Projets avancés des réseaux

Master en Architecture des Systèmes Informatiques 2017-2018

LONGREE Gaëtan
PICCAR Isabelle

Table des Matières

Introduction

Une société travaillant dans l'événementiel décide de s'étendre sur de nouveaux sites. Ce rapport décrit l'infrastructure mise en place ainsi que les différentes configurations nécessaires pour répondre au mieux à ses besoins.

Dans un premier temps, le cadre du projet est présenté en commençant par une liste des demandes du client associées aux techniques et technologies concrètes pouvant y répondre. Ensuite les objectifs globaux sont définis et une liste du matériel nécessaire est fournie.

Ensuite, l'architecture du projet est présentée. D'abord dans sa globalité et ensuite plus détaillée, site par site.

S'en suivent quelques détails de configurations illustrant la mise en place des techniques que nous avons jugées pertinentes.

Avant de conclure, les problèmes rencontrés sont exposés et quelques améliorations possibles sont décrites.

Cadre du projet

Demandes client - Interprétations

Demandes	**Interprétations**
Fiabilité et robustesse	Utilisation de redondances entre les périphériques réseaux afin de tolérer une défaillance tout en minimisant l'impact sur la charge de travail.
Evolutivité	Utilisation de techniques et technologies capables d'être mises à l'échelle (ex: routage dynamique).
Délocaliser deux branches et communication performante entre les sites	Utilisation de tunnels VPN site-à-site entre les branches (flux à transporter à déterminer). Etablir une baseline entre les méthodes de chiffrement et les performances requises.
Présence de plusieurs services	Utilisation et séparation des réseaux intra-site via des VLAN.
Présence de studios visuels et studios sonores sur les sites branches	Utilisation de serveurs hautes performances et d'une connectique haut débit entre les serveurs et les employés. Utilisation d'un SAN important avec redondance et tolérance de panne ainsi qu'une connectique à très haut débit pour la communication entre serveurs de rendus et employés.
Echange de documents entre sites	Utilisation de serveurs de fichiers indépendants des SAN des studios visuels et audio.

Employés peuvent se rendre dans les autres sites	Présence d'un annuaire sur les sites branches avec synchronisation directe avec l'annuaire principal via tunnels VPN.
Quand la société est en déplacement, elle doit avoir accès à des informations se trouvant sur les sites	Utilisation de tunnels VPN client-à-site avec authentification via annuaire.
Présence d'un site vitrine et de vente de tickets	Utilisation d'une DMZ sur le site principal avec réservation d'adresses IPv4 publiques et mappage statique.
Présence d'invités au sein de l'entreprise	Utilisation d'un VLAN de type GUESTS et installation de points d'accès avec authentification par portail captif.
Présence de VoIP au sein d'un même site (sans liaison direct entre site)	Intégration d'une gestion de QoS sur les communications intra-site.

Objectifs

La société cliente travaillant dans le secteur multimédia, le prérequis principal est donc de mettre en place un réseau fiable et robuste afin de rendre le flux de travail au sein du réseau le plus fluide possible.

Afin d'assurer l'aspect fiabilité et robustesse, l'ensemble des périphériques mis en place seront dédoublés et configurés dans une topologie redondante. Le trafic des VLAN sera balancé entre les périphériques à travers des technologies de type Spanning Tree. L'accès au réseau externe (Internet) sera également redondant, mais ne présentera pas de technologie de balancement de charge afin d'assurer une redondance directe en cas de panne matériel. L'usage de protocoles de routage dynamique sera favorisé afin d'automatiser le basculement entre les routes en cas de perte de connectivité. Un ajustement manuel sera requis afin d'éviter un effet d'équilibrage et de concentrer le trafic en une direction principale.

La redondance d'accès au réseau externe Internet sera réalisable via la souscription de minimum deux lignes individuelles vers un fournisseur d'accès. Il est favorable de souscrire deux lignes chez deux fournisseurs différents afin de pallier tout soucis d'indisponibilité lié au réseau FAI.

L'aspect performance sera assuré par des connecteurs à haut débit entre les périphériques clé, notamment les switch connectant les serveurs aux systèmes de distribution backbone. La connectique sera alternée entre des agrégations de liens dans zone dont la demande de bande passante n'est pas excessive. Les liens entre les switch des serveurs vidéo/audio seront assurés par des connecteurs de type fibre optique avec agrégations afin de réduire la congestion et d'obtenir une redondance au niveau des liens.

Les connecteurs en fibre optiques seront surtout utilisés dans les "datacenter" des studios de New Delhi et Los Angeles. Ceci afin d'assurer une bande passante haut débit entre les serveurs SAN et les serveurs de rendu vidéo et audio.

Les connexions inter-site seront assurées par des tunnels IPsec. Les liaisons entre les site New Delhi-Paris et Los Angeles-Paris seront principalement utilisées pour des services peu gourmands (service messagerie, transfert de fichiers, synchronisation des annuaires LDAP, etc..). La liaison entre New Delhi et Los Angeles sera susceptible d'effectuer des transferts importants de flux audio et/ou vidéo. Il en est de même pour les tunnels IPsec client-à-site qui seront utilisés par les représentants itinérants et lors des événements. Il est importants d'établir dès lors un équilibre entre la confidentialité, dont le chiffrement des données impactera la performance du tunnel en terme de transfert. Cette étape pourrait être simplifiée déchargeant au serveur de rendu un transcodage préalable afin de réduire la quantité de flux a chiffré lors du transfert à travers les tunnel VPN.

Technologies de l’infrastructure LAN

Le réseau intra-net sera configuré en une topologie à 3 niveaux, comprenant une couche Accès à laquelle seront connectés les ordinateurs des employés. La couche Accès sera reliée à une couche dite Distribution, qui sera chargée d'établir les connexions entre les VLAN et également au serveur interne. La couche Distribution sera reliée à son tour à la couche Core, qui fera office de backbone pour la connexion à Internet.

Les technologies qui seront implémentées dans les LAN seront:

- 802.1Q VLAN Tagging
- VLAN Trunking Protocol
- Spanning Tree Protocol
- Hot Standby Router Protocol
- EtherChannel
- 10GB SFP
- Routage statique
- Access Control Lists

Technologies pour l’infrastructure WAN

Sauf indication contraire, le protocole attendu du FAI pour l'accès Internet est de type PPPoE à travers un modem type DSL avec connexion haut débit synchrone. Dans la mesure du possible, une connexion à la fibre FTTH est à privilégier au minimum pour la connexion principale.

Une connexion autre que la fibre est envisageable pour le lien de redondance du site de Paris, mais un débit élevé reste nécessaire afin de garantir la disponibilité du site vitrine et de la vente de tickets en ligne sans entraîner la congestion de la ligne.

Les sites de New Delhi et Los Angeles doivent impérativement être desservis par la fibre optique afin de garantir un haut débit pour les transferts vidéo/audio entre sites ainsi qu'entre les sites et les équipes en tournée.

Une série de pare-feux en redondance seront mis en place aux bordures du réseau, en liens direct avec les diverses connexions au FAI. Ceux-ci mettront en place une traduction NAT Overload pour les sous-réseaux internes. Dans le cas du site de Paris, une DMZ sera mise en place ainsi qu'un NAT statique afin de rendre les serveurs vitrine et de vente de ticket directement accessibles depuis Internet.

Afin de rendre le serveur vitrine et le serveur de vente accessibles depuis Internet, il sera nécessaire d'obtenir des adresses IP statiques auprès du FAI.

Technologies pour la communication inter sites

Les communications inter sites seront gérées par des tunnels VPN IPsec ESP en mode tunnel entre les pare-feux de chaque site. Chaque tunnel sera reproduit sur le pare-feu actif et le pare-feu redondant afin d'assurer une redondance sur les communications inter sites également.

Les pare-feux sont munis de routes vers les sous-réseaux distants afin de rediriger les trafics internes vers les sites. Un système d'ACL sera mis en place afin de limiter l'accès au réseau distant depuis certains sous-réseaux.

Matériel Nécessaire

Afin d'estimer la quantité de trafic auquel les périphériques seront sujet, le nombre d'employés sur les différents sites a été estimé à :

- Une centaine d'employés sur le site de Paris
- Une vingtaine d'employés sur le site de New Delhi
- Une quinzaine d'employés sur le site de Los Angeles

De plus, afin de comptabiliser l'expansion potentielle de l'entreprise, il a été estimé que le nombre d'employés risque de potentiellement doubler dans les quelques années à venir.

Pare-feu	Cisco Firepower 4150
Switch Layer 3 Distribution	Cisco 9300 1G 24-port
Switch Layer 2 Accès	Cisco Catalyst 2960-L 48-port
Switch Layer 2 Data Center	Cisco Nexus 3524-X

Quantités estimées:

- 2 pare-feux par site;
- 2 switch Layer 3 par site;
- 2 switch Layer 2 Data Center par site;
- 2 switch Layer 2 pour les sites de New Delhi et Los Angeles (2 X 46 ports utilisables = 92 ports au total par site);
- 4 switch Layer 2 pour le site de Paris (4 X 46 ports utilisables = 184 ports au total).

Architecture du projet

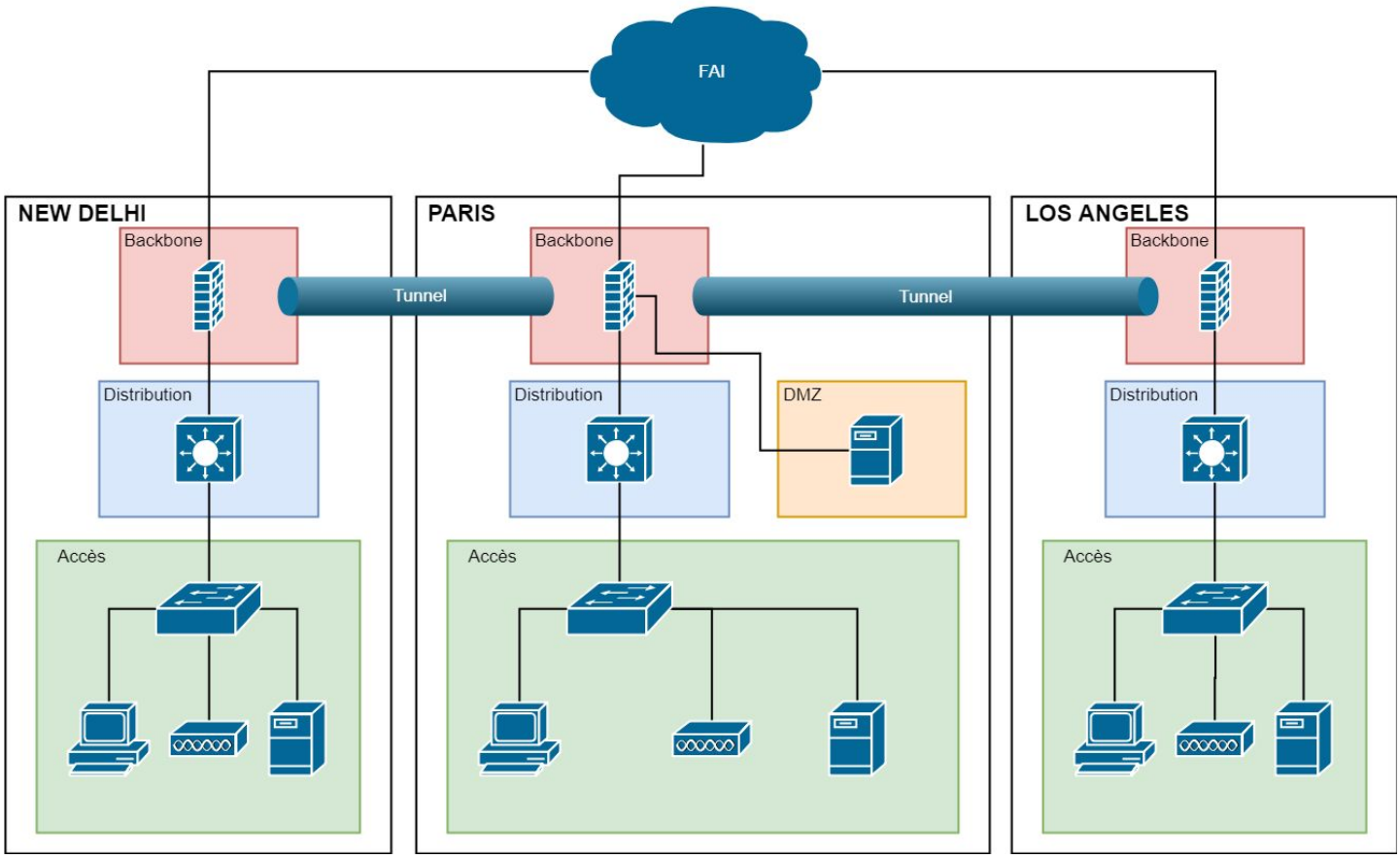
Cette section va couvrir l'architecture prévue pour le déploiement du réseau sous deux aspects:

- Une vue globale du réseau des trois sites;
- Une vue détaillée de chacun des sites.

Vue globale

La vue globale ci-dessous reprend les trois sites avec une représentation simplifiée (notamment l'absence de redondance). On peut voir le tunnel virtuel qui relie les trois sites, la zone DMZ sur le site de Paris et les serveurs vidéo/audio sur les site de New Delhi et Los Angeles.

Ces trois sites sont détaillés dans la section qui suit.


FAI
NEW DELHI
Backbone
Tunnel
Distribution
Accès
PARIS
Backbone
Tunnel
Distribution
DMZ
Accès
LOS ANGELES
Backbone
Distribution
Accès

Vues détaillées

Paris

Dans cette vue détaillée du site central de Paris, on peut voir la redondance au niveau des pare-feux. En opération, un seul des pare-feux est actif, afin de réserver le secondaire pour les cas d'urgence uniquement. La redondance est maintenue jusqu'à la zone DMZ où les serveurs peuvent utiliser la redondance en cas de pannes également.

Les pare-feux gèrent la traduction NAT de manière dynamique (PAT) pour le réseau interne, et de manière statique (NAT) pour les serveurs en DMZ. chaque serveur en DMZ dispose alors de deux adresses publiques, une par pare-feu en cas de panne.

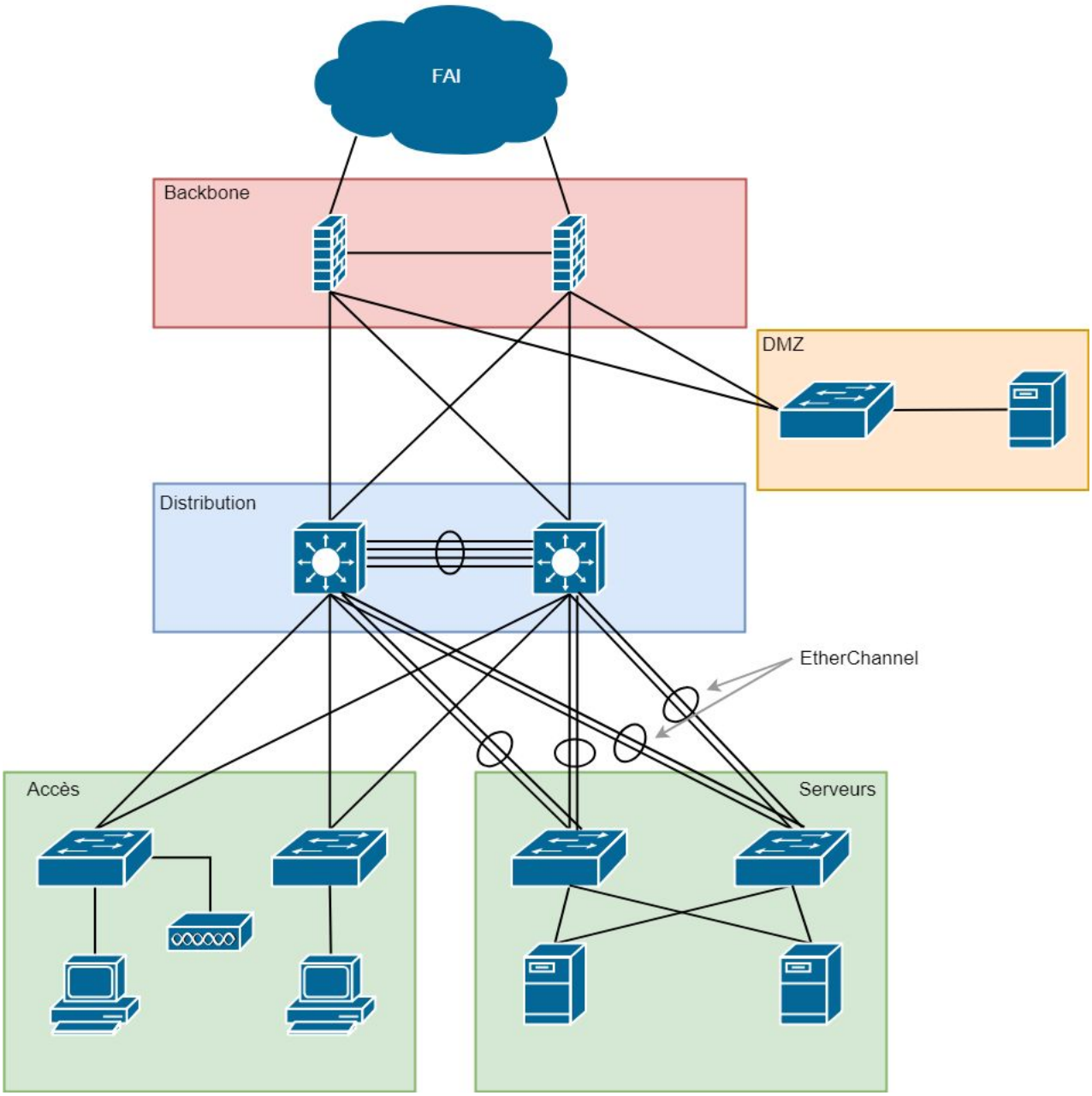
La connexion au tunnel IPsec se fait également depuis les pare-feux. Une fois de plus, la redondance oblige de maintenir les connexions au tunnel vers les sites distants pour chacun des pare-feux. Un tunnel est établi vers chaque site, et un système d'ACL restreint ou autorise l'accès selon une charte de sécurité.

Une redondance importante est également mise en place entre la couche de Backbone et la couche de Distribution à travers de multiple connexions point-à-point. Cette redondance est maintenue à travers une série de routes statiques avec un métrique calculé afin de privilégié un pare-feu dans le cas de flux upstream, et afin de respecter les les priorités root bridge par VLAN pour le flux downstream.

La couche distribution redondante est maintenue en communication à travers une agrégation de liens EtherChannel entre les deux switch. Ces deux Layer 3 font office de serveur VTP afin d'uniformiser la distribution des VLAN. Ils se répartissent également la charge à travers le protocol Spanning Tree où le nombre de VLAN auxquels ils font office de root bridge est départagé de manière équitable. Le protocole HSRP assure une transparence de la passerelle active pour chaque client au sein des VLAN.

La zone serveurs est également connectée avec redondance à la couche distribution, ainsi que par des liens agrégés EtherChannel pour pouvoir assurer un débit plus important et réduire les risque de congestions vers le réseau dédié aux serveurs. Chaque serveur est prévu pour être connecté aux deux switch afin d'offrire également ces services en redondance à travers des technologies tels que le "NIC Teaming".

La zone accès est également maintenue en liens redondants à la couche distribution. Les ports à attribuer aux différents VLAN sont à définir selon le déploiement dans les bâtiments. Certaines mesures de sécurité en été également mises en place. Il est également possible de connecter une série de points d'accès afin de permettre un accès sans fil au réseau.


FAI
Backbone
DMZ
Distribution
EtherChannel
Accès
Serveurs

Los Angeles & New Delhi

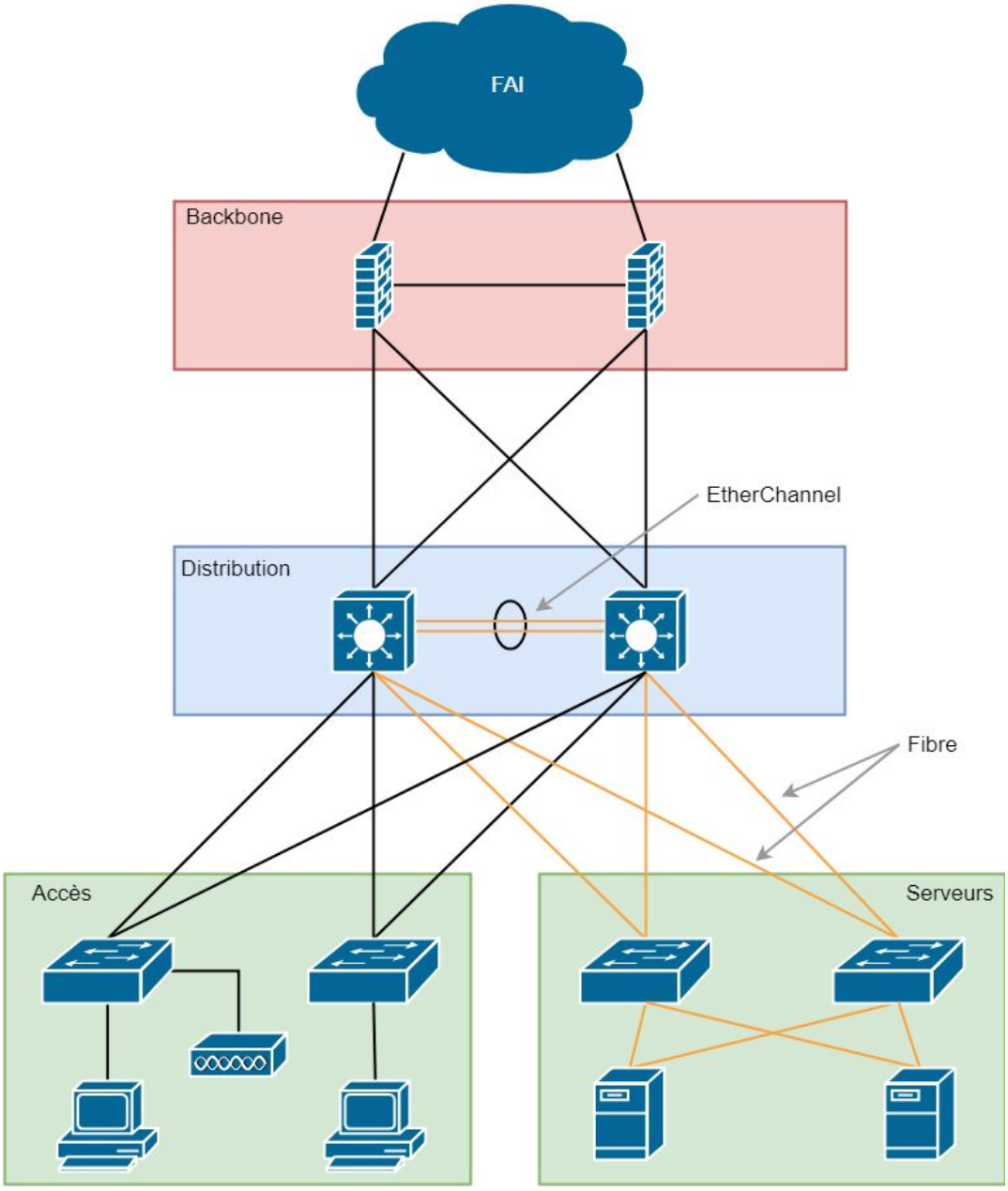
A l'instar du site de Paris, on retrouve une redondance de la couche Backbone avec les pare-feux redondants. Ceux-ci sont également configurés avec des tunnels IPsec vers le site de Paris et entre les sites branche. Ne mettant aucun service en public sur Internet, ces sites sont dépourvus de zone DMZ, et donc ne nécessitent qu'un seul NAT dynamique (PAT).

Une fois encore, une redondance importante est prévue entre la couche de Backbone et la couche de Distribution, avec le même système de routes statiques redondantes à travers un calcul de métrique.

La couche distribution devant distribuer le trafic entre la zone accès et la zone serveur, une agrégation de liens en fibre optique a été envisagée afin de réduire au maximum la congestion.

La connexion en fibre a été également utilisée entre la couche distribution et la zone serveur, ce dernier contenant des serveurs de rendu et des serveurs de fichiers contenant des ressources audio/vidéo. La fibre a donc été mise en place dans ce cas afin de ne pas présenter de goulot d'étranglement pour la communication entre serveurs de fichiers et serveurs de rendu, ainsi que la communication entre les utilisateurs travaillant sur site.

Les fonctionnalités de la couche accès et serveurs sont en tout point identiques au site de Paris, avec des accès pour les employés sécurisés contre certaines attaques. Une redondance entre les serveurs et les switch pour assurer le plus haut taux de disponibilité avec le moins de congestion et de latence possible est également mise en place.


FAI
Backbone
EtherChannel
Distribution
Fibre
Accès
Serveurs

Configurations

Administrative

```
hostname PARIS-EDGE-D

enable secret 5 $1$mERr$DWwx4W/5HXD2oail62IeB1

ip domain-name pktsux.com
crypto key generate rsa
1024
username Waldo secret 5 $1$mERr$DWwx4W/5HXD2oail62IeB1
line vty 0 15
transport input ssh
login local
access-class 10 in
exit
ip ssh version 2
access-list 10 permit 10.80.10.0 0.0.0.255
access-list 10 deny any

```

Les mots de passe sont cryptés dans les fichiers de configuration afin d'assurer une meilleure sécurité.

Une ACL bloque l'accès au SSH pour tout autre VLAN que le VLAN 10 correspondant à l'administration.

Spanning Tree

```
spanning-tree mode rapid-pvst
spanning-tree vlan 10,20,30,40,50,60,70,80,90,100,200,250
spanning-tree vlan 10 root primary
spanning-tree vlan 30 root primary
spanning-tree vlan 50 root primary
spanning-tree vlan 70 root primary
spanning-tree vlan 90 root primary
spanning-tree vlan 250 root primary
spanning-tree vlan 20 root secondary
spanning-tree vlan 40 root secondary
spanning-tree vlan 60 root secondary
spanning-tree vlan 80 root secondary
spanning-tree vlan 100 root secondary
spanning-tree vlan 200 root secondary
```

Les Switch de couche 3 se divisent les rôles de root primary pour les différents VLAN afin d'améliorer l'équilibre des charges sur les différents Switch.

VLAN Trunking Protocol et Etherchannel

```
interface range gig1/0/11-12
channel-group 1 mode on

interface port-channel 1
switchport trunk encapsulation dot1q
switchport mode trunk
switchport trunk allowed vlan 10,20,30,40,50,60,70,80,90,100,200,250
switchport trunk native vlan 99
no shutdown
```

Les deux interfaces Gigabit 1/0/11 et Gigabit 1/0/12 sont regroupées pour former un EtherChannel et ainsi augmenter la bande passante.

Hot Standby Router Protocol

```
65  int vlan 10
66  ip address 10.80.10.252 255.255.255.0
67  ip helper-address 10.80.200.10
68  ip access-group ADMINISTRATION-IN in
69  standby version 2
70  standby 10 ip 10.80.10.254
71  standby 10 priority 255
72  standby 10 preempt
73
74  int vlan 20
75  ip address 10.80.20.252 255.255.255.0
76  ip helper-address 10.80.200.10
77  ip access-group DIRECTION-IN in
78  standby version 2
79  standby 20 ip 10.80.20.254
80  standby 20 priority 0
```

Comme pour le protocole Spanning-tree, les Switch de couche 3 se partagent les VLAN à router de façon à améliorer l'équilibre des charges.

Port Security

```
55  int range fa0/1-6
56  switchport mode access
57  switchport access vlan 200
58  switchport port-security
59  switchport port-security maximum 1
60  switchport port-security mac-address sticky
61  spanning-tree portfast
62  spanning-tree bpduguard enable
63  no shutdown
```

Il s'agit d'un snippet de configuration d'une interface du Data center de Paris. C'est pourquoi le nombre maximal de périphériques différents acceptés par les interfaces a été défini sur 1. En effet, à priori un seul serveur sera destiné à être connecté sur ce port.

Pour les interfaces d'accès clients, le nombre a été augmenté à 2 afin de prévoir un ordinateur et un téléphone VoIP.

Static Routing Redundancy

```
43  ip route 0.0.0.0 0.0.0.0 209.165.72.254
44  ip route 0.0.0.0 0.0.0.0 10.80.254.26 5
45
46  ip route 10.80.10.0 255.255.255.0 10.80.254.2
47  ip route 10.80.10.0 255.255.255.0 10.80.254.6 5
48
49  ip route 10.80.30.0 255.255.255.0 10.80.254.2
50  ip route 10.80.30.0 255.255.255.0 10.80.254.6 5
51
```

Sur les pare-feux de chaque site sont configurées des routes statiques vers chacun de VLAN présents sur le site ainsi que vers les FAI.

Une redondance est assurée vers les FAI (le premier lien était directement connecté vers le réseau externe Internet, le second pointant vers le deuxième pare-feu (connecté à un FAI différent).

Pour permettre cette redondance, la route statique dirigée vers le deuxième pare-feu et elle comporte une métrique plus élevée de façon à ne pas être employée par défaut.

Le même principe est appliqué aux routes statiques à destination des VLAN. Chacun des pare-feux prend la moitié des VLAN mais comporte également des routes vers les autres VLAN afin de pouvoir continuer à assurer le routage en cas de panne de l'autre pare-feu.

Static NAT and PAT

```
75  ! NAT
76  ip nat inside source static 10.80.210.10 209.165.72.31
77  ip nat inside source static 10.80.210.20 209.165.72.33
78  ip nat inside source static 10.80.210.30 209.165.72.35
79  access-list 1 permit 10.80.0.0 0.0.255.255
80  ip nat inside source list 1 interface FastEthernet 0/0 overload
81  interface FastEthernet 0/0
82  ip nat outside
83  interface FastEthernet 0/1
84  ip nat inside
85  interface FastEthernet 1/0
86  ip nat inside
87  interface FastEthernet 1/1
88  ip nat inside
89  interface Ethernet0/2/0
90  ip nat inside
```

Ce snippet appartient à un des pare-feux du site de Paris, sur lequel on peut voir les configurations du NAT/PAT pour les clients intranet (appartenant au sous-réseau 10.80.0.0/16) ainsi que la configuration du NAT statique en direction des serveurs en DMZ.

Problèmes connus et améliorations possibles

Afin de simplifier la redondance et la connectivité entre les switch Layer 3 de la couche de distribution, il aurait été intéressant d'utiliser des techniques telles que le Virtual Switching System ou les cisco avec technologie StackWise. Ceci aurait permis de travailler avec deux switch Layer 3 physique reconnus comme un seul switch virtual par le switch de couche accès.

Une amélioration notable serait de pouvoir proposer un rapport de “Penetration Testing” au client. De la sorte, il pourrait avoir une analyse détaillée de la sécurité de l'infrastructure mise en place.

Dû à l'utilisation de Packet Tracer comme outil de virtualisation de ce projet, un nombre important de limitations se sont présentées quant à la création d'un proof of concept pour ce projet. Le plus important étant l'instabilité de Packet Tracer face à un réseau Spanning Tree aussi important que celui envisagé dans ce projet .

L'implémentation totale d'IPv6 a également été impossible pour cause de l’indisponibilité du choix de version pour HSRP sous Packet Tracer, commande indispensable pour du HSRP en IPv6. Cependant, vous trouverez en annexe un plan d'adressage IP qui prend un compte un déploiement en IPv6.

Packet Tracer ne présente également qu'un seul modèle de pare-feu de type ASA. Ce dernier étant d'une instabilité invraisemblable lors d'une configuration à trois couches avec NAT/PAT.

Conclusion

Ce projet nous a permis de conceptualiser une topologie de type industriel avec des technologies de pointe tout en déployant des techniques de redondance et de fiabilité diverses.

Sur base d'une demande client que nous avons analysée et interprétée, nous avons conçu un réseau composé de deux branches distantes, dans lesquelles nous avons englobé au maximum les demandes client.

Cependant suite à de nombreuse complications, notamment dans les contraintes de temps, mais principalement dans le manque de ressources pour déployer ce projet, nous n'avons pas eu l'opportunité de pouvoir rendre un déploiement le plus complet possible. Notre seul outil à disposition, Packet Tracer, a été un frein majeur, tant dans les possibilités de configuration (ASA, IPv6, réseau FAI) que dans sa stabilité non existante avec une topologie aussi vaste et aussi complexe qu'un réseau à trois sites avec un accent prononcé sur la redondance.

Annexe 1 - Adressage Réseau

ADRESSAGE DE BASE					
IPv4	10.X.Y.0/24		IPv6	2000:0000:0000:XXYY::/64	
	X	Site	XX	Site	
	Y	VLAN	YY	Vlan	
SITES					
Paris	80			50	
Los Angeles	76			4C	
New Delhi	78			4E	
VLANS			Gateways		
Administration	10		Virt DG	254	
Direction	20		Phys Gateway 1	253	
RH	30		Phys Gateway 2	252	
Commerciaux	40				
SAP	50				
Artistes	60		Interface Management SW		
Ingénieurs	70			10.X.10.	
Monteur de scène	80		SVR_S1	101	
Experts Son/Vidéo	90		SVR_S2	102	
Voice	100		DMZ_L3	103	
Serveurs	200		S1	111	
DMZ	210		S2	112	
Invités	250		S3	113	
Native/Blackhole	*99*		S4	114	
Backbone	254				

Addressage Serveurs

Site Paris

Intranet	
DHCP	10.80.200.10
DNS	10.80.200.11
Active Dir	10.80.200.12
File server	10.80.200.13
Mail	10.80.200.14
VoIP	10.80.200.15

DMZ	
Web	10.80.210.10
Mail edge	10.80.210.20
DNS	10.80.210.30

Site New Delhi

Serveurs	
DHCP	10.78.200.10
Audio	10.78.200.20
Video	10.78.200.30
SAN	10.78.200.40

Site Los Angeles

Serveurs	
DHCP	10.76.200.10
Audio	10.76.200.20
Video	10.76.200.30
SAN	10.76.200.40

Annexe 2 - Attributions des interfaces physiques

PARIS			
PARIS_S1	Gi0/1	Gi1/0/1	PARIS_L3_G
PARIS_S1	Gi0/2	Gi1/0/1	PARIS_L3_D
PARIS_S2	Gi0/1	Gi1/0/2	PARIS_L3_G
PARIS_S2	Gi0/2	Gi1/0/2	PARIS_L3_D
PARIS_S3	Gi0/1	Gi1/0/3	PARIS_L3_G
PARIS_S3	Gi0/2	Gi1/0/3	PARIS_L3_D
PARIS_S4	Gi0/1	Gi1/0/4	PARIS_L3_G
PARIS_S4	Gi0/2	Gi1/0/4	PARIS_L3_D
PARIS_SW_SRV	Gi0/1	Gi1/1/1	PARIS_L3_G
PARIS_SW_SRV	Gi1/1	Gi1/1/2	PARIS_L3_G
PARIS_SW_SRV	Gi2/1	Gi1/1/1	PARIS_L3_D
PARIS_SW_SRV	Gi3/1	Gi1/1/2	PARIS_L3_D
PARIS_L3_G	Gi1/0/11	Gi1/0/11	PARIS_L3_D
PARIS_L3_G	Gi1/0/12	Gi1/0/12	PARIS_L3_D
PARIS_L3_G	Gi1/0/24	Gi1/0	PARIS_EDGE_G
PARIS_L3_G	Gi1/0/23	Gi2/0	PARIS_EDGE_D
PARIS_L3_D	Gi1/0/23	Gi2/0	PARIS_EDGE_G
PARIS_L3_D	Gi1/0/24	Gi1/0	PARIS_EDGE_D
PARIS_L3_DMZ	Gi1/0/23	Gi3/0	PARIS_EDGE_G
PARIS_L3_DMZ	Gi1/0/24	Gi3/0	PARIS_EDGE_D
PARIS_EDGE_G	Gi0/0	Gi1/0/1	ISP
PARIS_EDGE_D	Gi0/0	Gi1/0/2	ISP

Interfaces Physiques Serveurs

DMZ	
Web	Gi1/0/1
Mail Edge	Gi1/0/2
SVR	
DHCP	Gi4/1
DNS	Gi5/1
AD	Gi6/1
Files	Gi7/1
Mail	Gi8/1
VoIP	Gi9/1