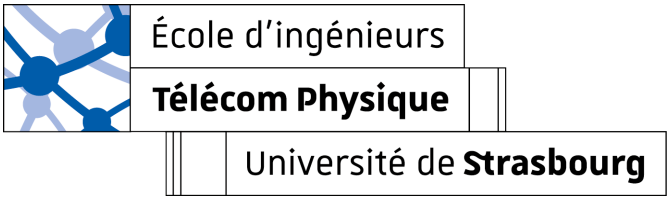

3A INOC - Groupe 4

Mise en oeuvre des réseaux

Equipe :
Loubna Hennach
Elisa Scheer

Enzo Dibella
Martin Médaillon

Octobre 2018

Sommaire

1 Introduction

L'objet de ce document est de présenter la solution proposée par l'équipe Foxtrot de restructuration du réseau de l'entreprise Weeloo. En effet, l'entreprise Weeloo souhaite restructurer son réseau et mettre en place un datacenter nouvelle génération. Pour ce faire, elle alloue un budget de 300000 pour la mise en place ainsi que 15000 mensuels.

1.1 Présentation du projet

Le projet Foxtrot vise à améliorer le réseau de l'entreprise Weeloo spécialisée dans les NTIC. Les différents sites de Weeloo présentent des profils très différents. L'entreprise fait un usage intensif du réseau et les différents sites ont des besoins multiples. Le réseau régional en question est organisé ainsi : d'un coté les 2 bâtiments centraux, de l'autre des bureaux d'études, centres de R&D, usines de production plus ou moins dispersées dans la région. Il s'agit dans le cadre du projet Foxtrot de moderniser et améliorer le réseau de Weeloo ainsi que des sites. Il faudra pour cela bien évaluer les besoins et travailler en accord avec les administrateurs locaux.
Les objectifs qui ont été fixés par la présidence sont les suivants :

- Rationaliser le réseau et augmenter le débit en tenant compte des besoins des utilisateurs.
- Assurer la sécurité et la confidentialité des données.
- Assurer une fiabilité forte du réseau et des données (sauvegardes).
- Créer une architecture pouvant répondre facilement à d'éventuelles évolutions (financières, techniques, politiques ...)
- Permettre la mobilité des personnels.
- Rationaliser le système d'information de Weeloo.
- Proposer une architecture pour le siège de l'entreprise avec la création d'un datacenter.

1.2 Présentation de l'équipe Foxtrot

L'équipe est composée de 4 membres ayant chacun un rôle défini pour la mise en place du nouveau réseau :

- Enzo Di Bella (Pierre Rapide) : responsable de l'enveloppe budgétaire qui a été confiée.
- Martin Médaillon (Jean Bono) : responsable de la sécurité.
- Elisa Scheer (Philippine Pasgeek) : responsable de la fiabilité.
- Loubna Hennach (Laurence Moinsdrole) : responsable du débit et Data Center.

1.3 Schéma réseau physique

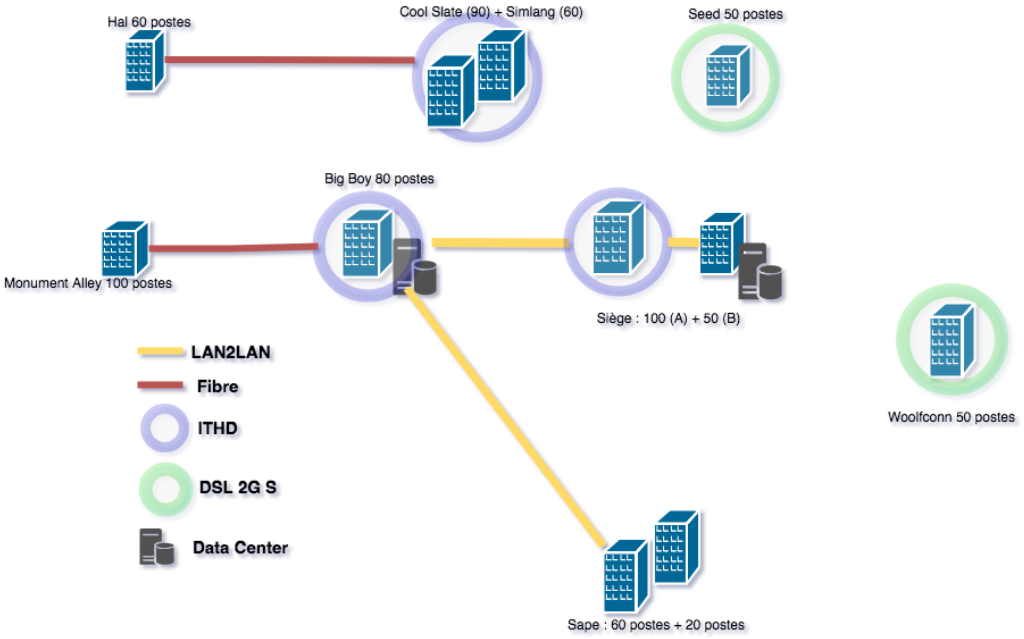

FIGURE 1 – Schéma réseau physique (OSI1)

1.4 Schémas réseau logique & adressage

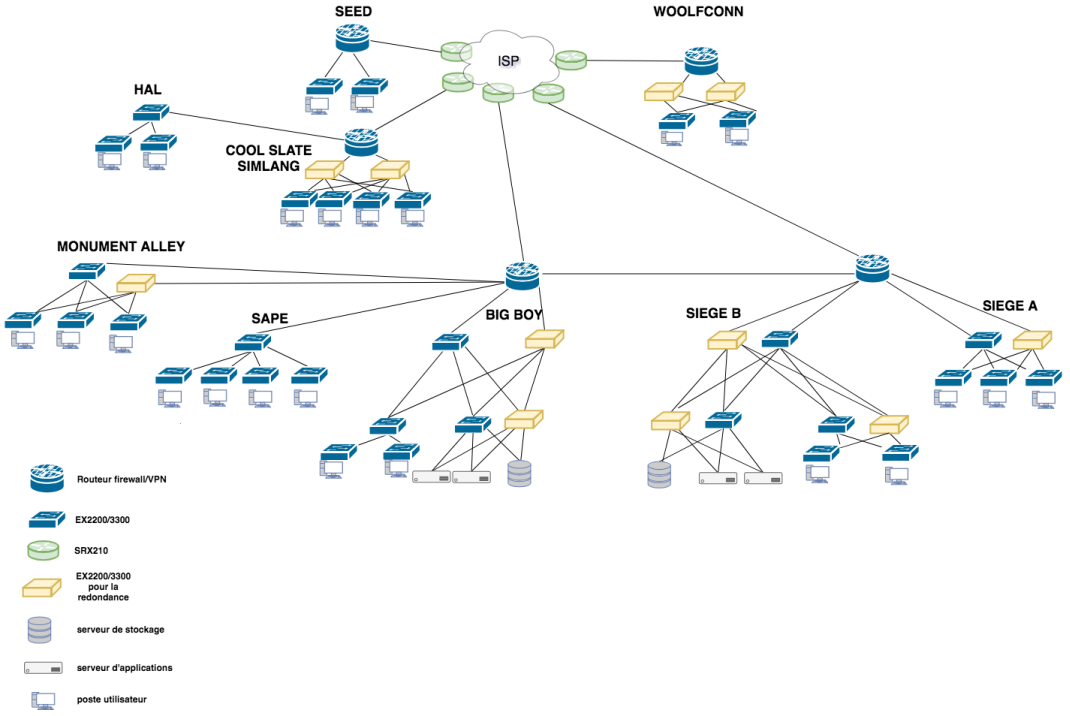

FIGURE 2 – Schéma réseau logique (OSI2/3)

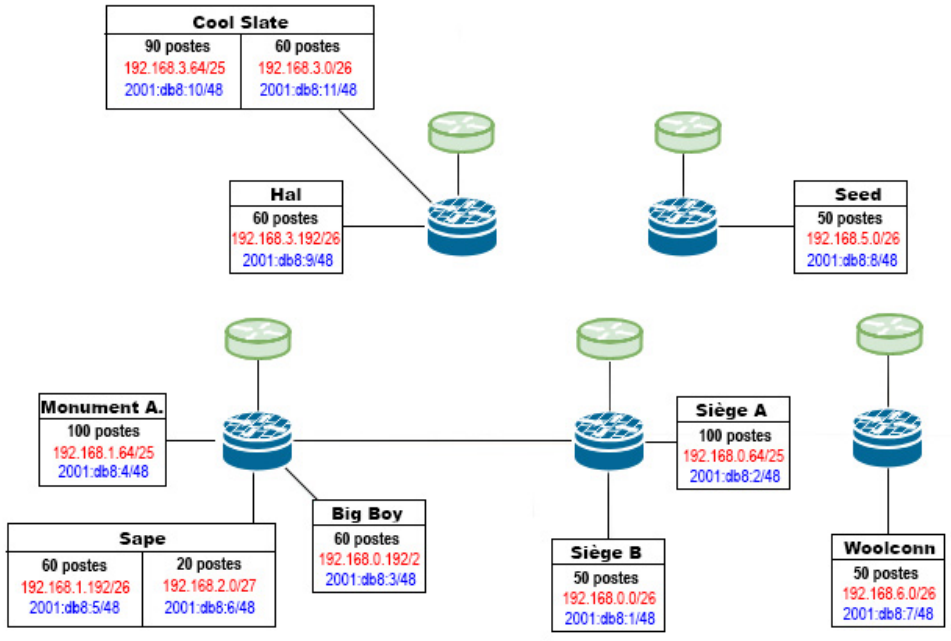

FIGURE 3 – Schéma adressage IPV4/IPV6)

2 Budget

Mon rôle dans l'équipe est de superviser les choix des autres membres dans le but de m'assurer que le budget soit respecté tout en affectant le moins possible la qualité finale du projet.

2.1 Budget Global

Au niveau global, des choix ont dû être faits pour s'assurer que les différentes parties du projet ne disposent pas d'une part trop inégale. En effet il fut dans un premier temps important de répartir le budget initial et le budget mensuel en fonction des besoins de différents types.

2.1.1 Vue générale

Il convenait d'abord d'avoir une idée générale de l'ordre de grandeur des dépenses ainsi que de leus origines. Pour cela il convenait bien évidement de s'informer des besoins des différents sites, mais surtout de connaître les tarifs des différents organismes.

Avec une analyse rapide des différents documents et notamment des offres Boostor et Cablotin il devenait évident que si Boostor était clairement bien plus coûteux au niveau du prix mensuel que de l'installation. Cablotin était en revanche plus mixte là-dessus. La raison à cela étant que si le prix du raccordement de la fibre était exclusivement à payer sur le budget d'installation, le prix de location en revanche pouvait être choisit selon deux systèmes. Il fallait donc non seulement décider de la quantité de budget à allouer aux fibres, mais également choisir la manière de le dépenser.

En choisissant les offres Boostor et Cablotin il fallait également prendre en compte que chaque choix à ce niveau impliquait également un achat d'équipements futurs qui allait directement s'ajouter au prix de l'installation. Les dits équipements incluaient à la fois les différents routeurs et switchs mais aussi les serveurs et les pare-feux.

En prenant toutes ces potentielles dépenses en compte il était extrêmement improbable que le budget de base permettent d'obtenir une solution optimale, fort heureusement un prêt nous fut proposé.

2.1.2 Choix du prêt

A cet effet le prêt mis en place avec le soutient de monsieur Goissé fut d'une importance capitale. Il était nécessaire de décider à combien il allait devoir s'élever. Un prêt trop important aurait mis en péril le budget mensuel nous empêchant de sélectionner les offres Boostor les plus intéressantes, mais un prêt trop faible ne nous aurait pas permit d'obtenir

le budget nécessaire au raccordement de notre réseau ainsi qu'à l'achat d'équipements efficaces.

Une fois la possibilité du prêt présente, la première grande décision fut le choix de prendre la proposition de location sur 15 ans payable à la livraison plutôt que de choisir la livraison mensuel. La raison de ce choix est assez simple :

— Le prêt nous a permit de récupérer 627605 euros, parmi ceux là la location sur 15 ans ne nous a coûté que 442736 euros le prêt couvre donc amplement cette location et d'autres achats supplémentaire, le tout pour 4610,93 euros par mois.

— La location mensuel aurait elle de son côté coûté 7906 euros par mois pendant 15 ans. Bien que n'ajoutant aucun prix d'installation.

On constate donc aisément que les deux budgets que ce soit celui à l'installation ou le mensuel bénéficient très largement de la présence du prêt et du choix de payer la location sur 15 ans à la livraison. La décision a donc été prise de choisir le prêt le plus élevé possible avec la marge laissée par les dépenses mensuelles estimées.

2.1.3 Méthode globale choisie

En prenant en compte l'existence du prêt il devenait donc envisageable d'obtenir une solution viable sur ce projet. Pour cela il fallait à la fois trouver un bon équilibre entre les avantages donnés par le prêt pour les dépenses d'installation et les dépenses mensuelles.

L'équilibre choisit fut d'allouer au maximum 5000 euros de dépenses mensuelles au prêt permettant ainsi de couvrir les dépenses d'installations ainsi que la locations sur 15 ans des fibres tout en gardant suffisamment de budget de côté pour l'achat des équipements avec une redondance respectable.

Ce choix nous permit également de conserver assez de budget mensuel pour la mise en place d'un LAN2LAN et de trois ITHD, ce qui permit un service qu'il soit au niveau filaire ou réseaux acceptable sans pour autant dépasser le budget initial.

2.2 Budget d'installation

2.2.1 Idée générale

Il est claire que le budget d'installation est alloué en majorité à Cablotin, que ce soit au niveau des raccordement commandés au génie Civil ou au niveau de la location sur 15 ans des fibres optiques. Mais il ne faut pas non plus négliger l'importance du budget laissé aux équipements qui reste considérable. Au total les dépenses en locations sur 15 ans se sont donc élevés à 442736 euros soit environs 47 pourcent du prix final à l'installation. Cependant ce prix peut difficilement être donné par sites étant donné qu'il s'agit de liens entre eux, on pourra simplement dire que les seuls sites n'étant impliqué dans aucune

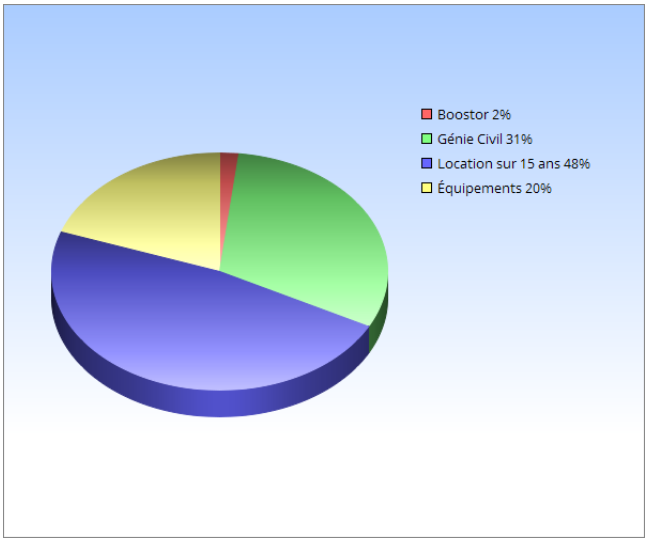

FIGURE 4 – Graphique du Budget à l'installation

location de fibre sont Woolfconn et Seed tout deux isolés et n'utilisant que l'xDsl couplé à un VPN pour une communication sécurisée avec le reste de l'entreprise.

Au niveau du budget Cablotin la grande majorité des sites ont nécessités un raccordement par le Génie civil. Cette dépense a beaucoup influencé certaines autres décisions étant donné que le choix de raccorder ou non un site jouait à la fois sur la possibilité de le relier par câble aux autres sites mais aussi sur la possibilité de l'équiper en ITHD. C'est pour cette raison notamment que Seed n'a pas été équipé en ITHD malgré la possibilité de le faire, en effet si la dépense ITHD pour Seed était réalisable, son raccordement en revanche aurait ajouté une dépense trop importante en surplus.

En plus du coût de raccordement il convient également d'ajouter pour chaque site son coût en équipement pour avoir une idée de la dépense réalisée. Sans oublié les éventuelles dépenses de mise en service des offres Boostor quand bien même comme nous pouvons le voir sur le graphique ci-dessus, elles sont bien souvent négligeables par rapport aux autres dépenses d'installation.

2.2.2 Présentation par sites

— **Siège Bâtiment A** : Le Siège A étant porteur de l'une des connexion ITHD son coût en équipements allait naturellement être assez élevé. Cependant cette dépense a été compensée par la remise offerte par Cablotin, permettant d'économiser sur le raccordement.
Prix des équipements : 9901 euros
Prix du raccordement : offert
Boostor : 3500 euros + installation LAN2LAN vers Big Boy 4000 euros

— **Siège Bâtiment B** : Bien que le siège B ne possédant pas de connexion ITHD, la présence du datacenter principal rendait le coût en équipement bien plus élevé de manière inévitable. Il était donc normal de consacrer quasiment 30 pourcent du budget équipement à ce lieu.
Prix des équipements : 43811.97 euros
Prix du raccordement : offert
Prix Boostor : installation LAN2LAN vers Siège A 4000 euros

— **Big Boy** : Tout comme le siège B, Big Boy est porteur d'un datacenter. De plus il ets également central pour la zone principal reliée par la fibre optique étant donné qu'il est connecté au siège, à Sape et à Monument Alley. En ajoutant à cela le fait que Big Boy est également porteur de la seconde connexion ITHD la plus importante, il était tout à fait logique d'allouer une grand partie du budget en équipement non seulement à sa mise en place mais également sa redondance. Environs 35 pourcent du budget équipement lui a été alloué, en y ajoutant la présence du raccordement, cela en fait aisément le site le plus cher, mais son importance justifie aisément ce coût.
Prix des équipements : 55676.97 euros
Prix du raccordement : 62000 euros
Prix Boostor : 3500 euros + installation LAN2LAN vers Sape offerte

— **Sape** : Sape n'a pas été si coûteux de base, cependant la nécessité d'une puissante liaison avec Big Boy pour optimiser leurs gigantesque transferts de données a justifié un budget un peu plus important que pour la moyenne des sites de cette importance.
Prix des équipements : 14995 euros
Prix du raccordement : offert

— **Monument Alley** : Monument Alley fut un choix difficile. En effet étant donnés que leur serveur de jeu seront déplacés à Big Boy (ce que je détaillerai plus tard) il y avait des raisons de débattre de l'utilité du raccordement fibre. Ce débat était également renforcé par le fait que le raccordement sur une distance importante en milieu urbain était particulièrement coûteux. cependant le fait que le dit site gagnait en importance et en taille aussi rapidement nous a motivés à le lier à Big Boy par une fibre. Cette décision a donc impliqué des équipements avec une certaines portée et en grand nombre étant donné que le bâtiment accueillera 100 postes d'ici peu.
Prix des équipements : 11029 euros
Prix du raccordement : 96000 euros

— **Hal** : Hal était un cas assez contraignant, malgré sa grande distance du point de raccordement fibre impliquant un grand prix de Génie Civil et des équipements à grande portée donc coûteux, le xDsl n'était cependant pas une solution pour des raisons de prix. nous avons donc dût nous résoudre à le relier à Cool Slate pour les faire partager un ITHD évitant ainsi de faire don d'une connexion aussi coûteuse uniquement pour un petit site comme Hal. Mais le prix final reste important par rapport à la taille du site, bien que nécessaire.
Prix des équipements : 6001 euros
Prix du raccordement : 115600 euros

— **Seed** : Seed comme Woolfconn n'étant équipé que d'une liaison xDsl, les dépenses furent simple à mettre en place. Ils seront donc équipés simplement du nécessaire en équipement pour une telle connexion avec VPN.
Prix des équipements : 3149 euros
Prix du raccordement : Pas de raccordement
Prix Boostor : 1000 euros
— **Woolfconn** : De même que pour Seed, le simple équipement nécessaire pour la connexion mais avec un peu plus de redondance en raison de sa position de site de production.
Prix des équipements : 5095 euros
Prix du raccordement : Pas de raccordement
Prix Boostor : 1000 euros
— **Cool Slate** : Cool Slate est devenu un emplacement stratégique très intéressant dès l'instant où les possibilités de fermetures ont été infirmées. En effet non seulement le site a grandement augmenté en taille en absorbant Simlang mais en plus son placement nous a permit de le faire partager sa connexion ITHD avec Hal sans trop de soucis. Enfin son prix de raccordement étant relativement peu onéreux, le relier en fibre à Hal et en ITHD a été plus facile à gérer.
Prix des équipements : 11326 euros
Prix du raccordement : 12500 euros
Prix Boostor : mise en place de l'ITHD offerte

2.3 Budget mensuel

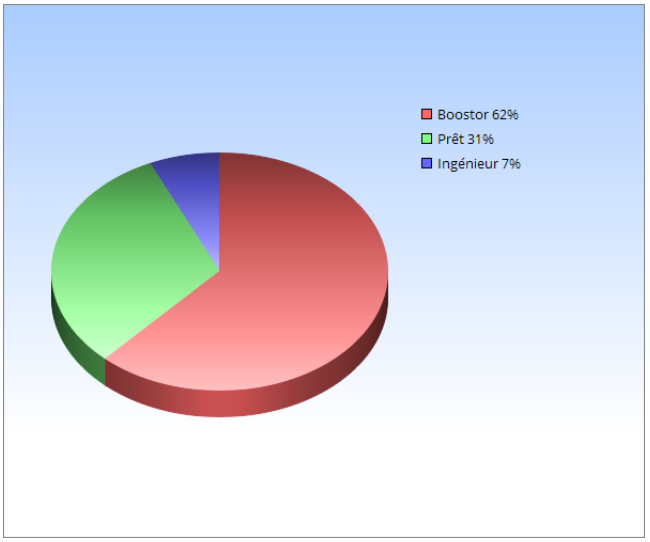

FIGURE 5 – Graphique du budget mensuel

2.3.1 Idée générale

Le prix mensuel est essentiellement composé de trois choses :
- Les offres Boostor
- Le remboursement du prêt
- La prime pour l'ingénieur chargé de la mise en place du datacenter

En prenant en compte ces trois dépenses, il est bien plus logique d'estimer le prix des sites par zones plutôt que par site. En effet le prix de certains sites est directement lié à la présence d'un autre, notamment les sites comme Monument Alley ou Sape qui en soit ne génèrent aucune dépense, mais qui en réalité sont dépendant des dépenses générés par les connexion ITHD du Siège et de Big Boy ainsi que par les dépenses du LAN2LAN dans le cas de Sape.

Je vais donc traiter ces dépenses mensuelles pour chaque zone tout en les justifiant autant que faire se peut.

2.3.2 Présentation par sites

- **Siège A et B / Big Boy / Sape / Monument Alley** : Ces quatre sites constituent le backbone central de l'entreprise et sont donc équipés en conséquences avec deux connexions ITHD de `50Mb/s` au niveau de Big Boy et de Siège A, mais aussi d'un service LAN2LAN entre Les deux sièges, Big Boy et Sape. Les dépenses alloués à cette partie sont donc conséquentes mais nécessaires étant donné son importance.
  Dépenses mensuelle : 6700 euros par mois + 1000 euros de paiement pour l'ingénieur
- **Seed** : En raison de son fort coût de raccordement à la fibre, il a été décidé que Seed ne serrait équipé que de la meilleurs offre xDsl disponible à savoir le DSL 2G S : 2048kbit/s. Il ne coûte donc que relativement peu par rapport à la zone centrale.
  Dépenses mensuelles : 600 euros par mois
- **Woolfconn** : Même constat que pour Seed à la différence que le choix a été fait en prenant en compte que de toute manière les besoins de Woolfconn n'étaient pas si élevés en terme de débit.
  Dépenses mensuelles : 600 euros par mois
- **Cool Slate / Hal** : Étant donné la prise d'importance de Coolslate ainsi que l'impossibilité de relier Hal au reste du réseau par un simple xDsl il a été décidé que la solution la plus abordable était de leur faire partager une connexion ITHD de 20 `20Mb/s` de manière à fournir une connexion à Hal pour ses quelques besoins, tout en donnant suffisamment de bande passante à Cool Slate pour ses futurs besoins.
  Dépenses mensuelles : 1200 euros par mois

2.4 Autres décisions budgétaires

Pour conclure sur le budget il est important de noter les quelques autres décisions budgétaires qui ont indirectement affecté les choix et les prix des différents sites.

La première fut le choix de déplacer les serveurs de jeux localisés à Monument Alley vers Big Boy. En effet ce choix est assez simple à expliquer mais capital. Des serveurs de jeux demandent une puissante connexion vers internet, il fallait donc que Monument Alley en dispose. Et techniquement c'est le cas grâce à la fibre posée entre le site et Big Boy on pouvait considérer que Monument Alley disposait d'une telle connexion. Cependant quand on considère que la fibre entre Monument Alley et Big Boy est une fibre aérienne qui mettrait donc éventuellement plus d'une journée à être réparée en cas de panne, on arrive donc à un risque de panne inacceptable pour ce genre de service. la solution subsidiaire aurait été de placer la connexion ITHD a Monument Alley mais dans ce cas une panne de ce câble aurait entraîné une perte de connections considérable pour les trois autres sites bien plus importants en taille ce qui n'aurait pas été appréciable non plus. Il fut donc décider de profiter du bon débit et des pare-feux performants de Big boy pour tout simplement placer les pare-feux sur place.

La seconde décision importante au niveau pratique pour éviter d'avoir à donner une connexion gigantesques à Hal envers tous les sites sera de centraliser les ISO produit par Hal dans les Datacenters. De cette manière plutôt que d'avoir faire communiquer ces données confidentielles de nombreuses fois en partant d'un site difficile à connecter, un seul transfert serra nécessaire depuis Hal vers les Datacenters d'où les autres sites pourront aisément récupérer les données sécurisées.

3 Sécurité

L'objectif de la sécurité est de mettre en place des moyens afin d'éviter des failles au sein du réseau. Ces failles peuvent prendre différentes formes en fonction de l'attaque portée sur le réseau, allant des attaques de déni de service au vol d'informations par un agent ou un "man in the middle". Afin d'éviter ce type d'attaque, différent moyens on été mis en oeuvre et vont vous être expliqués ci-dessous.

3.1 VLANS

Les VLANs permettent de séparer différentes parties au sein d'un réseau de niveaux 2 du modèle OSI (Liaison), les deux réseaux ainsi séparés ne peuvent plus se contacter à moins d'avoir recours à un équipement de niveau supérieur. Ainsi les VLANs permettent de restructurer un réseau déjà existant. Leur utilité n'est plus à démontrer et rare sont les réseaux d'entreprise qui n'en utilise pas pour gérer un flux d'administration.

Lors de la mise en place du réseau de Foxtrot, l'une des priorités fut la sécurité, hors afin d'établir des règles efficaces de sécurité, il est nécessaire de préalablement dissocier les différentes parties du réseau. Pour ce faire, différents VLANs ont été mis en place au sein du réseau comme le résume le schéma de la figure 6. Celui-ci ayant une vision simplifiée des équipements de niveau 2 afin de ne pas alourdir la compréhension.

Les VLANs sont ici présentés via des liaisons d'une couleur autre que le noir (le noir une liaison sans VLAN). On constate ainsi que de nombreux sites tels que Seed, Woolconn et Hal n'ont pas eu à être répartis sur un VLAN. Cela se justifie en regardant l'agencement de l'équipement réseau, qui séparait déjà ces différents sites jusqu'au pare-feu. En revanche, une distinction a été faites entre les employés et les serveurs se trouvant sur les sites Big Boy (respectivement rouge et rose) et le Siège B (respectivement cyan et rose) et entre les différentes populations de Cool Slate (rouge et bleu) et Sape (rouge et vert). L'utilité de cette distinction sera expliquée plus tard.

Pour finir, deux VLANs ont été mis en place à des fins d'administration (de couleur bleue et orange). Le VLAN de couleur bleue permet d'identifier les postes chargés de l'administration (soit Bruno Geheme à Big Boy et l'équipe informatique du Siège B). Le VLAN orange quant à lui permet l'accès aux serveurs.

3.2 Pare-feu

Le pare-feu (ou firewall en français) est un outil clef pour établir de la sécurité dans un réseau. Celui-ci permet d'appliquer des règles afin de filtrer les différents paquets le traversant, permettant ainsi de bloquer les intrusions. Pour ce faire, l'équipement a besoin d'être équipé à la fin du réseau, afin de s'assurer que les paquets à risques transitent bien par celui-ci. Dans l'architecture de Foxtrot sa position est de choix puisqu'il est présent

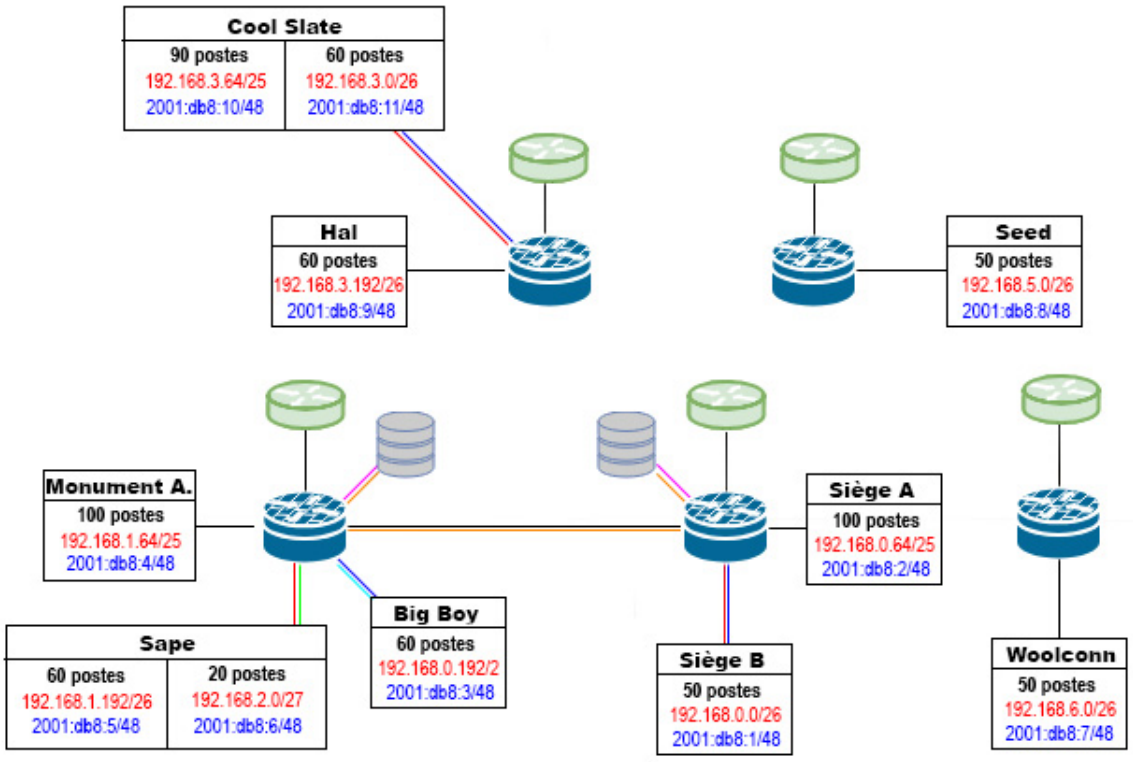

FIGURE 6 – Répartition des différents VLAN au sein du réseau

entre tous les sites utilisés entre les utilisateurs, les serveurs et internet. De plus, sa position lui permet d'analyser tous les paquets envoyés entre différents sites ou population de site.

Le pare-feu choisit provient de la marque Palo Alto Network réputé pour sa simplicité d'exécution ainsi que sa vision d'ensemble. Ce choix a été fait car il s'agit d'un des leader du marché et afin de préserver une sécurité optimale tout en respectant l'équipe informatique qui n'a jamais eu à travailler avec ce type de matériel au sein de l'entreprise. Le modèle a quant à lui a été choisi afin d'avoir les ressources nécessaires pour le réseau (voir PA5220 sur le tableau ci-dessous) et en obtenant les fonctionnalités présentées dans les sections suivantes.

Concernant les règles appliquées au pare-feu, sa politique par défaut sera de refuser tous les paquets. Pour les requêtes venant de l'extérieur dont l'adresse IP n'est pas enregistré, seul les messages vers l'adresse IP du serveur de jeu présente sur les machines virtuelles des serveurs sera disponible (en utilisant bien entendu le port adéquat uniquement). Si l'adresse IP correspond à l'un des équipements mobiles de nos agents, celui-ci sera rédigé vers le portail captif (voir section suivante), ce qui lui permettra d'avoir accès au réseau interne. Il possédera alors le droit d'accès aux serveurs en tant que client. Cela permettra

Capacités et performances	PA-5280	PA-5260	PA-5250	PA-5220
Débit du pare-feu[1] (App-ID activé)	68 Gbit/s	68 Gbit/s	39 Gbit/s	18 Gbit/s
Débit de la prévention des menaces[2]	30 Gbit/s	30 Gbit/s	20 Gbit/s	9 Gbit/s
Débit VPN IPsec	24 Gbit/s	24 Gbit/s	16 Gbit/s	8 Gbit/s
Nombre de sessions max.	64 000 000	32 000 000	8 000 000	4 000 000
Nouvelles sessions par seconde[3]	462 000	462 000	348 000	171 000
Systèmes virtuels (base/ max[4])	25/225	25/225	25/125	10/20

FIGURE 7 – Capacité et performances de la gamme PA5200

à l'agent de terrain de pouvoir accéder à ses mails et autres fonctionnalités proposées par le serveur dont ils ont utilité (voir les offres commerciales). En résumé, seul l'accès vers les serveurs est possibles depuis l'extérieur, cet accès étant décomposé en différents privilèges selon le type de connexion souhaitée. Les serveurs étant considéré comme une zone démilitarisée (DMZ). Il est à noter que les IP propre au VM contenant des données sensibles telles que les versions des OS développées par l'entreprise ne sont pas accessibles depuis l'extérieur.

Concernant les équipements utilisateurs appartenant au sous-réseau privé de l'entreprise, ceux-ci le droit d'utiliser les services clients proposés par les serveurs. Pour ce faire, les sites Sape, Monumment Alley, Big Boy, Siège A et Siège B ont un accès simple aux serveurs (en passant néanmoins par un pare-feu). Alors que les sites de Hal, Cool Slate Seed et Woolcoon en revanche se relie aux serveurs de l'entreprise en utilisant les VPN IPsec mit en place sur les pare-feux. Ainsi les données transitant en dehors de notre réseau sont cryptées.

Concernant les communications entre différent sites, celles-ci peuvent être gérées à l'aide des serveurs mis en place. Cependant, afin d'être sûr qu'aucune méthode de communication précédemment utilisé soit désormais inutilisable, les demandes concernant un besoin de trafic entre différent sites définit dans l'énoncer seront autorisées. À savoir les liens entre : Big Boy et le Siège, Big Boy et Sape, Monument Alley et le Siège, Sape et le Siège, Seed et le Siège, Seed et Monument Alley, Cool Slate (postes originaires de Simlang) et le Siège, Cool Slate (postes originaires de Simlang) et le Woolfcon, Cool Slate (postes originaires de Simlang) et Seed, Hal et le Siège, que Hal et Slate, Hal et Monument Alley ainsi que Hal et Woolfcoon.

Les connexions citées précédemment peuvent avoir d'autres besoins que le simple envoie de mail, comme les données envoyées quotidiennement entre Big Boy et le Sape. Cependant, afin de s'assurer que ces liens soient utilisés correctement, un questionnaire sera envoyé aux différents employés afin de connaître les besoins de ces connexions et de n'autoriser que les ports adéquats.

Pour finir concernant la configuration de base de ces pare-feux, ceux-ci possèdent un système de règles permettant d'éviter des attaques de type DOS (déni de service). Celle-ci sera activé sur chaque pare-feu sur le port le reliant au CPE (donc à l'extérieur du sous-réseau). Cette protection est d'autant plus nécessaire sur les pare-feu de Big Boy et le Siège car ceux-ci sont reliés au serveur contenant le site web de l'entreprise ainsi que les jeux mobiles.

3.3 Sondes IDS

Une sonde IDS est un dispositif permettant d'analyser le réseau et de prévenir les intrusions (exemple : Man in the Middle ou cheval de Troie). Ce type d'attaque se fait généralement par une vulnérabilité au sein de l'entrée d'une application. Une fois ce type d'attaque réalisé, l'attaquant possède les droits de l'équipement ciblé et peut donc porter préjudice. Afin d'éviter ce type d'attaque, la sonde a besoin de sonder les paquets envoyés au niveau applicatif. Si une attaque est détecté les actions possibles sont : un message est envoyé à l'administrateur ; le rejet du paquet concerné ; le blocage de l'adresse source ; et la ré-initialisation de la connexion.

Ainsi l'IPS est une analyse plus approfondit que celle effectuée par le pare-feu initialement, analysant les paquets du niveau 4 à 7 du modèle OSI afin d'éviter différents types d'attaques. Lors de la mise en place du réseau de foxtrot, il a été décidé d'utiliser un pare-feu "next-gen" afin de remplir ce rôle. Ce choix a été effectué car le besoin de sécurité était crucial pour l'entreprise qui a déjà subi plusieurs pertes de données auparavant. Le pare-feu permet par conséquent d'utiliser différentes méthodes afin d'éviter les intrusions, à savoir : App-ID, IPS, Antivirus, Anti-Spyware, WildFire. Celles-ci ont l'avantage d'être complètes et permettent même d'être à jour sur les "zero-day exploit" (dernières failles trouvés). Toutes ces méthodes sont donc à configurer sur chacun des pare-feux de l'entreprise.

Comme précisé précédemment, seuls les paquets transitant par le pare-feu peuvent être analysés par celui-ci. Les paquets échangés entre différents sites sont donc analysés, mais ceux échangés entre deux employés travaillant dans le même site non (puisque leurs paquets sont échangés au niveau 2 à l'aide des commutateurs). Ainsi afin de s'assurer qu'une attaque provenant de l'intérieur ne puisse pas s'étendre entre les différents pôles, il est nécessaire de faire en sorte que les différents paquets échangés entre deux pôles passent par le pare-feu. C'est pour cette raison que le site de Sape et Cool Slate possèdent respectivement deux VLANs : afin de séparer les deux pôles se trouvant sur chacun de ces sites. Ainsi si l'ordinateur d'un commercial se trouvant à Sape est corrompu, cette corruption ne pourra pas s'étendre aux développeurs se trouvant à Sape sans passer par le pare-feu.

Cette protection bien qu'importante, ne pourra pas être appliquée à tous les types de connexion entre les différents sites. La connexion entre Big Boy et Sape par exemple à besoin d'un débit particulièrement conséquent. Hors le débit permis par le pare-feu avec ce type d'analyse est de 9 Gbit/s, l'utilisation de ce type d'analyse sur ce lien fonctionnant à 8 Git/s saturerait les capacités offertes par le pare-feu (qui subit déjà les flux des autres sites ainsi que ceux dirigés vers les serveurs). Ce type de connexion n'utilisera donc pas les techniques de préventions des menaces et aura donc un débit supérieur : 18Gbit/s ce qui permettra de ne pas surcharger le pare-feu.

Afin de s'assurer que ces connexions privilégiées ne soient pas utilisées à mauvais escient, les postes pouvant en bénéficier seront identifiés à l'aide de leur IP, de leur adresse MAC et il leur sera également nécessaire de se connecter sur un compte ayant les droits adéquats (voir prochaine section).

3.4 Authentification forte

L'authentification permet comme son nom l'indique d'identifier la personne utilisant un équipement sur le réseau. Elle est fortement recommande en terme de sécurité puisqu'elle permet de déterminer les droits en fonction des identifiants utilisés. Cette identification est indispensable pour tout agent voulant se connecter depuis un équipement externe au sous-réseau. Cependant, même au sein du sous-réseau elle possède une grande importance : toute personne peut utiliser un ordinateur laissé à disposition ou simplement se brancher sur un port Ethernet libre. Ceci est une faille de sécurité élémentaire qui peut être atténuée par l'utilisation de l'authentification.

L'identification sera donc requise pour toute personne voulant se connecter sur le réseau. Celle-ci se fera à l'aide d'un portail captif généré par le pare-feu. Ainsi toute tentative de connexion établie dans l'enceinte du sous-réseau sans s'être identifiée préalablement sera renvoyé vers le portail. De même tout employé essayant de se connecter dans le sous-réseau à l'aide d'un équipement mobile enregistré sera envoyé sur le portail. Seuls les individus venant de l'extérieur et souhaitant uniquement utiliser les services jeux mobiles fournis par nos serveurs n'auront pas besoin de s'identifier préalablement.

Les mots de passe utilisés pour l'identification devront suivre les règles de sécurités suivantes : être changés tous les deux mois ; un nouveau mot de passe ne doit pas avoir été préalablement utilisé par le même utilisateur ; le mot de passe doit comporter aux moins 8 caractères, dont une majuscule, un chiffre et un caractère spécial.

Enfin, les utilisateurs seront répartis entre différents rôles, ainsi il sera facilement possible de savoir si un employé se soit connecté sur un équipement n'appartenant pas à son site à l'aide des identifiants utilisés. De plus, certaines connexions seront interdites pour la plupart des utilisateurs. Par exemple, seul un membre de l'équipe informatique (ou notre informaticien de Big Boy) aura le droit de se connecter via un des équipements reliés à l'aide du VLAN administrateur. Un autre privilège est celui d'utiliser un des équipements

qui permettent une connexion direct entre différent sites (sans passer par l'analyse IPS). Ainsi une gestion des utilisateurs doit être mise en place.

4 Fiabilité

Mon rôle au sein de l'équipe était de concevoir un réseau le plus fiable possible tout en respectant le budget imposé. Je devais également réfléchir à un système de sauvegarde et de haute disponibilité afin que les données de Weeloo ne soient pas perdues et que les services déployés aient une disponibilité maximale.

4.1 Redondance des liaisons

4.1.1 Redondance des liaisons physiques

Afin d'assurer un maximum la fiabilité dans le réseau, la meilleure option serait de doubler chaque lien afin de s'assurer qu'aucun site ne puisse perdre de connectivité avec les autres sites et en particulier le siège. Malheureusement, le budget imposé ne permettait pas de réaliser cela. C'est pourquoi notre architecture ne présente pas de lien doublé ni de boucle. En revanche, nous avons souscrit à l'offre LANtoLAN de Boostor qui inclut la redondance. En effet, si une liaison physique est coupée, le fournisseur s'occupera de rediriger le trafic pour l'acheminer à destination. Les données circulant entre Sape et Big Boy ainsi que les données transitant entre le siège B (comprenant le centre de données principal) et Big Boy (comprenant le centre de données secondaire) étant importantes, nous avons conclu que cette offre répondait à la problématique de redondance.

4.1.2 Redondance des liaisons réseaux

Afin de respecter le budget restant pour doubler au maximum les équipements réseaux, j'ai analysé les besoins de chaque site et me suis intéréssée au trafic circulant entre les différents sites (gros trafic, trafic de réplication de données...etc) :

— Le service production exigeant une haute fiabilité, les équipements au niveau des sites de Woolfconn, Monument Alley et Simlang (fusionné avec Cool Slate) ont été doublés.

— Les équipements du siège ont été doublés car c'est le site principal et il doit ´tre hautement disponible car le siège B héberge le centre de données principal.

— Les équipements du site Big Boy ont également été doublés car il héberge le centre de données secondaire.

Ainsi, si un équipement tombe en panne, seulement les postes reliés à l'équipement perdront leur connectivité mais le réseau sera toujours opérationnel. En revanche, dû au budget limité, nous n'avons pas pu satisfaire l'ensemble des sites au niveau de la redondance.

4.2 Niveau de fiabilité par site

Voici un tableau récapitulatif du niveau de fiabilité par site :

Site	Besoins en débit
Sièges	fiable
Big Boy	fiable
Monument Alley	fiable
Sape	peu fiable
Woolfconn	fiable
Seed	peu fiable
Simlang	fiable
Hal	peu fiable
Cool Slate	fiable

FIGURE 8 – Récapitulatif solution fiabilité

4.3 Redondance du datacenter

Le centre de données étant la nouveauté dans l'entreprise, nous avons discuté avec William Gibson au niveau des besoins du datacenter. Il nous a expliqué que ce centre centralisera l'ensemble des données de l'entreprise et qu'il était éxigé de se pencher sur une solution de virtualisation de type IAAS. Mais également penser à toute l'architecture de sauvegarde afin de ne pas perdre de données en cas d'incident ainsi que de gérer le basculement en cas de panne.

4.3.1 Redondance au niveau du système de stockage

Afin d'améliorer la performance du serveur de stockage, nous avons choisi un NAS qui supportent des contrôleurs de type RAID 0, 1, JBOD, 5, 10, 6. Les serveur NAS que nous avons choisis sont équipés de 16 disques d'une capacité de 14To. Nous avons opté pour la technique RAID 5 car après la perte d'un des disques, nous sommes capable de reconstituer le disque défaillant à partir des 3 autres. Bien que le RAID réduise la capacité de stockage totale, il assurera une haute redondance des données. Le serveur supportant également

le changement à chaud d'un disque, nous placerons donc 5 disques dont 4 utilisés pour l'écriture des données et un passif qui sera utilisé en cas de panne d'un des disques.

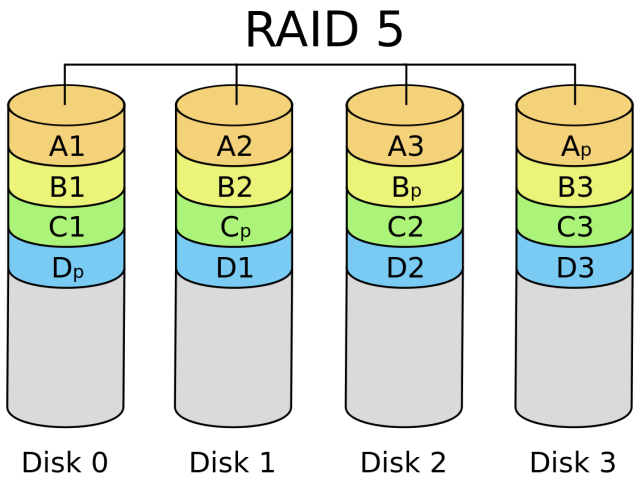

FIGURE 9 – Principe du RAID 5

La disponibilité du serveur NAS est cruciale car si l'on perd un serveur, on perd l'ensemble des données. L'objectif sera donc de répliquer les données d'un serveur à un autre en temps réel, mais également mettre en place un cluster afin de pouvoir basculer rapidement vers le serveur en marche en cas de panne. Voici donc la solution proposée :
Nous proposons donc de mettre en place un système de stockage principal dans le centre de données principal et un système de stockage de secours dans le centre de données secondaire.
Afin de pouvoir mettre en place le cluster, nous proposons d'utiliser :

— Corosync et Pacemaker (licence GPL) qui permettent de mettre en place et gérer le cluster et donc le basculement en cas de panne.
— DRBD (licence GPL) qui gère la synchronisation des données entre les deux serveurs en temps réel.

Bien que le RAID assure la haute redondance des données, il ne permet en aucun cas de sauvegarder ses données. Et en dehors de la perte d'un disque, nous pouvons faire face à des incendies, virus ou effacement accidentel (erreur humaine). C'est pourquoi avoir un disque NAS de secours qui réplique les données du NAS primaire permet d'avoir une haute disponibilité des données.

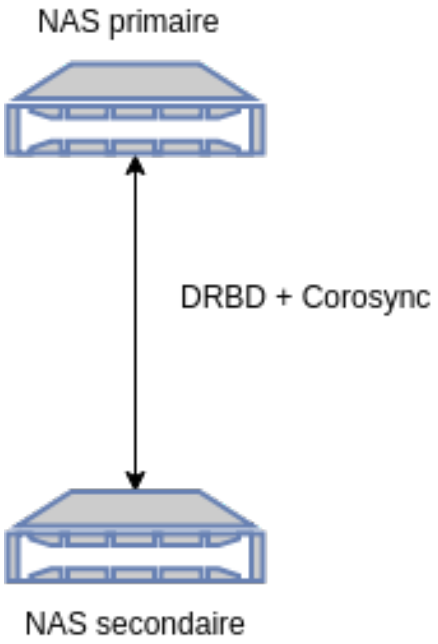

FIGURE 10 – Architecture de la solution

4.3.2 Système de sauvegarde

Afin d'éviter de perdre les données d'une VM, par exemple après une mise à jour qui pourrait rendre le serveur défaillant, il est nécéssaire de mettre en place un système de sauvegarde régulier afin de capturer l'état de la VM. Ainsi, en cas de défaillance, la VM pourra être restaurée. Cela revient à effectuer un snapshot de la VM, c'est à dire qu'à un instant t, l'état entier de la machine sera capturé (contenu de la mémoire virtuelle, ses paramètres, état des disques virtuels), cela va permettre de créer des points de restauration pour revenir dans le temps. Afin de pouvoir réaliser cela, un agent de sauvegarde devra être installé sur l'hyperviseur : Open Nebula, qui sera décrit dans le chapitre Débit & Datacenter, permet la sauvegarde des VM qui se trouve sur un hyperviseur.

4.3.3 Cluster de virtualisation KVM

Un cluster de basculement est une architecture composée de plusieurs VM formant des noeuds, où chaque noeud est capable de fonctionner indépendamment des autres, il a pour objectif d'assurer la haute disponibilité et fonctionne selon le principe suivant :

Quand un des noeuds tombe en panne, un autre noeud du cluster prend le relais dans le but d'assurer la disponibilité des données ou des services.
Ainsi, la solution proposée est la mise en place d'un cluster actif/passif. C'est à dire que le serveur primaire possèdera l'adresse IP de référence et en cas de défaillance, le secondaire

prendra cette IP et deviendra le serveur principal. Ainsi, chaque VM associée à un service se trouvera dans un cluster spécifique à ce service. Pour mettre en place le cluster :

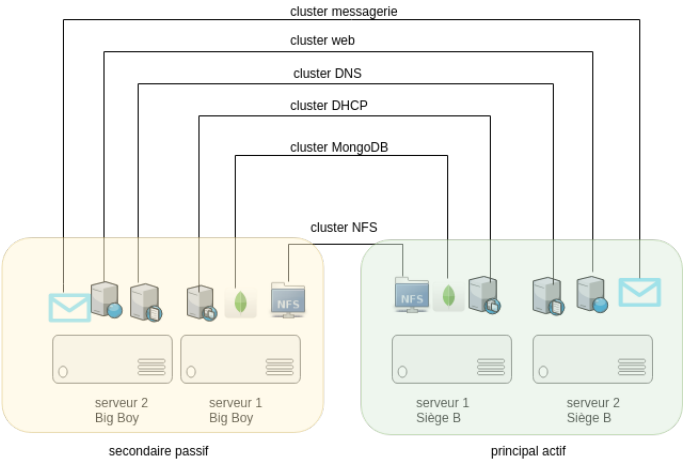

FIGURE 11 – Cluster de VM

— utilisation de corosync et pacemaker pour créer et gérer le cluster.
— DRBD pour la réplication des données.

4.4 Supervision des équipements

Afin que l'administrateur réseau puisse avoir une vue d'ensemble sur l'état des services et du réseau, nous proposons d'utiliser Nagios. C'est une application permettant la surveillance système et réseau. Elle surveille les hôtes et services spécifiés, alertant lorsque les systèmes ont des dysfonctionnements et quand ils repassent en fonctionnement normal. C'est un logiciel libre sous licence GPL. Ce système de supervision offrira à l'administrateur la possibilité de réagir le plus rapidement possible face aux pannes qui peuvent intervenir afin d'éviter un arrêt de production de trop longue durée. Nagios s'installera donc sur une VM primaire sur le siège B et une VM secondaire sur Big Boy. Il sera nécéssaire de définir les utilisateurs ayant droit d'accéder à l'interface web de Nagios, de définir les hôtes puis les différents services à surveiller.

5 Débit & Data Center

5.1 Débits choisis

Mon rôle dans l'équipe Foxtrot est essentiellement basé sur l'aspect débit. Le choix que j'ai pu effectué pour les différents sites a été fait après une étude détaillée des besoins et une communication directe avec les responsables des sites et en fonction des contraintes du budget imposé :

- **Siège** (100 postes Bâtiment A et 50 postes Bâtiment B) : le bâtiment B, hébergeant le Datacenter, est relié au siège A avec une liaison LAN2LAN qui assure un débit de `2Gb/s`. Ensuite nous avons équipé le siège A par l'ITHD (Internet Très Haut Débit) qui permet un accès à Internet très performant avec un débit de `50Mb/s`
- **Big Boy** (80 postes) : Nous avons élu ce siège pour être le site secondaire du Datacenter, hébergeant donc les seveurs de backup. Il a donc besoin d'un gros trafic vers le Siège. Nous avons relié Big Boy au siège avec un liaison LAN2LAN qui assure in débit de `2Gb/s`.Ce site étant également un grand centre de données spécialisées dans le big data et machine learning, il a besoin d'un très grand débit vers Internet. Nous l'avons donc équipé de l'ITHD avec un débit de `50Mb/s`. Aussi, Sape envoie quotidiennement 100 téraoctets de données vers ce site, nous avons donc choisi une liaison LAN2LAN entre Sape et ce site d'un débit de `8Gb/s`
- **Sape** (80 postes) : Ce site étant un centre d'intégration d'ERP (Entreprise Ressources Planning), il a besoin d'une forte connexion à Internet, par contrainte de budget nous n'avons pas pu l'équiper de l'ITHD, mais nous l'avons relié à Big Boy qui lui a l'ITHD d'un débit de `50Mb/s` avec un lien LAN2LAN de `8Gb/s`.
- **Monument Alley** (100 postes) : ce site développe des applications jeux pour tablettes et téléphones et a besoin d'un fort débit vert Internet. Nous avons choisi de le relier à Big Boy en fibre avec un débit de `1Gb/s` après avoir décidé de migrer leurs serveurs de jeux au site Big Boy pour faire des économies.
- **Hal** (60 postes) : ce site étant un centre de R&D dans les systèmes d'exploitation embarqués pour les terminaux mobiles et autres objets connectés, il a besoin de communiquer avec le siège et Cool Slate, nous avons donc choisi de le relier en fibre à Cool Slate qui lui est équipé de l'ITHD d'un débit de `20Mb/s`. Pour la communication avec Monument Alley et Woolfcoon, ce site passe par internet en utilisant un vpn.
- **Seed** (50 postes) : ce site étant un bureau de R&D ultra-secret qui conçoit les derniers smartphones et montres connectées du moment il a besoin d'une bonne connexion avec le siège, nous l'avons équipé d'une connectivité DSL 2G avec un débit de `2048Kb/s` et communique avec le siège au travers d'un vpn.
- **Woolfconn** (50 postes) : ce site est un site de production de smartphones, tablettes et autres objets connectés, nous avons choisi de l'équiper d'une connectivité DSL 2G avec un débit de `2048Kb/s`
- **Cool Slate** (90 postes) : ce site étant un centre de recherche, il a besoin d'un gros débit vers Internet, nous avons choisi de l'équiper de l'ITHD avec un débit de

`20Mb/s`.

— **Simlang** (60 postes) : c'est un site de production de composants électroniques de pointe. Il a migré dernièrement à Cool Slate. Il est donc doté de la même connectivité que ce dernier.

Site	Besoins en débit	Solution retenue
Sièges	gros débit	ITHD 50Mb/s
Big Boy	gros trafic vers Siège et Sape	ITHD 50Mb/s
Monument Alley	forte communication avec Siège	fibre <-> Big Boy migration de serveurs de jeu à Big Boy
Sape	forte connexion à Internet	LAN2LAN <-> Big Boy
Woolfconn	connexion à Internet site de production	DSL 2G S 2048Kb/s
Seed	communication gros débit avec Monument Alley	DSL 2G S 2048Kb/s
Simlang	communication gros débit avec Monument Alley	fusionne avec Cool Slate
Hal	Communication avec Siège et Cool Slate	fibre <-> Cool Slate
Cool Slate	gros débit vers internet	ITHD 20Mb/s

FIGURE 12 – Récapitulatif solution fiabilité

5.2 Outils de métrologie

La métrologie permet d'obtenir, de garder et de tracer la valeur numérique d'une charge. Par exemple le pourcentage de CPU utilisé sur un serveur, le nombre de personnes connectées sur le site web de l'entreprise, le trafic sortant et entrant sur un switch. Notre choix s'est porté sur le logiciel Cacti.
Cacti est un logiciel libre de mesure de performances réseau et serveur basé sur la puissance de stockage de données de RRDTool.Il permet de représenter sous forme de graphiques n'importe quelle donnée quantifiable collectée soit par le biais de protocoles réseaux tels que SNMP ou soit par des scripts personnalisés par l'utilisateur. Il est souvent utilisé avec des logiciels de supervision (par exemple Nagios).
Caractéristiques de Cacti :

— Licence : GPL
— Technologie : PHP

5.3 Data Center

Le centre de données (Data Center) regroupe les serveurs, les sous-systèmes de stockage, les commutateurs de réseau, les câbles et les racks physiques permettant d'organiser et d'interconnecter tous ces équipements informatiques.
Le bâtiment A du siège accueillera une partie du Data Center. Ce choix est dû au fait que le siège est le site central et tous les autres sites sont connectés à lui. Il répond également aux contraintes de disponibilité et de haute connectivité.
La deuxième partie du Data Center sera hébergée à Big Boy. Nous avons choisi un site différent du Siège pour accueillir la seconde partie du Datacenter, pour éviter, en cas de problème électrique au niveau du Siège, la perte des données de l'entreprise.

5.3.1 Serveurs Data Center

Nous avons choisi des serveurs rack, ces serveurs sont faits pour être rangés dans des armoires et permettent le changement à chaud des disques.
Les modèles que nous avons choisi répondent aux contraintes de haute disponibilité et haute performance. Nous avons opté pour un premier modèle rack 3U : le QNAP TDS-16489U qui fera office de serveur de stockage NAS.
Ce modèle de serveur combine la fonctionnalité de stockage haute capacité et la qualité de serveurs d'applications haute performance dans un seul boîtier. Cette solution nous a permis d'économiser plus d'argent et d'espace grâce à une solution unique dotée de performances d'applications et d'un TCO de stockage plus bas.
Nous avons donc équipé chaque partie du Datacenter de ce modèle de serveur de stockage et nous avons prévu 16 disques de 14To pour chaque serveur, ce qui fait une capacité totale de stockage de 448To.
Le deuxième modèle de serveurs qu'on a choisi est le serveur Rack 2U DELL PowerEdge R740 qui fera office de serveur d'application.
Ce modèle de serveur permet de simplifier et d'accélérer les déploiements de machines virtuelles, et offre de puissantes ressources de stockage et de traitement dans une plateforme 2U à 2 sockets.
Nous avons donc équipé chaque partie du Datacenter de deux serveurs de ce modèle, et nous avons également prévu du stockage en achetant 6 disques de 14To pour chacun des serveurs.

5.3.2 Sous-système de stockage

Le système que nous avons choisi pour le stockage au niveau du Datacenter est le NAS qui est un périphérique de stockage permettant de stocker et partager des fichiers au travers du réseau, les baies du NAS sont accessibles au travers de leur adresse IP via le protocole

de partage de fichiers NFS (Network File System) Nous avons équipés notre Datacenter

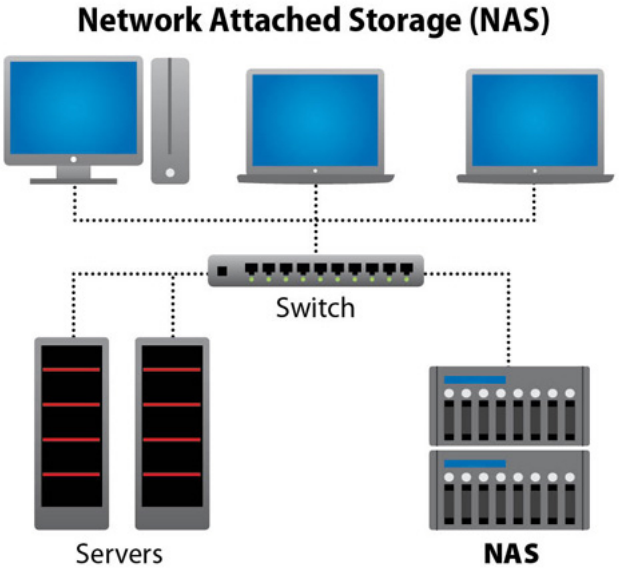

FIGURE 13 – Système de stockage NAS

de deux NAS distants ; le premier sur le siège B et le deuxième à Bigboy. Nos serveurs d'applications seront connectés aux serveurs NAS avec des switchs EX3300-24T comme le montre la figure 13, les serveurs NAS permettent ainsi de centraliser le stockage de l'entreprise et sont accessibles par les utilisateurs via le réseau.
Les NAS sont adaptés avec des fonctionnalités de stockage developpées, en effet, ils embarquent plusieurs disques durs travaillant en mode RAID 1 ou RAID 5 afin de faciliter la copie des données sensibles.

5.3.3 Outils de virtualisation

Nous utilisons une virtualisation Open Source :
Pour une virtualisation de type IAAS (Infrastructure As A Service) nous avons choisi le logiciel KVM qui est un hyperviseur libre de type I pour Linux permettant de créer et placer de nouvelles machines virtuelles. Un maximum de ressources peut être alloué aux machines virtuelles car ce type d'hyperviseur est directement lié à la couche matérielle. KVM est une technologie de virtualisation complète qui ne nécessite pas de modifications du système d'exploitation invité.
Nous avons également choisi OpenNebula comme outil de gestion de l'hyperviseur. C'est un logiciel libre et ouvert sous licence Apache qui fournit un ensemble de fonctionnalités permettant de gérer un cloud. OpenNebula organise le fonctionnement d'un ensemble de serveurs physiques, fournissant des ressources à des machines virtuelles. Il orchestre et

gère le cycle de vie de toutes ces machines virtuelles. Les composants de base d'un système OpenNebula sont les suivants :

— Interface qui exécute les services OpenNebula. (Front-End)
— Des hôtes activés par l'hyperviseur qui fournissent les ressources nécessaires aux machines virtuelles.
— les images de base des machines virtuelles. (Datastores)
— Les réseaux physiques utilisés pour prendre en charge des services de base tels que l'interconnexion des serveurs de stockage et les opérations de contrôle OpenNebula, ainsi que les VLAN des machines virtuelles.

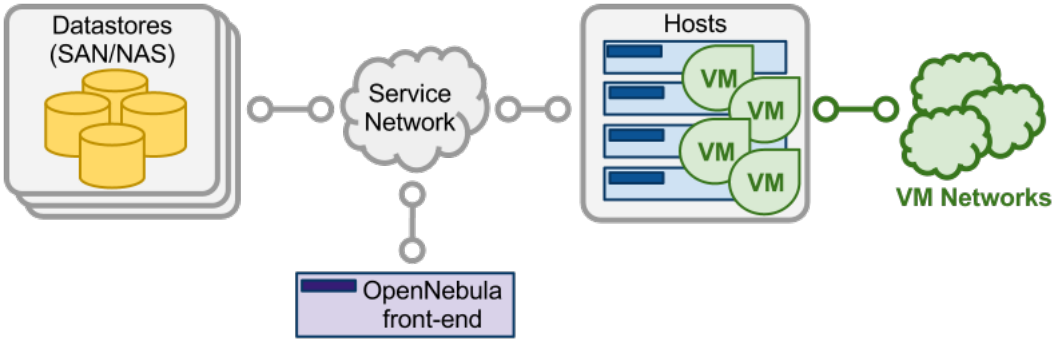

FIGURE 14 – Architecture OpenNebula

Dans notre Datacenter, Opennebula va gérer les machines virtuelles (VM) par le biais de l'hyperviseur KVM et en utilisant NFS comme système de fichiers. L'hyperviseur sera installé et activé sur les serveurs d'application du siège B et de Big Boy qui sont dans un même VLAN. Ensuite le Front-End d'OpenNebula sera installé sur une VM du siège B qui va accueillir la solution OpenNebula à travers les paquets Opennebula, Opennebula-sunstone (interface graphique destiné à l'administration d'opennebula),Opennebula-gate (collecter les paramètres et les problèmes sur les machines virtuelles qu'opennebula monitore) et Opennebulaflow. Les machines virtuelles des serveurs d'application du siège B et de Big Boy que le front-end opennebula va administrer sont les hôtes qu'on appelle Node Opennebula. Ainsi, à travers l'interface graphique web Sunstone d'opennebula on peut ajouter les hôtes, qui ont accès à Internet, pour les gérer.

5.3.4 Services pilotes

— Système de fichiers : notre choix s'est porté sur le NFS (Network File System) qui permet aux hôtes distants de monter des systèmes de fichiers sur le réseau et de les utiliser exactement comme des systèmes de fichiers locaux. Ceci permet à l'administrateur système de stocker des ressources sur les serveurs centralisés sur le réseau.

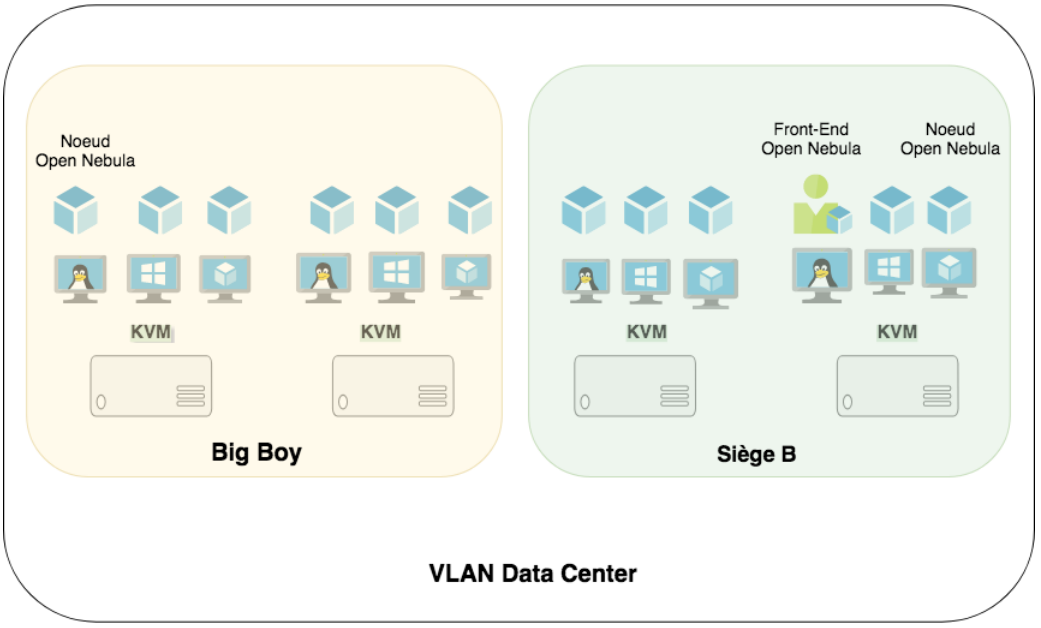

FIGURE 15 – Solution OpenNebula Datacenter

— Base de données : Pour le système de base de données, notre choix s'est porté sur MongoDB qui est un système de gestion de base de données NoSQL open source orienté documents. Il prend en charge des types de données très divers. Le modèle de données documentaire de MongoDB permet de stocker et de combiner des données, quelle que soit leurs structures, sans sacrifier l'accès à ces données ni leur indexation. Ainsi, les administrateurs de base de données peuvent modifier dynamiquement le schéma sans aucune interruption de service.
— Service de messagerie : développé par l'entreprise, il sera hebergé dans les serveurs d'application du Datacenter.
— Serveur HTTP Apache qui est aussi un logiciel libre.

6 Conclusion

Nous avons donc réussit autant que possible à respecter les demandes des différents sites sans pour autant dépasser le budget qu'il soit mensuel ou de départ. Tout en respectant ce dernier nous sommes également parvenus à fournir des solutions sécurisées d'interconnexion entre les différents sites, qui bien que parfois inférieures en débit ou en fiabilité par rapport aux demandes, permettront une communication au moins suffisante étant donné des moyens à notre disposition. Nous sommes également parvenus à mettre en place un Datacenter principal au niveau du Siège B ainsi qu'un secondaire au niveau de Big Boy, garantissant un fonctionnement sûr de l'entreprise. Enfin la redondance n'a pu être que partiellement assurée encore une fois pour des raisons de budget, mais les sites en ayant le plus besoin ont tout de même été identifiés et équipés en conséquence.

Nous vous remercions pour le temps consacré à la lecture de ce document. Au plaisir de rencontrer l'équipe d'administration prochainement pour la présentation finale.

7 Bibliographie

https://opennebula.org/documentation/
https://fr.wikipedia.org/wiki/Kernel-based_Virtual_Machine
https://www.supinfo.com/articles/single/1684-cacti
https://www.dell.com/fr-fr/work/shop/povw/poweredge-r740
https://www.ldlc.com/fiche/PB00212191.html
https://www.ldlc.com/fiche/PB00251782.html
https://en.wikipedia.org/wiki/Network-attached_storage
https://www.calculatricecredit.com/mensualite-emprunt.php
https://docs.opennebula.org/5.6/operation/vm_management/vm_instances.html
https://www.tala-informatique.fr/wiki/images/a/ae/Haute_dispo.pdf
https://www.sanog.org/resources/sanog8/sanog8-datacenter-desgin-app-opt-zeeshan.pdf