Institut Universitaire de Technologie,
Aix-Marseille Université

RAPPORT DE STAGE de fin de deuxième année
Bachelor Universitaire de Technologie
Spécialité Réseaux et Télécommunications
Parcours cybersécurité

Assistant RSSI

Hadji MOUIGNI

KLANIK

Responsable entreprise : Julien MONTROZIER

Responsable académique : Rabah IGUERNAISSI

2023

Table des matières

1 Introduction 5
2 L'entreprise KLANIK 5
2.1 Introduction 5
2.2 Présentation 5
2.3 Organigramme 5
2.4 Département IT System 6
3 Missions et projets 7
3.1 Divers sujets et missions 7
3.1.1 Authentification Wi-Fi en SSO 7
3.1.2 Mise en place d'un VLAN Sécurité 9
3.1.3 Réalisation de noyaux 11
3.2 Sujets liés à la norme ISO 27001 12
3.2.1 La cartographie IT 14
3.2.1.1 Cartographie Physique 14
3.2.1.2 Cartographie logique/réseau 15
3.2.1.3 Cartographie Fonctionnelle 17
3.2.2 Wi-Fi Invité 19
3.2.2.1 Mise en place 19
3.2.2.2 Limites du réseau 21
4 Conclusion 23
5 Remerciements 25
6 Glossaire 27
7 Sitographie 29

1 Introduction

Dans le cadre de ma formation à l'IUT Réseaux & Télécommunications de Marseille Luminy, j'ai eu l'opportunité de réaliser un stage en tant qu'Assistant Responsable Sécurité des Systèmes d'Information (RSSI) chez KLANIK, au sein de la Direction des Opérations.

Ma mission principale lors de ce stage était d'assister le RSSI dans ses missions. Pour cela, j'ai été amené à réaliser différentes missions. Plusieurs sujets étaient proposés et donc j'ai pu aborder et intervenir de loin ou de près dans divers projets pour l'entreprise

Ce rapport de stage est structuré de la manière suivante : dans un premier temps, je présenterai la société KLANIK, ensuite, j'aborderai différentes missions et sujets traitées durant ce stage. Enfin, je terminerai par un focus sur deux sujets.

2 L'entreprise KLANIK

2.1 Introduction

Dans le cadre de mon stage, j'ai eu l'opportunité de travailler au sein de l'entreprise KLANIK. Cette section vise à présenter brièvement l'entreprise, en mettant l'accent sur ses activités principales, sa structure organisationnelle et plus particulièrement sur le service dans lequel j'ai effectué mon stage. De plus, nous aborderons également le rôle du Responsable de la Sécurité des Systèmes d'Information (RSSI) au sein de l'entreprise

2.2 Présentation

KLANIK est une société de conseil spécialisée en IT. Fondée en 2011 par Johan GUEDJ, elle s'est rapidement développée pour se faire sa place dans le monde des ESN. L'activité principale est l'accompagnement de grandes entreprises dans leurs projets de transformation digitale dans des domaines tels que le software, la cybersécurité, le cloud et bien d'autres encore. Elle se distingue par son expertise dans ces domaines ainsi que le fait d'être étendue en France et implantée à l'international que ce soit en Europe, en Amérique du Nord ou encore au Moyen-Orient.

2.3 Organigramme

Chez KLANIK il existe 3 types de personnes.

Tout d'abord il y a les consultants, qui vont être amenés à travailler directement avec les autres entreprises en étant sous contrat avec KLANIK.

Ensuite il y a les freelances qui eux aussi travaillent avec les clients mais à leurs propres comptes.

Enfin il y a le staff qui lui regroupe toutes les fonctions internes à l'entreprise.

Dans le staff il existe différents corps de métiers que ce soient les ressources humaines, les business managers en passant par la comptabilité ou encore la communication.

Durant mon stage j'ai pu intégrer l'équipe de la directions des opérations dans le département IT System qui fait partie du staff. Voici l'organigramme de cette équipe :

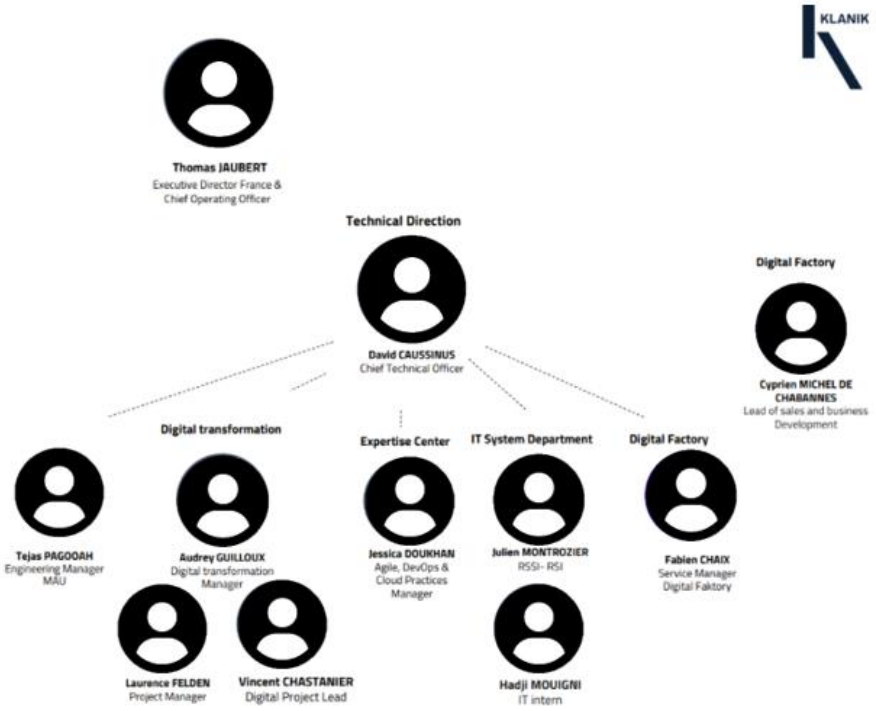


Figure 1 : Organigramme de la direction des opérations

2.4 Département IT System

Comme le montre l'organigramme le département IT System est composé d'une seule personne qui est le RSSI. Il est le garant de la sécurité des systèmes d'information. Il s'occupe de définir et déployer la politique de sécurité de l'information de l'entreprise en assurant la mise en œuvre et le suivi des projets et des réalisations techniques. Il s'occupe également de tout ce qui concerne la protection des données sensibles, la prévention des cyberattaques ou encore la gestion des risques informatiques. Il est également le responsable du système d'information (RSI). Il a la charge de mettre en place et de gérer les outils (PC, logiciels, applications, etc.) qui permettent aux collaborateurs de travailler

La sécurité des systèmes d'information est d'une importance capitale pour l'entreprise, car elle assure la protection des données, la continuité de l'activité et la confiance des clients.

Pour mener à bien ces missions le RSSI de KLANIK travaille quotidiennement en étroite collaboration avec une société sous-traitante, ONE COMPUTER, qui va s'occuper des différentes réalisations techniques ainsi que tout ce qui concerne l'IT en général de KLANIK.

C'est donc dans cet environnement de travail que j'ai pu réaliser un certain nombre de missions et intervenir dans divers projets.

3 Missions et projets

Pendant ce stage j'ai eu la chance de pouvoir être impliqué dans beaucoup de projets différents et d'avoir pu éplucher plusieurs sujets plus ou moins liés les uns aux autres. Dans un premier temps on abordera certaines missions que j'ai eues à réaliser ou auxquelles j'ai participé puis on se focalisera sur deux sujets qui concernent la norme ISO 27001, qui eux seront plus détaillés.

3.1 Divers sujets et missions

3.1.1 Authentification Wi-Fi en SSO

Un des premiers sujets sur lequel je me suis penché est l'authentification Wi-Fi en SSO

(Single Sign-On). L'objectif était de déterminer les solutions possibles pour que la connexion au réseau Wi-Fi de l'entreprise ne se fasse plus par un mot de passe commun mais en SSO avec les identifiants présents sur l'Azure Active Directory de l'entreprise. Azure est le service cloud de Microsoft sur lequel Klanik s'appuie beaucoup pour régir son environnement de travail.

La première mission que j'ai réalisée a été de comprendre comment fonctionnait le Wi-Fi actuel. Pour son réseau en général, Klanik utilise des équipements ZyXEL. La plupart des équipements de ZyXEL sont administrable par le cloud via leur plateforme appelée « Nebula » :

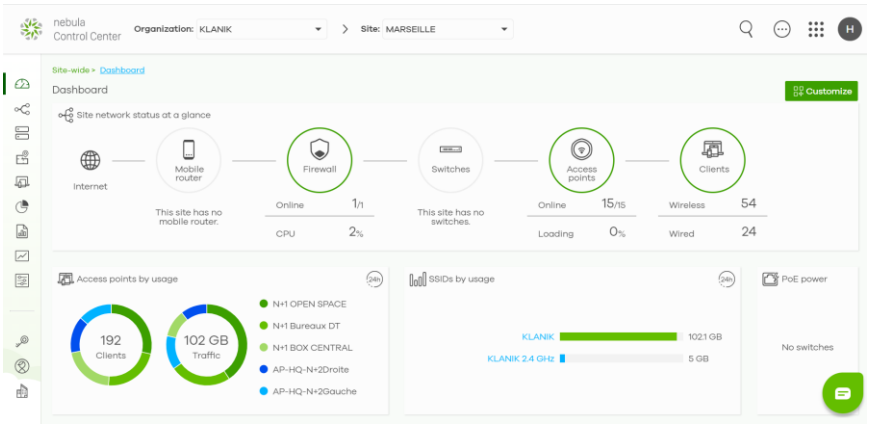


Figure 2 : Page d'accueil de la plateforme ZyXEL Nebula

Les bornes Wi-Fi qui sont utilisées dans les locaux sont administrées directement sur Nebula donc tout ce qui va concerner les méthodes d'accès et d'authentification aussi.

Dans l'onglet qui correspond au paramétrage des bornes on peut voir qu'il existe plusieurs moyens pour accéder au réseau sans fil :

- Open : Les utilisateurs se connectent librement et les données sont en clair
- Enhanced-open : On se connecte librement aussi mais avec les données cryptées
- WPA personnel : On utilise un mot de passe commun que l'on peut accompagner d'un QR code
- Dynamic personal psk : attribue automatiquement des clés de pré-partagée uniques pour chaque appareil client
- WPA entreprise : Connexion avec des identifiants uniques

Toutes ces méthodes sont utilisables en fonction des cas d'utilisation. Dans notre cas, plusieurs méthodes peuvent répondre à notre besoin.

Afin de mettre en place la connexion en SSO, l'option qui semble la plus adaptée est le WPA Entreprise (Wi-Fi Protected Access). Cette option permet la connexion au réseau avec un nom d'utilisateur et un mot de passe par personne. Pour pouvoir utiliser ce moyen d'accès il faut disposer d'un élément qui va permettre de stocker les identités ainsi que les mots de passe. C'est là que la notion de RADIUS est importante.

Le RADIUS (Remote Authentication Dial-In User Service) est un protocole client-serveur permettant de centraliser des données d'authentification. Lorsqu'un utilisateur tente de s'authentifier, le périphérique envoie un message au serveur RADIUS.

Si celui-ci est correctement configuré avec le périphérique comme client, RADIUS renvoie un message d'autorisation ou de refus au périphérique.

L'adresse IP du serveur RADIUS utilisé devra être indiquée sur Nebula pour permettre la connexion.

Pour cela il faut choisir quel type de serveur serait le plus adapté parmi : Un serveur physique, une solution SaaS ou une solution cloud (IaaS) (Annexe 9) :

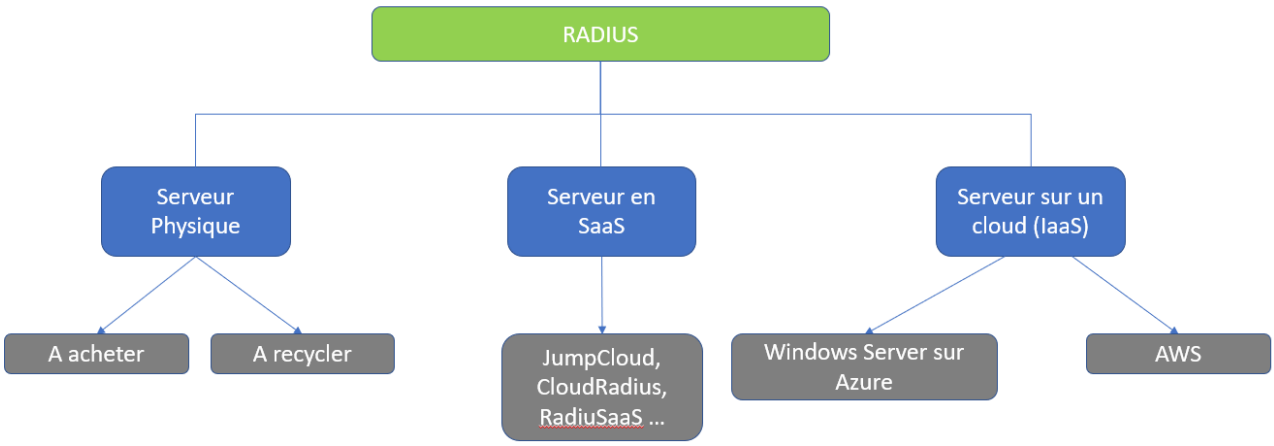


Figure 3 : Types de RADIUS envisageables

Dans notre cas, le serveur RADIUS est utilisé pour être synchronisé avec l'Azure AD, qui est l'annuaire de Klanik où les infos des collaborateurs sont stockées. Pour synchroniser les deux il faut utiliser une extension de Microsoft appelée NPS qui va permettre de faire le lien entre un Active Directory *on-premise* (c'est-à-dire hébergées par KLANIK ou leur sous-traitant) et les éléments contenus dans Azure (donc dans le Cloud).

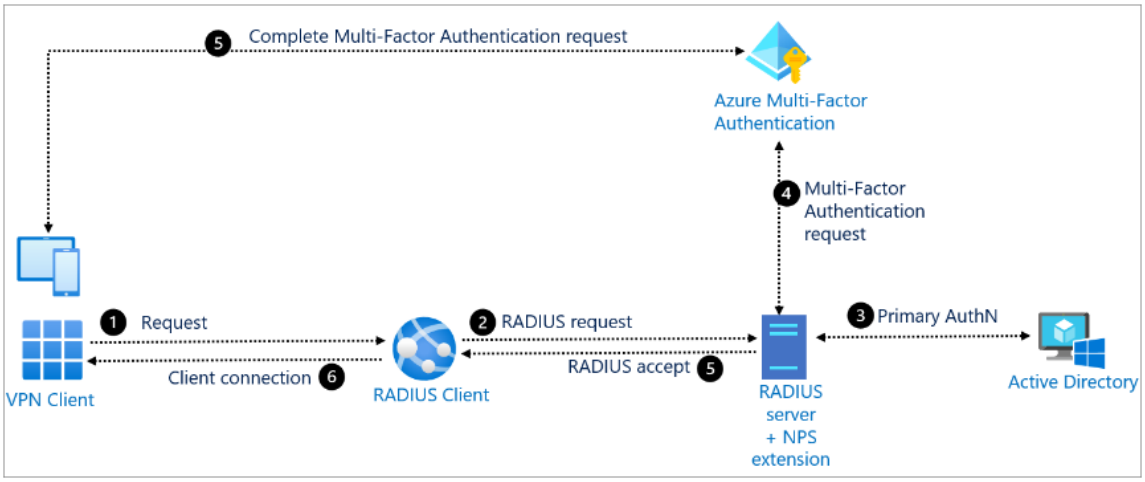


Figure 4 : Flux lors d'une requête RADIUS avec l'extension NPS

Après ces recherches j'ai estimé que la solution la plus simple à mettre en place serait d'utiliser un serveur physique et d'y ajouter l'extension NPS (Network Policy Server), toutefois comme le réseau de Klanik est en plein évolution j'ai dû mettre de côté ce sujet et me focaliser sur d'autres sujets plus prioritaires.

3.1.2 Mise en place d'un VLAN Sécurité

L'objectif de ce projet est de mettre en place un système de sécurité pour le contrôle d'accès au bâtiment, qui contient les systèmes de contrôle de porte, les systèmes d'alarme et les dispositifs de vidéosurveillance.

Il est important d'isoler dans un VLAN (Virtual Local Area Network) les équipements situés sur deux sites distincts, tout en leur permettant de communiquer entre eux. De plus, nous avons besoin d'un accès distant sécurisé pour que la société sous-traitante puisse superviser et gérer ces systèmes à distance. Le but étant de renforcer la sécurité globale de l'entreprise ainsi que l'accès aux locaux notamment la salle réseau.

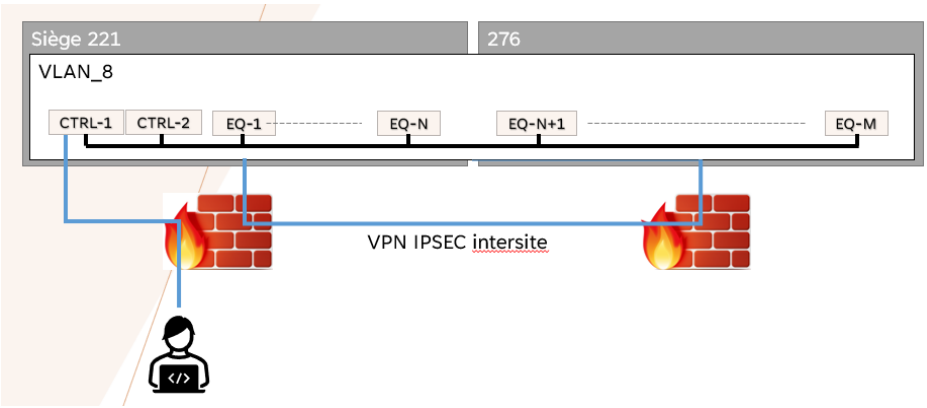


Figure 5 : Schéma de l'objectif de réalisation

Premièrement, il a fallu mettre en place le VPN inter-sites qui relie le siège et l'agence de Marseille. Il permettra de faire communiquer les différents équipements de sécurité présents dans les deux bâtiments. Les firewalls des deux agences étant de la marque ZyXEL, la configuration du VPN s'est faite sur Nebula. Cette plateforme fonctionne en organisation. C'est-à-dire que l'administrateur d'une entreprise peut avoir plusieurs sites qu'il peut diriger directement via la plateforme.

Ensuite il a fallu créer et déclarer les VLANs auprès des switches et des firewalls, le VLAN 8 coté siège et le VLAN 9 coté agence. Les identifiants de VLAN sont différents car initialement, les agences ne sont pas dans le même réseau. Aussi pour éviter tout conflit ou problèmes de connectivité nous avons opté pour cette démarche.

Une fois les interfaces réseau créées, les paramètres réseaux configurés (ports, pool DHCP, etc…), il a fallu se rendre sur Nebula pour mettre en place le VPN sur les deux sites.

Avec l'interface web, la configuration est simplifiée il suffit de bien comprendre ce que l'on fait et ce qu'il se passe lors de la réalisation.

L’onglet des paramètres VPN contient la rubrique ci-dessous :

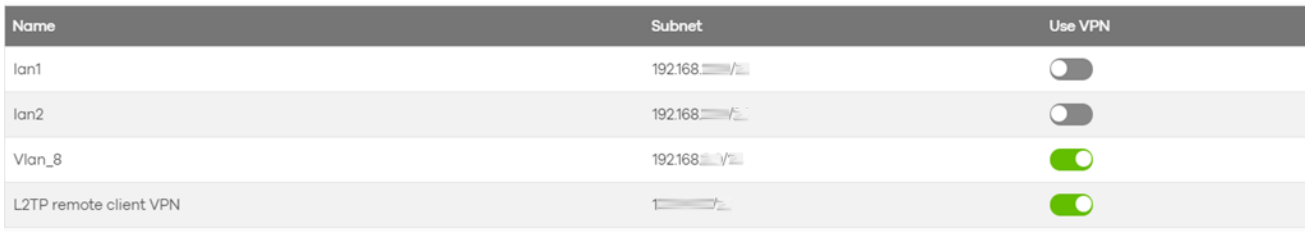


Figure 6 : Rubrique de mise en place VPN

Pour mettre en place le réseau VPN reliant les deux sites, il suffit de procéder à une configuration simple grâce à la plateforme Nebula au niveau des réseaux locaux concernés. Cette opération peut être réalisée en sélectionnant les réseaux locaux spécifiques que l'on souhaite inclure dans le VPN, aussi bien pour le siège social que pour l'agence (voir Annexe 1 pour l’agence).

En ce qui concerne le VPN distant, il faut d’abord créer le réseau virtuel sur Nebula avec tous les éléments principaux (adresse, mot de passe, méthode d’encryptions et d’authentification, etc…), puis établir une connexion VPN sur l'ordinateur de la machine distante qui se connectera. Une fois le VPN mis en place, il est important de configurer les règles de sécurité appropriées auprès du pare-feu. C’est-à-dire qu’il faut autoriser le client distant à accéder seulement au VLAN approprié ainsi que le trafic du VLAN 8 vers le VLAN 9. Ces règles doivent donc être créées sur Nebula (voir Annexe 2 et 3 pour les détails).

Une fois toutes ces étapes réalisées, les équipements de sécurité sont assignés aux VLAN respectifs et peuvent ainsi communiquer entre eux.
Grâce à cette configuration VPN, les sites distants sont interconnectés de manière sécurisée, permettant une communication efficace entre les équipements de sécurité des deux sites. Cette mise en place permet également un accès à distance sécurisé pour les opérations de maintenance, ce qui simplifie la gestion et garantit réactivité optimale en cas de besoin.

3.1.3 Réalisation de noyaux

Une des missions que j'ai effectuées est la réalisation de noyaux (Annexe 4). Les noyaux sont les « prises RJ45 femelles » que l'on retrouve au niveau des panneaux de brassages dans les baies ou, alors dans nos appartements.

Figure 7 : Cas d'utilisation des noyaux (panneau de brassage et prise murale)

Le réseau de Klanik étant en évolution, une solution de Backup 4G en cas de panne d'internet a été mise en place et il a donc fallu rajouter des nouveaux noyaux pour les équipements à raccorder au réseau. Comme pour tout type de câblage un ordre est à respecter (Annexe 5). Il m'a fallu plusieurs essais avant de pouvoir réellement réaliser les noyaux.

Une fois les noyaux placés, il faut vérifier qu'ils fonctionnent un à un avec un testeur de câbles.

Figure 8 : Testeur de câbles

Ces machines servent à déterminer si le câblage à bien été réalisé. Il faut brancher les câbles sur les deux extrémités (ex : un sur la baie, l'autre sur la prise murale), et regarder si les lumières s'allument dans l'ordre, des deux côtés. Si ce n'est pas le cas, il y a sûrement une erreur de câblage qu'il faut donc rectifier.

Cette mission m'a rappelé l'importance du câblage et de la couche physique que l'on a tendance à oublier dans un réseau. Un problème ou une mauvaise réalisation à ce niveau met en péril tout le réseau car elle est l'élément fondamental du réseau.

3.2 Sujets liés à la norme ISO 27001

La norme ISO 27001 est une norme internationale, non obligatoire, qui définit les exigences pour établir, mettre en œuvre, maintenir et améliorer un système de management de la sécurité de l'information (SMSI) au sein d'une organisation. Elle vise à garantir la protection des informations sensibles et à prévenir les risques liés à la sécurité de l'information.

Elle fournit un cadre et des lignes directrices pour assurer la sécurité des données et des informations au sein d'une entreprise notamment à propos l'identification des risques, l'évaluation des vulnérabilités et la mise en place de mesures de sécurité appropriées.

En se conformant à la norme ISO 27001, une entreprise montre son engagement envers la sécurité de l'information, renforce la confiance de ses clients et partenaires, et minimise les risques liés à la cybercriminalité et aux atteintes à la confidentialité des données.

Cette norme suit le modèle PDCA (Plan-Do-Check-Act). Ce modèle fournit un cadre structuré pour la mise en œuvre, le suivi et l'amélioration continue du système de gestion de la sécurité de l'information.

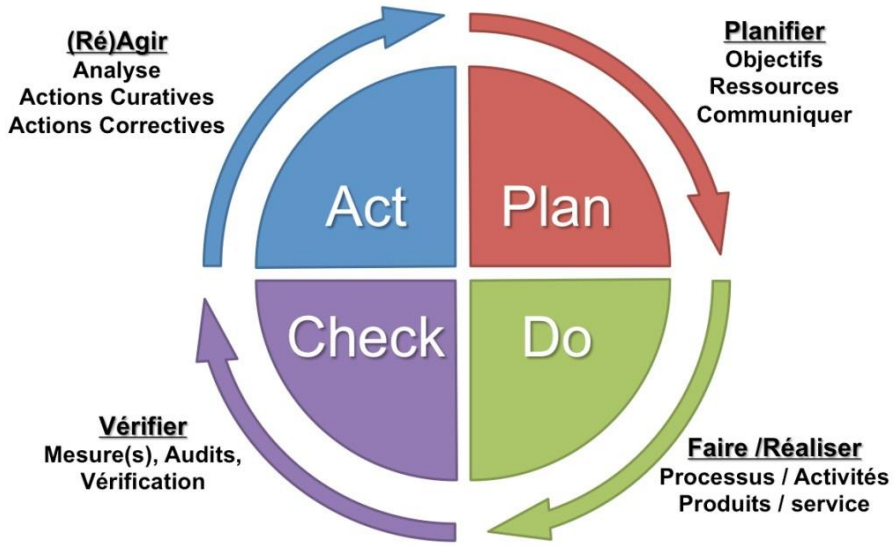


Figure 9 : PDCA appelée roue de Deming

Les notions de norme ISO 27001 et SMSI sont étroitement liées et se complètent mutuellement.

La norme ISO 27001 fournit le cadre et les exigences pour établir un SMSI efficace et guide l'élaboration de la politique de sécurité des systèmes d'information (PSSI).

Le SMSI, quant à lui, est le système de gestion mis en place par une organisation pour gérer de manière globale la sécurité de l'information. Il englobe l'ensemble des politiques, procédures, processus et mesures de sécurité mis en place pour protéger les actifs informationnels.

Ensemble, ils permettent à l'organisation de prendre une approche structurée et complète en matière de sécurité de l'information, en assurant la conformité aux réglementations et en minimisant les risques.

La Politique de Sécurité des Systèmes d'Information (PSSI) est un document clé qui établit les règles générales en termes de sécurité de l'information au sein d'une organisation, elle définit les objectifs de sécurité de l'information, les responsabilités des acteurs impliqués et les directives à suivre pour assurer la protection des données sensibles et la continuité des activités. Elle joue un rôle important dans la mise en place du SMSI et est aussi en étroite relation avec la norme ISO 27001.

5.9	**Inventaire des informations et autres actifs associés**
Règle générale	Il faut élaborer et tenir à jour un inventaire des informations et des autres actifs associés, Notamment les propriétaires.

Figure 10 : Exemple de règle générale contenue dans la PSSI

En se conformant à la PSSI et à la norme ISO 27001, Klanik s'assure d'établir un SMSI solide, conforme aux meilleures pratiques internationales en matière de sécurité de l'information. Cela lui permet de faire valoir son engagement envers la sécurité, de renforcer la confiance des clients et des partenaires.

Pendant le stage j'ai donc eu besoin de comprendre tous ces éléments, les enjeux et les besoins de Klanik en termes de sécurité pour pouvoir apporter des éléments importants et intéressants à mettre en place à mon échelle.

Après la lecture de la PSSI, j'ai donc proposé 4 sujets sur lesquels je pourrais apporter des éléments intéressants et que je pourrais potentiellement mettre en place :

- La cartographie IT de Klanik
- Mise en place d'un réseau Wi-Fi pour les invités
- Séparation par VLANs du réseau
- Gestion des sauvegardes de la configuration des équipements.

R8.21.04	3	Lors de la mise à disposition d'un réseau wifi aux usagers externes (clients, collaborateurs externes, visiteurs…) les données suivantes doivent être collectées et conservées pour une durée minimum d'un an : - le terminal connecté (adresse MAC) - les informations sur l'identification des utilisateurs (Nom, Prénom, société, numéro de téléphone, date et heure de connexion ou mail, etc ...).
R5.09.01	1	Établir une cartographie du système métier : physique, logique et des applications (flux).
8.23	**Cloisonnement des réseaux (ségrégation)**	
Règle générale	Il faut que les groupes de services d'information, d'utilisateurs et de systèmes d'information soient cloisonnés dans les réseaux de l'organisation.	
8.13	**Sauvegarde des informations (continuité par récupération)**	
Règle générale	Il faut conserver des copies de sauvegarde de l'information, des logiciels et des systèmes et de les tester régulièrement à l'aide de la politique définie sur le thème de la sauvegarde.	

Figure 11 : Règles générales et détaillées liées aux sujets

Les 4 sujets ont été validés car ils sont utiles à l'entreprise, et se complètent les uns les autres.

C'est-à-dire que une fois la cartographie faite, on aura identifié les équipements présent et existants, ce qui nous permettra de connaitre les équipements dont la sauvegarde n'est pas sur le cloud et de gérer cela. Ensuite, avec une vision du réseau actuel, on pourra se projeter vers le futur pour voir comment on séparerait le réseau avec des VLANs et puis commencer à les mettre en place comme pour le réseau Wi-Fi invité.

Les 2 sujets qui seront traités dans ce document seront : La cartographie et la mise en place du Wi-Fi Invité.

3.2.1 La cartographie IT

La cartographie IT joue un rôle essentiel au sein d'une entreprise, car elle permet une compréhension approfondie de l'infrastructure réseau et de ses composants. Elle consiste à recueillir, à organiser et à représenter visuellement les différents éléments du réseau, tels que les équipements, les connexions et les flux de données. Elle offre une vue d'ensemble claire et détaillée de l'infrastructure informatique de l'entreprise.

Cela permet aux responsables de la sécurité de visualiser les connexions entre les systèmes, d'identifier les points faibles potentiels, de détecter les vulnérabilités et de prendre des décisions cohérentes pour renforcer la sécurité et optimiser les performances du réseau.

Pour la réalisation, nous avons les 3 types de cartographie les plus répandues :

- Physique
- Logique/réseau
- Fonctionnelle

3.2.1.1 Cartographie Physique

La cartographie physique permet de visualiser et de documenter l'emplacement physique des équipements et des ressources clés ainsi qu'une vue d'ensemble détaillée de l'infrastructure physique de l'entreprise. En identifiant et en localisant chaque composant matériel, la cartographie physique facilite la gestion et la maintenance du réseau, en permettant aux équipes informatiques de localiser rapidement les équipements, de suivre les connexions et d'effectuer des interventions si nécessaire.

En ayant une vision de l'infrastructure physique, les équipes peuvent anticiper les problèmes potentiels, optimiser l'agencement des équipements et planifier les opérations de maintenance de manière plus efficace.

De plus, la cartographie physique joue un rôle important dans l'évolution de l'infrastructure. En ayant une vue claire de l'emplacement des équipements existants, il devient plus facile d'identifier les zones disponibles pour de nouveaux équipements, d'évaluer les capacités disponibles et de prévoir les besoins futurs. Pour la cartographie, j'ai procédé par niveau c'est-à-dire que j'ai fait l'inventaire des équipements en fonction de leur position dans l'entreprise. Ce qui permet à un potentiel intervenant d'identifier directement la position d'un équipement défectueux par exemple.

Switches

Nom Equipement	Fonction principale	VLAN Portés	Infos Tech.	VLAN Admin	IP Admin
Klanik 01	Relie les prises réseau au Firewall	Aucun	Zyxel - GS1920 48HP (Non Nebula)	Aucun	Inconnu
Klanik 02	Relie les prises réseau au Firewall	Aucun	Zyxel - GS1920 24HP (Non Nebula)	Aucun	
Klanik 03	Relie les prises réseau au Firewall	Aucun	Zyxel - GS1920 24HP (Non Nebula)	Aucun	Inconnu
Switch OVER	Accès au VLAN SECU pour le système de surveillance	SECU (VLAN8)	Zyxel - GS1920 48HP (Non Nebula)	VLAN 8	

Sécurité

Nom Equipement	Fonction principale	VLAN Portés	Infos Tech.	Adresse IP WAN	Adresse IP LAN
FW13-HQ-BE1	Fait le lien entre Internet et le réseau local.	Par défaut + SECU	Zyxel – USG Flex 700 (Nebula)		

Figure 12 : Extrait de la cartographie physique

J’ai commencé par faire l’inventaire de ce qui se trouvait dans la salle réseau, là où la grande partie des principaux équipements se trouvaient. Dans cette salle réseau se trouvent plusieurs emplacements pour les équipements, la baie 1, la baie 2, ainsi que le mur. On y retrouve l’arrivée de la fibre, des switches, le firewall principal, les boitiers du système de sécurité etc. (Figure 12)

Dans un second temps il a fallu identifier tous les autres équipements qui se trouvait dans le bâtiment comme les imprimantes et le bornes Wi-Fi. Là aussi, leur position, leurs modèle et d’autres informations sont importantes à connaître en cas de panne ou d’une intervention quelconque.

Enfin, j’ai essayé de répertorier les éléments principaux qui sont dans le Cloud. Un exemple chez Klanik : un serveur appelé « Commun » qui n’est pas dans les locaux de l’entreprise mais qui est hébergé et accessible seulement par le biais d’un VPN.

La réalisation de cette première partie de cartographie a permis de savoir quels équipements sont présents dans les locaux, leur état et leur position. Nous avons aussi la connaissance des équipements dont on a besoin de récupérer les configurations (Ex : « Non Nebula » sur figure 12).

3.2.1.2 Cartographie logique/réseau

La cartographie logique ou réseau permet de représenter la topologie et les interconnexions logiques d'un réseau informatique.

Elle permet de mieux comprendre le réseau et facilite la configuration et la maintenance.

Avec cette cartographie, on établit une vue abstraite et conceptuelle du réseau et cela permet de visualiser les sous-réseaux, les segments, les connexions virtuelles et les protocoles utilisés pour acheminer les données entre les différentes parties du réseau. Ainsi les entreprises peuvent garantir un réseau efficace, fiable et évolutif pour répondre à leurs besoins opérationnels et de communication.

Après quelques semaines passées au sein de l’entreprise j’ai commencé à me familiariser avec le réseau en discutant avec les intervenants ou encore en visitant la salle réseau.

L’objectif était donc de faire une cartographie qui représente le réseau actuel, ses détails ainsi que son évolution, la manière dont on voyait le réseau de demain.

J’ai réalisé plusieurs maquettes de cette cartographie car beaucoup d’éléments étaient à prendre en compte. Avec l’aide de la cartographie physique j’ai donc pu faire la topologie du réseau en impliquant le maximum d’éléments présent dans les inventaires. Il fallait distinguer le réseau local, qui lui est divisé avec des VLANs, les connexions VPN ainsi que les éléments présents dans le Cloud.

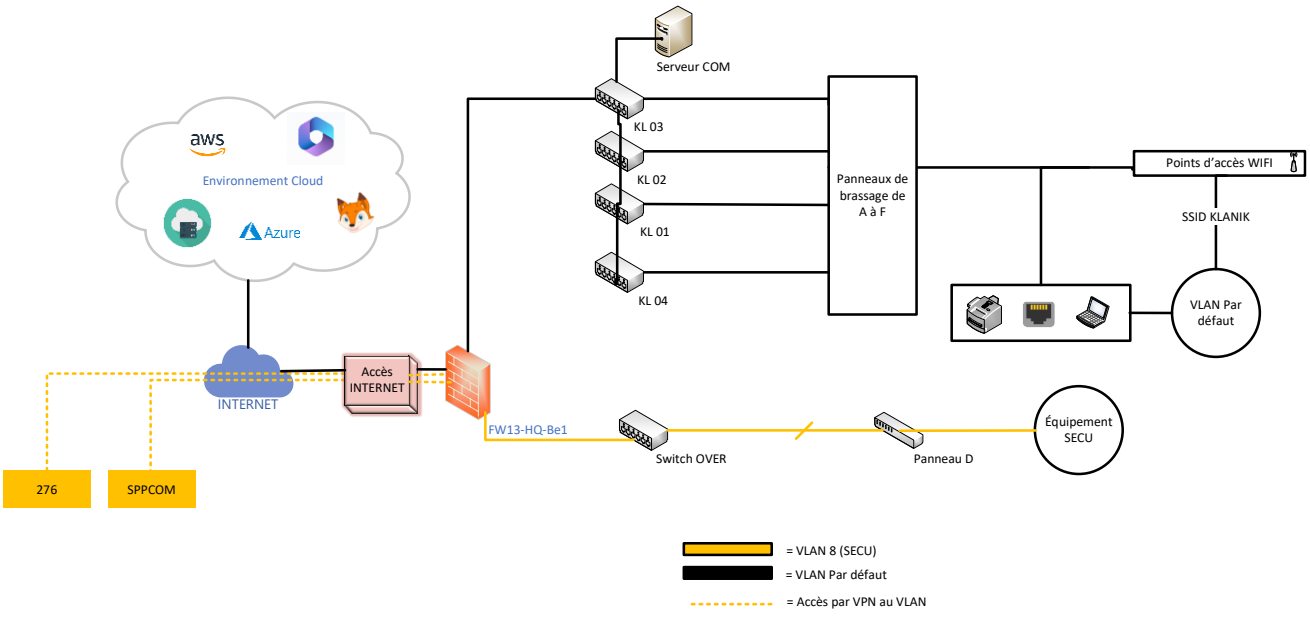


Figure 13 : Topologie du réseau actuel de Klanik

Chaque topologie générale est accompagnée de des détails des VLANs qui constituent le réseau. Dans le réseau actuel (Figure 14), le réseau est constitué du VLAN par défaut ainsi que du VLAN dédié aux équipements de sécurité. On peut aussi voir la présence des VPN qui ont accès au sous-réseaux jaune.

Si on devait détailler le réseau actuel, il serait composé des éléments suivants t :

- Le VLAN par défaut
- Le VLAN sécu
- L'arrivée INTERNET
- Le Cloud

Pour que le document soit complet et que tout soit clair, un détail des 4 éléments a été fait. C'est-à-dire que l'on se focalise uniquement sur les équipements qui interviennent dans ces éléments, donc premièrement la topologie sans les autres éléments puis un descriptif des équipements qui interviennent ainsi que l'utilité du sous réseau.

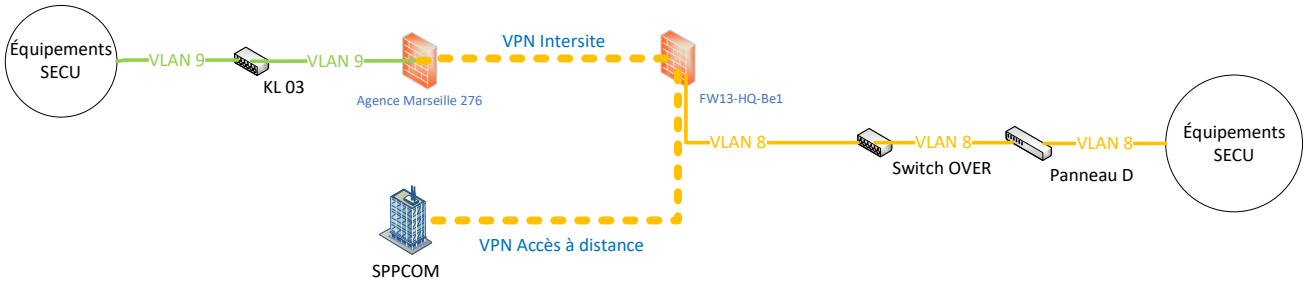


Figure 14 : Détail du VLAN sécurité

Une fois la cartographie actuelle terminée il a fallu penser aux différents sous-réseaux que l'on souhaiterait mettre en place pour anticiper un des 4 projets proposé qui est la séparation des réseaux.

La seconde partie de la cartographie est donc dédiée aux objectifs à atteindre en termes de de réseaux. On y retrouve : les nouveaux VLANs, leur détail et les nouveaux moyens d'accès à Internet.

A terme, Klanik a pour objectif de mettre en place un total de 4 sous-réseaux (Annexe 11) :

- Le VLAN sécurité (Existant)
- Le VLAN KLANIK (Actuel Par Défaut)
- Le VLAN ADMIN
- Le VLAN Guest

Le VLAN Sécurité qui existe déjà contient, comme vu précédemment, tous les équipements nécessaires au système de contrôle de porte, de vidéosurveillance, et d'alarme du bâtiment.

Le VLAN KLANIK, qui est le par défaut actuel, sera lui réservé aux utilisateurs qui sont authentifiés via le SSO, les serveurs ainsi que les imprimantes.

Le VLAN ADMIN permettra lui d'administrer les switches qui ne sont pas pilotable via Nebula. Ce qui peut permettre une manipulation des switches à distance et ainsi de gérer les sauvegardes de configurations.

Le VLAN Guest sera un sous-réseau réservé uniquement aux invités qui se connecteront au Wi-Fi. La suite du rapport abordera le sujet.

3.2.1.3 Cartographie Fonctionnelle

La cartographie fonctionnelle est un moyen de représenter les différentes activités et interactions fonctionnelles au sein d'une organisation. Elle permet de visualiser les flux d'informations entre applications, les responsabilités et les interactions entre les différents départements et les processus métier.

Elle permet aux entreprises d'avoir une meilleure compréhension et une vue d'ensemble claire des activités de chaque corps de métier. En identifiant les différentes étapes, les entrées et les sorties, ainsi que les personnes impliquées, elle facilite la visualisation des flux de travail entre les différentes fonctions de l'organisation.

La cartographie fonctionnelle a également un aspect sécurité au sein d'une organisation. En identifiant les processus métier et les flux d'informations importants, elle permet de comprendre les points d'accès potentiels aux données sensibles et de mettre en place des mesures de sécurité appropriées.

En incluant la sécurité dans la cartographie fonctionnelle, les entreprises peuvent détecter les risques liés à la confidentialité, à l'intégrité et à la disponibilité des données à chaque étape des activités. Ainsi, elles peuvent prendre des mesures de prévention pour protéger les informations sensibles, comme contrôler l'accès, chiffrer les données ou mettre en place des procédures de gestion des incidents.

Elle permet aussi de définir clairement les responsabilités de chacun en matière de sécurité. En identifiant les personnes impliquées dans chaque processus, elle clarifie les rôles et les responsabilités des acteurs ce qui sensibilise à la sécurité et donc favorise une culture de sécurité solide où chaque membre de l'organisation comprend sa part de responsabilité dans la protection des informations sensibles.

C'est dans cette optique que j'ai commencé à établir une maquette de cartographie qui recense tous les services, et applications par tous les corps de métiers présent dans la société. Pour cela j'avais à disposition une liste des services existant qui avec des informations sur chacune d'entre elles telle que le niveau de criticité du service et le type (On-Prem, SaaS…) (Annexe 6).

Une fois ces éléments à disposition je me suis rendu compte de deux choses :

- L'accès aux services se fait soit en SSO soit en créant un compte sur le service
- La plupart des flux impliquent l'utilisation de l'Azure AD

Il a donc fallu faire la distinction entre ceux qui se connectent en SSO et les autres, ainsi que les services hébergés / On-premise ou en SaaS.

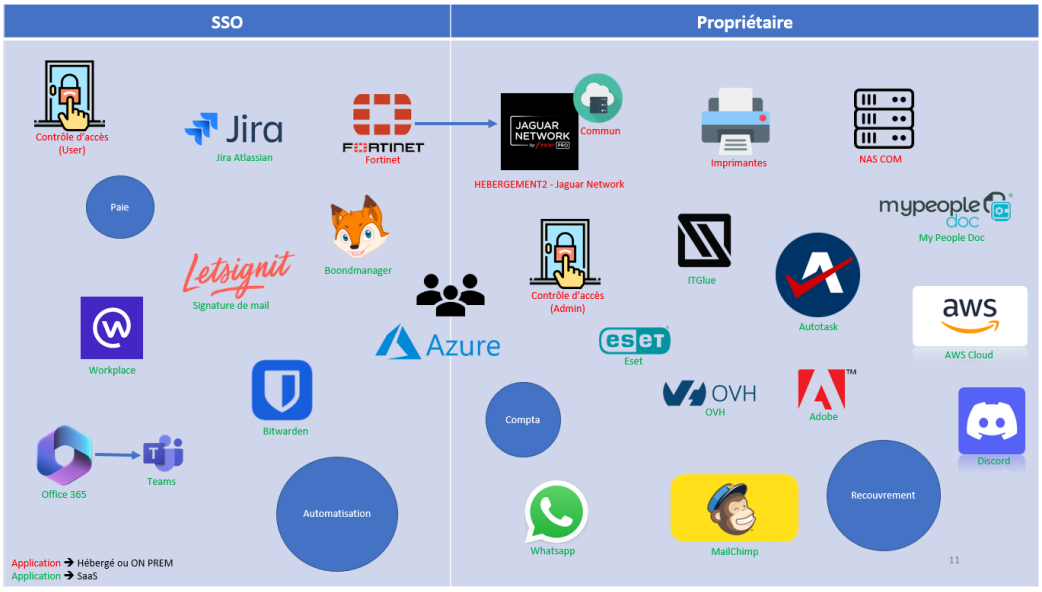


Figure 15 : Répartition des services et processus existants (Non exhaustif)

Une fois que les services utilisés étaient connus il fallait détailler les flux pour avoir une vision des applications et services impliqués dans chaque processus. C'est-à-dire de mettre en évidence les échanges entre application, les étapes pour chaque processus.

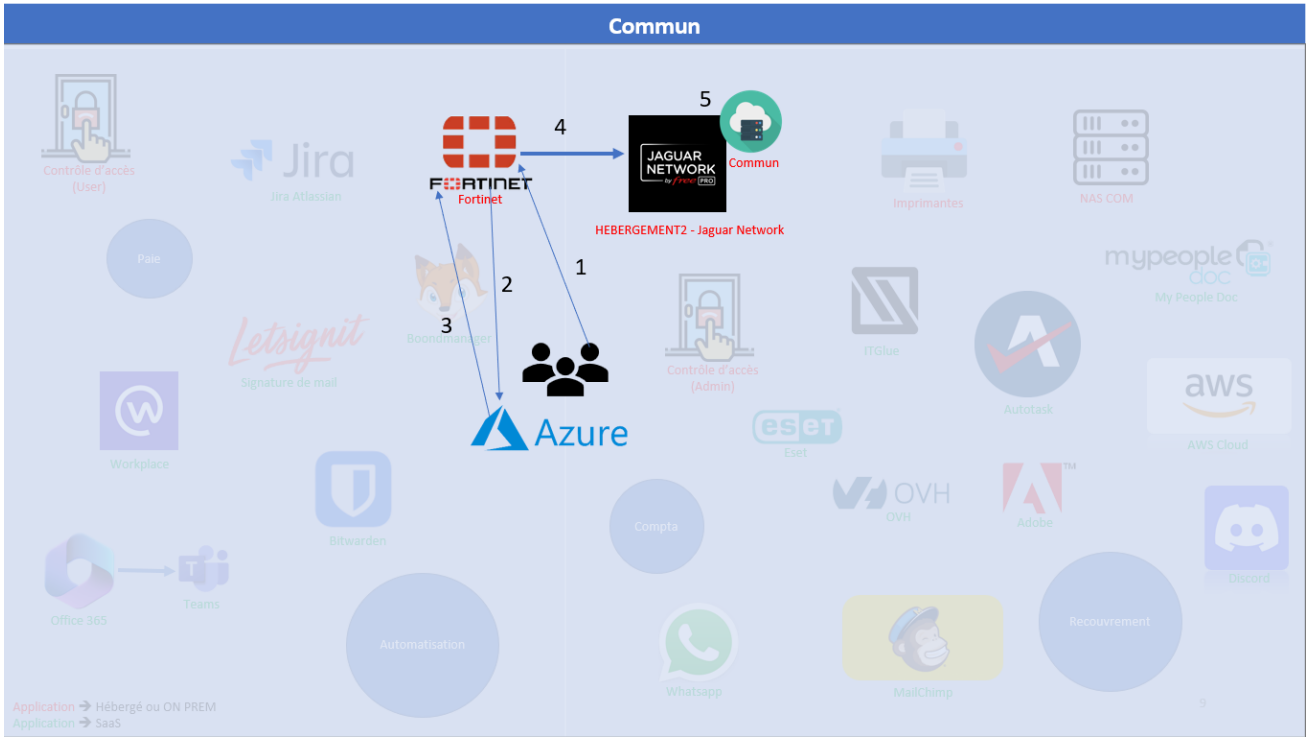


Figure 16 : Détails des flux pour accéder au serveur "COMMUN"

Ici, on peut voir comment l'accès au commun se fait. Les utilisateurs se connectent à un VPN Fortinet dont l'accès se fait en SSO avec l'Azure AD. Une fois connecté sur le VPN, on a accès au « Commun » qui lui est hébergé chez Free Pro et dont la connexion se fait avec des identifiants.

La carte que j'ai réalisée reste surement à compléter, mais elle peut-être une base de départ, Ce type de carte peut devenir chronophage si l'on souhaite lister l'ensemble des liens, des processus et interactions. Ici le but était plutôt d'avoir une vision globale de ce qui existe.

Afin de compléter cette cartographie, l'idéal serait d'interroger tous les corps de métier et de passer en revue chaque processus comme la paie, la facturation, pour ensuite identifier la totalité des services et applications présents au sein de l'entreprise et d'établir les flux qui se font pour chaque processus.

Ce qui serait un bon élément pour les équipes de transformation digitale de l'entreprise avec qui j'ai discuté et qui m'ont conseillé pour l'orientation de cette cartographie.

Ces cartographies sont importantes pour avoir une vue globale et une meilleure maîtrise de l'infrastructure IT de la société. Elles permettent d'identifier les vulnérabilités, de prendre des mesures préventives pour protéger les données sensibles. De plus, elles favorisent la sensibilisation à la sécurité car elles impactent tous les corps de métier, créant ainsi une culture de la sécurité au sein de l'entreprise.

Avec ces outils, lors de chaque changement ou panne, on pourrait potentiellement prévoir quels sont les éléments impactés, quels services sont disponibles ou non. Elles garantissent donc la continuité des opérations et renforcent la confiance des clients et des partenaires.

3.2.2 Wi-Fi Invité

Il est important d'avoir un réseau Wi-Fi invité au sein d'une entreprise car il permet aux visiteurs, aux clients et aux collaborateurs externes d'accéder à Internet de manière pratique et sécurisée, sans avoir à compromettre la sécurité du réseau interne de l'entreprise.

Le principal avantage du réseau Wi-Fi invité est qu'il isole les appareils des visiteurs du réseau principal de l'entreprise, offrant ainsi une couche de protection supplémentaire. Cela permet de réduire les risques de pertes des informations sensibles et améliore la protection des données internes.

En fournissant un accès Wi-Fi dédié aux invités, l'entreprise améliore également l'expérience de leurs visiteurs. Cela leur permet de rester connectés, de travailler à distance et d'accéder à leurs applications et services en ligne sans interruption. Un réseau Wi-Fi invité de qualité est essentiel pour maintenir une image professionnelle et accueillante, en offrant aux visiteurs le confort et la flexibilité dont ils ont besoin. Dans la PSSI, la notion de réseau Wi-Fi est abordée (figure 12), elle est donc importante pour une organisation qui tend à se plier à la norme ISO 27001.

Dans notre cas, Klanik reçoit souvent des collaborateurs externes ou des candidats qui viennent passer des entretiens, Klanik organise aussi des évènements qui rassemblent parfois des centaines de personnes. Il est donc important dans ces moments de fournir aux invités une connexion fiable mais qui ne met pas notre système de sécurité en péril.

Pour l'instant les invités se connectent au même réseau que les employés.

Chez Klanik, la configuration du Wi-Fi se fait aussi via Nebula car les point d'accès sont aussi des ZyXEL (Annexe 7). Grâce à certaines fonctionnalités disponible sur la plateforme, la compréhension et la mise en place du Wi-Fi Guest a été très efficace ;

Sur Nebula, le paramétrage de tous les points d'accès d'un même site est la même. La configuration effectuée sera poussée sur tous les points d'accès liés au site. Au sein de chez Klanik, il existe deux SSID (service set identifier), « KLANIK » et « KLANIK 2.4 GHz ». La seule différence est la fréquence de signal utilisée.

3.2.2.1 Mise en place

L'objectif est donc de créer un SSID « Klanik_Guests » qui permettra aux invités de se connecter au réseau. Ensuite, il faut choisir la méthode de connexion parmi plusieurs proposées pas ZyXEL.

La plus adaptée à notre situation était : « WPA Personal With WPA 2 » (Wi-Fi Protected Access)

C'est une solution classique avec un mot de passe pour se connecter au Wi-Fi. La solution est accompagnée d'un QR Code à scanner.

Ensuite j'ai créé un VLAN pour y isoler le SSID Guests en créant le sous-réseau avec toute ses caractéristiques (Adresse, DHCP, DNS, etc…) ainsi que l'interface LAN correspondante auprès du Firewall. Ces configurations sont les plus classiques lors de création de réseau et de sous réseau.

Après avoir configuré les bases, il fallait donc faire le nécessaire pour que le réseau soit réellement dédié aux invités.

Un réseau Wi-Fi pour invités « efficace » est une connexion sécurisée qui permet seulement à ses utilisateurs d'aller sur Internet et rien d'autre.

L'utilisateur ne peux ni communiquer avec les autres équipements présents sur le réseau, que ce soient les autres utilisateurs ou les appareils comme les imprimantes.

Ces limitations auraient très bien pu être mises en place grâce à des règles de firewall mais l'avantage que ZyXEL a est l'existence de 2 outils qui permettent d'atteindre nos objectifs d'une manière plus optimisée.

Ces deux outils sont :

- Le « layer 2 isolation »
- Le « Intra-BSS traffic blocking »

Avec ces 2 paramètres, on a pu mettre en place un réseau Wi-Fi efficace et sécurisé.

Le « Layer 2 isolation » est une technique de sécurité qui vise à séparer les communications au niveau du réseau local en limitant les échanges entre les différents périphériques. Cela signifie que les appareils connectés au même réseau local ne peuvent pas se voir mutuellement ni accéder aux données des autres appareils.

Cela limite la propagation de logiciels malveillants ou d'attaques potentielles entre les appareils des utilisateurs du réseau invité et permet également d'empêcher l'accès non autorisé au réseau local de l'entreprise.

Pour pouvoir réaliser cela, il faut activer l'option sur Nebula (Annexe 8). Mais ce que fait réellement l'option c'est créer une liste blanche d'adresses MAC avec laquelle les appareils connectés au SSID correspondant pourront échanger. Pour isoler les utilisateurs et permettre l'accès seulement à Internet, seule l'adresse MAC de la passerelle est incluse dans la liste blanche. Ce qui signifie qu'un utilisateur qui se connecte au réseau invité pourra « discuter » uniquement avec la passerelle qui elle, lui permettra d'accéder à Internet.

Pour tester j'ai connecté 2 appareils au réseau via le SSID « Klanik_Guest » et j'ai testé les connectivités :

```
C:\Users\hmouigni>ping 192.168.31.56

Envoi d'une requête 'Ping'  192.168.31.56 avec 32 octets de données :
Réponse de 192.168.29.46 : Impossible de joindre l'hôte de destination.
Réponse de 192.168.29.46 : Impossible de joindre l'hôte de destination.
Réponse de 192.168.29.46 : Impossible de joindre l'hôte de destination.
Réponse de 192.168.29.46 : Impossible de joindre l'hôte de destination.

Statistiques Ping pour 192.168.31.56:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
```

Figure 17 : Résultat du ping avec le "Layer 2 isolation"

Les appareils, malgré qu'ils soient connectés au même réseau, pouvaient accéder à Internet mais les pings entre eux n'aboutissait pas. On a donc bien rempli les objectifs pour le Wi-Fi Guest. J'ai aussi fait des tests pour vérifier que lorsque je retirais l'option, les pings était réalisés avec succès (Annexe 9).

En ce qui concerne le « Intra-BSS traffic blocking », cette option est automatiquement activée lorsque la précédente l'est aussi. L'objectif ici est de pouvoir bloquer les communications entre les équipements qui seraient connectés au même point d'accès mais avec un SSID différent. Elle contribue également à optimiser les performances du réseau en évitant les collisions et la congestion. Dans ce cas aussi les tests de ping étaient concluants :

```
C:\Users\hmouigni>ping 192.168.29.52

Envoi d'une requête 'Ping'  192.168.29.52 avec 32 octets de données :
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.

Statistiques Ping pour 192.168.29.52:
    Paquets : envoyés = 4, reçus = 0, perdus = 4 (perte 100%),
```

Figure 18 : Résultat du ping avec le « Intra-BSS traffic blocking »

Après avoir réalisé les tests, nous avons conclu que le service rendu par ces options suffisait amplement en termes d'isolation et donc que la création d'un VLAN n'était pas nécessaire et que l'on pouvait donc supprimer celui créée en amont.

3.2.2.2 Limites du réseau

Le Wi-Fi Guest étant mis en place il a fallu réfléchir à comment le réguler pour que les utilisateurs bénéficient d'une expérience correcte en termes de performance et que le tout soit sécurisé. Deux idées sont ressorties et concordaient bien avec ce que ZyXEL proposait :

- Limiter le débit
- Programmer des horaires de disponibilité du SSID

Pour répondre à ces deux besoins, nous avons utilisé Nebula qui contient deux outils spécifiques pour accomplir ces tâches. Le premier est une sorte de jauge qui permet de déterminer le débit maximum par client en débit « Upload » et « Download » (Annexe 10).

Le fait d'instaurer une limite de débit pour les invités sur le réseau Wi-Fi offre plusieurs avantages en termes de sécurité et de gestion des ressources. Cela permet de prévenir les abus, de protéger contre les attaques par déni de service (DoS) qui est la cyberattaque la plus courante. Les attaques DoS visent à saturer la bande passante d'un réseau en envoyant un trafic excessif.

Cela permet aussi de gérer la qualité de service (QoS) car on évite qu'ils consomment excessivement les ressources réseau, ce qui pourrait impacter négativement les performances globales du réseau.

Pour jauger quel était le bon débit à accorder on a fait une simulation de l'activité la plus répandue qui se fait dans les locaux : Les appels vidéo Teams.

Limité à 5Mb/s, l'appel s'est parfaitement déroulé et on a jugé que c'était suffisant. Voici une comparaison de tests de débit avant et après la mise en place de la limite :

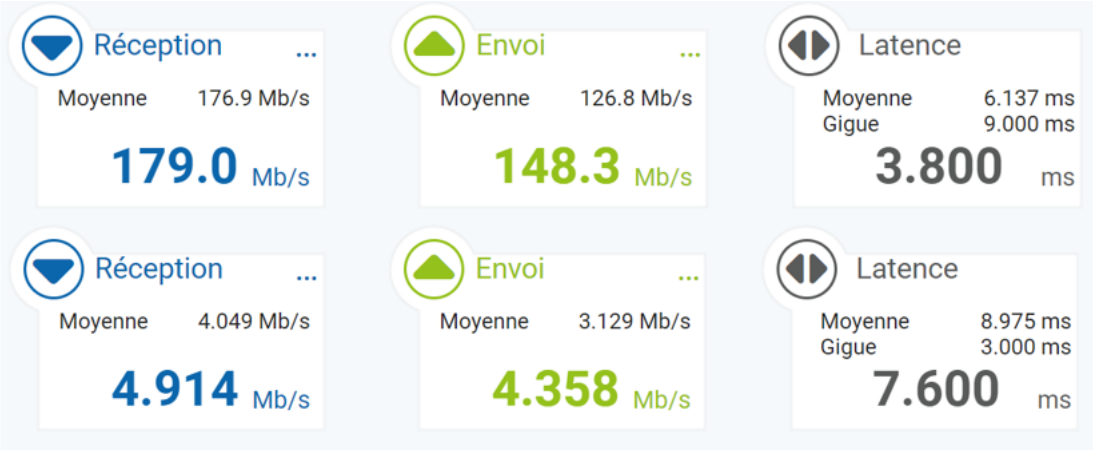


Figure 19 : Comparaison de débit avant/après la limite

Malgré la diminution du débit pour les invités, on peut voir que l'application de cette limite permet de maintenir des conditions d'utilisation très correctes tout en préservant les performances et la sécurité globales du réseau.

La disponibilité du SSID est aussi un élément à prendre en compte lors de ce genre de mise en place. Cela offre une meilleure sécurité, en limitant l'exposition du réseau sans fil seulement aux périodes où il est réellement nécessaire. Cela réduit la surface d'attaque potentielle en empêchant les connexions non autorisées en dehors des heures de fonctionnement prévues.

C'est aussi un moyen d'améliorer les performances globales car si plusieurs SSID coexistent dans la même zone, il y a des risques d'interférences et forcément en le rendant indisponible, on peut économiser la bande passante ainsi que de l'énergie.

Pour répondre à ce besoin, ZyXEL met à disposition un outil qui permet de créer des emplois du temps pour SSID. On peut adapter les heures, retirer des jours de disponibilités, créer des pauses.

Dans notre cas, nous avons préféré établir un emploi du temps qui respecte les heures de travail. C'est-à-dire du lundi au vendredi de 7h30 à 20h. Cela signifie que le SSID sera activé uniquement pendant ces plages horaires et sera indisponible après ces horaires.

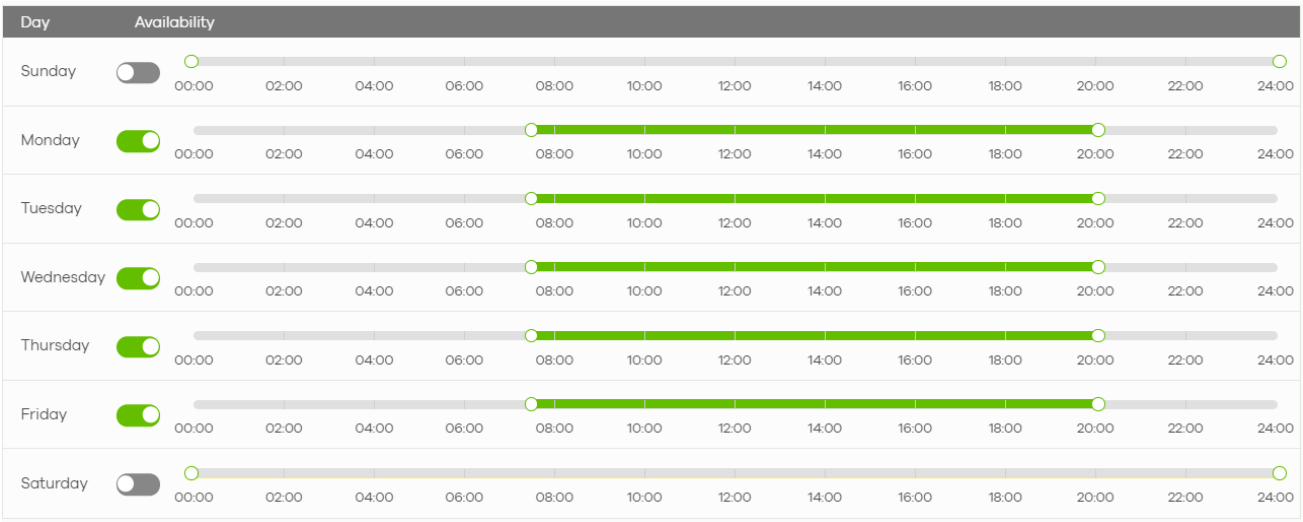


Figure 20 : Interface de gestion d'emploi du temps

La mise en place du réseau Wi-Fi a été réalisée avec succès en prenant en compte différents éléments clés tels que la configuration des bornes Wi-Fi, la gestion des SSID, la sécurité des accès et la gestion des disponibilités.

Les tests réalisés ont confirmé la performance et la fiabilité du réseau Wi-Fi, en respectant les besoins de sécurité. Les différentes fonctionnalités, telles que la gestion des accès avec des méthodes d'authentification adaptées ou encore la limitation du débit pour les invités et le « Layer 2 isolation », ont contribué à renforcer la sécurité et la stabilité du réseau.

Un point que l'on pourrait améliorer serait la mise en place d'un moyen de récupération des informations et de l'adresse MAC de l'invité comme il est indiqué dans la PSSI (Figure 11). Cela pourrait se faire via un portail captif par exemple. Mais cela impliquerait une réflexion sur que faire des données et de tout ce qui concerne le RGPD (Règlement général sur la protection des données).

Après avoir effectué ces tests concluants, la mise en place du réseau Wi-Fi a été déployée de manière officielle dans les locaux du siège et de l'agence de Marseille.

4 Conclusion

Lors de mon stage, j'ai réalisé divers travaux de recherche, de pratique, et j’ai surtout participé à deux projets principaux : la cartographie et la mise en place du réseau Wi-Fi invité.

Pour la cartographie, j'ai pu réaliser comme je le souhaitais deux des trois cartographies prévues, fournissant ainsi une vision détaillée d'une grande partie du réseau de l'entreprise. J'ai également pu démarrer la troisième cartographie et poser les bases pour son développement futur.

Par ailleurs, certaines recherches, notamment celles portant sur le SSO (Single Sign-On), ont été laissées en suspens car là n'était pas la priorité, laissant ainsi des perspectives d'évolution et de développement pour de futurs travaux.

Ce stage m'a permis de découvrir un nouvel aspect des réseaux d'entreprise et de la cybersécurité. J'ai beaucoup appris sur le plan professionnel que ce soit en pratiquant mais aussi en observant notamment lors des interventions et des mises en place comme les changements d’équipements et leurs configurations. J 'ai découvert de nouveaux outils dont la plupart me seront utiles pour la suite de ma carrière mais surtout de nouvelles notions qui elles solidifient et enrichissent mes connaissances.

J'ai aussi pu mettre en application et approfondir mes compétences de synthèse et de rédaction qui m'aideront elles aussi dans mon quotidien.

Les formations que j'ai suivies à l'IUT ont grandement contribué à mon expérience de stage en me permettant de mieux comprendre les concepts et les termes techniques liés au domaine de la cybersécurité et des réseaux. J'ai ainsi pu acquérir de nouvelles notions, approfondir mes connaissances notamment sur les VLANs et mieux comprendre les enjeux de la sécurité des réseaux en entreprise.

Cette expérience a également eu un impact positif sur mon projet professionnel, en consolidant mon intérêt déjà existant pour le domaine de la cybersécurité. Elle m'a permis d'approfondir mes connaissances et compétences dans ce domaine en constante évolution, tout en me donnant une vision plus concrète des différentes opportunités de carrière qui s'offrent à moi.

Au-delà des aspects techniques, j'ai également eu l'opportunité de découvrir la dimension humaine et le management au sein de l'entreprise, l'équipe a fait preuve d'une grande disponibilité et d'un réel intérêt à partager leurs connaissances.

J'ai bénéficié d'un encadrement attentif de la part de mon maître de stage qui a su instaurer un bon équilibre entre l'autonomie et l'accompagnement ce qui est important pour une première dans le milieu professionnel.

Remerciements

Je tiens à exprimer ma profonde gratitude à toutes les personnes qui ont rendu possible la réalisation de ce stage et ce rapport.

Premièrement, je souhaite exprimer ma reconnaissance à l'ensemble de l'équipe de KLANIK qui m'a accueilli au sein de leur structure. Merci pour votre confiance et votre ouverture.

Je tiens à remercier particulièrement Julien MONTROZIER, Responsable Sécurité des Systèmes d'Information, qui m'a guidé tout au long de ce stage. Sa disponibilité, son expertise, sa patience et son professionnalisme ont été d'une grande importance pour moi.

À toute l'équipe de la Direction des Operations, notamment David CAUSSINUS et Audrey GUILLOUX, merci pour votre aide, votre soutien et les échanges enrichissants. Vous avez contribué à faire de ce stage une expérience très bénéfique pour mon développement professionnel et personnel.

Je voudrais également souligner l'importance des équipes de ONE COMPUTER avec lesquelles j'ai eu le plaisir de travailler et d'échanger au cours de mon stage. Leurs compétences techniques et leur professionnalisme ont enrichi mon expérience. En particulier, je tiens à remercier Jean-Baptiste SENGHOR, avec qui j'ai réalisé plusieurs interventions pratiques. Sa patience et sa volonté de partager ses connaissances ont eu un impact significatif sur mon apprentissage et ma compréhension du domaine.

Je souhaite également exprimer ma gratitude à l'ensemble des professeurs l'IUT Réseaux & Télécommunications de Marseille. Grâce à eux, j'ai acquis des connaissances qui m'ont aidé à comprendre et à évoluer dans le domaine de la sécurité des systèmes d'information.

J'aimerais remercier aussi remercier ma famille et mes amis pour leur soutien inconditionnel, leurs encouragements et leur écoute tout au long de cette période.

5 Glossaire

ESN : Entreprise de Services du Numérique, Société offrant des services dans le domaine des technologies de l'information et de la communication.

ISO : International Organization for Standardization (Organisation internationale de normalisation)

SSO : Single-Sign-On, Authentification unique pour accéder à plusieurs applications ou systèmes avec un seul ensemble d'identifiants

Active Directory : Service de répertoire de Microsoft pour la gestion centralisée des utilisateurs, groupes et ressources réseau

Clés pré-partagées : Les clés pré-partagées sont des clés de chiffrement ou d'authentification partagées à l'avance entre les parties communicantes pour sécuriser les échanges

Extension : Une extension d'application est un module additionnel qui ajoute des fonctionnalités ou des capacités supplémentaires à une application existante.

VLAN : Virtual Local Area Network. C'est une technologie de réseau qui permet de diviser un réseau local physique en plusieurs sous-réseaux virtuels.

VPN : Virtual Private Network, c'est un réseau sécurisé qui permet de créer une connexion cryptée entre un appareil et un réseau distant, offrant ainsi une confidentialité et une sécurité lors de l'accès à Internet ou à des ressources réseau.

DHCP : Dynamic Host Configuration Protocol, protocole réseau qui attribue automatiquement des adresses IP et d'autres paramètres de configuration aux dispositifs connectés à un réseau

Backup : Solution de secours en cas de panne. Signifie « sauvegarde »

Chiffrer : crypter des données ou du contenu en les convertissant dans un format illisible ou codé, afin d’assurer leur confidentialité

SSID : Service Set Identifier, c’est le nom attribué à un réseau sans fil pour se connecter à un réseau spécifique

WPA : Wi-Fi Protected Access, Protocole de sécurité pour les réseaux sans fil, offrant chiffrement des données et authentification des utilisateurs.

LAN : Local Area Network, Réseau local permettant la communication entre les appareils connectés localement

Adresse MAC : Identifiant unique d'une interface réseau permettant l'identification d'un périphérique sur un réseau local.

Ping : La commande "ping" permet de tester la connectivité avec un appareil distant en envoyant des paquets et en mesurant le temps de réponse

Upload : Envoi de données depuis un appareil local vers un emplacement distant

Download : Téléchargement de données depuis un emplacement distant vers un appareil local.

6 Sitographie

https://learn.microsoft.com/en-us/azure/active-directory/fundamentals/auth-radius

https://www.amazon.com.be/deleyCON-Testeur-C%C3%A2bles-R%C3%A9seau-Patch/dp/B09MQQR5LQ

https://fr.wikipedia.org/wiki/ISO/CEI_27001

https://www.iso.org/fr/standard/27001

https://academie2080.com/pdca-plan-do-check-act/

https://support.zyxel.eu/

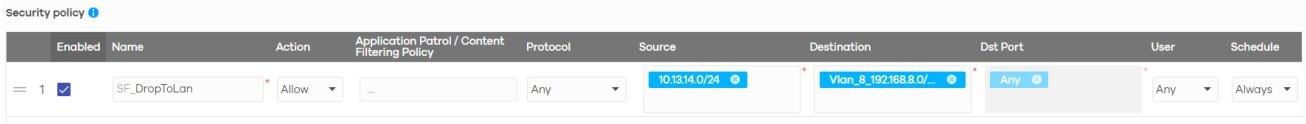
ANNEXES

Annexe 1 :

Name	Subnet	Use VPN
lan1	192.168.16.0/24	
lan2	192.168.17.0/24	
Vlan_Secu_9	192.168.9.0/24	

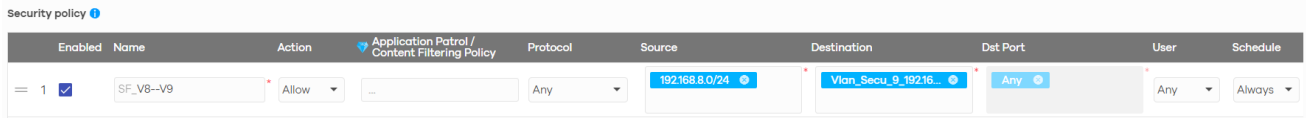
Annexe 1 : Réseaux locaux de l'agence dans le VPN

Annexe 2 :



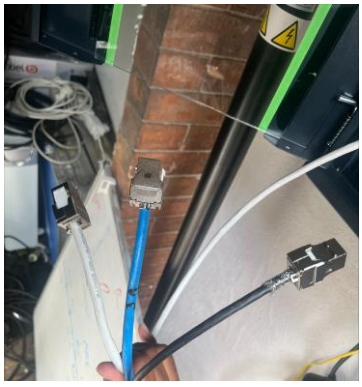
Annexe 2 : Règle de Firewall pour le client distant

Annexe 3 :



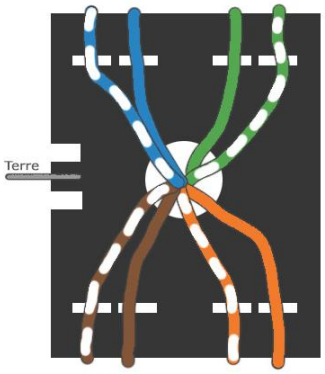
Annexe 3 : Règle de Firewall pour le trafic entre VLANs

Annexe 4 :



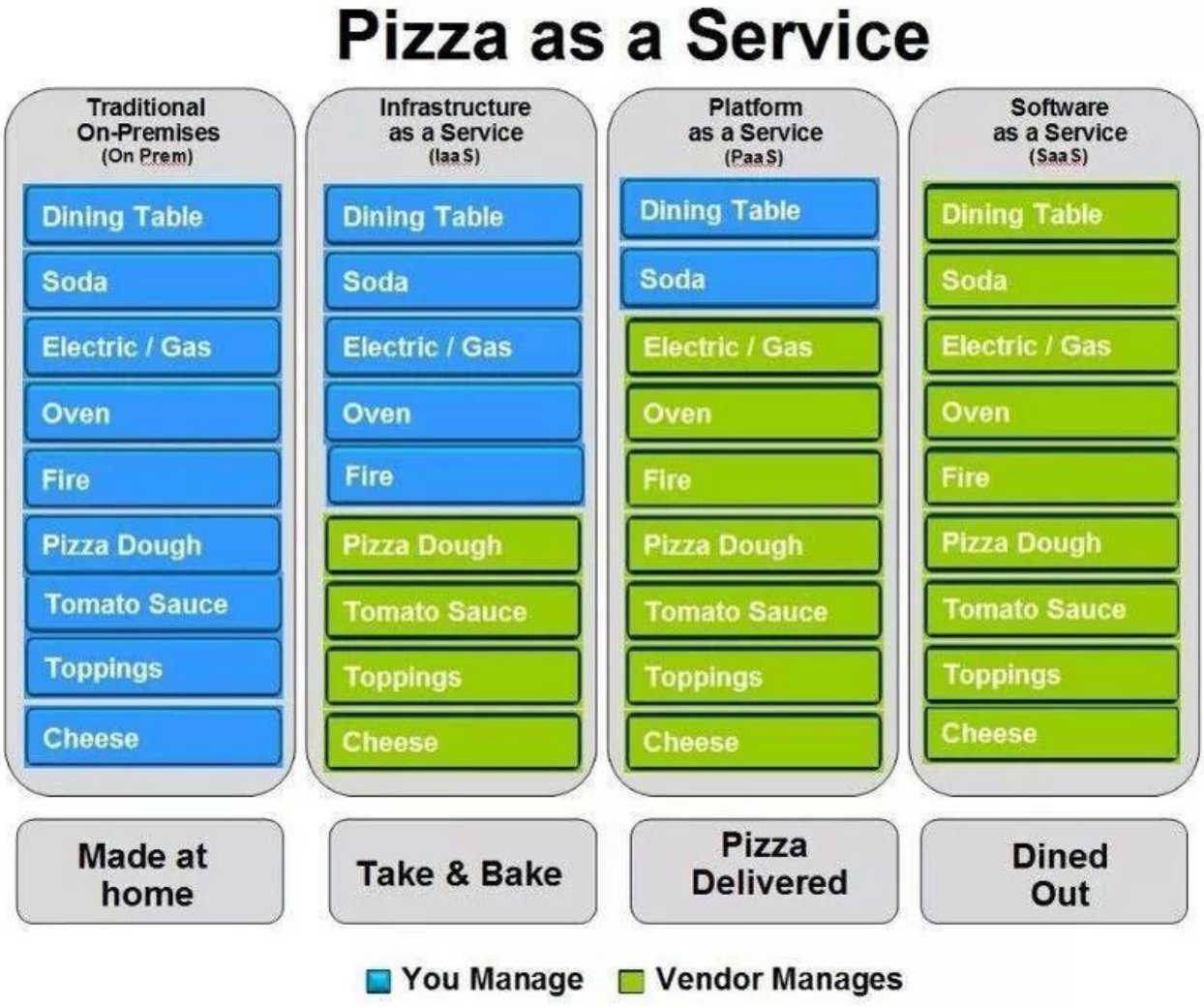
Annexe 4 : Réalisation des noyaux

Annexe 5 :



Annexe 5 : Cablage d'un noyaux

Annexe 6 :

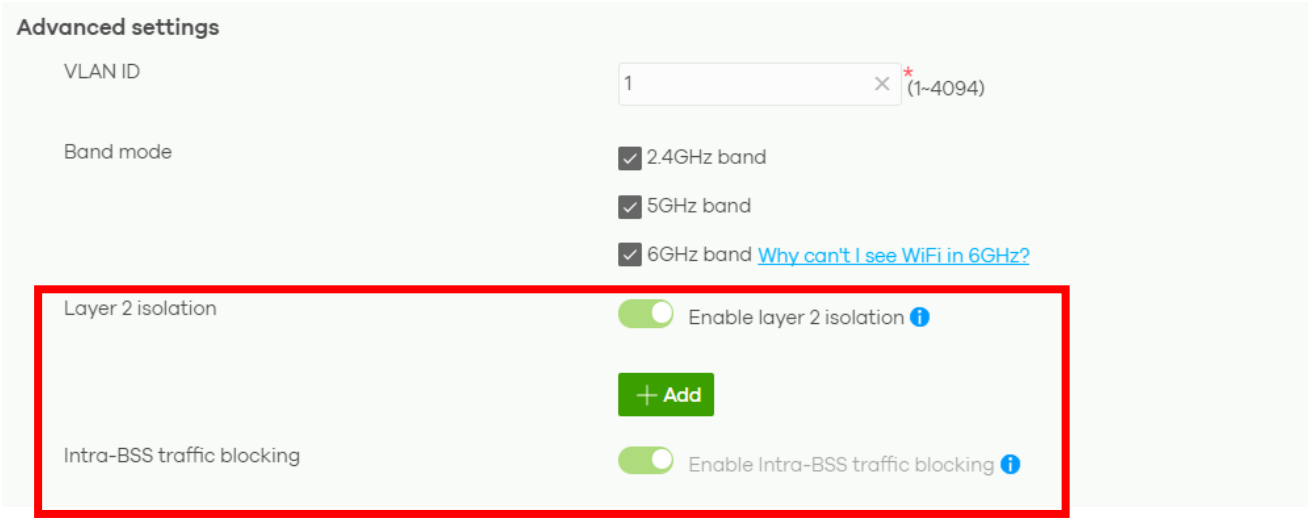


Annexe 6 : Différences entre les services comparé à une pizza

Annexe 7 :

Annexe 7 : Borne Wi-Fi ZyXEL NWA110AX

Annexe 8 :



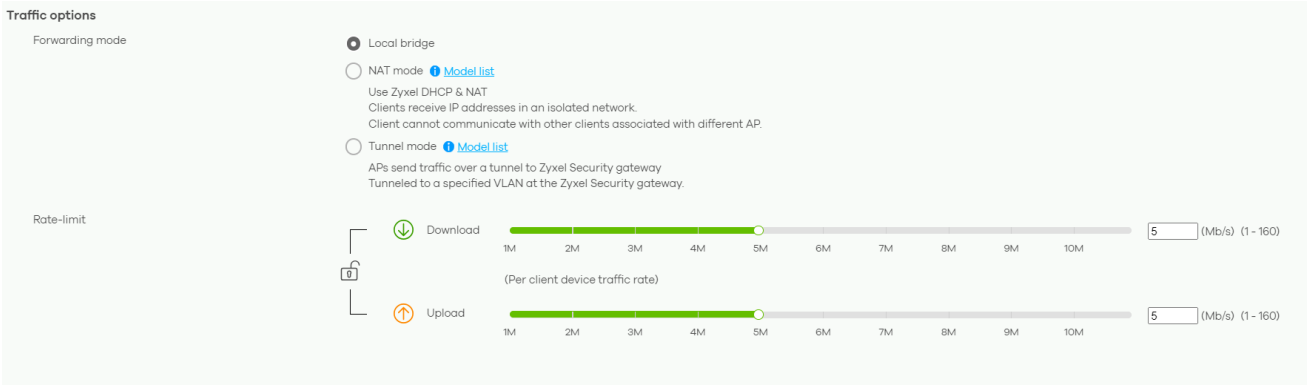
Annexe 8 : Options à activer

Annexe 9 :

```
PS C:\Users\:                 > ping 192.168.16.174

Envoi d'une requête 'Ping'  192.168.16.174 avec 32 octets de données :
Réponse de 192.168.16.113 : Impossible de joindre l'hôte de destination.

Statistiques Ping pour 192.168.16.174:
    Paquets : envoyés = 1, reçus = 1, perdus = 0 (perte 0%),
Ctrl+C
PS C:\Users'                  > ping 192.168.16.174

Envoi d'une requête 'Ping'  192.168.16.174 avec 32 octets de données :
Réponse de 192.168.16.174 : octets=32 temps=275 ms TTL=64
Réponse de 192.168.16.174 : octets=32 temps=91 ms TTL=64
Réponse de 192.168.16.174 : octets=32 temps=9 ms TTL=64
Réponse de 192.168.16.174 : octets=32 temps=18 ms TTL=64
```

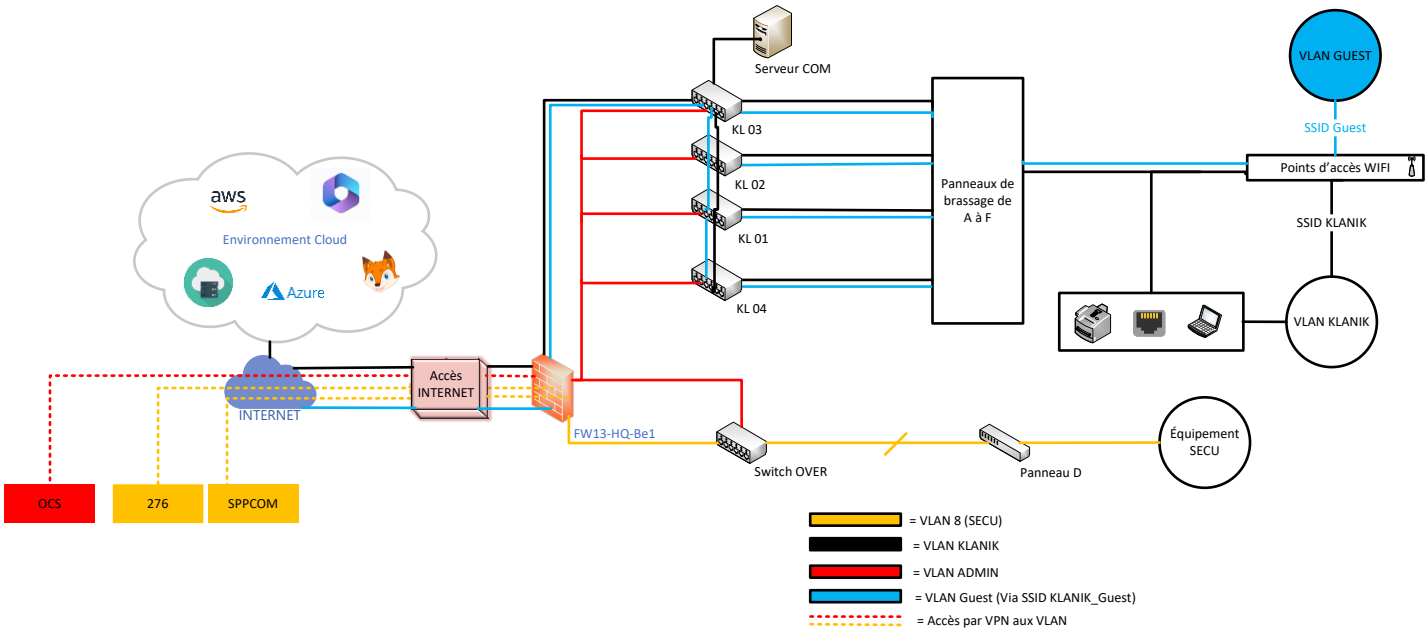
Annexe 9 : Ping sans succès puis réponse

Annexe 10 :



Annexe 10 : Jauge pour la limite de débit

Annexe 11 :



Annexe 11 : Cartographie logique/Réseau à terme