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.

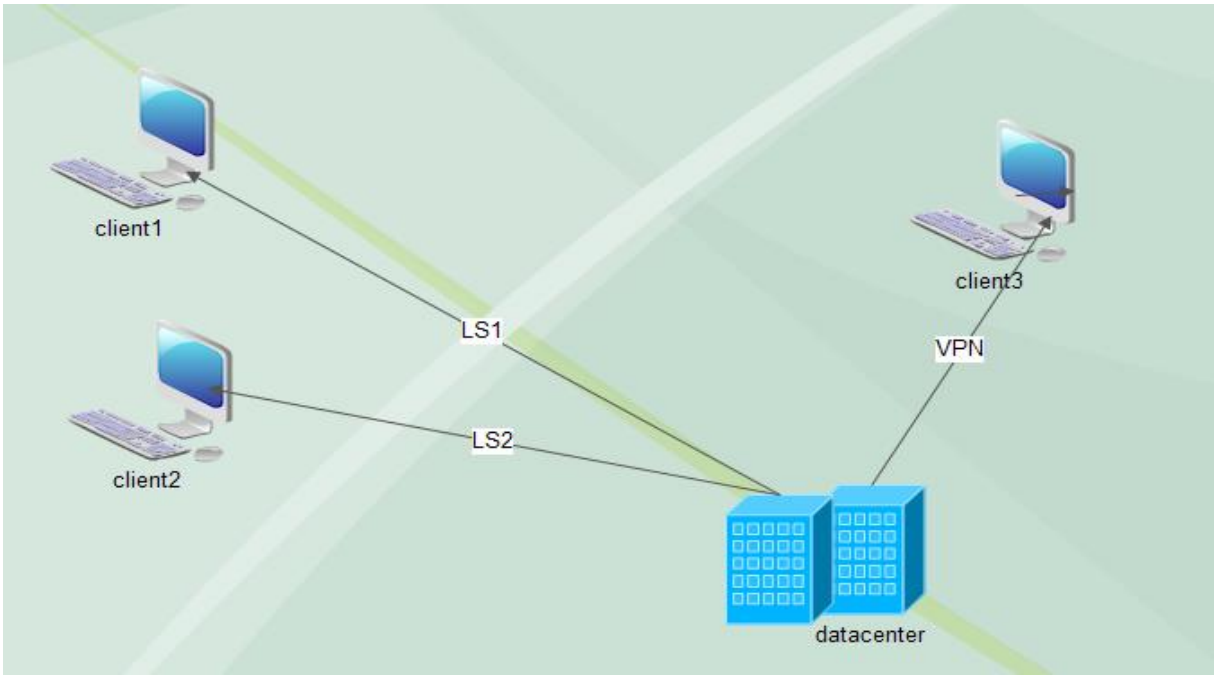

Figure17: description connexion client-datacenter

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.

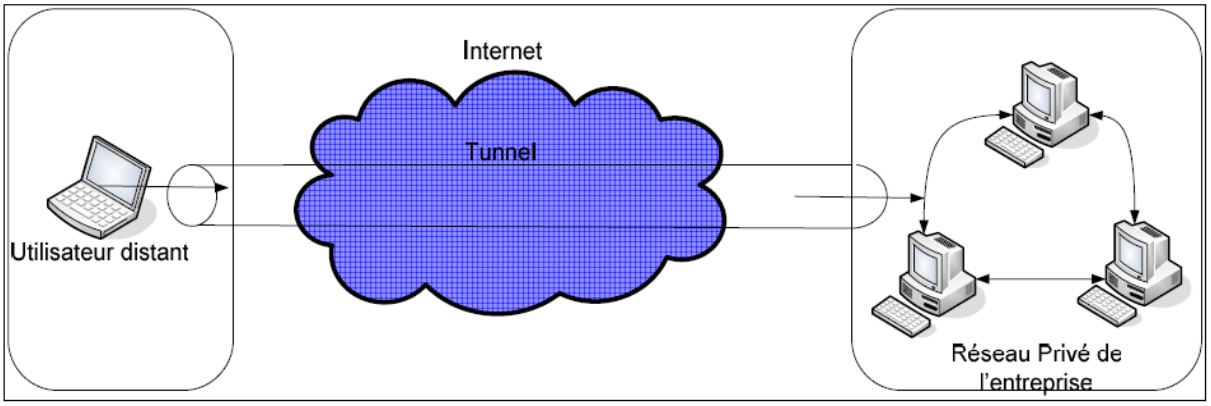

Figure18 : schéma d'un VPN

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.

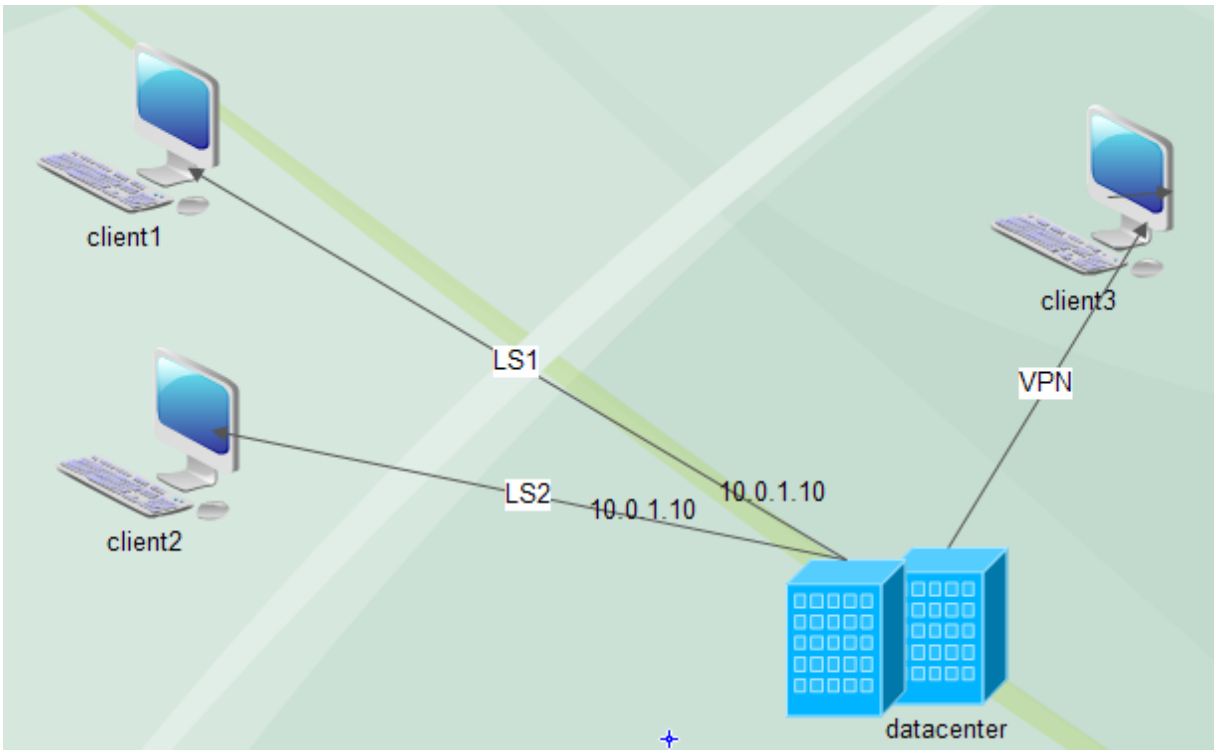

Figure19 : schéma descriptif du problème

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.

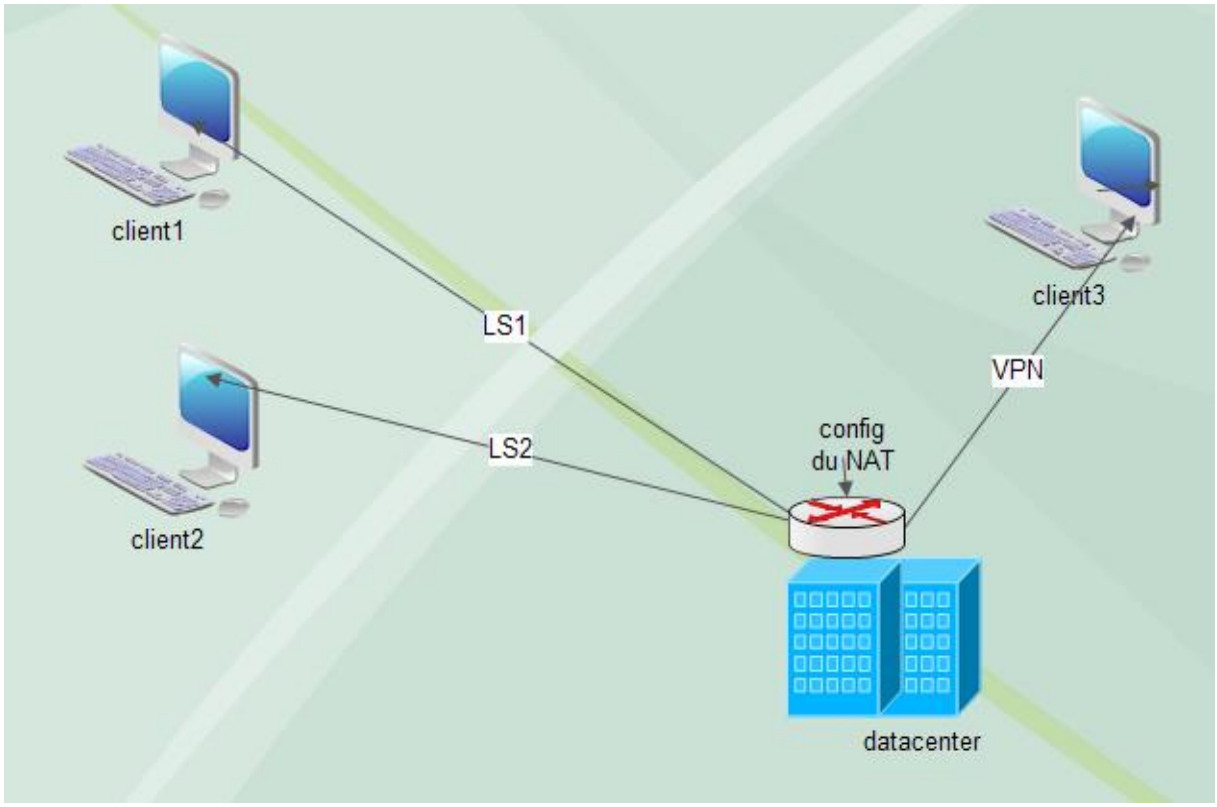

Figure 20: schéma descriptif du scenario

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.

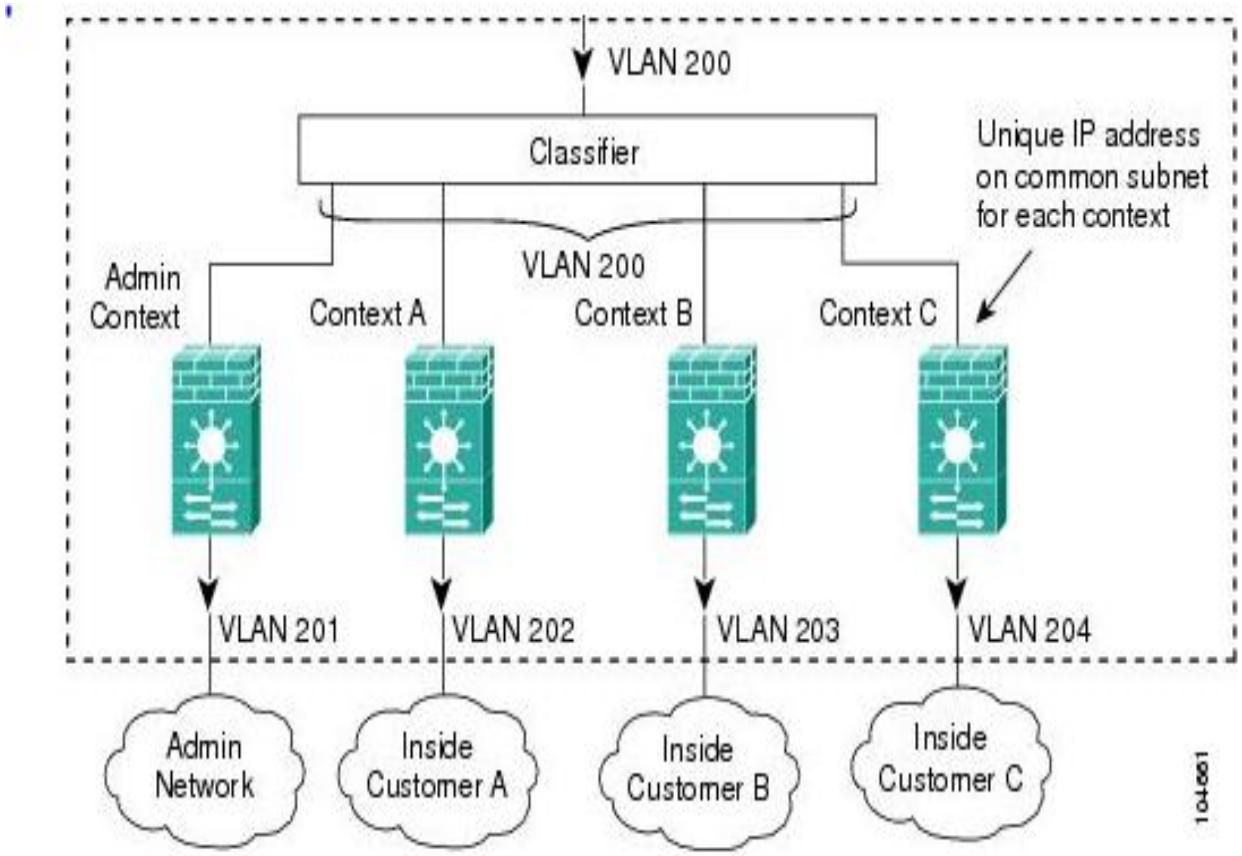

Figure21 : exemple de multiple contexte de sécurité

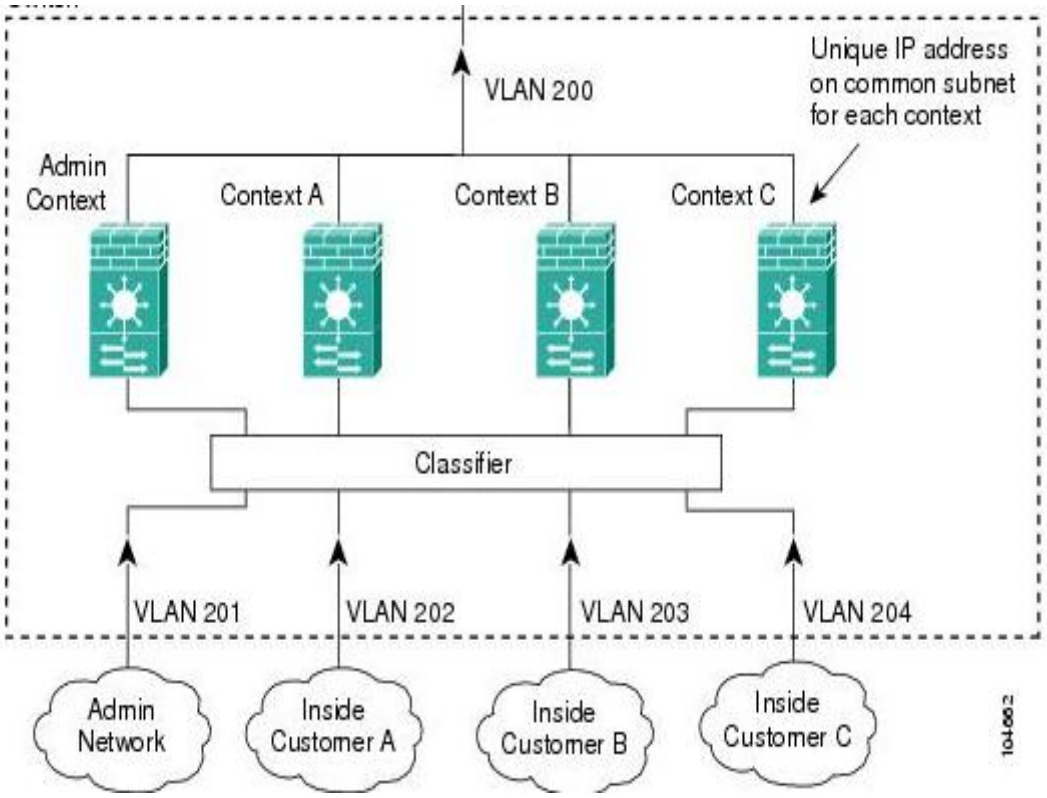

Figure22 : exemple du trafic venant de réseaux Intérieur

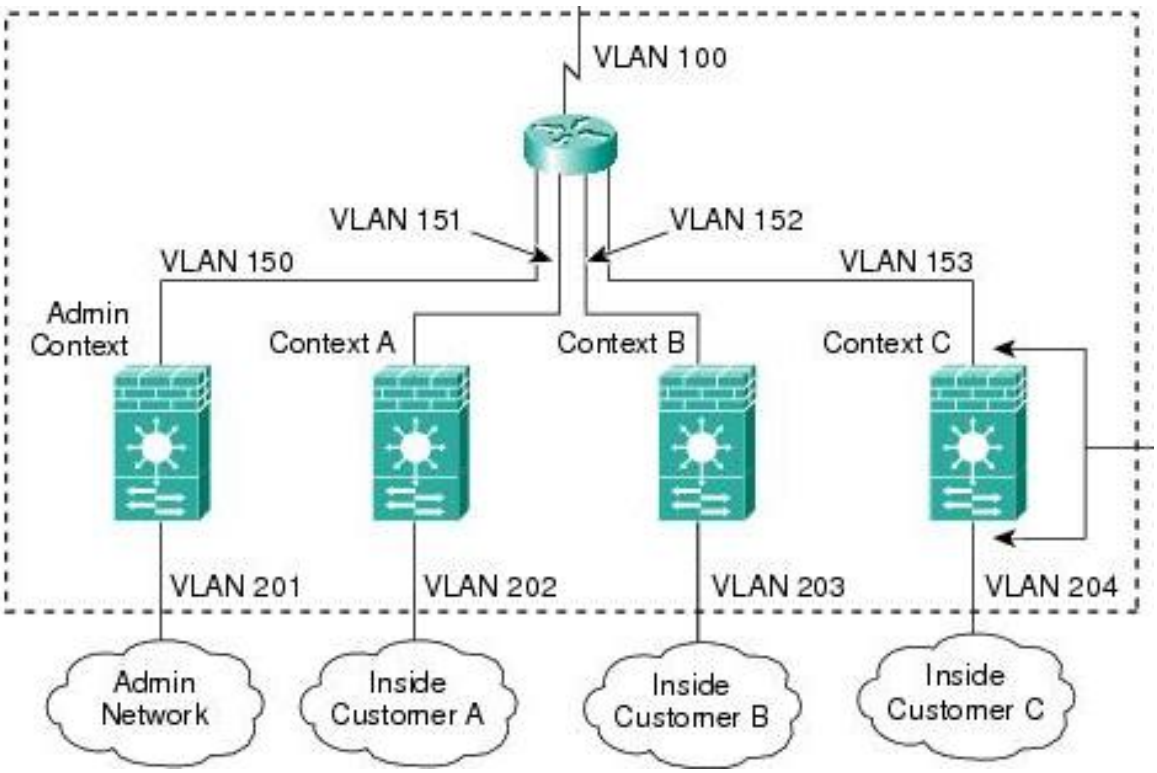

Figure23 : exemple du parfeu transparent

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.

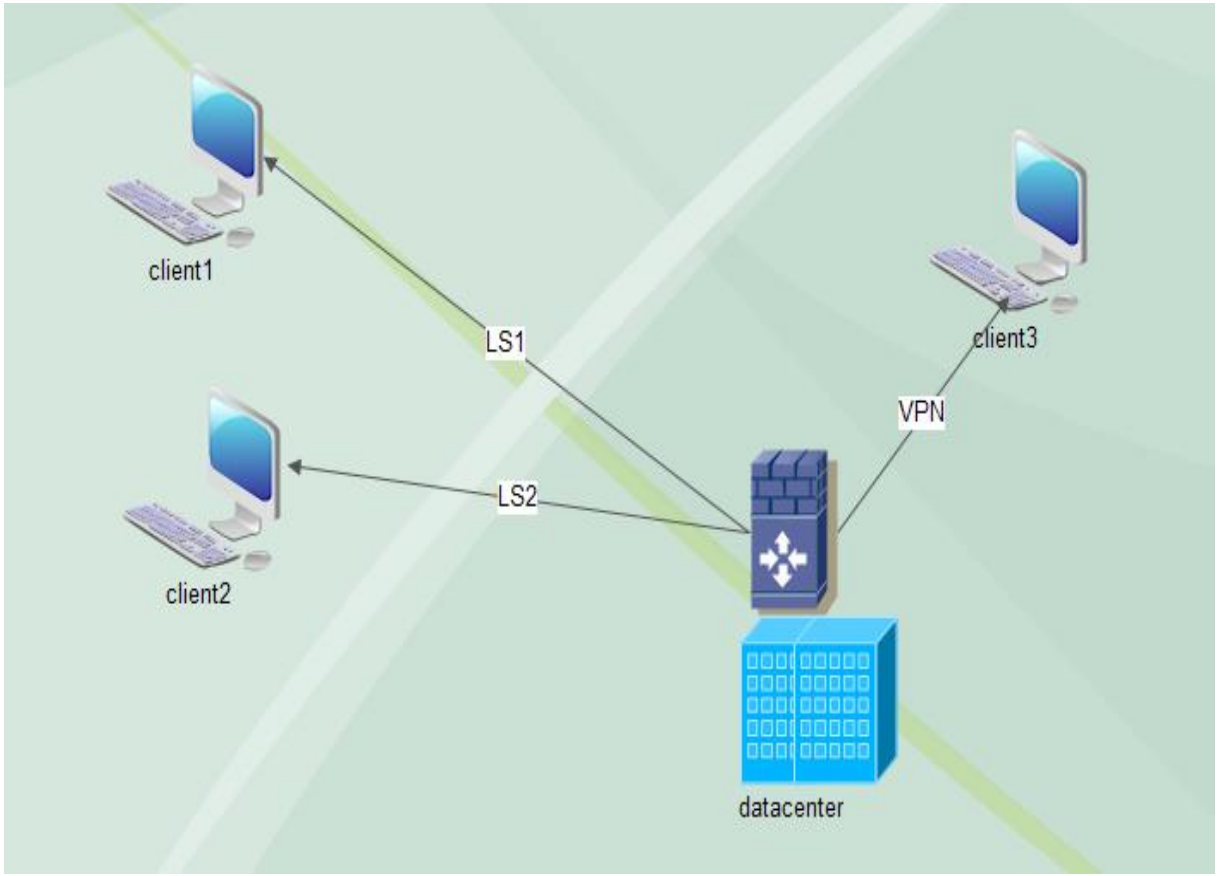

Figure 24: schema descriptif du positionnement du firewall

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.

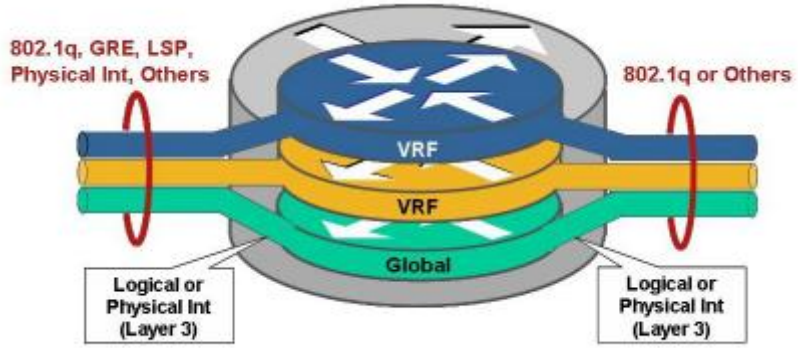

Figure25 : descriptif du VRF

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.

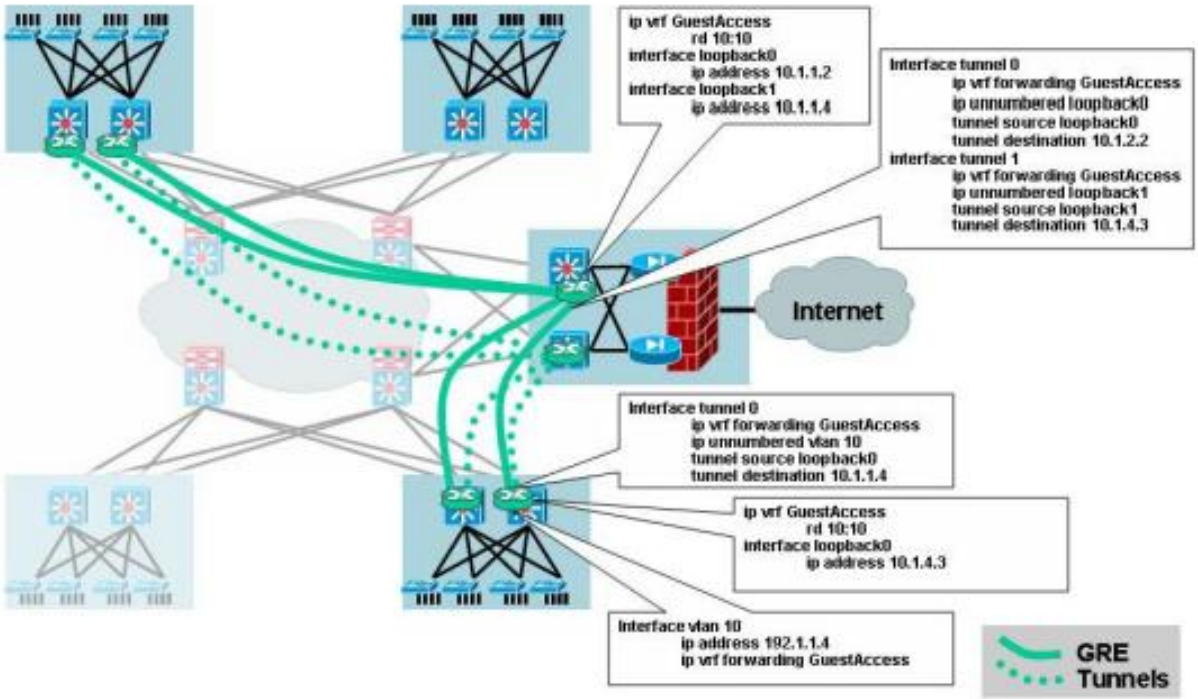

Figure26 : utilisation du GRE

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 :

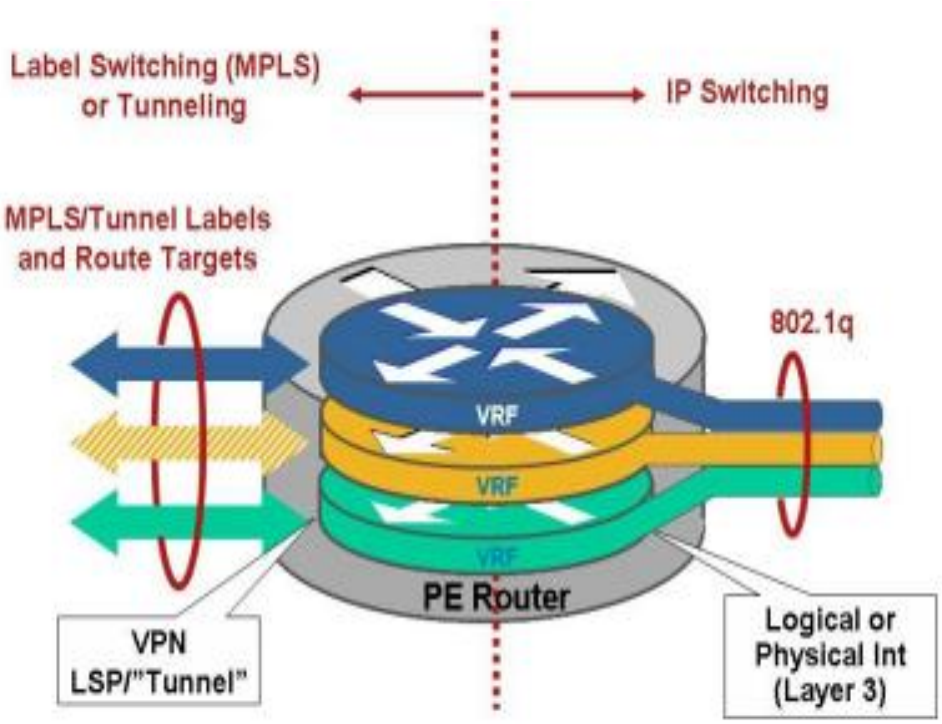

Figure27 : descriptif d'utilisation du VPN

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.

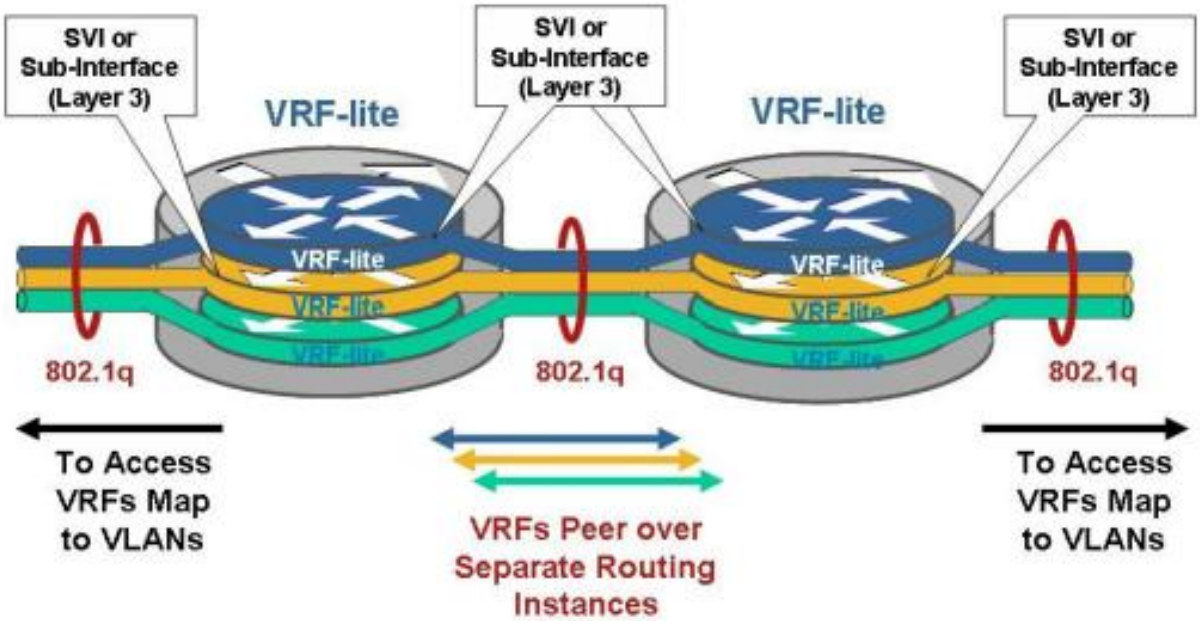

Figure28 : descriptif d'utilisation du VRF-lite

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

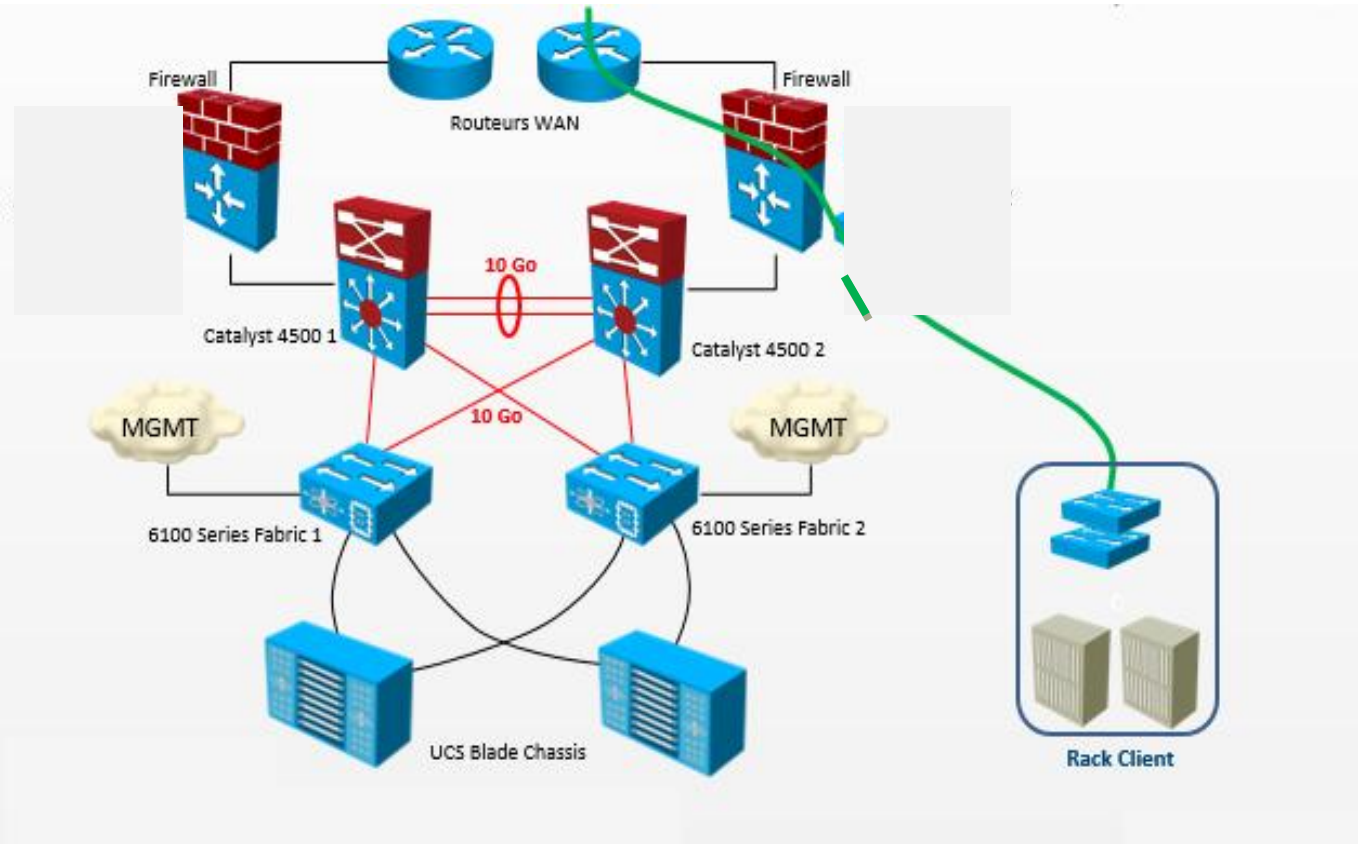

Figure29 : architecture réseau de la solution

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.