Infrastructure d’une PME avec deux sites distants

Fontana Andrea

Av. de la Gare 14

1450, Ste-Croix

cpnv
Centre professionnel du Nord vaudois
Filière d'informatique

SI-CA2a

07.04.2025

Table des matières

1 Analyse préliminaire 4
1.1 Introduction 4
1.2 Organisation 4
1.3 Objectifs 4
1.4 Méthode de travail 5
1.5 Planification initiale 6
1.6 Structure du dossier 7
1.7 Gestion des versions et sauvegarde du travail 7

2 Analyse 8
2.1 Cahier des charges détaillé 8
2.1.1 Définition du contenu et des fonctionnalités 12
2.1.2 Situation actuelle 12
2.1.3 Utilisateurs cibles 12
2.1.4 Présentation des solutions matérielles et logiciels 12
2.2 Solution Choisie 13
2.3 Etude de faisabilité 13
2.4 Stratégie de test 13

3 Conception 15
3.1 Plans topologiques 15
3.1.1 Topologie Hybride Logique/physique 15
3.1.2 Conventions de dénomination et d'adressage 15
3.1.3 Structures logiques et arborescences 16
3.2 Mise en place de la Sécurité 18

4 Réalisation et mise en service 19
4.1 Description des tests effectués 21
4.2 Erreurs restantes 22
4.3 Liste des documents fournis et dossier d'archivage 22

5 Conclusions 22

6 Annexes 22
6.1 Sources – Bibliographie 22
6.1.1 Intelligences Artificielles : 22

6.1.2 Sites internet : 22
6.1.3 Personnes extérieures au projet : 23
6.2 Glossaire 23
6.3 Table des illustrations 23
6.4 Journal de bord 23

1 Analyse préliminaire

1.1 Introduction

Ce projet a pour objectif de concevoir et de mettre en place une infrastructure informatique complète pour une petite entreprise fictive Kicroit basée à Bullet. L'entreprise cherche à se développer et veux repenser toute son infrastructure réseau pour incorporer une succursale à Lausanne. La sécurité des données est une prérogative pour l'entreprise.

Le choix de sujet s'explique par mon intérêt marqué pour l'administration des systèmes et réseaux. Ce projet me permet d'approfondir mes compétences techniques dans un contexte concret et d'acquérir une expérience précieuse dans la mise en œuvre de solutions informatiques adaptées aux besoins spécifiques d'une organisation. De plus, il constitue une opportunité d'appliquer mes connaissances actuelles en réseau (Lan, Vlan, VPN, …), en gestion des services Windows Server (Active Directory, DNS, DHCP, …) et en configuration de solutions de stockage centralisé comme le NAS.

Pour l'école ce projet permet de mettre en application ce qui m'a été enseigné. Il permet également de valoriser la formation en illustrant la mise en œuvre de solutions modernes et adaptées aux exigences du marché du travail.

L'infrastructure proposée comprendra la mise en place d'un réseau structuré autour d'un serveur Windows en assurant les services de bases tels que l'authentification des utilisateurs (AD), la gestion des ressources réseau (DHCP, DNS), la gestion de fichier et un pool d'impression. La sauvegarde des données sera sécurisée via un NAS Synology. De plus la sécurité sera assurée par un Firewall. Enfin la connexion VPN site à site se fera par l'intermédiaire de deux routeur Sisco.

Ainsi, ce projet permettra d'approfondir mes compétences en gestion d'infrastructure IT tout en répondant aux besoins concrets de l'entreprise, en proposant une solution adaptée, sécurisée et évolutive.

1.2 Organisation

Élève : Fontana Andrea, andrea.fontana@eduvaud.ch, 078 635 58 59

Chef de projet : Vitor Coval, vitor.coval@eduvaud.ch, 079 784 52 81

Expert 1: Daniel Berney, daniel.berney@heig-vd.ch, 079 209 87 93

Expert 2: Cédric Schaffter, cedric_schaffter@outlook.com, 076 822 41 27

1.3 Objectifs

Les objectifs à atteindre durant ce projet sont les suivants :

Installer et configurer l'infrastructure réseau d'une petite entreprise.

- Installer deux routeurs
- Installer un firewall
- Installer un serveur : DHCP, DNS, AD, Serveur d'impression, Serveur de fichier.

- Installer un serveur pour la redondance
- Configurer deux imprimantes
- Configurer trois postes de travail
- Installer deux Access Point
- Installer un serveur de Back up sur un NAS.
- Installer deux Switchs PoE
- Connecter deux routeurs distants et les appareils qui en découlent via VPN

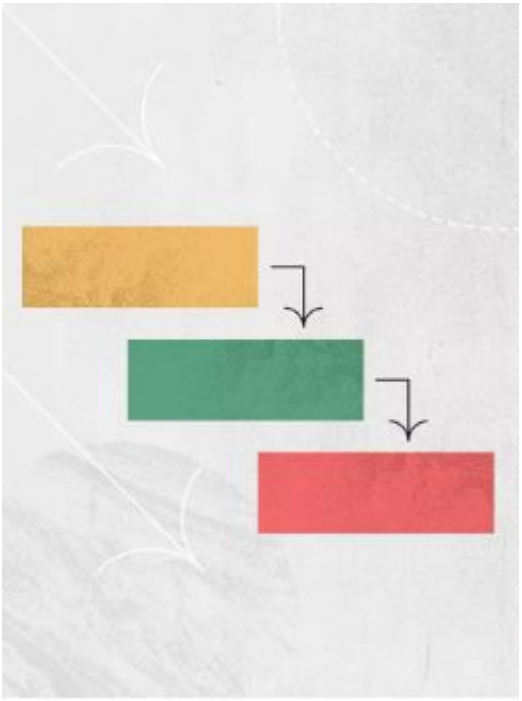
Critères de validation des objectifs :

- Le schéma de l'infrastructure réseau doit être complet et explicite.
- Les services AD, DNS, DHCP, FS et impression doivent être fonctionnels et redondants.
- Le tunnel IPSEC doit être fonctionnel et sont installation doit être précisément documentée.
- Le firewall doit respecter les règles de sécurité de base.
- Les access point doivent être correctement configurés.
- Le NAS doit effectuer un back up des données contenues sur le serveur complet et un back up incrémentiel. L'installation doit être clairement documentée.
- Les appareils ne doivent pas pouvoir communiquer entre eux que lorsque que c'est nécessaire.
- Les imprimantes doivent être installées et visibles sur le réseau.

1.4 Méthode de travail

Pour ce projet la méthode de travail Waterfall[1] est la plus adaptée. C'est une méthodologie de gestion de projet séquentielle, organisée en plusieurs phases, ou chaque phase dépend de la dernière.

[1] https://asana.com/fr/resources/waterfall-project-management-methodology



Ce projet applique ce processus. En effet il n'est pas possible de réaliser la mise en place de l'infrastructure si l'analyse préliminaire n'a pas été faite. De même il n'est pas possible d'effectuer des tests si la réalisation n'est pas encore effectuée. Cette méthode est donc la plus adaptée au projet. Cependant toutes les étapes d'un Waterfall « classique » ne sont pas nécessaires. Voici donc les étapes qui seront appliquées ici :

Définition des besoins

Durant cette phase le cahier des charges est analysé pour en ressortir les objectifs et les difficultés.

Conception de l'infrastructure

Durant cette phase les moyens déployés pour répondre aux objectifs sont définis. Les solutions apportées sont référencées et explicitées.

Mise en œuvre

Durant cette phase l'infrastructure réseau est mise en place conformément à la conception.

Tests

Durant cette phase les différents tests imaginés durant la conception sont réalisés et les erreurs potentielles sont documentées et corrigées.

Il est à noter que pour faciliter la résolution de problèmes certains tests seront réalisés durant la phase de mise en œuvre afin de limiter l'impacte sur le reste de la réalisation. Cependant les tests ne pouvant être fait qu'après la mise en service de l'appareil la chronologie est respectée.

1.5 Planification initiale

1.6 Structure du dossier

Ce dossier est structuré en fonction des différentes étapes du projet. Il débute par une introduction qui présente les grandes lignes du projet. Ensuite vient l'analyse qui développe les solutions envisagées ainsi que les objectifs du projet. La conception apporte des éléments concrets qui correspondent aux besoins identifiés durant l'analyse. La réalisation est l'étape qui décrit les tâches effectuées, les problèmes rencontrés et les problèmes persistants. Enfin la conclusion vient résumer le dossier et apporte une ouverture sur les améliorations possibles du projet.

1.7 Gestion des versions et sauvegarde du travail

Afin de garantir l'intégrité des données, la règle du 3-2-1 est mise en place. Cette règle recommande d'avoir au moins trois copies des données dans deux lieus de stockages différents et une copie hors site. Les documents produits sont sauvegardés en trois points distincts. Le premier est l'ordinateur de travail présent à Sainte-Croix, le deuxième est une clé USB présente aussi à Sainte-Croix et le troisième est un repository GitHub[2]. Chaque fichier est sauvegardé en local après modification et une sauvegarde complète du dossier est effectuée durant la dernière période de chaque journée sur la clé USB et push sur GitHub.

[2]https://github.com/andreafont/TPI-Infrastrucutre-d-une-PME-avec-deux-sites-distants/tree/main

2 Analyse

2.1 Cahier des charges détaillé

1 INFORMATIONS GENERALES

Candidat :	Nom : **FONTANA**	Prénom : **ANDREA**
	🖃 : andrea.fontana@eduvaud.ch	☎ : 078 635 58 59
Lieu de travail :	☐ CPNV, Rue de la Gare 14, 1450 Sainte-Croix	
Orientation :	☐ 88601 Développement d'application ☐ 88602 Informatique d'entreprise ☐ 88603 Technique des systèmes ☒ 88614 Informaticienne d'entreprise CFC	
Chef de projet :	Nom : COVAL	Prénom : Vitor
	🖃 : vitor.coval@eduvaud.ch	☎ : 079 784 52 81
Expert 1 :	Nom : BERNEY	Prénom : Daniel
	🖃 : daniel.berney@heig-vd.ch	☎ : 079 209 87 93
Expert 2 :	Nom : SCHAFFTER	Prénom : Cédric
	🖃 : cedric_schaffter@outlook.com	☎ : 076 822 41 27
Période de réalisation :	Du **lundi 7 avril 2025 à 8h15** au **mercredi 14 mai 2025 à 10h40**	
Horaire de travail :	Lundi 08h15-12h30 13h20-15h50 Mardi 08h15-10h50 13h20-16h40 Mercredi 08h15-12h30 13h20-15h50 Jeudi 08h15-12h30 - Vendredi 08h15-11h40 - *Toutes les demi-journées ont une pause obligatoire de 15 minutes le matin et de 10 minutes l'après-midi, sauf si elles commencent à 10h05 ou si elles se terminent à 14h55. Les vacances scolaires auront lieu du 12 avril 2025 au 27 avril 2025.*	
Nombre d'heures :	90 heures	
Planning (en H ou %)	Analyse 20%, Implémentation 40%, Tests 15%, Documentation 25%	
Présentation :	Dates retenues : 27 ou 28 mai 2025	

2 PROCÉDURE

Le candidat réalise un travail personnel sur la base d'un cahier des charges reçu le 1er jour.

Le cahier des charges est approuvé par les deux experts. Il est en outre présenté, commenté et discuté avec le candidat. Par sa signature, le candidat accepte le travail proposé.

Le candidat a connaissance de la feuille d'appréciation avant de débuter le travail.

Le candidat est entièrement responsable de la sécurité de ses données.

En cas de problèmes graves, le candidat avertit au plus vite les deux experts et son CdP.

Le candidat a la possibilité d'obtenir de l'aide, mais doit le mentionner dans son dossier.

A la fin du délai imparti pour la réalisation du TPI, le candidat doit transmettre par courrier électronique le dossier de projet aux deux experts et au chef de projet. En parallèle, une copie papier du rapport doit être fournie sans délai en trois exemplaires (L'un des deux experts peut demander à ne recevoir que la version électronique du dossier). Cette dernière doit être en tout point identique à la version électronique.

3 TITRE

Infrastructure d'une PME avec deux sites distants

4 MATÉRIEL ET LOGICIEL À DISPOSITION

2 Routeurs Cisco 1921

1 Firewall Fortinet FG-50E

1 Serveur HP Proliant MicroServer Gen10

1 Serveur redondant HP Proliant MicroServer Gen10

1 NAS Synology DS923+

2 AP Cisco Aironet AIR-SAP2602I-E-K9

3 Ordinateurs (1 poste client fixe DELL Optiplex 9020 et deux mobiles DELL Latitude E6520)

2 Imprimantes DCP-L8400CDN

2 Switchs Cisco Catalyst 3560

5 PRÉREQUIS

Avoir suivi les modules 117, 123, 126, 127, 129, 143, 146, 159, 182, 304, 305.

Le candidat maitrise les divers concepts réseau et système, a déjà utilisé divers outils de sauvegarde

6 DESCRIPTIF DU PROJET

La société Kicroit (société fictive) est une petite entreprise familiale basée à Bullet.

Son activité principale nécessitant la proximité d'un centre urbain, de nouveaux locaux ont été acquis en ville de Lausanne.

N'ayant pas de parc informatique – les employés utilisaient les fichiers sur leurs ordinateurs et se les partageaient par email – il faut créer toute l'infrastructure réseau.

Sur le site de Bullet il faut installer un serveur avec les services AD, DNS, DHCP, FS (sur le NAS) et impression. Une solution de sauvegarde doit être effectuée sur le NAS (complète les samedis 01h00 et incrémentielle du Mardi au Vendredi 01h00). Les utilisateurs doivent avoir accès à Internet. Un serveur de redondance/backup des services AD, DNS, DHCP, FS et impression doit aussi être installé.

Les employés sur le site de Lausanne doivent pouvoir accéder aux services proposés à Bullet. Ils accèdent aux mêmes serveurs à travers une connexion sécurisée (VPN).

- Une copie papier aux experts du rapport de travail.

8 POINTS TECHNIQUES ÉVALUÉS SPÉCIFIQUES AU PROJET

La grille d'évaluation définit les critères généraux selon lesquels le travail du candidat sera évalué (documentation, journal de travail, respect des normes, qualité, ...).

En plus de cela, le travail sera évalué sur les 7 points spécifiques suivants (Point A14 à A20):

1. *Schéma de l'infrastructure réseau :*
   - *3 points = schéma complet (routes, adresses, masques, noms, ...)*
   - *2 points = manque 1 élément ou schéma non conventionnel*
   - *1 point = schéma incomplet*
   - *0 points = pas fait*
2. *Explication de la mise en place du tunnel IPSEC*
   - *3 points = explication claire et précise*
   - *2 points = manque 1 élément*
   - *1 point = explication incomplète*
   - *0 points = pas fait*
3. *Les services AD, DNS, DHCP, FS et impression sont redondants*
   - *3 points = tous les services sont redondants*
   - *2 points = manque 1 service*
   - *1 point = manque plusieurs services*
   - *0 points = pas fait*
4. *Configuration du firewall*
   - *3 points = toutes les règles de base (sécurité minimum) sont configurées*
   - *2 points = manque 1 règle de base*
   - *1 point = manque plusieurs règles de base*
   - *0 points = pas fait*
5. *Configuration de l'AP*
   - *3 points = configuration complète*
   - *2 points = manque la configuration d'un élément*
   - 1 point = manque la configuration de plusieurs éléments
   - 0 points = pas fait
6. *Explication installation serveur de backup*
   - *3 points = explication claire et précise*
   - *2 points = manque 1 élément*
   - *1 point = beaucoup d'éléments manquent*
   - *0 points = pas fait*
7. *Installation des imprimantes*
   - *3 points = les imprimantes sont installées et vues dans le réseau*
   - *2 points = les imprimantes sont installées mais quelques bugs persistent*
   - *1 point = une imprimante n'est pas installée*
   - *0 points = pas fait*

Schéma modèle comprenant le matériel à disposition. Le schéma de l'infrastructure finale sera créé par le candidat.

6.1 La partie du projet que le candidat doit développer est la suivante

- Infrastructure réseau à Bullet :
  - Serveur (AD, DNS, DHCP, FS et impression)
  - Serveur redondant (AD, DNS, DHCP, FS et impression)
  - Firewall
  - Routeur
  - Switch
  - NAS
  - AP
  - Imprimante
  - Poste client fixe
- Infrastructure réseau à Lausanne :
  - Router
  - Switch
  - AP
  - Imprimante
- Utilisateurs
  - Jean Dupont – jean.dupont@kicroit.ch – groupe Marketing
  - Marie Martin – marie.martin@kicroit.ch – groupe Marketing
  - Pierre Lefevre – pierre.lefevre@kicroit.ch – groupe Marketing
  - Sophie Durand – sophie.durand@kicroit.ch – groupe Finances
  - Lucie Bernard – lucie.bernard@kicroit.ch – groupe Finances
- Divers
  - Les deux PC portables doivent pouvoir avoir accès au réseau et ses ressources depuis les deux sites

Le candidat connectera les deux routeurs ensemble par un câble Ethernet, afin de ne pas ajouter la complexité du FAI et ainsi protéger son travail d'éventuelles attaques informatiques pouvant surgir de l'extérieur.

7 LIVRABLES

Le candidat est responsable de livrer à son chef de projet et aux deux experts :

- Une planification initiale
- Un rapport de projet
- Un journal de travail
- A la fin du TPI (14 mai 2025 à 10h40)
  - Le rapport de travail sous forme électronique
  - Le journal de travail sous forme électronique
  - Une archive contenant tous les scripts et fichiers de configuration utilisés/créés

2.1.1 Définition du contenu et des fonctionnalités

L'entreprise Kicroit souhaite moderniser son infrastructure informatique afin de mieux gérer ses ressources, optimiser la collaboration entre ses membres, assurer la sécurité des données et permettre aux deux sites d'accéder aux mêmes ressources.

Pour pouvoir faire fonctionner et sécuriser l'infrastructure un firewall faisant la liaison entre les différentes parties du réseau est nécessaire. De plus un tunnel VPN site à site fera la liaison entre le site de Bullet où se trouvent les serveurs et le site de Lausanne. Les utilisateurs de Lausanne doivent avoir accès aux services des serveurs de Bullet et pouvoir se connecter au domaine

Il est nécessaire de mettre en place un contrôleur de domaine basé sur un micro-serveur, avec une gestion centralisée des utilisateurs et des permissions. L'installation d'un AD, d'un DNS et d'un DHCP est requis. Le serveur devra aussi offrir un service d'impression et service de fichier. De plus pour plus de sécurité un serveur redondant proposant les mêmes services sera installé.

Il faut également installer un NAS le Back up des données. Ainsi que définir et appliquer les groupes de sécurité pour restreindre l'accès aux différentes ressources.

Enfin, L'entreprise veut un wifi pour ces employés. Il faudra sécuriser les deux Access Point pour éviter tout risque d'intrusion.

2.1.2 Situation actuelle

Actuellement la société n'a pas d'installation Informatique viable. Ils n'ont pas de parc informatique, chaque utilisateur travaille sur son poste personnel et les fichiers étaient transmis par email. Cette solution n'est, en effet, pas suffisante pour l'ouverture d'une succursale. Les données ne sont pas sauvegardées, les utilisateurs impriment via le logiciel HP classique ce qui ne permet pas de gérer efficacement les imprimantes et n'ayant pas de serveur il n'est pas possible d'avoir un domaine permettant à chacun de se connecter sur tous les postes.

2.1.3 Utilisateurs cibles

L'objectif est de fournir une infrastructure clé en main pour que l'entreprise puisse travailler sans avoir à se soucier du réseau. A ce titre, et comme l'entreprise n'a pas d'IT à proprement parler, ils n'auront pas accès aux comptes administrateurs pour éviter toute complication.

2.1.4 Présentation des solutions matérielles et logiciels

Le point critique de ce projet se situe au niveau de la structure du réseau. La présence de deux sites crée plusieurs problèmes. Premièrement, le site de Lausanne n'ayant pas de DHCP il doit utiliser celui de Bullet. Deuxièmement, l'imprimante de Lausanne doit être accessible par le serveur de Bullet mais elle doit aussi être sécurisée. Troisièmement, les ordinateurs de Lausanne doivent avoir accès aux fichiers et services de Bullet. Il existe plusieurs solutions pour répondre à ce problème.

Pour régler ces problèmes il faut les prendre d'abord individuellement. Pour l'imprimante il n'y a pas beaucoup de solutions, le plus simple et efficace est de séparer l'imprimante dans un réseau dédié. Ainsi elle ne peut pas communiquer librement avec les autres appareils et il est possible de mettre en place des règles de firewall spécifiques pour ne laisser transiter que les protocoles d'impression. Il serait aussi possible de bloquer manuellement les requêtes de la machine en se basant sur

son IP et donc de la laisser dans le même réseau mais cela laisse plus de place à l'erreur et cela implique de le refaire si une autre imprimante est ajoutée.

Pour le problème du DHCP et des ressources une première solution serait de mettre toutes les adresses IP en statique à Lausanne. En faisant cela il n'y a plus le problème du DHCP. Le tunnel VPN permettrait d'accéder aux ressources de l'entreprise. Cette solution est la plus simple dans le cadre de cet exercice mais la plus laide et la moins efficace dans un cas concret. En effet elle implique de devoir configurer manuellement chaque appareil ce qui est une perte de temps conséquente et laisse place aux erreurs. Comme personne à Kicroit n'est IT cela implique aussi un suivit constant de la part de notre entreprise.

Une deuxième solution serait de créer le même réseau sur les deux sites. Si le réseau est identique alors le DHCP pourra fonctionner et donner les adresses des deux côtés. Après discussion avec monsieur Varela cette technique comporte cependant un risque. Comme le réseau est le même de part et d'autre du routeur il ne sait pas ou il doit envoyer le paquet ou risque de l'envoyer par défaut toujours au même endroit. Il est possible de contrecarrer ce problème en utilisant le NAT pour spécifier dans quelle partie du réseau les routeurs doivent envoyer les requêtes. Cette solution fonctionne mais complexifie considérablement le projet.

Une troisième solution serait de créer deux réseaux séparés et d'utiliser un relai DHCP. Sur le service DHCP du serveur il faudrait créer deux étendues distinctes et suivant qui fait la requête le DHCP donnerait une adresse d'une plage ou de l'autre. Cette solution demande de mettre en place sur le routeur de Lausanne un relai DHCP en unicast qui redirige sur le serveur. Elle est relativement simple à mettre en place et répond à tous les problèmes posés par les deux sites.

2.2 Solution Choisie

Pour répondre aux contraintes de sécurités les imprimantes de Lausanne seront dans leur propre réseau. L'idée est d'utiliser deux Vlans pour séparer la partie imprimantes et la partie utilisateurs sur le site. Pour répondre aux contraintes d'accès aux ressource deux étendues seront crées dans le DHCP et un relai DHCP sera mis en place sur le routeur de Lausanne. La combinaison de ces solutions offre un bon niveau de sécurité puisque les connexions seront gérées par le firewall et permettent de gérer facilement le parc de Lausanne avec le serveur de Bullet.

2.3 Etude de faisabilité

La principale contrainte de ce projet est le temps. 90 heures pour mettre en place une infrastructure complète est très serré. Chaque tâche n'est pas très complexe mais un problème qui entrainerait une perte de temps est à prendre très au sérieux.

Une autre contrainte est la contrainte technique. En effet je n'ai que peu travaillé avec un firewall. Mettre en place comme je le désire ce service risque donc de prendre du temps et le résultat n'est pas garanti. Je n'ai jamais configuré de sauvegarde incrémentielle avec un NAS. Même si la configuration demandée n'est pas très poussée les recherches risquent de prendre du temps.

2.4 Stratégie de test

Pour ce projet les tests se feront sur chaque appareil installé. L'ordre des tests suivra l'ordre d'installation des appareils dans sa globalité (Routeur, Firewall, PC 1 et 2, Serveur, Switch, Imprimante, Access point, NAS, Serveur redondant, Routeur Lausanne, PC 1 Lausanne, Imprimante Lausanne, Access point Lausanne, Connexion

VPN). Cependant comme certaines parties des configurations se feront après avoir mis en place le reste des infrastructures les tests se feront à ce moment-là. Par exemple il n'est pas possible de tester le service d'impression avant d'avoir installé l'imprimante mais on peut quand même tester les autres fonctionnalités et le fonctionnement du serveur.

Les tests ne demandent pas de matériel supplémentaire. Ils fonctionnent de la manière suivante :

- Quel appareil ou service ?
- Qu'est ce qui est testé ?
- Quel est le résultat attendu ?
- Est-ce que le test est une réussite ou un échec ?
- Remarques supplémentaires.

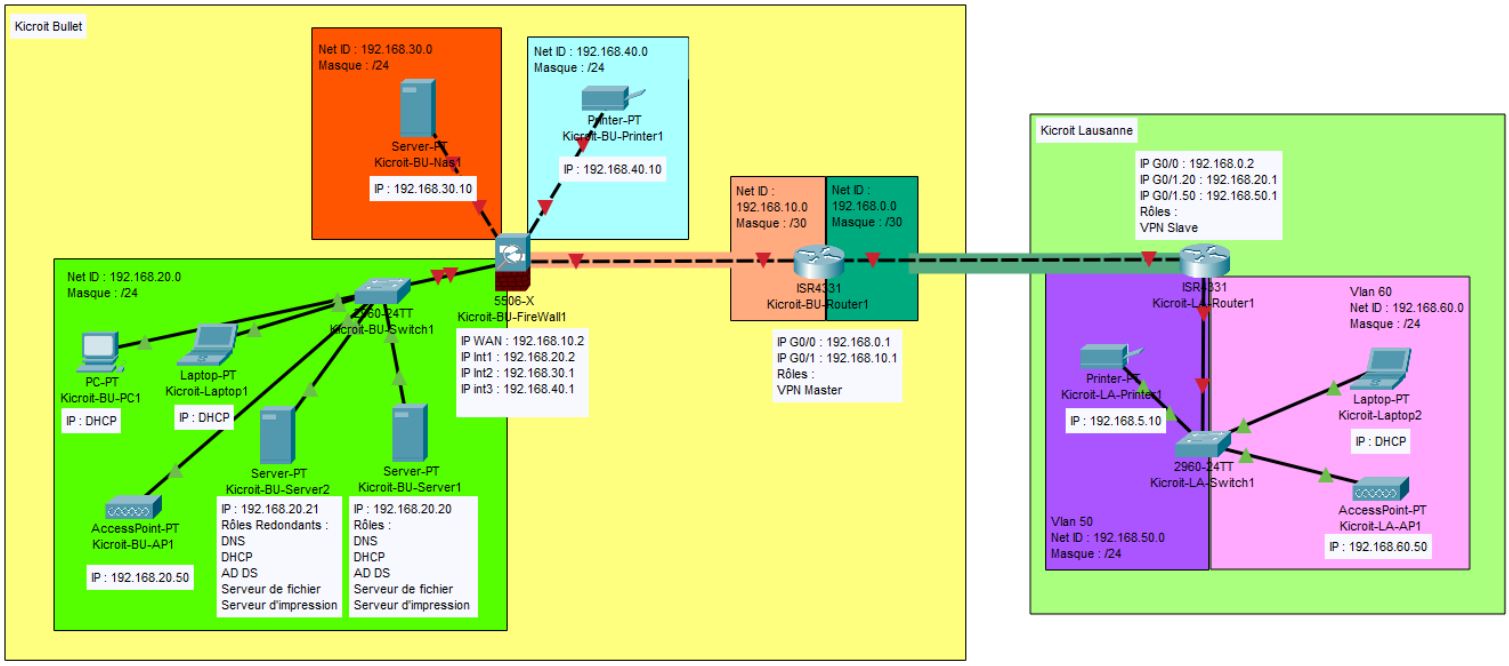
Les tests ont pour objectifs d'êtres exhaustifs et d'assurer du bon fonctionnement de l'infrastructure. Ils seront tous réalisé par la personne qui met en place l'infrastructure.

3 Conception

3.1 Plans topologiques

3.1.1 Topologie Hybride Logique/physique

La topologie a été faite avec le logiciel Cisco Packet Tracer[3]. Cette représentation est le schéma logique/physique réel du projet. Si c'était un cas pratique le Net ID 192.168.0.0 n'existerait pas. Les deux routeurs seraient reliés à internet via le FAI et un tunnel VPN serait fait entre les deux.



3.1.2 Conventions de dénomination et d'adressage

A des fins d'unicité et de clarté, tous les appareils présents dans les réseaux suivent une dénomination commune. Elle prend la forme suivante : Kicroit- « abréviation du site » - « type d'appareil » « numéro de l'appareil ». Par exemple le premier ordinateur fixe installé à Bullet s'appellera : Kicroit-BU-PC1. Le numéro dépend aussi des sites, si un ordinateur fixe était installé à Lausanne il s'appellerait : Kicroit-LA-PC1 et non Kicroit-LA-PC2. Avec cette dénomination il est possible de savoir immédiatement de quelle machine on parle et sur quel site. Les tables d'adressages sont les suivantes.

[3] https://www.netacad.com/cisco-packet-tracer

Table d'adressage						
Nom	Rôle	IP	Masque	Passerelle	DNS	DNS secondaire
Kicroit-Laptop1	Ordinateur portable	DHCP	255.255.255.0	192.168.20.2	192.168.20.20	192.168.20.21
Kicroit-Laptop2	Ordinateur portable	DHCP	255.255.255.0	192.168.60.1	192.168.20.20	192.168.20.21
Kicroit-BU-PC1	Poste de travail	DHCP	255.255.255.0	192.168.20.2	192.168.20.20	192.168.20.21
Kicroit-BU-Server1	Contrôleur de domaine, DHCP, DNS, serveur de fichier et d'impression	192.168.20.20	255.255.255.0	192.168.20.2	127.0.0.1	192.168.20.21
Kicroit-BU-Server2	Serveur redondant	192.168.20.21	255.255.255.0	192.168.20.2	127.0.0.1	192.168.20.20
Kicroit-BU-AP1	Access point Bullet	192.168.20.50	255.255.255.0	192.168.20.2	192.168.20.20	192.168.20.21
Kicroit-BU-Nas1	Serveur de backup	192.168.30.10	255.255.255.0	192.168.30.1	-	-
Kicroit-BU-Printer1	Imprimante Bullet	192.168.40.10	255.255.255.0	192.168.40.1	-	-
Kicroit-LA-Printer1	Imprimante Lausanne	192.168.50.10	255.255.255.0	192.168.50.1	-	-
Kicroit-LA-AP1	Access point Lausane	192.168.60.50	255.255.255.0	192.168.60.1	192.168.20.20	192.168.20.21

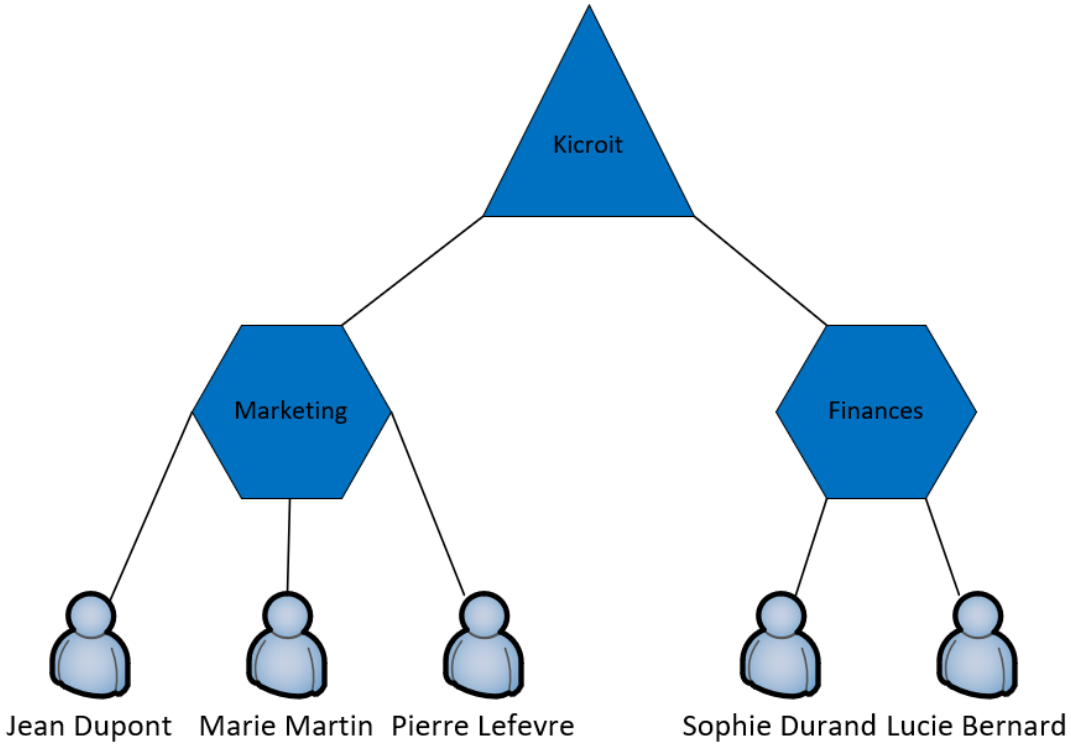
Table d'adressage Firewall				
Interface	Role	IP	Masque	Passerelle
lan1	Réseau de l'entreprise	192.168.20.2	255.255.255.0	192.168.10.2
lan2	Réseau du serveur de backup	192.168.30.1	255.255.255.0	192.168.10.2
lan3	Réseau des imprimantes	192.168.40.1	255.255.255.0	192.168.10.2
Wan1	Connexion au routeur	192.168.10.2	255.255.255.252	192.168.10.1

Table d'adressage Routeurs					
Nom	Interface	Role	IP	Masque	Passerelle
Kicroit-BU-Router1	G0/0	Connexion Lausanne	192.168.0.1	255.255.255.252	192.168.0.2
Kicroit-BU-Router1	G0/1	Connexion firewall	192.168.10.1	255.255.255.252	192.168.0.2
Kicroit-LA-Router1	G0/0	Connexion Bullet	192.168.0.2	255.255.255.252	192.168.0.1
Kicroit-LA-Router1	G0/1.50	Vlan imprimantes LA	192.168.50.1	255.255.255.0	192.168.0.1
Kicroit-LA-Router1	G0/1.60	Vlan utilisateurs	192.168.60.1	255.255.255.0	192.168.0.1

3.1.3 Structures logiques et arborescences

Cette rubrique présente le fonctionnement de l'entreprise fictive, les différents groupes et employés ainsi que les permissions qui leur seront accordées.

ORGANIGRAMME GROUPES ET EMPLOYES



Permissions NTFS

Dossier \ Groupes		Admins du domaines	Marketing	Finances
F:\		CT		
	\Marketing	CT	M	
	\Finances	CT		M

CT	Contrôle total
M	Modification
LX	Lecture et exécution

Utilisateurs & Groupes

Utilisateurs \ Groupes	Admins du domaine	Utilisateurs du domaine	Marketing	Finances
admin	x	x		
Jean Dupont		x	x	
Marie Martin		x	x	
Pierre Lefevre		x	x	
Sophie Durand		x		x
Lucie Bernard		x		x

3.2 Mise en place de la Sécurité

La mise en place de la sécurité se fait directement à la configuration des différents appareils de l'infrastructure. Les mots de passes seront soit générés par un gestionnaire de mot de passe soit fonctionneront via un code par exemple Kicroit24-[Nom de l'appareil]_MdP$ ce qui garantit une bien meilleure sécurité.

Les Switchs, le routeur et les access point doivent avoir un mot de passe pour passer en mode Enable. Les lignes Vty doivent être sécurisées et l'accès via le port console doit avoir un mot de passe. De plus les ports non utilisés des switchs doivent être verrouillés manuellement pour éviter toute intrusion sur le réseau. Les Wifis fournis par les Access Points doivent avoir un mot de passe crypté. Les ordinateurs et le serveur doivent avoir un mot de passe. Pour les utilisateurs les permissions NTFS permettent de limiter les données auxquelles ils auront accès afin de limiter les fuites.

Le firewall s'occupe de la sécurité des connexions. Chaque réseau est par défaut séparé. Le réseau principal ne doit pouvoir communiquer qu'avec le réseau du routeur, celui de l'imprimante et celui du NAS et les deux réseaux de Lausanne. Uniquement les protocoles utilisés par ces derniers sont autorisés. Ainsi le Réseau principal ne peut pas ping les autres par exemple. Les réseaux des imprimantes ne peuvent communiquer qu'avec le réseau principal, de même pour le réseau du NAS. Enfin des règles concernant le trafique entrant scannent les emails et des règles concernant le trafique limitent les sites auxquels les internautes peuvent accéder.

Pour ce projet comme le GitHub est public les mots de passes sont gérés grâce à keepass[4] pour éviter de donner accès aux mots de passes au monde entier. L'application est portable, il suffit de télécharger le fichier et elle est directement utilisable. Elle crée une base de données contenant les mots de passes des différents appareils. Le mot de passe de la database à été transmis par mail aux experts et au chef de projet.

[4] https://keepass.info/

4 Réalisation et mise en service

4.1 Description des tâches effectuées

La réalisation de ce projet s'est faite en plusieurs partie entremêlée. En effet certains éléments ont vu leur configuration changer au fur et à mesure des avancées du projet. Par exemple le firewall a été installé une première fois puis sa configuration à été modifiée pour permettre aux autres éléments de l'infrastructure de fonctionner correctement. Pour des raisons de clarté les éléments rapportés dans ce rapport sont structurés suivant le type d'appareil qui est mis en service et non de manière chronologique. Les différentes procédures d'installation seront misent à jour au fur et à mesure Cette rubrique contient donc l'installation et la configuration des routeurs, du firewall, des serveur, des switchs, des pcs, des imprimantes, du nas et des access point.

4.1.1 Putty

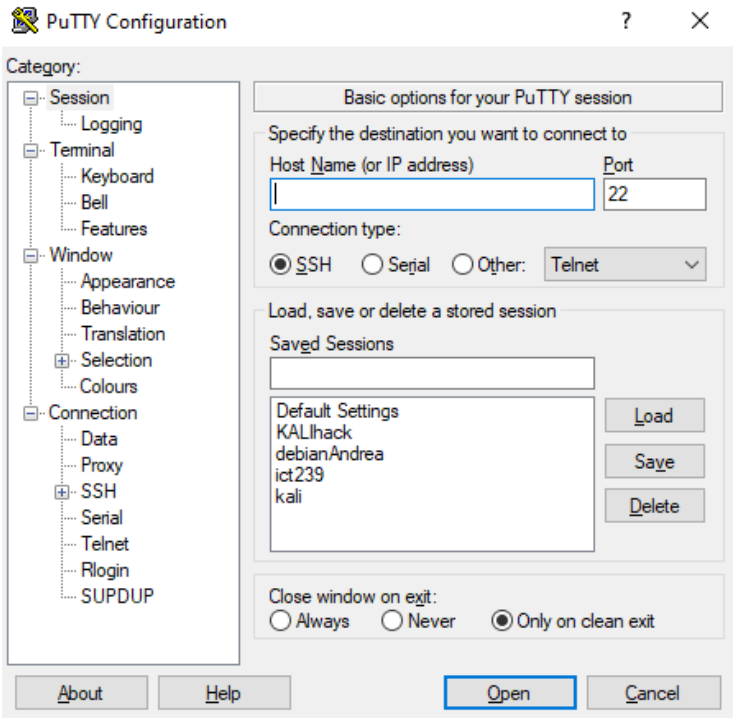
Putty est une application qui permet de se connecter en SSH ou via un câble Serial à un appareil. Dans le projet il est utilisé à de multiples reprises pour la configuration de différents appareils. Pour ne pas devoir expliquer à chaque fois les manipulations effectuées voici une marche à suivre pour se connecter à un appareil.

Via SSH :

Lors de l'ouverture de Putty il faut entrer l'adresse IP de la machine cible et le port 22 (port par défaut pour le ssh) puis appuyer sur « open ».

Via Serial :

Vérifier que le câble sérial soit bien connecté à la machine à configurer, sélectionner l'option sérial et cliquer sur « open ».



4.1.2 Poste fixe

Pour ce projet un poste fixe est fourni. Il faut premièrement installer l'os. Il faut installer Putty[5]. L'installation se fait via internet et ne demande pas de configuration particulière. Une fois le serveur installé il faut rentrer l'ordinateur dans le domaine et modifier le nom de l'ordinateur. Pour ce faire il faut aller dans « Renommer ce PC avancé>Nom de l'ordinateur>modifier ». Après avoir écrit le nouveau nom de l'ordinateur selon la convention de nommage il faut redémarrer l'ordinateur et revenir au même endroit pour sélectionner « membre d'un domaine », écrire le nom de domaine « Kikroit.com » et se connecter via un compte présent dans l'AD. Finalement il faut vérifier que les paramètres IPv4 soient bien sur DHCP via centre de réseau et partage>modifier les options d'adaptateur> (sur la carte réseau) propriétés>Protocol internet ipv4. Quand toute la configuration est correcte voici la configuration obtenue.

4.1.3 Imprimante Bullet

La configuration de l'imprimante se fait sous network>Wired Lan> TCP/IP. Il faut mettre une adresse en statique : 192.168.40.10/24 gateway : 192.168.40.1. Le nom de l'imprimante doit aussi être changé sous « node name » pour correspondre aux conventions de nommages (Kicroit-BU-Printer1). L'imprimante ne demande pas plus d'installation.

[5] https://www.putty.org/

4.1.4 Switch Bullet

4.1.5 Routeur Bullet

4.1.6 Firewall

4.1.7 Premier serveur

4.2 Description des tests effectués

Appareil ou service testé	Quoi	Résultat Attendu	Réussite/échec	Commentaire
Routeur BU	Allumage du routeur	Le routeur s'allume et démarre correctement		
Routeur BU	Configuration initiale	La configuration itiale du routeur est correctement effectuée (nom, adresse)		
Routeur BU	Sécurité	Le routeur demande un mot de passe pour pouvoir se connecter en Vty et avec un câble console		
Routeur BU	Connection avec le firewall	le routeur doit pouvoir ping l'interface wan du firewall		
Routeur BU	VPN	Le routeur assure son rôle de VPN master		
Firewall	Allumage du firewall	Le firewall s'allume correctement		
Firewall	Configuration initiale	La configuration initiale du firewall est correctement effectuée et il est possible d'y accéder via un navigateur web		
Firewall	Compte admin	Un compte admin propre à Kicroit existe et possède tous les droits		
Firewall	Connection avec le réseau 1	les appareils du réseau lan 1 doivent pouvoir ping l'interface 1		
Firewall	Connection avec le réseau 2	les appareils du réseau lan 1 doivent pouvoir ping l'interface 2		
Firewall	Connection avec le réseau 3	les appareils du réseau lan 1 doivent pouvoir ping l'interface 3		
Firewall	Configuration des polices	Les sites webs sotn filtrés suivant des filtres pertinants pour une entre prise		
Firewall	Routes statiques	interconnectés		
Firewall	Règles firewall	Les règles firewall bloquent le trafic de manière précise entre les réseaux		
Serveur 1	Allumage du serveur	le serveur s'allume et démarre correctement		
Serveur 1	Installation initiale	Windows serveur 2022 est correctement installé sur le serveur		
Serveur 1	Ping	Le serveur peut ping les appreils du réseau		
DHCP	Livraison d'adresse BU	Le DHCP donne des adresses suivant la plage sélectionnée		
DHCP	Livraison d'adresse Lausanne	Le DHCP donne des adresses suivant la plage sélectionnée		
DNS	Inscription DNS	Le DNS inscrit dans ses registres les adresses ip avec les appareils correspondants		
AD DS	Le service est fonctionnel	Le domaine Kicroit.ch existe et il est possible de s'y connecter		
AD DS	Utilisateurs et groupes	Les utilisateurs et groupes sont créés conformément à la planification		
Serveur de fichier	Arborescence	Les dossier de l'arborescence existent conformément à la planification		
Serveur de fichier	Partage	Le partage fonctionne		
Serveur de fichier	GPO	Les Gpo permettent le déploiement automatique du partage		
Serveur de fichier	NTFS	Les permissions NTFS existent conformément à la planification		
Serveur d'impression	Imprimante	Le serveur d'impression possède l'imprimante		
Serveur d'impression	GPO	Le serveur d'impression distribue l'imprimante via GPO		
Serveur redontant	Allumage du serveur	le serveur s'allume et démarre correctement		
Serveur redontant	Installation initiale	Windows serveur 2022 est correctement installé sur le serveur		
Serveur redontant	Ping	Le serveur peut ping les appreils du réseau		
DHCP	Livraison d'adresse BU	Le DHCP donne des adresses suivant la plage sélectionnée		
DHCP	Livraison d'adresse Lausanne	Le DHCP donne des adresses suivant la plage sélectionnée		
DNS	Inscription DNS	Le DNS inscrit dans ses registres les adresses ip avec les appareils		
AD DS	Le service est fonctionnel	Le domaine Kicroit.ch existe et il est possible de s'y connecter		
AD DS	Utilisateurs et groupes	Les utilisateurs et groupes sont créés conformément à la planification		
Serveur de fichier	Arborescence	Les dossier de l'arborescence existent conformément à la planification		
Serveur de fichier	Partage	Le partage fonctionne		
Serveur de fichier	GPO	Les Gpo permettent le déploiement automatique du partage		
Serveur de fichier	NTFS	Les permissions NTFS existent conformément à la planification		
Serveur d'impression	Imprimante	Le serveur d'impression possède l'imprimante		
Serveur d'impression	GPO	Le serveur d'impression distribue l'imprimante via GPO		
Serveur redontant	Redondance	Le serveur reprend le rôle de l'autre s'il n'est plus en ligne		
PC fixe Bullet	Installation initiale	Windows 10 pro est installé sur le pc		
PC fixe Bullet	Putty	Putty est installé et permet de se connecter aux appareils		
PC fixe Bullet	Domaine	Le pc fait partie du domaine		
PC fixe Bullet	Ping	le PC peut ping les appareil du réseau		
PC portables	Installation initiale	Windows 10 pro est installé sur les deux pc		
PC portables	Putty	Putty est installé et permet de se connecter aux appareils		
PC portables	Domaine	Les pc font partie du domaine		
PC portables	Ping	les pc peuvent ping les appareil du réseau		
Imprimantes	Configuration initiale	La configuration initiale des l'imprimantes est correctement effectuéelip		
Imprimantes	Impression	L'impression depuis les postes de travail fonctionne		
Switch Bullet	Configuration initiale	La configuration initiale de switch est correctement effectuée		
Switch Bullet	Sécurité	Les principes de sécurités élémentaires sont respectés		
Switch Lausanne	Configuration initiale	La configuration initiale de switch est correctement effectuée		
Switch Lausanne	Sécurité	Les principes de sécurités élémentaires sont respectés		
Switch Lausanne	Vlan	Le switch gère correctement les Vlans		
AP Bullet	Configuration initiale	La configuration initiale des AP est correctement effectuée		
AP Bullet	Distribution adresse IP	L'AP donne des adresses et elles sont référencées dans le DHCP		
AP Lausanne	Configuration initiale	La configuration initiale des AP est correctement effectuée		
AP Lausanne	Distribution adresse IP	L'AP donne des adresses et elles sont référencées dans le DHCP		
NAS	Configuration initiale	La configuration initiale du NAS permet de se connecter via WEB		
NAS	Raid	Les disques sont initialisé en raid 5		
NAS	Stratégie de backup	Les stratégies de backup sont fonctionnelles et représentent les choix fait pendant la conception		
NAS	Ping	Le serveur ne peut rien ping		
Routeur Lausanne	Allumage du routeur	Le routeur s'allume et démarre correctement		
Routeur Lausanne	Configuration initiale	La configuration itiale du routeur est correctement effectuée (nom, adresse)		
Routeur Lausanne	Sécurité	Le routeur demande un mot de passe pour pouvoir se connecter en Vty et avec un câble console		
Routeur Lausanne	VPN	Le routeur remplit son rôle de VPN slave		
Routeur Lausanne	Vlans	Le routeur gère correctement les Vlans		

4.3 Erreurs restantes

4.4 Liste des documents fournis et dossier d'archivage

5 Conclusions

6 Annexes

6.1 Sources – Bibliographie

6.1.1 Intelligences Artificielles :

Pour les cas d'utilisation de l'IA le prompt et le problème auquel il répond est spécifié.

Grok :

Prompt	Problème sous-jacent
Fais-moi le logo d'une entreprise fictive qui s'appelle Kicroit.	Créer le logo pour la page de garde.

Chat GPT 4o :

Prompt	Problème sous-jacent
Pour mon travail de fin de CFC je dois créer un réseau pour une petite entreprise. L'entreprise est sur deux sites distincts (Bullet et Lausanne) et je dois les interconnecter avec un VPN site à site. Mon problème est le suivant : J'ai un serveur Windows 2022 qui fait service d'impression mais j'ai une imprimante à Bullet et une à Lausanne. Pour sécuriser mon infrastructure je ne veux pas que les imprimantes soient dans le même réseau que les serveurs et les utilisateurs. Pour Bullet le site est équipé d'un firewall du coup je pensais faire un réseau distinct et limiter le trafic via des règles mais je ne sais pas comment sécuriser les deux imprimantes de manière logique	Il faut connecter l'imprimante de Lausanne en tenant compte de la sécurité. Elle ne doit donc pas pouvoir communiquer avec les autres appareils du réseau mais doit quand même être accessible pour que le serveur d'impression puisse l'intégrer.
J'ai un firewall fortigate 50e. je dois sécuriser les différents LAN qu'il interconnecte. Quel sont les protocoles utilisés par les imprimantes ? quels sont les protocoles utilisés par un NAS ?	Afin de limiter le trafic il faut identifier les différents protocoles et les ports utilisés pour les services d'impression et de sauvegarde. Comme ça il est possible de n'autoriser qu'eux

6.1.2 Sites internet :

https://asana.com/fr/resources/waterfall-project-management-methodology

https://github.com/andreafont/TPI-Infrastrucutre-d-une-PME-avec-deux-sites-distants/tree/main

https://neptunet.fr/relais-dhcp/

https://www.netacad.com/cisco-packet-tracer

https://keepass.info/

6.1.3 Personnes extérieures au projet :

Grégory Renaud

Francis Varela

6.2 Glossaire

6.3 Table des illustrations

Aucune entrée de table d'illustration n'a été trouvée.

6.4 Journal de bord