

# Stagiaire Administrateur Réseaux

Samuel LAFORGE

2021

**Numéro d'étudiant : 21801299**

Stage réalisé sous la direction de M. Arnaud **Barbosa Leclercq**

**Stage réalisé à l'entreprise BEL (2 allée de Longchamp, 92 150  
Suresnes) :**

du 10/05/2021 au 30/07/2021

**Diplôme / Année en cours :**

Département Réseaux et Télécommunications – Licence Professionnelle  
Internet Des Objets

## **1. Remerciements**

Avant tout développement sur cette expérience professionnelle, il apparaît opportun de commencer ce rapport de stage par des remerciements à ceux qui m'ont beaucoup appris au cours de ce stage et même à ceux qui ont eu la gentillesse de faire de ce stage un moment très profitable.

Ainsi, je remercie Fabrice LAFORGE, mon oncle qui m'a permis de trouver mon stage au sein de la société BEL.

Aussi, je remercie Mr Barbosa Leclercq, mon maître de stage qui m'a formé et accompagné tout au long de cette expérience professionnelle avec beaucoup de patience et de pédagogie.

Je remercie également EL ASRI Reda, Rossignol Julien et leur équipe d'administrateurs réseaux pour m'avoir appris beaucoup de choses sur les réseaux informatiques.

Enfin, je remercie l'ensemble des employés de la société BEL pour les conseils qu'ils ont pu me prodiguer au cours de ces 3 derniers mois.

## **2. Résumé**

Ce stage a été une très grande opportunité pour moi d'apprendre des choses dans le réseau informatique et dans le management informatique. Il va beaucoup m'aider pour ma poursuite d'études en master dans le domaine des réseaux informatiques et des systèmes en alternance ou bien pour m'insérer professionnellement. En effet durant ce stage j'ai pu apprendre ce qu'était que le SD-WAN dans les moindres détails car nous avons migré les réseaux WAN MPLS vers des réseaux de type SD-WAN. J'ai aussi effectué pleins de petites missions en tant que technicien réseau ou IT Manager. Par exemple la remise à zéro de vieux switchs à donner ou des bornes Wi-Fi et aussi remis de nouvelles images dedans par le biais d'un serveur tftp afin de ne plus passer par le contrôleur des bornes, le remplacement et la configuration des switchs sur les sites français... Au final nous aurons migré plusieurs sites étranger comme Chostka en Ukraine, Vale de Cambra au Portugal ou même Sevenoaks en Angleterre et j'aurais pu apprendre à utiliser un logiciel très courant dans les entreprises pour administrer des Firewalls (Web SMC).

### **3. Sommaire**

1. Remerciements.....	2
2. Résumé.....	3
3. Sommaire.....	4
4. Introduction.....	5
5. Présentation du Groupe BEL.....	6
5.1. La place de l'informatique au sein du groupe.....	7
5.2. Données économiques.....	8
5.3. Organisation administrative.....	8
5.4. Les équipes de travail.....	9
5.5. L'organigramme de l'entreprise.....	10/11
6. Mon rôle au sein de la DSI.....	12
6.1. Les missions et objectifs professionnels du stage.....	12
6.2. Les moyens matériels, humains et financiers mis en œuvre.....	12
6.2.1. Outils utilisés lors de mon stage.....	13
6.2.2. Journées Types.....	14
6.3. Tâches effectuées lors du stage.....	15
6.3.1. Migration des réseaux WAN MPLS vers un réseau de type SD-WAN.....	15
6.3.2. Remise à zéro de bornes Wi-Fi Cisco.....	22
6.3.3. Remplacements des anciennes imprimantes.....	25
6.4. Les difficultés rencontrées.....	28
7. Conclusion.....	29
8. Glossaire.....	30
9. Liste des figures.....	31
10. Annexes.....	32

## **4. Introduction**

Dans le but de finaliser et d'obtenir mon diplôme en Licence professionnelle MRIT spécialité Internet des Objets, j'ai effectué un stage de 12 semaines, du 10 mai 2021 au 30 juillet 2021, au siège social de la fromagerie BEL à Suresnes (92), qui est spécialisée dans le domaine de l'agroalimentaire.

Le stage a pour objectif d'appréhender une première expérience dans le domaine professionnel en entreprise tout en participant, de manière active, à la mise en place de solutions sur de vrais projets. Ainsi ce stage s'est déroulé dans les équipes de manager informatique et réseau du site et comprend donc des enseignements tels que les systèmes, le management ou encore le réseau, qui sont des sujets qui ont été vus et acquis lors de ma formation à l'IUT de Béziers.

J'ai pu obtenir ce stage grâce à l'aide de mon oncle Fabrice LAFORGE qui travaille actuellement chez BEL à Vendôme et qui a fait passer mon CV jusqu'au siège social. Suite à cela mon maître de stage m'a appelé pour un entretien qui s'est très bien déroulé et qui m'a permis de rentrer dans l'entreprise.

Les principaux objectifs sont donc de participer aux différentes migrations réseaux avec l'équipe d'ingénieurs directement sur site mais aussi de renouveler les anciens appareils qui ne suivent plus les sécurités d'aujourd'hui avec les mises à jour.

Ainsi ce rapport va permettre de décrire le déroulement de mon stage, il est séparé en plusieurs parties distinctes (voir Table des matières) : la présentation détaillée de l'entreprise et de son environnement économique, les missions, les objectifs, les moyens utilisés et les difficultés rencontrées lors de mon stage, une conclusion ainsi qu'une annexe.

Je vais tout d'abord présenter l'entreprise dans laquelle j'ai effectué mon stage.

## 5. Présentation du Groupe Bel

Le groupe BEL a été créé en 1865 par Jules BEL à Orgelet dans le Jura, c'est un groupe familial qui est spécialisé dans l'industrie agroalimentaire et plus précisément dans la production de fromage en portion possédant comme marques connues La Vache qui rit, Babybel, Kiri, Boursin, Leerdammer, Mont Blanc ou bien Pompote.

Le groupe BEL cible une clientèle plutôt générale, dépendante des marques qu'elle possède.

Pour la marque La Vache qui rit, qui a permis de faire connaître la marque un peu partout dans le monde. Elle cible une clientèle assez générale en déposant sa marque sur divers objets du quotidien (pour l'école des enfants, en sponsorisant des événements comme le tour de France pour les adultes).

Pour la marque Babybel, c'est plus une jeune clientèle qui est ciblée grâce au mini babybel, avec des publicités orientées pour les enfants (super héros etc).

Pour les marques Kiri, Mont blanc et Pompote, elles ciblent exclusivement les enfants. On le voit notamment par les publicités diffusées à la télévision.

Puis certaines marques ciblent une clientèle plus générale comme le Port salut, Leerdammer ou bien Boursin.

Aujourd'hui la clientèle du groupe est très générale. Les fromages en portions se vendent très bien à l'heure actuelle et les marques sont bien implantées dans le marché français mais aussi à l'international.

Figure 1 : Slogan des grandes marques de fromage de BEL



MINI BABYBEL, KIRI, LA VACHE QUI RIT

**LE FROMAGE C'EST SÉRIEUX, MAIS PAS QUE !**

## **5.1. La place de l'informatique au sein du groupe :**

Le type d'informatique du groupe est un informatique industrielle, de cybersécurité et de support.

Dans le cadre du support, c'est le kiosque qui s'occupe du support informatique au sein du groupe. Il a une place très importante pour le groupe car c'est lui qui s'occupe de la gestion du matériel informatique et de la téléphonie, de la gestion de tickets mais aussi à la résolution de problèmes des utilisateurs. C'est une équipe très importante dans la vie au sein du groupe permettant aux utilisateurs d'avoir une assistance à tout moment au sein de leur parcours chez Bel. Le Bel Desk est un service d'aide aux utilisateurs qui est disponible 7 jours sur 7 et 24 heures sur 24.

La cybersécurité protège les réseaux et les ordinateurs du groupe contre les attaques malveillantes, sécurise les sites, les données et les serveurs. Elle lance des campagnes de préventions pour les utilisateurs, par exemple une campagne de phishing ou en créant l'encodage des badges d'accès pour les sites et en sécurisant les serveurs.

L'informatique industrielle, permet de faciliter le travail des ouvriers et cadres de l'entreprise. Elle permet également la gestion de la production et de la logistique. Par exemple sur le site de Suresnes avec l'impression par badge récupérable partout sur le site. On peut donc récupérer des impressions au réfectoire ou à d'autres endroits.

Mais aussi la maintenance du matériel de production automatisée, des serveurs, du réseaux sur les sites.

## **5.2. Données économiques :**

Le groupe BEL est implanté sur les 5 continents avec 30 filiales sur 33 pays, le groupe distribue leur production dans près de 120 pays. 19 milliards de portions vendues en 2019 pour 3,4 milliards de chiffre d'affaire. Le groupe c'est plus de 13 000 employés dans le monde. Le groupe BEL est une société anonyme, le prix d'une action est de 434 (8 juin).

## **5.3. L'organisation administrative :**

Tout d'abord, la fonction de IT Manager présent ici, est assurée par une personne qui gère la branche informatique du site. Le principe de ticket n'est pas inhérent au groupe mais il possède sa propre plateforme de ticket, Digital Kiosk qui est édité par Servicenow. Elle permet de gérer les tickets envoyés par les utilisateurs et de régler le problème en question. De plus, la branche IT ici est tournée aussi dans l'industriel, et ne gère pas que le support informatique.

Ensuite, les équipes de support sont assez courantes dans les entreprises mais c'est différent du Bel Desk, c'est un numéro que l'on peut appeler en cas de problème 7 jours sur 7 disponible en français/anglais afin de régler le problème. Ce service se situe en Roumanie mais est géré depuis le site de Suresnes.

L'entreprise utilise des logiciels disponibles seulement dans le groupe, comme le logiciel qui effectue les mises à jours entreprise pour les GPO (Group Policy Object) afin de passer certaines mises à jour ou logiciel ou aussi des serveurs sur le PC de tous les utilisateurs. L'entreprise utilise aussi comme beaucoup d'autre entreprise, le pack office 365 et un Intranet sous Sharepoint qui permet d'accéder à tous les outils de l'entreprise (Smile, weHr, ...)



## 5.4. Les équipes de travail :

Au sein du site de Suresnes, je suis situé côté des bureaux du support du groupe, de mon tuteur qui gère la branche IT France, mais aussi proche des administrateurs réseaux de l'entreprise. Je suis placé au rez-de-chaussée du siège social. Je fais partie du groupe DSI – IT France et toute la branche informatique du groupe BEL, qui regroupe toutes les équipes (cybersécurité, support, ...). Ci-dessous , le plan de la zone de travail :

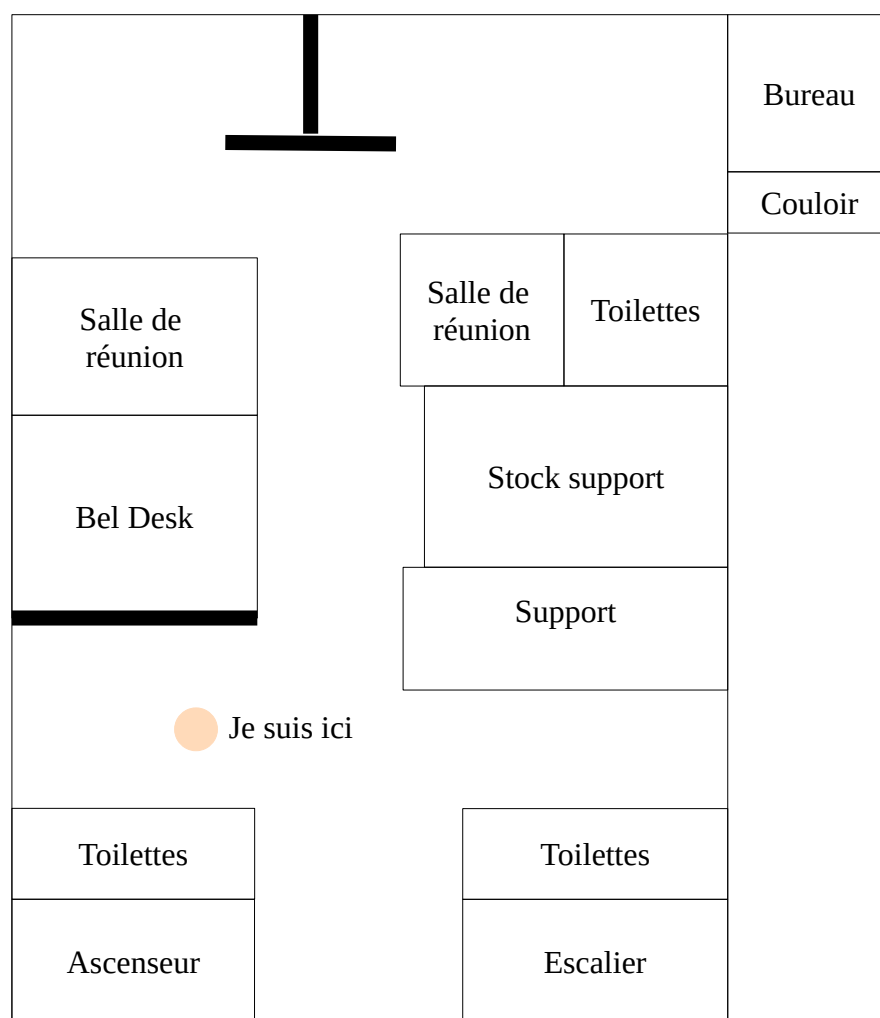
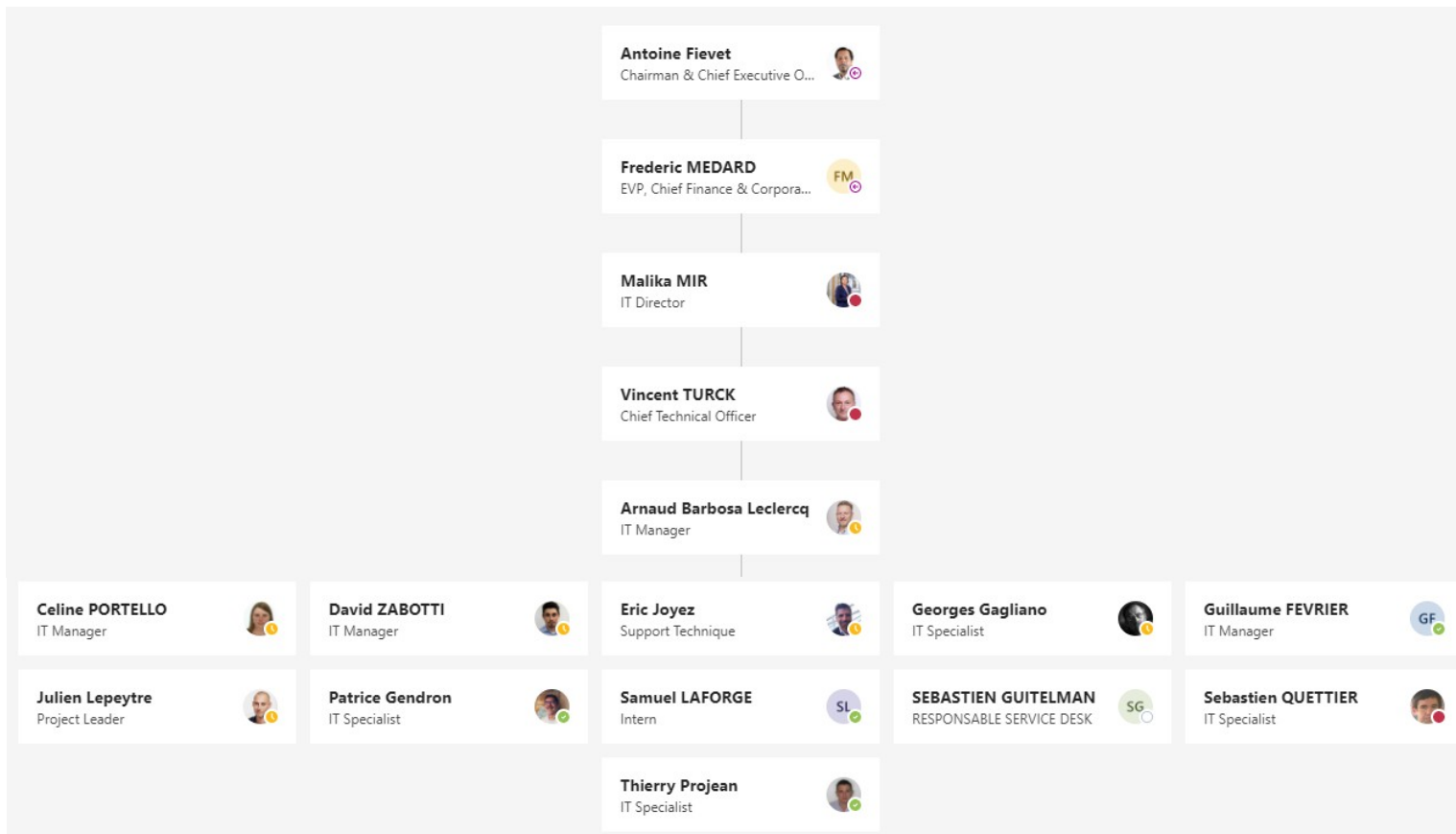
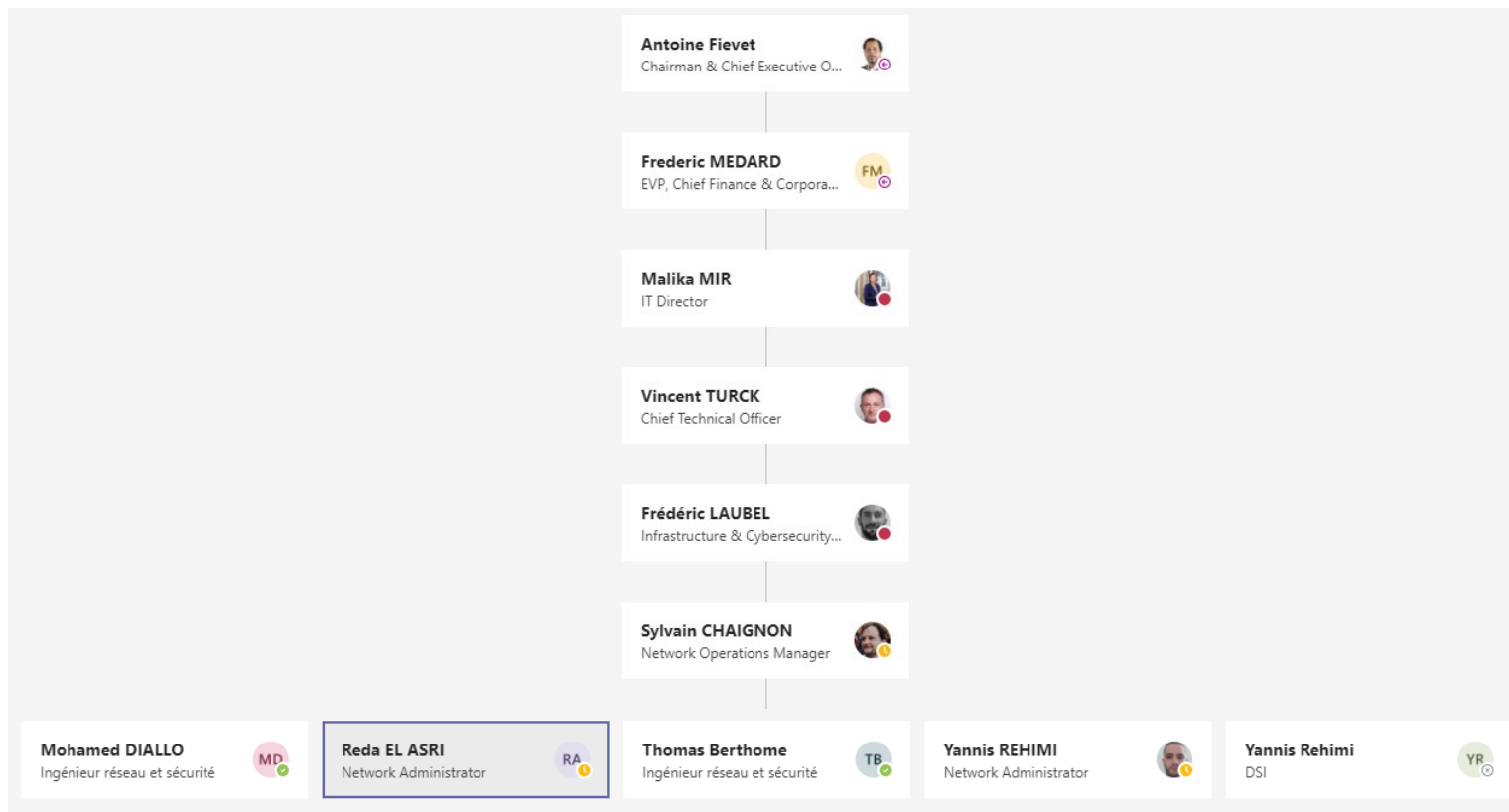


Figure 2 : Schéma de l'étage 0 au niveau informatique

## 5.5. L'organigramme de l'entreprise :



Voici l'organigramme de la branche informatique du groupe, il n'est pas complet. Je me situe dans l'équipe informatique car Arnaud Barbosa Leclercq est mon supérieur mais je travaille principalement avec l'équipe réseau. La fonction principale de mon supérieur est de constamment analyser les besoins technologiques de nos sites français et recommander des mises à niveau ainsi que des correctifs de sécurité. Il gère l'implémentation de nouveaux logiciels et matériels tout en respectant le budget et les délais.



Voici maintenant l'organigramme de l'équipe réseau. Je travaille principalement avec les 5 personnes en bas de l'organigramme.

## **6. Mon rôle au sein de la DSI :**

### **6.1. Les missions et objectifs professionnels du stage :**

Tout au long de mon stage, plusieurs missions m'ont été confiées en collaboration avec l'équipe réseau et l'équipe d'IT Manager :

- Remplacement des anciennes imprimantes à l'étage informatique par de nouvelles plus récentes avec plus de sécurité
- Étude de la migration des réseaux MPLS français et étranger vers un réseau de type SD-WAN + réalisation de ces migrations à l'aide de Firewalls, Switchs, VPN et de routeurs opérateurs
- Remise à zéro de vieux switchs et remplacements des switchs France par des nouveaux plus sécurisés et plus performants en passant à des ports en Gigabit faisant le PoE (Power over Ethernet) pour y connecter des AP Cisco Meraki et préparer les migrations réseaux + mise à jour des switchs n'étant pas accessibles en SSH
- Remise à zéro de plusieurs bornes Wi-Fi Cisco et remplacement de leur ancienne image afin de ne plus avoir besoin d'un contrôleur pour ensuite les donner dans différentes usines

### **6.2. Les moyens matériels, humains et financiers mis en œuvre**

Durant ce stage un ordinateur portable m'a été confié ainsi qu'un nom d'utilisateur et des accès sur les différents logiciels réseaux. C'est sur cet ordinateur que j'ai pu effectuer mes différentes missions. Un casque, un clavier, une souris et un sac m'ont été remis pour que je puisse travailler et me déplacer plus facilement dans les transports. Lorsque j'étais sur le site de Suresnes, 2 écrans externes avec bras articulés étaient à ma disposition.

Tout au long de mon stage une trace écrite a été faite tous les jours sur un Notebook où l'on peut y trouver toutes les informations de mes missions mais aussi des liens enregistrés sur mon ordinateur de stage.

### **6.2.1. Outils utilisés lors de mon stage :**

Durant mon stage j'ai pu utiliser différents outils comme :

- Microsoft Edge et Google Chrome pour naviguer sur internet
- Suite Office 365 (fournit par l'entreprise) pour la création de documents (Word, Excel, PowerPoint), l'envoi et la réception de mails (Outlook) et l'organisation de tâches (Teams, Calendar)
- SMILE (site interne) pour la création d'absences et me placer en télétravail certains jours de la semaine
- BelComeBack pour s'inscrire en présentiel et venir à l'entreprise
- DigitalKiosk pour la déclaration d'incidents, les demandes de droits et d'accès et accéder à la base de connaissances
- Sharepoint qui est notre point de partage interne pour récupérer des outils ou des fichiers

#### **Pour les migrations :**

- SMC (Security Management Center) pour accéder aux Firewalls Forcepoint et configurer leurs interfaces, leur routage, leur VPN et les règles de flux à appliquer en entrée et en sortie du LAN
- Centreon pour la supervision de toutes les machines des sites mondiaux (supervision des switchs, des Firewalls, des applications, des PABX...)
- IPAM pour la réservation des adresses IP et créer un DNS sur les machines comme les imprimantes
- Microsoft Visio pour créer des schémas d'infrastructures réseaux et préparer les migrations réseaux
- Putty ou SecureCRT pour me connecter en SSH et configurer les différents switchs des sites
- Zscaler pour filtrer les flux internet (Proxy)

## **6.2.2. Journées types :**

### **Journée type en présentiel :**

8h30 : Arrivée aux bureaux, pointage avec le badge puis lecture des mails, relecture des notes prises la veille et visionnage du calendrier pour les réunions prévues

9h – 10h : Réunion avec les différents collaborateurs informatiques pour obtenir des missions en attendant la préparation des migrations

10h - 12h : Exécution des différentes missions données (étude de couverture wifi avec orange pour notre site à Vendôme, projet de changement de switchs...)

12h – 12h45 : Pause déjeuner

13h – 16h : Suite des missions données le matin s'il n'y a pas de migrations prévues

16h – 16h30 : Prise de notes sur la journée et les informations importantes + problèmes rencontrés

Les horaires de travail varient en fonction de la journée passée

Moyenne de travail de 7h par jour (3h30 matin et après-midi)

### **Journée type à distance :**

8h30 : Mise sous tension de l'ordinateur, création d'une absence pour télétravail dans SMILE puis lecture des mails, relecture des notes prises la veille et visionnage du calendrier pour les réunions prévues

9h – 10h : Réunion teams avec l'IT Manager du site à migrer pour obtenir les informations nécessaires à la préparation de la migration

10h - 12h : Préparation des Firewalls (règles, interfaces, routage...) et des VPN pour anticiper les migrations réseaux

12h – 12h45 : Pause déjeuner

13h – 16h : Migration du réseau MPLS vers un réseau de type SD-WAN à distance en réunion teams avec les ingénieurs réseaux et l'IT Manager du site

16h – 16h30 : Prise de notes sur la journée et les informations importantes + problèmes rencontrés

Les horaires de travail varient en fonction de la journée passée

Moyenne de travail de 7h par jour (3h30 matin et après-midi)

### **6.3. Tâches effectuées lors du stage :**

#### **6.3.1 Migration des réseaux WAN MPLS vers un réseau de type SD-WAN**

Ma mission principale lors de ce stage a été la refonte du réseau WAN France en passant d'un réseau WAN de type MPLS vers un réseau de type SD-WAN.

##### **Le WAN :**

Avant d'expliquer le terme SD-WAN, commençons par le début. Le WAN (Wide Area Network) est un réseau informatique d'un opérateur qui interconnecte les sites d'une entreprise entre eux et à Internet. Ce réseau utilise une technologie spécifique, appelé MPLS. Elle permet aux données informatiques internes à l'entreprise de rester sur un réseau privé et donc être plus sécurisé.

Prenons un exemple. Si les réseaux informatiques étaient des routes alors internet serait l'équivalent des routes départementales qui sont accessibles par tous le monde alors que le MPLS lui est équivalent à des routes privées que seule l'entreprise peut prendre.

##### **Le SD-WAN :**

Il permet de construire un réseau virtuel qui prend appui sur un réseau physique et de le piloter depuis un point central. C'est une nouvelle approche des réseaux professionnels qui permet de supprimer au maximum voir complètement les lignes MPLS qui coûtent très chères et de souscrire à la meilleure offre Internet selon la localisation de l'entreprise. L'entreprise n'est donc plus obligé de rester avec son opérateur historique et peut passer à la concurrence pour optimiser ses coûts. Il est possible d'utiliser plusieurs opérateurs pour augmenter le débit internet.

Le SD-WAN est une solution adaptée aux nouvelles approches de l'informatique, avec l'externalisation des applications dans le cloud et aux nouvelles contraintes, comme la souscription de services logiciels hors du contrôle des services informatiques, ce qu'on appelle le Shadow IT.

### **L'externalisation des applications :**

Historiquement, les applications étaient hébergées au siège de l'entreprise (SAP, email, ...). Le WAN était essentiellement utilisé pour connecter les sites distants au siège. Internet était principalement utilisé pour le loisir (email personnel, navigation, ...).

Ce modèle commence à évoluer dans les années 2005 – 2010 avec l'arrivée d'application disponibles directement sur Internet comme Salesforce ("dans le cloud"). Les éditeurs de logiciel ont suivi, notamment Microsoft avec Office 365. Les applications se sont donc retrouvées dans des "Datacenters". Ces centres de données regroupent des ressources informatiques (serveurs). Les applications sont ainsi accessibles directement depuis n'importe quelle connexion Internet.

En restant avec l'exemple précédent des réseaux informatiques qui correspondent aux routes, les datacenters eux correspondent aux villes dans lesquelles on se déplace.

### **Les limites de l'externalisation des applications :**

Cette solution connaît quelques faiblesses comme :

- Le besoin de beaucoup de débit entre l'entreprise et internet ce qui génère des bouchons lors des heures de pointe (9h le matin quand la majeure partie des utilisateurs se connectent en même temps)
- Plus de sécurisation des données internes car elles transitent sur internet

En continuant l'exemple d'avant, les applications se retrouvent toutes dans la même ville et il ne reste plus qu'une seule route pour y accéder ce qui génère des bouchons aux heures de pointes.



### **Solution à ces problèmes :**

Nous utilisons des applications de guidage comme Google Maps qui nous renseigne sur le trafic routier et le meilleur chemin à prendre pour aller à notre destination.

La technologie SD-WAN utilise le même type de solution. Elle permet d'accéder aussi bien aux applications internes qu'à celles externalisées, en utilisant le meilleur chemin suivant le trafic. Alors que le MPLS ne donnait que des chemins privés, le SD-WAN peut aussi bien utiliser ces mêmes chemins privés ou des chemins publics (les connexions Internet).

On peut avoir plus d'informations sur ce site internet : [sd-wan-ebook-final\\_fr\\_v2.pdf](http://sd-wan-ebook-final_fr_v2.pdf) ([orange-business.com](http://orange-business.com))

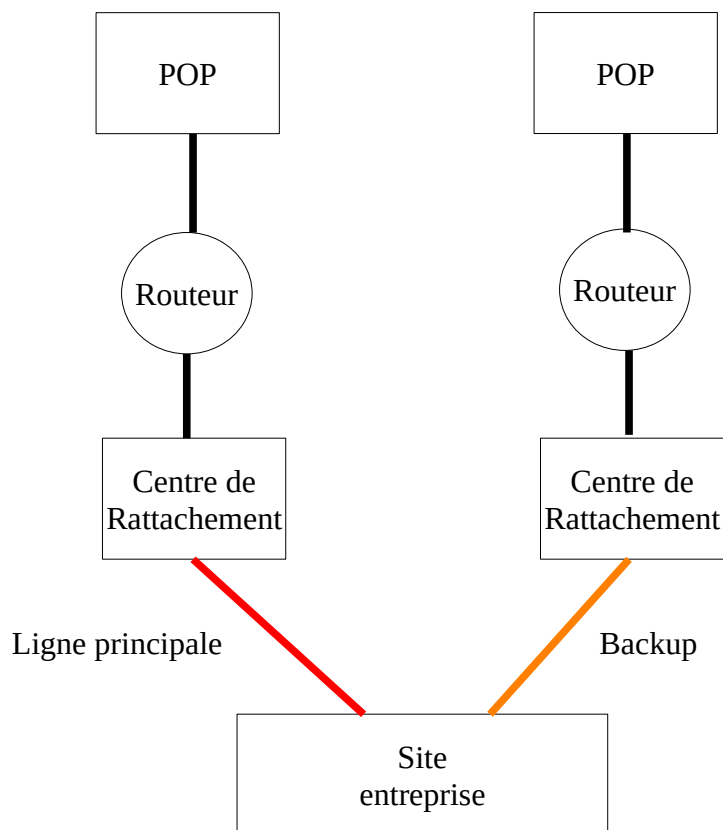
### **Les différentes étapes réalisées pour la mise en place du projet:**

Ce projet a déjà été commencé l'année dernière sur différents site étranger mais est encore en cours pour au moins 1 an car il y a beaucoup de sites à migrer. Pour mener ce projet a bien il faut suivre certaines étapes dans un ordre précis :

#### **1. Étude des opérateurs à choisir pour la connexion internet**

Pour cette étape il n'y a rien de bien compliqué. Nous avons choisis de sélectionner deux opérateurs pour nous fournir la connexion internet afin de faire de la haute disponibilité. En tirant du câble de fibre venant de deux côtés différents des sites nous avons pu sécuriser le réseau du site (appelé RS2 ou RS3 chez orange)

### Schéma explicatif du raccordement niveau 3 :



L'avantage de faire ce système de raccordement est que si jamais il y a un problème sur n'importe quel système de la ligne principale (Centre, routeur ou POP), la ligne de Backup prend la relève et assure ainsi une connexion à internet 24h/24h le temps de réparer le problème de la ligne principale.

Pour les sites français nous avons choisis comme opérateur **Orange** et **Linkt**. Orange car ils sont actifs partout mondialement et Linkt car ce sont ceux qui proposent les meilleurs services au prix le plus réduits. Nous avons souscrit pour des offres FTTO sur nos gros sites et des offres FTTH sur nos plus petits sites.

Pour les sites étrangers ce sont les IT manager de chaque site qui ont choisis leurs opérateurs.

## **2. Faire un point sur le matériel disponible de chaque site + IP opérateur**

Cette étape consiste à vérifier avec chaque IT manager s'ils ont déjà le matériel disponible sur leur site et si non nous devons les acheter et les configurer avant de leur envoyer. Grâce à un fichier Excel que nous avons préparé pour les sites nous avons pu vérifier par exemple qu'ils avaient assez de ports disponibles sur leurs switches et sur leurs Firewalls pour venir connecter les routeurs opérateurs. Il fallait du côté opérateur obtenir une plage d'IP publique pour les Firewalls et la gateway.

## **3. Préparation du matériel et pré configuration des firewalls + Migration**

Après vérification du matériel disponible nous avons dû principalement commander des Firewalls forcepoint 330 Series car sur la plupart des sites français il n'y en avait pas du fait que ce sont des petits sites sans trop d'importance.

Pour les configurer il suffisait de les alimenter puis de se connecter dessus par le biais d'un câble console et de taper la commande "sg-reconfigure". Au préalable une image récente des Firewalls a été copiée dans une clé usb pour les mettre à jour. Une fois mis à jour il fallait simplement leur attribuer une adresse IP entrante dans le LAN de chaque site.

Après la configuration des Firewalls il a fallu créer un cluster dans la SMC pour y ajouter les IP des deux Firewalls et faire de la haute disponibilité.

Avant de faire les migrations et pour gagner du temps nous avons fait en amont tout ce qui pouvait être fait sans que cela n'impacte le réseau actuel de l'entreprise. Par exemple nous avons configuré les nouvelles interfaces sur lesquelles les routeurs opérateurs sont connectés.

Interface 2	00:00:5e:00:0...	Provider Telefonica	Packet Dispatch
(CVI & NDI)			
CVI			
Node 1 NDI		C	Control Primary
Node 2 NDI		C	Control Primary
Interface 3	00:00:5e:00:0...	Provider Telefonica	Packet Dispatch
(CVI & NDI)			
CVI			
Node 1 NDI		c	Control Backup
Node 2 NDI		c	Control Backup

Figure 3 : interfaces de connexion avec les opérateurs du site de Madrid

On pouvait aussi à l'avance faire la création des règles de flux entrants et sortants du LAN (les règles sont désactivées tant que la migration n'est pas faite pour éviter les problèmes réseaux) et créer les tunnels VPN sur zscaler à configurer ensuite sur les Firewalls.




Ethernet		IPv4 Access	IPv6 Access	Inspection		
ID	Logical Interface	Source	Destination	Service	Action	Logging
Ethernet Insert Point (Before) - add rules here						
1	 ANY	±± ANY	±± ANY	◆ ARP ◆ RARP ◆ STP (Spa	✔ Allow	
2	 ANY	±± ANY	±± ANY	◆ IPv4	✔ Allow	
3	 ANY	±± ANY	±± ANY	◆ IPv6	✔ Allow	
Allow all						

Figure 4 : Exemple de politiques à mettre sur un Firewall

Pour effectuer les migrations sans se perdre car elles sont très longues (en moyenne 3 à 4h sans avoir de problèmes et avec les préparations faites en amont) nous avons suivis un template de migration sur Excel créée par les administrateurs réseaux. Nous avons 4 grandes étapes principales à faire pendant les migrations :

1. L'IT Manager du site à migrer devait brancher un câble Ethernet entre les routeurs opérateurs et les switchs appelés "CDR". Les CDR sont les switchs principaux de nos sites. Ce sont eux qui permettent l'interconnexion entre chaque vlan. Il devait aussi connecter un câble Ethernet entre les CDR et les Firewalls. Une fois fais je devais me connecter sur les switchs et configurer les interfaces connectées aux routeurs des opérateurs et les mettre dans le vlan crée spécifiquement pour eux puis passer le port en mode "Access".
2. Pour la 2ème étape nous devons monter les tunnels VPN créés en amont avec zscaler pour accéder à internet.
3. Il fallait ensuite que configurer les Firewalls pour qu'ils soient accessibles depuis leurs IP publiques et plus avec leurs IP LAN.
4. La dernière étape était d'intégrer les Firewalls dans le full-mesh de l'entreprise pour avoir encore plus de chemin d'interconnexion entre les sites et pas que via internet.

Figure 5 : Schéma physique des infrastructures de BEL en MPLS :

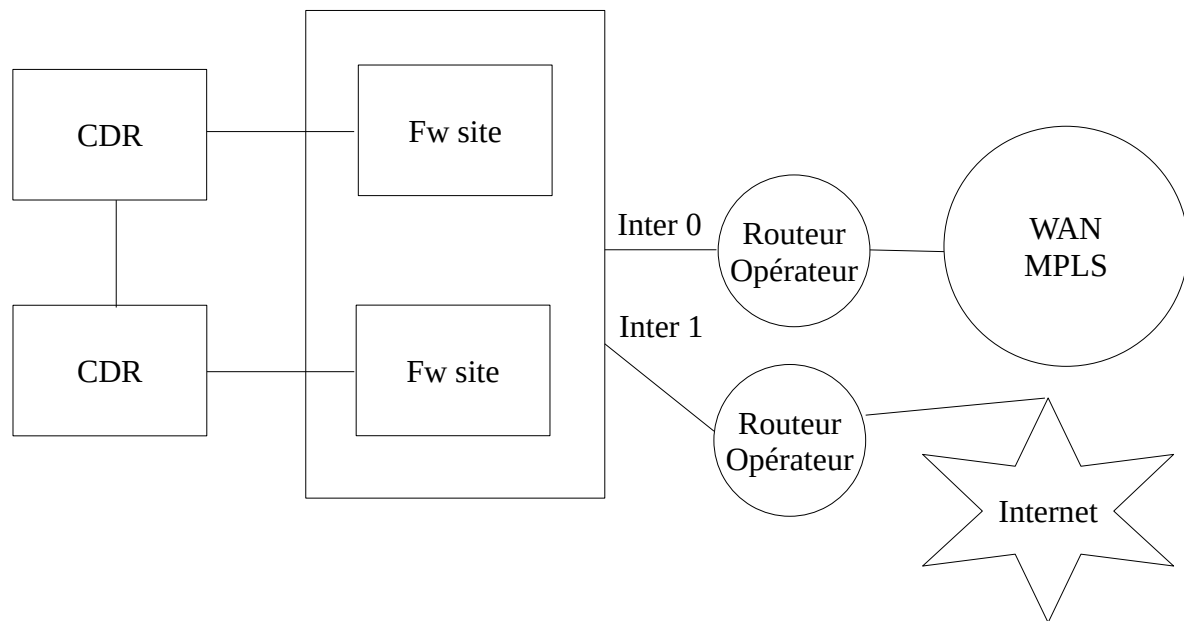
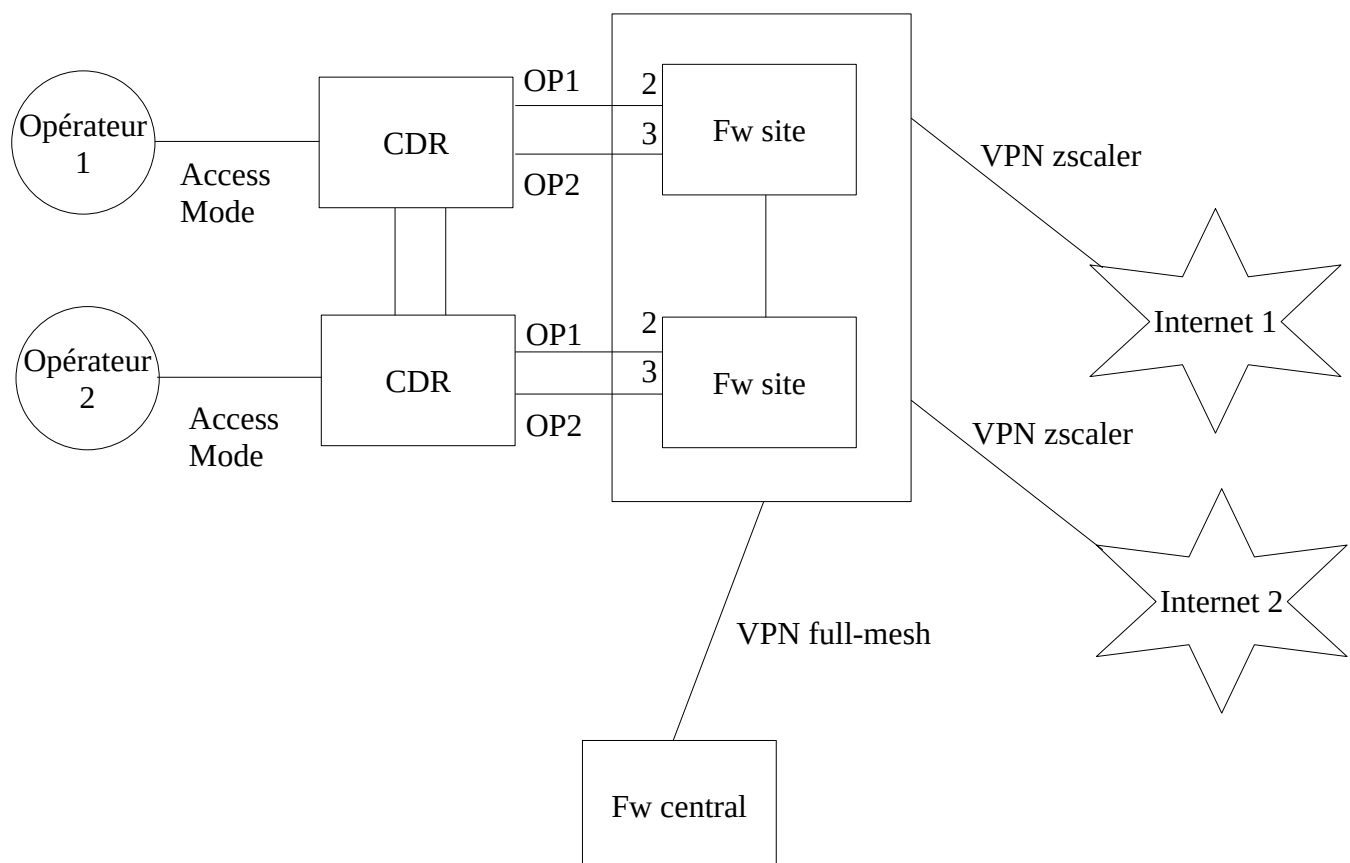


Figure 6 : Schéma physique des infrastructures de BEL en SD-WAN



### **6.3.2. Remise à zéro de bornes Wi-Fi Cisco**

Au cours de mon stage j'ai pu effectuer différentes petites missions comme celle-ci. Lors de cette mission mon chef m'a demandé de remettre à zéro des bornes Wi-Fi Cisco et de remplacer leur image par une image standalone (image qui fonctionne sans utiliser de contrôleur). On m'a demandé ceci parce que l'entreprise a pour but de changer toutes les bornes Wi-Fi par d'autres bornes appelées "Meraki". Ce sont des bornes qui fonctionnent dans le cloud ce qui permet de paramétrer à distance tous les équipements qui sont connectés dessus. Ces anciennes bornes que nous avons sont emmenées dans des lieux où il n'y a pas de contrôleur (maisons, petites usines...).

Il existe deux types de bornes Wi-Fi :

- Le Lightweight Access Point (LAP)
- L'Autonomous Access Point (AP) ou appelée standalone

Ces bornes sont les mêmes mais fonctionnent de façons différentes.

La borne en mode LAP est une borne gérée par un contrôleur WLC (Wireless LAN Controller), ce qui permet de l'administrer complètement au sein d'un réseau Wi-Fi comprenant plusieurs bornes. Dans ce mode de fonctionnement lorsque l'on met sous tension la borne, elle cherche automatiquement à se connecter à un WLC afin de récupérer sa configuration et les informations du réseau de l'entreprise. Si elle n'a pas de contrôleur alors la borne ne peut pas fonctionner. Voilà pourquoi il fallait que je change l'image des bornes de l'entreprise.

La borne en mode AP est une borne qui se gère de façon autonome. Elle n'a pas besoin de WLC pour fonctionner. Ce type de borne est utilisé dans un petit réseau Wi-Fi comme une maison ou une petite entreprise.

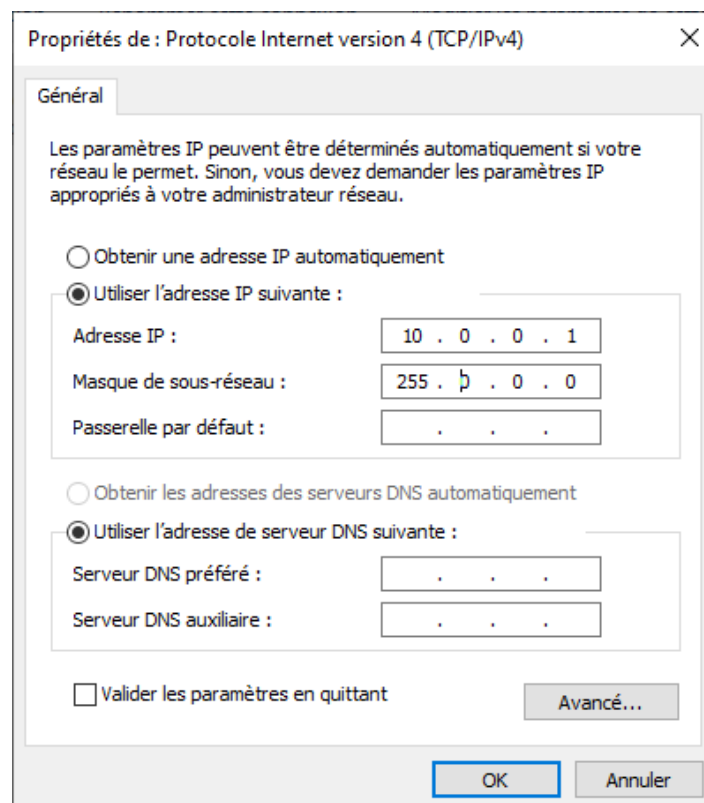
## 1. Remise à zéro d'une borne Wi-Fi

Pour remettre à zéro une borne Wi-Fi il suffit simplement de l'alimenter en même temps de rester appuyé sur le bouton "reset" de la borne pendant environ 30s jusqu'à ce que la LED devienne bleue. Après avoir fait ceci on arrive dans un mode appelé "ROMMON" C'est un mode qui permet de passer des commandes à l'AP mais sans être démarré sur une image. Une fois dedans il fallait supprimer le fichier private-multiple-fs (delete flash: private-multiple-fs) puis relancer l'AP (reboot).

## 2. Configurations des différents appareils pour installer la nouvelle image

Pour alimenter les bornes j'ai dû utiliser le PoE (Pover over Ethernet) d'un switch Cisco WS-C2960CX-8PC-L car je n'avais pas d'alimentation sur le site. Au niveau de la configuration des différents appareils j'ai dû configurer en 1<sup>er</sup> l'adaptateur USB-Ethernet du pc pour lui donner une adresse IP afin qu'il communique avec les autres appareils :

Figure 7 : Configuration IP de l'adaptateur



En deuxième temps j'ai dû configurer l'IP du vlan 1 du switch pour qu'il interconnecte les équipements:

```
Switch#conf t                                (configuration du terminal)
Switch(config)#interface vlan 1              (connexion à l'interface)
Switch(config-if)#ip address 10.0.0.2 255.0.0.0 (attribution d'adresse IP)
Switch(config-if)#no shut                    (allumage de l'interface)
Switch(config-if)#end                        (retour en mode privilège)
Switch#sh ip inter brief                     (vue sur les interfaces)
```

Interface	IP-Address	OK?	Method	Status	Protocol
Vlan1	10.0.0.2	YES	manual	up	down

Pour finir j'ai configuré l'interface de l'AP :

```
APa46c.2a27.dab0#debug capwap con cli        (déblocage du mode privilège)
APa46c.2a27.dab0#conf t                      (configuration du terminal)
APa46c.2a27.dab0(config)#interface GigabitEthernet 0 (connexion à l'interface)
APa46c.2a27.dab0(config-if)#ip address 10.0.0.3 255.0.0.0 (attribution d'adresse IP)
APa46c.2a27.dab0(config-if)#no shut          (allumage de l'interface)
APa46c.2a27.dab0(config-if)#end              (retour en mode privilège)
```

Il ne me restait plus qu'à installer un serveur tftp sur mon ordinateur. J'ai décidé d'installer tftpd64. Ce serveur m'a permis de placer l'image des bornes dedans et de me connecter dessus avec la borne pour récupérer cette image et écraser la précédente.



### **3. Installation de l'image**

Une fois que tous les appareils étaient configurés il ne me restait plus qu'à lancer une commande sur l'AP afin de se connecter au serveur et récupérer l'image :

```
archive download-sw /force-reload /overwrite tftp://[IP_Serv]/[Image]
```

archive download-sw : Commande pour télécharger

/force-reload : Syntaxe pour redémarrer la borne après téléchargement

/overwrite : Syntaxe pour écraser l'image actuelle de la borne

tftp://ip/image : chemin vers l'image se situant dans le serveur

### **6.3.3. Remplacement des anciennes imprimantes**

Le projet de remplacement des anciennes imprimantes à l'étage informatique m'a été confié ainsi qu'à l'apprenti Manager. Cette mission a été divisée en plusieurs parties. Tout d'abord j'ai dû m'occuper de configurer le port du switch sur lequel est connecté l'imprimante pour le passer dans le bon vlan (vlan printers). Avant de pouvoir configurer le port il m'a fallut retrouver sur quel switch était connecté l'imprimante. Pour cela je pouvais remonter au port petit à petit grâce à l'adresse MAC de l'imprimante en partant de notre switch principal :

Figure 8 : Vue sur la table d'adresses MAC avec filtre

```
FRSURCDR001#sh mac address-table | inc f7e5
2803      9c93.4ed3.f7e5    dynamic ip,ipx,assigned,other TenGigabitEthernet1/1/1
3
```

Grâce à la table d'adresse MAC et un filtre sur la MAC précise que l'on veut on peut retrouver sur quel port est connecté l'imprimante. Ici on peut voir qu'elle est sur l'interface TenGigabitEthernet1/1/1/3.

Je peux donc aller voir la description de cette interface pour savoir à quoi elle correspond :

Figure 9 : Description de l'interface

```
FRSURCDR001#sh inter TenGigabitEthernet1/1/13 description
Interface                               Status      Protocol Description
Tel/1/13                               up          up        FRSURSWI014-1E
```

J'ai pu voir dans la description que cette interface correspond au switch numéro 14 du site de Suresnes. J'ai donc dû me connecter dessus en ssh.

Une fois que j'étais connecté dessus il me fallait retrouver le port sur lequel est connecté l'imprimante toujours avec la même commande :

Figure 10 : Vue sur la table d'adresses MAC du switch 14 avec filtre

```
FRSURSWI014#sh mac address-table | inc f7e5
2803      9c93.4ed3.f7e5      DYNAMIC      Gi2/0/45
```

Je n'avais plus qu'à me connecter sur le port et le configurer pour changer sa description et le mettre dans le bon vlan :

Figure 11 : Configuration de l'interface

```
FRSURSWI014#conf t
Enter configuration commands, one per line. End with CNTL/Z.
FRSURSWI014(config)#inter Gi2/0/45
FRSURSWI014(config-if)#switch
FRSURSWI014(config-if)#switchport vl
FRSURSWI014(config-if)#switchport vla
FRSURSWI014(config-if)#switchport vlan
FRSURSWI014(config-if)#switchport vlan
FRSURSWI014(config-if)#switchport acc
FRSURSWI014(config-if)#switchport access vl
FRSURSWI014(config-if)#switchport access vlan 2801
FRSURSWI014(config-if)#inter
FRSURSWI014(config-if)#inter des
FRSURSWI014(config-if)#desr
FRSURSWI014(config-if)#de
FRSURSWI014(config-if)#des
FRSURSWI014(config-if)#description "Imprimante"
```

Une fois l'interface configurée j'ai vérifié que la configuration a bien été prise en compte et j'ai terminé en sauvegardant la configuration :

Figure 12 : Vérification des modifications + enregistrement

```
FRSURSWI014#sh inter GI2/0/45 status

Port      Name           Status      Vlan      Duplex  Speed Type
Gi2/0/45  "Imprimante"   connected   2801      a-full  a-1000 10/100/1000Ba
seTX
FRSURSWI014#wr mem
Building configuration...
[OK]
```

Une fois le port configuré j'ai dû m'occuper de faire la réservation IP dans notre IPAM. La réservation se fait très facilement. Il fallait simplement que j'aille dans l'onglet réseaux puis que je sélectionne le réseau correspondant au vlan des imprimantes et que je trouve une IP de libre. La réservation se fait de la façon suivante :

ADD AN IPV4 ADDRESS

Between IP address

IP address name

FR\_PRTSUR\_E1618

IP address

MAC address

Shortname

FR\_PRTSUR\_E1618

Domain

☒ Create DHCP static

☒ Use IPAM name instead of DHCP client name

Advanced properties

Default

Comment

FR\_PRTSUR\_E1618

PREVIOUS

NEXT

OK

CANCEL

Dès que la réservation a été faite il ne restait plus qu'à réalimenter l'imprimante pour qu'elle prenne son IP fixe et l'apprenti s'est occupé de faire la configuration directe de l'imprimante pour qu'elle soit fonctionnelle et que l'on puisse imprimer.

## **6.4. Les difficultés rencontrées**

Au cours du stage j'ai rencontré des difficultés sur la SMC de Forcepoint car je ne connaissais pas le logiciel et il y avait beaucoup d'options à comprendre. Encore aujourd'hui il me reste pas mal de choses à apprendre sur les Firewalls mais j'ai pu comprendre les bases grâce à du travail régulier sur ce logiciel.

Au cours des migrations avec l'équipe réseau nous avons rencontré beaucoup de difficultés relativement simple mais qui nous ont fait perdre pas mal de temps. Par exemple lorsqu'il fallait faire monter les tunnels VPN vers notre proxy zscaler cela ne fonctionnait pas à cause de certaines règles de flux qui en bloquaient d'autres ou bien une IP publique qui était mal écrite sur le Firewall.

Nous avons aussi eu des difficultés de compréhension entre la partie technique et les IT Manager qui eux ne connaissaient pas forcément les infrastructures ce qui a causé des problèmes sur les branchements des câbles lors des migrations. Le fait de devoir parler en anglais avec les sites étrangers n'a pas aidé à la compréhension.

J'ai pu avoir aussi quelques difficultés sur la remise à zéro des bornes Wi-Fi car il y avait des problèmes de communication entre les différents appareils. Sur ce projet j'ai aussi commis une erreur en démarrant une ancienne borne configurée ce qui avait fait buguer tout le réseau Wi-Fi de l'entreprise mais ceci m'a appris à toujours devoir prendre mon temps et ne pas me précipiter pour faire les choses.

## **7. Conclusion**

Pour conclure, au vu de mon évaluation positive auprès des équipes de manager informatique et de réseau que j'ai eu tout au long de mon stage et lors de mon aide sur les différentes missions qui m'ont été confié, mon travail a été bénéfique pour l'entreprise qui a pu se mettre à jour au niveau de la sécurité informatique.

Mon sujet principal qui était les migrations réseaux m'a fortement intéressé et ces migrations qui nous ont pris beaucoup de temps sera un avantage économique pour l'entreprise qui devient petit à petit indépendant des opérateurs. De plus j'ai pu voir ce qu'était que le métier d'administrateur réseau et ceci m'a encore plus motivé à l'idée d'exercer des métiers dans le domaine des systèmes et des réseaux informatiques.

Durant ces 12 semaines j'ai su analyser la problématique donnée pour les migrations, étudier l'architecture des différents sites mondiaux, augmenter la sécurité de nos sites par le remplacement de nouveaux appareils informatiques plus récents, apprendre à administrer des Firewalls pour effectuer du routage vers des tunnels VPN IPsec ou bien configurer leurs nouvelles interfaces.

Les difficultés rencontrées m'ont permis de travailler ma logique concernant les migrations du fait que nous faisions des erreurs d'inattention. De plus elles m'ont permis d'améliorer en partie mon anglais technique mais aussi l'anglais général pour la communication.

## **8. Glossaire**

LAN	Local Area Network
WAN	Wide Area Network
SD-WAN	Software Defined WAN
FW	Firewall
CDR	Cœur de réseau
DSI	Direction du Système d'Information
SMC	Security Management Center
GPO	Group Policy Object
PABX	Private Automatic Branch Exchange
FTTH	Fiber To The Home
FTTO	Fiber To The Office
AP	Access Point
LAP	Lightweight Access Point
WLC	Wireless LAN Controller
PoE	Power over Ethernet
VPN	Virtual Private Network
SSH	Secure Shell
MPLS	MultiProtocol Label Switching
TFTP	Trivial File Transfer Protocol

## 9. Liste des Figures

Figure 1 – Slogan des grandes marques de fromages de BEL.....	6
Figure 2 – Schéma de l'étage 0 au niveau informatique.....	9
Figure 3 – Interfaces de connexion avec les opérateurs du site de Madrid.....	19
Figure 4 – Exemple de politiques à mettre sur un Firewall.....	20
Figure 5 – Schéma physique des infrastructures de BEL en MPLS.....	21
Figure 6 – Schéma physique des infrastructures de BEL en SD-WAN.....	21
Figure 7 – Configuration IP de l'adaptateur.....	23
Figure 8 – Vue sur la table d'adresses MAC avec filtre.....	25
Figure 9 – Description de l'interface.....	26
Figure 10 – Vue sur la table d'adresses MAC du switch 14 avec filtre.....	26
Figure 11 – Configuration de l'interface.....	26
Figure 12 – Vérification des modifications + enregistrement.....	27

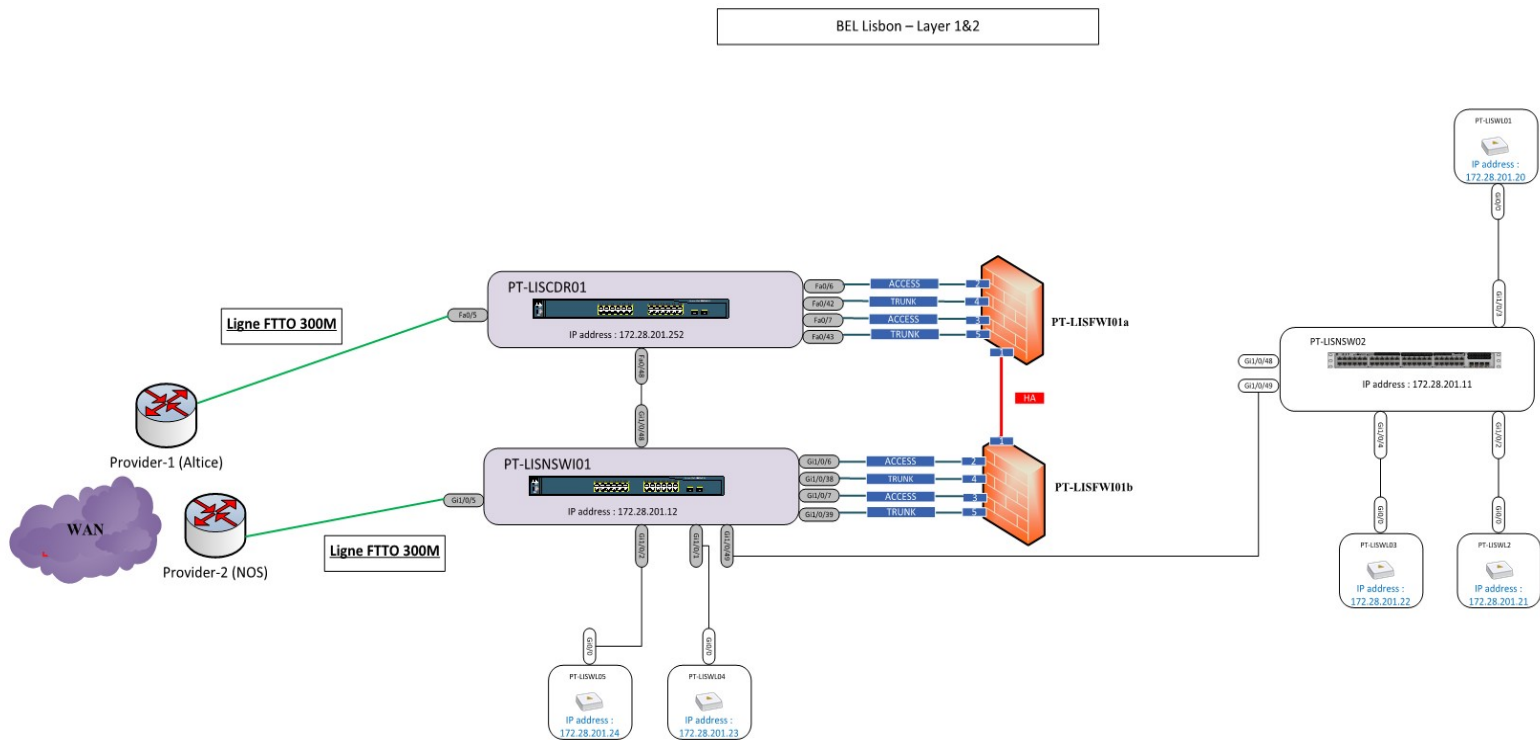
## 10. Annexes

### 10.1. Procédure à suivre pour les migrations

2	Planification	Actions			
3	Role	#	Equipement	Action	Commentaire
4		0	Prerequis	<ul style="list-style-type: none"> <li>* Contact IT local (check console cable drivers, Mobile connexion, local admin on PC)</li> <li>* Check cabling ( rack pictures, number of cables )</li> <li>* Level 1 architecture before and after migration</li> <li>* Retrieve OBS routers reference on OBS portal</li> <li>* Declare the public ip on Zscaler platform</li> </ul>	
5	BEL	1	Configuration switch Matosinozh	<ul style="list-style-type: none"> <li>* Creation and propagation of Vlan 101 on Switch SE_HELCDR1 &amp; SE_HELCDR2</li> <li>* Configure interface gig1/0/9 for WAN_OBS1 as access vlan 101 on SE_HELCDR1</li> <li>* Configure interface gig1/0/9 for WAN_OBS2 as access vlan 102 on seHELCDR2</li> <li>* Configuration of new interfaces Gi0/10 on SE_HELCDR1 for ISP1 (in access Vlan 101).</li> <li>* Configuration of new interfaces Gi0/10 on SE_HELCDR2 for ISP2 (in access Vlan 102).</li> <li>* Add vlan 101 on interfaces gig0/4 &amp; gig0/5 on both CDR (for the firewall as we do not have enough interfaces on CDRs)</li> </ul>	
6	BEL	2	Cablage Switch sur Routeurs Operateur	<ul style="list-style-type: none"> <li>* On port Gi0/9 of switch SE_HELCDR02 connect the frb Interface</li> <li>* On port Gi1/0/10 of switch SE_HELCDR01 connect the ISP2 Interface</li> <li>* On port Gi0/9 of switch SE_HELCDR01 connect the frb interface</li> <li>* On port Gi0/10 of switch SE_HELCDR01 Connect the ISP1 Interface</li> </ul>	After circuit testing, delete OBS/Switch Interco (gi0/7)
7	BEL	3	Configuration SE-HELFWU01b	<ul style="list-style-type: none"> <li>* Add Virtual interfaces on interface 2 : CVI : 195.67.13.19/28 fva: 195.67.13.20/28 frb: 195.67.13.21/28</li> <li>* Add Public IP on Control Interface as backup (Interfaces &gt; Interface Options) and Private IP stay the primary.</li> <li>* Creation of traffic handler : Outbound-SE-HEL-Internet ; constituted of : nlink-SE-HEL-WAN 1 (@Public IP)</li> <li>* Creation of policy NAT : 'Office, Office_Wifi, Mobile_Wifi and infra' to Internet'</li> <li>* Activate NAT policy</li> <li>* Replace the default route by 172.16.0.0/12 on the routing table</li> <li>* Add default route on the new interface with the nlink as gateway</li> <li>* Copy the policy internet - Bel standard direct access policy</li> </ul>	<p>Pour Creation interface sur le firewall: ajouter mac address 00:00:5e:00:00:1X (X étant le numero de l'interface) Ajout adresse IP sur l'interface X Au niveau du interface interco, suppression route par défaut et ajout route 172.16.0.0/12 1. Création des nlink pour les 2 opérateurs (SDWAN &gt; Traffic Handler &gt; Static Netlink) 2. Création du traffic Handler (SDWAN &gt; Traffic Handler &gt; New (Outbound multi-link) Copier les règles 5.6.24.3 sur fw MAD (Internet-&gt; Grp-Net-Bel-Internet) Copier les règles 5.6.24.4 sur FW MAD (outbound-FR-&gt; Pare-feu du site)</p>
8				PUSH	
9	BEL	4	Configuration FR-CLAFW01	<ul style="list-style-type: none"> <li>* Check the Network Group (Grp-Net-Bel-SE-HEL) for the site with all network subnet</li> <li>* Add Group Network SE-HEL (Grp-Net-Bel-SE-HEL) on the Bel-site-to-site VPN policy (Forcepoint-&gt;Forcepoint)</li> </ul>	
10	BEL	7	Configuration SE-HELFWU01	<ul style="list-style-type: none"> <li>* Creation of Zscaler Gateways :</li> <li>* Activate endpoint on the Gateway SE-HELFWU01 (after creation of interface 3)</li> <li>* Creation of VPN policy based VPN : BEL-SE-HEL-WAN 1-Zscaler &amp; BEL-SE-HEL-WAN 2-Zscaler</li> <li>* Activate tunnels in policy based vpn</li> <li>* Modification of policy IPV4</li> <li>* Belnet to Internet through VPN Zscaler (Enforced)</li> <li>* Activate IPV4 policy</li> </ul>	<p>Pour créer IT-Zscaler, aller dans SDWAN &gt; Policy-Based VPN &gt; Bel-SE-HEL-zscaler. Il faut ensuite "Edit" et créer un New External VPN Gateway "UK-Zscaler" et ajouter les différents nœuds Zscaler. Test connectivité sans Tunnel Zscaler. Si tests concluant, ajout du Enforce VPN Zscaler dans la règle. Ajoute dans l'onglet "Sites" tous les réseaux lors de l'ajout VPN Gateway Puis dans VPNEndpoint, désactiver les tunnels avec ip privée</p>
11		6	Configuration Zscaler	<ul style="list-style-type: none"> <li>* Add the vpn credentials then Location Mgmt</li> <li>* Modify the tunnel pre-shared key (Administration &gt; VPN Credentials)</li> </ul>	Ne pas oublier la sub-location Mobile en désactivant l'authentification users
12	BEL	8	Configuration SE-HELFWU01	<ul style="list-style-type: none"> <li>* Add security Policies section for DHCP purpose then add DHCP traffic policies to be allowed through the VPN Full mesh</li> <li>* Add security policy to allow traffic for local subnets (from Grp-Net-Bel-SE-HEL to Grp-Net-Bel-SE-HEL)</li> <li>* Enforce Wifi and Mobile traffic flows on Zscaler VPN Tunnel Link1</li> <li>* Enforce Office and Server traffic (HTTPS, HTTP and FTP Services) to be allowed through Zscaler VPN Tunnel Link1</li> <li>* Enforce All other traffic (site to site or Site to DC) on Full_Mesh_Corporate_VPN</li> </ul>	
13			Configuration FR-CLAFW01	<ul style="list-style-type: none"> <li>* Add the Engines on claranet firewall to allow the engines with public ip then PUSH on claranet firewall</li> </ul>	* Update Group Network SE-HEL (Grp-Net-Bel-SE-HEL) on the Bel-site-to-site VPN policy (Forcepoint->Forcepoint) on FR-CLAFW01
14	BEL	11	Configuration SE-HELFWU01	<ul style="list-style-type: none"> <li>* Change the DNS from private dns to the public dns (KEMP)</li> <li>* Change the location (outside_bel)</li> <li>* Add the engine to the remote firewall groupe</li> <li>* Change the ip of the engine with sg-reconfigure</li> <li>* Configure the smc public ip address (85.208.192.10) on both firewall (sg-reconfigure)</li> </ul>	<p>Mettre l'IP publique de la SMC : 85.208.192.10 (à faire sur les deux FW) Etapre Sg-reconfigure Connecter en 4G pour éviter la perte de connectivité générer la clé OTP : clic droit 'save initial configuration' &gt; View Details Après avoir effectué le sg-reconfigure sur les deux-pare-feux, il faut push de nouveau la configuration Configuration-&gt; Install Policy Après la fin du sg-reconfigure, ajouter les groupes BE-8RL sur le pare-feu de CLAO1</p>
15	BEL	10	Configuration MAN 1 & 2	<ul style="list-style-type: none"> <li>* ip route 172.16.70.0 255.255.255.0 172.19.111.17 name SE-HELSEINGBORG</li> <li>* ip route 172.17.70.0 255.255.255.0 172.19.111.17 name SE-HELSEINGBORG</li> <li>* ip route 172.17.71.0 255.255.255.0 172.19.111.17 name SE-HELSEINGBORG</li> <li>* ip route 172.18.70.0 255.255.254.0 172.19.111.17 name SE-HELSEINGBORG</li> <li>* ip route 172.20.70.0 255.255.254.0 172.19.111.17 name SE-HELSEINGBORG</li> <li>* ip route 172.28.70.0 255.255.255.128 172.19.111.17 name SE-HELSEINGBORG</li> <li>* ip route 172.28.71.0 255.255.255.128 172.19.111.17 name SE-HELSEINGBORG</li> <li>* ip route 172.28.71.128 255.255.255.192 172.19.111.17 name SE-HELSEINGBORG</li> <li>* ip route 172.16.71.240 255.255.255.240 172.19.111.17 name SE-HELSEINGBORG</li> </ul>	ip route 172.17.78.0 255.255.255.0 172.19.111.22 name SE-HELSEINGBORG (summary)?
16		9	Configuration SE-HELFWU01	<ul style="list-style-type: none"> <li>* Add the Firewall object (SE-HELFWU01) on the Bel_Full_Mesh_Corporate_VPN</li> </ul>	172.19.111.17 : CLARANET2
17				PUSH SUR TOUS LES FIREWALLS DU FULL MESH	
18	BEL	12	Monitoring	<ul style="list-style-type: none"> <li>* Update Monitoring Tools</li> <li>* Update Groupe Datexion</li> <li>* Send an Email to OBS to stop supervision on old obs router</li> <li>* Send an Email to Datexion for the new firewall supervision</li> <li>* Collect ISP information (name of provider, line bandwidth, incident mgmt, contacts etc...)</li> </ul>	



## 10.2. Schéma SD-WAN de Lisbonne



## 10.3. Exemple de checklist pour les sites France

Migration Checklist : < Evron (Patrice Gendron) >				
Phase I				
Migration Type	Firewalls	<input checked="" type="checkbox"/> Physical	<input type="checkbox"/> Virtual	
	Site type	<input checked="" type="checkbox"/> Plant	<input type="checkbox"/> Office	
	Zscaler tunnel	<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No	
	Full- mesh	<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No	
	Multi-Link	<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No	If yes, Download and Upload Speed ?
	Change of the switch core	<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No	Ref : Catalyst 3850 24 S
	Providers	<input checked="" type="checkbox"/> 1	<input type="checkbox"/> 2	Orange (1 fibre + 1 backup)
	SFP availables ?	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No	If yes, give us the port numbers
	How many Core/Central technical room ?	<input type="checkbox"/> 1	<input type="checkbox"/> 2	Baie informatique dans le sous sol
Induction places Fibre 1 : Arrive devant le bat administratif et Fibre 2 : Arrive parking Evron 2				
Phase II				
Type	Element	Amount	Done	Comments
Devices and cables	Core switch	2	<input checked="" type="checkbox"/>	Les 2 dans le bat administratif (aucun dans le second local)
	Firewalls	2	<input checked="" type="checkbox"/>	Les 2 dans le bat admin. Aucun firewall dans le 2ème local
	Console cable for the Firewall	1	<input checked="" type="checkbox"/>	Sent with the firewalls
	Power cable for the Firewalls	2	<input checked="" type="checkbox"/>	Sent with the firewalls
	RJ45 cables for office core switch-F/W	6	<input checked="" type="checkbox"/>	
	RJ45 cables for HA firewalls	1	<input checked="" type="checkbox"/>	
Free ports	On the core switch	6	<input checked="" type="checkbox"/>	3 ports on each switch (ports 12 à 14)
	On the access switch	0	<input checked="" type="checkbox"/>	
Installation	Firewalls installed on same rack as CDR	-	<input checked="" type="checkbox"/>	
	Rack unit for each Firewall	2	<input checked="" type="checkbox"/>	
	Power supply on UPS for each firewall	-	<input checked="" type="checkbox"/>	
IP Addresses	Public IP fixed by operators (f29)	-	<input type="checkbox"/>	To provide
Provider's ports	Ports should be on Access Mode	-	<input type="checkbox"/>	



**FICHE D'ÉVALUATION DE STAGE**  
**DUT Réseaux et Télécoms - 2021**

À faire parvenir en fin de stage (au plus tard la veille de la soutenance) à : [carole.pitot@umontpellier.fr](mailto:carole.pitot@umontpellier.fr)  
ou bien par l'intermédiaire de l'étudiant ou du tuteur

*Elle doit être remplie (si possible en présence de l'étudiant) par la personne qui a suivi l'étudiant  
(entourez ou mettez en gras ou surbrillance le nombre correspondant à votre appréciation)*

Entreprise : BEL S.A .....

Etudiant : Samuel Laforge .....

Maître de stage : Arnaud Barbosa-Leclercq.....

**A/ Le travail réalisé** Évaluer la qualité des produits et services réalisés

• **respect des cahiers des charges, pertinences des solutions techniques proposées, tests effectués...**  
parfait = 6 5 4 3 2 1 0 = inexistant

Réinitialisation des Switch, préparation de la migration SDWAN, Configuration des bornes Wifi

• **qualités fonctionnelles, ergonomiques, esthétiques...**  
parfaites = 6 5 4 3 2 1 0 = nulles

**B/ La formation R&T**

La formation R&T vous semble-elle répondre à vos besoins en termes de compétences ?

Formation en parfaite adéquation avec les projets confiés

La durée du stage vous semble-t-elle adéquate ?

Très bien





C/ L'étudiant/e Évaluer l'attitude et les capacités du/de la stagiaire

**Qualités « personnelles »**

- ponctualité, assiduité, qualités relationnelles, fiabilité, disponibilité, qualités d'expression, curiosité...

parfaites = 6 5 4 3 2 1 0 = nulles

Commentaire

**Qualités « professionnelles »**

- connaissances techniques, méthode et organisation, créativité, capacité d'analyse, capacité de synthèse...

parfaites = 6 5 4 3 2 1 0 = nulles

Commentaire

**D/ Appréciation globale**

Merci de proposer une appréciation du type :

- stagiaire de grande valeur
- ...

Samuel a été d'une grande aide à la préparation et l'audit des sites pour la migration SDWAN.



### E/ Autres

Souhaiterez-vous accueillir un ou plusieurs stagiaires l'année prochaine ?

Si vous êtes assujetti, souhaitez-vous contribuer à la qualité de la formation de l'IUT de Béziers par le biais de la Taxe d'Apprentissage ?

Dans ce cas, merci de nous transmettre les coordonnées du responsable de la Taxe d'Apprentissage dans l'entreprise (prénom et nom, email, n° de téléphone...)

L'IUT accueille quatre départements (réseaux, commerce, multimédia, action sociale).

Si vous souhaitez des informations complémentaires, merci de nous transmettre les coordonnées du responsable des ressources humaines (prénom et nom, email, n° de téléphone...)

Date, signatures, cachet de l'entreprise :

28/07/2011

  
**BEL**  
S.A. Capital 10 308 502,50 €  
2 Allée de Longchamp – 92150 SURESNES  
Tél. : 01 84 02 72 50  
SIREN 542 088 067 - RCS NANTERRE – NAF 1051 C  
-9-