Projet de Fin d'Etudes

Master Sciences et Techniques
systèmes intelligents & réseaux

Mutualisation d'infrastructure et sécurité d'accès dans un environnement Datacenter

Lieu de stage : Compagnie bureautique informatique

Réalisé par: Hasnae Kharbach

SOUTENU LE 22/06/2013

Encadré par :

Pr. R. BEN ABBOU

Pr. M.C.ABOUNAIMA

Mr. Y. MOUNIR

Devant le jury composé de :

Pr. R. BEN ABBOU

Pr. J.KHARROUBI

Pr. I.CHAKER

Pr. A.BEGDOURI

Année Universitaire 2012-2013

Dédicaces

À mes très chers parents ;

Vous avez été toujours là pour nous, vous nous avez donné un magnifique modèle de labeur et de persévérance. Nous espérant que vous trouverez dans ce travail toute notre reconnaissance et tout notre amour.

À la mémoire de mes grands parents;

Vous êtes toujours gravé dans ma mémoire.

À mes très chères sœurs ;

Nul mot ne pourra exprimer ma gratitude envers vous.

À tous mes amis de FST;

Je vous dis merci

Remerciement

Au terme de ce travail, je tiens à remercier vivement le président d'CBI, **M. Kamil BENJELLOUN** qui a accepté de m'accueillir en stage au sein de son organisme.

Je tiens à exprimer ma profonde gratitude et mes sincères remerciements **Mr Abdellah ZAROUALI** le directeur technique, **Mr Yassine MOUNIR** Senior Project Engineer et mon encadrant, pour tout le temps qu'ils m'ont consacré, leur directives précieuses, et pour la qualité de leur suivi durant toute la période de mon stage.

Je voudrai remercier également toute l'équipe d'CBI pour leur accueil et pour l'intérêt qu'ils ont manifesté envers mon travail.

Mes profonds remerciements vont à mes encadrants de la FST **Mr R. BEN ABOU et Mr R M.C.ABOUNAIMA** qui ont accepté d'encadrer mes travaux durant ces 4 mois de stage.

Mes plus vifs remerciements s'adressent aussi à tout le cadre professoral et administratif de FST.

Mes remerciements vont enfin à toute personne qui a contribué de près ou de loin à l'élaboration de ce travail.

Résumé

Le présent document constitue le fruit d'un travail accompli dans le cadre de notre projet de fin d'études au sein de la société CBI.

La société CBI est encours de mettre en place un centre donné pour offrir une large gamme des services à ses clients. Alors le long du stage, l'objectif était de faire une vision globale des Datacenter, en définissant ses fonctionnalités et ses services. Puis, proposer une solution pour l'accès des clients au Datacenter.

Ce rapport est axé sur trois grands chapitres. Le premier chapitre définit le contexte général du projet à savoir la présentation de la société d'accueil et la définition du projet. Le deuxième chapitre décrit l'étude détaillée de l'environnement ''Datacenter'' en définissant les différents composants ainsi ses services. Le troisième chapitre décrit les scénarios possibles pour qu'un client puisse avoir l'accès à son environnement.

Sommaire

Liste des figures

Liste des tableaux

Liste des abréviations

Abréviation	Désignation
TIC	Technologies de l'information et de la communication
PME	Petites et moyennes entreprises
SMSI	Système de management de la sécurité de l'information
ANSI	American national standards institute
UPS	Uninterruptible Power Supply
ASI	Alimentation Statique sans Interruption
AVI	Audio Video Interleave
FTP	protocole de transfert de fichier
SSH	Secure Shell
SaaS	Software as a Service
PaaS	Platefom as a Service
IaaS	Infrastructure as a Service
VLAN	Virtual Local area network
VPN	virtual Private Network

LS	**ligne spécialisée**
RPV	**réseau privé virtuel**
NAT	**Network Address Translation**
FW	**FireWall**
VRF	**Virtual Routing and Forwarding**
GRE	**Generic Routing Encapsulation**
MPLS	**MultiProtocol Label Switching**
DC	**Datacenter**

Introduction Générale

Les systèmes d'information continuent d'évoluer aussi vite que les technologies, ils proposent de nouveaux services et de nouveaux usages.

Cette évolution des TIC prend toujours la forme d'une spirale, revisitant une technologie ou un paradigme déjà existant tout en y associant quelques éléments nouveaux, qui parfois seront le déclencheur du succès espéré (voir les usages SMS des messagers récupérés).

Avec cette évolution les entreprises ont besoin des applications divers, et aussi un nombre important des serveurs de type différent ce qui nécessite un emplacement pour ces derniers, une architecture réseau complexe et une notion de sécurité plus résistante.

Le Datacenter est une solution pratique pour les petites et les moyennes entreprises prenant en charge l'hébergement des serveurs, et offre aussi une sécurité complète divisée en deux niveaux de coté matériel et de coté données.

Dans un Datacenter plusieurs clients tentent à se connecter à ses services offerts qui se peut produire un problème de connexion, alors la gestion de la sécurité d'accès nécessite une solution qui répond aux besoins des clients en termes de disponibilité, fiabilité et performance.

C'est dans cette perspective que la société CBI nous a proposé comme projet de fin d'étude mutualisation d'infrastructure et sécurité d'accès dans un environnement Datacenter.

L'objectif de ce rapport est de décrire le Datacenter comme environnement et sa fonctionnalité. Puis en second lieu proposer une solution pour l'accès des clients au Datacenter.

Dans le premier chapitre de ce rapport, nous allons présenter la société CBI '' **compagnie bureautique et informatique** '' et aussi le descriptif du projet. Ensuite dans le deuxième chapitre sera consacré pour l'étude théorique et détaillée de l'environnement ''Datacenter''. Finalement nous allons faire une étude comparative entre les solutions possibles qui nous permettra de choisir la solution optimale.

Chapitre I *Contexte générale du projet*

1. Présentation de la société

1.1. Introduction

CBI (compagnie bureautique et informatique) est une société anonyme à capital entièrement de 60.000.000 Dhs.

Depuis sa création en 1970, l'offre globale solutions (produit et services) de CBI est restée centré sur les technologies de l'information et n'a cessé de s'enrichir en intégrant les innovations technologiques afin de pouvoir répondre aux besoins de ses clients et d'être toujours en avance dans un monde en perpétuelle mouvance.

L'offre solutions de CBI couvre des produits et des marchés complémentaires (bureautique, informatique, système d'information, télécommunication, internet/intranet), mais toujours orientés vers les nouvelles technologies et les outils de productivité.

Cette constituée de produit de haute technologie leaders sur leurs marchés, et construite grâce à des partenaires très étroits avec les fournisseurs internationaux représente une consolidation continue de savoir-faire et de compétences.

CBI répond aux besoins du marché grâce à ses équipes propres et aux partenariats internationaux ou locaux passés avec les acteurs majeurs du marché.

1.2. Historique

CBI est né sur la base d'un contrat de distribution avec TOCHIBA pour OFFICE AUTOMATION et RUF pour les machines mécanographiques. Un certain nombre des dates clefs jalonnent depuis l'histoire CBI :

- 1970 : Création de CBI-Partenariat avec TOCHIBA.
- 1980 : Première connexion pour les banques.
- 1986 : Introduction des 1ers ordinateurs portables et fax au Maroc (TOCHIBA).
- 1989 : Membre fondateur de l'APEBI.
- 1991 : Développement de la 1ère architecture client/serveur avec SCO UNIX, NOVEL et BD INFORMIX.
- 1992 : Exposition au Salon Unix à Paris.
- 1993 : Lancement de la marque : CBI SYSTEMES.
- 1995 : Partenariat avec Informix/Unix.
- 1997 : Partenariat avec IBM.
- 1999 : Installation du 1er réseau Frame relay.
- 2001 : Partenariat CISCO.
- 2004 : Installation de la première liaison DWDM en Afrique.
- 2006 : Inauguration de l'agence CBI Sénégal à Dakar.
- 2008 : Installation de systèmes de gestion électronique de bibliothèques.
- 2010: Solution innovation of the year Cisco.
- 2011: Partner Cisco of the year (North Africa & Levant).
- 2012: -Certification Partenaire Cisco Gold.
  -Certification du Centre de Services CBI.

1.3. Organisation et alliances

1.3.1. Structure

Aujourd'hui, CBI est structuré en 4 divisions (business unit) :

Division software :

CBI SOFTWARE assure la mise en œuvre d'une infrastructure logicielle globale répondant à différentes problématiques de l'entreprise quant à la génération et la disponibilité de son information.

CBI SOFTWARE propose des solutions dans les domaines suivants :

- Business Information Management.
- Décisionnel.
- CRM.
- Process.
- ERP.

Division systèmes :

CBI SYSTEMES a pour vocation de mettre à disposition de ses clients les meilleures solutions répondant aux différents besoins suivants :

- Le Traitement de l'Information.
- La Disponibilité de l'Information.
- La Pérennité de l'Information.

CBI SYTEMES s'assure par ailleurs, que ses produits & services fournissent un haut niveau d'efficacité et de rendement, valorisant de façon optimale l'infrastructure informatique de ses clients.

Les solutions fournies relèvent des domaines suivants :

- Poste utilisateur
- Serveurs
- Stockage
- Virtualisation
- Datacenter

Division télécoms :

CBI TELECOMS s'est, depuis sa création, positionné comme le spécialiste dans la mise en place des solutions Réseau et Télécommunication.

Par ses partenariats, CBI TELECOMS accompagne ses clients dans la mise en œuvre d'une véritable politique collaborative de la façon la plus efficiente possible.

Le Pôle propose une gamme complète de solutions :

- Réseaux
- Sécurité
- Solution opérateur
- Communications unifiées

Division éditique :

CBI EDITIQUE a su développer son savoir-faire en intégrant les enjeux de la gestion du document dans des Systèmes d'information (SI) de plus complexe.

Par ailleurs, à travers sa présence sur les six plus grandes villes du royaume, CBI est à même d'assurer la plus large couverture géographique.

A ces divisions s'ajoute une unité administrative et logistique qui supporte l'ensemble des activités de l'entreprise.

Le travail au sein de la CBI s'organise aussi bien au niveau du siège que par l'intermédiaire d'un réseau de 8 agences réparties à travers les grandes villes du Royaume : Casablanca, Rabat, Fès, Tanger, Marrakech, ainsi qu'au Sénégal.

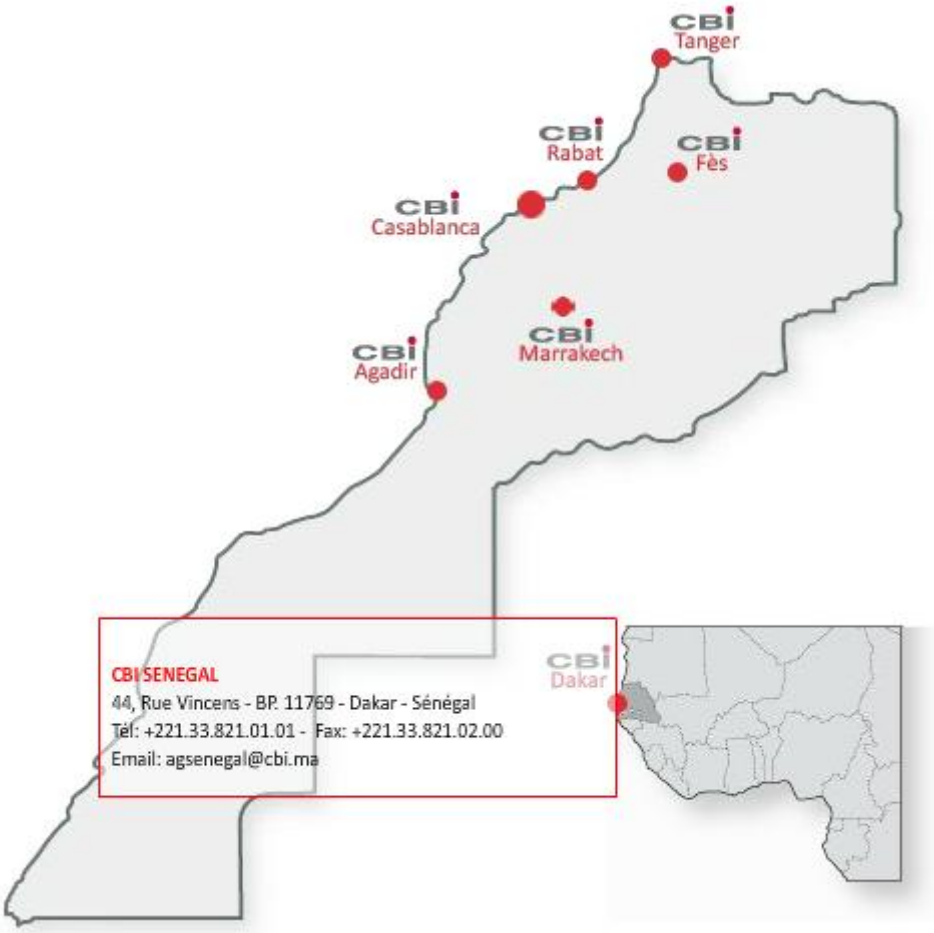

Figure1 : agences de CBI

1.3.2.

1.3.3. Les principaux domaines de compétences de CBI

- Conseil/ Audit
- Mise en place d'infrastructures.
- Suivi de projets de développement et d'implémentation.
- Transfert de compétences.

1.3.4. Vision globale

Intégrateur Global TI aux standards internationaux fondés sur une très forte veille technologique qui anticipe les exigences des clients, CBI s'est fixée comme objectifs de :

- Satisfaire ses clients
- Fournir à ses clients des solutions informatiques de qualité, complète et répondant à leur besoins
- Accompagner ses clients dans l'implémentation des solutions informatiques tout en assurant un transfert de compétences.

1.3.5. Partenaires

Afin de concourir à la réalisation de ses objectifs, divers contrats lient CBI à ses partenaires fournisseurs :

Figure 2 : les partenaires CBI

2. Présentation du projet

Dans le cadre d'amélioration de ses services, CBI veut mettre en place d'une nouvelle organisation des moyens d'infrastructure informatique pour ses clients d'où le projet Datacenter est créé.

Notre Projet de Fin d'Etudes s'inscrit dans le cadre d'un grand projet, intitulé «**la solution Datacenter CBI**».

Notre mission dans le projet se divise en deux parties :

- La première partie est de faire une étude dont le but est de définir sans ambigüité Datacenter afin d'identifier les mécanismes nécessaires à son implémentation. Il convient, par ailleurs, d'analyser les enjeux que revêt cette action sur le segment de l'Internet et ses implications techniques.

- La deuxième partie consiste à proposer une solution pour le problème de conflit d'adresse entre les clients connectés au Datacenter.

Alors le résultat attendu est :

A la fin nous devons fournir une définition claire du concept de Datacenter, les spécifications techniques nécessaires à sa mise en œuvre ainsi que la description détaillée de la solution d'accès des clients. Un rapport devra être fourni en versions papier et électronique et comprendra :

- Un état de l'art du Datacenter.

- Une analyse des enjeux liés à leur déploiement.

- Un état des lieux comprenant une analyse environnementale et technique relativement à l'implémentation du Datacenter.

- Une étude comparative entre les solutions suggérées.

- Le choix de la solution qui apparait la meilleure.

- Proposition du matériel associé à la solution choisie.

3. Conclusion

Dans ce chapitre nous avons commencé par présenter la société d'accueil, ensuite nous avons passé à la présentation de notre projet.

Pour le chapitre qui suit, on va faire une étude théorique de l'environnement ''Datacenter'' en présentant le local technique et les différents services de ce dernier.

Chapitre II *Le centre de données "datacenter "*

1. Introduction

Chaque entreprise et plus précisément PME a besoin de plusieurs services tel que la messagerie pour l'envoi des rapports, le stockage des données ainsi que l'utilisation de plusieurs applications.

Tous ces services requièrent un nombre important des serveurs qui nécessitent un emplacement pour les adopter. Ces serveurs requièrent un niveau de sécurité et de bon fonctionnement en termes de climatisation et d'alimentation.

En effet Les PMEs continuent à chercher la croissance et une meilleure gestion des coûts, elles doivent affronter les défis constitués par le climat économique imprévisible, l'escalade de la réglementation, les progrès technologiques et l'augmentation des volumes et de la complexité des données sur lesquelles repose leur activité.

Face au changement, les entreprises cherchent des méthodes flexibles et évolutives pour gérer les infrastructures TIC sans compromettre la sécurité et la fiabilité.

Alors la mise en place d'un centre de données présente une solution faisable et a comme avantage principal : assurer la qualité des infrastructures et le niveau de sécurité. Cela devient encore plus avantageux pour une PME car il lui serait impossible de se doter d'un local informatique équivalent.

Dans ce chapitre nous allons définir ce qu'est le centre de données, en donnant une définition, en expliquant les différents composants et ses fonctionnalités.

2. Définition

L'expression Datacenter ou centre de traitement de données crée beaucoup de polémiques dans le domaine de la technologie et de l'information.

Pour certaines personnes, un Datacenter est un endroit (salle, bâtiment…) où l'on entrepose les serveurs d'une entreprise sous surveillance. D'autres, par contre, le définissent comme étant l'environnement qui part du local aux matériels et logiciels permettant d'assurer la sécurité, la garantie, la disponibilité 24h sur 24h des données de particuliers et/ou d'entreprises.

La définition retenue dans le cadre de notre stage est celle qui présente le Datacenter ou centre de traitement de données comme étant l'ensemble formé par le local et la plateforme techniques assurant le traitement et l'hébergement de plusieurs types de données et applications informatiques conformément , aux normes strictes préétablies (électricité, température, humidité, protection incendie, communications, accessibilité, etc.). C'est donc un espace aménagé et sécurisé pour abriter, traiter et protéger les données. Il peut éventuellement être un centre de backup (centre de sauvegarde), un centre de fall

back (centre de secours) ou un centre de documentation électronique pour les applications existantes ou à venir. Il doit être discret, tout en étant accessible et sécurisé.

3. Aspects normatifs

3.1. Norme de sécurité de l'information

Pour la mise en place d'un Datacenter fiable, plusieurs normes de sécurisation de l'information sont disponibles. Celles que nous relatons dans ce rapport sont les plus importantes du SMSI (Système de Management de la Sécurité de l'Information) qui est destiné à choisir les mesures de sécurité afin d'assurer la protection des biens sensibles d'une entreprise sur un périmètre défini.

- **ISO 27001**

La norme ISO 27001 publiée en octobre 2005 a été créée dans le but de protéger les informations capitales d'une entreprise contre les différentes menaces de sécurité. Elle fournit une plateforme pour la mise en œuvre et l'exploitation des mesures de sécurité. Le processus fonctionne sur quatre principes bien connus : le PDCA « Plan, Do, Check, Act ». [1]

- **Plan phase**

C'est la phase de planification du processus. Au cours de cette phase, une analyse de risque est effectuée afin d'identifier les systèmes et applications critiques pour la survie de l'entreprise et leur niveau de dépendances respectives vis-à-vis de celle-ci. Ces résultats aident à identifier les exigences de sécurité à prévoir et à déterminer les demandes de disponibilité sur les systèmes et applications.

- **Do phase**

C'est la phase de mise en œuvre. Elle introduit des mesures spécifiques pour l'identification et la réduction des risques.

- **Check phase**

C'est la phase de contrôle régulier des mesures mises en œuvre par la surveillance de routine et la vérification périodique. Elle permet d'identifier les potentielles améliorations (Voir les différences entre ce qui a été dit et ce qui a été fait).

➢ **Act phase**

Cette phase consiste à entreprendre des actions correctives pour les écarts qui ont été constatés précédemment dans le check phase.

- **ISO 27002**

La norme ISO 27002 est un ensemble de 133 mesures dites « best practices » (bonnes pratiques en français), destinées à être utilisées par tous les responsables de la mise en place ou du maintien d'un Système de Management de la Sécurité de l'Information (SMSI). La sécurité de l'information est définie au sein de la norme comme la préservation de la confidentialité, de l'intégrité et de la disponibilité de l'information. [2]

3.2. Norme de la mise en place technique de data center

- **ANSI/TIA-942-2005**

L'ANSI/TIA 942-2005 est libellée comme suit : Télécommunications Infrastructure Standard for Datacenter, qui signifie Norme d'Infrastructure de télécommunications pour Datacenter. [3]

Elle a pour objectif de proposer les exigences propres à la spécification, la réalisation et l'équipement des Datacenter garantissant ainsi les meilleurs niveaux de conformité et de disponibilité. C'est un document de travail, approuvé par l'ANSI (American National Standards Institute) et le TIA (Telecommunications Industry Association) qui est revu tous les 5 ans.

L'avantage de posséder cette norme est qu'on dispose comme résultat un document définissant de manière très précise les moyens dont il faut s'équiper pour obtenir un bon niveau de disponibilité des données dans les datacenters. Ce document doit reconnu par la communauté internationale.

Les inconvénients de cette norme sont qu'elle est orientée télécom, elle n'est pas assez aigüe sur la sécurité des informations et elle est limitée en terme de sécurité physique.

La norme ANSI/TIA 942-2005 prévoit plusieurs recommandations dans différents domaines pour la construction d'un Datacenter fiable. Les domaines sont les suivants :

- **Le local technique**

Pour le choix du local technique, la norme ANSI/TIA 942-2005 énumère plusieurs conditions à respecter, comme le site se trouve sous les routes aériennes ou pas et le type du matériaux avec lequel va être construit.

- **Accès au local technique**

L'accès au Datacenter doit être hautement sécurisé.

- **Au niveau architectural**

Pour l'architecture du Datacenter, la norme prévoit des prescriptions à certains niveaux :

- **Hauteur au plafond.**
- **Faux plancher.**
- **Eclairage.**
- **Les murs.**

- **Au niveau environnemental**

La température et l'humidité dans les Datacenter doivent être sujettes un contrôle strict. Pour cela, la norme a prévu un tableau récapitulatif des différentes limites à respecter.

Tableau 1: conditions environnementales requises

Libellé	Plage
Température	Entre 20°C et 25°C
Taux d'humidité relative	Entre 40% et 55%
Vitesse maximale de fluctuation	5°C par heure
Température maximum au point de rosée	21°C

On a souvent recours l'humidification ou à la déshumidification selon les contraintes environnementales du local technique. Aussi, La norme conseille que la température ambiante et l'humidité soient mesurées après que les différents appareils soient mis sous tension. Les mesures doivent être faites à une distance de 1,5 m au-dessus du niveau du sol et tous les 3 à 6 m le long de la ligne centrale des allées froides et à tout endroit dans la prise d'air de l'exploitation des équipements.

3.3. Norme de prévention et de protection contre les incendies

- **NFPA-75**

La norme NFPA-75 est la norme que conseille le ANSI/TIA 942-2005 pour les systèmes de protection incendie et les extincteurs portatifs. Elle a été écrite par le Comité technique sur les systèmes électroniques et informatiques en accord avec le National Fire Protection Association (NFPA) et publiée le 4 février 1999 à Atlanta aux Etats-Unis. La norme NFPA-75 est internationale et est composée de 10 chapitres et de 4 appendices qui traitent des équipements de détection et de protection en cas d'incendie. [4]

Toutes les normes énumérées sont actuellement en vigueur dans le domaine des Datacenter, la majorité d'elles sera révisée en cette même année 2010 mais toute fois elles permettent de réglementer les dispositions à prendre pour réussir la construction d'un Datacenter fiable. Connaissant les normes qui régissent les Datacenter, il est cependant important de connaître les architectures et la classification des Datacenter afin d'y constater l'application réelle de ces différentes normes précitées.

4. Architectures de Datacenter

4.1. Architectures d'un Datacenter

4.1.1. Architecture des espaces dans le Datacenter

Selon le troisième chapitre de la norme ANSI/TIA 942-2005, l'espace dans le site du Datacenter peut être séparé en neuf (09) parties dont sept (07) parties composent le Datacenter et deux (02) parties en dehors du Datacenter. Le schéma ci-dessous illustre notre argumentation.

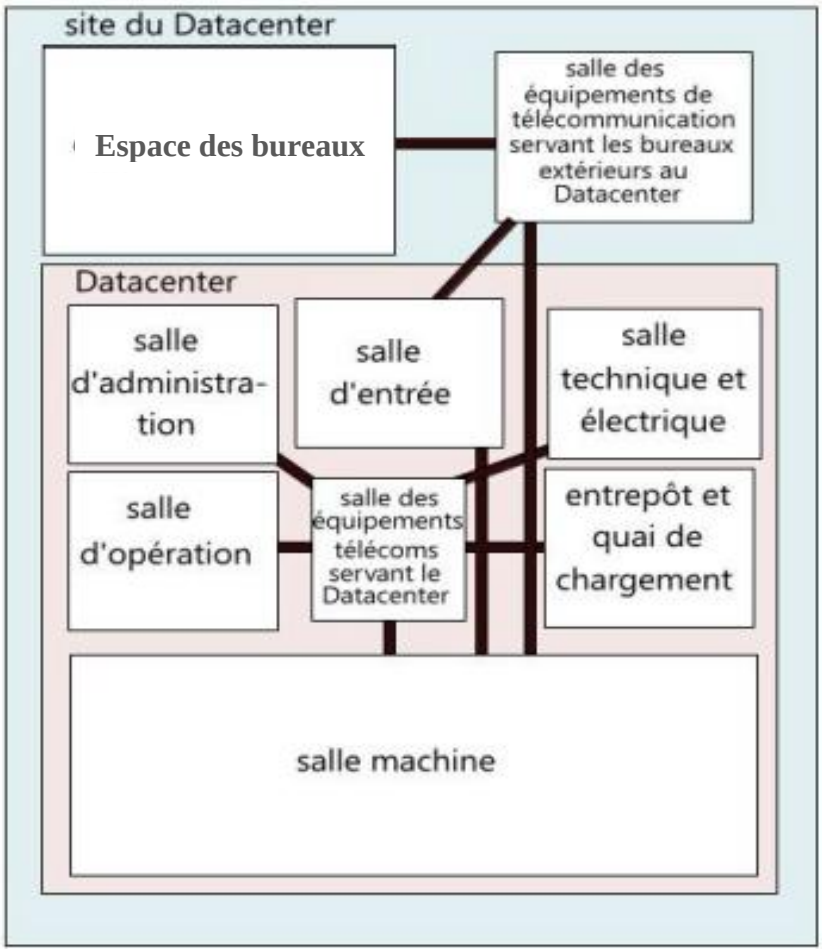

Figure3 : Répartition des espaces du Datacenter selon la norme ANSI/TIA 942 : 2005

Selon la norme, le Datacenter en lui-même est composé des parties suivantes :

- **Une salle des équipements de télécommunication servant le Datacenter**

Cet endroit est l'espace qui permet d'interconnecter toutes les différentes salles du Datacenter par ricocher tous les matériels réseaux du Datacenter. Aussi, il permet d'assurer la communication l'intérieur du Datacenter.

- **Une salle d'administration**

C'est le lieu de surveillance des matériels, des applications et des données du Datacenter. C'est dans la salle d'administration que l'on exploite les différents logiciels de surveillance et les services du Datacenter.

- **Une salle d'opération**

Elle permet la surveillance des accès physiques (intrusion) au Datacenter. C'est le lieu où l'on examine les différents fichiers de vidéosurveillance en cas d'intrusion ;

Les personnes travaillant dans cette salle sont alertées en cas de détection d'incendies et prennent les premières mesures de sécurité.

- **Une salle technique et électrique**

La salle technique et électrique permet d'installer et de contrôler tous les systèmes électriques et mécaniques. On y trouve les différents tableaux électriques, les générateurs, les systèmes de climatisation…

- **Un entrepôt et quai de chargement**

L'entrepôt permet de conserver tous les matériels non encore utilisés dans le Datacenter ainsi que les différents matériels de sauvegardes des données. Le quai de chargement sert d'interface entre le site du Datacenter et le monde extérieur en matière de logistique ; elle permet le stockage et facilite le transport des matériels l'intérieur comme l'extérieur du site.

- **Une salle machine**

C'est le lieu destiné à la disposition des différents racks, des systèmes de refroidissement et d'alimentation du Datacenter. Cet espace est composé de :

- **Racks et compartiments**

Les racks servent à stocker plusieurs machines (serveurs physiques, routeurs, commutateurs…) sur une même surface en les empilant les unes sur les autres. Ce qui fait que l'on peut avoir jusqu'à 48 machines de 1U (1,75''=4,445 cm) sur une surface de 1 mètre carré. Les racks assurent entre autre la sécurité des appareils et donnent une beauté et une clarté à la salle.

- **Systèmes de climatisation**

Les Datacenter sont équipés de systèmes de climatisation qui permettent de maintenir leur température constante et conforme aux spécifications thermiques de la norme.

- **Systèmes de détection et de lutte anti-incendie**

Dans les Datacenter, on trouve des extincteurs qui permettent de lutter contre les incendies éventuels. En outre, il est prévu, pour ne pas arriver aux incendies, des méthodes de détection de fumée et d'incendie.

- **Une salle d'entrée**

C'est la salle des différents contrôles physiques (badge, carte magnétique, empreinte digitale…).

Ces différentes salles précitées constituent l'espace du Datacenter. Aussi, sur tout le site du Datacenter on trouve des bureaux extérieurs au Datacenter et une salle de télécommunication servant les bureaux extérieurs au Datacenter. Ces deux entités ont respectivement pour fonction:

- **Espace de bureaux**

C'est l'espace qui regroupe les différents bureaux qui traitent des sujets n'étant pas en rapport avec les services du Datacenter (comptabilité, ressources humaines…).

- **Une salle des équipements de télécommunication servant le Datacenter**

Cet endroit est l'espace qui permet d'interconnecter tous les différents bureaux extérieurs en termes de câblage réseau.

4.1.2. Architecture réseau des espaces dans le Datacenter

La topologie réseau d'un Datacenter classique comprend, une salle entrée, une ou plusieurs salles de télécommunication, une aire de distribution principale, plusieurs aires de distribution horizontale reliées à des aires de distribution d'équipement.[5]

- **Architecture réseau générale**

L'architecture générale ci-après montre les différents câblages au niveau d'un Datacenter à une entrée.

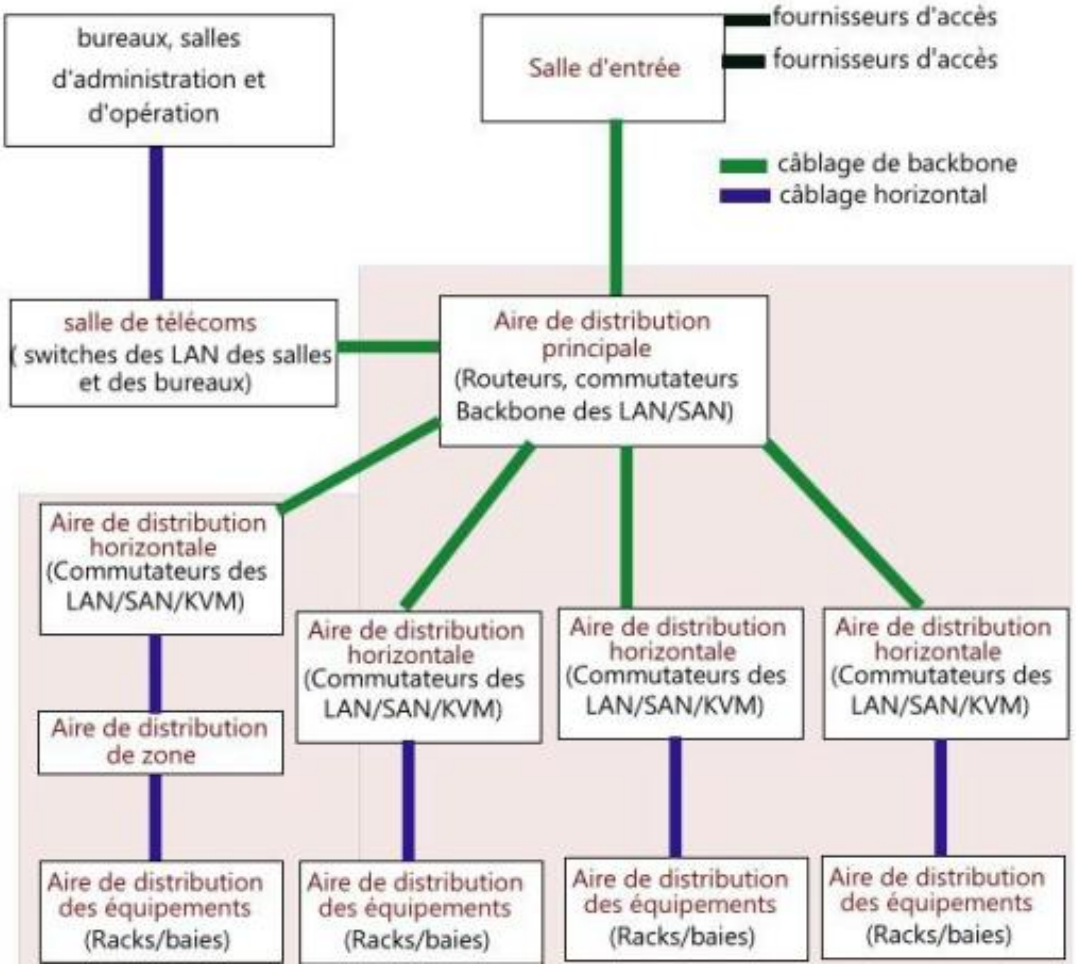

Figure4 : Architecture réseau d'un Datacenter classique

LAN : Local Area Network est un réseau local situé dans une zone réduite comme une salle, un bâtiment, un immeuble ou un bloc d'immeubles etc.

SAN : Storage Area Network est un réseau de grande capacité reliant des serveurs mettant à disposition d'importants espaces de stockage de données. Les serveurs en question ne contiennent guère autre chose que des disques, ce qui libère les autres serveurs qui peuvent alors travailler exclusivement sur le traitement des données.

Commutateur KVM : Keyboard Video Mouse permet de connecter un seul écran-clavier-souris sur plusieurs ordinateurs; Il favorise la suppression des écrans, claviers, souris inutiles tout en facilitant l'accessibilité et le partage des accès serveurs, libère de la place dans les bureaux et salles informatiques et rationalise l'organisation physique des différents équipements.

- **Architecture réseau réduite**

L'architecture réduite montre un regroupement de certaines aires de distribution pour simplifier la mise en œuvre de façon pratique.

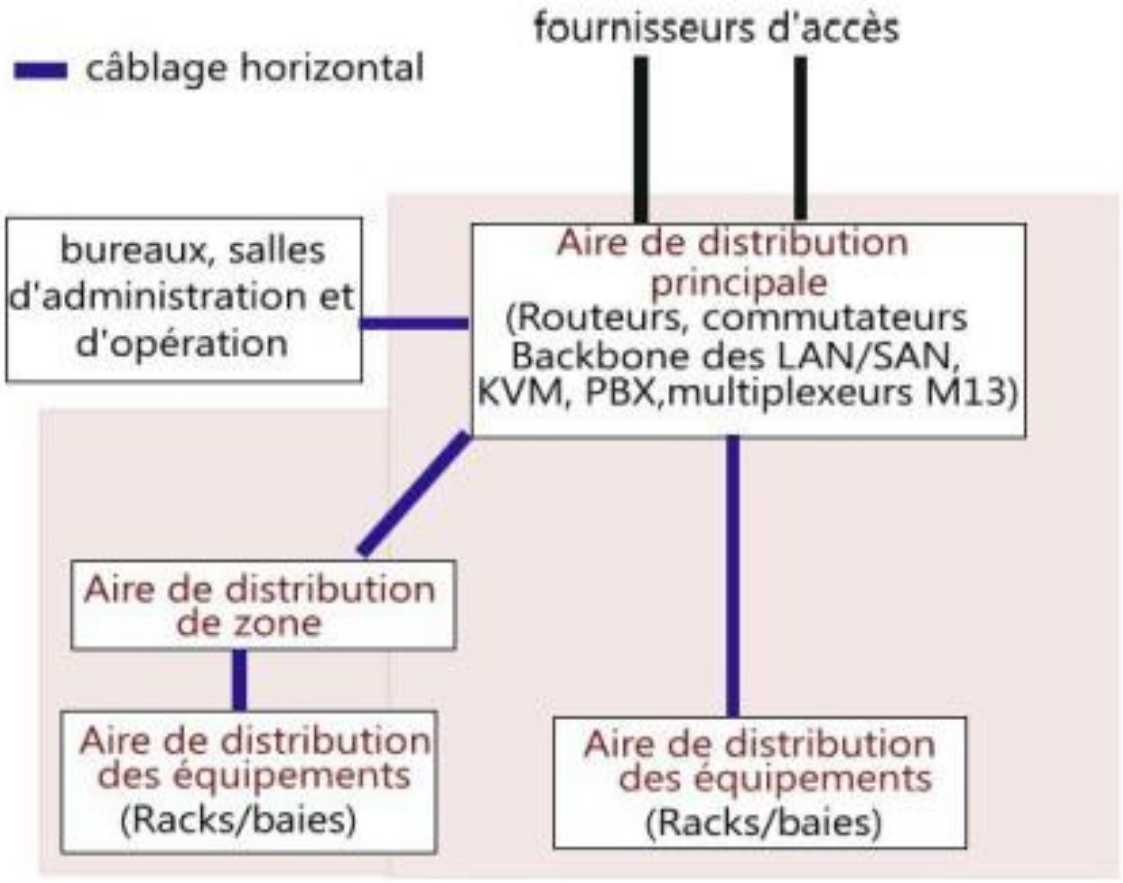

Figure5 : Architecture réduite du réseau d'un Datacenter

4.2. Classification des Datacenter

L'Uptime Institute qui est l'une des plus grandes autorités de Datacenter dans le monde a classé les Datacenter selon différents critères techniques. Ces principaux critères sont : le taux de disponibilité global, le niveau de redondance des circuits électriques et de climatisation, le dimensionnement des équipements. Ainsi, l'institut a fait ressortir 4 différents groupes de Datacenter nommés de Tier I à Tier IV. Le choix du Tier du Datacenter à implémenter est fonction de la criticité des équipements qui seront dans le Datacenter.[6]

- Tier I

Dans cette catégorie, les Datacenter sont composés d'un seul circuit électrique pour l'énergie et pour la distribution de refroidissement, sans composants redondants, ils offrent un taux de disponibilité de 99,671% correspondant à un temps d'arrêt cumulé moyen de 28,8 heures par an.

- Tier II

Les Datacenter de Tier II sont composés d'un seul circuit électrique pour l'énergie et pour la distribution de refroidissement, avec des composants redondants, ils offrent un taux de disponibilité de 99,749% (soit 22 heures d'arrêt).

- Tier III

Au niveau du Tier III, les Datacenter sont composés de plusieurs circuits électriques pour l'énergie et pour la distribution de refroidissement, mais seulement un circuit est actif à la fois. Ceux-ci ont des composants redondants et offrent un taux de disponibilité de 99,982% soit 1,6 heures d'arrêt dans l'année.

- Tier IV

Dans ce groupe, les Datacenter sont composés de plusieurs circuits électriques pour l'énergie et pour la distribution de refroidissement, ceux-ci ont des composants redondants, tous actifs et supportent la tolérance aux pannes, ils offrent un taux de disponibilité de 99,995% correspondant à 0,4 heures par an.

Tableau2 : Tableau récapitulatif de la classification des Datacenters

Critères	Tiers I	Tiers II	Tiers III	Tiers IV
Date de déploiement	1965	1970	1985	1995
Nombre de voies d'alimentation	1	1	1active+1passive	2 actives
Redondance composants	N	N+1	N+1	2N ou 2(N+1)
Compartimentage bâtiment	Non	Non	Non	Oui
Cooling classe A sans interruption	Non	Non	Souhaitable	Oui
Maintenance sans arrêt d'exploitation	Non	Non	Oui	Oui
Tolérance à un sinistre majeur	Non	Non	Non	Oui
Temps d'interruption annuel de l'IT	28,8H	22H	1,6H	0,8H
Disponibilité représentative du site	99,671%	99,749%	99,982%	99,995%

N : fournit le nombre de moyens requis pour le fonctionnement habituel.

N+1 : fournit le nombre de moyens requis pour le fonctionnement habituel plus un moyen de secours.

2N : double le nombre de moyens requis pour le fonctionnement habituel.

2(N+1) : deux fois (le nombre de moyens requis plus un moyen de secours).

Le *tiering* est un critère global d'appréciation qui introduit à ce qui suit et qui ne doit pas être le seul critère de choix**.** Cela reste une simplification grossière qui doit être détaillée.

5. Enjeux de l'implémentation des Datacenter

5.1. Enjeux techniques

Au niveau technique, l'avantage de l'implémentation et de l'utilisation d'un Datacenter par une entreprise est visible en trois points essentiels :

- **La disponibilité et la fiabilité des données**

Dans les parties précédentes de notre document, nous avons montré que les Datacenter étaient conçus avec des équipements redondants c'est-à-dire malgré la maintenance de certains serveurs, d'autres en assurent la relève sans difficulté et cela permet une haute disponibilité et une fiabilité des données hébergées. Par exemple pour un Datacenter en Tier IV, le temps d'indisponibilité annuel est de 48mn, ce qui montre que les données sont disponibles à tout moment et fiables lorsqu'elles sont hébergées dans un Datacenter. [7]

- **La sécurité**

Au niveau sécuritaire, fort est de constater que l'implémentation des Datacenter utilise les meilleures méthodes de sécurité tant au niveau des données qu'au niveau physique (des matériels et personnes). En effet les Datacenter offrent un meilleur niveau de sécurité en prévoyant des mesures d'une part contre les menaces numériques que sont : la criminalité informatique, la cybercriminalité, l'ingénierie sociale et d'autre part contre les catastrophes que peuvent être les intempéries, les panes informatiques, les erreurs humaines…

Déplus, Ils assurent le premier niveau de sécurité (la sécurité physique) qui concerne tout l'environnement du système d'information (sécurité d'accès, climatisation, électricité régulée, sécurité incendie, protection contre les inondations, ...) par des moyens bien étudiés et bien conçus. [8]

➢ **La qualité de service**

Le recours à un Datacenter apporte une meilleure qualité de service à l'entreprise, un service à l'état de l'art. A priori, il n'est pas logique de placer ses données stratégiques à l'extérieur de sa structure administrative. Cependant, la plupart des responsables semblent admettre aujourd'hui que leurs données sont plus en sécurité externalisées auprès de spécialistes dont c'est le métier que les conserver en interne.

La qualité de service se fera ressentir aussi par l'amélioration de la réactivité aux demandes des clients. En effet, les entreprises ne se souciant plus de leurs données étant en sécurité dans le Datacenter vont donc répondre plus rapidement et facilement aux attentes de leurs différents clients. [9]

5.2. Enjeux économiques

Les enjeux économiques sont à deux niveaux, d'une part il y a des enjeux pour les entreprises clientes qui hébergent leurs données dans le Datacenter et d'autre part des enjeux pour le détenteur du Datacenter.

➢ **Pour les clients**

Les clients hébergeant leurs données dans les Datacenter gagnent à plusieurs niveaux :

- **L'externalisation**

Héberger son système d'information de façon sécurisée requiert des niveaux d'investissement extrêmement élevés. L'externalisation ou outsourcing est le fait pour un prestataire de Datacenter de prendre en son compte le risque de réaliser ces investissements lourds et nécessaires afin de garantir la sécurité des systèmes d'information de ses clients.

Ainsi, le client gagne puisque les coûts d'hébergement de son système d'information sont insignifiants face aux coûts qu'il aurait engrangés pour la sécurisation de celui-ci en interne. [10]

- **Réduction du nombre de serveurs au sein des entreprises clientes**

Tout le système d'information des entreprises étant externalisé dans les Datacenter, le nombre de serveurs utiles pour le fonctionnement de ces entreprises sera donc réduit.

Ainsi ces entreprises gagnent car elles économisent le coût d'achat et d'administration des serveurs supplémentaires dont elles se sont privées. [11]

- **Réduction de la consommation d'énergie**

Les entreprises qui prennent l'engagement d'externaliser leurs systèmes d'information réduisent considérablement leurs différents coûts. En effet, ces entreprises réduisent ou suppriment des coûts comme celui de l'achat et de la maintenance des

matériels, les coûts de consommation d'énergie, les coûts liés à la mise en œuvre de leurs salles informatiques (onduleurs, climatiseurs, personnels…). Ainsi, ces entreprises gagnent car les coûts dont elles se sont privées sont largement supérieurs aux coûts d'hébergement des systèmes d'information dans les Datacenter. [12]

➢ **Pour le détenteur du Datacenter**

La mise en œuvre d'un Datacenter est d'abord une activité commerciale pour son détenteur. Les différents coûts engendrés par l'hébergement des systèmes d'information des entreprises clientes et des différents services rendus sont aussi importants même si cela n'est pas perçu à court terme et permettent au Datacenter de nourrir son homme. [13]

5.3. Enjeux politiques et sociaux

L'implémentation d'un Datacenter a aussi des avantages que ce soit au niveau social qu'au niveau politique.

➢ **Au niveau social**

Les enjeux au niveau social sont montrés par les services qui sont rendus aux entreprises clientes.

Au-delà des évolutions techniques, technologiques et des aspects commerciaux, les objectifs des décideurs vis-à-vis des investissements réalisés pour mettre en place un Datacenter sont nombreux. Il s'agit premièrement d'assurer la sécurité du patrimoine informationnel et d'offrir aux partenaires et clients des infrastructures appropriées pour l'hébergement et le traitement de leurs données. En outre, le centre de traitement des données, en privilégiant la mutualisation des ressources informatiques, offre également un espace d'hébergement aux entreprises moins nanties et favorise ainsi l'émergence d'une plus large expertise locale.

➢ **Au niveau politique**

Au niveau politique, l'avantage de l'implémentation d'un Datacenter se fait ressentir par :

- **Un challenge technologique**

Le fait pour CBI de posséder un Datacenter d'envergure montre son alignement vis-à-vis de l'avancé technologique.

Les enjeux de l'implémentation d'un Datacenter sont donc nombreux et importants pour le pays, les entreprises clientes et aussi pour le détenteur du Datacenter.

6. Etude conceptuel d'un Datacenter

6.1. Etude du local technique

6.1.1. Caractéristiques physiques du local technique

Etude du bâtiment d'un Datacenter

L'étude appropriée du site du local technique et ses matériaux de construction est d'une importance capitale dans la mise en place d'un Datacenter. La norme ANSI/TIA 942 :2005 prévoit les caractéristiques suivantes pour le choix du local technique d'un Datacenter :

- **Caractéristiques géologiques du site**

Le site d'un Datacenter doit se présenter loin des différents risques géologiques que sont:

- Les crues
- Les inondations
- Les ruissellements
- Les débordements
- Les séismes
- Les remontées des nappes.

En effet le site du Data Center doit être situé sur le coefficient le plus faible de l'échelle de risque. [14]

- **Caractéristiques des bâtiments environnants**

Pour la sécurité du Datacenter, celui-ci doit être construit à une grande distance de certaines infrastructures. En effet il ne doit pas se trouver :

- Sous les routes aériennes d'aéroports proches.
- A moins de 800m d'une autoroute, d'un axe majeur routier, d'une base militaire.
- A moins de 1,6 km d'un site nucléaire, d'un dépôt de munitions et d'un site de défense.
- A moins de 400m d'un aéroport, d'un barrage, de la côte d'une rivière, d'une usine chimique. [15]

- **Caractéristiques du bâtiment**

Le bâtiment du Datacenter doit être très solide et résistant aux différents dangers présents dans les Datacenter. Selon la norme ANSI/TIA 942 :2005, il doit respecter les caractéristiques suivantes : [16]

- **Charge au sol**
- **La superstructure et enveloppe**
- **Structure stable au feu**
- **Hauteur au plafond**

Le site du Datacenter et ses matériaux de construction doivent respecter les prescriptions des normes en vigueur. Par ailleurs, pour une bonne évacuation de la chaleur des Datacenter, il est impérieux de connaître les différentes méthodes de climatisation afin de choisir celles qui conviennent au Datacenter à implémenter.

Conditionnement des équipements

- ***Importance de l'évacuation de la chaleur***

Les différents équipements qui composent les Datacenter produisent beaucoup de chaleur. Cette chaleur présente en quantité importante est un grand danger dans le Datacenter de plusieurs manières :

➢ **Pour le Datacenter**

Une présence massive de chaleur dans une enceinte fermée provoque une élévation rapide de la température. Cette température élevée au contact d'une petite étincelle provoque un incendie. Le non évacuation de la chaleur dans un Datacenter est donc un risque d'incendie pour celui-ci.

➢ **Pour les équipements**

La chaleur dans le Datacenter réduit considérablement le rendement et la durée de vie des équipements et matériels du Datacenter.

Pour amoindrir les risques d'incendie et prolonger la durée de vie des équipements dans les Datacenter, il est important d'évacuer la chaleur dans l'enceinte de celui-ci. Pour ce faire, différentes méthodes d'évacuation de la chaleur sont disponibles. Ainsi le choix d'une sera fonction des atouts environnementaux et des moyens financiers que possède le Datacenter.

- ***Méthodes de climatisation et d'évacuation de la chaleur***

Au niveau des Datacenter, multiples solutions de refroidissement existent. Celles que nous présentons ici sont les principales. A l'exception du Free Cooling, les autres méthodes de climatisation reposent sur le principe de la pompe à chaleur.

- **Centrale de climatisation air-air**

Le système de climatisation air-air est le système le plus utilisé dans les Datacenter. En effet ce système est celui implémenté dans les climatiseurs domestiques (les splits). Dans ce système, les différents échanges d'abord entre le condenseur et l'extérieur puis entre l'évaporateur et le Datacenter se font avec de l'air. Le système de climatisation air-air est celui qui convient au mieux pour les petites installations. [17]

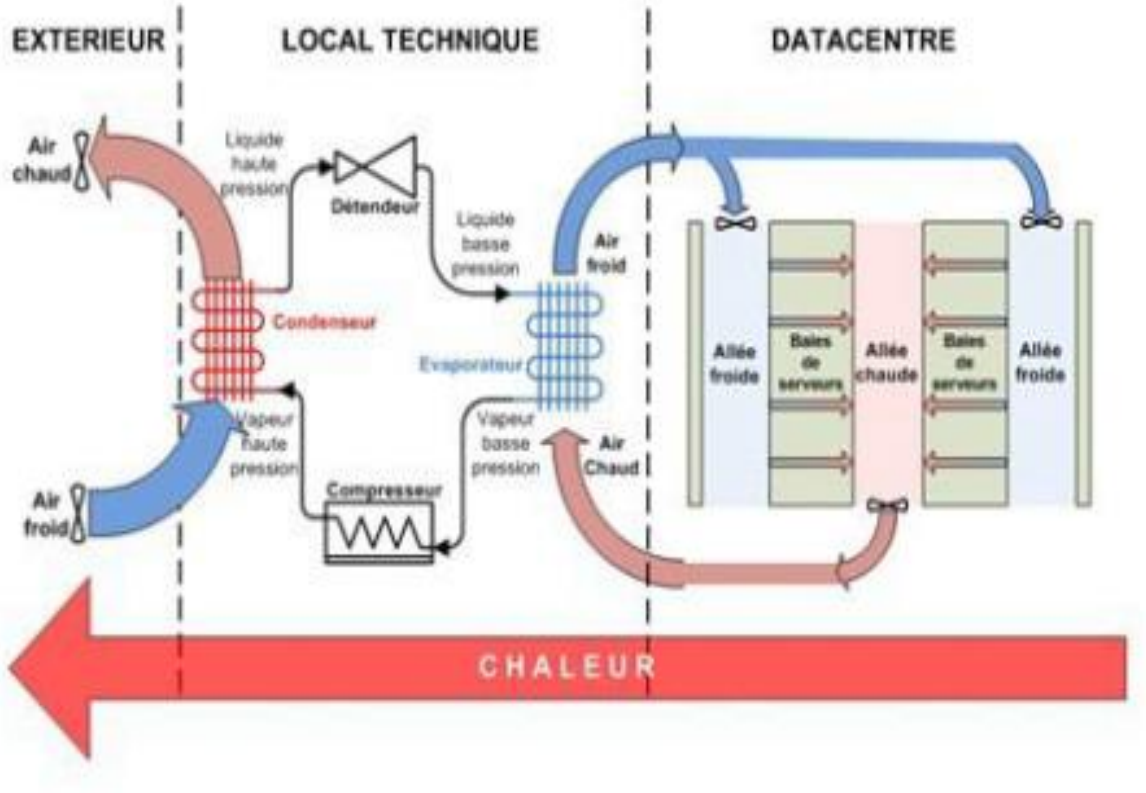

Figure6: Centrale de climatisation air – air

- **Machine frigorifique eau-air**

Dans le système de refroidissement eau-air, il s'agit d'utiliser de l'eau pour apporter de l'air frais au Datacenter. Une tour de refroidissement est nécessaire car elle permet de refroidir le circuit d'eau qui a son tour permettra de refroidir le condenseur. Au niveau du Datacenter, l'échange entre celui-ci et l'évaporateur se fait avec de l'air qui sera conduit dans les différentes allées froides (air froid) et de l'air chaud sera évacué des allées chaudes vers les évaporateurs. [18]

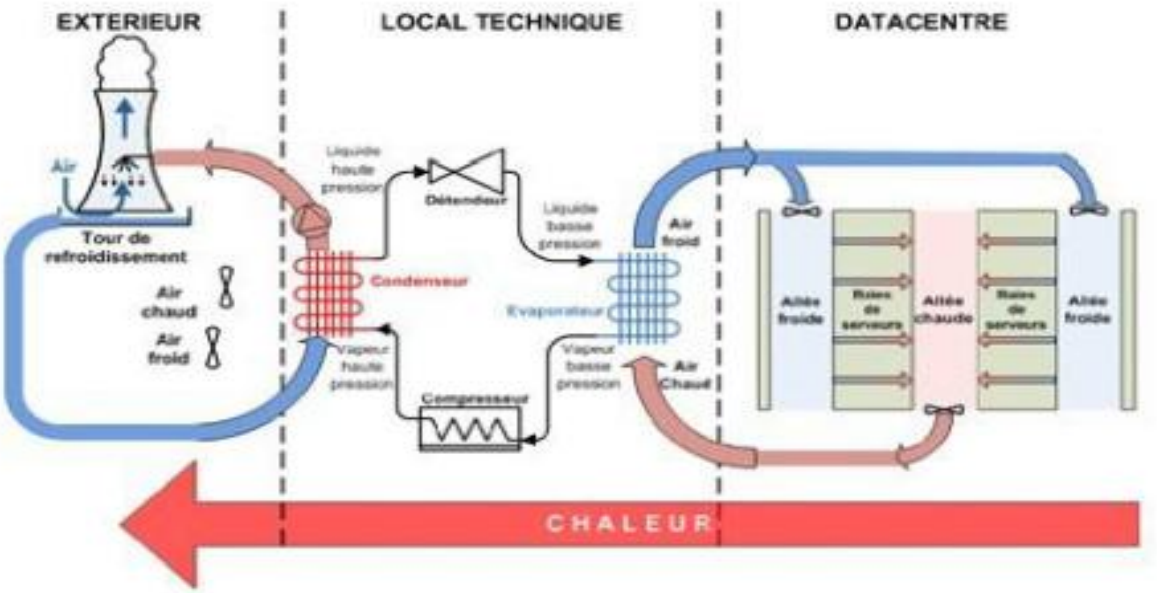

Figure7: Machine frigorifique eau – air

- **Le Free Cooling**

Le système largement exploité (réfrigérateur, congélateurs, climatiseurs) permet de produire du froid mais consomme en contrepartie une quantité significative d'énergie car fonctionnant avec un système de pompe à chaleur. Le Free Cooling a été créé pour palier cette consommation d'énergie devenue très couteuse pour les entreprises. On entend donc par Free Cooling, le refroidissement d'un Datacenter sans le recours à la pompe à chaleur. Il existe de nombreux systèmes permettant de réduire ou de supprimer le recours à la pompe à chaleur, nous avons pu déceler quatre types de Free Cooling. [19]

- Free Cooling à air-direct

Dans ce système, l'air frais de l'extérieur entre directement dans le circuit d'air de refroidissement du Datacenter. L'air extérieur peut éventuellement être rafraichi en passant dans un échangeur air - eau si le Datacenter dispose d'eau industrielle. Si nécessaire, il peut y avoir une pompe à chaleur qui ne prendra alors le relais qu'en cas de nécessité (lorsque la température extérieure est par exemple supérieure à 30°C). [20]

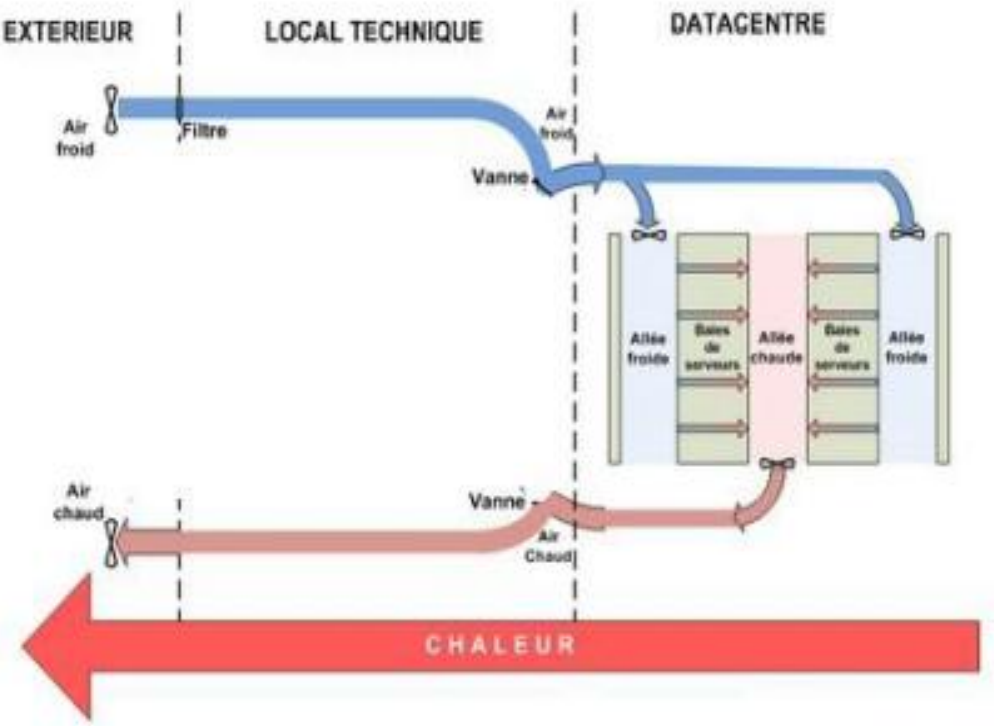

Figure8: Schéma du refroidissement d'un Datacenter en Free Cooling à air – direct

- Free Cooling à air indirect

Ce système est utilisé dans le cas où l'air extérieur frais est impropre pour une entrée directe dans le circuit de refroidissement du Datacenter (taux d'humidité trop élevée, trop chargé en particules) il est tout de même possible d'effectuer un échange de chaleur. L'air du circuit de refroidissement du Datacenter est recyclé et passe par un échangeur de chaleur air - air avec l'air extérieur. [21]

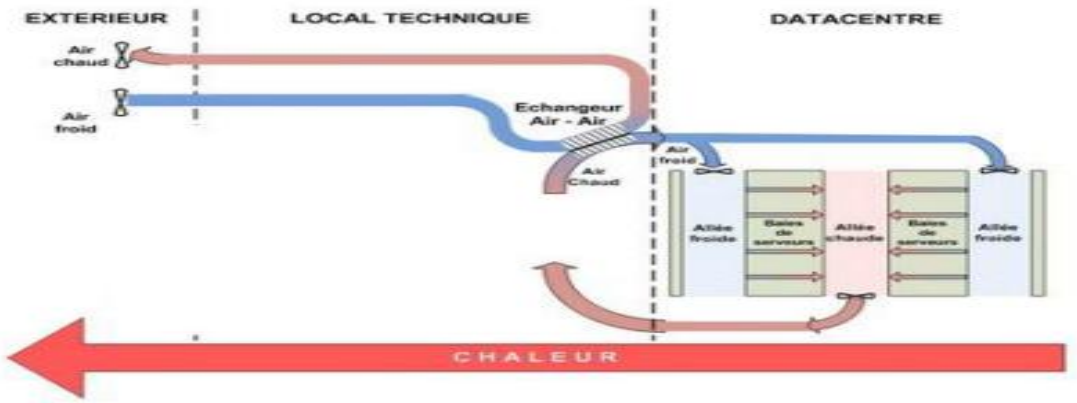

Figure9: Schéma du refroidissement d'un Datacenter en Free Cooling à air – indirect

- Free Cooling à eau direct

Pour l'utilisation de ce système, il faut que le Datacenter soit situé à proximité d'une source d'eau fraîche (cours d'eau, eau industrielle, etc.) pouvant être encore rafraichie à l'aide d'un échangeur eau - air ou par une tour de refroidissement (refroidissement par évaporation). Ainsi l'eau est directement distribuée dans le circuit d'eau glacée du Datacenter. Comme montré dans les systèmes précédents avec refroidissement par eau glacée, des ventilo-convecteurs, montés en série sur le circuit d'eau glacée permettent de distribuer le froid dans les allées du Datacenter. Ce système est encore plus efficace avec l'exploitation de baies réfrigérées (refroidissement au plus près de la source de chaleur). [22]

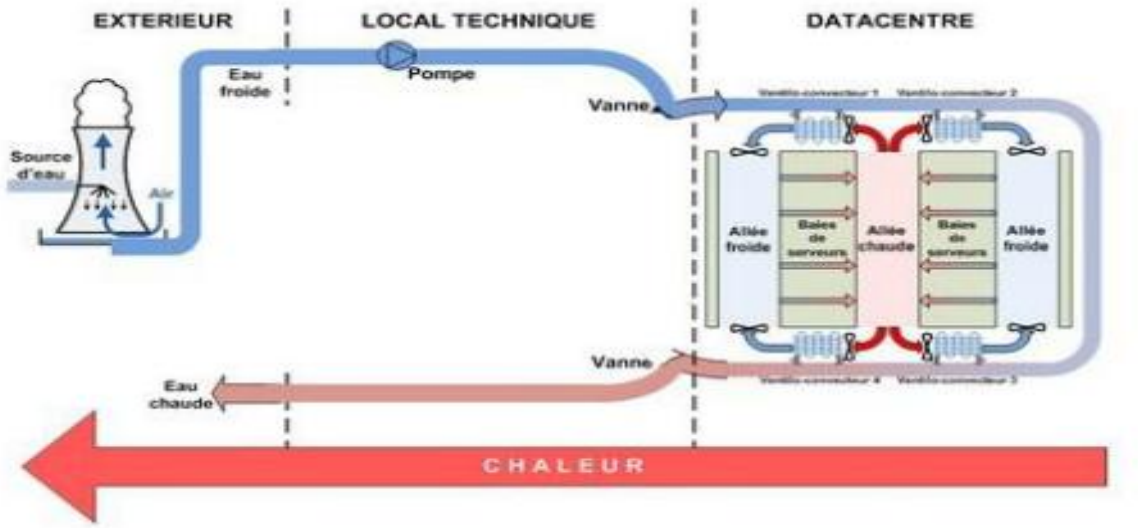

Figure10: Schéma du refroidissement d'un Datacenter en Free Cooling à eau – direct

- Free Cooling à eau indirect

La différence majeure entre ce système et le free Cooling à eau direct est qu'ici l'eau n'est pas directement distribuée dans le circuit d'eau glacée du Datacenter mais passe par un échangeur de chaleur eau - eau. [23]

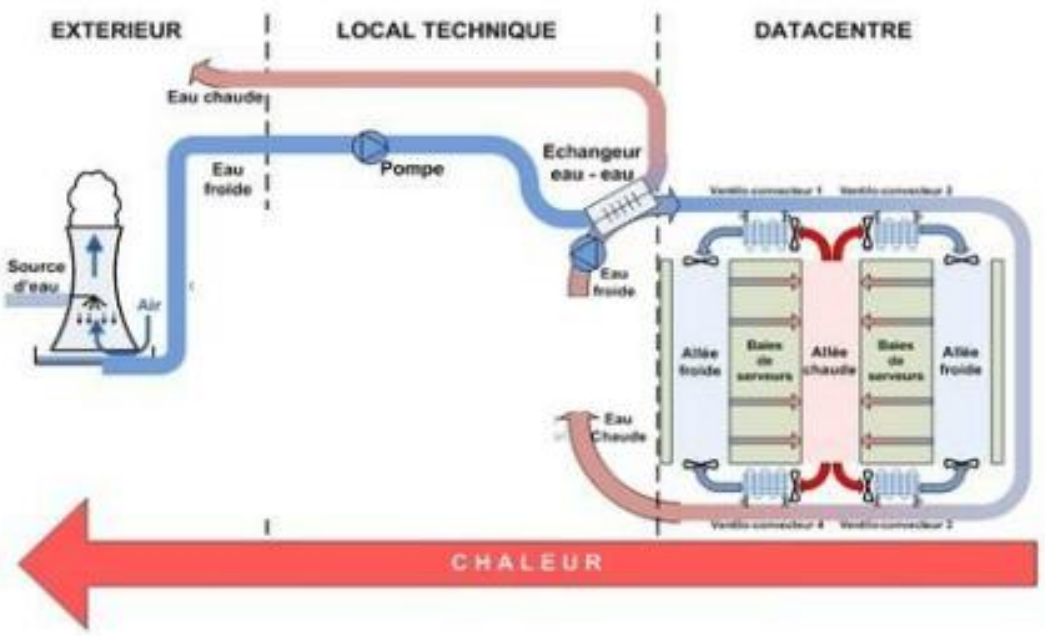

Figure11: Schéma du refroidissement d'un Datacenter en Free Cooling à eau – indirect

- ***Modes de climatisation***

Le mode de climatisation est la manière dont l'air frais est distribué dans l'enceinte du Datacenter. En effet des allées froides et des allées chaudes sont crées. Les allées froides sont les allées par lesquelles les racks prennent l'air frais et les allées chaudes sont celles par lesquelles ils dégagent l'air chaud. Les racks sont disposés de sorte à mettre face à face pour deux alignements de racks proches les faces de dégagement de la chaleur, créant ainsi les allées chaudes et les allées froides. Nous avons deux modes de climatisation :

- **Climatisation inverse**

La climatisation inverse est le premier mode de climatisation qui était mis en place avec les systèmes de climatisation générale. Cette climatisation se fait à partir du plancher. [24]

- **Climatisation directe**

C'est le mode de climatisation horizontal qui se fait à partir des splits actuels. Plusieurs méthodes de climatisation existent. Il faut donc les analyser avant de faire un choix qui convienne au Datacenter à implémenter en fonction du coût des équipements et des différents atouts naturels et industriels (cours d'eau proche, eau industrielle…) que possèdent celui-ci. La plupart de ces méthodes de climatisation ne saurait fonctionner sans source d'énergie, sans courant électrique. [25]

Identification des sources d'alimentation

Au niveau de la production et de la distribution de l'énergie dans les Datacenter, trois entités prennent part active. En effet, la production du courant électrique dans les Datacenter se fait par des sources d'alimentation. Pour la bonne utilisation de ce courant électrique, il existe des stabilisateurs et des onduleurs.

- ***Les sources d'alimentation***

Plusieurs sources d'alimentation en courant électrique existent, celles qui sont présentées dans ce rapport sont les plus importantes et les plus utilisés par les Datacenter.

➢ Les compagnies d'électricité

La source d'alimentation la plus utilisée au niveau des Datacenter est le courant électrique produit par les compagnies ou entreprises d'électricité. [26]

➢ Les groupes électrogènes

Les groupes électrogènes sont des dispositifs autonomes capables de produire de l'électricité. Ils sont utilisés en parallèle avec une autre source d'énergie. [27]

Figure12: un groupe électrogène

Les différentes sources d'alimentation produisent le courant électrique. Celui-ci est acheminé vers les installations mais passe d'abord par des stabilisateurs qui l'amplifient ou le diminuent de façon automatique en fonction des besoins des équipements dans les Datacenter.

- ***Les stabilisateurs de tension***

Les stabilisateurs de tension sont des équipements qui permettent de régler automatiquement la tension électrique en sortie. Ils sont capables d'augmenter ou de réduire de façon automatique la tension qui provient des différentes sources d'alimentation en fonction de la tension nominale souhaitée. Les stabilisateurs permettent donc de garantir une tension constante en sortie quelque soit la valeur de la tension en entrée. Le courant ainsi transformé sera acheminé via des câbles électriques jusqu'aux différents onduleurs. [28]

Figure13 : Stabilisateur de tension

- ***Les onduleurs***

➢ **Définition**

Egalement connus sous le nom d'UPS (Uninterruptible Power Supply) ou ASI (Alimentation Statique sans Interruption), les onduleurs assurent une source d'électricité propre. Ils ont trois fonctions principales: [29]

- Ils fournissent d'abord une source d'électricité propre (pas de variation de tension et de fréquence, pas de microcoupure ni de parasites.).
- Ils assurent ensuite une alimentation de secours en cas de coupure d'électricité pendant un certain temps.

- Les plus performants interagissent avec les systèmes d'exploitation pour sauvegarder et arrêter les applications sur les différents serveurs.

➢ **Les types d'onduleurs**

Il existe plusieurs types d'onduleurs mais trois sont actuellement utilisés. Ce sont:

- **Les onduleurs Off-Line**
- **Les onduleurs In-Line ou Line interactive**
- **Les onduleurs On-line**

Après avoir parcouru les différents contours du local technique du Datacenter c'est à dire le bâtiment, les méthodes d'évacuation de la chaleur et les sources d'alimentation, il est maintenant important de connaître les différents aspects de la sécurisation physique du Datacenter.

6.1.2. Aspects sécuritaires

Mécanismes de contrôle d'accès au Datacenter

Le contrôle d'accès physique au Datacenter consiste à vérifier l'identité des personnes qui accèdent au Datacenter. En effet, en utilisant des mécanismes appropriés, il est possible de connaître l'identité des personnes qui se présentent afin de leur interdire ou autoriser l'accès selon des prescriptions définies. Il existe plusieurs mécanismes de contrôle d'accès physique à un Datacenter. Les plus utilisés sont ceux énumérés ci-dessous: [30]

- ***Contrôle d'accès badge***

Au niveau du contrôle d'accès par badge, il s'agit au préalable d'établir des badges pour les personnes censées entrer à l'intérieur du Datacenter. A chaque fois qu'elles se présentent, il y a des agents de sécurité qui contrôlent la validité de ces badges. [31]

➢ **Avantage du contrôle d'accès par badge**

L'avantage du système d'accès par badge est qu'il est très facile à mettre en œuvre et son coût de déploiement n'est pas élevé.

➢ **Inconvénient du contrôle d'accès par badge**

Puisque ce système n'est pas automatique et qu'il fonctionne avec le consentement humain alors il y a risque d'intrusion en cas de non vigilance ou de corruption des agents de sécurité.

- ***Contrôle d'accès cartes magnétiques, empreinte digital, iris***

Le point commun de ces trois (03) méthodes de contrôle d'accès est qu'elles n'ont pas besoin de la présence d'un agent de sécurité pour effectuer les différents contrôles d'où un avantage par rapport au système d'accès par badge. En effet, ces méthodes utilisent des

lecteurs soit d'empreinte digital, soit de carte magnétique, soit d'iris reliés à une base de données dans laquelle l'on enregistre les différentes empreintes, cartes magnétiques ou iris qui sont autorisés à entrer à l'intérieur du Datacenter. Ces différents lecteurs à leur niveau se charge en utilisant des fonctions qui leur sont propres de contrôler avec efficacité l'accès au Datacenter. [32]

- **Avantage de ces trois méthodes de contrôle d'accès**

L'avantage commun de ces trois méthodes de contrôle d'accès est qu'il n'y a pas de contrôle humain donc les risques d'erreur sont moindres.

Mécanisme de surveillance du Datacenter: La Vidéosurveillance

- ***Définition***

La vidéosurveillance est une technologie qui permet à une unité de surveillance d'avoir des vidéos en temps réel du lieu qu'elle surveille. Pour le Datacenter, il s'agira d'avoir des vidéos de l'intérieur et de l'extérieur disponible sur internet que l'on pourra visualiser à travers une identification (login/mot de passe).

- ***Principe de fonctionnement***

Dans le système de vidéosurveillance, des caméras de surveillance sont connectées à internet et les résultats sont enregistrés sous forme de vidéos AVI. Ces vidéos sont accessibles via un espace FTP accessible par identification. Son principe de fonctionnement est résumé dans le schéma ci-dessous.

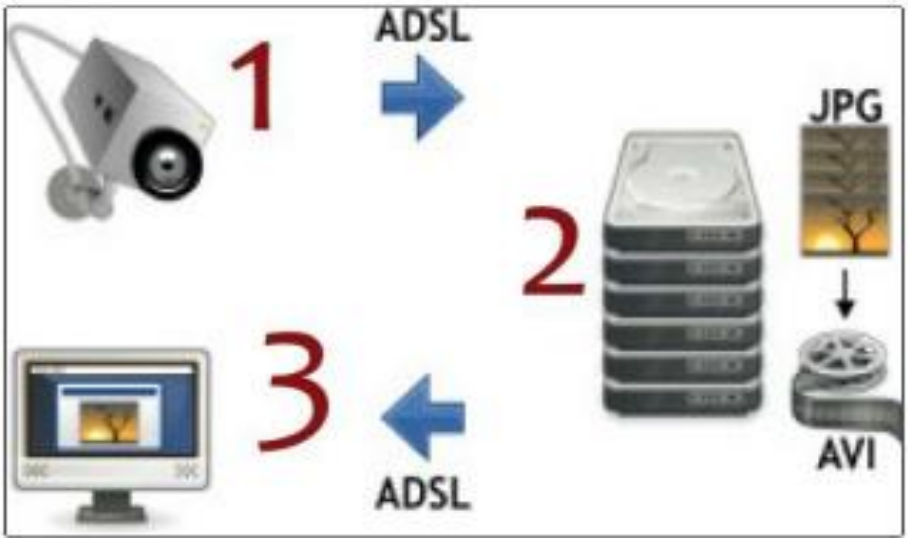

Figure14: Fonctionnement de la vidéosurveillance

1 : La caméra web est connectée à un ordinateur qui envoie un signal à une unité de traitement

2 : Cette unité de traitement réceptionne le signal de la caméra sous forme d'une suite d'images JPG, qui sont ensuite assemblées sous forme de vidéos. Celles ci sont mises à disposition sur Internet.

3 : l'on peut donc visionner ou télécharger la vidéo depuis un ordinateur connecté à Internet.

La vidéosurveillance est très importante pour la sécurité du Datacenter car elle permet d'obtenir des vidéos en temps réel des recoins du Datacenter. Ce qui permet donc de prendre des dispositions pratiques en cas d'intrusions et même d'incendie. Cependant plusieurs systèmes sont mis en place pour éviter les incendies dans les Datacenter.

Systèmes anti-incendie

Le risque d'incendie dans les Datacenter est élevé du fait de la présence de matériels électroniques et mécaniques qui produisent beaucoup de chaleur. Pour la détection et l'extinction de l'incendie, plusieurs méthodes existent, celles que nous présentons dans ce document sont les plus utilisées.

- ***Méthodes de détection d'incendie***

Il est préférable dans un Datacenter de détecter l'incendie afin d'en apporter une solution rapide que d'attendre son apparition et de chercher à l'extraire. Différents appareils sont disponibles sur le marché pour la détection de fumée et pour la détection de l'incendie. Ci-dessous sont présentés quelques uns. [33]

- **Détecteur de fumée**

Les détecteurs de fumée ont pour rôle de détecter très rapidement la fumée et d'alerter les personnes concernées (à partir d'alarme) pour prendre des dispositions pratiques afin d'éviter l'incendie. Ils sont le plus souvent placés sur les plafonds des salles à contrôler. [34]

Figure15: Un détecteur de fumée

- **Détecteur d'incendie**

Les détecteurs d'incendie jouent le même rôle que les détecteurs de fumée. Ils permettent de détecter la présence d'un incendie. La majorité de ces détecteurs utilisent l'infrarouge ou l'ultraviolet. [35]

Figure16 : Système infrarouge pour détection d'incendie

6.2. Etude des services du Datacenter

6.2.1. Méthodes d'hébergement dans les Datacenter

Les Datacenter, comme nous l'avons signifié dans les paragraphes précédentes de notre rapport ont été très améliorés ces derniers temps pour un but commercial. En effet, les Datacenter hébergent des serveurs informatiques, des équipements réseau, des logiciels et espaces de stockage de données d'entreprises tierces.

Les méthodes d'hébergement dans les Datacenter sont diverses et variées. Ainsi ces méthodes partent depuis l'hébergement de toute une baie jusqu'à l'hébergement d'une partie d'un serveur ou l'utilisation de simples applications.

Les choix de la méthode d'hébergement, des différents systèmes d'exploitation et outils de configuration des serveurs sont souvent laissés aux entreprises clientes. Les différentes méthodes d'hébergement qui existent sont:

housing ou Méthode de colocation

Les Datacenter proposent généralement des formules de baies entières, de demi-baie, de quart de baie, ou bien d'hébergement des propres serveurs du client à l'unité, on parle alors de colocation (en anglais housing). [36]

Ce type d'offre permet au client d'installer les serveurs de son choix et d'en avoir la totale maîtrise. Le Datacenter fournit ainsi l'infrastructure d'accueil des serveurs, la bande passante ainsi qu'un certain nombre de services et de garanties. Les différentes offres de Housing sont :

- **Méthode de baies privées**

C'est la méthode par laquelle l'entreprise cliente sollicite une baie entière dans le Datacenter. Cette entreprise y place ses serveurs qui sont sa propriété privée et les configure à sa manière. Elle ne partage donc pas la baie avec d'autres entreprises clientes.

- **Méthode de baies partagées**

Dans la méthode de baies partagées, différentes entreprises clientes sollicitent la même baie pour héberger leurs différents serveurs. En effet, chaque entreprise peut solliciter soit une demi-baie ou un quart de baie. Les clients y placent les serveurs de leur choix et les configurent à leur manière car ils en ont une totale maîtrise.

- **Hébergement de serveurs propres**

A ce niveau, l'entreprise cliente sollicite l'hébergement d'un ou plusieurs de ses serveurs.

Dedicated hosting ou méthode d'hébergement dédié

L'hébergement dédié consiste à mettre à la disposition du client un serveur complet. En effet, une entreprise tierce sollicite de façon intégrale un serveur dans le Datacenter. A la différence de la méthode de serveur propre, le serveur dédié appartient au Datacenter. [37]

Mutualized hosting ou méthode d'hébergement mutualisé

La mutualisation des serveurs consiste pour plusieurs entreprises clientes d'utiliser les mêmes ressources d'un même serveur. Les serveurs mutualisés sont utilisés pour l'hébergement des sites internet, de mail, de nom de domaine etc. Ce type de formule propose donc un serveur avec une configuration donnée et une offre logicielle (serveur, bases de données, comptes de messagerie, serveur de listes de diffusion, etc.) ainsi qu'un espace de stockage bien défini. Dans ce type de solution, les clients n'ont pas accès directement au serveur en tant qu'administrateur, la configuration se fait ainsi par l'intermédiaire d'interfaces web. Il est donc important de vérifier les paramètres de configuration sur lesquelles il est possible d'agir (configuration du serveur de nom, du serveur web, du système de gestion de base de données, etc.). [38]

Le système d'exploitation et les différents outils de configuration des serveurs mutualisés ne sont pas choisis ni gérés par les entreprises clientes mais par le gestionnaire du Datacenter.

Les différents critères de choix des serveurs mutualisés sont :

- Espace disque alloué
- Bande passante autorisée
- Type de serveur
- Langages supportés côté serveur
- Noms de domaines
  -Possibilité de configurer les domaines virtuels
  - Nombre de noms de domaines
  -Nombre de sous-domaines
- Accès par SSH
- Mise à jour des fichiers par FTP
- Serveur de messagerie
  -Présence d'un webmail
  -Nombre de comptes email alloués
  -Nombre d'alias mail autorisés
  -Possibilité de collecter les mails sur un alias
  -Possibilité de forwarder (faire suivre) les mails vers une adresse externe
  -Présence d'un antivirus et d'un antispam
  -Gestionnaire de liste de diffusion fourni
- Serveur de gestion de bases de données

6.2.2. La virtualisation

Définition

La virtualisation, très utilisée dans les Datacenter est définie comme l'ensemble des techniques matérielles et logicielles qui permettent de faire fonctionner sur une machine physique des systèmes qui ne sont pas conçus initialement pour son architecture. Par exemple, grâce à la virtualisation, il est possible de faire fonctionner plusieurs systèmes d'exploitation, séparément les uns des autres sur un même serveur physique, comme s'ils fonctionnaient sur des machines physiques distinctes. [39]

Les différents types de virtualisation

Il existe différents types de virtualisation mais le plus connus est la virtualisation des serveurs. Ces différents types de virtualisation sont :

- Virtualisation des serveurs
- Virtualisation des applications

- Virtualisation des postes de travail
- Virtualisation des réseaux

Quelques outils de virtualisation

Les outils les plus connus et les plus utilisés dans le domaine de la virtualisation sont :

- **Vmware**

Vmware est le leader mondial des solutions de virtualisation pour les serveurs et les postes de travail 32 bits. Il offre une plate-forme de virtualisation performante capable d'évoluer sur plusieurs ordinateurs physiques et périphériques de stockage interconnectés pour former une infrastructure virtuelle complète. [40]

- **Microsoft**

Les offres proposées par Microsoft sont : [41]

- Virtual Server 2005 R2

Microsoft Virtual Server 2005 R2 Édition Entreprise est un outil stable pour la consolidation de plusieurs charges de travail sur un serveur physique, permettant aux organisations d'utiliser plus efficacement leurs ressources matérielles.

- Windows Server 2008 Hyper-V

Windows Server 2008 Hyper-V est le moteur de virtualisation (hyperviseur) fourni dans Windows Server 2008.

- System Center Virtual Machine Management (SCVMM)

SCVMM est une solution d'administration complète pour les Datacenter virtualisé qui augmente l'utilisation des serveurs physiques, accélère le déploiement, et centralise l'administration des infrastructures de systèmes virtuels.

6.2.3. Les services du Datacenter

Le Cloud computing

Le Cloud computing ou informatique en nuages est un concept faisant référence à l'utilisation de la mémoire et des capacités de calcul des ordinateurs et des serveurs répartis dans le monde entier, et liés par un réseau, tel qu'Internet. Le Cloud Computing désigne donc une forme de traitement et un ensemble de ressources informatiques massivement extensibles, exploités par de multiples clients externes sous forme de services fournis via Internet.

Les utilisateurs ne sont plus propriétaires de leurs serveurs informatiques, mais peuvent ainsi accéder de manière évolutive à de nombreux services en ligne sans avoir à gérer

l'infrastructure sous-jacente, souvent complexe. Les applications et les données ne se trouvent plus sur l'ordinateur local, mais dans un nuage (Cloud) composé d'un certain nombre de serveurs distants interconnectés au moyen d'une excellente bande passante indispensable à la fluidité du système. L'accès au service se fait par une application standard facilement disponible, la plupart du temps un navigateur Web.

Le Cloud Computing est constitué de trois principaux services qui sont :

- **Le SaaS**

Le logiciel en tant que service ou Software as a Service (SaaS) est un concept consistant aux Datacenter à proposer à des entreprises clientes un abonnement à un logiciel plutôt que l'achat d'une licence. Il n'y a alors plus besoin d'installer une application de bureau ou client-serveur par ces entreprises. Les clients ne paient donc pas pour posséder le logiciel en lui-même mais plutôt pour l'utiliser. Ils l'utilisent soit directement via l'interface disponible, soit via des API fournies (souvent réalisées grâce aux Web Services). [42]

Les avantages du SaaS sont :

- Abstraction de l'infrastructure
- Un modèle de paiement à l'usage
- Une consommation à la demande
- Une montée en charge et une haute disponibilité

- **Le PaaS**

La plateforme en tant que service ou Platform as a Service (Paas) est comme le SaaS un service qui peut être proposé par les Datacenter permettant aux entreprises clientes de développer rapidement et exécuter des applications.

Le modèle PaaS fournit une plate-forme de développement basée sur des langages de programmation et des outils supportés par le Datacenter, permettant un déploiement automatique sur l'infrastructure Cloud de celui-ci.

Et comme un service public, le concept PaaS s'appuie sur un calcul de consommation ou sur un modèle d'abonnement ; ainsi, les utilisateurs ne paient que pour ce qu'ils utilisent. Ce modèle permet aux fournisseurs indépendants de logiciels et aux services informatiques des entreprises de se consacrer à l'innovation plutôt qu'à l'infrastructure complexe. Grâce au modèle PaaS, les entreprises peuvent utiliser une part considérable de leur budget consacrée auparavant au maintien du système à la création de nouvelles applications à réelle valeur ajoutée.

En plus de posséder les mêmes avantages que le SaaS, le PaaS permet de concevoir des applications personnalisables. [43]

- **L'Iaas**

L'infrastructure en tant que service ou Infrastructure as a Service peut être comparée à un Datacenter dynamique, élastique et virtualisé. L'IaaS est une usine de production d'infrastructures hardware apportant flexibilité, fiabilité et montée en charge. Il présente un déploiement simplifié. [44]

Les avantages de l'IaaS sont :

- Déploiement rapide
- Outils de monitoring et de reporting intégrés
- Réduction de coûts de maintenance

Le computing on-demand ou informatique à la demande est un concept qui consiste à allouer aux entreprises de la puissance de calcul à la demande, en fonction de leur besoin.

Cette approche radicalise la notion d'infogérance puisque l'infrastructure informatique n'est plus la propriété du client, ni même physiquement présente dans ses locaux, mais louée auprès d'un Datacenter distant.

En effet, la mise en œuvre de l'informatique à la demande se base également sur le Grid Computing ou technologie de "grille" qui désigne la mutualisation des ressources informatiques.Cette approche permet cependant d'assurer à l'entreprise cliente une fiabilité et une disponibilité des ressources dont elle a besoin.

7. Conclusion

Dans ce chapitre nous allons montrer c'est quoi un centre de donnée en définissant les mécanismes pour son implémentation ainsi que les services offertes.

Dans le chapitre suivant nous allons faire une étude comparative entre les solutions d'accès possible en donnant le meilleur choix avec le matériel associés pour implémenter cette solution.

Chapitre III Etude Comparative

1. Introduction

Comme le Datacenter offre un ensemble de services dans différents domaines, alors il reçoit plusieurs demandes des services ce qui génère un conflit d'adresses entre les clients.

Dans ce chapitre nous allons essayer de présenter la problématique de façon détaillée. Ensuite, nous allons proposer un ensemble de scénarios pour la résoudre. Puis, nous allons choisir un scénario répondant aux besoins techniques et financiers. Finalement, après avoir choisi la solution nous proposer les équipements et l'architecture réseau convenable.

2. Présentation du problématique

Comme on le décrit dans le chapitre précédent, le Datacenter offre une connexion réseau permanente 24/24 et 7jrs/7 aux clients et aussi plusieurs clients peuvent se connecter simultanément ce qui peut générer un problème d'accès.

2.1. Scenario de connexion

Dans un datacenter le client peut se connecter de deux façons soit par une ligne spécialisée ou à travers un VPN.

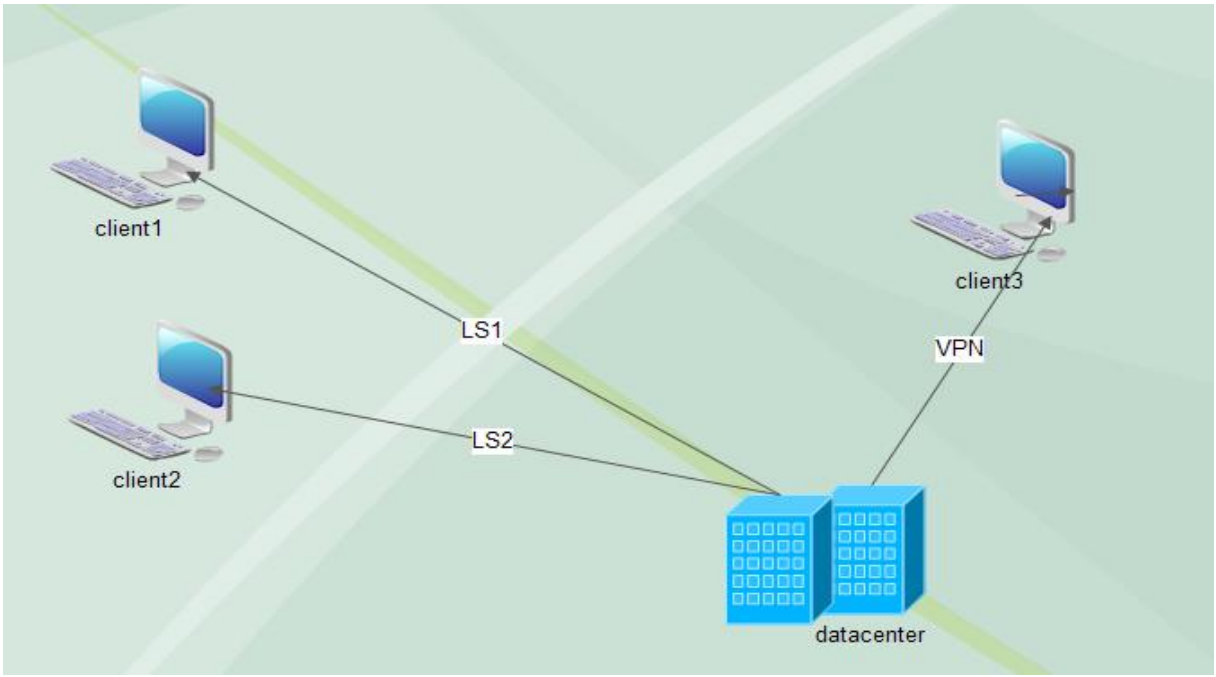

Figure17: description connexion client-datacenter

2.1.1. Ligne spécialisée

La ligne spécialisée (LS) est une liaison établie d'une manière permanente. Elle est constituée d'un ou plusieurs tronçon d'un réseau ouvert au public et réservé à l'usage exclusif d'une entreprise.

La ligne spécialisée supporte un trafic important symétrique et n'est pas tributaire du temps de connexion. Ce service convient aux entreprises dont l'activité nécessite une disponibilité de liaisons car elle leur permet d'effectuer des échanges de données, en évitant toute coupure de connexion préjudiciable à leurs activités.

- **Avantage**

  - Un accès rapide permanent
  - Une vitesse de transmission
  - Une disponibilité garantie
  - Une facturation forfaitaire

2.1.2. VPN (Virtual Private Network)

VPN : virtual Private Network ou RPV (réseau privé virtuel) en francais est une technique permettant à un ou plusieurs postes distants de communiquer de manière sure, tout en empruntant les infrastructures publiques. Ce type de liaison est apparu suite à un besoin croissant des entreprises de relier les différents sites, et par une façon simple et économique.

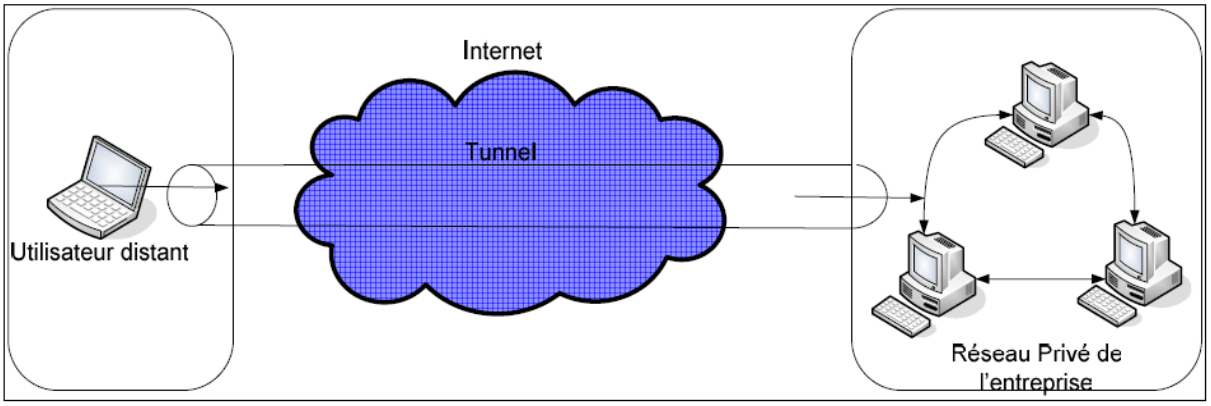

Figure18 : schéma d'un VPN

Principe de fonctionnement

Un réseau VPN repose sur un protocole appelé ''protocole de tunneling''. Ce protocole permet de faire circuler les informations de l'entreprise de façon cryptée d'un bout à l'autre de tunnel. Ainsi, les utilisateurs ont l'impression de se connecter directement sur le réseau de leur entreprise.

Le principe de tunneling consiste à construire un chemin virtuel après avoir identifié l'émetteur et le destinataire. Par la suite, la source chiffre les données et les achemine en empruntant ce chemin virtuel. Afin d'assurer un accès aisé et peu couteux aux intranets ou aux extranets d'entreprise, les réseaux privés virtuels d'accès simulent un réseau privé, alors qu'ils utilisent en réalité une infrastructure d'accès partagée, comme internet.

Les donnés à transmettre peuvent être prises en charge par un protocole différent d'IP. Dans ce cas, le protocole de tunneling encapsule les données en ajoutant un en-tête. Le tunneling est l'ensemble des processus d'encapsulation, de transmission et de désencapsulation.

Les principaux avantages d'un VPN :

- Sécurité : assure des communications sécurisées et chiffrées.
- Simplicité : utilise les circuits de télécommunication classiques.

Les contraintes d'un VPN

Le principe de VPN est d'être transparent pour les utilisateurs et pour les applications y ayant accès. Il doit être capable de mettre en œuvre les fonctionnalités suivantes :

- Authentification d'utilisateur : seuls les utilisateurs autorisés doivent avoir accès au canal VPN.

- Cryptage des données : lors de leur transport sur le réseau public, les données doivent être protégées par un cryptage efficace.

- Gestion de clés des cryptages pour client et le serveur doivent pouvoir être générées et régénérées.

Types VPN

Les architectures VPN sont de 3 types :

- Le VPN intranet qui permet de connecter de façon permanente les différents établissements de l'entreprise ou les télétravailleurs avec le site principal.

- Le VPN nomade qui est une extension du VPN Intranet. Il permet de connecter les utilisateurs nomades aux bureaux de l'entreprise.

- Le VPN extranet qui est aussi une extension du VPN intranet. Il permet de connecter les utilisateurs ne faisant pas partie de l'entreprise (partenaires, fournisseurs, clients…).

2.2. Description du problème

Un client donné dans une entreprise veut recevoir ses services, pour cela tente à se connecter à travers son réseau local c'est-à-dire avec son adresse IP privée.

Les clients demandeurs des services se connectent au Datacenter via l'adresse locale de son entreprise. Puisque l'entreprise fournisseur des services reçoit plusieurs demandes, on peut avoir un conflit d'adresse IP.

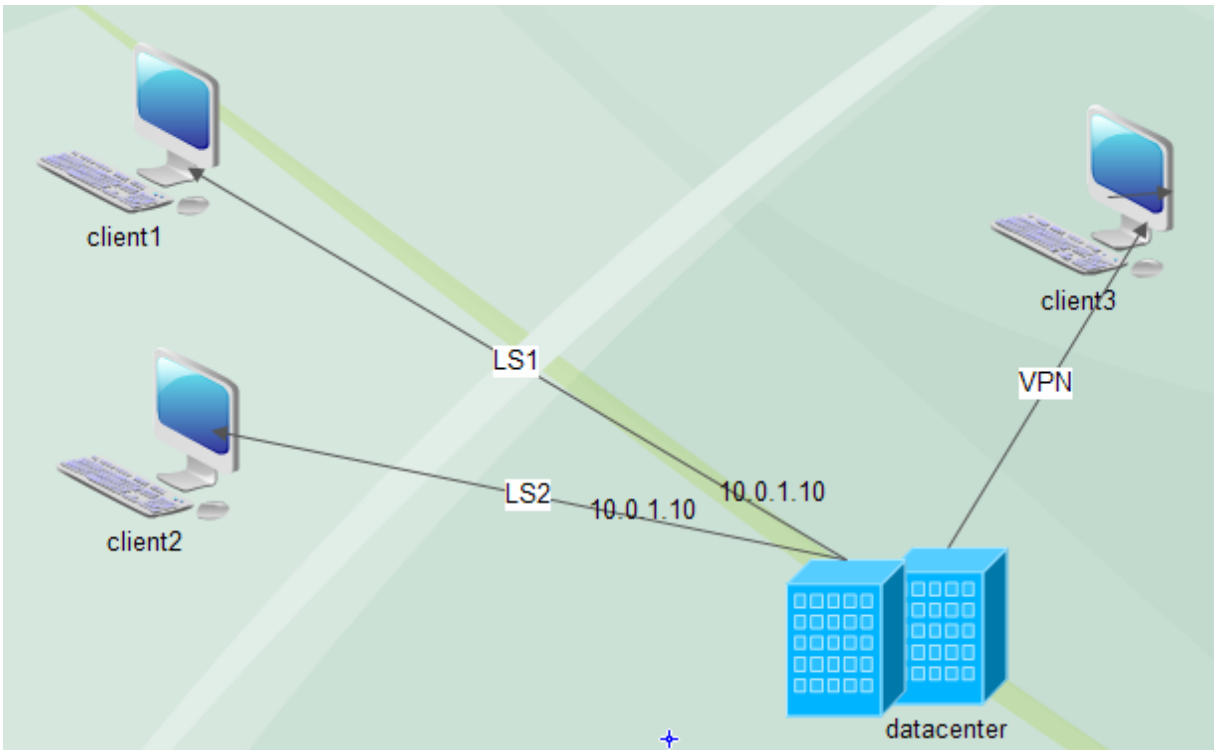

Figure19 : schéma descriptif du problème

Pour remédier à ce problème CBI propose quelque scénario de solution à implémenter de sa part.

3. Etude comparative des solutions proposées

Parmi les solutions suggérées nous trouvons :

- Intégration du NAT
- Utilisation des contextes
- Utilisation des VRF

Dans la suite nous allons présenter et expliquer chaque solution en montrant l'impact financière et de coté administration de chacune.

3.1. Intégration du NAT

En réseau informatique, on dit qu'un routeur fait du ***Network Address Translation*** (NAT) lorsqu'il fait correspondre les adresses IP internes non-uniques et souvent non routables d'un intranet à un ensemble d'adresses externes uniques et routables. Ce mécanisme permet notamment de faire correspondre une adresse externe publique visible sur Internet à toutes les adresses d'un réseau privé, et pallie ainsi l'épuisement des adresses IPv4.

3.1.1. Implémentation du NAT

Les correspondances entre les adresses privées (internes) et publiques (externes) sont stockées dans une table sous forme de paires (*adresse interne*,*adresse externe*). Lorsqu'une trame est émise depuis une adresse interne vers l'extérieur, elle traverse le routeur NAT qui remplace, dans l'en-tête du paquet TCP/IP, l'adresse de l'émetteur par l'adresse IP externe. Le remplacement inverse est fait lorsqu'une trame correspondant à cette connexion doit être routée vers l'adresse interne. Aussi, on peut réutiliser une entrée dans la table de correspondance du NAT si aucun trafic avec ces adresses n'a traversé le routeur pendant un certain temps (paramétrable).

Tableau3 : exemple d'une table NAT

IP interne	IP externe	Durée (s)	Réutilisable ?
10.101.10.20	193.48.100.174	1 200	non
10.100.54.251	193.48.101.8	3 601	oui
10.100.0.89	193.48.100.46	0	non

La première ligne indique que la machine interne, possédant l'adresse IP 10.101.10.20 est traduite en 193.48.100.174 quand elle communique avec le monde extérieur. Elle n'a pas émis de paquet depuis 1 200 secondes, mais la limite étant 3 600, cette entrée dans la table lui est toujours assignée. La seconde machine est restée inactive pendant plus de 3 600 secondes, elle est peut-être éteinte, une autre machine peut reprendre cette entrée (en modifiant la première colonne puisqu'elle n'aura pas la même IP interne). Enfin, la dernière machine est actuellement en conversation avec l'extérieur, le champ de Durée étant 0.

3.1.2. Types de NAT

NAT statique

Où un ensemble d'adresses internes fait l'objet d'une traduction vers un ensemble de même taille d'adresses externes.

Ces NAT sont dites *statiques* car l'association entre une adresse interne et son homologue externe est statique (première adresse interne avec première externe…). La table d'association est assez simple, de type un pour un et ne contient que des adresses. Ces NAT servent à donner accès à des serveurs en interne à partir de l'extérieur.

NAT dynamique

Où un ensemble d'adresses internes est transféré dans un plus petit ensemble d'adresses externes. Ces NAT sont dites dynamiques car l'association entre une adresse interne et sa contre-partie externe est créée dynamiquement au moment de l'initiation de la connexion. Ce sont les numéros de ports qui vont permettre d'identifier la traduction en place : le numéro du port source (celui de la machine interne) va être modifié par la machine. Il va servir pour identifier la machine interne.

3.1.3. NAT de côté CBI

Pour résoudre le problème envisagé (conflit d'adresse), parmi les solutions proposées à CBI l'intégration du NAT. Alors nous allons configurer le NAT dans le routeur de coté CBI c'est-à-dire de coté Datacenter sans intervenir le client.

Dans notre cas puisque chaque client de la même entreprise a des droits d'accès différents à l'autre, il nous faut de donner à chaque adresse interne une adresse externe, c'est pour cela nous choisissons le NAT statique.

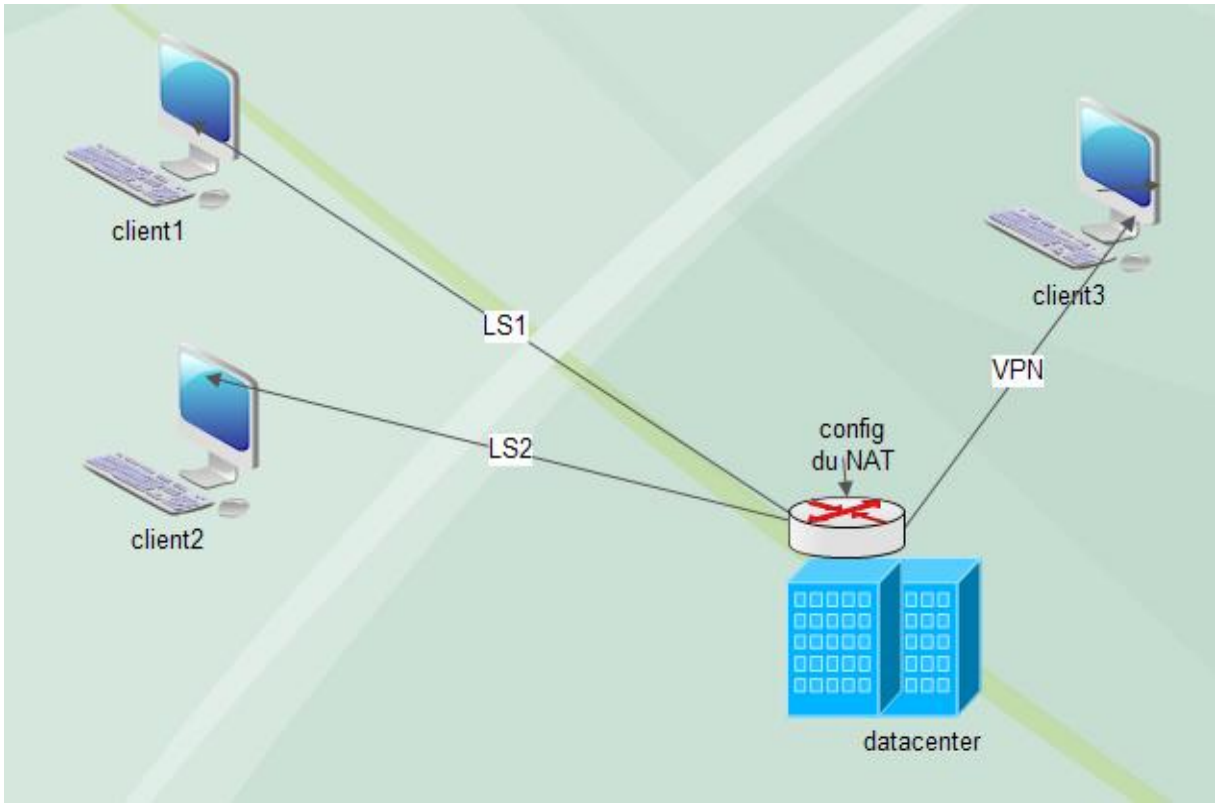

Figure 20: schéma descriptif du scenario

3.1.4. Avantages et inconvénients du NAT de côté CBI

Le NAT c'est une solution répondant aux contraintes envisagés, elle est aussi moins chère, et il n'y a un pas impact financier sur l'entreprise fournisseur des services (CBI).

D'un autre côté, si l'entreprise possède plusieurs demandeurs de services, il nous faut toujours une intervention pour la configuration, et aussi nous aurons une surcharge des lignes de la configuration au niveau de routeur.

Pour conclure le NAT est légère de côté financier, par contre il est trop lourd de côté technique.

3.2. Implémentation des contextes firewall

D'après le chapitre précédent nous connaissons sans doute le principe de l'outil VMWARE permettant la virtualisation des machines physiques afin de mutualiser l'exploitation de divers types de système d'exploitation. Ce concept a subit certaines évolutions, notamment dans le domaine des équipements de sécurité.

3.2.1. Concept des contextes firewall

Certains constructeurs dont Juniper ou Cisco intègrent des fonctionnalités permettant la virtualisation des appliances. Le concept initial est relativement simple, mutualiser une appliance physique en des multiples instances logiques. On peut prendre l'image qu'une VMWARE avec son hyperviseur ESX SERVER permettant d'héberger sur un même système hôte plusieurs systèmes hotes (windows 2003 server, Linux Redhat etc …).

3.2.2. Présentation des contextes de sécurité

En se basant sur la virtualisation, nous pouvons avoir un seul firewall contenant plusieurs pare-feu virtuels, appelés contextes de sécurité

Chaque contexte fonctionne comme un périphérique virtuel indépendant, avec sa propre politique de sécurité, les interfaces et les administrateurs.

De nombreuses fonctionnalités sont prises en charge en mode multi-contexte, y compris les tables de routage, des fonctions de pare-feu, IPS, et la gestion.

3.2.3. Les cas d'utilisation des contextes de sécurité

Nous pouvons utiliser de multiples contextes de sécurité dans les situations suivantes:

- si un prestataire de service et veut vendre des services de pare-feu pour de nombreux clients. En permettant à de multiples contextes de sécurité sur le FWSM, il peut implémenter une solution rentable et peu encombrante qui maintient tout le trafic client distinct et sûr, et facilite également la configuration

- une grande entreprise ou un campus d'université veut garder les départements à part entière.

- une entreprise veut fournir des stratégies de sécurité distinctes pour différents départements.

- un réseau nécessite une distinction entre les utilisateurs.

Comment le firewall classifie les paquets

Chaque paquet qui arrive sur le FW doit être classé, de sorte que le FW peut déterminer dans quel contexte d'envoyer un paquet. Le classificateur vérifie les caractéristiques suivantes:

- Interface Source (VLAN).
- L'adresse de destination.

Pour définir un contexte, on doit l'affecter à une interface VLAN d'utilisateur et l'adresse IP de destination et on définit aussi une interface administrateur pour gérer l'ensemble des contextes.

Puisque chaque client dans un contexte est défini par une interface VLAN, on peut partager un VLAN entre les contextes.

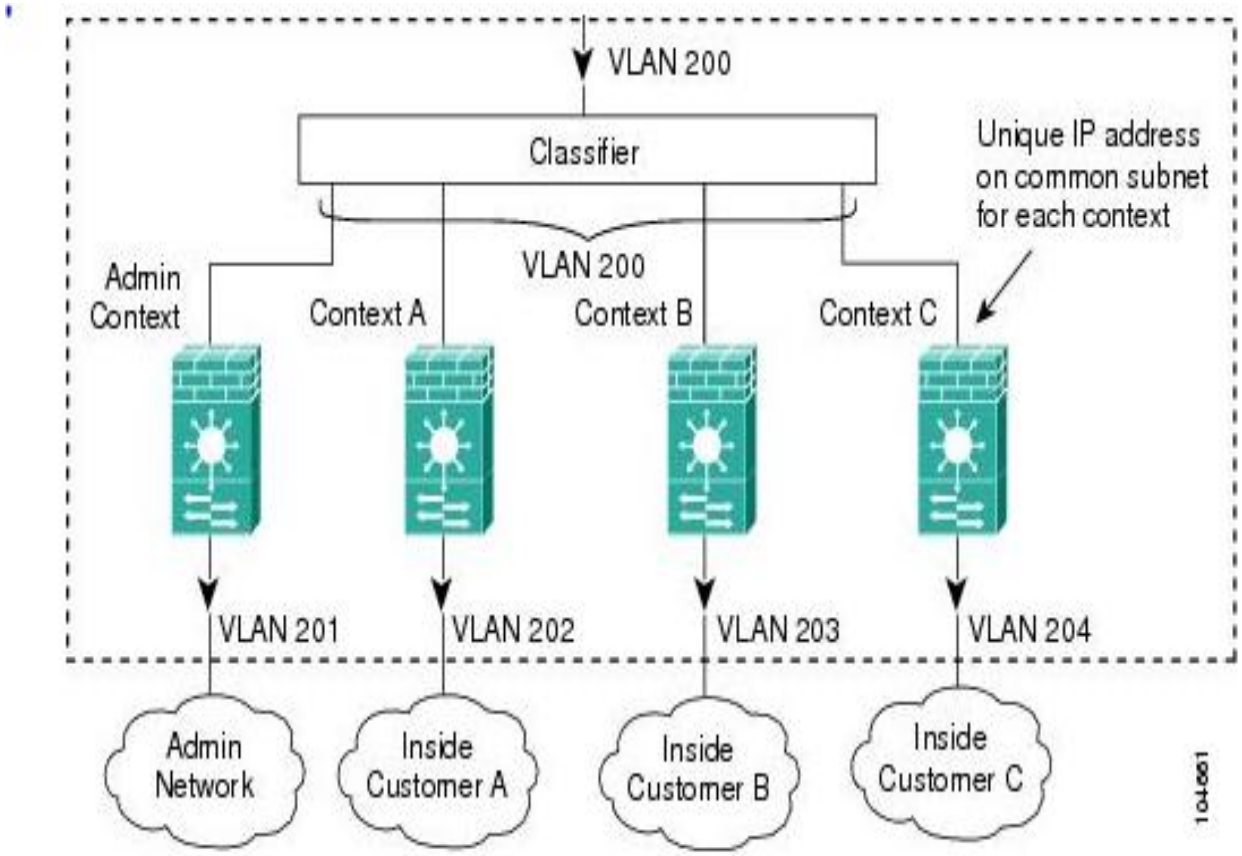

Figure21 : exemple de multiple contexte de sécurité

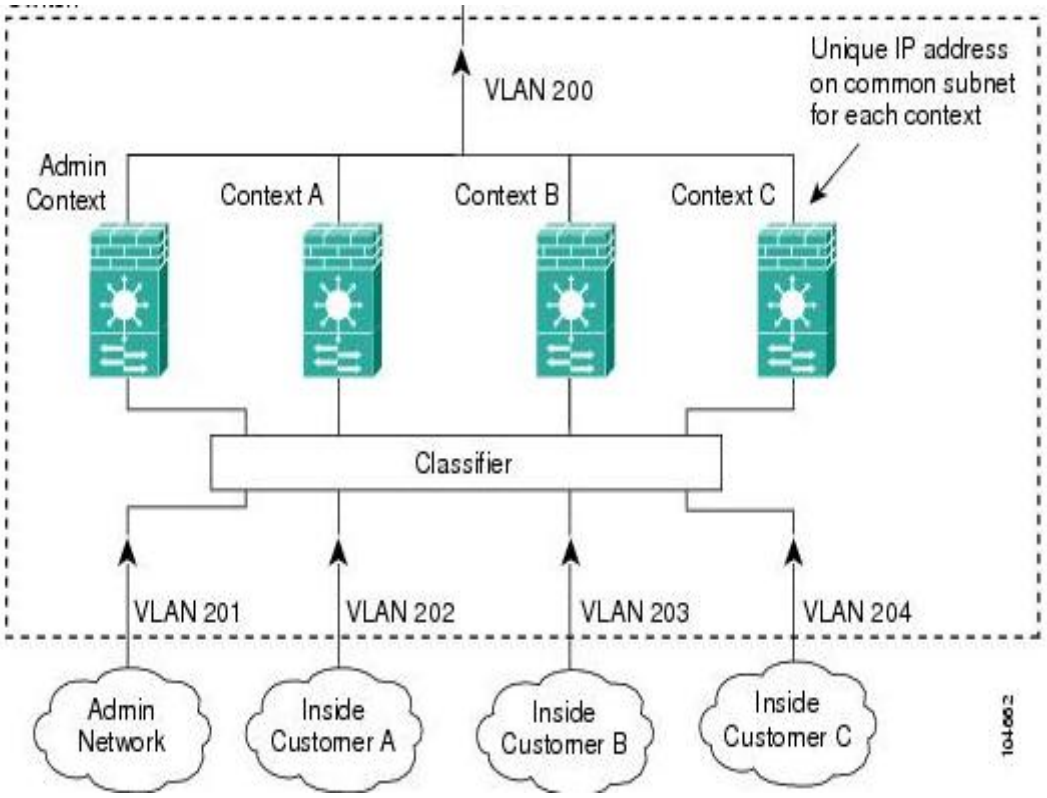

Figure22 : exemple du trafic venant de réseaux Intérieur

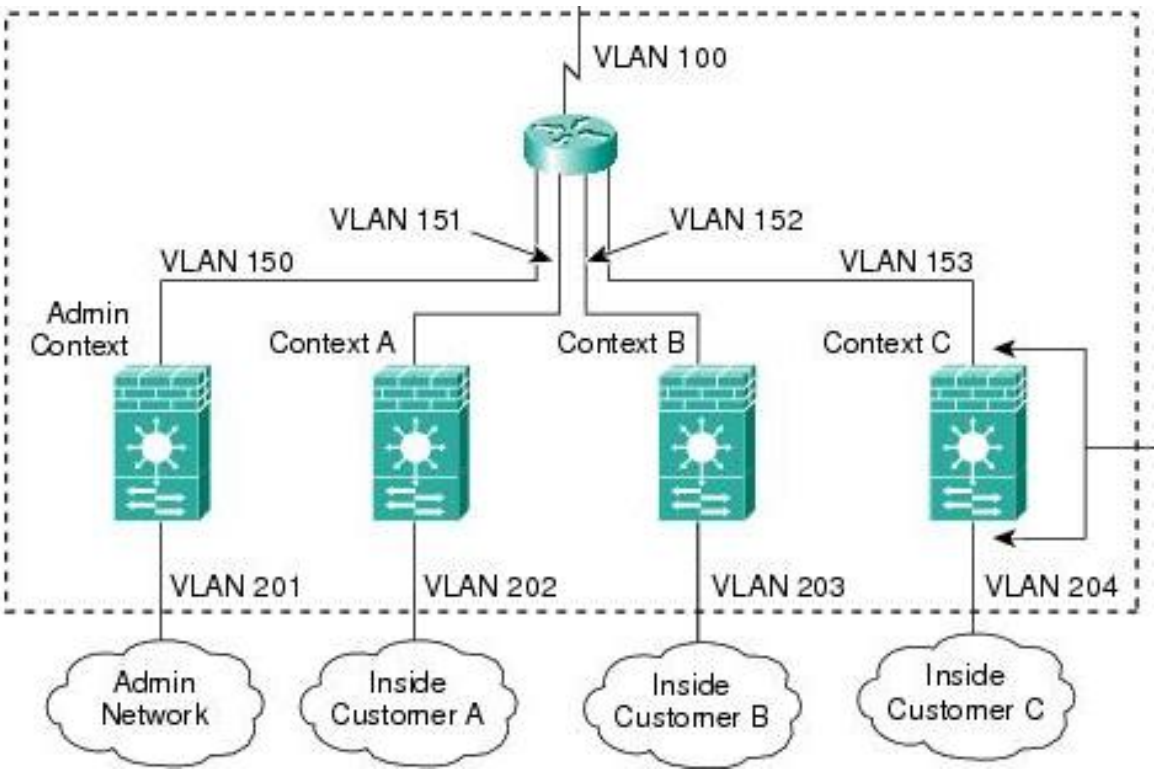

Figure23 : exemple du parfeu transparent

On déduit que nous pouvons partager une interface entre les contextes. Typiquement en mode routé, nous partageons l'interface externe pour conserver les VLAN. Nous pouvons également partager VLAN intérieur pour partager les ressources entre les contextes, ou vous pouvez placer la ressource partagée sur un cadre unique et de garantir l'accès à cette ressource à d'autres contextes.

Alors les contextes peuvent traiter les sujets suivant :

- Partage des ressources
- Limite des interfaces

3.2.4. Fonctionnalités des contextes de sécurité

Tableau 4: différentes fonctionnalités des contextes de sécurité

Principales fonctionnalités	avantages
performance	-5 Gigabit/s - 1 million de connexions simultanées - Plus de 100 000 cps (établissements de connexions par seconde)
Interfaces multiples	-Supporte jusqu'à 100 VLAN pare-feu n'importe lequel des 4000 VLANs du Catalyst peut être un VLAN pare-feu -Compatible avec les protocoles 802.1q et ISL (Inter-Switch Link)
Support NAT/PAT	Assure la translation dynamique ou statique des adresses de réseau (NAT) ou de ports (PAT)
Administration sécurisée de réseau	Protection de l'accès aux fonctions de gestion du réseau par cryptage 3DES (Triple Data Encryption Standard)
Listes de contrôle d'accès	Jusqu'à 128 000 listes de contrôle d'accès
Protection contre les attaques par saturation	-DNS Guard -Flood Defender -Flood Guard -TCP Intercept -Unicast Reverse Path Forwarding -Mail Guard -FragGuard et Virtual Reassembly
Routage	-Routage statique -Routage dynamique – protocole RIP (RoutingInterface Protocol) et protocole OSPF (Open Shortest Path First)
Journal d'évènements	Historisation des évènements dans un fichier au format syslog exploitable localement ou exploitable sur un serveur externe

3.2.5. Les contextes de sécurité et conflit d'adresse

Dans notre cas nous essayons de faire une séparation entre les utilisateurs (les clients) afin de palier au problème posé. Cette séparation sera faite à l'aide du concept des contextes de sécurité. Alors nous avons besoin d'un firewall qui supporte le concept présenté (contextes), en l'installant du côté CBI.

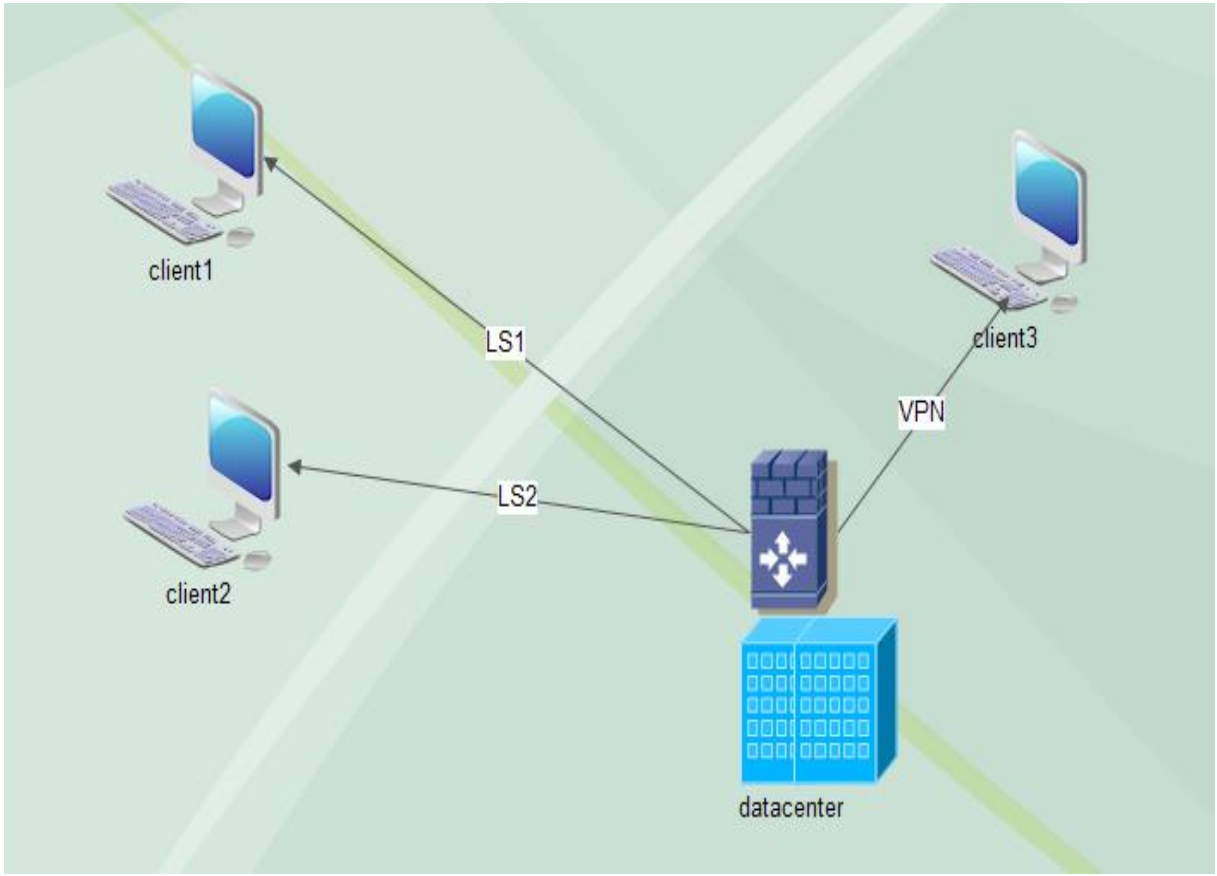

Figure 24: schema descriptif du positionnement du firewall

Chaque client demandeur de service a un contexte séparé de l'autre, cette séparation à plusieurs avantages pour le client :

- Permettre un niveau de sécurité élevé.
- Pas de conflit d'adresse.
- Augmenter les performances globales du réseau.

3.2.6. Inconvénient des contextes de sécurité de côté CBI

Malgré l'ensemble des avantages du concept contexte de sécurité, CBI laisse cette solution à côté à cause de son impact financier.

L'équipement permet de configurer seulement cinq contextes et après un certain temps, CBI doit acheter des licences pour configurer plusieurs contextes.

Cette solution apparait trop chère et coûteuse pour CBI.

3.3. Implémentation des VRF

Les entreprises implémentent aujourd'hui majoritairement des infrastructures routées, pour des besoins de haute disponibilité et d'évolutivité.

Le réseau fédère les flux de diverses entités d'une même entreprise, de partenaires ou sous-traitants ainsi que d'invités. Le besoin de segmentation et de virtualisation au sein du réseau de l'entreprise est donc de plus en plus important afin de supporter les nouvelles applications, la sécurité entre les groupes d'utilisateurs ainsi que la nécessaire souplesse d'évolution en fonction des demandes.

3.3.1. Principe de virtualisation

La virtualisation permet au réseau de fournir une isolation de couche 2 et de couche 3, et de renforcer aussi la sécurité pour les abonnés partageant cette même infrastructure. Les entités n'auront aucune possibilité de communiquer les unes avec les autres, sans une définition explicite de ces autorisations.

La solution de virtualisation d'un réseau de campus comprend :

- la virtualisation des routeurs
- la virtualisation des liens reliant les routeurs pour assurer l'isolation du trafic
- la virtualisation des services tels que firewall, etc.

La virtualisation des équipements est assurée par la fonction Virtual Routing and Forwarding (VRF). Les VRFs ainsi utilisées pour assurer le partitionnement de l'infrastructure :

- Permettent la constitution de Virtual Private Network (VPNs)
- Fournissent un moyen sécurisé d'accéder à l'ensemble des machines des centres de production de l'entreprise.
- Permettent également aux différentes entités d'utiliser des réseaux IP en overlapping, ce qui n'est pas supporté avec du routage IP global.

3.3.2. Virtualisation du routage

La segmentation du réseau est réalisée en séparant les abonnés dans des instances de routage et de forwarding différentes appelées VRF pour Virtual Routing and Forwarding.

Cette technologie est aujourd'hui déployée dans les réseaux LAN & MAN des entreprises et dérive directement de la notion de Virtual Routing and Forwarding (VRF) implémentée dans les réseaux.

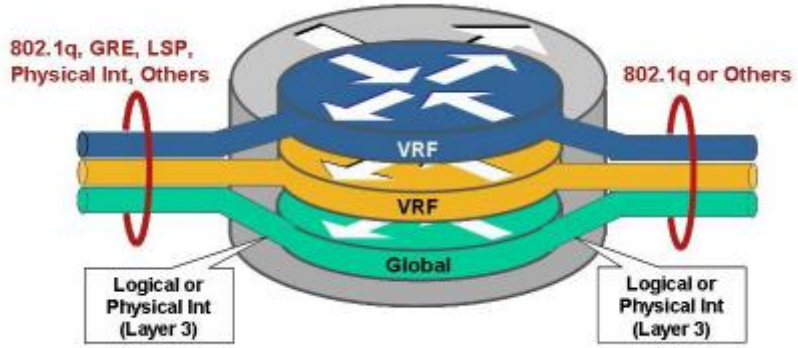

Figure25 : descriptif du VRF

Les VRF ainsi créées seront associées avec les éléments suivants :

- La table de routage. Cette table contient uniquement les routes de l'entité.
- La table de forwarding hardware dérivée de la table de routage, qui est basée sur la technologie CEF (Cisco Express Forwarding).
- Un groupe d'interfaces appartenant à la VRF. Ces interfaces pourront être physiques, mais elles pourront également être de type logique.
- Les processus de routage.

3.3.3. Interconnexions des équipements virtualisés

Les interconnexions d'équipements utilisant des VRF sont de niveau 3, et doivent évidemment apporter une isolation totale des flux entre chaque VRF.

Plusieurs solutions existent pour isoler les flux appartenant à des VRFs différentes sur les liens entre les routeurs, mais elles peuvent être regroupées dans trois catégories principales:

- Utilisation de tunnels GRE
- Utilisation de MPLS-VPN
- Utilisation de VRF-Lite

Utilisation GRE

Dans ce cas de figure, on utilise un tunnel GRE pour relier une VRF avec une autre VRF au travers d'un réseau IP.

Typiquement une méthode facile pour implémenter un guest access. L'encapsulation GRE est supportée en hardware et en software.

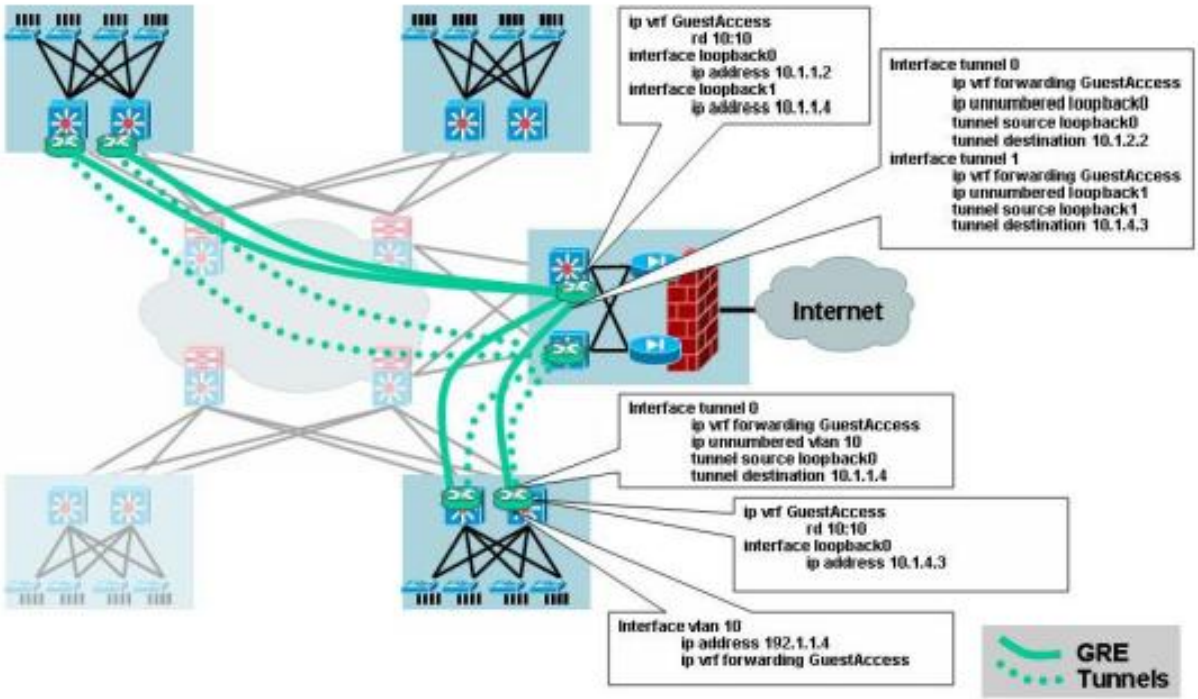

Figure26 : utilisation du GRE

L'avantage est de ne pas toucher au cœur du réseau et de n'implémenter les VRFs que là où il y en a besoin.

L'inconvénient majeur et que cela peut entrainer une complexité importante. Cette méthode est donc plutôt utilisée dans une architecture hub and spoke où tous les tunnels se terminent sur des Catalyst 6500 centraux.

Utilisation de MPLS-VPN

Il s'agit là de la méthode classique de constitution des VPNs. Cela suppose de mettre en phase la labellisation dans le cœur du réseau, de mettre en place LDP pour la distribution de ces labels.

Dans ce cas, les routeurs de distribution faisant l'interconnexion entre le réseau MPLS de cœur et la périphérie peuvent être vus comme ci-dessous, d'un coté avec des interfaces 802.1Q et de l'autre des interfaces labellisées MPLS :

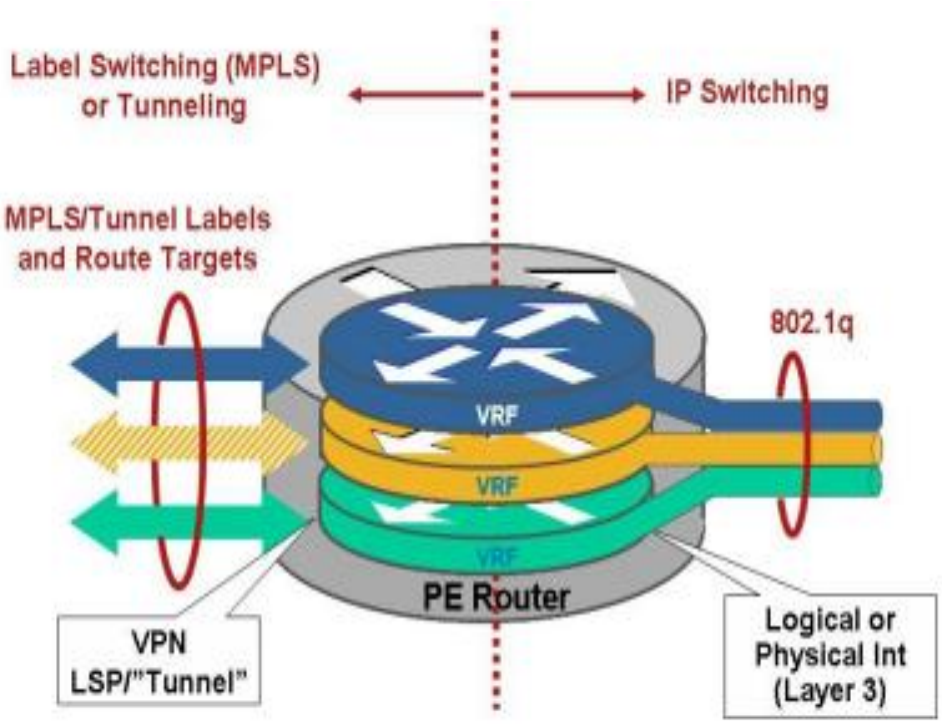

Figure27 : descriptif d'utilisation du VPN

Utilisation de VRF-lite

On trouve ce dernier modèle plus récemment mais de plus en plus souvent. L'idée est de conserver les VRFs mais de ne pas implémenter le modèle MPLS. Au lieu de cela, les routeurs seront interconnectés avec des interfaces permettant de relier les VRFs en conservant l'isolation.

Pour ce faire, nous établissons un trunk 802.1q entre les 2 équipements à connecter.

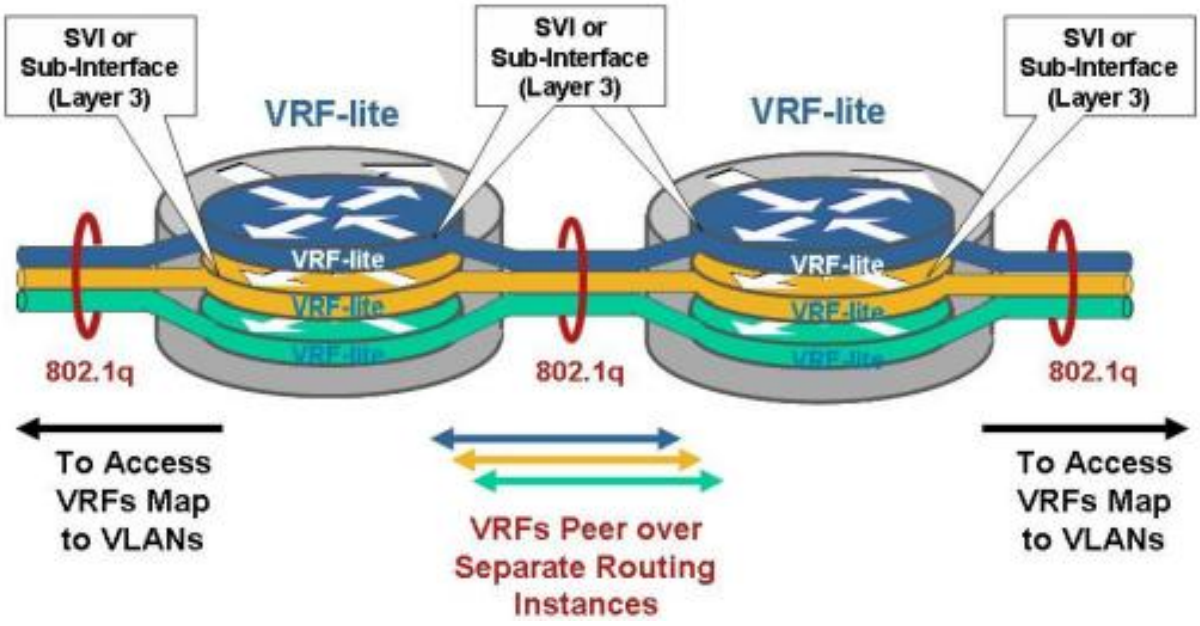

Figure28 : descriptif d'utilisation du VRF-lite

Il suffit alors de définir des sub-interfaces sous l'interface physique d'interconnexion, et d'associer ces sub-interfaces aux VRF à router sur le trunk.

La table de forwarding n'autorisant pas la commutation de paquet entre des sub-interfaces associées à des VRF-id différents, aucun paquet ne pourra être commuté entre ces sub-interfaces.

Le réseau est alors dit VRF-lite End-to-End, c'est-à-dire que ce modèle est répercuté et implémenté dans tous les Catalyst/routeurs du réseau.

Les avantages évidents de cette méthode sont dans la facilité d'utilisation puisque cela reste un réseau routé.

3.3.4. Utilisation VRF du côté CBI

L'utilisation des VRFs comme solution du problème posé à la CBI est considéré une solution faisable de côté financier et du côté technique, il suffit juste avoir des équipements qui supportent ce concept pour y configurer.

Les services de virtualisation et segmentation sur les réseaux permettent d'apporter une très grande souplesse dans la constitution des groupes d'utilisateurs tout en assurant leur sécurisation.

Les solutions actuelles sont très utilisées et Cisco travaille de manière importante sur ce sujet pour continuer à apporter de la valeur ainsi que des fonctionnalités permettant un déploiement plus rapide et une exploitation simplifiée.

4. Choix de la solution adéquate

D'après les scénarios proposés pour la résolution du problème de conflit d'adresses pendant la connexion des abonnées au Datacenter, nous avons vu :

- L'implémentation du NAT
- Utilisation des contextes de sécurité
- Utilisation des VRFs

Nous avons vu que pour chaque solution ses impacts fianciés et techniques pour l'entreprise CBI :

- Pour le NAT, il est moins cher mais il pose une surcharge au niveau du routeur puisque nous avons un nombre important des demandeurs de services.
- Pour les contextes de sécurité, ils demandent des licences à acheter et à renouveler, alors ils sont trop chers comme solution permanente.
- Pour les VRFs, ils répondent aussi bien pour la résolution du problème, ils sont moins chers comme solution à longue terme, et ils donnent aussi un niveau de sécurité.

A la fin nous avons choisi les VRFs, donc pour adopter ce concept nous devons aussi chercher les équipements et l'architecture réseau adéquate.

5. Les équipements et l'architecture réseau associés à la solution proposée

5.1. Les équipements

Nous avons choisi comme solution l'implémentation des VRFs, alors nous devons chercher les équipements associés.

Cisco se positionne très fortement dans les architectures Datacenter, il est donc tout à fait logique que ses stratégies apportent des innovations dans le cadre de la protection et le bon acheminement des réseaux des Datacenters.

Il y a plusieurs gammes introduites par cisco supportant le concept des VRFs et aussi un niveau de protection très élevé pour les Datacenters.

Parmi ces gammes on trouve :

- ASR 1000 pour les routeurs.
- Catalyst 4500 pour les commutateurs.
- ASA 5585 pour les par-feus

Pour des raisons financières au sein de la société CBI, nous ne pouvons pas choisir la gamme ASR 1000 pour y définir les VRFs, par ce que le prix d'achat de cette gamme est très élevé.

Alors la gamme Cisco Catalyst 4500 offre une commutation non bloquante des couches 2/3/4 grâce au VRF et intègre la tolérance de pannes pour améliorer encore le contrôle des réseaux convergents.

Pour renforcer la sécurité d'accès du réseau, nous essayons d'ajouter un ensemble de par-feu. Cisco introduit une gamme particulière pour les Datacenters sous le nom ‘’ASA 5585’’, c'est une gamme de FW multi-gigabits qui s'appuie sur une architecture multiprocesseurs.

5.2. Architecture réseau proposé

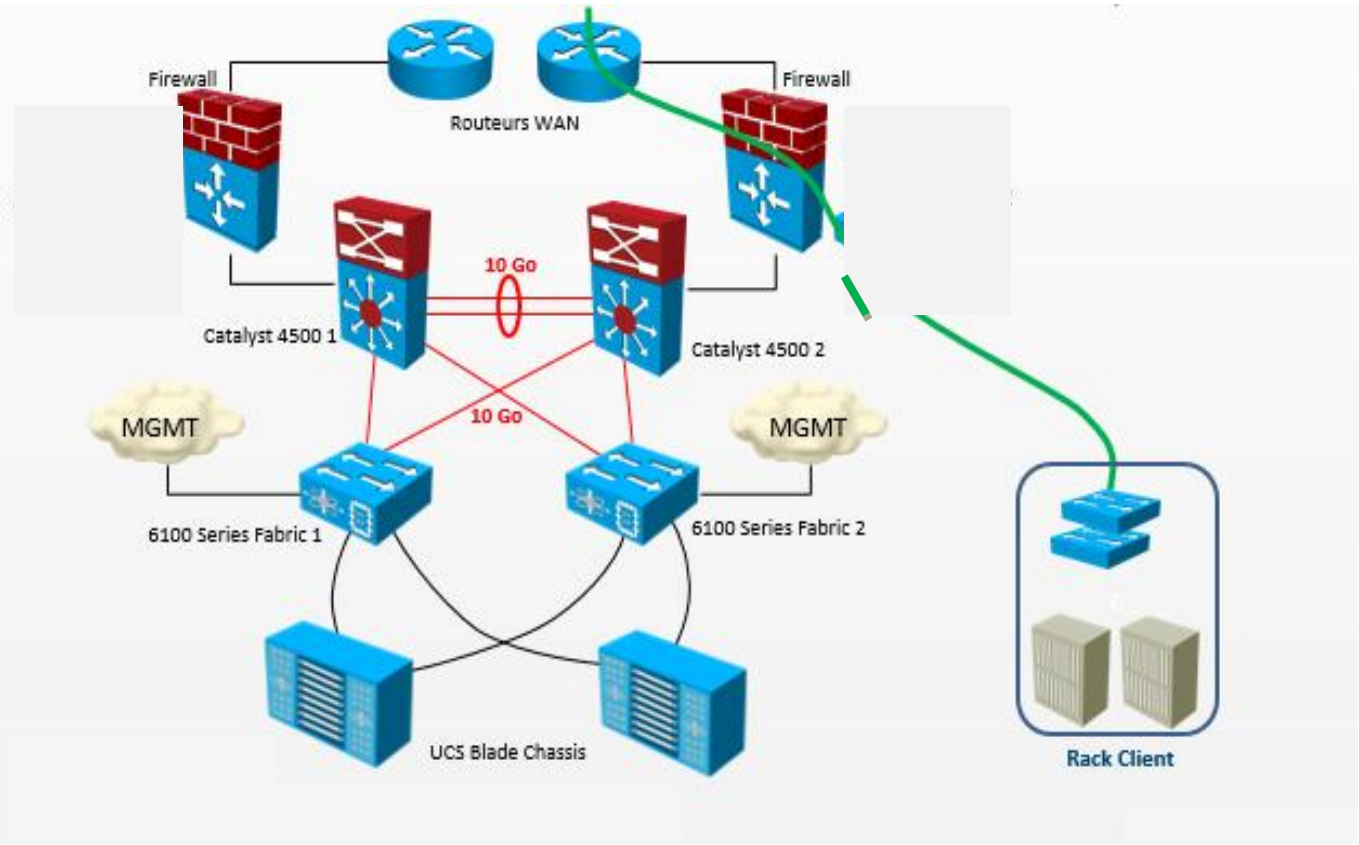

Figure29 : architecture réseau de la solution

5.2.1. Présentation des différents composants de l'architecture

- CBI fournira au client un espace physique, l'acheminement du trafic sera assuré via l'infra DC CBI (Routeurs, Firewalls, Switches…).
- l'étanchéité sera assurée par l'implémentation des VLANs et des VRFs sur les switches d'accès.
- Le Client sera authentifié au niveau Cloud via le logiciel VMware vSphere.
- Le commutateur Cisco 6100 de la 3eme génération fournit une connectivité réseau pour les châssis, les serveurs lames et serveurs en rack.
- Cisco UCS va assurer la partie management des réseaux.
- L'utilisation des switchs Cisco Catalyst « fortement recommandé » est une gamme destinée au Datacenter, parmi ses avantages :

- Technologie 10 Gigabit Ethernet à hautes performances.
- Technologie Cisco Data Center.
- Services VM optimisés.

5.2.2. Description de l'architecture choisie

La mise en place d'une politique d'architecture dans le Datacenter doit apporter un certain nombre de réponses aux problématiques suivantes :

- Haute disponibilité.
- Performances.
- Virtualisation .
- Contrôle d'accès aux applications

Nous allons voir dans la suite comment répondre à ces différents points

Haute disponibilité

L'architecture Datacenter doit être construite afin de garantir une très haute disponibilité des services. La gamme ASA permet la mise en place d'architectures redondantes et performantes, la mise en place de FW doit pouvoir garantir la disponibilité des services.

La gamme ASA offre la possibilité d'utilisation de paire de FW en Failover. La fonction failover a été optimisée afin de pouvoir garantir un basculement tout en gardant les sessions utilisateurs actives. Pour cela une synchronisation permanente de l'état des sessions est réalisée entre les deux boitiers, et le pooling est maintenant réglable en ms. Ce qui permet d'obtenir des temps de basculant pouvant être à la seconde.

Performance

Le second point sur lequel nous avons travaillé, ce sont les performances, nous avons vu précédemment que l'architecture permet l'agrégation de boitiers et de liens, ce qui augmente le taux de performance.

virtualisation

La mise en place d'une architecture de virtualisation du Datacenter doit être assurée de bout en bout, en partant de l'architecture virtualisée des serveurs mais aussi via des mécanismes comme les VLAN, ou les VRF et bien sur la la virtualisation des services.

Contrôle d'accès aux applications

Le contrôle d'accès aux applications à travers l'outil TrustSec, c'est une solution d'authentification des utilisateurs, ainsi que la mise en place de filtrage associé via les group tag.

6. Conclusion

La prise en compte de l'architecture globale d'un Datacenter nous a permis d'implémenter des fonctions uniques sur le marché, en pariculier au niveau du mode d'insertion des services de sécurité.

Conclusion Générale

Conclusion et Perspectives

Ce projet de fin d'étude a été réalisé dans le but de proposer une solution d'accès aux clients Datacenter. Nous avons commencé par une étude qui présente l'état de l'art sur Datacenter et ses fonctionnalités, ainsi que les services offerts aux PME. Puis, nous avons proposé quelques scénarios pour le problème d'accès '' NAT, sécurité des contextes et VRF''. Enfin, nous avons choisi la politique VRF comme solution parce qu'elle répond aux besoins des deux côté, soit du côté fournisseur des services ''CBI'', soit du côté demandeur des services ''client''.

Le stage que nous avons effectué au sein de la société CBI, nous a donné l'occasion de faire le lien entre nos connaissances académiques et le monde professionnel. D'une part, il nous a appris à nous imprégner du milieu professionnel en nous soumettant à des défis qui nous ont permis d'améliorer notre aptitude à analyser et résoudre des problèmes. D'autre part, il nous a permet d'améliorer notre savoir-faire, notre savoir être, notre rigueur et d'affermir notre professionnalisme.

Parmi les perspectives et améliorations possibles pour ce projet, nous pouvons :

- Proposer un autre scenario d'authentification des clients à travers un serveur d'authentification pour répondre aux besoins des clients

Références

[1] http://fr.wikipedia.org/wiki/ISO/CEI_27001

[2] http://fr.wikipedia.org/wiki/ISO/CEI_27002

[3] Telecommunications Infrastructure Standard for Data Centers

René CHALON, Jean-Pierre BERTHET (2005)

[4] NFPA 75 Standard for the Protection of electronic and computer/DATA Processing Equipement

[5] A Scalable, Commodity Data Center Network Architecture

[6] http://www.ornthalas.net/comment-choisir-un-datacenter/

[7] Les enjeux des datacenters aujourd'hui et demain, 2010 IBM Corporation

[8] http://www.apl-france.fr/maintenance-gestion-technique-data-centers-r16.html

[9]https://www.sstic.org/2008/presentation/Securisation_etat_de_l_art_et_nouveaux_enjeux_des_Green_Data_Centers/

[10] http://www.interxion.com/fr/data-centers/pourquoi-externaliser-votre-data-center-/

[11] focus DataCenters CB RICHARD ELLIS / France (2010)

[12] focus DataCenters CB RICHARD ELLIS / France (2010)

[13]Stratégies de déploiement de serveurs lames dans les datacenters existants, Livre blanc n°125, Neil Rasmussen

[14] Bouygues Construction, acteur majeur sur le marché des data centers, Dossier de presse (23 mai 2011)

[15] Bouygues Construction, acteur majeur sur le marché des data centers, Dossier de presse (23 mai 2011)

[16] Bouygues Construction, acteur majeur sur le marché des data centers, Dossier de presse (23 mai 2011)

[17] étude d'un data center en phase d'exécution, Armel JEGOU, Charles CHRISTIN, François BOUCHEIX, (2011)

[18] étude d'un data center en phase d'exécution, Armel JEGOU, Charles CHRISTIN, François BOUCHEIX, (2011)

[19] http://hebergement-et-infrastructure.fr/actualites-et-innovations/free-cooling-et-consommation-datacenters

[20] http://fr.wikipedia.org/wiki/Free_cooling)

[21] http://www.daikin.co.uk/industrial/applications/data-centre/

[22] Rittal White Paper 507: Understanding Data Center Cooling Energy Usage & Reduction Methods, Daniel Kennedy

[23] Rittal White Paper 507: Understanding Data Center Cooling Energy Usage & Reduction Methods, Daniel Kennedy

[25] http://www.alternativedatacenter.com/glossaire/f.php

[26] focus DataCenters CB RICHARD ELLIS / France (2010)

[27] http://groupelectro2.canalblog.com/archives/2012/11/05/25503507.html

[28 Data Center, Les solutions pour une alimentation électrique fiable, sécurisée et évolutive des infrastructures informatiques

[29] http://fr.wikipedia.org/wiki/Centre_de_traitement_de_donn%C3%A9es

[30] http://www.apeltec.fr/amenagement-techniques/

[31] http://www.apeltec.fr/amenagement-techniques/

[32] http://www.apeltec.fr/amenagement-techniques/

[33] Data Center Condorcet, Excellence technique et éco-efficacité

[34] Data Center Condorcet, Excellence technique et éco-efficacité

[35] Data Center Condorcet, Excellence technique et éco-efficacité

[36] http://outsourcing.openwide.fr/Infra/Data-centers

[37] DATA CENTER STRATEGIES, Simplifying high-stakes, mission critical decisions

in a complex industry, John Rath , Rath Consultin(July 2011)

[38] DATA CENTER STRATEGIES, Simplifying high-stakes, mission critical decisions

in a complex industry, John Rath , Rath Consultin(July 2011)

[40] http://www.vmware.com/fr/products/

[41]Understanding Microsoft Virtualization Solutions

[42]http://fr.wikipedia.org/wiki/Cloud_computing

[43]http://fr.wikipedia.org/wiki/Cloud_computing

[44]http://fr.wikipedia.org/wiki/Cloud_computing

[45]http://fr.wikipedia.org/wiki/Cloud_computing

[46]http://www.cisco.com/en/US/products/sw/secursw/ps1018/products_tech_note09186a0080094e8b.shtml

[47]http://www.cisco.com/en/US/docs/security/fwsm/fwsm22/configuration/guide/context

[48]http://www.cisco.com/en/US/docs/security/fwsm/fwsm22/configuration/guide/context

[49http://www.cisco.com/en/US/products/hw/modules/ps2706/products_configuration_example09186a00809bfce4