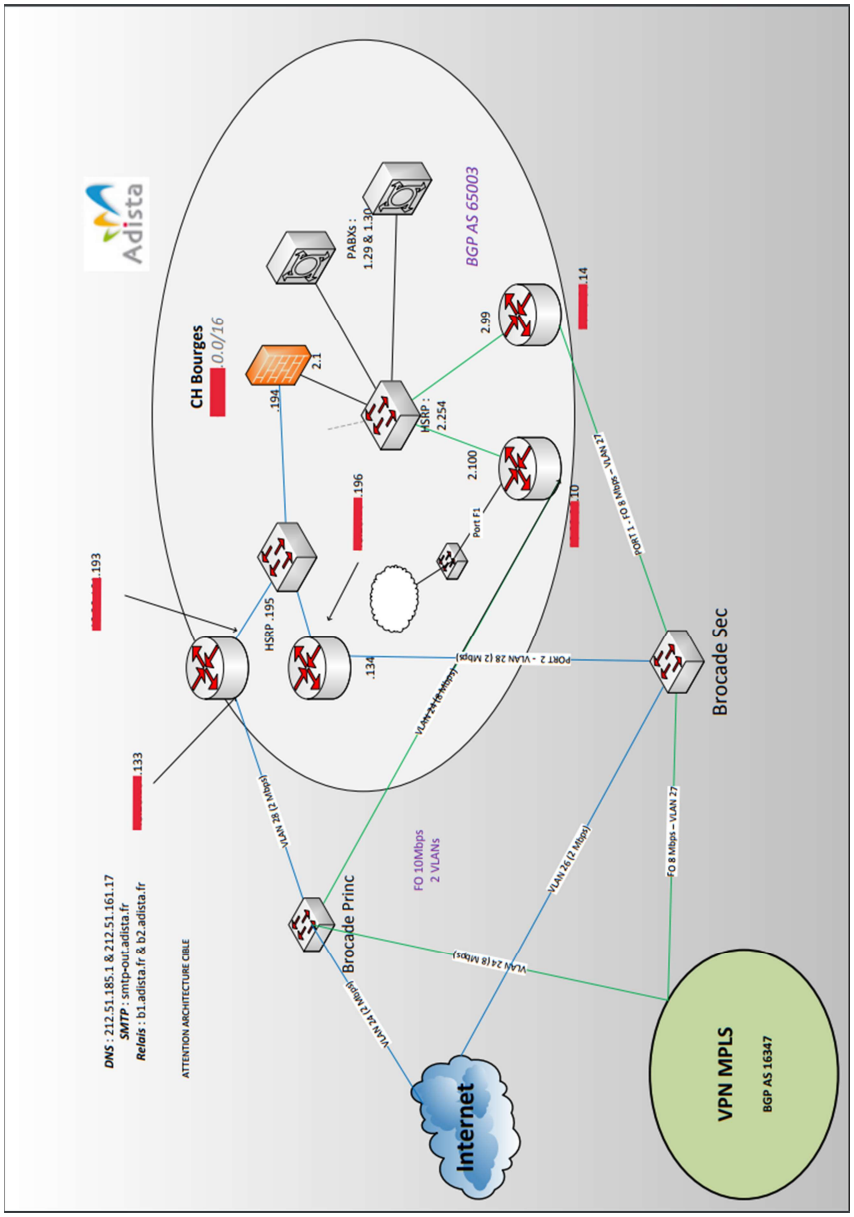
17. Remerciements

Je remercie Eric Faure qui est le Chef du service informatique, de m'avoir accepté au sein du service informatique. Je remercie également tout le service informatique en particulier, mon maitre de stage Mr Olivier Murzeau pour avoir répondu à toutes mes questions et avoir fait partager son travail et de ses connaissances. Je les remercie également pour la confiance dont ils ont fait preuve à mon égard, en me communiquant les divers mots de passe.

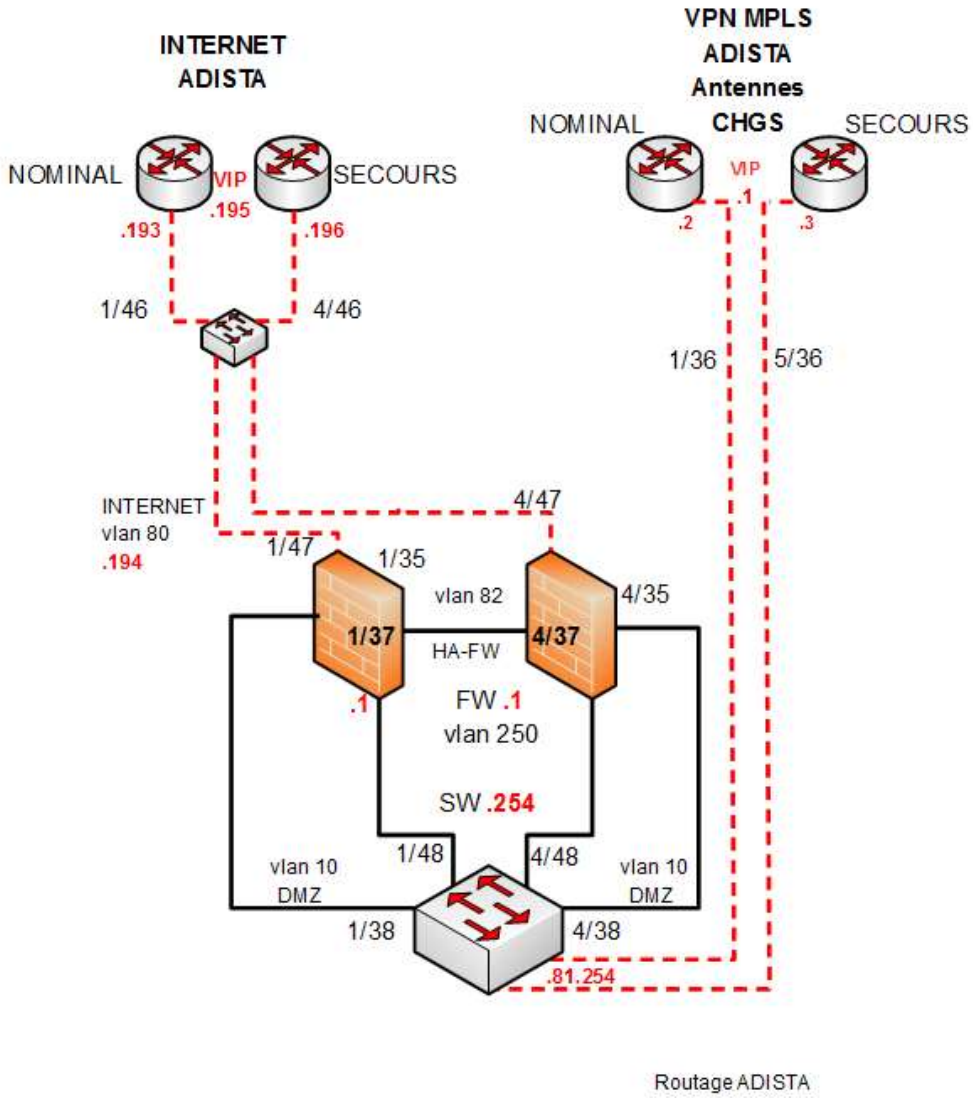
18. Annexes

a. Schémas Réseaux




Adista
CH Bourges
0.0/16
BGP AS 65003
PABXs :
1.29 & 1.30
HSRP :
2.254
2.1
.194
2.99
.14
2.100
.10
.196
Port F1
.193
HSRP .195
.134
PORT 2 - VLAN 28 (2 Mbps)
PORT 1 - FO 8 Mbps - VLAN 27
Brocade Sec
.133
VLAN 28 (2 Mbps)
FO 10Mbps
2 VLANs
VLAN 26 (2 Mbps)
FO 8 Mbps - VLAN 27
Brocade Princ
VLAN 24 (8 Mbps)
VLAN 24 (2 Mbps)
DNS : 212.51.185.1 & 212.51.161.17
SMTP : smtp-out.adista.fr
Relais : b1.adista.fr & b2.adista.fr
ATTENTION ARCHITECTURE CIBLE
Internet
VPN MPLS
BGP AS 16347

CONNEXION FIREWALL



b. *Procédure d'installation VPN*