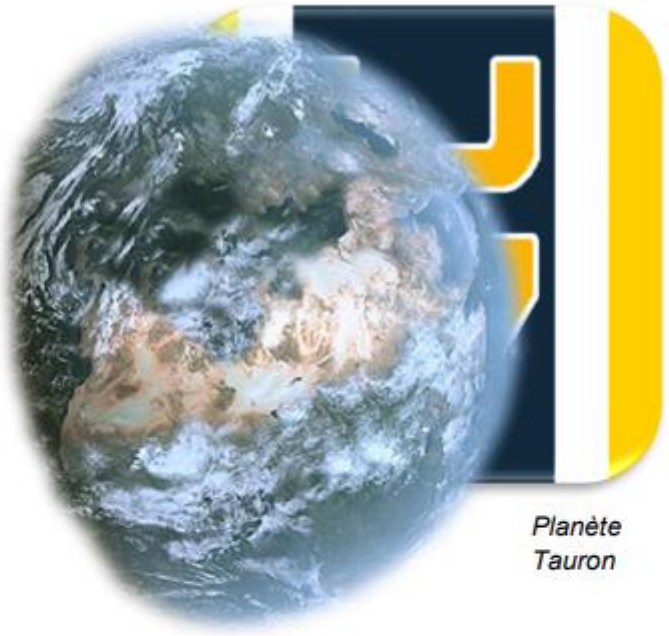
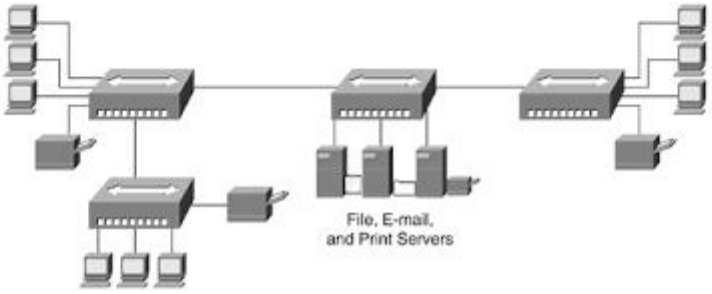
PROJET RÉSEAU

Rapport de spécifications détaillé





cesi ÉCOLE D'INGÉNIEURS

Lhinares Tanguy, Simonneau Olivier, Aoustin Quentin, Chauvel Antoine.

FICHE DE CONFIDENTIALITE DES RAPPORTS ET MEMOIRES
CESI ECOLE D'INGENIEURS

Titre du rapport ou du mémoire : Rapport de spécifications détaillées

Nom et prénom des étudiants : AOUSTIN QUENTIN | SIMONNEAU OLIVIER | LHINARES TANGUY | CHAUVEL ANTOINE

Date de la soutenance : 27/03/2020

Confidentialité du rapport ou du mémoire (soutenance)

☐ **Diffusion libre**

Les rapports / mémoires sont conservés en archives et ils peuvent être librement consultés. Ils peuvent être utilisés par les destinataires, les études peuvent faire l'objet de publication …

☒ **Diffusion restreinte**

Les rapports / mémoires **sont restitués aux élèves** à l'issue de la soutenance. Aucune reproduction n'est autorisée. La responsabilité de cette opération est confiée aux étudiants. Dans le cadre de la politique de lutte contre le plagiat, les rapports / mémoires seront susceptibles d'être analysés pour en vérifier les sources et ceci quel que soit le mode de diffusion prévu ci-dessus.

SOMMAIRE :

Introduction

Pour introduire ce rapport de spécifications techniques, il convient de présenter brièvement le projet.

Vergis Corporation, entreprise basée sur Tauron a trouvé la clé de l'intelligence artificielle en développant le processeur méta-cognitif (MCP), ce qui en fait un concurrent sérieux de Graystone Industries (Caprica City), pour le contrat militaire des Cyber Combat Units.

En effet, les deux entreprises se livrent une guerre industrielle pour remporter un contrat avec le gouvernement Caprican pour développer des technologies pour des applications militaires. Une partie de ce contrat porte sur l'unité cybernétique de combat.

Muni du MCP, le prototype cybernétique de combat U-87, construit par Graystone, montre des signes d'une intelligence comparable à celle des humains et le gouvernement de Caprica signe le contrat. Graystone lance alors la production des Cybernetic Lifeform Nodes, mieux connus sous le nom de Cylons.

Le PDG de Vergis Corporation, Tomas Vergis, furieux de ce vol des plans de son MCP, souhaite revoir rapidement l'architecture de son réseau informatique et la sécurité de son entreprise. C'est à ce moment que notre équipe intervient. Nous avons la lourde tâche de présenter à Tomas Vergis, dans un délai très court, une maquette de la nouvelle infrastructure informatique.

Tomas souhaite repenser l'ensemble du réseau et mettre l'accent sur la sécurité, nous faisant donc partir d'une feuille vierge.

L'entreprise comporte actuellement 4 bâtiments dans le centre de Tauron City : le bâtiment principal, le bâtiment Est, le bâtiment Ouest et une salle informatique principale. Chaque bâtiment est constitué d'un rez-de-chaussée et de deux étages. Parallèlement à cela, l'entreprise est prospère : elle envisage de faire construire un nouveau site à l'image du site principal (constitué des bâtiments précédemment énoncés).

La société souhaite également disposer d'une agence dans l'idée de développer des gammes de robots grands publics. Pour relier les trois sites, Tomas Vergis envisage un réseau MPLS avec comme point central un datacenter. Ce datacenter sera présente en périphérie de la ville dans des locaux sécurisés.

La société nous a fait savoir que le réseau MPLS n'était pas à notre chargé. Nous sommes donc responsables de la constitution d'une architecture réseau pour les sites suivants :

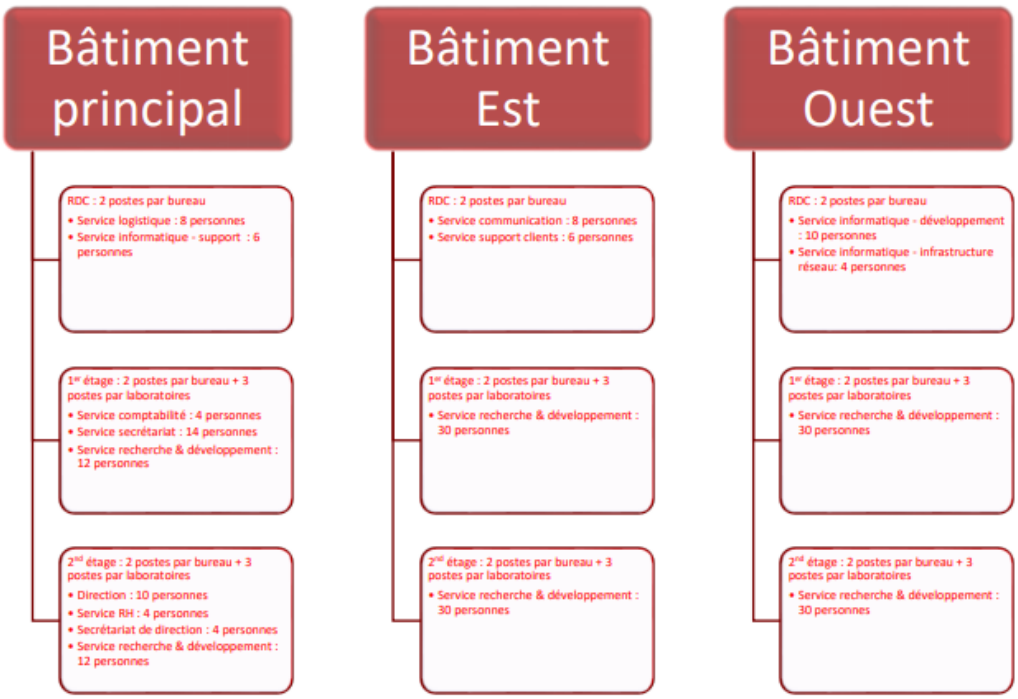
- Site principal
- Site secondaire
- Agence
- Datacenter, épicentre des communications

Il convient de présenter dans le présent document les différents choix que notre équipe a pu réaliser, afin d'arriver à une configuration effective, sécurisée du réseau de l'entreprise Vergis Corporation.

Choix du matériel d'interconnexion

La première étape purement « technique » a été de définir quel type de matériel d'interconnexion allait nous être utile dans l'architecture du réseau.

Le site principal et le site secondaire compteront 12 services, répartis selon les bâtiments et les étages :



Quant à elle, l'agence agrégera deux services : les commerciaux et le support clients. Le datacenter a pour rôle d'assurer le routage des différents sites, tout en autorisant l'accès à certains serveurs pour des services spécifiques.

C'est fondamentalement en considérant les exigences des différents sites et des bâtiments qui les composent que notre choix du matériel d'interconnexion a pu être facilité.

Nous avons utilisé les périphériques intermédiaires fondamentaux :

- Switch
- Routeurs
- Serveurs

Un switch, commutateur en français, permet de connecter plusieurs segments de réseaux entre eux. Un switch possède un nombre de ports déterminé, sur lesquels peuvent être branchés une grande variété de composants (par exemple : des ordinateurs). Un switch agit au niveau 2 du modèle OSI, mais peut aussi agir au niveau 3, ce sont les switchs de niveau 3.

Ainsi, nous avons fait le choix d'utiliser des switchs de niveau 2 pour agréger les ordinateurs et périphériques réseau des différents services des différents sites. Nous avons choisi des switchs de niveau 2 PT-Empty, nous permettant de choisir quels types de ports utiliser, à savoir des connexions GigabitEthernet pour assurer un meilleur débit.

Selon les exigences fournies, un même étage peut contenir plusieurs services. C'est la raison pour laquelle nous avons choisi d'utiliser des switchs de niveau 3, afin d'agréger les switchs de

niveau 2 en un point convergent. Plusieurs switchs de niveau 3 sont utilisés pour réaliser cette agrégation, sans perdre de vue la volonté d'avoir une redondance quasi-parfaite sur les sites de l'entreprise, pour maximiser la disponibilité réseau. Nous avons utilisé des switchs de niveau 3, référence 3650.

Nous nous sommes interrogés sur la pertinence de choisir des switchs de niveau 3 au lieu de routeurs pour agréger le trafic au niveau des différents sites. En lien avec le modèle d'architecture choisie (détaillée ci-après) et les exigences comme par exemple de permettre la communication entre les différents VLANs exigés, le choix de commutateurs de niveau 3 s'est imposé naturellement. En effet, ces derniers permettent un routage inter-VLAN simplifié, ont un coût plus faible que les routeurs, et permettent d'avoir une forte densité de ports, nous permettant d'envisager un maillage afin d'obtenir une redondance quasi-parfaite comme souhaitée.

Nous avons également choisi d'utiliser des routeurs, au niveau du datacenter, pour permettre le routage des différents sites, et pour limiter la propagation de certains protocoles comme VTP (utilisé pour propager les VLANs), afin de ne pas les propager sur les différents sites, tout en ayant la possibilité de choisir un protocole de routage adapté (point explicité dans la suite du présent document). Nous avons utilisé des routeurs PT-Empty, là encore, permettant une plus grande flexibilité dans le choix des ports utilisés (fibres, gigabitEthernet…).

Choix de la topologie réseau adaptée

Après avoir décidé quels matériels d'interconnexion utiliser, il a fallu définir la topologie, c'est-à-dire l'organisation du réseau, sa sémantique, qui a pour but de permettre aux employés des différents services de sites distincts de communiquer et accéder à leurs services dédiés (exemple : serveur FTP pour les chercheurs).

Il nous a fallu avoir du recul pour envisager une topologie adaptée, en ayant conscience qu'il fallait limiter le plus possible l'impact d'une panne d'un équipement d'interconnexion. En effet, Vergis Corporation souhaite avoir une redondance quasi-parfaite, pour le site principal ainsi que le site secondaire et le datacenter.

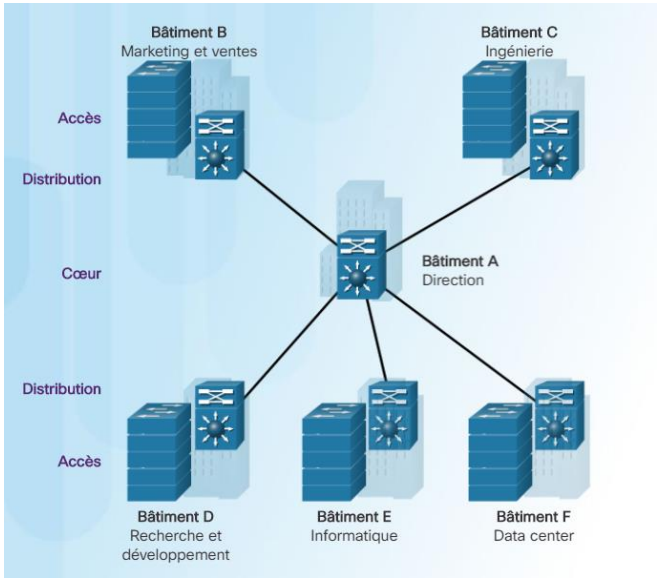
Une même philosophie d'architecture a été considérée sur l'ensemble des sites : réaliser une architecture respectant le modèle à 3 couches/niveaux. Un modèle de conception sert à construire des réseaux en respectant certaines règles d'architectures qui leur permettent de répondre aux besoins actuels et futurs de l'entreprise considérée. Le modèle à 3 couches (Access, Distribution, Core) propose trois niveaux d'agrégation du trafic.

Le Core constitue la moelle osseuse de toute l'architecture, elle sert à transférer rapidement les paquets entre les sites et assure une haute disponibilité. Le Core de notre architecture est donc le datacenter.

La couche distribution agrège les connexions des différents utilisateurs du réseau, par le biais de commutateurs de niveau 3 pour segmenter et organiser le système d'informations en groupes. Nous avons donc réalisé une couche distribution au sein de chaque site, organisée grâce à plusieurs sous-couches de commutateurs de couche 3, directement reliée au Core.

La couche Access, quant à elle, permet aux utilisateurs (ici, aux employés de l'entreprise), d'accéder aux périphériques du réseau. Nous avons donc réalisé une couche Access au sein de chaque service de l'entreprise. Physiquement, cela se matérialise par des commutateurs de niveau 2 reliés aux ordinateurs des employés à chaque étage de chaque bâtiment du site principal, site secondaire et agence.

Ce modèle en 3 couches distribué au sein des différents sites peut se représenter visuellement de la manière suivante :

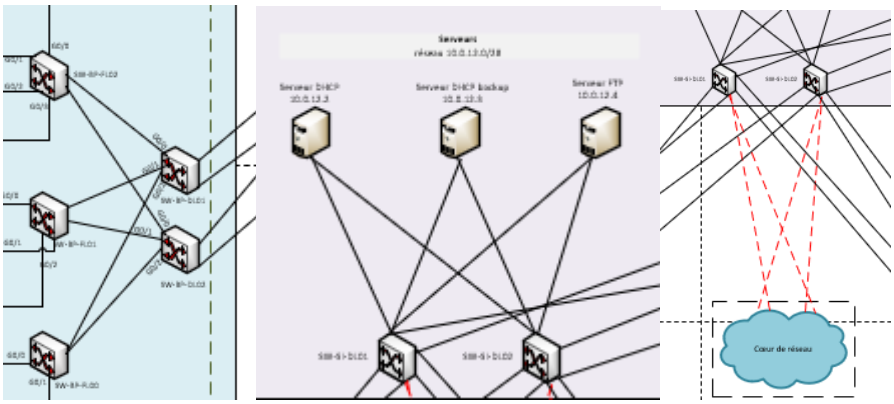


Source : cisco.com

Après avoir défini que nous utiliserons ce modèle d'architecture et en suivrons les grands principes, il a fallu définir quel type d'architecture utiliser pour répondre aux besoins de redondance quasi-parfaite.

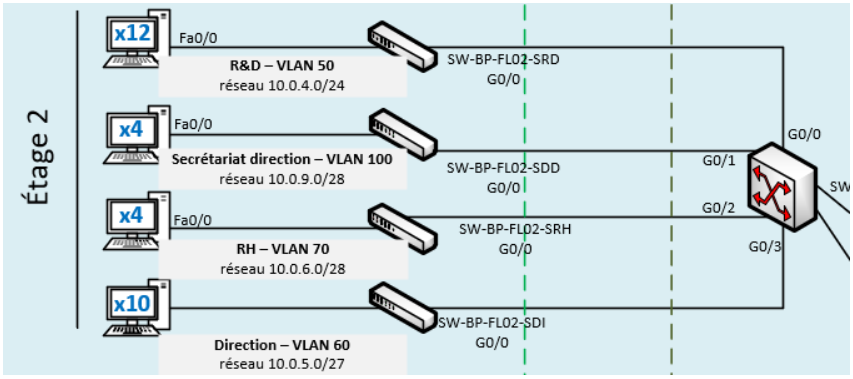
Les topologies bus et anneaux n'étaient pas adaptées pour les couches Core et Distribution, dans le sens où elles dépendent principalement du support de transmission (câble), la panne de celui-ci pouvant paralyser l'ensemble du réseau.

Nous avons donc choisi une topologie maillée, au sein du datacenter et au niveau de la couche Distribution de chaque site, pour assurer une redondance quasi-parfaite, et ne pas compromettre l'accès au réseau à cause d'une panne d'un appareil d'interconnexion ou d'un câble.



Pour de plus amples détails concernant la topologie logique, veuillez-vous référer au fichier dédié fourni.

Au niveau des couches Access, la redondance n'était pas une exigence absolue, nous avons donc relié sans maillage les commutateurs de niveau 2 aux commutateurs de niveau 3, puis aux périphériques utilisateurs. C'est en quelque sorte une topologie arbre, avec une dépendance vis-à-vis du commutateur de niveau 3 et du commutateur de niveau 2 pour l'ordinateur d'un employé en fin de chaîne.



Ces choix ont été appliqués sur l'ensemble des sites, afin d'obtenir une topologie complète, redondante, sans coût excessif en limitant la redondance quasi-parfaite aux couches Distribution et Core, répondant aux exigences de la société Vergis Corporation.

A noter que la topologie logique présentée dans le fichier fourni constitue la topologie dite idéale, inscrivant l'ensemble de la redondance. La relative fragilité du logiciel de simulation Packet Tracer, sur lequel nous avons réalisé la maquette du réseau, lorsqu'il s'agit de réseaux complexes faisant intervenir de nombreux protocoles, ne nous a pas permis d'implémenter une telle redondance (ce qui aurait été possible dans la réalité). C'est donc une version simplifiée qui a été modélisée, dû aux limitations de Packet Tracer.

Choix de la nomenclature

Pour permettre une opérabilité effective et une compréhension facile de l'architecture déployée par l'ensemble des acteurs de l'entreprise Vergis Corporation, il nous a fallu définir une nomenclature simple et claire.

En effet, nous avons été amenés à nommer le matériel d'interconnexion (routeurs, switchs…), les périphériques connectés (ordinateurs, imprimantes réseau…), mais également les réseaux des différents services se trouvant dans les différents sites par des acronymes pour éviter de complexifier les noms de façon non pertinente. Ainsi, notre nomenclature se base sur la règle fondatrice suivante pour le site principal, le site secondaire et l'agence :

Type-equipement batiment-du-site etage-du-site [acronyme-service]

Les différents types d'équipement définis sont les suivants :

- Switchs ➔ SW
- Routeurs ➔ Router
- Ordinateur ➔ PC
- Imprimante ➔ IMPRIMANTE
- Serveur ➔ SER

Le site principal et le site secondaire ayant la même architecture, les bâtiments sont nommés de la façon suivante :

- Bâtiment Principal ➔ BP
- Bâtiment Ouest ➔ BO
- Bâtiment Est ➔ BE

Pour l'agence, n'ayant qu'un unique bâtiment, l'acronyme utilisé est AG.

Pour les différents étages, la convention est la suivante :

- Rez-de-chaussée : FL0
- Étage 1 : FL1
- Étage 2 : FL2

Enfin, les différents services de l'entreprise possèdent tous un acronyme :

Nom du service	Acronyme utilisé
Service logistique	LOG
Service informatique – support	SIS
Service comptabilité	SCO
Service secrétariat	SEC
Service R&D	SRD
Service direction	SDI
Service RH	SRH
Service communication	COM
Service support clients	SSC
Secrétariat de direction	SDD
Service informatique – développement	SID
Service informatique – infrastructure	SII

Ainsi, pour désigner le switch associé au service R&D situé au deuxième étage du bâtiment principal du site principal, on utilisera le nommage suivante : **SW-BP-FL2-SRD**.

Choix de l'adressage IP

Nous avons choisi de définir nos réseaux privés dans la plage 10.0.0.0/8.

Pour répondre aux demandes de l'entreprise, de multiples réseaux ont été imaginés. Un réseau par service et par site, tout d'abord, puis des réseaux pour les serveurs, imprimantes réseau…

Au total, ce sont plus de 70 réseaux qui ont été conçus, sur l'ensemble des sites considérés. Sans réelle expérience dans la constitution d'une architecture respectant le modèle à 3 couches, prévoir à l'avance le nombre exact de réseaux était tâche difficile. Ainsi, l'adressage a été réalisé en amont, mais a subi quelques modifications de manière empirique.

L'utilisation du VLSM n'était pas une contrainte exigée par l'entreprise Vergis Corporation, qui souhaitait une facilité d'organisation et de compréhension de la solution. Ainsi, en choisissant de réaliser l'ensemble de nos réseaux dans la plage 10.0.0.0/8, nous n'avons pas choisi d'utiliser du VLSM, la plage d'adresses IP disponibles étant supérieure à 16 millions.

Voici un extrait du fichier d'adressage réalisé :

SITE PRINCIPAL (La marge sert pour le recrutement et les réseaux bonus pour les évolutions de l'entreprise (nouveau service par exemple)

Acronyme	Service	Marge	Quantité	Réseaux	Masque	CIDR	Gateway	Broadcast	Plage	VLAN	Statique	Numéro Réseau
LOG	Service logistique	22	8	10.0.0.0	255.255.255.224	27	10.0.0.1	10.0.0.31	10.0.0.1 - 10.0.0.30	10	NON	0
SIS	Service informatique - Support	24	6	10.0.1.0	255.255.255.224	27	10.0.1.1	10.0.1.31	10.0.1.1 - 10.0.1.30	20	NON	1
SCO	Service comptabilité	10	4	10.0.2.0	255.255.255.240	28	10.0.2.1	10.0.2.15	10.0.2.1 - 10.0.2.14	30	NON	2
SEC	Service secrétariat	16	14	10.0.3.0	255.255.255.224	27	10.0.3.1	10.0.3.31	10.0.3.1 - 10.0.3.30	40	NON	3
SRD	Service R & D	110	144	10.0.4.0	255.255.255.0	24	10.0.4.1	10.0.4.255	10.0.4.1 - 10.0.4.254	50	NON	4
SDI	Service direction	20	10	10.0.5.0	255.255.255.224	27	10.0.5.1	10.0.5.31	10.0.5.1 - 10.0.5.30	60	NON	5
SRH	Service RH	10	4	10.0.6.0	255.255.255.240	28	10.0.6.1	10.0.6.15	10.0.6.1 - 10.0.6.14	70	NON	6
COM	Service communication	22	8	10.0.7.0	255.255.255.224	27	10.0.7.1	10.0.7.31	10.0.7.1 - 10.0.7.30	80	NON	7
SSC	Service support clients	24	6	10.0.8.0	255.255.255.224	27	10.0.8.1	10.0.8.31	10.0.8.1 - 10.0.8.30	90	NON	8
SDD	Secrétariat de direction	10	4	10.0.9.0	255.255.255.240	28	10.0.9.1	10.0.9.15	10.0.9.1 - 10.0.9.14	100	NON	9
SID	Service Informatique - Développement	20	10	10.0.10.0	255.255.255.224	27	10.0.10.1	10.0.10.31	10.0.10.1 - 10.0.10.30	110	NON	10
SII	Service Informatique - Infrastructure	10	4	10.0.11.0	255.255.255.240	28	10.0.11.1	10.0.11.15	10.0.11.1 - 10.0.11.14	120	NON	11
SER	Serveurs	8	6	10.0.12.0	255.255.255.240	28	10.0.12.1	10.0.12.15	10.0.12.1 - 10.0.12.14		OUI	12
INT	Réseau interne		254	10.0.13.0	255.255.255.0	24	10.0.13.1	10.0.13.255	10.0.13.1 - 10.0.13.254	140	OUI	13
IMPRIMANTE	Réseau pour chaque imprimante bâtiment principal	3	3	10.0.14.0	255.255.255.248	29	10.0.14.1	10.0.14.7	10.0.14.1 - 10.0.14.6	150	OUI	14
IMPRIMANTE	Réseau pour chaque imprimante bâtiment Est	3	3	10.0.15.0	255.255.255.248	29	10.0.15.1	10.0.15.7	10.0.15.1 - 10.0.15.6	160	OUI	15
IMPRIMANTE	Réseau pour chaque imprimante bâtiment Ouest	3	3	10.0.16.0	255.255.255.248	29	10.0.16.1	10.0.16.7	10.0.16.1 - 10.0.16.6	170	OUI	16
BONUS	BONUS		254	10.0.17.0	255.255.255.0	24	10.0.17.1	10.0.17.255	10.0.17.1 - 10.0.17.254	180	OUI	17
BONUS	BONUS		254	10.0.18.0	255.255.255.0	24	10.0.18.1	10.0.18.255	10.0.18.1 - 10.0.18.254	190	OUI	18
BONUS	BONUS		254	10.0.19.0	255.255.255.0	24	10.0.19.1	10.0.19.255	10.0.19.1 - 10.0.19.254	200	OUI	19
ADMIN	Administration à distance (SSH)	54	200	10.0.254.0	255.255.255.0	24	10.0.254.1	10.0.254.255	10.0.254.1 - 10.0.254.254	99	OUI	254

Pour de plus amples détails, veuillez-vous référer au fichier d'adressage complet fourni en annexes à ce fichier.

Acronyme	Service	Marge	Quantité	Réseaux	Masque	CIDR	Gateway	Broadcast	Plage	VLAN	Statique	Numéro Réseau
LOG	Service logistique	22	8	10.1.0.0	255.255.255.224	27	10.1.0.1	10.1.0.31	10.1.0.1 - 10.1.0.30	210	NON	0
SIS	Service informatique - Support	24	6	10.1.1.0	255.255.255.224	27	10.1.1.1	10.1.1.31	10.1.1.1 - 10.1.1.30	220	NON	1
SCO	Service comptabilité	10	4	10.1.2.0	255.255.255.240	28	10.1.2.1	10.1.2.15	10.1.2.1 - 10.1.2.14	230	NON	2
SEC	Service secrétariat	16	14	10.1.3.0	255.255.255.224	27	10.1.3.1	10.1.3.31	10.1.3.1 - 10.1.3.30	240	NON	3
SRD	Service R & D	110	144	10.1.4.0	255.255.255.0	24	10.1.4.1	10.1.4.255	10.1.4.1 - 10.1.4.254	250	NON	4
SDI	Service direction	20	10	10.1.5.0	255.255.255.224	27	10.1.5.1	10.1.5.31	10.1.5.1 - 10.1.5.30	260	NON	5
SRH	Service RH	10	4	10.1.6.0	255.255.255.240	28	10.1.6.1	10.1.6.15	10.1.6.1 - 10.1.6.14	270	NON	6
COM	Service communication	22	8	10.1.7.0	255.255.255.224	27	10.1.7.1	10.1.7.31	10.1.7.1 - 10.1.7.30	280	NON	7

Acronyme / Catégorie	Service	Marge	Quantité	Réseaux	Masque	CIDR	Gateway	Broadcast	Plage	VLAN	Statique	Numéro Réseau
DMZ	Internet - Firewall	252	2	10.0.0.0	255.255.255.0	24	10.0.0.1	10.0.0.255	10.0.0.1 - 10.0.0.254		OUI	0
DMZ	Firewall - Serveur web commercial	4	2	10.3.1.0	255.255.255.248	29	10.3.1.1	10.3.1.7	10.3.1.1 - 10.3.1.6		OUI	1
DMZ	Firewall - Datacenter	4	2	10.3.2.0	255.255.255.248	29	10.3.2.1	10.3.2.7	10.3.2.1 - 10.3.2.6		OUI	2
DMZ	Firewall - Datacenter Backup	4	2	10.3.3.0	255.255.255.248	29	10.3.3.1	10.3.3.7	10.3.3.1 - 10.3.3.6		OUI	3
ROUTEUR - ROUTEUR	Routeur : Agence - Datacenter	4	2	10.3.4.0	255.255.255.248	29	10.3.4.1	10.3.4.7	10.3.4.1 - 10.3.4.6		OUI	4
ROUTEUR - ROUTEUR	Routeur : Agence - Routeur backup	4	2	10.3.5.0	255.255.255.248	29	10.3.5.1	10.3.5.7	10.3.5.1 - 10.3.5.6		OUI	5
ROUTEUR - ROUTEUR	Routeur : Agence - Site principal	4	2	10.3.6.0	255.255.255.248	29	10.3.6.1	10.3.6.7	10.3.6.1 - 10.3.6.6		OUI	6
ROUTEUR - ROUTEUR	Routeur : Agence - Site secondaire	4	2	10.3.7.0	255.255.255.248	29	10.3.7.1	10.3.7.7	10.3.7.1 - 10.3.7.6		OUI	7
ROUTEUR - ROUTEUR	Routeur : Agence - Datacenter Backup	4	2	10.3.8.0	255.255.255.248	29	10.3.8.1	10.3.8.7	10.3.8.1 - 10.3.8.6		OUI	8
ROUTEUR - ROUTEUR	Routeur : Routeur Backup - Site principal	4	2	10.3.9.0	255.255.255.248	29	10.3.9.1	10.3.9.7	10.3.9.1 - 10.3.9.6		OUI	9
ROUTEUR - ROUTEUR	Routeur : Routeur Backup - Site secondaire	4	2	10.3.10.0	255.255.255.248	29	10.3.10.1	10.3.10.7	10.3.10.1 - 10.3.10.6		OUI	10

Choix du protocole de routage

La prochaine étape dans la constitution d'une maquette fonctionnelle de toute l'architecture imaginée, comprenant le routage entre les différents sites comme exigé par l'entreprise Vergis Corporation, était de choisir quel protocole de routage utiliser.

Il existe de multiples protocoles de routage. Nous avons dû choisir un protocole de routage interne. En effet, un tel protocole s'occupe de la gestion des routeurs à l'intérieur d'un domaine. Une de leurs principales caractéristiques est de trouver automatiquement les autres routeurs et de découvrir la topologie du réseau (de manière totale ou partielle) pour déterminer le chemin le plus adapté afin de faire transiter un paquet d'un point A à un point B. Parmi les protocoles de routage interne, nous pouvons citer notamment :

- RIP / RIPv2
- EIGRP
- OSPF

RIP et RIPv2 ne sont pas suffisamment évolués pour les mises en œuvre de réseaux relativement vastes et une croissance dans l'environnement réseau. OSPF et EIGRP s'adaptent bien aux réseaux de grande taille et à la croissance. Il nous a donc fallu faire un choix entre ces deux derniers pour notre projet.

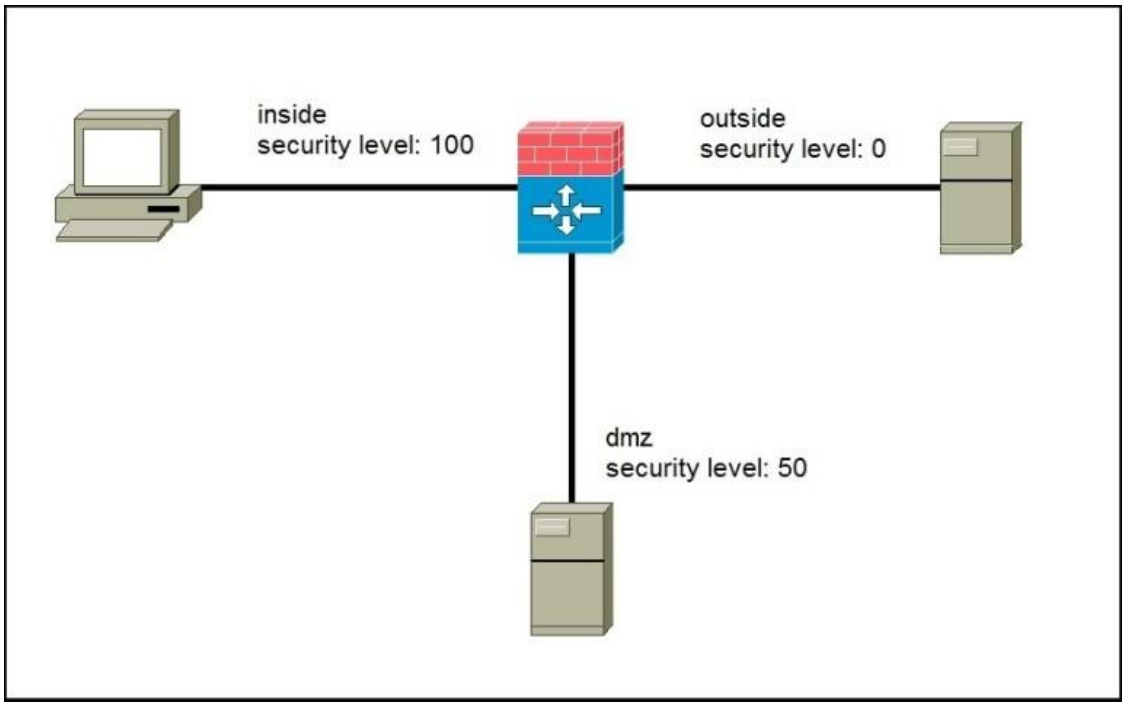
OSPF est un standard de l'IETF (Internet Engineering Task Force, organisation qui élabore et promeut les standards Internet), ce qui n'est pas encore totalement le cas de EIGRP, qui est à la base un protocole propriétaire Cisco.

EIGRP possède une distance administrative de 90, et OSPF 110, et fonctionne sous le principe de systèmes autonomes, quand OSPF travaille avec des zones.

Notre choix s'est porté vers le protocole de routage OSPF, qui fonctionne sous l'algorithme Dijkstra pour déterminer le chemin le plus court entre deux points, en calculant une métrique par le coût (bande passante).

Gestion des niveaux de sécurité par le firewall

L'ASA utilise des niveaux de sécurité associés à chaque interface. Il s'agit d'un nombre compris entre 0 et 100 qui définit la fiabilité du réseau auquel l'interface est connectée. Plus le nombre est élevé, plus la confiance dans le réseau est grande. Le réseau interne local devrait avoir le niveau de sécurité 100. Le réseau extérieur doit être considéré non fiable (Internet par exemple) doit avoir le niveau de 0. L'interface connectée à la zone démilitarisée doit avoir un niveau de sécurité compris entre 1 et 99 (généralement 50 ou 70). Les niveaux de sécurité sont utilisés pour définir comment le trafic initié par une interface est autorisé à revenir d'une autre interface. Par défaut, les interfaces de niveau de sécurité supérieur peuvent initier le trafic à un niveau inférieur. L'inspection de paquet détermine ensuite si le paquet de réponse est autorisé à pénétrer le Firewall.



Source geek-university.com

Dans l'image ci-dessus, nous avons un exemple de réseau géré par un firewall ASA avec trois niveaux de sécurité définis :

- niveau 100 pour le réseau interne

- niveau 50 pour le réseau DMZ

- niveau 0 pour le réseau extérieur

Par défaut, l'ASA arrêtera tout le trafic initial qui tente de passer de niveaux de sécurité inférieurs à des niveaux de sécurité supérieurs. Cela signifie, par exemple, qu'un serveur sur le réseau extérieur ne pourra pas démarrer une communication avec le serveur de notre réseau DMZ ou avec un hôte du réseau interne local. Le serveur de la DMZ peut initialiser le trafic vers l'extérieur (niveau haut vers bas, 50 à 0), mais il ne peut pas initialiser une conversation vers l'intérieur (niveau bas vers haut, 50 essayant d'aller jusqu'à 100). L'hôte à l'intérieur peut initialiser le trafic à la fois vers la DMZ et vers le serveur Internet. Lorsque le serveur extérieur répond à l'hôte intérieur, l'ASA doit être configuré à l'aide d'un NAT afin qu'il autorise dynamiquement ce trafic en retour.

Choix de la méthode NAT

L'une des contraintes de ce projet était de pouvoir accéder à Internet depuis le réseau privé de l'entreprise, notamment pour les employés de l'agence. Ainsi, nous avons implémenté un firewall assurant un filtrage et un premier rempart de sécurité vis-à-vis du réseau privé de la société. Les IPs du réseau de l'entreprise sont des adresses IP privées. Par conséquent, elles ne permettent pas d'accéder à Internet. C'est la raison pour laquelle il a fallu implémenter le NAT au niveau de ce firewall dans le datacenter.

Le NAT, pour Network Address Translation, nous permet donc de traduire, entre autres, une adresse IP privée vers une adresse IP publique pour accéder à Internet, ou communiquer depuis Internet vers le réseau privé. Il existe plusieurs types de NAT :

- NAT statique : correspondance d'une adresse IP privée à une IP publique
- NAT dynamique : correspondance d'un ensemble d'adresses IP privées à un ensemble restreint d'adresses IP publiques (système du « premier arrivé, premier servi »)
- PAT : Similaire au NAT dynamique, incluant la gestion des ports en prime

Considérant notre architecture, nous avons implémenté du NAT statique au niveau des adresses IP privées de la DMZ, comprenant le serveur hébergeant un site vitrine appuyant la stratégie de développement commercial. En effet, n'ayant qu'une unique adresse, il était essentiel que n'importe qui de l'extérieur puisse y accéder sans que la « translation » ne soit amenée à changer. Plus précisément, c'est du NAT statique PAT qui a été implémenté.

Par suite, du NAT dynamique a été implémenté au niveau du firewall pour l'ensemble des autres adresses IP privées du réseau de l'entreprise, qui sont donc traduites en une adresse IP publique. En effet, plusieurs employés peuvent être amenés à communiquer sur Internet, le NAT dynamique s'inscrivant comme une solution pertinente et mieux adaptée que le statique.

Choix de la sécurisation des équipements

L'une des priorités de Tomas Vergis, PDG de la Vergis Corporation est d'assurer la sécurité de son entreprise et des services associés, tout particulièrement informatiques.

La sécurité a été envisagée à deux niveaux : informatique et physique.

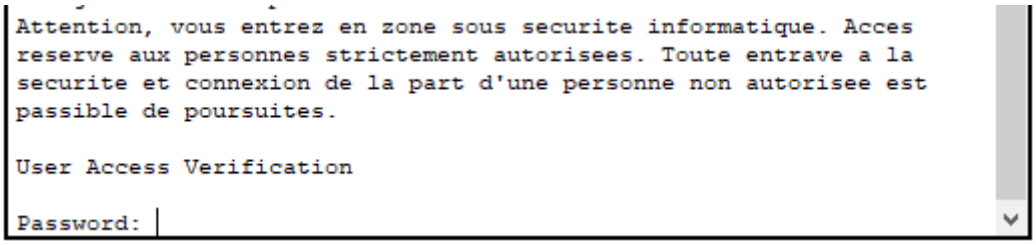
Ainsi, nous avons considéré la sécurité informatique dans toute la réalisation de ce projet, en protégeant tout d'abord les équipements d'interconnexion. En effet, nous avons mis plusieurs mots de passe sur ces derniers pour permettre aux personnes autorisées d'y accéder, et freiner toute intrusion d'un attaquant. Nous avons appliqué un mot de passe :

- Au mode sans privilège
- Au mode « enable »
- Aux lignes vty (accès à distance, SSH)

Le mot de passe diffère d'un mode à l'autre. Pour une question de praticité dans les manipulations Packet Tracer, les mots de passe utilisés sont relativement courts, mais seront changés lors du déploiement à échelle 1 dans l'entreprise de la Vergis Corporation, en utilisant des mots de passe complexes.

Pour également protéger les fichiers de configuration, nous avons utilisé, en mode enable, la commande **service password-encryption**, pour chiffrer les mots de passe et éviter qu'ils ne soient visibles en clair dans les configurations.

De plus, nous avons configuré l'affichage d'une bannière (commande **banner motd**), pour rendre visible un message d'avertissement d'entrée dans une zone sécurisée lorsqu'un utilisateur tente de se connecter à un appareil d'interconnexion.



D'un point de vue physique cette fois, les équipements d'interconnexion seront placés dans des baies de brassage fermées et sécurisées, pour éviter toute manipulation physique ne respectant les règles éthiques de l'entreprise, limitant les intrusions physiques, les baies n'étant accessibles qu'aux administrateurs réseau.

Prix des équipements choisis pour le devis

Pour obtenir un devis détaillé, nous avons regroupé tous les liens référençant les prix des différents équipements choisis.

EQUIPEMENT	PRIX UNITAIRE (HT)	LIEN
CISCO CATALYST C2950	235€24	IT-PLANET
CISCO CATALYST 3650	2978€99	GROS-BILL
ORDINATEUR FIXE WIN 10 PRO	541€61	LDLC
ORDINATEUR FIXE R&D / CHERCHEURS	684€00	LDLC
SERVEURS MULTIFONCTIONS (DHCP, RH, FTP...)	1979€15	PC21
IMPRIMANTE LASER BROTHER	1129€00	BROTHER
PARE-FEU CISCO	416€61	LDLC
ROUTEUR CISCO 887	607€53	INMAC WSTORE

Pour les ordinateurs, il est possible de remarquer une baisse de prix considérable. Effectivement sur LDLC les ordinateurs mis à la disposition des membres du service R&D et de quelques autres personnes sont affichés à un prix de 1359€95. Avant tout durant cette crise sanitaire les prix varient très régulièrement et nous avons appliqué un code promotion sur chaque ordinateur d'une valeur de 50€ (code WINDOWS10) ce qui abaisse le prix par ordinateur à 1309€95.

La différence de prix s'explique désormais car le site principal possède déjà 164 ordinateurs « classiques » destinés aux services R&D, informatiques... ainsi nous reprendrions ces 164 ordinateurs au prix actuel 541€61 et remplacerions les machines susdites par ceux de nouvelle génération pour la différence de prix seulement. Cependant si vous calculez vous remarquerez que le prix n'est pas exact, en effet il ne s'agit là que d'une suggestion nous sommes en mesure de vous fournir un devis sans, mais nous avons inclus une offre CONFORT pour chacun de ces ordinateurs ce qui garantirait la sécurité, la stabilité et la reprise en garantie en cas de défaut pour une période de 3 ans. Les frais de livraisons sont aussi pris en compte.