Cahier des Charges du Nouveau Réseau de Rubik’s Cube

Ce document explique en détails l’ancien et le nouveau réseau informatique de l’entreprise Rubik’s Cube ainsi que les configurations nécessaires pour le mettre en place.

Table des matières

Introduction

Dans la cadre d'une campagne de modernisation, l'entreprise de Rubik's Cube a décidé de refaire tout son réseau. Cette décision a été prise d'un commun accord avec tous les chefs des sites de Nantes, Brest, Rennes et Bristol. La cyber sécurité est aujourd'hui un enjeu majeur pour n'importe quelle entreprise. C'est pourquoi cette décision visera à renforcer la sécurité de l'entreprise en mettant en place les mesures nécessaires et conformes aux normes. Ainsi, le présent cahier développera la description des anciens et nouveaux réseaux de chaque site, en passant par une brève présentation des équipes et des sites, ainsi qu'une description des OS, logiciels et serveurs, et une documentation pour la description des équipements.

1 – Présentation des équipes et des sites

1.1 – Equipes en charge du projet

Afin de mener au mieux la refonte du réseau informatique des 4 sites de l'entreprise à savoir le site de Brest, Rennes, Nantes et Bristol, le travail a été réparti aux seins de 4 équipes s'occupant chacune d'un site. Toutes les équipes sont composées d'un chef de projet, d'un ingénieur, d'un ou deux techniciens, ainsi que d'un commercial et toutes supervisées par un directeur de projet.

Le directeur de projet, Arnaud BLANC, a la charge de la supervision des équipes. Sa mission principale est de définir et garantir le bon déroulé du projet, c'est-à-dire de scinder le projet en plusieurs étape avec des durées bien spécifiques afin d'assurer la fluidité de celui-ci. Il est principalement en relation avec les différents chefs de projets et s'occupe de contrôler les travaux rendus par les différentes équipes afin d'en garantir la qualité et l'uniformité. Il compile tous les rendus des équipes pour créer un seul dossier uniforme. Pour finir, il s'assure que toutes les équipes avances au même rythme et réponds aux interrogations des chefs de projet.
Les chefs de projet quant à eux supervisent le déroulé du projet de leurs équipes respectives. Ils s'occupent de gérer aux mieux leurs équipes afin de finir les missions souhaitées par le directeur de projet dans le temps imparti. Cependant, ils réalisent aussi des tâches afin d'épauler leurs équipes.
Les ingénieurs travail en synergie avec les techniciens et s'occupent principalement de la réflexion du nouveau réseau de leur site. Les ingénieurs sont les personnes ayant une très bonne connaissance en informatique pour pouvoir répondre au mieux à des problèmes. De plus, ils aident également les techniciens lors de la création du réseau sur Packet Tracer.
Les techniciens sont en charges de la réalisation techniques et de l'exécutions des solutions proposées par les ingénieurs. Enfin, ils sont en échanges constant avec leur ingénieur respectif.
Les commerciaux rédigent et documentent les taches réalisées par l'équipes. Ils se doivent de retranscrire les éléments techniques de manière compréhensible pour tout le monde.

Voici les équipes en charges du projet :

Site	Chef de projet	Ingénieur	Technicien(s)	Commercial
BREST	Alexandre GERRIER	Johan SECOND	Ugo JANUTOLO	Hubert de NOIROT de TOURNAY
RENNES	Telmo NEIVA MARTINS	Edgar BOBILLON	Emilio FERRAND	Axel FOTSING

			Hedi DRIDI	
NANTES	Alexandre CORNETTO	Jean DEVIC	Agathe DEPELLEY Alexandre LASSEUR	Benoit DOUBLE
BRISTOL	Thomas Da Costa	Clément Passelaigue	Johan Gucciardi	Lorentz Matrundola

1.2 – Les différents sites de l'entreprise

Comme cité précédemment, l'entreprise est composée de 4 sites distincts. Le site de Brest, de Rennes, de Nantes et de Bristol.

1.2.1 - Site de Brest

Le site de Brest est une société sous forme juridique SAS (société par action simplifiée). Une société SAS est une personne morale, une société par action qui ne peut cependant pas offrir ses actions au public, ni les faire admettre sur un marché réglementé. La société est composée au minimum de deux associés, qu'il s'agisse de personnes physiques ou morales. Le SAS est le statut juridique le plus souple, n'obligeant pas la mise en place d'une Assemblée Générale (AG) annuelle, et n'ayant aucun poste obligatoire mis à part celui du président. Ainsi, nos obligations vis-à-vis de ce type de société sont beaucoup plus laxistes, et les démarches moins complexes à effectuer et mettre en place.
Il s'agit du siège social de la marque Rubik's Cube au capital de 550 000€, et le site réunit les départements du marketing, finances, ressources humaines et direction des services informatiques (DSI), ce qui en fait le site le plus imposant des quatre. Il possède aussi un service d'accueil, un accueil visiteur, une salle de conférence, une salle de serveurs dédiés, et une salle de back-up, service non connectée à Internet, pour remettre le service en marche le plus rapidement possible en cas d'attaque ou de panne.

1.2.3 - Site de Rennes

RUBIK'S CUBE de nationalité française est une société de conception et de fabrication de Rubik's Cubes, composée de 900 personnes réparties autour de trois sites géographiques :
Brest, Rennes et Nantes.

L'entreprise vise principalement une tranche d'âge tout public et pour tous les niveaux, depuis peu elle connaît un essor considérable en étant la seule à proposer des Rubik's Cubes 3D grâce à une technique d'impression des pièces holographique unique au monde.

Le site de Renne dont le capital social est de 255 000€, est composé de 100 utilisateurs, de 109 stations de travail et de 15 serveurs, c'est une filiale de Rubik's Cube qui gère principalement l'acheminement et la production de la livraison des produits de l'entreprise. Le site comporte donc l'usine et l'entrepôt de Rubik's Cube.

1.2.3 - Site de Nantes

Le site de Nantes a pour objectif de se concentrer sur la Recherche et le Développement des Rubik's cube, afin d'assurer le futur de l'entreprise. Ce site se doit d'être à la pointe de la cyber sécurité, notamment pour son service de Recherche et Développement.
Il est constitué d'un bâtiment de trois étages : le rez-de-chaussée est composé du service Design, des salles de réunions et de l'accueil, le 1er étage est quant à lui composé du service informatique et de la salle serveur, et les 2èmes et 3èmes étages comportent le service Recherche et Développement.
Tous ces services utilisent un total de 13 serveurs, afin d'assurer le bon fonctionnement et la sécurité de ses 300 postes et de ses 250 utilisateurs.

1.2.4 - Site de Bristol

Le site Bristol a pour objectif de construire et organiser le site existant dans le but d'en faire une antenne commerciale de l'entreprise RUBIK'S CUBE. L'infrastructure actuelle du site de Bristol compte un seul domaine Windows NT4.0 Server. Ce dernier est composé de 55 postes, 53 utilisateurs et 5 serveurs. La succursale de Bristol, qui concerne uniquement quelques utilisateurs, ne comprend ni serveur d'infrastructure ni domaine car ce n'est pas nécessaire.

2 – Description du réseau actuel

2.1 - Site de Brest

2.1.1 - Description de l'existant

La société par action simplifiée (SAS) au capital social de 550 000 € RUBIK'S CUBE est divisée entre quatre sites. Son siège social, situé à Brest regroupe la direction, l'organe de marketing, la finance, les ressources humaines (RH) ainsi que la direction des systèmes d'informations (DSI).
La lecture du document fourni a permis d'obtenir un inventaire du système d'information du site. Le siège social possède donc 410 stations de travail, séparées en services, en vlan. Ces postes disposent de systèmes d'opération différents, on y trouve notamment plusieurs versions de Windows, dont certaines très anciennes. De plus, le site possède 20 serveurs, 4 serveurs Windows 2008 Server ; un contrôleur principal de domaine, un manager de la configuration système, un serveur d'impression, et un serveur dédié aux machines virtuelles, 3 serveurs Windows Server 2003 ; un serveur antivirus, un serveur de messagerie et un de téléphonie, 7 serveurs Ubuntu 12 ; dont un serveur de l'inventaire et de la gestion du parc informatique, un serveur Cisco, quatre serveurs recensant les logs et un aidant à la supervision du réseau, un serveur CentOS de téléphonie et deux serveurs de supervision sans système d'exploitation installé. Actuellement, le site dispose de Kaspersky Lab comme antivirus, ses employés n'ont pas signé de charte informatique et ne sont pas formés aux bons réflexes à avoir en termes de cyber sécurité.
De plus, les postes n'ont pas les mêmes systèmes d'exploitation, ni les mêmes solutions, ce qui oblige les utilisateurs à devoir apprendre à utiliser plusieurs applications pour faire le même travail. L'entreprise RUBIK'S CUBE souhaite envisager une orientation vers le développement durable en numérisant son SI, une réduction des coûts, un SI plus réactif et sécurisé.
Cependant, cette étude n'est valable que pour le site de Brest car chaque site dispose d'un SI différent.

2.1.2 - Description des problèmes

La non-uniformisation des solutions utilisées :

Tout d'abord, le site de Brest regroupe de nombreux postes de travail, mais ces derniers ne sont pas uniformes, certains ont comme système d'exploitation Windows Professionnel, tandis que d'autres utilisent Windows Vista, Windows XP... Ces versions de Windows sont toutes différentes, ce qui force les employés à se former sur plusieurs solutions. Ce problème se répercute également sur les applications, qui peuvent être installées en plusieurs versions, ou qui ne servent à rien puisque d'autres permettent d'effectuer le même travail. Ainsi, les employés doivent apprendre à utiliser plusieurs applications, certaines peuvent utiliser des formats de

fichiers non-accessibles par les autres, et l'entreprise doit acheter des licences inutiles pour garder toutes ses licences conformes.

La cybersécurité du réseau :

Le site de Brest est très sensible aux risques informatiques. En effet, comme expliqué précédemment, les machines ne sont pas uniformisées. Certaines applications ne sont donc pas mises à jour, tandis que d'autres ne sont simplement plus suivies par leurs créateurs. De plus, les employés n'ont pas signé de charte informatique lors de leur entrée dans l'entreprise, la SAS RUBIK'S CUBE est donc actuellement légalement responsable de chaque action effectuée sur son réseau, ce qui est problématique. Enfin, ses employés n'ont jamais été formés pour se protéger sur internet, ils peuvent donc attaquer malgré eux l'entreprise en utilisant une clé USB trouvée dans la rue, ou en téléchargeant des logiciels malveillants puisqu'ils sont administrateurs de leurs machines par exemple. L'entreprise ne dispose pas d'un serveur de récupération en cas de perte de données.

L'évolutivité du SI :

Un autre problème recensé lors de la lecture du document fourni est la difficulté de modifier le SI actuel. En effet, puisque de nombreuses applications différentes sont installées et utilisées, certaines sont propriétaires, on peut donc en déduire que dans le cas où plus tard, ces applications ne sont plus assez performantes ou simplement non mises à jour, on ne puisse plus modifier ces fichiers avec d'autres applications, ce qui rend difficile l'évolution du SI. De plus, le réseau actuel ne permet pas d'envisager le rajout potentiel d'un autre site, voire l'agrandissement du site actuel.

Le développement durable :

L'entreprise RUBIK'S CUBE souhaite s'inscrire dans la logique du développement durable en numérisant toutes ses activités (archives papier, documents, supprimer les imprimantes installées...). Cependant, la solution proposée par l'entreprise et le développement durable sont antithétiques.

2.1.3 - Solutions envisagées

Rendre uniforme le SI de Brest et diminuer les couts :

Nous avons expliqué plus tôt que le site de Brest mettait à disposition de ses employés beaucoup d'applications différentes. Il faudrait donc déployer de nouvelles applications dans tout le SI. Afin, de ne pas perturber l'activité de l'entreprise, les techniciens pourraient faire les

modifications par groupes de 10 postes étant donné qu'il y a 400 employés pour 410 postes. Chaque poste devrait être complètement réinitialisé, afin d'installer Windows 11 sur chacun d'entre eux (le choix de l'OS a été effectué en se basant sur son accessibilité, l'expérience des employés sur des OS similaires, sa sécurité et sa compatibilité vis-à-vis des machines et des applications). L'entreprise devrait également effectuer une installation d'applications neuves, ces dernières devraient être les mêmes sur chaque poste, communes afin d'être gardées à jour le plus longtemps possible. Les licences nécessaires seront proposées plus tard, mais les licences de type OEM sont envisagées afin de minimiser les coûts d'installation et d'entretien nécessaires. En parallèle de l'installation des nouveaux postes de travail, les employés devront être formés aux nouveaux outils.
Adopter ces solutions permettra d'augmenter l'efficacité des employés, mais aussi de baisser les coûts puisque moins de licences devront être payées chaque année.

Rendre le SI sécurisé :

Remettre à neuf chaque poste permettra de réduire les risques d'infection, mais ces derniers restent élevés. Il faudrait en premier lieu et dès la réception de ce cahier des charges, modifier les droits de chaque employé. En effet, chacun possède l'administration de sa machine, ce qui crée des failles de sécurité critiques. De plus, les applications devraient être mises à jour régulièrement et automatiquement grâce à des MAJ centralisées. La mise en place d'un serveur de récupération dit « à froid », non relié au réseau de l'entreprise est envisagé afin de pallier de potentielles pertes de données, mais aussi pour restaurer les machines en cas d'une mise à jour mal effectuée Ensuite, puisque l'entreprise ne possède aucune donnée personnelle sensible, la mise en place d'antivirus différents sur chaque VLAN n'est pas nécessaire, elle peut donc garder KASPERSKY. Cependant, chaque employé devra être formé sur les bons réflexes à avoir en termes de cyber sécurité. Enfin, le pare-feu dont les réglages ne sont pas fournis dans le document devrait potentiellement être configuré différemment, et ce pour empêcher de consulter des applications non utiles aux employés (les jeux vidéo par exemple), mais aussi les menaces potentielles.

L'évolutivité du SI et son intégration au développement durable :

Actuellement, le SI du site de Brest rend difficile sa modification. Il faudrait donc penser à faciliter une future évolution, ce qui explique certaines modifications proposées dans le plan d'adressage IP fourni avec ce document. De plus, l'entreprise RUBIK'S CUBE souhaite s'inscrire dans la logique du développement durable, la solution proposée est de numériser tous les documents, et donc de supprimer l'usage du papier et des imprimantes. Il est important de noter que l'usage des services informatiques consomment bien plus que l'usage du papier, il faut donc laisser le choix à l'entreprise entre continuer l'usage du papier ou jeter les imprimantes actuelles et numériser toutes les informations et les échanges, malgré les frais et la pollution engendrés.
Il est important de noter que ces modifications ne concernent que le site de Brest, d'autres modifications peuvent être envisagées, cependant ces dernières nécessitent l'accord des autres équipes travaillant sur le projet.

2.2 - Site de Rennes

2.2.1 - Description de l'existant

Les différents serveurs et leurs fonctionnalités :

Le site de Rennes possède 15 serveurs portant sur des tâches différentes. Sans connaître le nombre exact des serveurs, nous savons toutefois qu'au moins un serveur CCBoot ainsi qu'au moins un serveur "Backup CCBoot" sont mis en place.
Le serveur CCBoot est un serveur pouvant lancer sur un poste physique un système d'exécution sans avoir recours à l'installation d'un stockage interne sur chaque poste physique. De plus, cela nous permet d'accéder à un serveur de fichiers central pour éviter d'avoir un stockage interne sur chaque poste. Le serveur Backup CCBoot nous permet de faire une sauvegarde de ces fichiers pour éviter toute perte en cas de dysfonctionnement du Serveur CCBoot. Ces deux serveurs sont basés sur le système d'exploitation Windows.
Ce serveur de stockage est le serveur Samba, basé sur Linux, contenant tous les fichiers utilisés par les postes. Le site possède également un serveur de déploiement basé sur Windows pour pouvoir attribuer à l'utilisateur le compte adéquat.
Le serveur TSE permet aux utilisateurs d'avoir accès à leurs données à l'extérieur du site. Finalement, le serveur de téléphonie "Rennes Elastix" permet de gérer les appels entrants sur le site.

Installation des postes physiques :

Une partie des postes ont des systèmes d'exploitation se basant sur Windows : nous savons qu'il y a au moins une version de Windows NT Workstation qui est une version de Windows orientée sur le réseau et la sécurité, au moins une version de Windows Professionnel plus récente ainsi que d'autres versions de Windows Professionnel plus anciennes, les versions Windows XP Professionnel et Windows Vista professionnel.
Les postes ayant ces systèmes d'exploitation n'ont pas activé les mises à jour automatiques et sont configurés de façon que chaque utilisateur soit le propre administrateur de son poste. Chaque employé à donc accès à tous les paramètres de leurs postes et peut installer et gérer son poste comme il l'entend.

Organisation réseau :

Pour avoir accès à tous ces serveurs, le réseau du site est composé d'un seul routeur menant à un commutateur. Les commutateurs sont connectés à tous les postes au réseau local afin de communiquer entre les postes et les serveurs. Mais ces commutateurs servent également à avoir accès à internet. Chaque poste communiquant entre eux, a une adresse IP : celle-ci est attribuée grâce au "Serveur Windows NT 4.0" qui sert de domaine pour déterminer la plage d'adresses IP

pouvant être attribuée. Ce sont les postes en contactant ce serveur qui vont se voir attribuer une adresse. Le réseau est ainsi équipé de deux pares-feux pour éviter des problèmes venant de l'extérieur ou des communications et connexions non souhaitées au site en question.

Logiciels et services :

Au sein du site les différents postes peuvent avoir ses propres logiciels, systèmes d'exploitation ainsi que des antivirus : à chaque nouvelle installation ou addition, les appareils et logiciels obtenus ne sont pas forcément les mêmes que les précédents.
Tous les postes possèdent la suite bureautique Office de Microsoft pour avoir accès aux outils indispensables, mais les versions de cette dernière sont multiples selon les postes.
Il est prévu que chaque site (Site de Nantes, Rennes et Brest) possède son propre serveur d'infrastructure lié au domaine auquel il appartient.

2.2.2 - Description des problèmes

Le réseau actuel semblant poser de nombreux problèmes que ce soit par sa réactivité, ses coûts de gestion, sa sécurité ou bien sa complexité, l'entreprise Rubik's Cube a demandé un audit du système d'information à une société extérieure en 2021. Cet audit a soulevé de nombreux problèmes confirmant les doutes qui avaient été soulevés précédemment.

Des systèmes d'exploitation différents :

Le système d'information utilise de nombreux systèmes d'exploitation différents. Nous avons, comme dit précédemment, plusieurs systèmes d'exploitation Windows, ce qui pose un problème d'homogénéité. Nous retrouvons la même chose pour les logiciels, où plusieurs versions d'Office peuvent être installées sur différents postes. En effet, les différents services au sein de cette même entreprise peuvent donc utiliser des logiciels différents ou des versions non compatibles entre elles, pouvant poser des problèmes de communication ou de coopération.
On retrouve également ce problème pour les antivirus, chaque site possède son propre antivirus. Or, il est défavorable d'utiliser différents antivirus au sein du même site pour des raisons d'efficacité et de coût. En effet, les antivirus peuvent se détecter mutuellement et créer de fausses alertes de sécurité voir créer des problèmes et des ralentissements sur le réseau.

Une lenteur informatique touchant tous les utilisateurs du réseau :

A cause d'une diversité trop élevée, la qualification des logiciels est multipliée par 3. Essayer de mettre à jour un logiciel ou un système d'exploitation demande de procéder à des tests afin de s'assurer que tout fonctionne. Le but principal étant de ne pas impacter les

différents services. Mettre à jour une version de Microsoft Word demanderait beaucoup de temps afin de le tester sur les multiples postes et les différents systèmes d'exploitation.
De plus, cette hétérogénéité peut causer des ralentissements dans les communications entre les postes, utilisant des logiciels différents et incompatibles.

Un problème de cybersécurité trop important :

Les systèmes d'informations en plus d'être trop hétérogènes possèdent des versions trop anciennes. Le fait que les systèmes et les logiciels ne soient pas à jour pose des problèmes de sécurité et de rapidité. Une version pas à jour peut forcer l'utilisation de protocoles de communication anciens, c'est-à-dire l'utilisation de technologies non sécurisées. Les mises à jour peuvent également aider à améliorer les produits et à réparer les failles de sécurité potentielles. De plus, un logiciel trop ancien peut avoir été abandonné par le développeur et ne plus être tenu à jour, il reste donc important de s'assurer que les logiciels et systèmes d'exploitation soient toujours mis à jour par les développeurs. Ce qui n'est surement pas le cas de Windows XP ou Windows Vista.
Il n'y a pas non plus d'installation automatisée des mises à jour. Nous savons en effet que la cybersécurité passe entre autres par les mises à jour pouvant réparer des failles de sécurité importantes, c'est donc un réel problème de ne pas avoir de solutions centralisées pour mettre à jour les postes et les logiciels.
De plus, tous les utilisateurs ont les droits administrateurs sur leur poste de travail, posant un gros problème de sécurité. Les droits administrateurs doivent être réservés pour les administrateurs afin de procéder à certaines tâches, et non pour travailler de façon prolongée. Le risque est l'installation d'applications non autorisées par l'entreprise ainsi que l'utilisation de périphériques externes comme les clés USB pouvant amener des virus et d'autres risques.

Un SI avec des couts de gestions trop élevés :

Comme vu précédemment, le réseau possède de nombreux problèmes de performances et de sécurité. Cela est d'autant plus un problème que le système est onéreux au quotidien.
En effet, les administrateurs doivent donc administrer un grand nombre de postes différents (109) que ce soit par le système d'exploitation ou les logiciels. Il demande donc de grandes compétences et chaque action sur le parc demandera plus de temps que nécessaire à cause de cette même diversité. Cette perte de temps augmente le coût de gestion de façon significative. Utiliser plusieurs logiciels et systèmes d'exploitation pose aussi un problème pour la formation des utilisateurs qui doivent donc connaître plusieurs versions du même logiciel afin de faire le même travail. Cela peut donc demander plus de formations, une charge de travail plus importante augmentant en conséquence les coûts.
De plus, posséder plusieurs licences demande de multiples achats et abonnements. Ces achats faits petit à petit selon les besoins actuels font en sorte que l'entreprise paye le prix fort et ne négocie pas ses achats pour de grosses quantités.

Une gestion par les administrateurs trop compliqué :

Finalement, la gestion d'un parc aussi hétérogène rend la mise en œuvre de modifications plus compliquée qu'elles ne sont censées l'être.
La gestion et le suivi des licences est trop compliqué et peut causer des oublis de licence ou bien des abonnements pour des logiciels ou des postes qui ne sont plus utilisés. C'est pourquoi il vaut mieux repartir de zéro afin de revoir et de refaire l'architecture de l'entreprise Rubik's Cube.

2.2.3- Solutions envisagées

La DSI propose les solutions suivantes pour répondre aux problèmes repérés :
Une centralisation de la gestion des logiciels mise en place par la configuration d'un serveur TSE et d'un serveur WSUS. Le serveur TSE met à disposition des postes, des logiciels, de telle manière qu'il n'est pas nécessaire de les installer sur tous les postes. Cela permet aux utilisateurs de pouvoir travailler avec les logiciels standardisés par l'entreprise sans pour autant les avoir installés sur son ordinateur. Le serveur WSUS (ou serveur de gestion de mises à jour) permet de gérer les mises à jour des postes du réseau. Il est par exemple possible de différer les mises à jour de systèmes d'exploitation pour éviter que le réseau soit saturé à chaque nouvelle mise à jour.

L'utilisation de matériel adapté à l'usage serait une bonne solution. Ainsi, les éléments du réseau recevant une contrainte de débit plus élevée devront être équipés avec des équipements plus performants (câbles FTP, STP, optiques, utilisation de commutateurs plutôt que de concentrateurs...). De même, les éléments du réseau les plus importants devront bénéficier d'un renforcement en termes de cybersécurité.

L'utilisation d'un serveur Active Directory et d'un firewall permettront d'augmenter grandement la sécurité au quotidien. Le serveur AD permet de modifier les droits de création, de modification et de lecture des fichiers utilisés par les utilisateurs, ainsi que les droits accordés aux sessions localement. De l'autre côté, le firewall définit les droits de communication entre les ordinateurs (en interdisant par exemple les protocoles inutiles à l'activité du site, tout en détectant les attaques par reniflement du réseau, ce qui est un logiciel pouvant lire ou enregistrer des données transitant par le biais d'un réseau local non-commuté). De ce fait, un utilisateur ne peut effectuer que les actions qui sont nécessaires à son activité, réduisant les risques de cyberattaque en empêchant un attaquant de s'emparer d'un poste administrateur trop facilement (note : le serveur AD sera installé sur le site de Brest).

La réutilisation des anciens serveurs permettra d'économiser des fonds, et la mise en place des solutions précédentes implique que les utilisateurs ne devront plus être formés sur une trop large variété de logiciels. De plus, la réorganisation du réseau par l'application des solutions mentionnées ci-dessus réduira les coûts d'administration. En effet, il ne sera plus nécessaire pour un technicien d'être formé sur une variété de systèmes d'exploitation différents, réduisant les coûts de formation et les qualifications requises.

2.3 - Site de Nantes

2.3.1- Description de l'existant

Le site de Nantes réunit en son centre 278 postes informatiques dont 260 stations ainsi que 18 serveurs. En addition à cela il y a 5 utilisateurs venant de la DSI.
Le réseau doit être paramétré en classe B (cela correspond au nombre de postes de travail qui peut être mis en place) avec un masque /19 et une plage IP allant de 172.18.64.0 à 172.18.96.0. En effet, toute l'entreprise est en classe B (172.18.x.x), c'est pourquoi un masque /19 a été mis en place pour répartir les sites selon des plages IP différentes.

2.3.2- Description des problèmes

La non-uniformisation des solutions utilisées :

Tout d'abord, le site de Nantes regroupe de nombreux postes de travail, mais ces derniers ne sont pas uniformes. Sur certains est installé le système d'exploitation Windows Professionnel, tandis que d'autres utilisent Windows Vista, Windows XP... Ces versions de Windows sont toutes différentes, ce qui force les employés à se former sur plusieurs solutions. Ce problème se répercute également sur les applications, qui doivent être installées en plusieurs versions, ou qui ne servent à rien puisque d'autres permettent d'effectuer le même travail. Ainsi, les employés se verront contraint d'apprendre à utiliser plusieurs applications, certaines pouvant utiliser des formats de fichiers non-accessibles par les autres, impliquant indirectement l'achat de licence inutiles. Cela cause également des problèmes de compatibilité dans le partage de fichiers, empêchant ainsi les employés de travailler correctement.

La cybersécurité du réseau :

Le site de Nantes est très sensible aux risques informatiques. En effet, comme expliqué précédemment, les machines ne sont pas uniformisées. Certaines applications ne sont donc pas mises à jour, tandis que d'autres ne sont simplement plus suivies par leurs créateurs, laissant ainsi de nombreuses failles exploitables par des personnes malveillantes. Ces types de vulnérabilités au niveau application peuvent entraîner des ransomwares, ou autre type de virus de la même catégorie. De plus, les employés n'ont pas signé de charte informatique lors de leur entrée dans l'entreprise, la SAS RUBIK'S CUBE est donc actuellement légalement responsable de chaque action effectuée sur son réseau. Cela signifie que n'importe quelle personne interne à l'entreprise qui aurait par exemple volontairement exécuté du code malveillant sur un poste ne serai pas responsable de son acte, ce qui est problématique pour la sécurité du réseau, et par conséquent, les données de l'entreprise. Enfin, ces employés n'ont jamais été formées pour se protéger sur internet, ils peuvent donc impacter malgré eux l'entreprise en utilisant, par

exemple, une clé USB trouvée dans la rue, ou en téléchargeant des logiciels malveillants. En effet, ayant tous les droits d'administrateur, les employés peuvent autoriser n'importe quelle installation ou exécution sur leur poste, voire sur le réseau. Ceci constitue donc une menace majeure pour l'entreprise pouvant ainsi répandre des potentiels virus ou malwares sur le réseau.

2.3.3- Solutions envisagées

Le site de Nantes comporte pour l'heure de nombreuses failles. Pour les corriger il faut mettre en place un Active Directory (c'est une base de données et un ensemble de services qui permettent de mettre en lien les utilisateurs avec les ressources réseau dont ils ont besoin pour mener à bien leurs missions) en donnant à chaque utilisateur les autorisations nécessaires à son travail sans non plus lui donner tous les droits d'administration. Sécuriser les mots de passe est aussi un enjeu majeur à appliquer dès maintenant pour éviter les attaques de type ingénierie sociale, dictionnaire ou force brute. En addition à cela les employés manquent de notion en cyber sécurité. Il faut donc les former à cela en leur proposant des séminaires de sensibilisation à la cyber sécurité. Il faut également leur demander de passer des certifications telles que le MOOC de L'ANSSI (certification accessible à tous permettant de s'armer contre les cybers risques). Il faut ensuite harmoniser l'administration des postes en installant les mêmes antivirus et systèmes d'exploitation. Enfin, les badges des employés donnent accès à tout le site, il faut donc restreindre les accès de ces derniers afin que les employés ne puissent accéder qu'aux lieux nécessaires au bon déroulement de leur travail.

2.4 – Site de Bristol

2.4.1- Description de l'existant

Sur le site étudié de Bristol, l'objectif du projet sera de construire et organiser le site existant dans le but d'en faire une antenne commerciale de l'entreprise RUBIK'S CUBE.
L'infrastructure actuelle du site de Bristol compte un seul domaine Windows NT4.0 Server, ce dernier est composé de 55 postes, 53 utilisateurs et 5 serveurs. La succursale de Bristol, qui concerne uniquement quelques utilisateurs, ne comprend ni serveur d'infrastructure ni domaine car ce n'est pas nécessaire.

2.4.2- Description des problèmes

Lors de l'étude de l'infrastructure existante, nous avons identifié 3 problèmes majeurs dans l'infrastructure actuelle du site de Bristol.

Cybersécurité du réseau :

Premièrement on retrouve un problème de sécurité car il n'y a aucune infrastructure réseau, ainsi il n'y a pas de droits particuliers pour les utilisateurs, il n'y a aucune restriction, on ne retrouve également aucun vlan ou firewall. Le réseau actuel est donc très vulnérable et fragile

OS et ressources logicielles non-compatibles :

De plus on retrouve un problème de compatibilité d'OS et de ressources logicielles, en effet les différents utilisateurs n'utilisent pas tous les mêmes logiciels ce qui posera des problèmes de compatibilité lors des transferts de fichiers par exemple et risque de ralentir le travail de chacun.

Problèmes de conception :

Lors de l'étude de la documentation liée au projet, nous avons rencontré certains problèmes dans la conception, ces problèmes devront alors être résolus afin de mener à bien le projet.
En effet, les utilisateurs sont administrateurs de leurs propres stations de travail, ainsi ils ont tous les droits et aucune restriction ne leur est imposée ce qui pourrait permettre à n'importe quel utilisateur d'effectuer des actions dangereuses pour le SI de l'entreprise.

2.4.3- Solutions envisagées

Afin de parer les problèmes de sécurité, nous proposons la mise en place d'un pare-feu afin de protéger le réseau de potentielles entrées frauduleuses, il faudrait également installer des antivirus sur les postes afin de les protéger, mettre en place un VLAN par switch afin d'isoler et de séparer les différents réseaux mis en place.
De plus, dans la perspective de réorganiser le réseau et de le rendre plus efficace, nous proposons de faire du VLSM afin d'optimiser l'utilisation des adresses IP, de mettre en place un service DHCP pour attribuer automatiquement des adresses IP aux postes, de mettre à jour les postes sous Windows 11 et d'installer les mêmes logiciels sur tous les postes afin de parer les problèmes d'incompatibilité.
Il sera important de mettre à jour les postes pour bénéficier des dernières fonctionnalités et d'améliorer la compatibilité avec les ressources logicielles, les solutions de sécurités mises en place permettront de protéger le réseau et les postes utilisateurs.

3 – Description du nouveau réseau

3.1 – Réseau du site de Brest

3.1.1 – Structure physique

Mise en place d'un routeur central

Afin d'avoir un réseau plus fluide et accessible, il a été décidé de mettre en place un routeur central afin d'avoir un sous-réseau disponible pour tout le site de Brest. Ce routeur sera un routeur de type Cisco, consommant moins d'énergie mais permettant un débit remarquable pour sa taille convenable. Il sera lui-même connecté à un switch central afin de ne pas prendre un routeur possédant trop de ports. Le réseau sera construit en suivant le modèle d'une architecture client-serveur, avec une topologie en étoile, présentant une meilleure sécurité et un risque de collision plus faible.

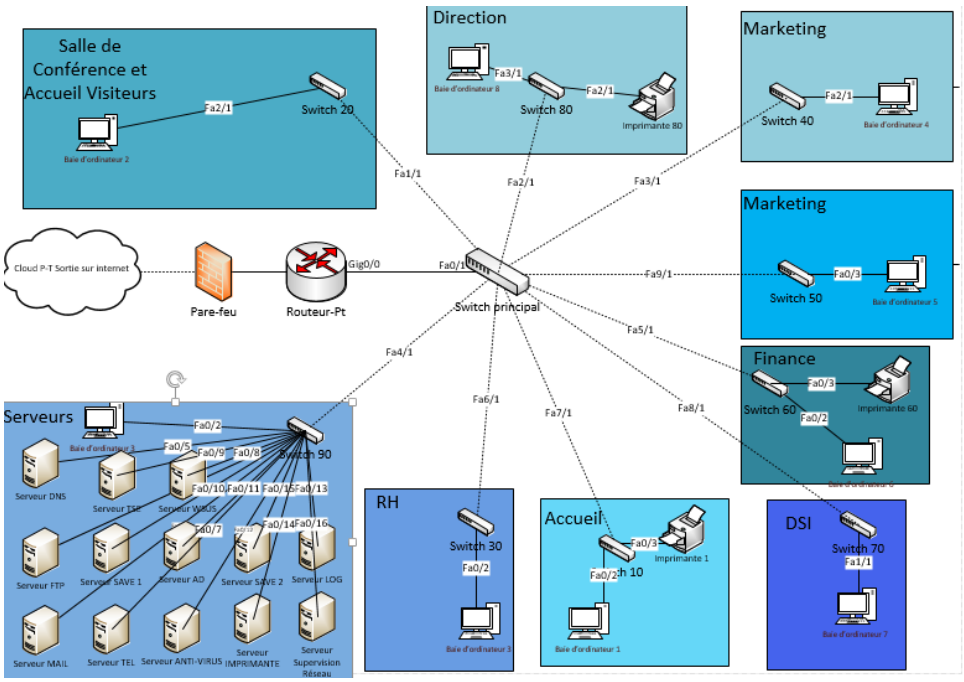
Mise en place d'un Switch central

Pour améliorer la sécurité et la fluidité des communications entre chaque service, un switch central sera mis en place, sur lequel sera installé un autre type d'équipement informatique (précisé plus tard). En effet, le service de l'accueil, possédant moins de postes et ne présentant pas un risque de cybersécurité majeur, ne nécessite pas un switch à lui tout seul, et le récupérer pour une autre utilisation présente une économie de coûts. Ce switch possède 10 ports, est connecté sur le port fa0/1 au routeur, et chaque autre port sera connecté à un service présent sur le site.
Le switch sera connecté au routeur central par un câble 10Gb/s. Le câble coûte plus cher, mais il n'y a qu'une seule connexion qui relie l'intégralité du système au routeur. Ainsi, un câble 1Gb/s serait moins efficace et n'assurerait pas la fluidité.
Cependant, du switch central aux switch secondaires, tous les câbles seront des câbles 1Gb/s, les services ne demandant pas chacun un débit trop élevé.

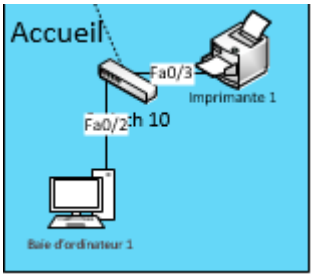
Réaménagement des services en place

Les services en place sont actuellement très anarchiques et présentent des failles de sécurité majeures, en plus d'un service lent et difficilement évolutif
Ainsi, voici la nouvelle installation en créée pour chaque service.
Pour tous les schémas, l'ordinateur fixe sur le schéma représente l'ensemble des postes par service.

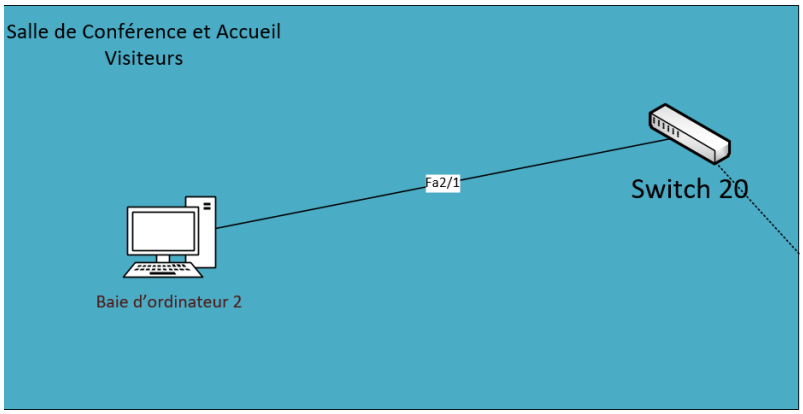
Voici le schéma global, il sera décrit plus en détail pour chaque service :



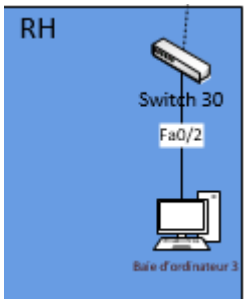
Accueil :
L'accueil ne nécessite pas de particulier entretien. Dans ce service, deux PC fixes seront mis en place pour les hôtes d'accueil ainsi qu'une imprimante.
Depuis le switch du service seront connectés des câbles droits avec un débit de 1Gb/s aux différents équipements informatiques du service. Il en sera de même pour tous les commutateurs des autres services. Il faut utiliser des câbles droits car il s'agit d'interfaces hôte/client :



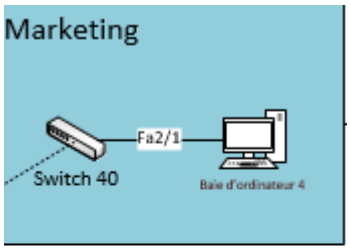
Accueil visiteur et salle de conférence :
Situé sur le même étage, l'accueil des visiteurs et la salle de conférence sont également des services ne présentant pas un entretien lourd nécessaire. Ainsi, le réseau restera le même sur cette partie du site, possédant deux postes à l'accueil visiteur. La salle de conférence possèdera quant à elle un projecteur ainsi qu'un poste fixe :

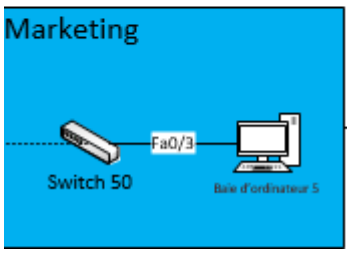


Ressources humaines :
Ce service possède 30 postes, tous connectés à un switch déjà en place. Le service possède des informations confidentielles. Cela donne le schéma suivant :

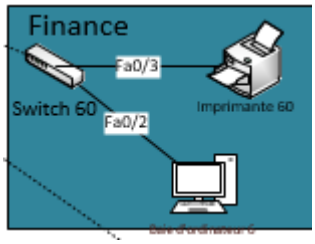


Marketing :
Le service du marketing est le plus gros du site de Brest, et est donc réparti sur deux étages. Le service possède un total de 200 postes et est organisé en tant que grand espace de coworking, sauf pour les postes les plus importants qui possèdent un bureau. L'espace de coworking permet une meilleure organisation des postes et d'utiliser des câbles moins longs, ce qui représente une économie des coûts totaux.
Les schémas représentant les deux étages sont donc similaires :

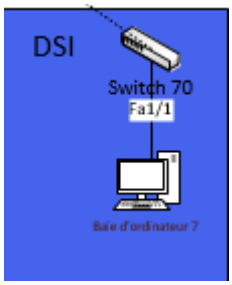




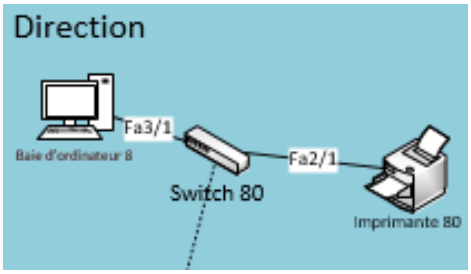
Finances :
Le service des finances est constitué de 100 postes, sur un étage. Il s'agit également d'un espace de coworking, sauf pour les postes à haute responsabilité.
Cela donne le schéma suivant :



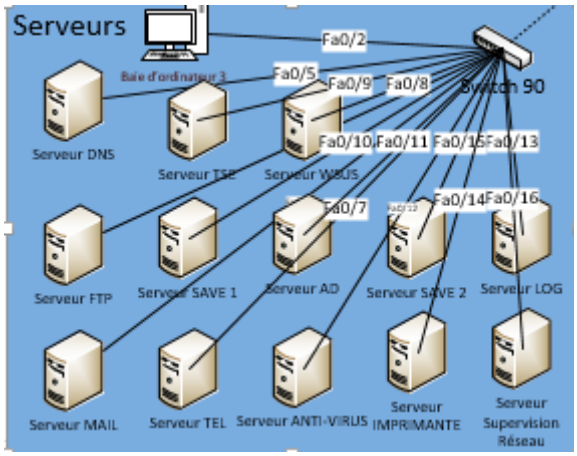
DSI :
La DSI est un service à haute responsabilité, la sécurité y est donc primordiale. Un étage lui est réservé, et il possède 37 postes, la majorité exerçant des responsabilités administrateurs.
Le schéma est donc celui-ci :



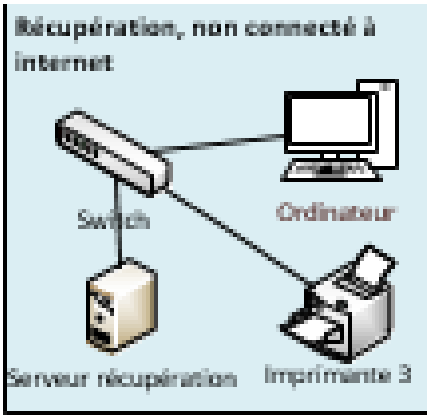
Direction :
La direction est le service le plus important de l'entreprise Rubik's Cube, il regroupe le PDG et l'administration la plus élevée. Ce département possède 33 postes, pour la haute administration et la direction (PDG, directeur, etc.). Il possède également plusieurs imprimantes.
L'installation suivante devra donc être mise en place :



Salle serveurs :
La salle des serveurs est actuellement composée de 20 serveurs différents. Un serveur DNS (Domain Name System) sera ajouté, permettant d'accéder au site Web de l'entreprise depuis l'extérieur.



Salle de récupération non connectée à Internet :
Afin d'éviter de lourdes pertes en cas de cyberattaque ou d'erreur du système compromettant son utilisation, une salle de récupération des données sera mise en place et ne sera pas connectée à Internet. Cette salle contiendra des serveurs de copie des données de l'entreprise, ainsi qu'un poste fixe pour gérer le service.
Le schéma suivant est donc donné :



Serveurs

Le réseau de l'entreprise et du site ne fonctionnera pas sans certains serveurs essentiels. C'est pourquoi une salle des serveurs a été prévue au sein du site de Nantes. Cette salle sera composée de serveurs DNS, FTP, TSE, NAS, de gestion de logs, téléphoniques, imprimantes, WSUS et AD.

Le serveur DNS (Domain Name System) qui sera utilisé servira à faire la liaison entre le nom de domaine du site internet et l'adresse IP de ce même site internet contenue dans le serveur WEB situé sur le site de Bristol.

Le serveur FTP (File Transfer Protocol) permettra de faciliter l'échange de données et de commandes entre les logiciels et les ordinateurs. Les employés pourront ainsi communiquer des documents via le réseau, selon leurs autorisations.

Le serveur TSE (Terminal Server Edition) utilisé permettra à plusieurs utilisateurs de se connecter au serveur à l'aide de clients ou de périphériques distants.

Les serveurs NAS qui seront installés serviront au stockage des fichiers de l'entreprise. Ainsi, il y aura un accès distant à ces serveurs de stockage afin de permettre aux employés de récupérer leurs fichiers en diminuant les risques de sécurité.

Le serveur de gestion de logs qui sera utilisé servira à recueillir la plupart des actions réalisées sur le réseau. Il sera donc facile de retracer une tentative de connexion, une mise à jour, des transferts d'information ou toute autre activité. Ce serveur permettra notamment en cas de problème lié à une cyber attaque, de fournir une preuve pour les autorités, et de garder une trace des actions réalisées lors de cette attaque pour remonter jusqu'à l'attaquant.

Le serveur téléphonique qui sera installé permettra aux employés de communiquer entre eux sans nécessiter un quelconque forfait mobile. Ils pourront donc appeler les services en interne via des numéros à 2 chiffres assignés à chaque bureau.

Le serveur d'impression permettra aux employés d'imprimer des documents depuis leur poste tout en gérant les différentes requêtes pour que le trafic ne soit pas encombré en cas de nombreuses demandes d'impressions. Cela évitera donc des problèmes au niveau de l'imprimante, et les éventuels problèmes de mélanges de photocopies.

Le serveur WSUS (Windows Server Update Services) sera utilisé à des fins de gestion de mise à jour. Sans avoir à faire les mises à jour en local sur chaque poste, il sera possible de mettre à jour l'ensemble du SI via ce serveur. Par conséquent, cela rajoute une couche de sécurité en plus au niveau du réseau car les mises à jour sont centralisées.

Le serveur AD qui sera utilisé servira pour gérer les autorisations de session utilisateurs ainsi que les accès aux ressources des employés en fonction de leurs statuts et besoins. Ce serveur jouera un rôle extrêmement important dans la sécurité de l'entreprise car il associe à chaque employé une session avec les autorisations nécessaires.

Câbles utilisés

Les câbles UTP sont constitués de paires torsadées individuelles sans aucun blindage extérieur. Ces câbles sont couramment utilisés pour les réseaux Ethernet et peuvent prendre en charge des débits allant jusqu'à 10 Gbps. Bien que les câbles UTP soient moins chers que les câbles STP et SSTP, ils sont également plus sensibles aux interférences électromagnétiques, ce qui peut entraîner une perte de qualité de signal.

Les câbles STP sont constitués de paires torsadées individuelles enveloppées d'un blindage métallique, qui est souvent un feuillard ou une tresse en cuivre. Le blindage protège les signaux contre les interférences électromagnétiques externes et minimise également les émissions électromagnétiques provenant du câble. Les câbles STP sont couramment utilisés pour les

réseaux informatiques à haute vitesse et peuvent prendre en charge des débits allant jusqu'à 10 Gbps.

Les câbles SSTP, également appelés câbles catégorie 7, sont constitués de paires torsadées individuelles, chaque paire étant enveloppée dans un blindage métallique, puis le câble complet est recouvert d'un blindage général en forme de feuille. Les deux couches de blindage fournissent une protection supplémentaire contre les interférences électromagnétiques et permettent des performances plus élevées que les câbles STP. Les câbles SSTP sont couramment utilisés dans les réseaux informatiques à haute performance, y compris les centres de données, et peuvent prendre en charge des débits allant jusqu'à 40 Gbps.

En général, les câbles STP et SSTP offrent une meilleure protection contre les interférences électromagnétiques que les câbles UTP, ce qui les rend plus adaptés aux environnements avec des sources d'interférences électromagnétiques élevées ou avec des exigences de performance élevées. Cependant, ils sont également plus coûteux que les câbles UTP.

Ainsi, le câble reliant le switch central au routeur sera un SSTP de 10Gbps. Il est nécessaire que ce câble soit performant subisse peu d'interférence.

Les câbles reliant le switch central aux autres switches seront des câbles STP de 10Gbps. Les câbles offrent un coût moins élevé mais restent performants. Le coût serait en effet trop élevé si seulement des câbles SSTP étaient installés.

Les câbles reliant les postes, imprimantes, etc. seront aussi des câbles de type STP. En effet, les câbles de type UDP ne semblent pas adapté au SI car le bâtiment regroupe de nombreux services, ce qui créer forcément des interférences. Les câbles UDP sont trop exposés à ces interférences. Ainsi, des câbles STP de 1Gbps seront installés.

3.1.2 – Structure logique

Adresses IP :

Sur le plan logique des locaux, le siège de Brest est séparé en dix parties, afin de faciliter leur installation et leur future gestion, elles représentent chacune un secteur du site. Le réseau interne de l'entreprise est donc divisé en dix parties, des vlan nommées vlanX (la description de chaque vlan se fait plus bas sur le cahier des charges). Les adresses IP de chaque machine au sein du réseau sont dynamiques, c'est-à-dire qu'elles peuvent être modifiées, notamment lors du rajout d'une potentielle machine grâce à une configuration DHCP.
Voici un tableau représentant chaque sous-réseau de l'entreprise :

Service	N° Vlan	Etage	Nb poste Dispo.	@Réseau	Masque	1ère IP	Passerelle	@Diffusion

Accueil	10	0	6	172.18.2.80/29	255.255.255.248	.2.81	.2.86	.2.87
Conférence	20	0-1	14	172.18.2.64/28	255.255.255.240	.2.65	.2.78	.2.79
RH	30	2	62	172.18.2.0 /26	255.255.255.192	.2.1	.2.62	.2.63
Marketing 1	40	3	126	172.18.1.0 /25	255.255.255.128	.1.1	.1.126	.1.127
Marketing 2	50	4	126	172.18.1.128/25	255.255.255.128	.1.129	.1.254	.1.255
Finance	60	5	126	172.18.0.128/25	255.255.255.128	.0.129	.0.254	.0.255
DSI	70	6	62	172.18.0.64/26	255.255.255.192	.0.65	.0.126	.0.127
Direction	80	7	62	172.18.0.0/26	255.255.255.192	.0.1	.0.62	.0.63
Serveurs	90	0	62	172.18.3.0/26	255.255.255.192	.3.1	.3.62	.3.63

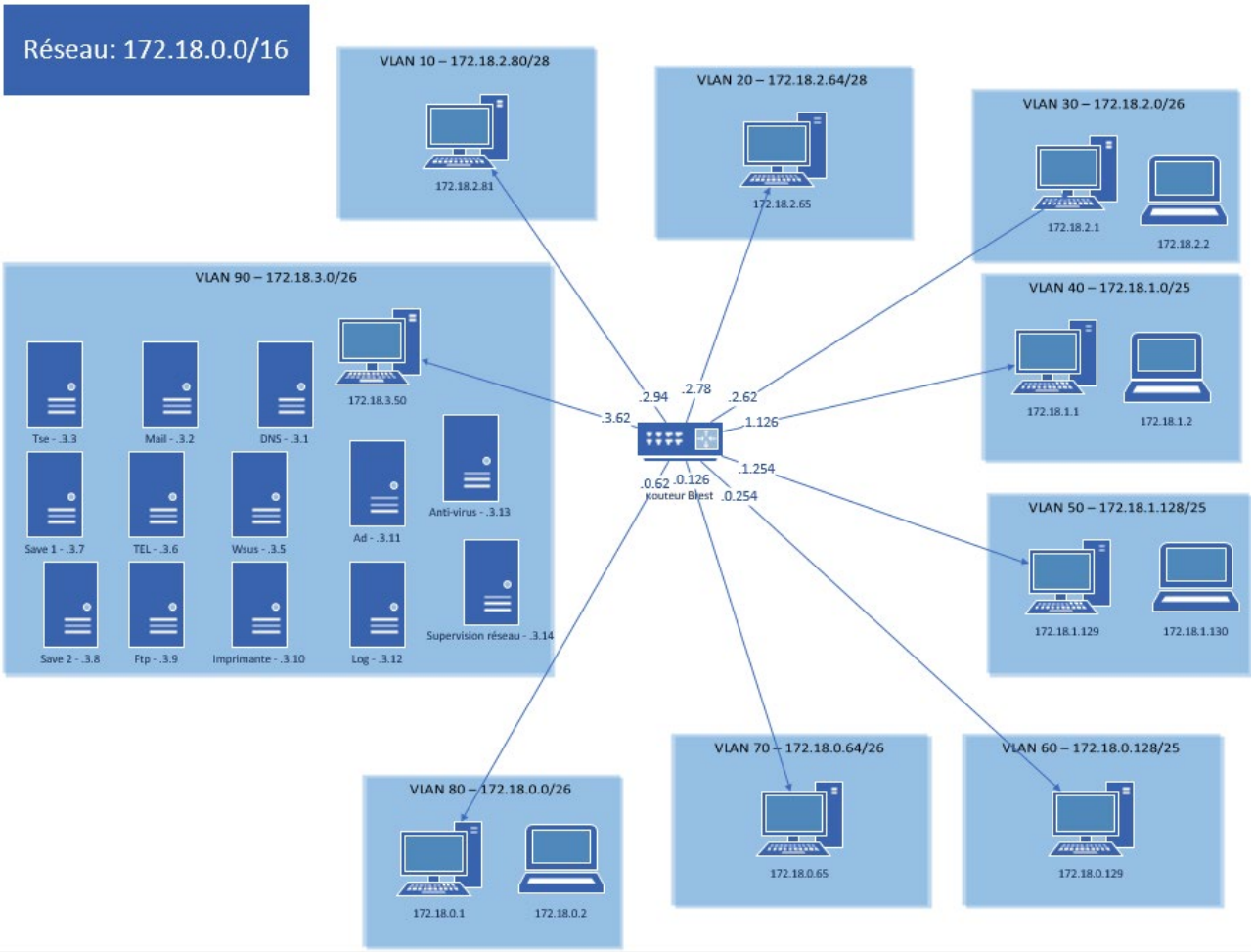
Le réseau étant très grand, de nombreuses adresses IP seront disponibles pour un rajout de sous-réseau ou l'agrandissement d'un sous-réseau déjà existant.
Il se trouvera à l'écart des locaux de l'entreprise un réseau interne, non connecté à internet permettant de sauvegarder le système pour réagir à la suite de pertes de données ou d'attaque pirate.
De plus, les adresses IP des différents serveurs devront être configurées selon le tableau suivant :

Nom du Serveur	Adresse attribuée
Serveur DNS	172.18.3.1
Serveur mail	172.18.3.2
Serveur tse	172.18.3.3
Serveur wsus	172.18.3.4
Serveur téléphonie	172.18.3.5
Serveur sauvegarde	172.18.3.6 - 172.18.3.7
Serveur ftp	172.18.3.8
Serveur imprimante	172.18.3.9
Serveur ad	172.18.3.10
Serveur log	172.18.3.11
Serveur anti-virus	172.18.3.12

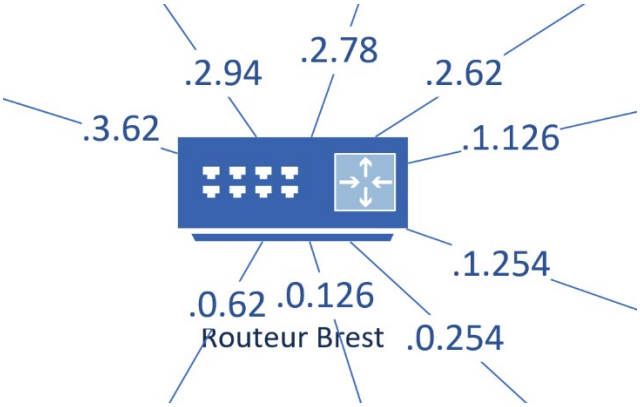
Serveur supervision réseau	172.18.3.13

Utilisation de VLANs

Le nouveau réseau est centré sur un Switch Principal, nommé S1. Ce commutateur sera connecté à un routeur, lui-même relié à Internet par l'intermédiaire d'un pare-feu, ce qui permettra de filtrer les échanges entre le réseau interne de l'entreprise et le reste du web. A partir de ce routeur, plusieurs vlan seront accessibles.
Le choix du nom et numéro des vlan a été réalisé en fonction de l'étage du service. Si le service est au 2ème étage, la vlan correspondante sera la vlan30, en effet, celle du rez-de-chaussée est la vlan10.
Voici le nouveau schéma logique complet du site de Brest, qui sera détaillé vlan par vlan en dessous pour plus de clarté :



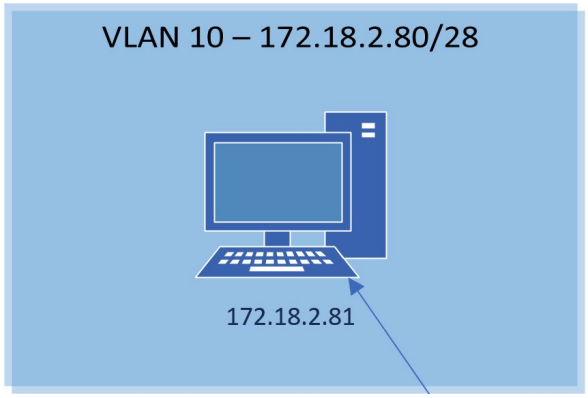
Adresses du routeur :



Vlan 10 - Accueil :

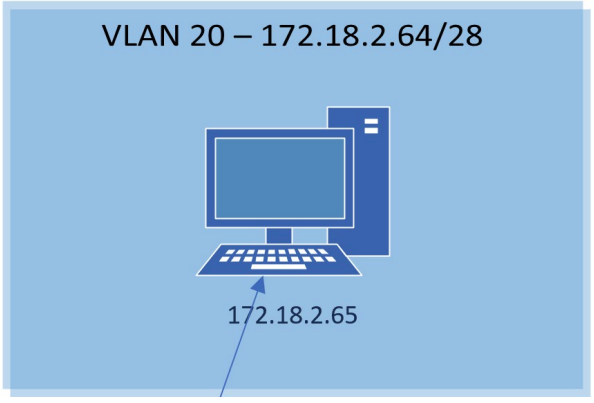
Cette vlan sera celle de la salle d'accueil. Elle sera composée d'une imprimante ainsi que de l'ordinateur de l'hôtesse de l'accueil.

Le schéma logique de cette vlan est le suivant :

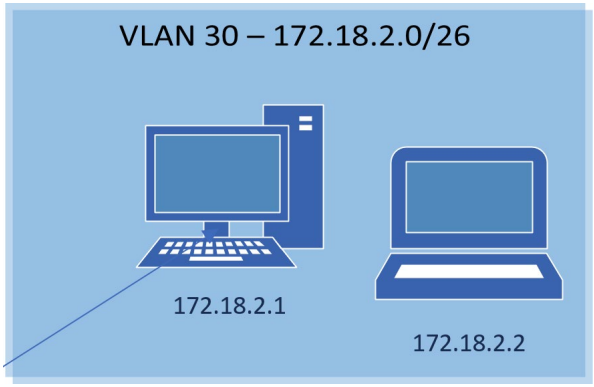


Vlan 20 - Salle de Conférence et Accueil Visiteurs :

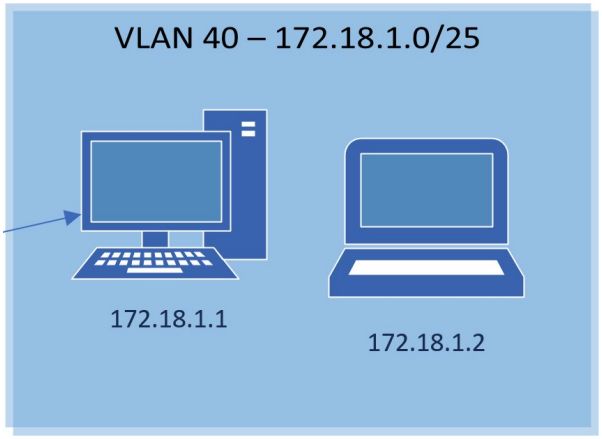
Au rez-de-chaussée se trouve également la salle de conférence et l'accueil des visiteurs. Ce service sera configuré sur le vlan20, il s'agit d'un petit réseau car le service ne possède qu'un poste et un projecteur

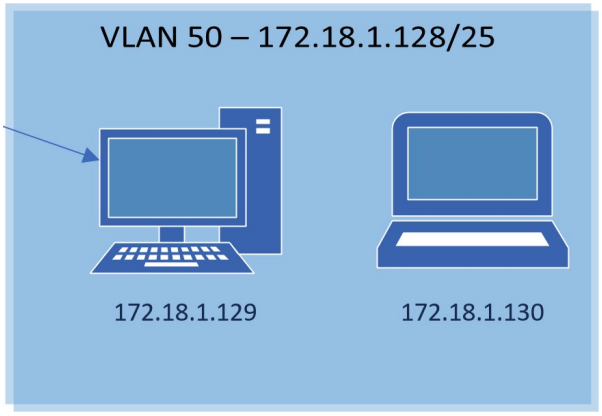


Vlan 30 - Ressources Humaines :
Ici, chaque employé disposera d'un ordinateur fixe. Les employés pourront aussi apporter des PC personnels qui seront branchés en filaire et connectés au sous-réseau.



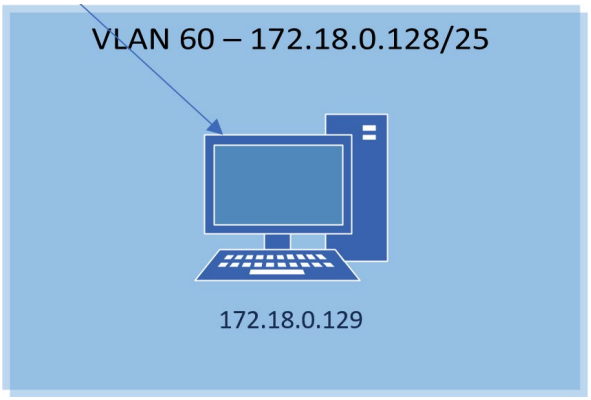
Vlan 40 et 50 - Marketing :
Le service marketing est différent des autres car il est présent sur deux étages. De plus, il s'agit du service le plus imposant de tout le site. Il sera par conséquent divisé en deux vlan. Ici aussi, les employés pourront connecter un ordinateur personnel via un câble au réseau. En voici les schémas :



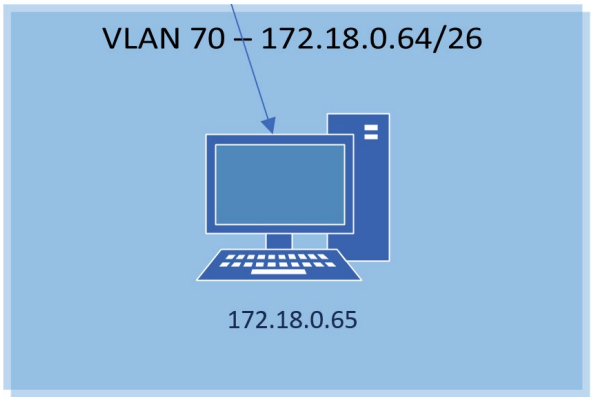


Vlan 60 - Finance :

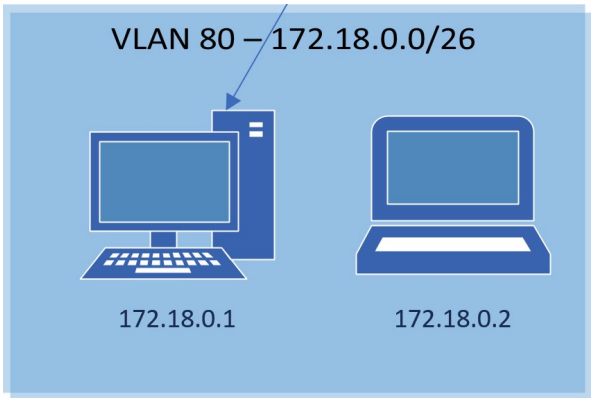
Dans le département des finances ne se trouvent que des postes fixes, et une imprimante. Les employés ne pourront pas amener de PC portable car le service est très sensible en termes de cybersécurité.



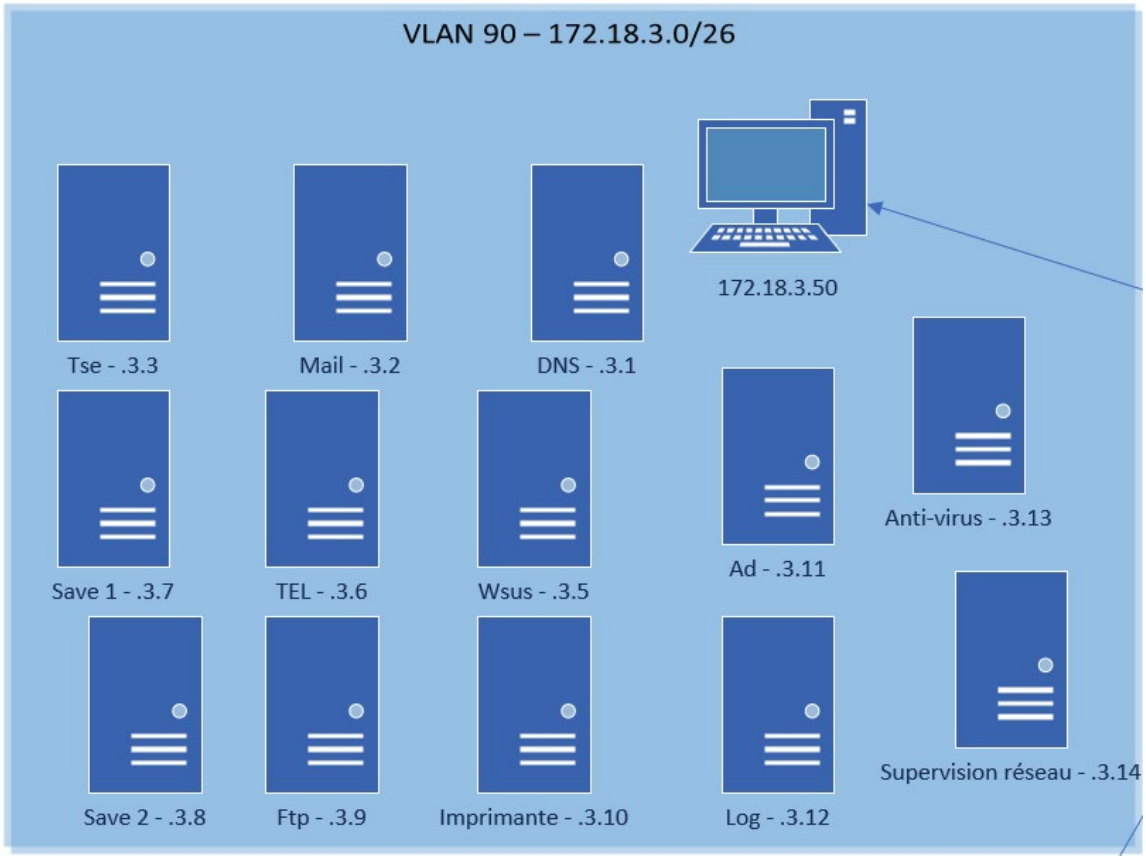
Vlan 70 - Direction des Systèmes d'information :
Ici aussi, il ne se trouve que des postes fixes. Le service est le plus sensible de tout le site.



Vlan 80 - Direction :
Le service de la direction doit accueillir des réunions et est le service permettant de centraliser les décisions politiques et économiques de l'entreprise. Ainsi, il s'agit d'un service très propice aux attaques qui doit être protégé logiquement. Cependant, les personnes travaillant dans ce secteur devront parfois amener leurs ordinateurs personnels et rendront donc le site de Brest spécialement vulnérables aux attaques.



Vlan 90 - Serveurs :
Cette vlan possède, tous les serveurs utiles au site de Brest. Le tableau récapitulatif des serveurs est disponible plus haut



Les Serveurs de Sauvegardes :

Les serveurs de sauvegardes ne sont pas considérés comme faisant partie du schéma logique car ils ne font pas partie du réseau du site de Brest. Ainsi, Seul une description physique peut en être faite.

Firewall :

Un Firewall sera aussi mis à jour avec les autorisations suivantes :

N° règle	Protocole	Port Source	Port destination	@ Source	@ Destination	Action
1	TCP	*	22	172.18.0.64/26	172.18.3.0/26	Autoriser
2	TCP	*	80	172.18.0.0/22	*	Autoriser
3	TCP	*	443	172.18.0.0/22	*	Autoriser
4	TCP	*	25	172.18.0.0/22	172.18.3.0/26	Autoriser
5	TCP	*	3389	172.18.0.64/26	172.18.3.0/26	Autoriser
6	TCP	*	21	172.18.0.0/22	172.18.3.0/26	Autoriser
7	TCP	*	1723	172.18.0.0/22	172.18.3.0/26	Autoriser
8	TCP	*	135	172.18.0.0/22	172.18.3.0/26	Autoriser
9	UDP	*	53	172.18.0.0/22	172.18.3.1	Autoriser
10	UDP	*	123	172.18.0.0/22	172.18.3.0/26	Autoriser
11	UDP	*	137-138	172.18.0.0/22	172.18.3.0/26	Autoriser
12	UDP	*	161	172.18.0.64/26	172.18.3.0/26	Autoriser
13	TCP	*	*	172.18.0.0/22	172.18.0.0/22	Autoriser
14	UDP	*	*	172.18.0.0/22	172.18.0.0/22	Autoriser
15	*	*	*	*	*	Bloquer

Ce tableau montre toutes les autorisations du firewall sur le réseau de Brest. Pour la configuration, le firewall sera installé entre le routeur et les connexions extérieures.

3.1.3 – OS et logiciels

Description des OS

Plusieurs OS seront installés dans le réseau afin de garantir son bon fonctionnement.
Pour commencer, Windows 11 sera installé. En effet, c'est la dernière version sortie à ce jour ce qui permettra d'avoir une version à la pointe de la technologie et également sécurisée.

Également, le réseau sera équipé de Windows Serveur 2022, ce qui permettra d'utiliser plusieurs services comme l'Active Directory et le WSUS. Cette dernière version est également la dernière sortie ce qui signifie que la sécurité est présente.

Enfin ALMA Linux sera utilisé, ce qui permettra l'utilisation de plusieurs services tels que le DNS. Cet OS permettra d'assurer une grande fiabilité ainsi qu'une grande sécurité. Le coût également est intéressant du fait qu'Alma Linux est open source et gratuite.

Description des logiciels

Concernant les logiciels, les salariés seront équipés de la suite Microsoft 365 qui permet d'avoir Word, Excel, Powerpoint, Teams et Share Point. Ces logiciels permettront une grande productivité pour les employés de l'entreprise notamment dans la rédaction, mise en page de documents ou encore dans la communication.

Concernant le service informatique, Wireshark qui permettra aux administrateurs réseaux d'avoir un logiciel qui permet de diagnostiquer et résoudre les problèmes de réseau, ainsi que pour maintenir et améliorer la sécurité du réseau sera installé.

Enfin, PuTTY, qui est un logiciel qui est utilisé pour fournir une connexion sécurisée à des serveurs distants et pour transférer des fichiers entre des ordinateurs locaux et distants sera également installé.

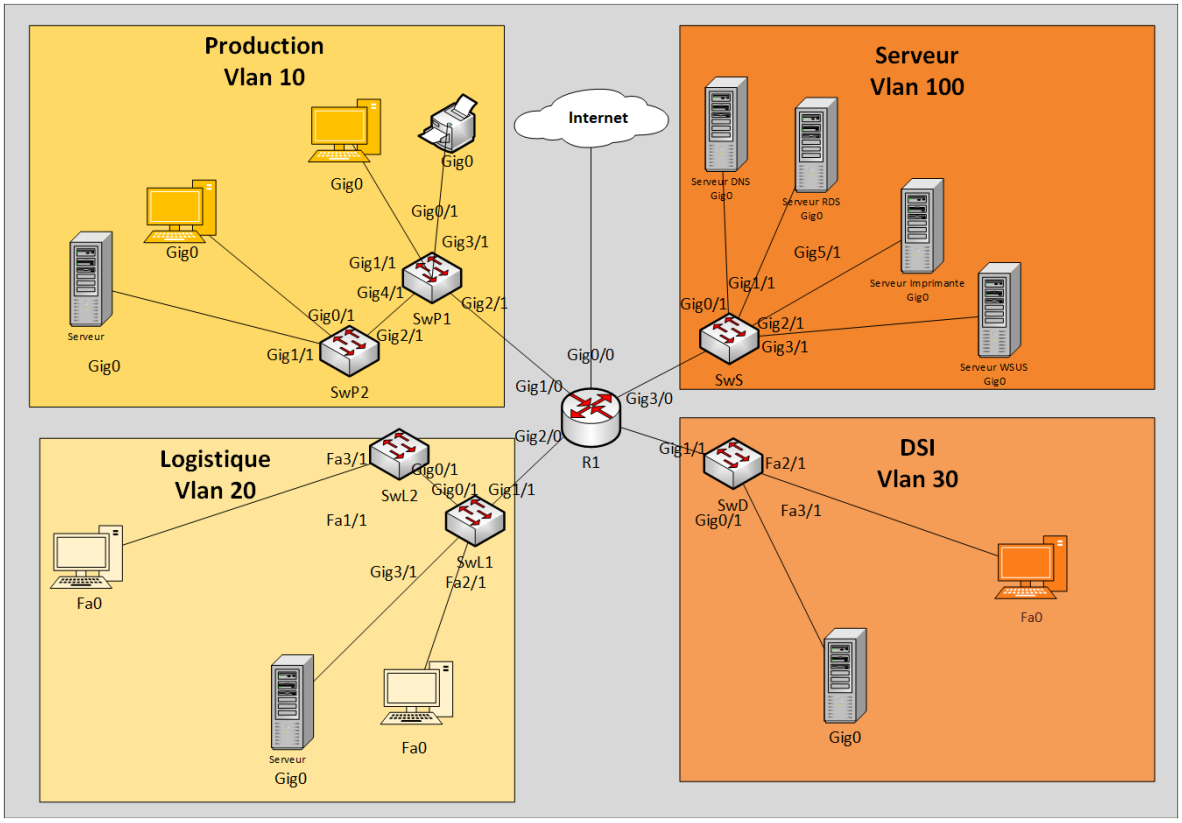
3.2 – Réseau du site de Rennes

3.2.1 – Structure physique

Description du nouvel agencement des services

Le réseau du site de Rennes sera centralisé au site de Brest. Le réseau interne de Rennes va disposer d'un routeur et de nombreux commutateurs avec un certains coût à prévoir, tel que 15 serveurs répartis sur les différents étages du site de Rennes (Production, Logistique, Serveur et DSI), 1 routeur, 6 commutateurs et plus de 100 utilisateurs, et donc de 100 postes pour le bon fonctionnement des salariés.

Concernant la salle des serveurs, ceux-ci seront répartis selon les différents services nécessaires. Parmi ces services, nous aurons besoin d'un Serveur DNS (Domain Name System) pour attribuer un nom de domaine plus adéquat à notre site internet, un serveur RDS (Remote Domain Services) pour avoir un accès à distance sur les postes de l'entreprise, puis un serveur WSUS (Windows Server Update Services) qui permettra d'alléger la bande passante de l'entreprise pour installer la dernière mise à jour Windows sur un serveur pour pouvoir la déployer localement sur tout le réseau, et enfin différents serveurs seront attribués sur chaque étage en guise de stockage de données.



Une architecture réseau reposant sur un routeur et des commutateurs

D'après le schéma physique, étant donné que nous avons plusieurs services différents et que ces derniers se trouvent répartis sur les étages du site de Rennes, il y aura donc un service attribué par étage, tel que la logistique, la production, les serveurs ou encore la DSI.

Au total, nous aurons besoin de plus d'une centaine de postes répartis dans chaque service de l'entreprise. Tout d'abord, l'architecture du réseau partira d'un routeur central qui sera lui-même connecté à chaque service de chaque étage et qui gérera tous les VLANs paramétrés sur chaque commutateur. Afin de gérer ces VLANs, le routeur central sera connecté sur tous les commutateurs de chaque service, qui finiront par se connecter sur tous les postes et serveurs des services correspondant.

Les commutateurs des services de production et de logistique seront tous deux en cascades pour ajouter d'avantages de ports dans ces deux réseaux qui en nécessitent, soit la production et la logistique.

Chaque commutateur de chaque étage aura les VLANs de paramétré pour les postes et les serveurs, puis le routeur aura des sous interfaces de paramétré de manière que le DHCP soit fonctionnel pour les VLANs.

Une architecture fonctionnelle grâce à des câbles blindés

Tout ce matériel devra donc être connecté et relié à l'aide de différents câbles en fonction des besoins.
Les câbles les plus performant utilisés dans cette architecture seront des câbles Gigabit Ethernet permettant une vitesse de 10Gb/s. Nous privilégierons une utilisation de ces câbles principalement pour les serveurs. Nous utiliserons également ces câbles entre les commutateurs et les routeurs afin de garantir une vitesse de connexion suffisante en cas d'utilisation intensive du réseau par de multiples postes. En effet, cette liaison doit être capable de faire transiter plusieurs connexions en même temps et donc avoir une bande passante maximale possible élevée afin de ne pas ralentir le réseau en servant de goulot d'étranglement.

Nous utiliserons également des câbles Fast Ethernet pour le reste du réseau avec une vitesse maximale de 1000 Mb/s soit 1Gb/s. Cela sera suffisant pour connecter la plupart des postes de travail aux commutateurs en garantissant une connexion rapide qui permettra à tous les employés d'avoir un flux de travail non impacté par le réseau.
Pour les câbles se trouvant notamment dans le VLAN 100 des Serveurs et les câbles Gigabit Ethernet en général qui nécessitent un débit très rapide et une grande stabilité, nous

privilégierons la norme STP, qui bénéficie d'un blindage au niveau des paires torsadées que les câbles FTP n'ont pas. Ce blindage au niveau de toutes les paires garantira une bonne isolation du câble aux interférences extérieures afin de garantir un réseau stable et protégé de toute corruption des données qui pourrait survenir lorsque les ondes produites par certains câbles pourraient modifier les données contenues dans le câble en cuivre. L'électricité étant en effet sujette à l'interférence électromagnétique.
Les câbles FTP blindés uniquement au niveau de la gaine seront utilisés dans un souci d'économie car bien que moins protégé, ils ne poseront pas de problèmes à la plupart des activités pour lesquelles on les réservera et ne devraient pas subir d'interférences car ils restent blindés néanmoins.
L'utilisation de ces câbles FTP sera alors réservée principalement pour connecter les postes des utilisateurs aux différents commutateurs.
Les câbles que nous possédons déjà seront suffisants afin de couvrir les 5700 mètres nécessaires pour le réseau.

Des serveurs et des postes

Le fonctionnement du réseau va alors reposer sur les multiples serveurs au sein du site de Rennes. En ce qui concerne les logiciels utilisés par les nombreux postes, la centralisation grâce aux serveurs sera possible par un serveur RDS et un serveur WSUS.

Les mises à jour étant une composante majeure de la sécurité de l'entreprise, nous nous devons d'installer un serveur WSUS. Cela permettra de s'assurer que tous les postes possèdent les mises à jour de sécurités les plus récentes en ayant permis à chaque poste de télécharger la mise à jour sur le réseau interne de l'entreprise, car seul le serveur aura téléchargé la mise à jour afin de préserver la bande passante. Le serveur WSUS devra donc être connecté au réseau internet pour pouvoir télécharger les données de mises à jour, il devra aussi être connecté au réseau de l'entreprise afin de pouvoir permettre la transmission des données à tous les postes de l'entreprise de Rennes.

Le serveur DNS ou Domain Name Server en Anglais permettra donc de renvoyer à l'utilisateur les données du site recherché, soit dans notre cas de rendre accessible depuis l'extérieur (en dehors du réseau interne de l'entreprise) le site web du site de Rennes. Le serveur DNS doit donc être connecté aux postes sur le réseau interne et doit également être connecté à internet pour pouvoir communiquer vers l'extérieur afin de récupérer les données nécessaires à son rôle de DNS.

Le serveur Active Directory aura pour but principal la sécurité du réseau en gérant les accès et les droits de tous les utilisateurs du site de Rennes sans exceptions. Elle doit alors contenir les informations sur les utilisateurs du réseau ainsi que leurs droits et autorisations afin que lors de l'authentification, elle puisse donner les accès nécessaires aux employés de Rennes. Installé sur un serveur Windows contrôleur de domaine, le serveur AD utilisera le protocole LDAP permettant de modifier l'Active Directory.

Le serveur RDS aussi appelé “Services de bureau à distance” permettra de garantir une standardisation des logiciels et des mises à jour de ces mêmes logiciels, par un seul serveur afin de garantir une uniformisation sur tous les services que l’on peut retrouver dans le site de Rennes. L’installation de ce serveur sera partagée avec Active directory, car l’AD est nécessaire pour l’installation du RDS et fonctionnera uniquement sur le réseau local du site de Rennes. Ce serveur physique combinant l’Active Directory et le RDS devra donc être connecté au réseau interne de l’entreprise.

Le serveur imprimante sera nécessaire afin de connecter les imprimantes des services de Rubik’s Cube à Rennes à tous les postes de l’entreprise. Il devra donc être connecté au réseau interne de l’entreprise et aux imprimantes.

Ces différents serveurs seront localisés dans la ferme des serveurs du site de Rennes, ensemble afin d’en faciliter la gestion et le suivi. Ils seront donc connectés au Commutateur de la salle serveur qui sera ensuite connecté aux routeurs. Le commutateur permettra l’existence du VLAN 100. Cette connexion des serveurs aux commutateurs se fera en Gigabit-ethernet 10 gigabits par secondes afin de garantir la vitesse la plus rapide possible car ces serveurs sont nécessaires à l’activité de l’entreprise et seront utilisés et sollicités potentiellement par tout le site de Rennes, que ce soit le service de logistique, le service de production ou bien la DSI. Le commutateur de la salle des serveurs sera donc lui aussi connecté en Gigabit-ethernet afin de maintenir le très haut débit. Les serveurs seront donc connectés sur leur port Gigabit-ethernet 0/0 respectivement.

Pour ce qui est des postes, ils seront utilisés par les employés et connectés aux différents serveurs nécessaires pour le fonctionnement des postes. Ces serveurs nécessaires à tous les postes seront les serveurs RDS, WSUS et Active Directory. Les autres serveurs de stockage ou à utilisation spécifique comme téléphonique et imprimante ne seront connectés qu’aux postes nécessaires ayant besoin d’y accéder pour leurs activités.
Le service qui nécessitera la plus grande bande passante est le service de Production, le VLAN 10 de production sera donc entièrement connectée en Gigabit-ethernet pour permettre une bande passante de 10 Gb/secondes. Les postes du service production auront donc une carte réseau avec un port Gigabit-ethernet 0/0 relié directement aux commutateurs. Tous les autres postes du site de Rennes seront cependant connectés en Fast Ethernet, sur leurs interfaces Fa0/0.

Les équipements utilisés par l’architecture

Le routeur sera centralisé et exclusivement en Gigabit-ethernet dû aux nombreuses connexions qu’il devra gérer. Il aura besoin d’un débit performant pour gérer les différentes interfaces la ou les différents commutateurs y seront connectés, du port Gig 1/0 à 5/0. Le routeur sera connecté à internet sur le port Gig0/0.

L'étage Production sera entièrement connecté en Gigabit-ethernet car comme mentionné précédemment, les employés en production nécessiteront d'une bande passante très rapide pour ne pas être ralentis dans leur travail. La production comportera deux commutateurs en cascades dans une baie de brassage, cascade nécessaire pour répondre au nombre de postes élevé. Le commutateur connecté directement au routeur par son port Gig2/1 aura une connexion au deuxième commutateur du port Gig4/1 à Gig2/1. Le serveur de stockage du service de production sera branché sur le port Gig1/1 du deuxième switch connecté en cascade. Avec plus de 100 postes dans ce service, nous répartirons les 100 connexions entre les deux commutateurs utilisant donc tous les ports un par un soit de 0 à 48 pour chaque.

L'étage Logistique comportera également la même configuration de commutateurs en cascade, connecté en Fast Ethernet vers des postes en Fast Ethernet. La configuration sera similaire, sauf pour le serveur qui lui sera en Gigabit-ethernet puisque sollicité par plusieurs postes en même temps et nécessitant alors un débit performant. Le commutateur connecté au routeur sera sur l'interface Gig 1/1, il sera en cascade avec son commutateur voisin en Gig 0/1 vers Gig 0/1. Le serveur de stockage de cet étage sera connecté en Gig 3/1 sur le commutateur. Pour ce qui est des 80 postes que l'on aura dans ce service, il nous faudra utiliser la totalité des ports du premier commutateur, soit les 48 ports en fast Ethernet. Le deuxième commutateur verra donc ses ports 0 à 33 d'utilisé, laissant une marge pour connecter de nouveaux appareils.

L'étage DSI verra son commutateur connecté sur le port Gig1/1 depuis le routeur. La connexion de ce service se fera en Fast Ethernet à l'exception du serveur de stockage DSI qui sera en Gigabit-ethernet également connecté à l'interface 0/1 du commutateur. Les 15 postes seront donc connectés sur le commutateur en fast Ethernet sur les interfaces Fa1/1 à Fa15/1.

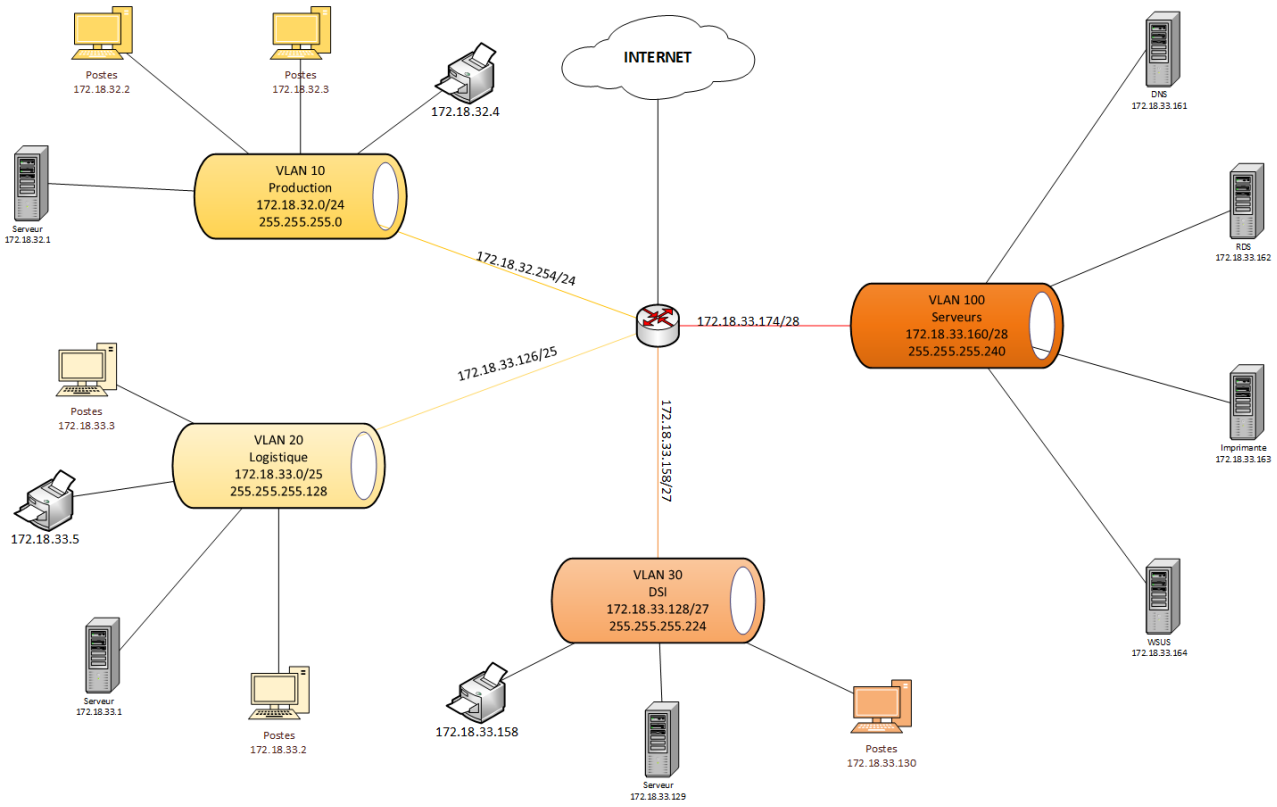
L'étage Serveur aura un commutateur unique pour relier les différentes machines qui seront également connectés en Gigabit-ethernet, puisqu'ils nécessiteront un besoin de bande passante importante car ils seront régulièrement sollicités. Le commutateur sera relié au routeur par son interface5/1. Les serveurs seront connectés sur le commutateur sur les interfaces Gig 0/1, 1/1, 2/1, 3/1 et 4/1.

Les câbles utilisés sur le site de Rennes seront standardisés pour toute l'entreprise Rubik's Cube, nous utiliserons alors 250 câbles RJ45 20m, 250 câbles RJ45 3m, et enfin des câble RJ45 50cm au nombre de 15. Le nombre élevé de ces câbles est justifié par la surface importante du site nécessitant environ 5700m comme mentionné auparavant.

3.2.2 – Structure logique

Présentation de l'architecture logique

L'architecture logique du réseau représentée sous forme de schéma.



Utilisation de masque de longueur variable

Afin d'avoir une optimisation maximale de l'utilisation des adresses IP. Nous opterons pour un réseau avec un masque sous VLSM (Variable Length Subnet Mask). En effet, nous avons adapté chaque masque pour chaque sous-réseau existant pour éviter le gaspillage d'adresse IP, et d'attribuer une plage d'adresse IP conforme aux nombres de machines dans le sous-réseau. Ainsi nous avons utilisés des masques longs ou des masques courts suivant le nombre de machines dans le sous-réseau.

L'étage Production sera composé 100 machines (postes et serveurs), sur l'adresse IP réseau 172.18.32.0/24. Comme dit précédemment nous avons dû traduire le 3ème octet pour convertir le masque /19 en /24 en ajoutant 5 bits à l'adresse IP
(172.18.001|0 0000.0000 0000/19 -> 172.18.0010 0000|.0000 0000 /24)

L'étage Logistique sera également composé de 100 machines (postes et serveurs également), son adresse IP réseau sera en 172.18.33.0/25 nous avons donc dû traduire le 3ème et 4ème octet pour convertir le masque /19 en /25 en ajoutant 6 bits à l'adresse IP réseau et ainsi adapter la plage IP réseau.
(172.18.001|0 0000.0000 0000/19 -> 172.18.0010 0001.0|000 0000 /25)

Pour le DSI 16 machines sont attribuées à ce réseau (15 postes + 1 serveur), sur l'adresse IP réseau 172.18.33.128/27, pour l'adapter au nombre de machines active nous avons alors dû également traduire le 3ème octet pour convertir le masque /25 en /27 en ajoutant 2 bits à l'adresse IP
(172.18.0010 0001.0|000 0000 /25 -> 172.18.0010 0001.100|0 0000 /27)
Enfin pour l'étage des Serveurs nous avons également le même nombre de machine que l'étage DSI, cet étage sera sous l'adresse IP réseau 172.18.33.160/29. Pour ce dernier réseau, la même méthodologie a été appliqué qu'auparavant, pour adapter le masque à l'adresse réseau de cet étage.
(172.18.0010 0001.100|0 0000 /27 -> 172.18.0010 0001.1010|0000 /28)

Ainsi, nous avons optimisé le réseau pour l'adapter aux nombres de machines utilisées et éviter un gaspillage sur la plage d'IP.
Puis, avec cette disposition nous ajouterons un protocole DHCP (Dynamic Host Configuration Protocol) qui permettra avec la plage d'adresse optimisée avec le VLSM et les VLAN, d'attribuer automatiquement pour chaque poste, une adresse IP dynamique de manière à automatiser le processus.

Tableau du VLSM du site de Rennes :

Nom du Sous-Réseau	Adresse Réseau	Masque de Sous-Réseau	Première Adresse Hôte	Dernière Adresse Hôte	Adresse de Diffusion
Production	172.18.32.0	255.255.255.0	172.18. 32.1	172.18. 32.254	172.18. 32.255
Logistique	172.18.33.0	255.255.255.128	172.18. 33.1	172.18. 33.126	172.18. 33.127
DSI	172.18.33.128	255.255.255.224	172.18. 33.129	172.18. 33.158	172.18. 33.159
Serveurs	172.18.33.160	255.255.255.240	172.18. 33.161	172.18. 33.174	172.18. 33.175

Utilisation de Réseaux locaux virtuels

Afin de pouvoir attribuer une adresse IP à chaque poste et serveur possible nous mettrons en place des VLANs (Réseau local virtuel). Grâce aux VLANs nous pouvons séparer les adresses entre les salles et éviter qu'un utilisateur d'une salle ait accès à des données d'une autre salle, rendant l'intégralité du réseau déjà plus sécurisé qu'avant.

Nous utiliserons un total de 4 VLANs dans notre site, divisés par chaque salle. La salle de Production aura le VLAN 10 avec une adresse de réseau 172.18.32.0 avec un masque de 24 bits, la salle de Logistique aura le VLAN 20 avec une adresse de réseau 172.18.33.0 avec un masque de 25 bits, la salle de DSI aura le VLAN 30 avec une adresse de réseau 172.18.33.128 avec un masque de 27 bits, enfin, la salle des Serveurs aura le VLAN 100 avec une adresse de réseau 172.18.33.160 avec un masque de 28 bits.

Table de routage du routeur central du site de Rennes

	Type	@ Réseau	Masque réseau	@ Passerelle	@ Interface
Production	C	172.18.32.0	255.255.255.0	172.18. 32.254	172.18. 32.254
Logistique	C	172.18.33.0	255.255.255.128	172.18. 33.126	172.18. 33.126
DSI	C	172.18.33.128	255.255.255.224	172.18. 33.158	172.18. 33.158
Serveurs	C	172.18.33.160	255.255.255.240	172.18. 33.174	172.18. 33.174
Réseaux inter-sites	S	128.51.0.0	255.255.0.0	128.51.60.253	128.51.60.254
	S	128.52.0.0	255.255.0.0	128.51.60.253	128.51.60.254
	S	192.168.0.0	255.255.0.0	128.51.60.253	128.51.60.254

Adresses IP et ports des serveurs

Afin de savoir quel serveur utilise quel port et des adresses attribuées aux serveurs, nous illustrons ces chemins par un tableau regroupant les adresses IP des serveurs de chaque étage avec leurs protocoles et leurs ports. Initialement ce tableau sert à démontrer les connexions logiques de chaque serveur au routeur central.
Les différents ports pour les services utilisées sur le site :

Serveur :	Adresse IP :	Protocole :	Port :
DNS	172.18.33.161	UDP	53

RDS	172.18.33.162	TCP	8080
Imprimante	172.18.33.163	TCP	515 (LDP)
WSUS	172.18.33.164	TCP / UDP	443 (HTTPS)
WEB	192.168.1.1	TCP / UDP	80 (HTTP) / 443 (HTTPS)
DSI	172.18.33.129	TCP	20/21 (FTP)
Logistique	172.18.65.42	TCP	20/21 (FTP)
Production	172.18.32.1	TCP	20/21 (FTP)

Les différents ports pour les services utilisées sur le site

TCP et UDP sont deux protocoles de communication utilisés pour transférer des données sur un réseau en utilisant leur adresse IP et un numéro de port.
La différence entre ces deux protocoles réside dans leur mode de transmission : TCP est orienté connexion, ce qui signifie qu'il établit une connexion fiable entre l'émetteur et le récepteur avant d'envoyer les données, alors que UDP est non-connecté et envoie les paquets sans se soucier de leur réception, de leur ordre ou de leur erreur.
TCP garantit que les données sont transmises sans erreurs et dans l'ordre correct, tandis que UDP ne garantit pas ces aspects. TCP est plus sûr mais plus lent que UDP, qui est plus rapide mais moins fiable car prioritisant une faible latence sans connexion.

Le Serveur DHCP utiliserait le protocole DHCP (Dynamic Host Configuration Protocol) qui est utilisé pour attribuer automatiquement des adresses IP aux périphériques connectés à un réseau. Le serveur DHCP utilise les ports 67 et 68 en TCP pour communiquer avec les clients DHCP.

Pour le serveur FTP qui utilise le protocole FTP (File Transfer Protocol) pour transférer des fichiers sur un réseau, nous utiliserons le protocole SFTP (SSH File Transfer Protocol) qui est une extension sécurisée de FTP et utilise le protocole SSH pour chiffrer les transferts de fichiers. Le serveur FTP utilise le port 22 en TCP pour communiquer avec les clients FTP.

Ensuite le Serveur Imprimante utilise le protocole LDP (Line Printer Daemon) qui est utilisé pour imprimer des documents à partir d'un serveur d'impression. Le serveur d'impression utilise le port 515 en TCP pour communiquer avec les clients d'impression.
Le serveur Web utilise le protocole HTTP (Hypertext Transfer Protocol) qui est utilisé pour accéder à des pages Web sur Internet. Les serveurs Web utilisent le port 80 en TCP pour le protocole HTTP

Le serveur WSUS utilise le protocole HTTPS WSUS (Windows Server Update Services) qui sert à gérer les mises à jour de logiciels sur les ordinateurs Windows. Le serveur WSUS utilise le port 443 en TCP pour le protocole HTTPS en TCP pour communiquer avec les clients WSUS.

Le serveur Mail utilise le protocole SMTP (Simple Mail Transfer Protocol) pour envoyer des courriels sur un réseau. Le serveur de messagerie utilise le port 587 en TCP pour le protocole SMTP.

Puis le serveur RDS utilise le protocole RDP (Remote Desktop Protocol) pour accéder à distance à un ordinateur Windows. Le serveur RDS utilise le port 3389 en TCP pour le protocole RDP.

Enfin, le serveur Log utilise le protocole Syslog utilisé pour envoyer des messages de journalisation (logs) à un serveur de log. Le serveur de log utilise le port 514 en UDP pour le protocole Syslog.

Les règles du pare-feu

Pour améliorer la sécurité de tous les postes sur internet et entre eux, nous ajouterons un pare-feu (aussi appelé Firewall) pour filtrer les connexions entrantes et sortantes : nous ferons en sorte que les postes aient accès à internet avec une autorisation de données entrantes et sortantes du DNS sur le port 53. De plus nous laisserons une autorisation de données entrantes et sortantes sur le port 3389 pour donner accès à l'outil Windows Bureau à distance. Nous laisserons une autorisation de données sortantes vers le port 22 pour le transfert de données sécurisé grâce au protocole SFTP.
Ci-dessous, le tableau récapitulatif de nos règles de gestion du firewall :

Numéro	@ source	@ Destination	Port/Protocole	Action
1	*	172.18. 33.161/28	DNS :53	PASS
2	172.18. 33.161/28	*	DNS :53	PASS
3	*	172.18. 33.162/28	RDP :8080	PASS
4	*	172.18.33.160/28	SFTP :22	PASS
5	172.18. 33.129/27	172.18.33.128/27	DHCP :67/68	PASS
6	172.18. 33.1/25	172.18. 33.0/25	DHCP :67/68	PASS
7	172.18. 32.1/24	172.18. 32.0/24	DHCP :67/68	PASS
8	172.18.33.163/28	*	SFTP :515	PASS
9	172.18.33.164/28	*	HTTPS :443	PASS
10	172.18.33.162/28	*	RDP :8080	PASS
11	*	*	*	BLOCK

Nous commençons par laisser passer l'interaction entre n'importe quel appareil vers le serveur DNS (adresse 172.18.33.145/28) par le port 53, qui est le port réservé pour le DNS. De plus, cette même adresse a le droit d'envoyer ses informations à travers n'importe quelle IP par le firewall.
Nous laissons passer les informations venant de toute adresse IP allant à l'adresse IP 172.18.33.146/28 à travers le port 3389, soit le port du Bureau à distance.
Nous laissons également passer les informations venant de toute adresse IP allant à l'adresse IP 172.18.33.144/28 à travers le port 22, qui est le port pour le transfert de fichiers (SFTP).
Ensuite, nous laissons les adresses 172.18. 33.129/27 allant à 172.18.33.128/27 passant par le port 67 ou 68, qui est le port DHCP permettant l'adressage automatique des appareils.
Nous laissons les adresses 172.18. 33.1/25 en direction de 172.18.33.0/25 passant par le port 67 ou 68.
Enfin, nous laissons les adresses 172.18. 33.1/25 allant à 172.18.33.0/25 passant par le port 67 ou 68.
Ceci-dit, les ports 172.18.33.146/28 ; 172.18.33.147/28 ; 172.18.33.148/28 peuvent communiquer par le firewall à travers des ports 3389 pour le bureau a distance, le port 515 pour le transfert de fichiers et le port 443 pour l'accès à internet respectivement.

Toutes les adresses IP peuvent communiquer avec l'adresse IP 172.18.2.102.
Finalement toute autre IP en dehors des règles de gestion du firewall seront bloqués

3.2.3 – OS et logiciels

Systèmes d'exploitation

En tant que Systèmes d'exploitation, nous utiliserons majoritairement Windows sous sa version la plus récente, soit, Windows 11 Professionnel. Ce système d'exploitation sera implémenté dans les salles de production, de logistique et de DSI. Pour la salle des serveurs, chaque serveur aura sa propre version de leur système d'exploitation selon leurs fonctionnalités.
Du côté des serveurs, nous utiliserons un serveur Windows server 2022 uniquement pour l'Active Directory et un serveur WSUS. Pour le restant des serveurs, nous utiliserons Linux et plus spécifiquement, Alma Linux.

Logiciels utilisés

La suite principale qui nous sera le plus utile est la suite Microsoft 365 E3 contenant un grand nombre d'applications et services variés. Dans notre cas, celle-ci nous propose les applications de base telles que Powerpoint, Word, Excel, OneNote, Publisher qui est un logiciel qui permettra de créer des documents tels que des brochures, des cartes de visite, des calendriers, des étiquettes, des cartes de vœux entre autres (disponible uniquement sur PC) et Access qui est un logiciel qui permettra de créer et de modifier des bases de données (disponible uniquement sur PC également).
La suite contient aussi un service de messagerie professionnelle Outlook doté d'un serveur mail appelé Exchange et d'un logiciel appelé Bookings qui nous permettra de prendre rendez-vous avec certaines personnes de l'entreprise de façon en ligne, synchronisée et en temps réel.
Pour ce qui est des visioconférences ou d'une messagerie instantanée, la suite a également un accès complet à la version professionnelle de Teams.
Concernant les réseaux sociaux, nous aurons accès au service SharePoint, une plateforme de partage de fichiers qui permettra aux équipes de travailler ensemble plus efficacement.
Par ailleurs, Yammer inclus dans cette suite, est un réseau social d'entreprise qui connecte des leaders, des communicateurs et des employés pour créer des communautés, partager des connaissances et faire participer tout le monde.
En outre, ayant accès à Viva Connections à travers Teams, Viva connections est une solution de communication pour les employés qui regroupe les informations, les conversations et les ressources sur les applications et appareils que vous utilisez quotidiennement. De même Viva Engage, inclus dans la suite et construit dans Teams, est une nouvelle expérience d'employé qui

connecte les personnes au sein de l'entreprise, où qu'elles travaillent et quand elles travaillent, afin que tout le monde se sente inclus et engagé.
En outre, nous aurons également un accès au service OneDrive, un service qui nous permettra de stocker des données sur le cloud et de pouvoir y accéder depuis n'importe quel appareil.
Nous aurons accès au logiciel Stream qui nous servira de service vidéo qui permettra aux membres de l'organisation de créer, stocker, partager et afficher des vidéos en toute sécurité.
Grâce à l'application Sway, il nous sera possible de créer et de partager facilement des rapports interactifs, des récits personnels, des présentations et toutes sortes d'autres contenus.
Par ailleurs, la plateforme Lists est une plateforme centralisée et permettra d'afficher et de gérer toutes nos listes individuelles et de groupe. Elles seront retrouvables lorsqu'elles seront partagées directement et celles qui nous seront communiquées par un groupe Teams.
Nous aurons accès à l'application Forms qui servira pour la création d'enquêtes de questionnaires et des sondages, ceux-ci accessibles à partir d'un smartphone, à partir du web ou à partir d'un ordinateur sachant que l'application est directement intégrée dans le logiciel Teams.
Par ailleurs, nous aurons accès au logiciel Visio qui nous permettra de faire des schémas professionnels avec un accès à un très grand nombre de formes pré-dessinées.
Concernant une meilleure gestion de travail, la suite nous donnera accès à différents outils tels que Microsoft planner qui nous servira de gestionnaire de tâches personnel ou même gestionnaire de tâches pour une équipe entière.
En outre nous aurons accès à Power automate qui est un service basé sur le cloud permettant aux employés de créer des environnements afin d'automatiser des tâches routinières et répétitives. De plus, l'accès à Power Virtual Agents nous permettra d'utiliser des intelligences artificielles proposées par Microsoft pour améliorer la qualité et l'efficacité du travail de chaque employé.
Nous aurons un accès à Microsoft To Do, une application directement intégrée à Teams, qui est une autre application nous permettant un suivi de près des tâches à effectuer tout en étant accessible sur tout appareil sachant que ces données sont stockées sur le cloud.
Pour une analyse du bien-être de chaque utilisateur, un service Viva Insights est fourni avec la suite et permettra, en tant qu'application intégrée dans Teams, de favoriser le bien-être des employés grâce à des informations et des recommandations axées sur les données reçues.
Concernant la gestion des identités et des accès, grâce à la suite nous aurons les services Windows Hello pour la numérisation de données telles que la reconnaissance faciale ou l'empreinte digitale si l'appareil en question le supporte, Microsoft Credential Guard qui est une fonctionnalité de sécurité pour protéger les données contre le piratage et pour bloquer certaines attaques de piratage.
La suite propose également le plan Premium 1 d'Azure Active Directory qui est un plan proposant un Active Directory simple avec une authentification multi facteur dans le cadre de certains scénarios.
Nous utiliserons une deuxième suite qui sera plutôt dirigée pour le côté logistique et production du site. Cette suite est la suite Oracle NetSuite qui comprend au moins deux logiciels qui nous intéresse. Sachant que ces suites ont un prix sur demande nous supposerons l'achat de la suite complète dans les prix. Sachant ceci, le logiciel le plus important sera NetSuite Warehouse Management System (WMS) qui est un système de gestion d'entrepôt qui optimise les opérations quotidiennes de l'entrepôt. Celle-ci utilise des pratiques de pointe telles que la numérisation des codes-barres mobiles RF (Radio Frequency) ainsi que des stratégies définies

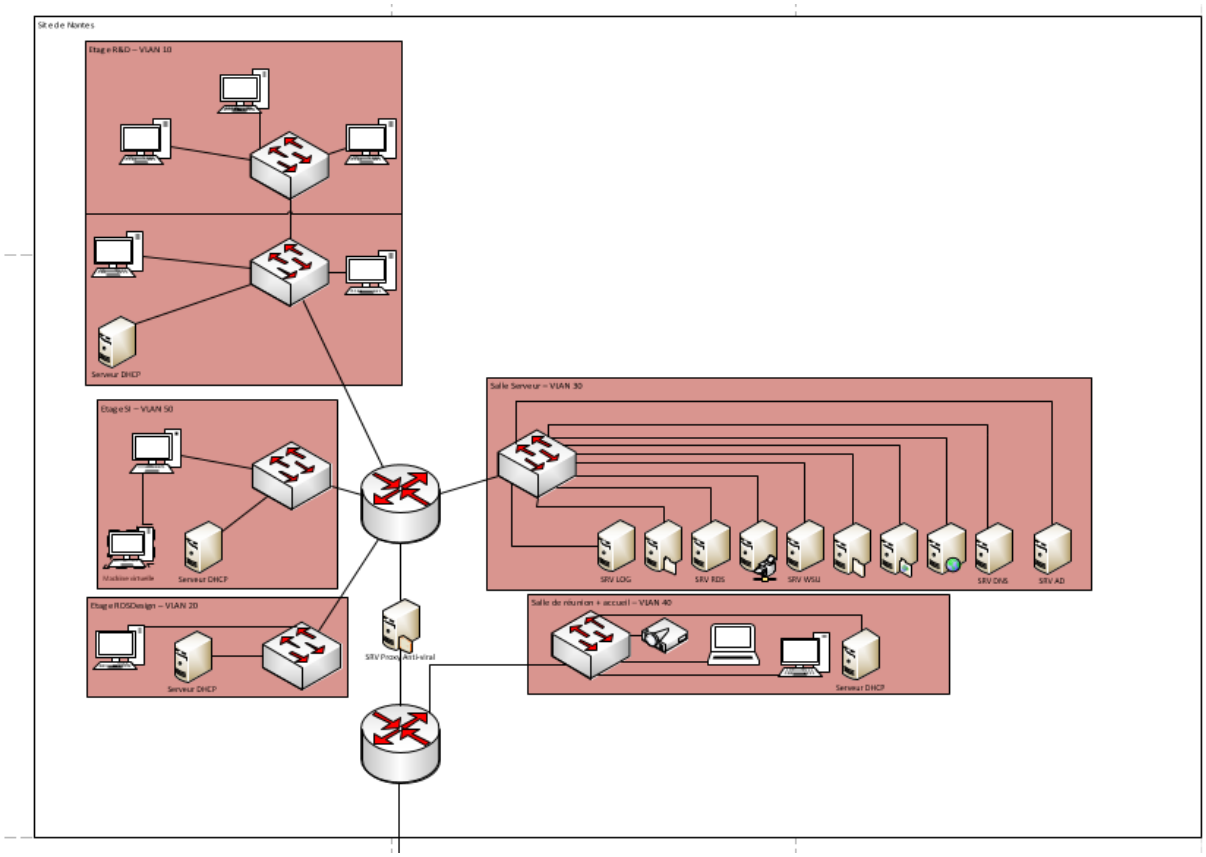
pour le stockage, la collecte, la gestion des tâches, les autorisations de retour et les plans de comptage cyclique.
NetSuite Warehouse Management System (WMS) est un système de gestion d'entrepôt qui optimise les opérations quotidiennes de l'entrepôt en utilisant des pratiques de pointe telles que la numérisation de codes-barres mobiles RF, des stratégies définies pour le stockage et la cueillette, la gestion des tâches, les autorisations de retour et les plans de comptage cyclique.

La suite contient plusieurs autres applications mais nous n'entrerons pas plus en détail sachant que l'achat est fait sur demandes et que le prix varie par rapport au nombre de logiciels et services qui nous seront nécessaires.

3.3 – Réseau du site de Nantes

3.3.1 – Structure physique

Le nouveau réseau de Nantes se présentera sous la forme suivante :



Le point de sortie du réseau est le routeur bordure qui est connecté au VLAN 40 nommé "Réunion accueil". Ce VLAN est équipé d'un serveur DHCP et peut accueillir 30 postes de travail. Le routeur bordure est également connecté à un serveur Proxy Anti-viral, qui est en mesure de protéger l'ensemble du réseau contre les virus et autres menaces malveillantes. Ce serveur est connecté à un routeur central qui se sépare ensuite en quatre autres VLANs. Le premier est le VLAN 10 nommé "R&D", qui dispose également d'un serveur DHCP et peut accueillir 254 postes de travail.
Le deuxième VLAN est le VLAN 20 nommé "STEDesign", qui dispose également d'un serveur DHCP et peut accueillir 30 postes de travail.
Le troisième VLAN est le VLAN 30 nommé "salle serveurs", qui est connecté à plusieurs serveurs tels qu'un serveur d'impression, un serveur FTP, un serveur de logs, deux serveurs NAS, un serveur ADDS, un serveur RDS, un serveur WSU, un serveur DNS et un serveur web. Ce VLAN est destiné à l'hébergement des serveurs de l'entreprise.
Le quatrième VLAN est le VLAN 50 nommé "SI", qui dispose également d'un serveur DHCP et peut accueillir 14 postes de travail. Ce VLAN est destiné au service informatique de l'entreprise.

Dans cette infrastructure, un routeur de bordure a été mis en place. C'est un élément crucial dans la sécurité et la gestion du trafic réseau pour l'entreprise. Il permet de connecter le réseau local de l'entreprise à Internet et de filtrer les accès non autorisés à l'infrastructure locale.
Ce routeur est essentiel du fait de plusieurs caractéristiques.
Sécurité du réseau ; En effet le routeur de bordure est utilisé comme la première ligne de défense pour protéger le réseau de l'entreprise contre les cyberattaques et les menaces en provenance d'Internet. Le routeur de bordure sera configuré pour bloquer les tentatives d'intrusion, les attaques de déni de service, les virus et autres malwares.
Gestion de la bande passante ; Le routeur de bordure sera utilisé pour gérer le trafic réseau en optimisant la bande passante disponible et en limitant l'accès à certaines applications ou sites web. Cela permet de garantir une utilisation efficace de la bande passante et d'éviter les ralentissements ou les congestions du réseau.
Accès à Internet ; Le routeur de bordure permettra également de connecter l'ensemble du réseau local de l'entreprise à Internet, offrant ainsi un accès rapide et fiable aux ressources en ligne.
Sécurité des données ; Le routeur de bordure permettra de protéger les données de l'entreprise en filtrant les accès non autorisés à l'infrastructure locale. Cela peut inclure la mise en place de pare-feu, de VPN et d'autres mécanismes de sécurité pour garantir la confidentialité et l'intégrité des données.

Routeur et commutateurs

Ayant de nombreux services à répartir sur plusieurs étages, le réseau du site de Nantes se basera sur une topologie en étoile et une architecture client-serveur. Cela signifie qu'il disposera de commutateurs reliés directement au routeur principal afin de créer un sous réseau par étage (cf. description logique ci-dessous). Cette organisation apporte plusieurs avantages. Dans un premier temps, une logique et organisation du réseau qui nous paraît optimale, celle-ci permettra une gestion de la part du service DSI efficace, étant donné la connaissance accrue du réseau. D'autre part, le sectionnement du réseau, entraine par la même occasion une couche de sécurité supplémentaire, qui aujourd'hui, est nécessaire sur le site de Nantes recueillant une grosse partie des données sensibles de l'entreprise.
Ainsi, au rez-de-chaussée, se situera le routeur auquel seront reliés des commutateurs. Au premier étage, se trouvera un commutateur pour le service DSI et un commutateur pour la salle des serveurs ; aux deuxièmes et troisièmes étages, sera installé une baie de brassage qui devra supporter 250 hôtes au minimum, c'est-à-dire qu'il faudra mettre en place 2 à 3 commutateurs en cascade afin de connecter tous les hôtes au réseau ; enfin, un commutateur au rez-de-chaussée pour l'accueil et la salle de réunion et un commutateur pour le service STEDesign seront installés.

Serveurs

Le réseau de l'entreprise et du site ne fonctionnera pas sans des serveurs essentiels. C'est pourquoi une salle des serveurs a été prévue au sein du site de Nantes. Cette salle sera composée

de serveurs DNS, proxy, FTP, TSE, NAS, de gestion de logs, téléphonique, imprimante, Web, WSUS et AD.

Le serveur DNS (Domain Name System) qui sera utilisé servira à faire la liaison entre le nom de domaine du site internet et l'adresse IP de ce même site internet contenue dans le serveur WEB, que nous expliquerons plus loin.

Le serveur proxy antiviral utilisé servira à filtrer les connexions entre les deux routeurs de l'entreprise, afin de détecter tout type de trafic anormal. Il assurera donc la sécurité des connexions entrantes et sortantes du site de Nantes.

Le serveur FTP (File Transfer Protocol) permettra de faciliter l'échange de données et de commandes entre les logiciels et les ordinateurs. Les employés pourront ainsi se transférer des documents via le réseau, selon leurs autorisations.

Le serveur TSE (Terminal Server Edition) utilisé permettra à plusieurs utilisateurs de se connecter au serveur à l'aide de clients ou de périphériques distants.

Les serveurs NAS qui seront installés serviront au stockage des fichiers de l'entreprise. Ainsi, il y aura un accès distant à ces serveurs de stockage rendu possible afin de récupérer son travail en toute sécurité. Ces serveurs NAS agiront aussi comme serveur de sauvegarde pour un RAID 50.

Le serveur de gestion de logs qui sera utilisé servira à recueillir la plupart des actions réalisées sur le réseau. Il sera donc facile de retracer une ouverture de connexion, une mise à jour, ou des transferts. Ce serveur permettra notamment en cas de problème lié à une cyber attaque, de fournir une preuve pour les autorités, et de garder une trace des actions réalisées lors de cette attaque pour permettre de remonter jusqu'à l'attaquant.

Le serveur téléphonique qui sera installé permettra aux employés de communiquer entre eux sans nécessiter un quelconque forfait mobile. Ils pourront donc appeler les services en interne via des numéros à 2 chiffres assignés à chaque bureau.

Le serveur imprimante permettra aux employés d'imprimer des documents depuis leur poste tout en gérant les différentes requêtes afin que le trafic ne soit pas encombré si de nombreuses demandes d'impressions venaient à arriver en même temps. Cela évitera donc des problèmes au niveau de l'imprimante, et les éventuels problèmes de mélanges de photocopies qui peuvent survenir parfois.

Le serveur WEB qui sera utilisé servira à stocker les fichiers du site internet sur le réseau, accessible via une adresse IP. Le DNS fera ensuite le transfert entre cette adresse IP et le nom de domaine.

Le serveur WSUS (Windows Server Update Services) sera utilisé à des fins de gestion de mise à jour. Sans avoir à faire les mises à jour en local sur chaque poste, il sera possible de mettre à jour l'ensemble du SI via ce serveur. Par conséquent, cela rajoute une couche de sécurité en plus au niveau du réseau car les mises à jour seront centralisées.

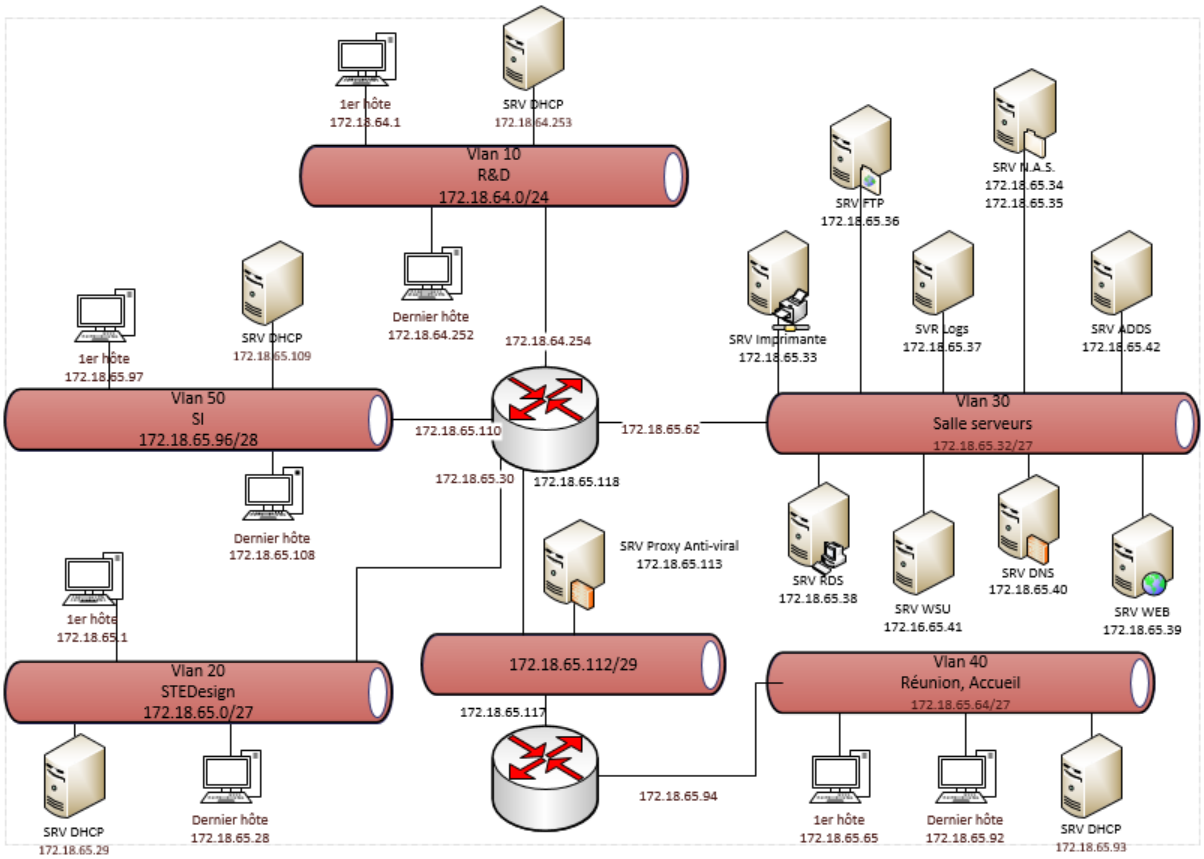
Le serveur AD qui sera utilisé servira pour gérer les autorisations de session utilisateurs ainsi que les accès aux ressources des employés en fonction de leurs statuts et besoins. Ce serveur jouera un rôle extrêmement important dans la sécurité de l'entreprise car il associe à chaque employé une session avec les autorisations nécessaires.

Câbles utilisés

Avec tous ces serveurs, le trafic sera très vite encombré puisque beaucoup de requêtes seront envoyées en direction des serveurs, de la même manière que les serveurs enverront eux aussi des requêtes vers les autres hôtes. Il est donc important d'avoir une bonne gestion des câbles, et de choisir pour chaque câble les caractéristiques nécessaires. Ainsi, des câbles Gigabit Ethernet supportant un trafic d'une vitesse de 1 Gb/s pour les liaisons entre les routeurs et les commutateurs seront utilisés. De la même manière, pour relier les différents hôtes entre eux, des câbles Fast Ethernet avec une vitesse de 100 Mb/s seront choisis. Le blindage des câbles inter hôtes sera du UTP car n'y aura pas besoin de plus pour ce type de liaisons. En revanche, pour les liaisons vers les commutateurs et vers les routeurs, il faudra privilégier des câbles de type SSTP car les données ne doivent pas être altérées, et doivent arriver à destination en toute sécurité le plus rapidement possible.

3.3.2 – Structure logique

Au niveau logique, le nouveau réseau de Nantes sera sous la forme suivante :



VLANs

Selon le principe de l'architecture client-serveur, il est nécessaire de créer des VLANs. Il sera donc créé un réseau par étage afin de faciliter son administration et de renforcer sa sécurité, en permettant toutefois aux différents postes de communiquer entre eux, quel que soit son emplacement.
Le réseau sera donc réparti en 5 VLANs : le VLAN 10 pour le service R&D, le VLAN 20 pour le service STEDesign, le VLAN 30 pour la salle des serveurs, le VLAN 40 pour la salle de réunion et l'accueil, et le VLAN 50 pour le DSI.
Selon cette répartition, chaque hôte appartenant à un VLAN pourra désormais être connecté en toute sécurité sur le réseau, sans toutefois pouvoir accéder aux informations contenues sur les hôtes des autres VLANs. De plus, la partition du réseau en VLAN facilite la gestion et l'organisation du réseau, rendant plus facile à isoler une partie du réseau afin d'intervenir dans des temps plus réduits.

VLSM

Pour répartir ces VLANs de la manière la plus sécurisée possible, la méthode « Variable Length Subnet Mask » (VLSM, Masque de sous-réseau à taille variable) a été choisie. En effet, cette méthode découpe le réseau en laissant le moins de « vide» possibles, c'est une optimisation de la distribution des adresses IP, c'est-à-dire qu'en changeant la taille du masque, nous laisserons beaucoup moins d'adresses IP non utilisées (et donc vulnérables) par rapport à un FLSM (« Fixed Length Subnet Mask », Masque de sous-réseau à taille fixe).
Avec cette disposition, des serveurs DHCP reliés à chaque commutateur seront ajoutés afin de répartir les adresse IP équitablement entre chaque poste. En effet, un serveur DHCP, étant paramétré pour donner des adresses IP selon le réseau donné, permet de répartir les adresse IP du réseau concerné et ainsi d'éviter les écrasements d'IP ou les confusions. Cela sécurise donc d'avantage le réseau.
Ainsi, selon le VLSM, les adresse IP seront réparties avec un masque approprié pour chaque VLAN en fonction du nombre d'hôtes. Le VLAN 10 aura alors un réseau en 172.18.64.0 avec un masque de 24 bits, le VLAN 20 aura un réseau en 172.18.65.0 avec un masque de 27 bits, le VLAN 30 aura un réseau en 172.18.65.32 avec un masque de 27 bits, le VLAN 40 aura un réseau en 172.18.65.64 avec un masque de 27 bits, et le VLAN 50 aura un réseau en 172.18.65.96 avec un masque de 28 bits.

Sous-réseau	@Réseau	Masque	Nb IP réservées	1ère IP valide	@Passerelle	@Broadcast
Vlan 10 : R&D	172.18.64.0	255.255.255.0	254	172.18.64.1	172.18.64.254	172.18.64.255
Vlan 20 : Design	172.18.65.0	255.255.255.224	32	172.18.65.1	172.18.65.30	172.18.65.31
Vlan 30 : Serveur	172.18.65.32	255.255.255.224	32	172.18.65.33	172.18.65.62	172.18.65.63
Vlan 40 : Réunion	172.18.65.64	255.255.255.224	32	172.18.65.65	172.18.65.94	172.18.65.95
Vlan 50 : SI	172.18.65.96	255.255.255.240	16	172.18.65.97	172.18.65.110	172.18.65.111

Adresses IP et ports des serveurs

Afin de faciliter la communication avec les différents serveurs nécessaire au bon fonctionnement du site, il a été choisi de leur donner une adresse IP fixe. En effet, si leurs adresses IPs ne change pas, les éventuels problèmes liés aux services des serveurs n'arriveront que si le réseau entier ne fonctionne plus. Voici un tableau des serveurs avec leurs assignements d'adresse IP ainsi que le protocole utilisé joint à leur port respectif.

Serveur :	Adresse IP :	Protocole :	Port :
DNS	172.18.65.40	UDP	53
Proxy	172.18.65.43		8080
TCP	172.18.65.36	TCP	22 (SFTP)
TSE	172.18.65.38	TCP	3389 (RDP)
NAS	172.18.65.34 / 172.18.65.35	FTP	10021
Log	172.18.65.36	UDP	516 (SYSLOG)
Téléphonique	172.18.65.42		
Imprimante	172.18.65.33	TCP	515 (LDP)
WEB	172.18.65.39	TCP	80 (HTTP) / 443 (HTTPS)
WSUS	172.18.65.41	TCP	443 (HTTPS)
AD	172.18.65.42	LDAP	636 (TCP)

Pare-feu

Enfin, pour avoir une sécurisation du réseau optimale, un pare-feu sera mis en place. Il permettra de filtrer le trafic entrant et sortant. Nous ferons en sorte que les postes aient accès à internet, mais uniquement sur des connexions sécurisées, donc en HTTPS, nous autoriserons également le transfert de données, les connexions de bureau à distance ainsi que les données entrantes et sortantes du DNS. Pour cela, nous autoriserons les connexions sur les ports 443 (HTTPS), 3389 (bureau à distance), 43 (DNS) et 22 (SFTP pour le transfert de données). Les règles principales du firewall, définissant ainsi les connexions autorisées entre les hôtes eux-mêmes ou avec l'extérieur du réseau, la configuration des firewalls ainsi que leur automatisation sera confié à un sous-traitant.

Numéro	**Plage IP d'origine**	**Protocole : Ports**	**Plage IP Destination**	**Action**
1	*	LPD : 515	172.18.65.33/27	ALLOW
2	*	HTTPS : 443	172.18.65.41/27	ALLOW
3	*	HTTP : 80	172.18.65.39/27	ALLOW

4	*	DNS : 53	172.18.65.40/27	ALLOW
5	*	RDP : 3389	172.18.65.38/27	ALLOW
6	*	SYSLOG : 514	172.18.65.37/27	ALLOW
7	172.18.64.1/24 à 172.18.64.252/24	SFTP : 22	172.18.65.36/27	ALLOW
8	172.18.64.1/24 à 172.18.64.252/24	SMB : 445	172.18.65.34/27	ALLOW
9	172.18.64.1/24 à 172.18.64.252/24	SMB : 445	172.18.65.35/27	ALLOW
10	172.18.65.1/27 à 172.18.65.28/27	SFTP : 22	172.18.65.36/27	ALLOW
11	172.18.65.1/27 à 172.18.65.28/27	SMB : 445	172.18.65.34/27	ALLOW
12	172.18.65.1/27 à 172.18.65.28/27	SMB : 445	172.18.65.35/27	ALLOW
13	172.18.65.97/28 à 172.18.65.108/28	SFTP : 22	172.18.65.36/27	ALLOW
14	172.18.65.97/28 à 172.18.65.108/28	SMB : 445	172.18.65.34/27	ALLOW
15	172.18.65.97/28 à 172.18.65.108/28	SMB : 445	172.18.65.35/27	ALLOW
16	172.18.65.40/27	DNS : 53	*	ALLOW
17	172.18.65.39/27	HTTP : 80	*	ALLOW
18	172.18.65.37/27	SYSLOG : 514	*	ALLOW
19	172.18.65.37/27	SYSLOG : 514	*	ALLOW

20	172.18.65.65/27 à 172.18.65.92/27	SFTP : 22	172.18.2.90	ALLOW
21	172.18.65.65/27 à 172.18.65.92/27	HTTP : 80	172.18.2.102	ALLOW
22	*	*	*	DENY

3.3.3 – OS et logiciels

Service STEDesign

Pour répondre aux besoins des employés du service STEDesign, nous aurons besoin de plusieurs logiciels et donc de souscrire à de nombreuses licences. C'est pourquoi il est important de définir chacun des logiciels afin d'être au clair sur leurs utilités.

Pour la réalisation vidéo, nous aurons besoin des logiciels de la suite Adobe Première Pro et Adobe After Effect.

Pour la retouche photo et l'illustration, nous aurons besoin d'Adobe Photoshop et d'Adobe Illustrator.

Enfin, pour la conception 3D, nous utiliserons Cinema 4D et SolidWorks. Cinema 4D est un logiciel très puissant, utilisé par beaucoup de professionnels pour créer des objets 3D et les animer. Cela s'avèrera très utile pour créer des animations 3D pour nos vidéos. Cinema 4D est aussi compatible avec Adobe After Effect, ce qui va faciliter les passages de l'un à l'autre. SolidWorks permet également de créer des rendus 3D mais sera utilisé à des fins de conception techniques des Rubik's Cubes. En effet, il nous permettra de visualiser les nouveaux concepts de Rubik's Cube à travers une modélisation détaillée.
Outre les logiciels de création et de conception, il sera également nécessaire de fournir aux employés du service STEDesign des outils de communication et de collaboration en ligne. Nous utiliserons pour cela la suite Google Workspace qui inclut des outils de messagerie, de visioconférence, et de travail collaboratif en temps réel tels que Google Docs, Sheets et Slides. Cette suite est très utile pour les équipes travaillant à distance ou en déplacement, car elle permet de travailler de manière efficace et synchronisée, même à distance.
En outre, il sera important de prévoir des outils de sauvegarde et de récupération de données. Nous utiliserons une solution de sauvegarde automatisée pour sauvegarder toutes les données importantes de l'entreprise et les récupérer en cas de sinistre. Nous utiliserons également un système de stockage en ligne pour stocker les données importantes de manière sécurisée et y accéder à tout moment, de n'importe où.

Enfin, nous prévoyons d'organiser des formations pour les employés du service STEDesign afin qu'ils puissent apprendre à utiliser efficacement les logiciels et outils fournis, ainsi qu'à développer leurs compétences en matière de création et de conception. Ces formations seront dispensées en interne ou en externe, en fonction des besoins spécifiques de chaque employé.

Services restants

Tous les postes fixes seront équipés d'une licence Windows 11 : il s'agit de la dernière version de Windows, constituant un système d'exploitation ergonomique et intuitif, donc facile d'utilisation. De plus, des mises à jour y sont effectuées régulièrement, protégeant ainsi chaque poste d'éventuelles failles 0-day ou autres.

Depuis chaque poste, l'accès à la suite Microsoft Office sera possible grâce au serveur TSE. Les employés pourront ainsi accéder à des logiciels comme Word ou Excel, afin d'accomplir leurs tâches et ne pas être dépaysé par de nouveaux logiciels qu'ils ne maîtrisent pas.

Afin de mieux gérer l'Active Directory (AD), seul l'administrateur réseau pourra disposer d'un poste fonctionnant sous Windows Server 2022. C'est la meilleure version de Windows pour gérer un AD : l'administrateur pourra ainsi créer des sessions utilisateurs, gérer les autorisations de chaque session, créer des dossiers de partage en fonction des besoins des employés, etc.

Pour configurer et optimiser les serveurs, la version Alma de linux sera installée. Il sera aisé d'y installer les outils nécessaires ("httpd" pour l'hébergement de sites, "named" pour le DNS, etc.) et d'y appliquer la meilleure configuration pour améliorer le réseau ainsi que l'activité de l'entreprise.

Enfin, dans un souci de sécurité maximale, l'antivirus McAfee sera installé sur toutes les machines branchées ou connectées sur le réseau. Des licences seront fournies en nombre afin de bien avoir une licence par poste. McAfee est l'un des meilleurs antivirus sur le marché avec un gestionnaire de mot de passe intégré, un scan en temps réel des navigations internet, et beaucoup d'autres fonctionnalités visant à une sécurisation optimale du poste en entreprise.

En plus des logiciels et des outils de communication, il sera également important de fournir aux employés des services d'assistance technique et de maintenance. Nous prévoyons de mettre en place un service d'assistance technique pour répondre aux besoins des employés en cas de problèmes techniques ou de questions. Ce service sera accessible par téléphone, par courrier électronique, ou par chat en ligne, selon les préférences de chaque employé.

En outre, nous prévoyons de mettre en place un plan de maintenance régulier pour les ordinateurs et les serveurs de l'entreprise. Ce plan inclura des mises à jour de sécurité, des tests de performance, des nettoyages de disque dur, et des réparations en cas de panne. Le but de ce plan est de garantir que tous les systèmes de l'entreprise fonctionnent de manière optimale et sans interruption.

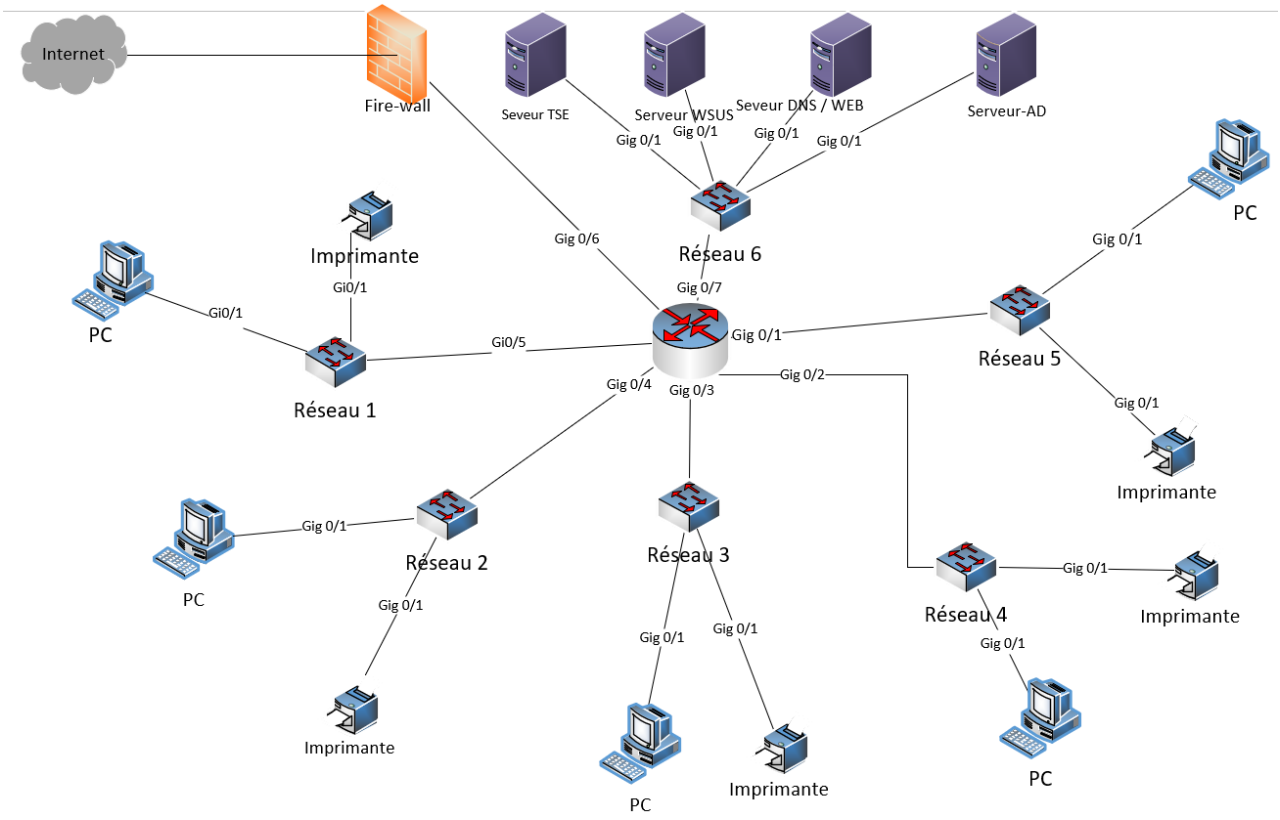
Enfin, il sera important de prévoir des mesures de sécurité pour protéger les données de l'entreprise contre les menaces de sécurité en ligne. Nous prévoyons de mettre en place un pare-

feu pour protéger le réseau de l'entreprise contre les attaques externes et des mesures de sécurité supplémentaires pour protéger les données de l'entreprise contre les malwares, les virus et les logiciels espions. Nous mettrons également en place des procédures de sécurité pour éviter les fuites de données sensibles et protéger les informations confidentielles de l'entreprise.

3.4 – Réseau du site de Bristol

3.4.1 – Structure physique

Pour la partie de la conception du réseau du site de Bristol, l'équipe a effectué les analyses et propositions de conception suivantes pour chaque paramètre, voici le schéma qui sera proposé par l'équipe :



Mise en place d'un routeur central

Afin d'avoir un réseau plus fluide et accessible, le site de Bristol sera équipé d'un routeur central afin d'avoir un sous-réseau disponible pour tout le site.
Ce routeur permettra d'avoir un débit remarquable pour une taille convenable. Il sera lui-même connecté au firewall et au switch central afin de ne pas prendre un routeur possédant trop de ports, ce qui présenterait un coût trop élevé. Le routeur sera connecté aux 5 commutateurs et au firewall par le biais de câbles Gigabit Ethernet. La topologie choisie est une topologie en étoile, cela garantit une meilleure sécurité et un risque de collision plus faible

De plus, un DHCP sera configuré sur le serveur afin d'avoir un adressage dynamique, cet adressage permettra d'obtenir une meilleure fluidité et un gain de temps conséquent lors de l'ajout d'un poste au réseau.

Mise en place d'un Switch par réseau

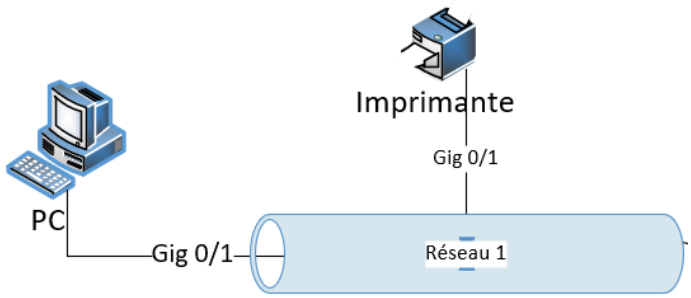
Chaque switch possède 10 ports qui est directement connecté sur son port fa0/1 au routeur, chaque autre port sera connecté à un service présent sur le site (pc et imprimante). Le switch sera connecté au routeur central par un câble 10Gb/s, ce câble représente un certain coût mais il n'y aura qu'une seule connexion qui relie l'intégralité du système au routeur. Ainsi, un câble 1Gb/s serait moins efficace et n'assurerait pas la fluidité.
Cependant, entre les commutateurs et les différents équipements, tous les câbles seront des câbles 1GB/s car les services ne demandent pas un débit très élevé.

Sous Réseau

Lors de la mise en place de la nouvelle infrastructure, 5 sous réseaux seront installés, ces derniers regrouperont chacun 1 switch, 11 pc et 1 imprimante. On retrouvera également un sous-réseau pour la salle des serveurs, ainsi 6 réseaux seront présents sur le site.

Un sous-réseau est un réseau informatique qui est créé en divisant un réseau plus grand en plusieurs segments de réseau plus petits. Chaque sous-réseau est généralement isolé des autres, avec un routeur ou un commutateur agissant comme un pont entre les différents sous-réseaux, cela permet de sécuriser le site en isolant et d'étanchéifier les postes au sein des sous-réseaux.
Dans chaque sous-réseau contenant 1 VLAN, 11 PC, 1 switch et 1 imprimante, chaque appareil sera connecté au switch. Le switch sera configuré pour utiliser le VLAN, qui permettra de créer un domaine de diffusion logique, c'est-à-dire un groupe de périphériques qui peuvent communiquer entre eux, mais pas avec les périphériques qui ne font pas partie du même VLAN.
De plus, tous les branchements des différents équipements se feront en mode "Access", en effet, brancher en mode "Access" dans un sous-réseau VLAN permettra de séparer efficacement le trafic entre différents groupes d'utilisateurs sur le réseau. Lorsque vous connectez un PC à un switch en mode "Access", cela signifie que le PC est configuré pour appartenir à un seul VLAN. Si vous configurez le port de switch pour le VLAN approprié, le PC ne sera en mesure de communiquer qu'avec d'autres périphériques du même VLAN. Cela permet de séparer le trafic entre différents groupes d'utilisateurs sur le réseau et d'isoler les problèmes de réseau à un seul VLAN.
Une fois que les adresses IP et les masques de sous-réseau sont configurés, les périphériques peuvent communiquer entre eux en utilisant le switch comme pont. L'imprimante peut être

partagée avec les PC du sous-réseau en la configurant pour qu'elle soit accessible via l'adresse IP du sous-réseau.
En utilisant un sous-réseau, il est possible de créer des réseaux plus petits et plus faciles à gérer, tout en offrant une sécurité accrue en limitant la diffusion de trafic à l'intérieur du réseau. Cela peut également améliorer les performances du réseau en réduisant le trafic de diffusion inutile qui peut ralentir le réseau.



Salle Serveur

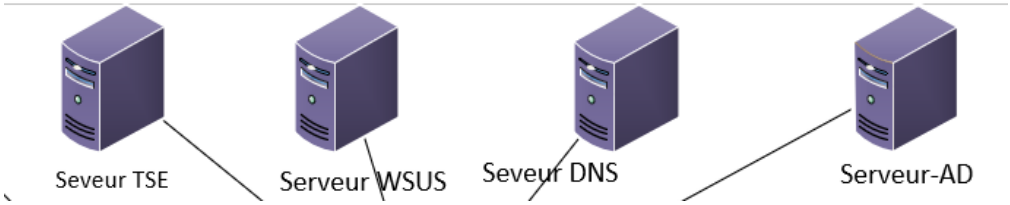
Sur ce nouveau réseau mis en place, différents serveurs seront installés et configurés afin d'accomplir des missions bien précises. Un serveur DNS, un serveur TSE et un serveur WSUS seront mis en place à part sur le site, ces trois serveurs seront reliés à un switch qui sera lui-même relié au routeur du réseau, ces serveurs seront regroupés dans un sous-réseau installé dans la salle des serveurs.

Le serveur DNS Un serveur DNS (Domain Name System) est un type de serveur informatique qui gère la résolution des noms de domaine en adresses IP. Les noms de domaine sont des adresses faciles à retenir, telles que "rubikscube.com", qui sont utilisées pour accéder à des sites web, ce serveur sera sous LINUX.

Le serveur RDS ((Remote Desktop Services) utilisé permettra à plusieurs utilisateurs de se connecter au serveur à l'aide de clients ou de périphériques distants.

Le serveur WSUS (Windows Server Update Service) qui aura pour rôle la distribution de mises à jour au sein du site.

Il y aura également 1 serveur AD dans la salle des serveurs, il sera sous Windows server 2022 et aura pour but de gérer et administrer les sessions.



PC

Il y aura donc 11 postes fixes, des PC de bureau seront choisis car les employés présents sur le site seront des commerciaux. De plus, l'ajout de postes fixes restera possible, les comptes utilisateurs et session seront configurés par l'administrateur réseau grâce à l'AD.

Switch

Afin de compléter l'organisation du réseau, 6 commutateurs seront installés, le switch (commutateur) est un boîtier doté de quatre à plusieurs centaines de ports Ethernet qui sert à relier en réseau différents éléments du système informatique. Il permet également de créer des circuits virtuels, de recevoir des informations et de les envoyer vers un destinataire précis sur le réseau, la particularité du switch est donc d'avoir la capacité à aiguiller les messages vers le bon destinataire. Le switch a aussi d'autres avantages, il sécurise les données qui passent par le réseau et permet d'augmenter facilement le nombre d'ordinateurs connectés sur un réseau Ethernet.

Imprimantes

Sur le site de Bristol, chaque sous-réseau (hormis la salle des serveurs) sera équipé d'une imprimante qui permettra de faire des impressions de documents, le choix de l'imprimante se tournera vers une imprimante ayant la capacité d'imprimer rapidement et qui comportera l'option de brancher une clé USB directement sur l'imprimante afin d'imprimer des documents depuis cette dernière, l'imprimante devra également présenter un code propre à chaque employé afin d'éviter des impressions frauduleuses et d'éviter la surutilisation de l'imprimante par un employé. L'imprimante devra pouvoir imprimer en filaire et en réseau.

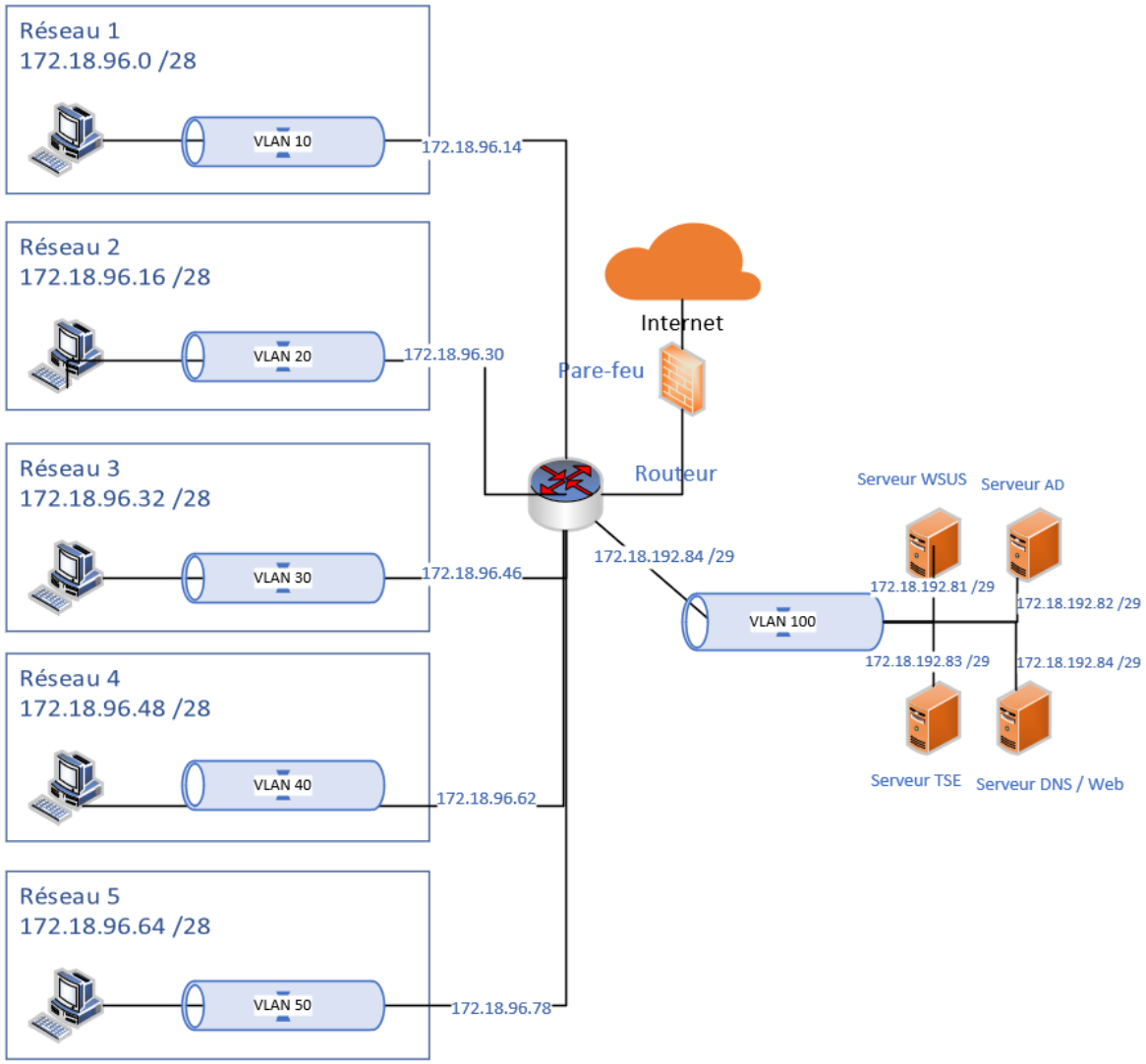
Cable Ethernet SFTP

Afin de connecter les équipements au réseau internet, des câbles Ethernet SFTP seront utilisés. En effet, ces derniers possèdent des fils de cuivre, une feuille d'aluminium et une gaine extérieure qui permet un double blindage, chaque fil de cuivre est torsadé, ce qui permet de limiter sa sensibilité aux interférences.

Plus précisément, des câbles Ethernet SFTP de catégorie 6 seront choisis car ils permettront de transmettre des fréquences jusqu'à 250 MHz, d'avoir un débit jusqu'à 1 Gbit/s ainsi que de présenter jusqu'à 100m de longueur maximale de câble SFTP de catégorie 6.

3.4.2 – Structure logique

Afin d'effectuer la création de la logistique du site de Bristol, le logiciel Visio a été utilisé dans le but d'instaurer un schéma logique du réseau.



Dans un premier temps, un routeur sera mis en place afin de connecter les différents réseaux entre eux, ensuite plusieurs réseaux seront organisés et découpés en différents Vlan. De plus, des switch (24 ports Gigabit Ethernet) seront installés afin de gérer chaque vlan et de rediriger

les messages provenant du réseau vers le routeur, un serveur DHCP sera également installé dans chaque vlan. La création des 5 vlan permettra d'isoler chaque réseau et de renforcer la sécurité car les réseaux seront séparés, chaque réseau comptera 11 utilisateurs ainsi que 1 imprimante et 1 serveur, chaque switch connectera donc 14 ports en ajoutant la liaison avec le routeur.
De plus, afin de renforcer la sécurité du site, un firewall sera mis en place entre le routeur et internet pour éviter les intrusions malveillantes.
Une imprimante multifonction sera également reliée à chaque réseau afin de permettre aux utilisateurs d'imprimer leurs documents.
Enfin 4 serveurs (TSE, WSUS, AD et DNS) seront connectés au routeur par un switch.

VLAN :

Un VLAN (Virtual Local Area Network) est une méthode pour créer des sous-réseaux logiques sur un réseau physique. Cela permet de regrouper des utilisateurs ou des équipements qui ont des besoins similaires en termes de sécurité, de performances ou de gestion de bande passante, indépendamment de leur emplacement physique sur le réseau.

Les VLANs sont généralement configurés sur les commutateurs réseau, qui sont utilisés pour connecter les différents équipements d'un réseau. Les ports physiques sur un commutateur peuvent être configurés pour appartenir à un VLAN spécifique, ce qui permet de limiter les communications entre les équipements connectés aux ports de ce VLAN.

Les VLANs peuvent également être utilisés pour séparer les différents segments d'un réseau en fonction de l'utilisation, tels que les réseaux d'invités, les réseaux d'entreprise, les réseaux de gestion, les réseaux de stockage de données, les réseaux de caméra de surveillance, etc.

Il est important de noter que les VLANs ne créent pas une séparation de sécurité physique, les utilisateurs malveillants peuvent encore accéder à des réseaux VLANs non autorisés via des ports mal configurés ou des vulnérabilités de sécurité. Les VLANs sont donc souvent utilisés en combinaison avec des technologies de sécurité réseau supplémentaires telles que les routeurs de sécurité ou les pares-feux pour renforcer la sécurité.

Un vlan sera attribué à chaque sous réseau, étant donné qu'il y aura 6 sous-réseaux il sera donc nécessaire de créer 6 vlan. Chaque réseau ne détient pas de caractéristique particulière et sera constitué de 11 postes et d'une imprimante.

Vlan 10 - Réseau 1
Sur le Vlan 10 il y a 11 postes et une imprimante qui sont reliés sur le réseau interne de l'entreprise.
Vlan 20 - Réseau 2
Sur le Vlan 20 il y a 11 postes et une imprimante qui sont reliés sur le réseau interne de l'entreprise.
Vlan 30 - Réseau 3
Sur le Vlan 30 il y a 11 postes et une imprimante qui sont reliés sur le réseau interne de l'entreprise.

Vlan 40 - Réseau 4
Sur le Vlan 40 il y a 11 postes et une imprimante qui sont reliés sur le réseau interne de l'entreprise.
Vlan 50 - Réseau 5
Sur le Vlan 50 il y a 11 postes et une imprimante qui sont reliés sur le réseau interne de l'entreprise.
Vlan 100 - Réseau 6
Le vlan 100 est le vlan des serveurs, ce vlan regroupe tous les serveurs dans le même réseau il n'y a que 4 serveurs dans ce vlan et rien d'autres

VLSM :

Pour faire du VLSM (Variable Length Subnet Mask), on doit d'abord comprendre les concepts de base du sous-réseautage et de l'attribution d'adresses IP. On doit ensuite utiliser ses connaissances pour créer les sous-réseaux de tailles différentes en utilisant des masques de sous-réseau de longueurs variables. Il est important de planifier soigneusement l'attribution des adresses IP pour éviter les gaspillages d'adresses et pour assurer que chaque sous-réseau a suffisamment d'adresses pour les besoins de l'entreprise.

L'adresse IP réseau de l'environnement principal est 172.18.96.0/19.
Le réseau du site Bristol se décompose en 5 VLANs de à peu près 10 postes chacun.

N° du VLAN	@Réseau	Masque	Nb d'utilisateurs
VLAN 10	172.18.96.0	255.255.224.0	14
VLAN 20	172.18.96.16	255.255.224.0	14
VLAN 30	172.18.96.32	255.255.224.0	14
VLAN 40	172.18.96.48	255.255.224.0	14
VLAN 50	172.18.96.64	255.255.224.0	14
VLAN 100	172.18.96.80	255.255.255.248	4

Voici également les différentes adresses IP des serveurs :

Nom du serveur	Adresse IP
Serveur DNS/WEB	172.18.96.84
Serveur TSE	172.18.96.83
Serveur AD	172.18.96.82
Serveur WSUS	172.18.96.81

Firewall

Il sera également nécessaire d'utiliser un firewall dans l'infrastructure réseau du site de Bristol qui permettra d'avoir une meilleure sécurité de l'infrastructure, une visibilité accrue sur les flux établis et bloqués et une meilleure utilisation des bandes passantes.

Le firewall permet également d'assurer la sécurité des informations d'un réseau en filtrant les entrées et en contrôlant les sorties selon des règles définies par son administrateur. Cela permet également de protéger les ordinateurs ou le réseau du trafic entrant et sortant nuisible.

Table de routage

	Type	@ réseau	Masque réseau	Passerelle	Interface
Réseau 1	C	172.18.96.0	255.255.255.240	172.18.96.14	FastEthernet 0/0
Réseau 2	C	172.18.96.16	255.255.255.240	172.18.96.30	FastEthernet 1/0
Réseau 3	C	1172.18.96.32	255.255.255.240	172.18.96.46	FastEthernet 6/0
Réseau 4	C	172.18.96.48	255.255.255.240	172.18.96.62	FastEthernet 7/0
Réseau 5	C	172.18.96.64	255.255.255.240	172.18.96.78	FastEthernet 8/0
Réseau 6	C	172.18.96.80	255.255.255.248	172.18.96.86	GigabitEthernet3/0
Réseaux Inter-sites	S	192.168.0.0	255.255.0.0	128.52.60.253	128.52.60.254
	S	128.50.0.0	255.254.0.0	128.52.60.253	128.52.60.254

Afin de faciliter la compréhension du réseau, voici un tableau qui définit les serveurs et les adresse IP utilisée, leur fonctionnalité et leur numéro de port

Serveur :	Adresse IP :	Protocole :	Port :
DNS	172.18.96.84	UDP	53
WEB	172.18.96.84	TCP	80 (HTTP) / 443 (HTTPS)
WSUS	172.18.96.81	TCP	443
TSE	172.18.96.83	TCP	3389 (RDP)

AD	172.18.96.82	LDAP	636

Table firewall

N°	Adresse Source	Port source	Adresse Destination	Port Destination	Protocole	Action
1	*	*	172.18.96.84 /29	443	TCP	Allow
2	*	*	172.18.96.84 /29	80	TCP	Allow
3	*	*	172.18.96.84 /29	53	UDP	Allow
4	172.18.96.0 /25	*	172.18.96.80 /29	22	TCP	Allow
5	172.18.96.0 /25	*	172.18.96.82 /29	445 / 636	TCP	Allow
6	*	*	172.18.96.0 /25	515	TCP	Allow
7	*	*	172.18.96.83 /29	3389	TCP	Allow
8	*	*	*	*	*	Deny

Description des règles du firewall

Les règles du firewall ont été effectués afin que tout le monde puisse accéder aux ressources des serveurs comme le serveur web, et que seules les postes du réseau peuvent avoir accès au serveur qui les concerne comme le serveur WSUS, DNS, TSE et AD. Cette solution permet se renforce la sécurité du site Bristol

DHCP :

Sur le site, un serveur DHCP sera configuré sur chaque VLAN du réseau.
Le protocole DHCP (Dynamic Host Configuration Protocol) est un protocole réseau utilisé pour attribuer des adresses IP de manière dynamique aux équipements connectés à un réseau. Il permet aux ordinateurs et autres appareils de recevoir automatiquement une adresse IP, une adresse de passerelle et d'autres paramètres de configuration réseau tels que les serveurs DNS lorsqu'ils se connectent à un réseau.
Lorsqu'un équipement connecté à un réseau DHCP envoie une demande de configuration, le serveur DHCP attribue une adresse IP libre à partir d'une plage d'adresses configurée et envoie cette information aux paramètres de configuration de l'équipement. Cette adresse IP est généralement temporaire et est renouvelée après un certain temps (appelé durée de bail), ou lorsque l'équipement se déconnecte du réseau.

L'utilisation d'un DHCP a de nombreux avantages, cela permet de faciliter la gestion des adresses IP en évitant d'avoir à configurer manuellement les adresses IP de chaque équipement. Cela permet également une meilleure utilisation de l'espace d'adresses IP en utilisant les adresses non utilisées et cela permet aux utilisateurs de se connecter à des réseaux différents sans avoir à configurer manuellement les paramètres de leur équipement.

Il est important de noter que pour utiliser le DHCP, un serveur DHCP doit être configuré et en cours d'exécution sur le réseau, et que les équipements connectés doivent prendre en charge le DHCP pour obtenir des adresses IP automatiquement.

Hébergement Web :

Le site de bristol hébergera le site internet “rubikscube.com” a l’aide du serveur DNS / WEB qui respectera la configuration du cahier des charges. Le serveur se situera dans le sous-réseau des serveurs, il fera office à la fois d’hébergeur web et de DNS, en utilisant l’OS Alma Linux ligne de commande, cela en fait un OS léger et sécurisé. Apache sera utilisé pour le service Web gratuit, open source et Bind DNS serviront à configurer le nom de domaine, open source est fiable, gratuit et pratique. Git permettra de stocker et partager les fichiers web, de suivre le code facilement et de simplifier le déploiement de nouvelles versions du code, enfin il offre une solution de sauvegarde efficace pour les fichiers web.

PAT :

Le Port Address Translation (PAT) est une méthode de traduction d'adresses IP qui permet à plusieurs ordinateurs sur un réseau privé de partager une adresse IP publique unique. Le PAT est une forme de Network Address Translation (NAT) qui utilise des numéros de port pour identifier les ordinateurs sur le réseau privé. Lorsque le trafic sort du réseau privé, le PAT modifie l'adresse IP source et le numéro de port source de la demande pour correspondre à l'adresse IP publique et au numéro de port du routeur.

La configuration du PAT implique généralement de définir une adresse IP publique sur l'interface de sortie, configurer l'interface du routeur qui est connectée à l'Internet avec une adresse IP publique statique. Créer une liste d'adresses IP privées à traduire, spécifier une plage d'adresses IP privées sur le réseau interne qu’il faut traduire en adresses IP publiques. Et définir une règle de traduction d'adresses, configurer une règle pour traduire les adresses IP privées vers les adresses IP publiques. La règle doit spécifier l'interface de sortie et le numéro de port qui doit être utilisé pour chaque adresse IP privée.

3.4.3 – OS et logiciels à utiliser

Description des OS

Plusieurs OS seront installés dans le réseau afin de garantir son bon fonctionnement.

Pour commencer, Windows 11 sera installé. En effet, c'est la dernière version sortie à ce jour ce qui permettra d'avoir une version à la pointe de la technologie et également sécurisée.

Également, le réseau sera équipé de Windows Serveur 2022, ce qui permettra d'utiliser plusieurs services comme l'Active Directory et le WSUS. Cette dernière version est également la dernière sortie ce qui signifie que la sécurité est présente.

Enfin ALMA Linux sera utilisé, ce qui permettra l'utilisation de plusieurs services tels que le DNS. Cet OS permettra d'assurer une grande fiabilité ainsi qu'une grande sécurité. Le coût également est intéressant du fait qu'Alma Linux est open source et gratuite.

Description des logiciels

Concernant les logiciels, les salariés seront équipés de la suite Microsoft 365 qui permet d'avoir Word, Excel, Powerpoint, Teams et Share Point. Ces logiciels permettront une grande productivité pour les employés de l'entreprise notamment dans la rédaction mise en page de documents ou encore dans la communication.

4 – Intercommunication entre les sites

4.1 – Structure physique

Les routeurs de sites seront reliés par un VPN SSL (le protocole SSL permet une interconnexion rapide à mettre en place et facile à migrer). La connexion à internet est assurée par le routeur du FAI.

4.2 - Structure Logique

4.2.1- PAT :

Chacun des routeurs étant paramétrés en NAT, il est impossible de communiquer directement avec les postes à l'intérieur des sites. De ce fait, tous les postes seront paramétrés en NAT Dynamique (PAT) afin de pouvoir accéder aux services fournis par chaque site par redirection (en communiquant directement avec le routeur du site). Les services accessibles via l'extérieur sur chaque site sont :

BREST		**Protocole**	**Port**
1	FTP	TCP	22
2	IMAPS	TCP	993
3	SMTPS	TCP	465
4	ADWS/ADMGS	TCP	9389
5	Global Catalog	TCP	3268/3269
6	LDAP	TCP/UDP	389
7	SSL	TCP	636
8	IPsec ISAKMP	UDP	500
9	NAT-T	UDP	4500
10	RPC	TCP	135

BRISTOL		Protocole	Port
1	HTTPS	TCP	443
2	HTTP	TCP	80

4.2.2- Plan d'adressage :

Chaque site recevra une adresse IP spécifique pour les lier au routeur central et Internet. Le plan d'adressage est comme suit :

Réseau	@Réseau	Masque	@routeur	@Broadcast
Brest	192.168.1.0	255.255.255.252	192.168.1.1	192.168.1.3
Rennes	128.50.60.252	255.255.255.252	128.50.60.254	128.50.60.255
Nantes	128.51.60.252	255.255.255.252	128.51.60.254	128.51.60.255
Bristol	128.52.60.252	255.255.255.252	128.52.60.254	128.52.60.255

4.2.3- Sécurité :

De plus, nous prévoyons l'utilisation d'un VPN SSL pour connecter de manière sécurisée les sites. Les entrées et sorties du VPN seront gérées par les routeurs de site et le routeur central, permettant donc d'être protégé sur l'entièreté du trajet par internet. De ce fait, les communications entre les sites ne pourront pas être interceptées et la confidentialité sera assurée.

4.3- Active Directory

4.3.1 – Structure de l'Active Directory

Afin de sécuriser au mieux l'entièreté du réseau de Rubixcube, gérer les accès et les comptes utilisateurs des salariés de l'entreprise est nécessaire. Ainsi, l'utilisation d'un contrôleur de domaine sera nécessaire.
Etant donné que les sites communiquent entre eux, le serveur Active Directory (AD) de Brest couvrira l'entièreté du réseau Rubix Cube. Ainsi, l'AD de Brest sera composé d'un domaine ayant pour nom de domaine « rubixcube.local ».
Dans cette forêt sera intégré 4 sites. Le site de Brest avec le nom de domaine « rubixcube.local.brest », le site de Rennes avec pour nom de domaine « rubixcube.local.rennes », le site de Nantes « rubixcube.local.nantes » et le site de Bristol « rubixcube.local.bristol ».
Ainsi, chacun de ces sites seront composées d'Unité d'Organisation (OU). Le site de Brest sera composé de 7 OU. L'OU DSI, accueil, RH, marketing, finance, direction et serveurs. Le site de Rennes aura 4 OU, L'OU production, logistique, DSI et serveurs. Le site de Nantes aura quant à lui uniquement l'OU accueil. Enfin, le site de Bristol sera composé de 3 OU, DSI, commercial et serveurs.

4.3.2 – GPO

Chaque OU sera géré par des GPO (Groupe Policy Object) afin de limiter les accès des comptes utilisateurs en fonction de leur OU. Ainsi, voici un tableau contenant les différentes GPO.

Toutes les OU :

Nom GPO	**Fonction**
Domain Policy	Mot de passe à changer tous les ans, 12 caractères
Suite Office	Installation Suite Office sur les postes
Fond Ecran	Ajout fond d'écran Rubix Cube et non modifiable
Firefox	Installation Firefox

DSI :

Nom GPO	Fonction
Wireshark	Installation et accès à Wireshark
Vsio	Installation et accès à Visio
Packet tracer	Installation et accès à Packet Tracer
Visual Studio Code	Installation et accès à Visual Studio Code
VMWare	Installation et accès à VMWare
PuttY	Installation et accès à Putty

STE Design :

Nom GPO	Fonction
Suite Adobe	Installation et accès à la Suite Adobe
Cinema 4D	Installation et accès à Cinema 4D
Solid Works	Installation et accès à Solid Works

4.3.3 – Domaine Locaux

Pour garantir la sécurité du réseau, il est nécessaire d'ajouter certaines restrictions. Les domaines locaux (DL) permettent de créer des types de permissions qui seront appliqué à des groupes d'utilisateurs. Ces DL seront appliqués sur les différents ficher du serveur FTP.

DL Fichier Design

Nom DL	Fonction	Groupe Global
DL_Design_CT	Accès Total	DSI
DL_Design_LM	Lecture/modification	Design, Direction
DL_Design_L	Lecture	R&D, Production
DL_Design_R	Refus	Autres

DL Fichier DSI

Nom DL	Fonction	Groupe Global
DL_DSI_CT	Accès Total	DSI
DL_DSI_LM	Lecture/modification	Direction
DL_DSI_L	Lecture	Aucun
DL_DSI_R	Refus	Autres

DL Fichier Accueil

Nom DL	Fonction	Groupe Global
DL_Accueil_CT	Accès Total	DSI
DL_Accueil_LM	Lecture/modification	Acceuil, Direction
DL_Accueil_L	Lecture	Aucun
DL_Accueil_R	Refus	Autres

DL Fichier RH

Nom DL	Fonction	Groupe Global
DL_RH_CT	Accès Total	DSI
DL_RH_LM	Lecture/modification	Direction, RH
DL_RH_L	Lecture	Aucun
DL_RH_R	Refus	Autres

DL Fichier Marketing

Nom DL	Fonction	Groupe Global
DL_Marketing_CT	Accès Total	DSI
DL_Marketing_LM	Lecture/modification	Direction, Marketing
DL_Marketing_L	Lecture	Aucun
DL_Marketing_R	Refus	Autres

DL Fichier Finance

Nom DL	Fonction	Groupe Global
DL_Finance_CT	Accès Total	DSI
DL_Finance_LM	Lecture/modification	Direction, Finance
DL_Finance_L	Lecture	Aucun
DL_Finance_R	Refus	Autres

DL Fichier Direction

Nom DL	Fonction	Groupe Global
DL_DirectionIT	Accès Total	DSI
DL_Direction_LM	Lecture/modification	Direction
DL_Direction_L	Lecture	Aucun
DL_Direction_R	Refus	Autres

DL Fichier Logistique

Nom DL	Fonction	Groupe Global
DL_Logistique_CT	Accès Total	DSI
DL_Logistique_LM	Lecture/modification	Direction, Logistique
DL_Logistique_L	Lecture	Aucun
DL_Logistique_R	Refus	Autres

DL Fichier Production

Nom DL	Fonction	Groupe Global
DL_Production_CT	Accès Total	DSI
DL_Production_LM	Lecture/modification	Direction
DL_Production_L	Lecture	Design
DL_Production_R	Refus	Autres

DL Fichier commun

Nom DL	Fonction	Groupe Global
DL_Commun_CT	Accès Total	DSI
DL_Commun_LM	Lecture/modification	Autres
DL_Commun_L	Lecture	Aucun
DL_Commun_R	Refus	Aucun

5 – Description des OS, des logiciels et des serveurs

5.1 – OS

5.1.1 - Windows 11

Le système d'exploitation Windows 11 fait partie des systèmes d'exploitation communs au sein des sites. Windows 11 est la dernière version du système d'exploitation de Microsoft, qui est utilisé pour faire fonctionner des ordinateurs de bureau, des ordinateurs portables, des tablettes et des appareils hybrides. Ce sera donc la version qui sera installée sur tous les postes.
Nous avons fait les choix de Windows 11 pour différentes raisons :
La première est que Windows 11 est encore très récent, en effet c'est la dernière version sortie par Microsoft et cela va dans le sens de la durabilité du SI et de ne pas le changer dans les prochaines années. Ce qui nous offre une bien meilleure sécurité sur le long terme en optant pour Windows 11.
Windows 11 offre notamment des performances plus accrues et une meilleure sécurité contre les logiciels malveillants notamment avec leurs mises à jour régulières. Windows 11 permet d'intégrer des options telles que Windows Hello qui offre une sécurité d'authentification plus élevée
Intégration avec Microsoft 365 (voir 5.2.1 - Microsoft 365) : Windows 11 est conçu pour fonctionner de manière transparente avec Microsoft 365, ce qui facilite l'accès à vos documents, courriels et calendriers

5.1.2 - Alma Linux

Alma Linux est un système d'exploitation de type Linux créé en 2021. Alma Linux est une distribution stable, sécurisée et adaptée aux entreprises. Il est construit à partir des mêmes sources que Red Hat Enterprise Linux (RHEL) et est entièrement compatible avec RHEL.
Nous avons choisi Alma Linux pour plusieurs raisons :
Fiabilité : Alma Linux est une distribution stable et fiable, adaptée aux charges de travail d'entreprise. Il est basé sur RHEL, qui est connu pour être un système d'exploitation stable et fiable.
Sécurité : Alma Linux est un système d'exploitation sécurisé qui suit les meilleures pratiques de sécurité. Il est régulièrement mis à jour avec les derniers correctifs de sécurité et dispose d'une communauté de soutien active.
Coût : Alma Linux est une distribution open source gratuite, ce qui peut aider les entreprises à réduire leurs coûts.
Communauté : Alma Linux est soutenu par une communauté active d'utilisateurs et de développeurs. Cette communauté peut fournir des conseils, un support technique et des mises à jour pour aider les entreprises à tirer le meilleur parti de leur système d'exploitation.
En résumé, Alma Linux est une distribution Linux stable, sécurisée, compatible avec RHEL, gratuite et soutenue par une communauté active. Pour ces raisons, Alma Linux peut être un

excellent choix pour les entreprises qui cherchent à utiliser une distribution open source dans leur environnement informatique.
Alma Linux va également permettre d'instaurer des services tels que le service DNS, la gestion des logs, la supervision réseau, la téléphonie ainsi que la messagerie (voir serveur).

5.1.3 - Windows Serveur 2022

Windows Serveur 2022 est un système d'exploitation de serveur développé par Microsoft. Il est conçu pour offrir des fonctionnalités avancées de gestion de serveur, de stockage, de virtualisation et de sécurité pour les entreprises de toutes tailles.
Nous avons fait le choix de Windows Serveur 2022 pour différentes raisons :
Windows Serveur 2022 étant la dernière version "serveur" sortie à ce jour. Ce choix a été également choisi pour la durée de l'utilisation de cet OS. Celui-ci étant très récent (1 an) il ne sera pas obsolète dans quelques années ce qui permet donc au SI de ne pas changer pendant un moment cet OS.
Gestion centralisée des ressources informatiques : Windows Server 2022 fournit une infrastructure de gestion centralisée pour les ressources informatiques, y compris les serveurs, les ordinateurs de bureau, les applications, les utilisateurs et les données. Cela facilite la configuration, la surveillance et la gestion de vos ressources informatiques à partir d'un seul emplacement.
Sécurité renforcée : Windows Server 2022 intègre des fonctionnalités de sécurité avancées pour protéger vos données et votre infrastructure informatique contre les menaces en ligne, les virus et les programmes malveillants. Les fonctionnalités de sécurité comprennent des pare feux, des filtres anti-spam et anti-malware, des contrôles d'accès, des politiques de sécurité et des outils de détection d'intrusion.
Virtualisation : Windows Server 2022 est doté de fonctionnalités de virtualisation avancées qui permettent de créer et de gérer des machines virtuelles (VM) pour consolider les ressources informatiques et réduire les coûts. Il prend également en charge la virtualisation de l'infrastructure de bureau (VDI) pour permettre aux utilisateurs d'accéder à leurs ordinateurs de bureau virtuels à partir de n'importe quel périphérique.
Windows serveur va également permettre d'instaurer des services tels que l'Active directory (Voir serveur).

5.2 – Logiciels

5.2.1 - Microsoft 365

Microsoft 365 est une suite d'applications et de services cloud développée par Microsoft pour les entreprises. Cette suite comprend les applications les plus populaires de Microsoft, notamment Word, Excel, PowerPoint, Outlook, OneNote, Access, Publisher, Teams, SharePoint, Exchange et Yammer, ainsi que d'autres outils de productivité et de collaboration tels que OneDrive et Skype.

Microsoft 365 offre aux entreprises une plateforme unifiée pour les communications, la collaboration et la productivité en ligne. Les employés peuvent accéder à leurs applications et fichiers à partir de n'importe quel appareil et de n'importe où dans le monde grâce à la technologie cloud de Microsoft. En outre, la suite comprend des outils de sécurité avancés pour protéger les données de l'entreprise contre les menaces en ligne.

L'utilité de Microsoft 365 en entreprise est multiple. Tout d'abord, elle permet une collaboration en temps réel sur des projets entre des membres d'une même équipe ou de plusieurs équipes. Les documents peuvent être partagés facilement et des modifications en temps réel sont possibles.

Word est un logiciel de traitement de texte développé par Microsoft. Il est principalement utilisé pour créer, éditer, mettre en forme et imprimer des documents tels que des rapports, des cv, des bulletins d'informations...

Excel est un logiciel de tableur conçu pour effectuer des calculs, analyser et organiser des données numériques. Il est souvent utilisé pour des tâches telle la gestion de listes et de bases de données ou encore la tenue de compte, etc.

Powerpoint est un logiciel de présentation développé par Microsoft qui permet de créer des diaporamas visuels et interactifs. Il est utilisé pour créer des présentations professionnelles.

Teams est une application de messagerie destinée aux entreprises. Mais pas seulement ! Il s'agit d'un espace de travail pour la collaboration et la communication en temps réel, les réunions, le partage de fichiers et d'applis … Le tout regroupé au même endroit, ouvert et accessible à tous. C'est en quelque sorte le « hub » de toutes les applications Microsoft.

En outre, la suite offre une intégration complète avec d'autres outils de productivité et de collaboration tels que SharePoint, OneDrive... Ces outils permettent aux employés de partager des fichiers et de communiquer plus efficacement, même à distance.
Enfin, Microsoft 365 offre également une plateforme de sécurité avancée qui permet aux entreprises de protéger leurs données sensibles contre les menaces en ligne. Les données sont stockées dans le cloud et les outils de sécurité de Microsoft surveillent en permanence les activités suspectes.

En somme, Microsoft 365 est une suite d'applications et de services de productivité et de collaboration qui offre aux entreprises une plateforme unifiée pour la communication, la collaboration et la productivité en ligne, ainsi qu'une sécurité avancée pour protéger les données sensibles contre les menaces en ligne.

5.2.2 Wireshark

Wireshark est un outil de capture et d'analyse de paquets réseau. Il permet aux utilisateurs de capturer, d'analyser et de visualiser le trafic réseau en temps réel ou à partir d'un enregistrement de capture.

Wireshark est utilisé pour dépanner les problèmes de réseau, comprendre la communication entre différents appareils et réseaux, et pour tester et déboguer des applications réseau.

Plus précisément, Wireshark peut aider à :

- Identifier les problèmes de réseau : Wireshark permet de capturer le trafic réseau pour identifier les problèmes de performance, les erreurs de connexion et autres problèmes de réseau.
- Analyser le trafic réseau : Les utilisateurs peuvent analyser les paquets capturés pour comprendre la communication entre différents appareils et réseaux.
- Dépanner les applications réseau : Wireshark peut être utilisé pour dépanner les problèmes d'application réseau en analysant les paquets de données échangés entre les applications.
- Tester la sécurité du réseau : Les utilisateurs peuvent utiliser Wireshark pour détecter les vulnérabilités de sécurité dans les communications réseau et les attaques de réseau.

En somme, Wireshark est un outil essentiel pour les administrateurs réseau et les professionnels de la sécurité informatique pour diagnostiquer et résoudre les problèmes de réseau, ainsi que pour maintenir et améliorer la sécurité du réseau.

5.2.3 PuTTY

Le logiciel PuTTY est un émulateur de terminal open source pour les protocoles de communication réseau tels que SSH. Il est principalement utilisé pour se connecter à des serveurs distants en toute sécurité à partir d'un ordinateur local.

PuTTY permet également de transférer des fichiers de manière sécurisée entre des ordinateurs locaux et distants en utilisant le protocole SCP. Il est disponible pour les systèmes d'exploitation Windows, Linux et Mac OS X.

En résumé, le logiciel PuTTY est utilisé pour fournir une connexion sécurisée à des serveurs distants et pour transférer des fichiers entre des ordinateurs locaux et distants.

5.2.4 La suite Adobe

Pour la réalisation vidéo, nous aurons besoin des logiciels de la suite Adobe Première Pro et Adobe After Effect.
Adobe Première Pro est un logiciel de montage vidéo très puissant et nécessaire pour la réalisation de clips dans le cadre de campagnes de publicités. Adobe After Effect est connu pour sa capacité à créer des effets spéciaux, mais aussi pour intégrer une partie 3D qui sera utile pour les rendus 3D effectués avec Cinema 4D. After Effect permet aussi la pratique du motion design.
Adobe Illustrator est un logiciel de création graphique vectorielle, il est largement utilisé par les designers professionnels pour créer des illustrations, des graphiques, des logos, des icônes, des typographies et d'autres éléments visuels de haute qualité pour l'impression, le web et les médias numériques. Une fonctionnalité clé d'Adobe Illustrator est la capacité de travailler avec des calques, qui permet aux utilisateurs d'organiser et de manipuler les éléments de leur illustration de manière indépendante.
Adobe Photoshop permettront de créer, retoucher et éditer des photos ou images afin de décorer le site internet, ajouter des images dans les vidéos, et promouvoir l'entreprise via des campagnes de publicités.

5.2.5 Cinema 4D

Cinema 4D est un logiciel de modélisation, d'animation, de rendu et de motion design utilisé dans l'industrie du cinéma, de la télévision, de la publicité et du design graphique. L'une des fonctionnalités les plus puissantes de Cinema 4D est son système d'animation, qui permet de créer des animations de personnages, d'objets et de caméras avec une grande flexibilité.

Il propose des outils d'animation traditionnels tels que l'enregistrement de clés d'animation, la cinématique inverse et la capture de mouvement, ainsi que des fonctionnalités plus avancées comme la simulation de tissu, la simulation de cheveux et la simulation de particules. Cinema 4D offre également des fonctionnalités de rendu haut de gamme, permettant de créer des images et des animations réalistes.

5.2.6 SolidWorks

SolidWorks est un logiciel de conception assistée par ordinateur (CAO) utilisé dans l'industrie pour la modélisation 3D, la simulation, l'analyse et la documentation de produits. Développé par Dassault Systèmes, SolidWorks est largement utilisé dans les domaines de l'ingénierie, de la conception industrielle, de la fabrication et de l'architecture pour créer des modèles 3D de pièces, d'assemblages et de systèmes complexes.

Il propose une variété d'outils de modélisation, y compris la modélisation paramétrique, la modélisation surfacique, la modélisation de tôlerie et la modélisation de pièces moulées, qui permettent de créer des modèles 3D réalistes

5.3 – Serveurs

5.3.1- Serveur DNS

Le serveur DNS (Domain Name System) que nous voulons utiliser pour le site de Nantes est un système informatique qui permet de traduire les noms de domaine en adresses IP. Les noms de domaine sont des noms conviviaux que les utilisateurs peuvent facilement mémoriser, tandis que les adresses IP sont des numéros qui identifient de manière unique les ordinateurs et les appareils sur Internet.

Il contient une base de données de noms de domaine et de leurs adresses IP correspondantes. Lorsqu'un utilisateur saisit un nom de domaine dans son navigateur web, le navigateur envoie une requête DNS au serveur DNS pour obtenir l'adresse IP correspondante. Le serveur DNS répond à la requête en fournissant l'adresse IP correspondante, permettant ainsi au navigateur web de se connecter au serveur web qui héberge le site de Nantes.

Le serveur DNS sera également utilisé pour la résolution de noms de domaine inversée, c'est-à-dire la traduction d'une adresse IP en un nom de domaine. Cela sera utile pour le dépannage et la sécurité réseau, car cela permet d'identifier l'emplacement et le propriétaire d'une adresse IP donnée.

Le serveur DNS peut également être utilisé pour configurer des sous-domaines et des enregistrements DNS personnalisés. Les sous-domaines sont des noms de domaine qui sont créés sous un domaine existant, ce qui permet de les utiliser pour des sites web ou des services spécifiques. Les enregistrements DNS personnalisés permettent de spécifier des paramètres supplémentaires pour les noms de domaine, tels que les adresses IP de plusieurs serveurs web ou les adresses IP pour les serveurs de messagerie électronique.

5.3.2- Serveur FTP

Le serveur FTP (File Transfer Protocol) permet de faciliter l’échange de données et de commandes entre les logiciels et les ordinateurs. Ce dernier permet de transférer des fichiers entre un client et un serveur via le réseau Internet. Il est utilisé pour la gestion de fichiers sur le site web, notamment pour le transfert de fichiers de contenu tels que des images, des vidéos, des fichiers audios, des documents texte, etc. Les utilisateurs peuvent accéder au serveur FTP à l'aide d'un logiciel FTP, qui permet de télécharger et d'uploader des fichiers sur le serveur. Le serveur FTP est particulièrement utile pour partager des fichiers volumineux avec des clients ou partenaires, ainsi que pour les développeurs web qui travaillent sur le site web et qui doivent transférer des fichiers de code source entre différents environnements. Le serveur FTP peut également être utilisé pour la sauvegarde de fichiers, la synchronisation de fichiers et la gestion de versions.

5.3.3 - Serveur TSE

Le serveur TSE (Terminal Server Edition) est un type de serveur qui permet à plusieurs utilisateurs de se connecter simultanément au serveur à l'aide de clients légers ou de périphériques distants. Le serveur TSE fournit un environnement de bureau virtuel partagé où les utilisateurs peuvent exécuter des applications et accéder aux données stockées sur le serveur. L'utilisation d'un serveur TSE est particulièrement utile pour les employés qui ont besoin d'accéder à des applications et des données centralisées à partir de différents emplacements, car cela permet de réduire les coûts d'administration et de maintenance, tout en améliorant la sécurité et la fiabilité des données. En outre, les serveurs TSE sont souvent utilisés pour héberger des applications métier complexes qui nécessitent des ressources système importantes et qui peuvent être facilement gérées et déployées à partir du serveur centralisé.

5.3.4 - Serveur NAS

Le serveur NAS est un serveur qui permet aux utilisateurs autorisés d'accéder aux fichiers et aux données stockés sur celui-ci. Les utilisateurs peuvent également accéder au serveur NAS à distance via Internet, en utilisant des protocoles de partage de fichiers tels que SMB (Server Message Block) ou FTP (File Transfer Protocol).

Ce type de serveur est conçu pour être évolutif, ce qui signifie qu'il peut être facilement étendu en ajoutant des disques durs supplémentaires ou en mettant à niveau la capacité de stockage existante. Il est également sécurisé avec des mesures de protection avancées pour garantir la confidentialité et la sécurité des données stockées.

Enfin, le NAS peut également être utilisé pour sauvegarder les données de l'entreprise de manière régulière et automatisée. Les sauvegardes peuvent être programmées pour s'exécuter à intervalles réguliers, ce qui permet de minimiser le risque de perte de données en cas de défaillance du matériel ou de corruption des données. Ces serveur NAS serviront donc de serveur pour le RAID de l'entreprise (RAID en commun avec tous les sites).

5.3.5 - Serveur de gestion de logs

Un serveur de gestion de logs est un élément essentiel dans toutes infrastructure informatique. Il permet de collecter et de stocker toutes les données générées par les différents serveurs, applications et équipements connectés au réseau. L'un des avantages clés d'un serveur de gestion de logs est qu'il permet de surveiller l'activité d'une infrastructure informatique en temps réel. En collectant et en stockant tous les logs système, les logs d'applications, les logs de sécurité, les logs d'audit, et autres données pertinentes, il permet rapidement d'identifier les problèmes potentiels et les résoudre avant qu'ils ne deviennent des problèmes majeurs.
En effet, les logs sont une source importante d'informations sur l'activité de votre infrastructure informatique. Ils contiennent des informations sur les erreurs, les anomalies, les activités suspectes, les tentatives de piratage, les problèmes de performance, les pannes, les

interruptions, etc. En utilisant un serveur de gestion de logs, il est facile de trier, filtrer, analyser et visualiser ces données pour en extraire des informations utiles. Un autre avantage clé d'un serveur de gestion de logs est qu'il permet de répondre rapidement aux demandes d'audit et de conformité. Les entreprises sont tenues de respecter un certain nombre de réglementations et de normes, telles que le RGPD, la norme ISO 27001, PCI-DSS, etc. Ces normes imposent des exigences strictes en matière de collecte, de stockage et d'analyse des logs.
Avec un serveur de gestion de logs, il est facile de générer des rapports d'audit détaillés pour répondre à ces exigences. Enfin, un serveur de gestion de logs peut également être utilisé pour améliorer la performance de votre infrastructure informatique. En collectant et en analysant les logs de performance, il peut identifier les goulots d'étranglement, les processus lents et les problèmes de configuration. Cela permet donc d'optimiser les serveurs, les applications et votre réseau pour améliorer la vitesse et la fiabilité d'une infrastructure informatique.

5.3.6 - Serveur Web

Le serveur WEB que nous souhaitons utiliser pour le site de Nantes est un système informatique dédié à l'hébergement des sites web de l'entreprise. Il est configuré pour exécuter des logiciels serveurs tels qu'Apache, Nginx ou Microsoft IIS, qui permettent de répondre aux requêtes HTTP des clients web et de leur fournir des pages web.
Ce serveur WEB dispose d'un système d'exploitation optimisé pour les serveurs, tel que Linux ou Windows Server, qui est configuré pour fournir une haute disponibilité, une sécurité renforcée et une gestion efficace des ressources.

Avec une connexion à Internet haut débit, le serveur WEB permettra aux utilisateurs de naviguer sur le site web de l'entreprise de manière rapide et fluide. Il est également équipé de matériel réseau avancé, tel que des commutateurs et des routeurs, pour assurer une connectivité fiable et une bande passante suffisante pour le trafic web.

Le serveur WEB peut héberger différents types de sites web, tels que des sites statiques ou dynamiques, des blogs, des forums ou des applications web. Il prend en charge différents langages de programmation tels que PHP, Python, Ruby ou Java, ainsi que les bases de données MySQL, PostgreSQL ou SQL Server pour stocker les données de l'application.
Pour renforcer la sécurité du site, le serveur WEB est configuré avec des mesures de sécurité avancées, telles que des pares-feux, des certificats SSL/TLS pour le chiffrement des données, et des systèmes de détection d'intrusion pour protéger les sites web contre les attaques malveillantes.

Enfin, le serveur WEB est évolutif et peut être configuré pour s'adapter à l'évolution des besoins de l'entreprise. Il peut être équipé de ressources supplémentaires, telles que de la mémoire vive ou des processeurs, pour améliorer les performances du site web et garantir une expérience utilisateur de qualité.

5.3.7 - Serveur téléphonie

Le serveur téléphonique est un système de communication avancé qui permet de gérer les appels entrants et sortants de manière efficace et professionnelle. Ce serveur est équipé d'une interface utilisateur conviviale qui permet aux agents de prendre les appels et de les gérer de manière efficace.
Le serveur téléphonique dispose également de nombreuses fonctionnalités avancées telles que la gestion des files d'attente, la distribution des appels en fonction de critères tels que la disponibilité des agents, la langue de l'appelant ou la nature de l'appel. Il permet également d'enregistrer les appels pour des raisons de formation ou de suivi qualité. Le serveur téléphonique est relié à un système de messagerie vocale qui permet aux appelants de laisser un message si tous les agents sont occupés ou en dehors des heures d'ouverture. Les messages sont stockés sur le serveur et peuvent être récupérés et écoutés à tout moment.

Enfin, le serveur téléphonique est conçu pour être extensible et évolutif, ce qui signifie qu'il peut être facilement mis à jour ou étendu pour répondre aux besoins futurs de l'entreprise. Il est également sécurisé avec des mesures de protection avancées pour garantir la confidentialité et la sécurité des données des appelants. En résumé, le serveur téléphonique que nous mettons en place pour le site de Nantes est un système avancé et polyvalent qui permet une gestion efficace et professionnelle des appels entrants et sortants. Il offre de nombreuses fonctionnalités avancées et est conçu pour être évolutif et sécurisé.

5.3.8 - Serveur imprimante

Un serveur imprimante est un dispositif qui est connecté à un réseau et qui est utilisé pour gérer les impressions de documents à partir d'ordinateurs connectés à ce réseau. Les serveurs imprimantes sont généralement équipés d'un certain nombre de ports d'imprimante, ce qui permet à plusieurs utilisateurs d'imprimer des documents en même temps.
Le principal avantage d'un serveur imprimante est sa capacité à centraliser la gestion des impressions pour l'ensemble du réseau. Au lieu que chaque ordinateur soit équipé de son propre pilote d'imprimante et soit configuré individuellement, le serveur imprimante est configuré une seule fois pour l'ensemble du réseau. Cela facilite la gestion de l'ensemble du parc d'imprimantes de l'entreprise, en permettant une surveillance centralisée des niveaux d'encre ou de toner, des pannes de matériel, des mises à jour logicielles, etc. De plus, les serveurs imprimantes offrent des fonctionnalités supplémentaires qui peuvent être très utiles dans un environnement d'entreprise. Par exemple l'authentification et le contrôle d'accès ; les serveurs imprimantes peuvent être configurés pour exiger une authentification avant de permettre l'accès à certaines imprimantes ou à certaines fonctionnalités d'impression. Cela peut aider à renforcer la sécurité des documents confidentiels.
Certains serveurs imprimantes offrent des fonctionnalités supplémentaires telles que la gestion de la file d'attente d'impression, la possibilité de configurer des profils d'impression pour différents types de documents, ou encore la possibilité d'envoyer des travaux d'impression à une file d'attente à distance pour une impression ultérieure. Les serveurs imprimantes peuvent générer des rapports sur les travaux d'impression effectués, les niveaux d'encre ou de toner restants, les pannes de matériel, etc. Ces rapports peuvent être utilisés pour suivre les coûts

d'impression ou pour planifier la maintenance du parc d'imprimantes. Il est important de noter que les serveurs imprimantes peuvent être configurés de différentes manières en fonction des besoins de l'entreprise. Par exemple, certains serveurs imprimantes peuvent être configurés pour fonctionner comme des serveurs d'impression de bureau, tandis que d'autres peuvent être configurés pour fonctionner comme des serveurs d'impression de production pour les grandes quantités d'impression. Les serveurs imprimantes peuvent également être équipés de différents types de connectivité, tels que des connexions Ethernet, sans fil, ou USB, en fonction des besoins de l'entreprise.

5.3.9 - Serveur WSUS

Le serveur WSUS (Windows Server Update Services) que nous utilisons pour l'entreprise Rubik's Cube est un système informatique dédié à la gestion des mises à jour de sécurité et de fonctionnalités des systèmes d'exploitation et des logiciels de l'entreprise.
Il est configuré pour télécharger automatiquement les mises à jour de Microsoft depuis le serveur de mise à jour de Microsoft et les distribuer sur le réseau interne de l'entreprise. Les mises à jour peuvent être approuvées manuellement ou automatiquement avant leur déploiement sur les postes de travail et les serveurs de l'entreprise.
Le serveur WSUS est équipé d'une base de données SQL Server qui stocke les informations sur les mises à jour, les groupes d'ordinateurs et les règles de déploiement. Il est également configuré avec des rôles et des autorisations pour assurer la sécurité de la distribution des mises à jour. Le serveur WSUS peut être configuré pour déployer des mises à jour à des groupes d'ordinateurs spécifiques, en fonction de leurs besoins et de leur environnement de travail.
Les mises à jour peuvent également être programmées pour être installées automatiquement en dehors des heures de travail afin de ne pas perturber la productivité des utilisateurs. Le serveur WSUS permet également de générer des rapports détaillés sur les mises à jour installées, les erreurs de déploiement et l'état de la conformité des mises à jour pour chaque poste de travail ou serveur. Ces rapports peuvent être utilisés pour évaluer la santé de l'environnement informatique de l'entreprise et pour planifier les futures mises à jour.

5.3.10 - Serveur Active Directory

Le serveur AD ou Active Directory est un système informatique basé sur le protocole LDAP (Lightweight Directory Access Protocol) qui permet de centraliser et de gérer l'authentification et l'autorisation des utilisateurs, des ordinateurs et des ressources.

Les informations d'identification des utilisateurs et des ordinateurs sont stockées dans une base de données centrale qui permet aux administrateurs de définir des règles d'accès pour les ressources de l'entreprise, telles que les fichiers, les dossiers, les imprimantes, les applications, etc. Le serveur sera configuré pour fournir des services d'authentification et d'autorisation aux utilisateurs et aux ordinateurs du domaine de l'entreprise.

Il permet également aux administrateurs de gérer les comptes utilisateur, les groupes de sécurité, les stratégies de mot de passe, les profils utilisateur, etc. Le serveur AD est également

utilisé pour la gestion des stratégies de groupe (GPO) de l'entreprise. Les stratégies de groupe sont des règles de configuration qui peuvent être appliquées à un ensemble d'utilisateurs ou d'ordinateurs pour définir les paramètres de sécurité, les paramètres de configuration, les paramètres de logiciels, etc.

Le serveur AD sera ainsi équipé d'outils d'administration qui permettent aux administrateurs de gérer efficacement les comptes utilisateur et les ordinateurs du domaine. Ces outils incluent notamment la console d'administration Active Directory, la console de gestion des utilisateurs et des ordinateurs, la console de gestion des stratégies de groupe, etc.

5.3.11 - Serveur proxy antiviral

Le serveur proxy antiviral utilisé sera un serveur informatique qui sert d'intermédiaire entre un utilisateur et Internet tout en offrant une protection antivirus. Il permet aux utilisateurs d'accéder à Internet de manière plus sécurisée et efficace en bloquant les menaces potentielles telles que les virus, les logiciels malveillants et les attaques de phishing.

Ce type de serveur est souvent utilisé dans les entreprises pour gérer l'accès à Internet des employés tout en offrant une protection supplémentaire contre les cybers menaces. Il peut être configuré pour filtrer et bloquer les sites Web dangereux, les fichiers potentiellement malveillants et les courriels de phishing. De plus, le serveur proxy antiviral peut être utilisé pour réduire la bande passante nécessaire pour accéder à Internet, en stockant en cache les pages Web les plus fréquemment consultées.

Le serveur proxy antiviral peut également être utilisé pour améliorer la sécurité des utilisateurs en cachant leur adresse IP, en masquant leur identité en ligne et en protégeant leur vie privée en ligne. De plus, il peut aider à prévenir les attaques de type DDoS (Distributed Denial of Service) en limitant la bande passante utilisée pour accéder à un site Web.

6 - Charte informatique

6.1 - Introduction

L'entreprise Rubik's Cube possède de nombreux équipements informatiques, des logiciels, des données et des systèmes qui sont essentiels pour son fonctionnement quotidien. Il est donc important que tous les utilisateurs de ces ressources informatiques respectent les règles de sécurité pour éviter toute violation de données, toute atteinte à la confidentialité ou toute interruption de service. Cette charte informatique définit les règles et les bonnes pratiques à suivre pour garantir la sécurité et la confidentialité des données informatiques de l'entreprise Rubik's Cube. Elle est destinée à tous les employés, les prestataires de services et les visiteurs qui utilisent les ressources informatiques de l'entreprise, et elle est contraignante pour tous. Nous encourageons tous les utilisateurs à lire attentivement cette charte et à la respecter scrupuleusement pour protéger les informations sensibles de l'entreprise et pour garantir un environnement de travail sécurisé et efficace.

6.2 - Utilisation des équipements informatiques

6.2.1 - Matériel informatique

Tous les équipements informatiques de l'entreprise Rubik's Cube, tels que les ordinateurs, les serveurs, les imprimantes, les scanners, les disques durs externes, les clés USB et les téléphones mobiles, doivent être utilisés de manière responsable et en conformité avec les politiques de l'entreprise. Les équipements informatiques doivent être protégés contre les dommages, les pertes ou les vols. Tout équipement informatique défectueux doit être signalé immédiatement au service informatique.

6.2.2 - Logiciels

Les logiciels installés sur les équipements informatiques de l'entreprise Rubik's Cube ne doivent être utilisés que dans le cadre des activités professionnelles de l'entreprise. Les employés ne sont pas autorisés à installer ou à utiliser des logiciels non autorisés ou piratés. Tout logiciel nouvellement installé doit être approuvé par le service informatique.

6.2.3 - Accès à internet

Les employés sont autorisés à accéder à Internet pour les besoins professionnels de l'entreprise Rubik's Cube. L'utilisation d'Internet à des fins personnelles est autorisée pendant les pauses déjeuner ou à d'autres moments approuvés par la direction. Toutefois, l'utilisation d'Internet doit être faite de manière responsable et conformément aux politiques de sécurité de l'entreprise.

6.2.4 - Sauvegarde des données

Il est de la responsabilité de chaque employé de sauvegarder régulièrement les données importantes sur les équipements informatiques de l'entreprise Rubik's Cube. Les données doivent être sauvegardées sur le serveur central ou sur tout autre support de stockage autorisé par le service informatique. Les données confidentielles doivent être stockées sur des disques durs chiffrés ou sur tout autre support de stockage chiffré.

6.2.5 - Respect de la vie privée

Les employés doivent respecter la vie privée des autres employés et de toute personne tierce en évitant d'accéder à des données personnelles ou confidentielles sans autorisation. Tout accès non autorisé à des données personnelles ou confidentielles est strictement interdit. Les employés doivent également protéger leurs propres données personnelles et confidentielles en utilisant des mots de passe complexes et en évitant de divulguer des informations sensibles à des tiers non autorisés.

6.2.6 - Gestion des mots de passe

Les employés doivent protéger les mots de passe de manière appropriée. Les mots de passe doivent être complexes, uniques et doivent être changés régulièrement. Les employés ne doivent pas divulguer leur mot de passe à quiconque, même à leur responsable hiérarchique. Si un employé suspect que son mot de passe a été compromis, il doit le signaler immédiatement au service informatique.

6.2.7 - Utilisation des équipements personnels

L'utilisation d'équipements personnels pour le stockage ou le traitement de données de l'entreprise Rubik's Cube est strictement interdite, à moins que cela ne soit expressément autorisé par la direction. Les employés doivent éviter de brancher des équipements personnels tels que des clés USB, des disques durs externes ou des smartphones sur les équipements informatiques de l'entreprise sans autorisation. En outre, les employés ne doivent pas utiliser leur propre matériel informatique pour accéder aux données de l'entreprise Rubik's Cube sans autorisation.

6.2.8 - Respect des politiques de sécurité

Tous les employés de l'entreprise Rubik's Cube doivent respecter les politiques de sécurité en matière d'utilisation des équipements informatiques. Les politiques de sécurité doivent être lues et comprises par tous les employés de l'entreprise. Les employés doivent signaler tout comportement suspect ou violation de la sécurité de l'information au service informatique.

6.2.9 - Sanctions en cas de non-respect des politiques

Le non-respect des politiques de sécurité en matière d'utilisation des équipements informatiques peut entraîner des sanctions disciplinaires, y compris un avertissement verbal ou écrit, une suspension ou une résiliation du contrat de travail. Les employés sont également tenus responsables des dommages ou pertes causés à l'entreprise Rubik's Cube en raison d'une utilisation abusive ou inappropriée des équipements informatiques.
En respectant les politiques et les pratiques de sécurité informatique, chaque employé peut contribuer à maintenir un environnement de travail sûr et protégé pour l'ensemble de l'entreprise Rubik's Cube.

6.2 - Utilisation des logiciels

6.2.1 - Utilisation des logiciels autorisés

Tous les employés de l'entreprise Rubik's Cube doivent utiliser uniquement les logiciels autorisés par le service informatique de l'entreprise. Les logiciels non autorisés peuvent entraîner des problèmes de compatibilité, de sécurité ou de performances des équipements informatiques de l'entreprise. Les employés ne doivent pas installer de nouveaux logiciels sur les équipements informatiques de l'entreprise sans l'autorisation préalable du service informatique.

6.2.2 - Utilisation de logiciels sous licence

L'utilisation de logiciels sous licence piratée ou non autorisée est strictement interdite. Les employés doivent s'assurer que les logiciels utilisés sur les équipements informatiques de l'entreprise sont dûment autorisés et enregistrés. Toute violation de cette politique sera considérée comme une infraction grave, pouvant entraîner des sanctions disciplinaires, y compris une résiliation du contrat de travail et une action en justice.

6.2.3 - Mise à jour des logiciels

Les employés doivent régulièrement vérifier la disponibilité des mises à jour des logiciels utilisés sur les équipements informatiques de l'entreprise et les installer dès qu'elles sont disponibles. Les mises à jour sont importantes pour assurer la sécurité et les performances des équipements informatiques de l'entreprise.

6.2.4 - Respect des licences d'utilisation

Les licences d'utilisation des logiciels doivent être respectées. Les employés ne doivent pas distribuer, copier, installer ou utiliser des logiciels en violation des termes et conditions de la licence d'utilisation. Toute violation de cette politique sera considérée comme une infraction

grave, pouvant entraîner des sanctions disciplinaires, y compris une résiliation du contrat de travail et une action en justice.

6.2.5 - Utilisation de logiciels de sécurité

Les employés doivent utiliser les logiciels de sécurité recommandés par le service informatique de l'entreprise pour protéger les équipements informatiques et les données de l'entreprise contre les virus, les logiciels malveillants et les attaques de hackers. Les employés doivent maintenir les logiciels de sécurité à jour pour une protection optimale.
En respectant les politiques et les pratiques d'utilisation des logiciels, chaque employé peut contribuer à assurer la sécurité et la performance des équipements informatiques de l'entreprise Rubik's Cube.

6.3 - Sécurité des données

6.3.1 - Protection des données confidentielles

Les employés de l'entreprise Rubik's Cube doivent protéger les données confidentielles de l'entreprise contre les accès non autorisés et les fuites. Les données confidentielles peuvent inclure des informations sur les clients, les fournisseurs, les stratégies de l'entreprise, les secrets commerciaux et les données personnelles des employés. Les employés ne doivent accéder qu'aux données qui leur sont nécessaires pour exécuter leurs tâches professionnelles. Les données confidentielles doivent être stockées dans des espaces de stockage sécurisés, tels que des serveurs protégés par des mots de passe et des autorisations d'accès spécifiques.

6.3.2 - Protection contre les virus et les logiciels malveillants

Les employés doivent protéger les équipements informatiques de l'entreprise contre les virus et les logiciels malveillants en utilisant les logiciels de sécurité recommandés par le service informatique. Les employés ne doivent pas ouvrir les fichiers suspects ou télécharger des logiciels non autorisés.

6.3.3 - Utilisation de mots de passe forts

Les employés doivent utiliser des mots de passe forts pour accéder aux équipements informatiques et aux applications de l'entreprise. Les mots de passe doivent être suffisamment complexes pour empêcher les attaques de deviner les mots de passe en utilisant des programmes automatisés. Les employés ne doivent pas partager leurs mots de passe avec d'autres personnes et doivent les changer régulièrement.

6.3.4 - Politique de sauvegarde des données

Les employés doivent suivre la politique de sauvegarde des données de l'entreprise pour garantir que les données importantes sont sauvegardées régulièrement. Les sauvegardes doivent être stockées dans des endroits sécurisés pour assurer la disponibilité des données en cas de sinistre ou de panne du système.

6.3.5 - Politique de destruction des données

Les employés doivent suivre la politique de destruction des données de l'entreprise pour garantir que les données confidentielles sont effacées de manière sécurisée lorsqu'elles ne sont plus nécessaires. Les données confidentielles doivent être détruites de manière à empêcher leur récupération ultérieure.
En suivant les politiques de sécurité des données de l'entreprise Rubik's Cube, les employés peuvent contribuer à assurer la sécurité et la confidentialité des données de l'entreprise.

6.4 - Utilisation d'internet

6.4.1 - Utilisation professionnelle d'Internet

L'utilisation d'Internet pour des activités professionnelles est autorisée et encouragée. Les employés doivent utiliser Internet pour accéder à des ressources liées à leur travail, telles que des sites Web de fournisseurs, des sites Web de recherche, des sites Web de formation et des sites Web de réseaux professionnels. Toutefois, les employés ne doivent pas passer un temps excessif sur Internet, ni utiliser les ressources d'Internet pour des activités non liées à leur travail.

6.4.2 - Politique de sécurité d'Internet

Les employés doivent prendre des mesures de sécurité appropriées lors de l'utilisation d'Internet, afin de protéger les données de l'entreprise et de réduire les risques de virus et de logiciels malveillants. Les mesures de sécurité comprennent la vérification des sites Web avant de télécharger des fichiers, l'installation et la mise à jour régulière d'un logiciel antivirus et pare-feu, la mise en place de mots de passe sécurisés et la mise à jour régulière des logiciels.

6.4.3 - Interdiction de télécharger du contenu illégal

Il est interdit de télécharger, de partager ou d'accéder à du contenu illégal, tel que des films, de la musique ou des logiciels piratés, sur les équipements informatiques de l'entreprise. Les employés ne doivent pas utiliser les ressources d'Internet pour des activités illégales ou pour transmettre des informations confidentielles de l'entreprise à des tiers.

6.4.4 - Respect des droits d'auteur

Les employés doivent respecter les droits d'auteur et les lois sur la propriété intellectuelle lorsqu'ils utilisent des informations ou des images trouvées sur Internet. Il est interdit de reproduire, d'afficher ou de distribuer des œuvres protégées par des droits d'auteur sans l'autorisation du détenteur des droits.
En suivant les politiques d'utilisation d'Internet de l'entreprise Rubik's Cube, les employés peuvent contribuer à assurer la sécurité et la légalité de l'utilisation d'Internet pour les activités professionnelles.

6.5 - Utilisation de la messagerie électronique

6.5.1 - Utilisation professionnelle de la messagerie électronique

L'utilisation de la messagerie électronique pour des activités professionnelles est autorisée et encouragée. Les employés doivent utiliser la messagerie électronique pour communiquer avec des collègues, des clients et des fournisseurs concernant des questions professionnelles. Toutefois, les employés ne doivent pas passer un temps excessif sur la messagerie électronique, ni utiliser la messagerie électronique pour des activités non liées à leur travail.

6.5.2 - Politique de sécurité de la messagerie électronique

Les employés doivent prendre des mesures de sécurité appropriées lors de l'utilisation de la messagerie électronique, afin de protéger les données de l'entreprise et de réduire les risques de virus et de logiciels malveillants. Les mesures de sécurité comprennent la vérification des pièces jointes avant de les télécharger, l'installation et la mise à jour régulière d'un logiciel antivirus et pare-feu, la mise en place de mots de passe sécurisés et la mise à jour régulière des logiciels.

6.5.3 - Interdiction de la transmission de messages offensants ou inappropriés

Il est interdit de transmettre des messages offensants ou inappropriés par le biais de la messagerie électronique de l'entreprise. Les employés doivent respecter les normes de conduite professionnelle lors de l'utilisation de la messagerie électronique et éviter les commentaires offensants, discriminatoires ou dégradants.

6.5.4 - Interdiction de transmettre des informations confidentielles

Il est interdit de transmettre des informations confidentielles de l'entreprise par le biais de la messagerie électronique. Les employés ne doivent pas utiliser la messagerie électronique pour

transmettre des informations confidentielles telles que des mots de passe, des informations de compte ou des données de clients à des tiers non autorisés.

6.5.5 - Archivage des messages électroniques

Les employés doivent archiver les messages électroniques pertinents dans un dossier approprié pour une utilisation future ou une référence rapide. Les messages électroniques doivent être archivés conformément à la politique de l'entreprise sur la conservation des documents.
En suivant les politiques d'utilisation de la messagerie électronique de l'entreprise Rubik's Cube, les employés peuvent contribuer à assurer la sécurité et la légalité de l'utilisation de la messagerie électronique pour les activités professionnelles.

7 - Charte informatique complémentaire

7.1 - Introduction

7.1.1 - Objectifs de la charte informatique

La présente charte informatique a pour objectif de garantir la sécurité des informations et des équipements informatiques, de protéger la propriété intellectuelle de l'entreprise Rubik's Cube, de définir les droits et les responsabilités des utilisateurs, de favoriser l'utilisation efficace et responsable des équipements et des logiciels informatiques, et de respecter les lois et les réglementations en matière de sécurité informatique. Les objectifs de cette charte sont essentiels pour assurer le bon fonctionnement des services STEDesign et R&D de l'entreprise.

7.1.2 - Contexte et porté de la charte informatique

La charte informatique s'applique aux services STEDesign et R&D de l'entreprise Rubik's Cube sur le site de Nantes. Elle est destinée à être respectée par l'ensemble des utilisateurs de l'informatique au sein de ces services. Cette charte est importante pour assurer la sécurité des informations et des équipements informatiques de l'entreprise et pour clarifier les droits et les responsabilités des utilisateurs.

7.2 - Utilisation des logiciels

7.2.1 - Présentation des logiciels

Les services STEDesign et R&D de l'entreprise Rubik's Cube utilisent des logiciels professionnels puissants tels que Cinema 4D, SolidWorks, Adobe After Effects et Adobe Premiere Pro. Ces logiciels sont utilisés pour la conception, la modélisation, l'animation et la production de vidéos et d'images pour les produits Rubik's Cube ainsi que pour la recherche et le développement de nouveaux produits.

7.2.2 - Droits d’utilisation

Les utilisateurs ont le droit d'utiliser ces logiciels à des fins professionnelles, conformément aux licences d'utilisation et aux contrats de service en vigueur. Les utilisateurs doivent prendre soin des logiciels et signaler tout problème technique ou de licence à la direction de l'entreprise.

7.2.3 - Règles d’utilisation

Les utilisateurs sont tenus de respecter les règles suivantes lorsqu'ils utilisent les logiciels :
Les utilisateurs ne doivent pas installer, modifier ou supprimer des logiciels sans autorisation préalable de la direction de l'entreprise.
Les utilisateurs doivent utiliser les logiciels conformément aux procédures et aux modes d'emploi recommandés par les éditeurs des logiciels.
Les utilisateurs ne doivent pas copier, reproduire ou distribuer des logiciels sans autorisation préalable de la direction de l'entreprise.
Les utilisateurs ne doivent pas utiliser des logiciels piratés ou des copies illégales de logiciels.
Les utilisateurs doivent protéger les logiciels contre les virus informatiques et autres menaces de sécurité.

7.2.4 - Responsabilité des utilisateurs

Les utilisateurs sont responsables de l'utilisation des logiciels qui leur sont confiés. Ils doivent s'assurer que l'utilisation des logiciels ne viole pas les droits d'auteur ou les autres droits de propriété intellectuelle. Ils doivent également signaler tout problème de sécurité ou de conformité lié à l'utilisation des logiciels à la direction de l'entreprise.

7.2.5 - Sécurité des données

Les utilisateurs doivent prendre toutes les mesures nécessaires pour garantir la sécurité et la confidentialité des données stockées sur les logiciels, conformément à la politique de sécurité de l'entreprise. Les utilisateurs doivent utiliser des mots de passe complexes et ne doivent pas partager leurs identifiants de connexion. Ils doivent également sauvegarder régulièrement les données pour éviter toute perte de données due à une défaillance du système.

7.2.6 - Contrôle et surveillance

L'entreprise se réserve le droit de contrôler et de surveiller l'utilisation des logiciels pour garantir la conformité aux règles et aux politiques de l'entreprise. Les utilisateurs doivent coopérer pleinement avec toute enquête menée par la direction de l'entreprise en cas de violation présumée de cette charte ou de toute autre politique de l'entreprise.

7.3 - Sécurité informatique

7.3.1 - Accès aux données

Les utilisateurs des services STEDesign et R&D ne doivent accéder qu'aux données qui leur sont nécessaires pour remplir leurs fonctions professionnelles. L'entreprise Rubik's Cube mettra en place des mesures de sécurité pour garantir que les données sensibles sont accessibles uniquement par les personnes autorisées. Les utilisateurs sont tenus de protéger les données sensibles contre toute perte, vol ou divulgation non autorisée.

7.3.2 - Sécurité des ordinateurs

Les utilisateurs doivent protéger leur ordinateur en utilisant un antivirus et un pare-feu, ainsi qu'en mettant à jour régulièrement leur système d'exploitation et leurs logiciels. Les utilisateurs ne doivent pas installer de logiciels non autorisés ou de logiciels provenant de sources non fiables.

7.3.3 - Gestion des mots de passe

Les utilisateurs doivent utiliser des mots de passe complexes et ne doivent pas partager leurs identifiants de connexion. Les mots de passe doivent être changés régulièrement, au moins tous les 90 jours. Les mots de passe ne doivent pas être stockés en clair ou dans un fichier non crypté sur l'ordinateur ou dans un lieu facilement accessible.

7.3.4 - Sécurité des réseaux

Les utilisateurs doivent protéger les réseaux de l'entreprise en ne connectant que des équipements approuvés et en ne partageant pas leur accès Internet avec des tiers. Les utilisateurs ne doivent pas utiliser de réseaux publics non sécurisés pour accéder aux données de l'entreprise.

7.3.5 - Politique de sauvegarde des données

Les utilisateurs sont tenus de sauvegarder régulièrement les données pour éviter toute perte de données due à une défaillance du système. Les données sensibles doivent être sauvegardées sur des supports de stockage cryptés et sécurisés.

7.3.6 - Gestion des incidents de sécurité

Les utilisateurs doivent signaler tout incident de sécurité ou toute violation présumée de la sécurité à la direction de l'entreprise. L'entreprise Rubik's Cube mettra en place une procédure

pour gérer les incidents de sécurité, y compris la notification des autorités compétentes en cas de violation de données à caractère personnel.

7.3.7 - Sensibilisation à la sécurité

Les utilisateurs des services STEDesign et R&D seront formés à la sécurité informatique et seront régulièrement informés des risques de sécurité informatique et des mesures de protection à prendre. L'entreprise Rubik's Cube organisera des campagnes de sensibilisation à la sécurité pour encourager les utilisateurs à adopter des comportements de sécurité informatique appropriés.

7.4 - Utilisation des équipements informatiques

7.4.1 - Ordinateurs et équipements

Les utilisateurs des services STEDesign et R&D seront formés à la sécurité informatique et seront régulièrement informés des risques de sécurité informatique et des mesures de protection à prendre. L'entreprise Rubik's Cube organisera des campagnes de sensibilisation à la sécurité pour encourager les utilisateurs à adopter des comportements de sécurité informatique appropriés.

7.4.2 - Périphériques de stockage

Les périphériques de stockage externes (tels que les clés USB, les disques durs externes, etc.) doivent être utilisés uniquement pour stocker des données liées aux activités professionnelles de l'entreprise. Les données stockées sur ces périphériques doivent être chiffrées et protégées par mot de passe.

7.4.3 - Imprimantes et photocopieuses

Les utilisateurs des services STEDesign et R&D ne doivent imprimer que les documents nécessaires à l'exercice de leurs fonctions professionnelles. Les utilisateurs ne doivent pas imprimer de documents contenant des données sensibles ou confidentielles sans autorisation préalable.

7.4.4 - Utilisation des équipements à distance

Les utilisateurs sont autorisés à utiliser les équipements informatiques de l'entreprise à distance, à condition de respecter les politiques de sécurité informatique et les mesures de protection

mises en place par l'entreprise. Les utilisateurs ne doivent pas divulguer leurs identifiants de connexion ou partager leur accès à distance avec des tiers non autorisés.

7.4.5 - Destruction des données

Les utilisateurs sont tenus de supprimer toutes les données stockées sur leur ordinateur ou tout autre équipement informatique fourni par l'entreprise avant de quitter leur emploi ou lorsque l'équipement n'est plus utilisé pour les activités professionnelles de l'entreprise. Les utilisateurs ne doivent pas supprimer de données sensibles ou confidentielles sans autorisation préalable.

7.4.6 - Utilisation des équipements personnels

Les utilisateurs ne doivent pas utiliser leurs équipements informatiques personnels pour stocker des données professionnelles sensibles ou confidentielles, ni pour accéder aux systèmes informatiques de l'entreprise sans autorisation préalable. L'entreprise Rubik's Cube ne peut pas garantir la sécurité des équipements personnels utilisés à des fins professionnelles.

7.5 - Responsabilité des utilisateurs

7.5.1 - Protection des données

Les utilisateurs sont responsables de la protection des données de l'entreprise auxquelles ils ont accès. Les utilisateurs ne doivent pas divulguer d'informations sensibles ou confidentielles à des tiers non autorisés, ni les copier ou les transférer sur des supports externes sans autorisation préalable. Les utilisateurs doivent signaler immédiatement toute violation de sécurité ou toute activité suspecte à leur responsable hiérarchique.

7.5.2 - Respect de la propriété intellectuelle

Les utilisateurs doivent respecter la propriété intellectuelle de l'entreprise, ainsi que celle des tiers. Les utilisateurs ne doivent pas utiliser des logiciels, des fichiers ou tout autre contenu protégé par des droits d'auteur sans autorisation préalable. Les utilisateurs ne doivent pas copier, distribuer ou modifier des logiciels ou des données appartenant à l'entreprise sans autorisation préalable.

7.5.3 - Respect des lois et des règlements

Les utilisateurs doivent respecter toutes les lois et les règlements en vigueur relatifs à l'utilisation des technologies de l'information et de la communication. Les utilisateurs ne doivent pas utiliser

les équipements informatiques de l'entreprise à des fins illégales ou inappropriées. Les utilisateurs doivent également respecter les politiques de l'entreprise concernant l'utilisation des équipements informatiques.

7.5.4 - Formation et sensibilisation

Les utilisateurs sont tenus de suivre les formations en matière de sécurité informatique proposées par l'entreprise, ainsi que de participer aux campagnes de sensibilisation à la sécurité informatique. Les utilisateurs doivent également être en mesure d'identifier les menaces de sécurité et de signaler immédiatement toute activité suspecte à leur responsable hiérarchique.

7.5.5 - Sanctions en cas de non-respect

Le non-respect des dispositions de cette charte informatique complémentaire peut entraîner des sanctions disciplinaires, y compris un avertissement, une suspension ou une résiliation du contrat de travail. Les sanctions peuvent être prises à l'encontre de tout utilisateur qui viole cette charte, quelle que soit sa fonction ou son statut au sein de l'entreprise.

7.5.6 - Mise à jour de la charte

La présente charte peut être modifiée par l'entreprise à tout moment. Les utilisateurs sont tenus de prendre connaissance de toute modification de la charte et de se conformer aux nouvelles dispositions.

7.6 - Conclusion

Cette charte informatique complémentaire a pour objectif de garantir l'utilisation sûre et responsable des équipements et des logiciels informatiques de l'entreprise par les utilisateurs des services STEDesign et R&D sur le site de Nantes. Les utilisateurs sont tenus de respecter les règles de sécurité et de confidentialité énoncées dans cette charte, ainsi que les lois et les réglementations en vigueur.

La sécurité informatique est une responsabilité partagée. L'entreprise fournit des équipements et des logiciels de qualité, ainsi que des formations et des sensibilisations pour aider les utilisateurs à se protéger contre les menaces de sécurité informatique. Cependant, les utilisateurs sont également tenus de jouer un rôle actif en matière de sécurité informatique en respectant les règles énoncées dans cette charte et en signalant toute activité suspecte.

Enfin, cette charte est un document vivant et peut être modifiée par l'entreprise à tout moment. Les utilisateurs sont tenus de prendre connaissance des nouvelles dispositions et de se conformer à ces dernières. Tout non-respect des dispositions de cette charte peut entraîner des sanctions disciplinaires.

Nous espérons que cette charte informatique complémentaire permettra aux utilisateurs des services STEDesign et R&D de travailler de manière efficace et sécurisée sur les équipements et les logiciels informatiques de l'entreprise.