Institut Universitaire de Technologie,
Aix-Marseille Université

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

SÉGMENTATION DU RÉSEAU

Aymane El MOUTAOUAKKEL
Clément DALIES

KLANIK

Responsable entreprise : Julien MONTROZIER

Responsable académique : Éric SOCCORSI

2024

Table des matières

1 Introduction

Durant notre stage au sein du siège social de KLANIK, nous avons été impliqués dans un projet crucial de segmentation du réseau, au sein du service de sécurité informatique. Notre objectif principal était de contribuer à renforcer la sécurité du réseau en mettant en œuvre des mesures de segmentation efficaces.
Dans cette perspective, nous avons été chargés de diverses missions, notamment l'analyse des besoins de sécurité, la conception de la segmentation du réseau, la configuration des équipements réseaux, et la documentation des processus et des procédures associés.
Ce rapport est articulé autour de trois axes principaux : tout d'abord, nous présenterons l'entreprise KLANIK et son service de sécurité informatique, ensuite nous examinerons en détail les objectifs et les missions de notre stage, et enfin nous détaillerons les étapes du stage, incluant l'analyse des processus de segmentation du réseau, les résultats obtenus, et les recommandations pour l'amélioration continue de la sécurité du réseau chez KLANIK.

2 L'entreprise KLANIK

2.1 Introduction

Dans le paysage de la transformation numérique, KLANIK se distingue par son rôle pivot en matière d'innovation et de leadership. Grâce à sa vision visionnaire et à son engagement sans faille envers l'excellence, KLANIK incarne l'alliance entre expertise technique et stratégie créative. Cette collaboration permet à KLANIK de développer des solutions personnalisées qui propulsent ses clients vers le succès dans un monde numérique en perpétuelle évolution.

2.2 Présentation

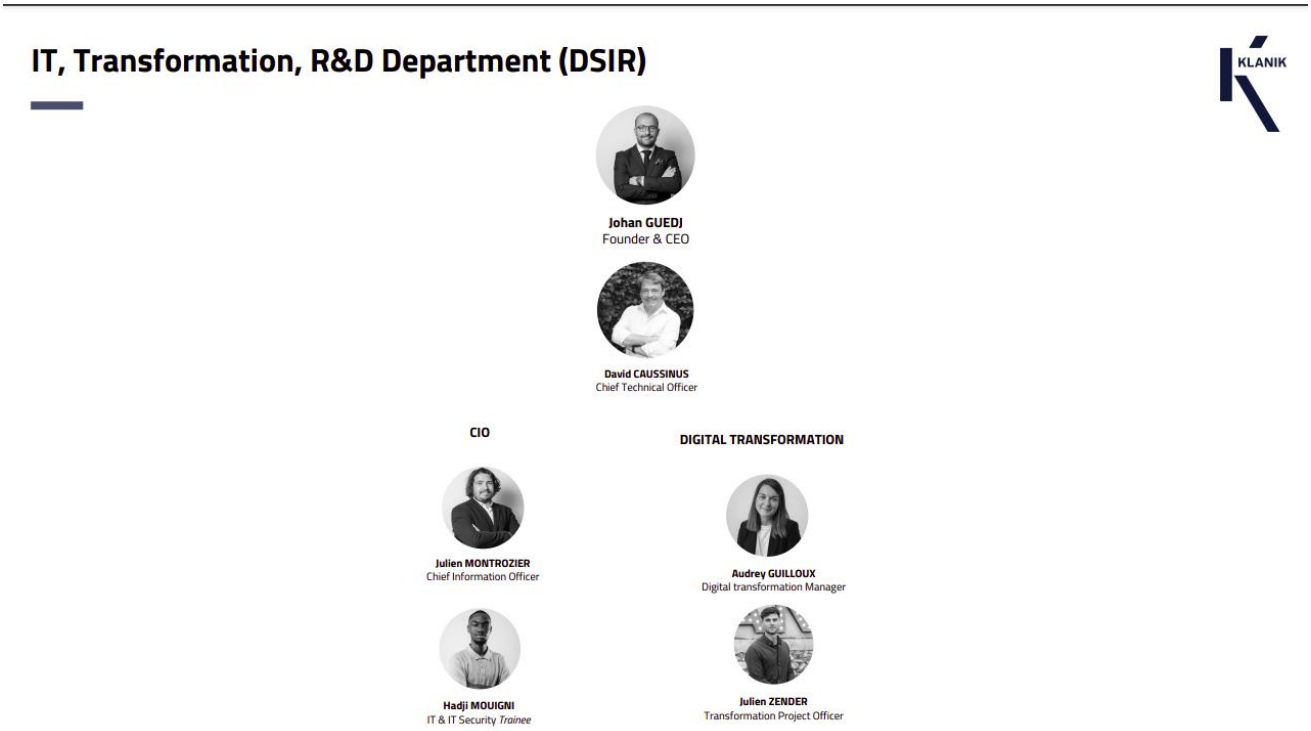
Fondée en 2011 par Johan GUEDJ, KLANIK est une société de conseil en ingénierie informatique, leader dans le domaine de la transformation digitale. KLANIK accompagne les grandes entreprises dans leurs projets technologiques, couvrant notamment les domaines du logiciel, de la cybersécurité et du cloud. En 2023, KLANIK est devenue une société à mission, affirmant son engagement envers des objectifs sociaux et environnementaux.
Avec une équipe de plus de 800 talents répartis dans 12 agences à travers le monde, KLANIK mise sur l'expertise et l'engagement de ses collaborateurs pour proposer des solutions innovantes à ses clients. Son modèle d'entreprise, fondé sur les valeurs de partage, de bienveillance et d'exigence, favorise l'épanouissement professionnel de chacun. À travers des initiatives telles que KONSCIOUS et KLANIK ESPORT, KLANIK encourage l'engagement et la collaboration au sein de son écosystème.
Le siège social de KLANIK est situé à Marseille, au 221 avenue du Prado. C'est depuis ce lieu que l'entreprise gère ses opérations internationales et développe ses projets. En s'appuyant sur une base solide d'expertise et de compétences, KLANIK se positionne comme un acteur clé de la transformation digitale pour ses clients, tout en cultivant un environnement de travail propice à l'épanouissement et à l'engagement de ses employés.

2.3 Organigramme

Le personnel de KLANIK se distingue de celui d'une entreprise classique. Il existe trois groupes distincts d'employés au sein de la société.
En tête d'affiche, se trouvent les consultants, ce sont les employés se déplaçant chez les clients, c'est-à-dire les entreprises ayant un contrat avec KLANIK. Ils apportent leur expertise directement sur le terrain, en travaillant sur les projets technologiques des clients. Ce sont pour dire, les produits de KLANIK.

Ensuite, il y a les freelances. À l'instar des consultants, ils se déplacent chez les clients, mais la différence principale est qu'ils travaillent à leur propre compte. KLANIK joue le rôle de médiateur entre le freelance et le client, facilitant la mise en relation et la collaboration entre les deux parties.
Enfin, le staff regroupe les employés de KLANIK qui travaillent directement pour l'entreprise. Ils s'occupent de la gestion interne de la société, assurant le bon fonctionnement des opérations et le soutien aux consultants et aux freelances. Le staff est lui-même divisé en plusieurs corps de métier : Ressource Humaine (RH), Business Manager (BM), Comptabilité, communication, finance, etc...
L'équipe dans laquelle nous avons fait notre stage est celle qui s'occupe de l'IT de l'entreprise. Ce corps de métier et très récent chez KLANIK, symbolisant une volonté de re centralisé la gestion du réseau et des technologies de l'entreprise, autrefois sous-traité totalement à une autre entreprise de service, One Computer Services (OCS).

Les membres de ce service sont organisés de la manière suivante :



2.4 Département IT

Comme le montre l'organigramme, le département IT est composé d'une seule personne, le Responsable de la Sécurité des Systèmes d'Information (RSSI). Il est le garant de la sécurité des systèmes d'information et s'occupe de définir et déployer la politique de sécurité de l'information de l'entreprise, tout en assurant la mise en œuvre et le suivi des projets et des réalisations techniques. Il gère également la protection des données sensibles, la prévention des cyberattaques et la gestion des risques informatiques.

En plus de ses responsabilités en matière de sécurité, 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 efficacement.

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 SERVICE, qui s'occupe des différentes réalisations techniques ainsi que de tout ce qui concerne l'IT en général chez KLANIK.

3 Projet du stage

Au cours de notre stage chez KLANIK, nous avons été assignés à un projet crucial visant à remodeler leur réseau local (LAN). L'objectif principal de ce projet était d'améliorer la sécurité et la gestion du trafic réseau de l'entreprise. Il nous a donc fallut diviser ce projet en plusieurs étape pour éviter toute précipitation.

3.1 Étude Préliminaire et Analyse des Besoins :

Nous avons commencé par une analyse approfondie des besoins de l'entreprise en matière de sécurité réseau et de gestion du trafic. Cette analyse s'est déroulée en deux volets : une évaluation physique des infrastructures et une étude technique du réseau existant.

3.1.1 Évaluation Physique

Le bâtiment de KLANIK se compose de quatre étages plus un jardin. Chaque étage est aménagé avec des bureaux, des open space et des salles de réunion. Il est courant que les employés se déplacent entre les étages pour collaborer avec d'autres collègues, travailler dans différentes salles de réunion, ou se rendre dans des zones spécifiques comme le jardin ou la zone de détente située au rez-de-jardin.

3.1.2 Étude Technique

D'un point de vue technique, chaque étage est équipé d'environ trois points d'accès (Access Points, AP) pour garantir une couverture Wi-Fi optimale. La majorité des employés utilisent une connexion Wi-Fi pour leurs activités professionnelles, principalement via leurs ordinateurs portables professionnels et leurs téléphones personnels. Bien que la majorité des appareils soient connectés via Wi-Fi, il existe également des connexions filaires Ethernet pour les serveurs et certains ordinateurs portables. Presque toutes les salles sont équipées de prises Ethernet pour ceux qui nécessitent une connexion filaire.
Le nombre maximal d'appareils connectés simultanément au réseau ne dépasse jamais 300 adresses IP, un pic atteint uniquement lors d'événements importants comme les réunions trimestrielles "ALLSTAFF". Pendant ces événements, tous les employés des différentes agences mondiales se réunissent au siège social (Headquarters, HQ) pour une réunion annuelle.
Le réseau de KLANIK repose principalement sur des équipements de la marque ZyXEL. Les switches, les points d'accès (AP) et le firewall sont tous des produits ZyXEL. Le monitoring du réseau est effectué via NEBULA, la plateforme cloud de ZyXEL.

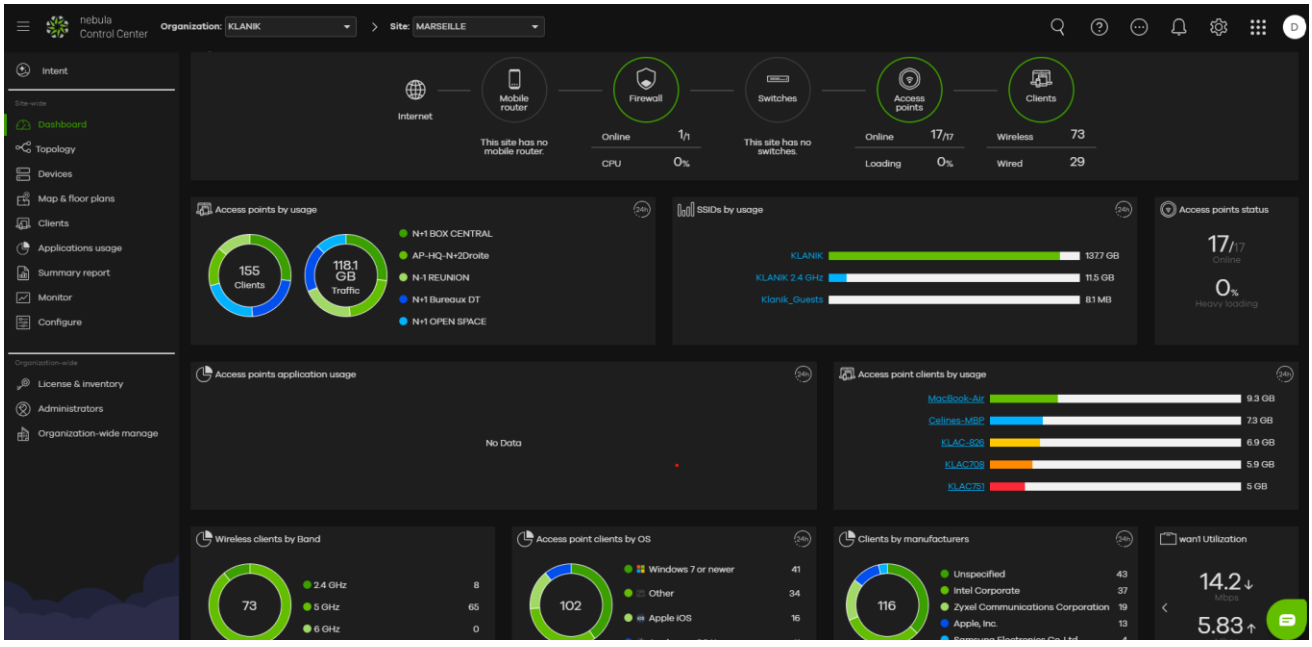


Figure 1 - Interface NEBULA

Grâce à l'interface NEBULA, il est possible de gérer et de configurer les appareils du réseau ZyXEL. Les points d'accès (AP) et le firewall peuvent être configurés et surveillés directement depuis cette

plateforme. Cependant, il est important de noter que les switches ne sont pas disponibles sur cette interface en raison de leur ancienneté, ce qui les rend incompatibles avec NEBULA. Ce problème d'incompatibilité représente un défi que nous devrons aborder ultérieurement.
Quant à la gestion des besoins de chacun en therme de réseau, il est quasiment identique pour tous. Ce qui fait que nous n'avons pas besoin de nous soucier de ce détail.

3.2 Planification et Définition des Étapes du Projet

Avant de se lancer dans la réalisation du projet, il est crucial de poser les problématiques, diviser le travail et définir les différentes étapes nécessaires. Cette planification permet de structurer les actions et de les prioriser efficacement.
Les trois grandes étapes définies pour ce projet sont :

1. Segmentation du Réseau : Cette étape consiste à créer différents VLAN pour garantir la sécurité et une gestion optimale du réseau.
2. Implantation d'un Serveur RADIUS : Mettre en place un serveur RADIUS pour appliquer une solution d'authentification au réseau de l'entreprise en utilisant les identifiants Microsoft SSO déjà en usage.
3. Redivisions du VLAN KLANIK : Réorganiser le VLAN actuel de KLANIK en plusieurs VLAN afin d'optimiser la gestion du trafic et de limiter les risques de sécurité.

3.3 Segmentation du réseau

Maintenant que nous savons comment le bâtiment et les appareils fonctionne dans ce bâtiment, nous devons réfléchir à la manière dont nous allons diviser ce réseau. Et pour cela le travail a déjà été fait en amont et nous avons une liste de VLAN à créer pour le réseau. Les voici :

Figure 2 - Cartes des VLAN

Nous savons donc combien de VLAN nous devront créer. Il nous reste maintenant à construire un plan d'adressage, quels VLANs ont besoins de communiquer avec quels VLANs, et comment mettre cela en place dans un environnement ZyXEL sans non plus perturber le réseau pour les autres utilisateurs.

3.3.1 Élaboration du plan d'adressage

Nous avons choisi de représenter l'ensemble des adresses et des plages avec un tableur Excel, comme cela nous avait été présenté par un collaborateur de l'entreprise lors d'une réunion. Cette réunion avait pour but de comprendre les attentes d'une entreprise pour un tel projet, en se basant sur des exemples

de projets similaires réalisés par d'autres groupes. Le tableur s'est avéré efficace pour visualiser la taille des plages d'adresses pour les VLANs, le nombre de VLAN et le nombre d'hôtes nécessaires pour chaque VLAN. Ce document sera également utile plus tard pour la gestion du réseau par un autre administrateur réseau lorsque nous ne serons plus là. C'est d'ailleurs un principe que nous avons maintenu tout au long de notre stage et de nos recherches : assurer une documentation claire et complète pour faciliter la continuité et la gestion du projet à l'avenir

3.3.2 Recherche technique

Une fois le tableur validé par la direction, il a fallu se poser la question technique qui se pose dans chaque projet : « Comment allons-nous procéder ? ». À cette question, une seule réponse s'impose : « Il faut chercher. » Alors, nous avons cherché. Nous nous sommes documentés sur les revues techniques des appareils ZyXEL [figure annexe – appareils ZyXEL] utilisés dans l'entreprise afin de nous familiariser avec une technologie bien différente de celle de Cisco, à laquelle nous étions formés. Cependant, ce qui semblait au départ être une tâche facile s'est révélé être plutôt complexe. En effet, la technologie ZyXEL et, surtout, les nomenclatures utilisées par ces appareils sont très différentes de celles de Cisco, voire incompréhensibles.

Nous avons également rencontré des problèmes de gestion des switches. En effet, la plupart des configurations des appareils ZyXEL se font via le cloud de ZyXEL NEBULA (cf. Figure 1 - Interface NEBULA, p.7). Cependant, nos switches ne sont pas compatibles en raison de leur ancienneté. La configuration doit donc se faire via une interface web hébergée directement sur le switch. Là encore, un nouveau problème s'est présenté : nous ne connaissions pas exactement les adresses IP des switches sur le réseau. Nous avons donc trouvé notre nouvelle tâche : scanner le réseau de l'entreprise pour identifier les adresses menant aux switches. Pour cela, nous avons simplement effectué un scan NMAP sur l'ensemble du réseau afin de répertorier toutes les machines connectées et de retrouver nos équipements ZyXEL.

Figure 3 - commande NMAP de découverte du réseau

Nous avons maintenant les adresses des switches, ainsi que les identifiants et l'accès à leur configuration. Cependant, au fur et à mesure du projet, nous nous rendons compte qu'il y a un véritable manque de documentation de l'infrastructure. Les documents que nous possédons sont soit très datés, soit inexistants. Ce manque d'information nous empêche de progresser dans le projet de segmentation du réseau. Après en avoir discuté avec la direction, nous avons décidé de revoir l'ensemble de la documentation et même la façons dont le réseau est construit.

3.4 Nomenclature

La première chose à faire avant de commencer à bouger les choses est de se mettre d'accord sur plusieurs normes à respecter tout du long et à graver dans le marbre pour les équipes à venir afin de garder une logique dans une perspective évolutive.
On pose alors les premières bases avec un système de nomenclature des appareils. Tout y passe, les point d'accès (cf. Figure 15 - Point d'accès ZyXEL NWA110AX), les SW (cf. Figure 16 - Switch ZyXEL GS1920-24HP), le Firewall (cf. Figure 14 - Firewall ZyXEL USG FLEX 700), Equipement fibre ou encore 4G. Le but est de pouvoir comprendre le à quel appareil nous avons affaire et où il se trouve :

Type équipement	>	Bâtiment	>	Etage	>	Emplacement	>	Index	>	NOM
EXEMPLE										
SW		HQ		RDC		SALON		1		SW-HQ-RDC-SALON-01
AP		PRV		N+1		Jardin		2		AP-PRV-N+1-Jardin-02
PC		276		N+2		Cuisine		3		PC-276-N+2-Cuisine-03

Nous avons alors créé un tableur contenant tous les nouveaux noms ainsi que leurs anciens noms pour faciliter la compréhension des anciennes documentations, qui pourraient ne pas être à jour. Maintenant que nous disposons d'un tableur bien structuré, nous devons réétiqueter les switches (SW), les points d'accès (AP) et tous les autres équipements. Cependant, les AP n'ont jamais été étiqueté dans la baie de serveurs. Heureusement, lors de leurs installations, les AP ont été branché avec des câbles Ethernet de couleur différente (jaune). Il nous reste donc à identifier chaque AP parmi les 17 présents.

Pour cette étape, nous avons exporté un fichier JSON depuis le cloud NEBULA regroupant le nom, l'adresse IP et surtout l'adresse MAC de chaque AP. Avec un petit programme Python parcourant ce fichier, nous avons comparé les adresses MAC des AP avec celles des appareils connectés aux switches via la table MAC disponible sur les interfaces web. Nous avons ainsi pu définir les correspondances entre les ports des switches et les AP, puis étiqueter les câbles dans la salle serveur.

Nous commencions à avoir une vision claire du réseau et avons débuté l'établissement d'une procédure pour tester la diffusion des VLAN sur le réseau KLANIK. L'objectif était d'examiner les résultats afin de pouvoir ensuite déployer cette configuration à grande échelle dans tout le bâtiment.

3.5 Le premier test

Le but de ce premier test était de configurer et de déployer trois SSID différents, chacun associé à un VLAN, le tout diffusé par un seul point d'accès. Ce test devait nous permettre de vérifier si la configuration réseau que nous avions prévue avec tous nos VLAN était réalisable à petite échelle.

3.5.1 Déroulement du test

Pour cela, nous avons rédigé un plan de mise en œuvre dans lequel nous avons décrit chaque étape du test et chaque configuration à effectuer sur les différents appareils, comme si nous rédigions un TP. Il fallait que n'importe qui puisse reproduire nos actions en suivant le document, il devait donc être clair et précis. Le rapport regroupait toutes les informations nécessaires pour comprendre le projet et le but de la manipulation. La plus grande partie du rapport présentait les interfaces de configuration pour le switch, le firewall et les points d'accès. Le document incluait de nombreuses captures d'écran afin de faciliter la compréhension de la mise en place des VLAN.

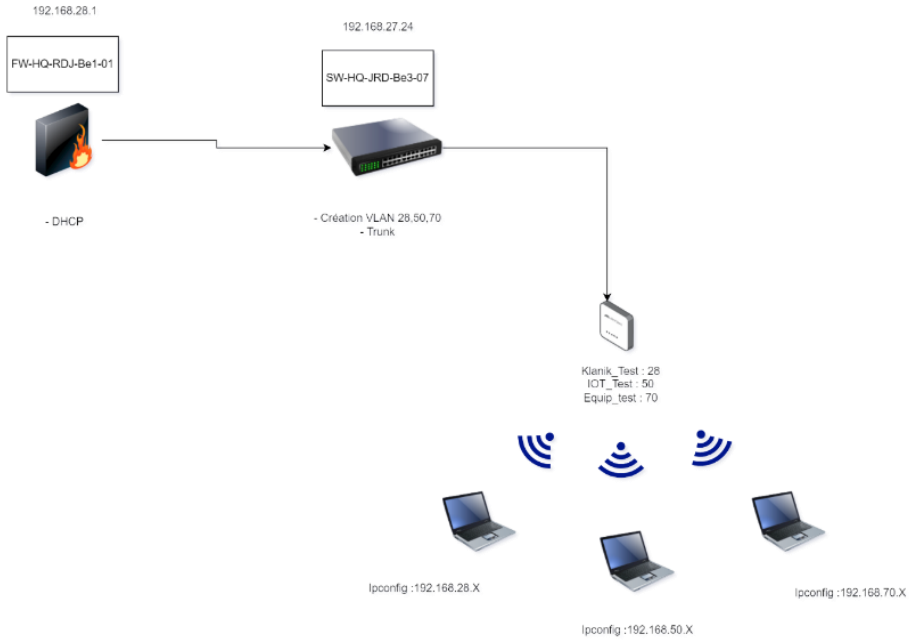


Figure 4 - schéma test n°1

Voici la configuration mise en place pour effectuer le test avec le moins de perturbations possible. La configuration a commencé par celle du firewall. Sous ZyXEL, il est nécessaire de créer des « LAN INTERFACE » pour déclarer nos VLAN (VLAN KLANIK, VLAN IOT, VLAN EQUIP) (cf. Figure 2 - Cartes des VLAN) au système. Il faut renseigner le nom du VLAN, son adresse IP, son masque, son ID de VLAN et son « PORT GROUP ». Le « PORT GROUP » est utilisé pour indiquer sur quels ports (« LAN INTERFACE ») du firewall les interfaces vont être publiées.

Ensuite, nous avons créé un serveur DHCP pour chaque VLAN avec leurs propres plages d'adresses, en veillant à éviter tout conflit avec les adresses IP du réseau déjà en place. Ici on utilise le LAN GROUPE 1, le LAN GROUPE utilisé déjà par l'interface principale « lan1 »

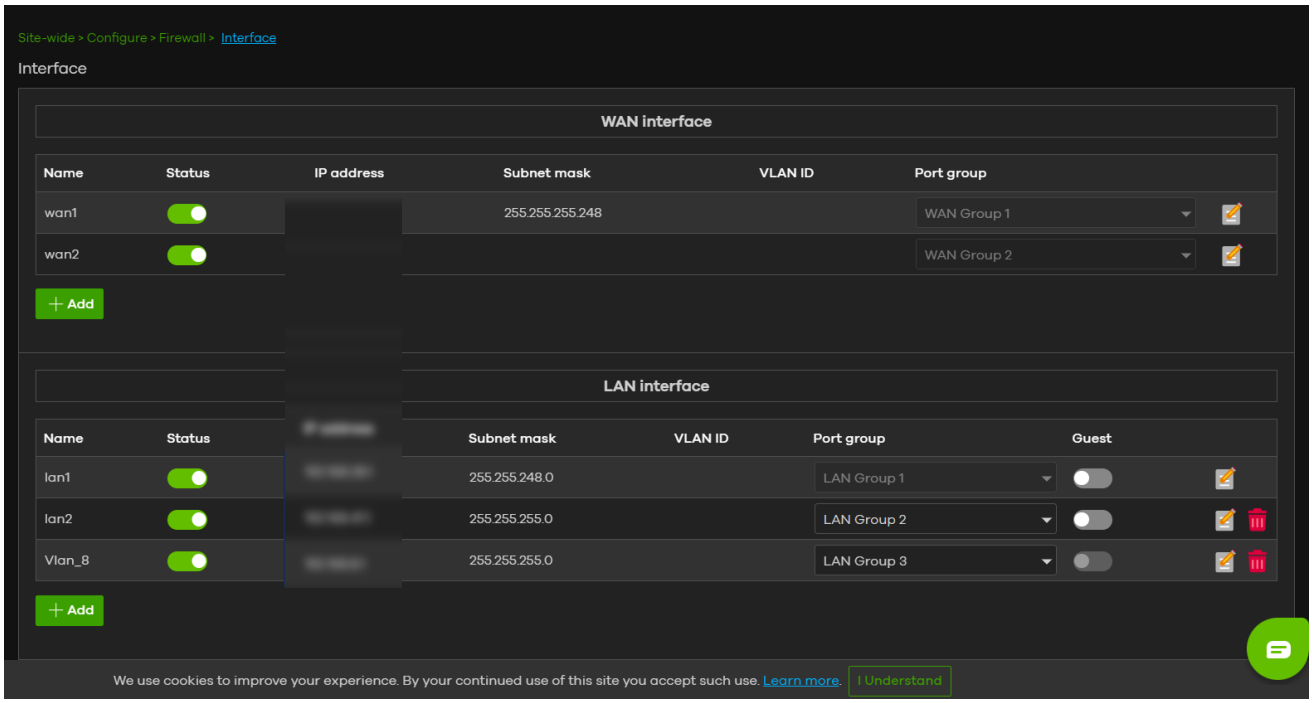


Figure 5 - Interface NEBULA, configuration des Interface FW

Une fois les VLAN créés et diffusés sur un port connecté au switch, nous passons à la configuration de ce dernier. Ici, nous déclarons les mêmes VLAN que ceux configurés sur le firewall.

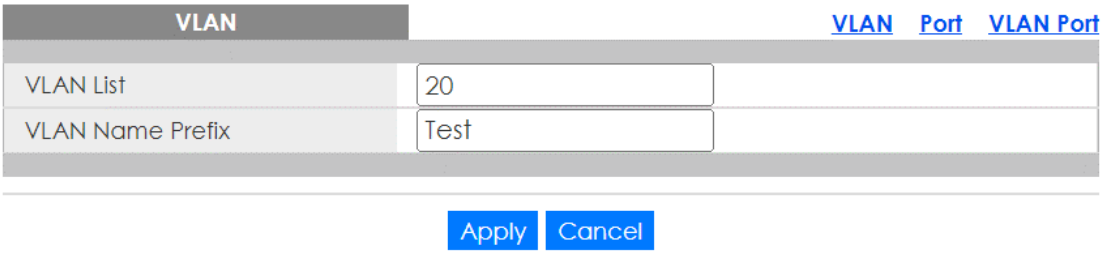


Figure 6 - interface de configuration de VLAN SW

Nous configurons donc nos trois VLAN et leurs identifiants comme suit :

- KLANIK_test = 28
- IOT_test = 50
- Equip_test = 70

Ensuite, nous configurons le port connecté à l'Access Point en mode trunk afin que les VLAN puissent tous passer par un seul port et être redirigés vers le port de connexion au firewall.

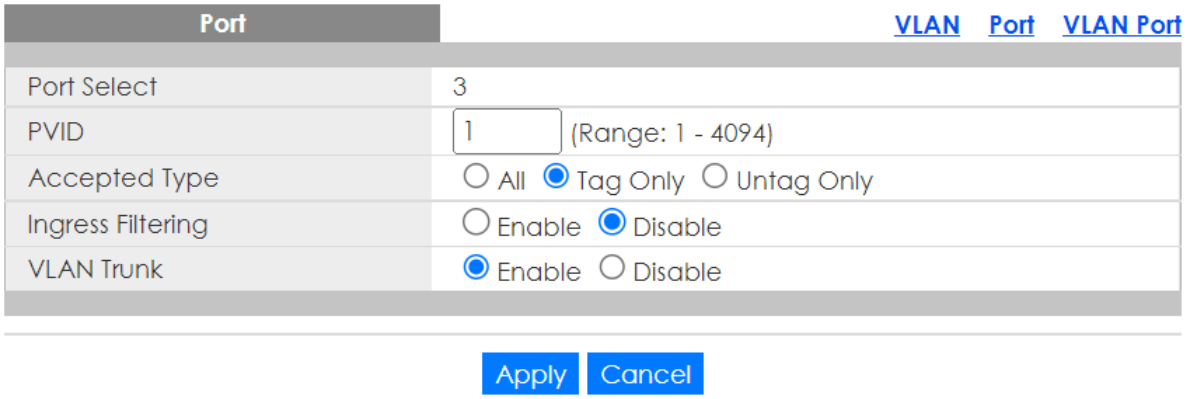


Figure 7 - Interface de configuration de port TRUNK

Enfin, nous créons les SSID pour chaque VLAN : KLANIK_test, IOT_test, Equip_test. Cela se fait sur le cloud NEBULA dans la configuration des Access Points. Nous isolons l'AP de la pergola pour ne pas diffuser les SSID dans tout le bâtiment. Ensuite, nous créons les SSID en attribuant à chacun un ID correspondant à leur VLAN, afin que les VLAN soient identifiables sur le port trunk du switch.

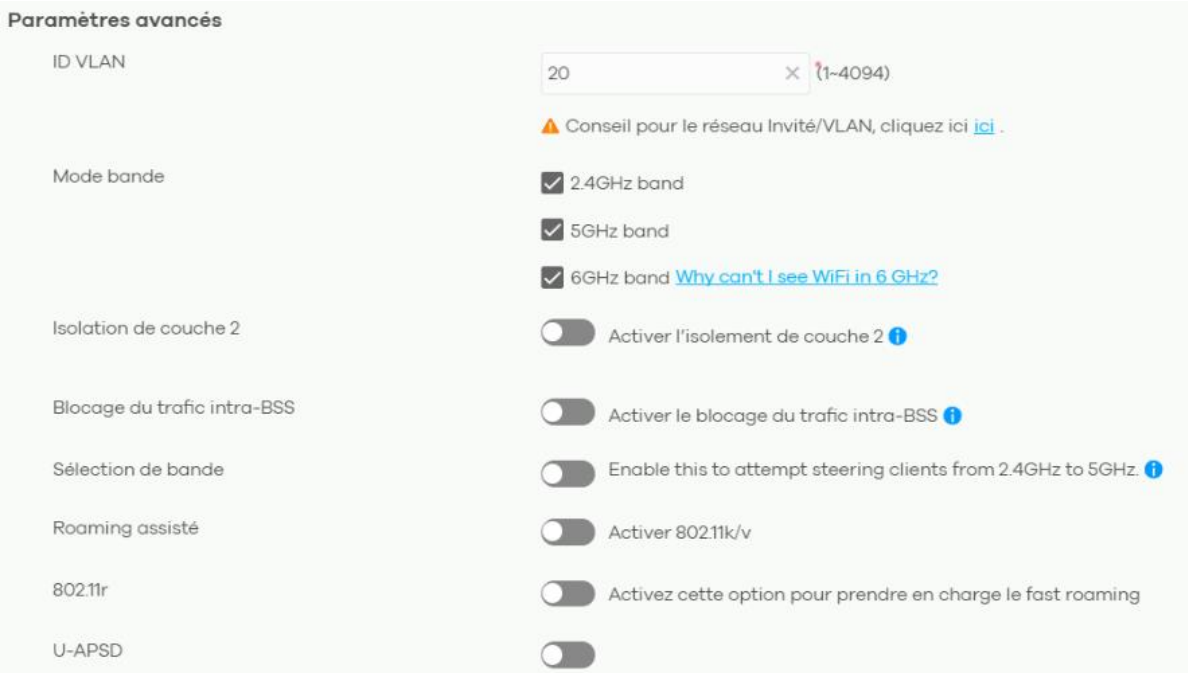


Figure 8 - Paramètre de création de SSID

Maintenant, le système est prêt pour le test. Nous sommes trois dans l'équipe, il y a trois SSID et trois VLAN. Le calcul est donc vite fait : chacun d'entre nous doit se connecter à son VLAN pour vérifier que tout le monde récupère bien une adresse IP du VLAN correspondant au SSID. Toute l'activité est surveillée grâce à un Wireshark qui tourne en arrière-plan. Nous nous connectons et nous vérifions, grâce à l'invite de commande de Windows, si notre IP a bien changé. Et là :

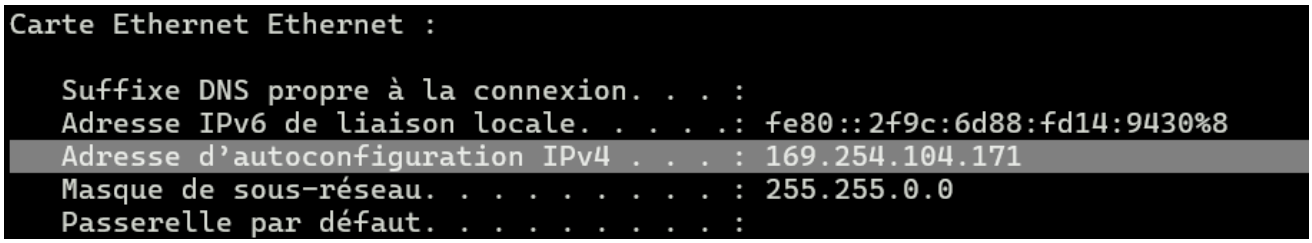


Figure 9 - résultat de la commande ipconfig sur CMD

Nous obtenons une adresse APIPA. Cela signifie que nous n'avons pas réussi à accéder au serveur DHCP et que nous n'avons donc pas obtenu d'adresse dans nos VLAN.

3.5.2 Panique à bord

Pendant que nous essayions de comprendre pourquoi nous ne parvenions pas à accéder au DHCP depuis nos SSIDs, un collègue du service communication nous a envoyé un message disant : “Il n’y a plus d’internet, c’est normal ?”. Silence total entre nous… Nous venons de comprendre que nous n’avons pas seulement un problème d’accès au DHCP, mais un problème d’accès à Internet tout court ! C’est donc à 15h07 que l’incident a commencé. Notre première action a été de défaire toutes les configurations sur le firewall pour vérifier si une erreur de configuration avait été faite. À 15h09, le retour à la configuration initiale n’a pas eu l’effet escompté. Pourquoi ? Parce que le service cloud NEBULA, sur lequel nous effectuons les modifications, ne peut lui non plus accéder au firewall étant donné qu’il passe par internet pour communiquer. Nous avons donc un firewall qui ne répond plus et aucun moyen de l’administrer.

C’est à ce moment-là que David CAUSSINUS et Julien MONTROZIER, nos maîtres de stage et supérieurs, nous ont rejoints à la pergola pour nous aider à reprendre le contrôle. Nous nous sommes ensuite rendus dans la salle serveur et avons tenté de nous connecter au firewall depuis un port Ethernet, sans succès. Même avec une adresse IP fixe, le firewall ne répondait ni aux pings (ICMP) ni au HTTP. Nous avons contacté OCS, le prestataire de KLANIK chargé de l’installation des équipements informatiques, pour obtenir des informations sur une méthode de connexion sans passer par NEBULA, mais ils n’en avaient pas. En effet, ZyXEL ne permet pas d’administrer le firewall directement et via NEBULA en même temps. Nous avons donc choisi, en dernière option, de débrancher puis rebrancher le firewall, n’ayant pas d’autre alternative. Après le redémarrage, le réseau est revenu à la normale à 15h43. Le firewall a récupéré la dernière configuration fonctionnelle enregistrée. Nous avons donc eu une panne de 42 minutes durant lesquelles personne n’avait accès à Internet via le Wi-Fi de l’entreprise.

Nous avons formulé plusieurs hypothèses pour expliquer les problèmes rencontrés. La création des interfaces dans le LAN GROUP 1, où se trouve l'interface principale, a probablement entraîné une tempête de broadcasts due aux demandes de DHCP, ce qui a abouti à une situation semblable à un DDOS. Une tempête de broadcasts se produit lorsqu'une quantité excessive de messages de diffusion est envoyée sur le réseau, entraînant une surcharge et une dégradation des performances. De plus, sans protocoles comme le Spanning Tree Protocol (STP), des boucles réseau peuvent se former, provoquant une circulation continue des paquets de diffusion et créant une surcharge. Le STP est un protocole utilisé pour éviter ces boucles en désactivant sélectivement certaines connexions pour créer un arbre de diffusion sans boucles, assurant ainsi qu'il n'y ait qu'un seul chemin entre deux stations du réseau. En créant les interfaces de test dans le même LAN GROUP que l'interface principale, un conflit de DHCP a probablement eu lieu. Lorsqu'un PC demande une adresse, il envoie un broadcast, ce qui a été propagé par les équipements, créant une tempête de broadcasts et saturant le réseau ainsi que le firewall. En conséquence, le firewall n'était pas accessible depuis l'interface cloud NEBULA. Sous cette surcharge, le firewall a également perdu son accès à Internet, affectant les points d'accès (AP) qui ont alors généré une surcharge de requêtes DHCP pour le firewall, créant une situation similaire à un DDOS. Notre erreur à donc été de ne pas créer un nouveau LAN GROUPE pour accueillir nos nouvelles interfaces.

3.5.3 Remise en question

Après cet échec cuisant, plusieurs questions se sont posées pour la suite du projet. Tout d'abord, il fallait bien sûr rechercher le plus d'informations possibles sur l'incident qui avait eu lieu, mais il fallait aussi revoir la manière de gérer les incidents futurs. L'une des raisons pour lesquelles nous avons mis autant de temps à résoudre le problème était que nous avancions à l'aveugle. Aucun d'entre nous ne savait vraiment comment gérer les appareils ZyXEL et nous étions obligés d'appeler OCS pour obtenir des informations de base. Nous aurions même pu choisir d'attendre qu'ils arrivent pour nous dépanner, ce qui aurait pris encore plus de temps. Cette situation ne devait pas se reproduire. Cependant, l'erreur étant humaine, il y aura forcément de nouveaux incidents un jour. Alors, au lieu d'essayer à tout prix de les éviter en vain, nous devons nous y préparer.

3.6 PRI & plan de récupération du Firewall

Nous nous sommes alors penchés sur la création d'un document de Procédure de Réaction à Incident (PRI) afin d'avoir le maximum de procédures possibles pour gérer les différentes pannes qui pourraient survenir dans notre réseau. Pour ce faire, nous avons organisé un grand brainstorming. L'idée était d'abord d'identifier les nombreuses pannes possibles. Même si cela peut sembler extravagant, nous sommes partis du postulat : « Tout ce qui est susceptible d'aller mal ira mal. » - *Edward A. Murphy Jr.* Nous avons matérialisé cela avec une carte mentale comme ci-dessous

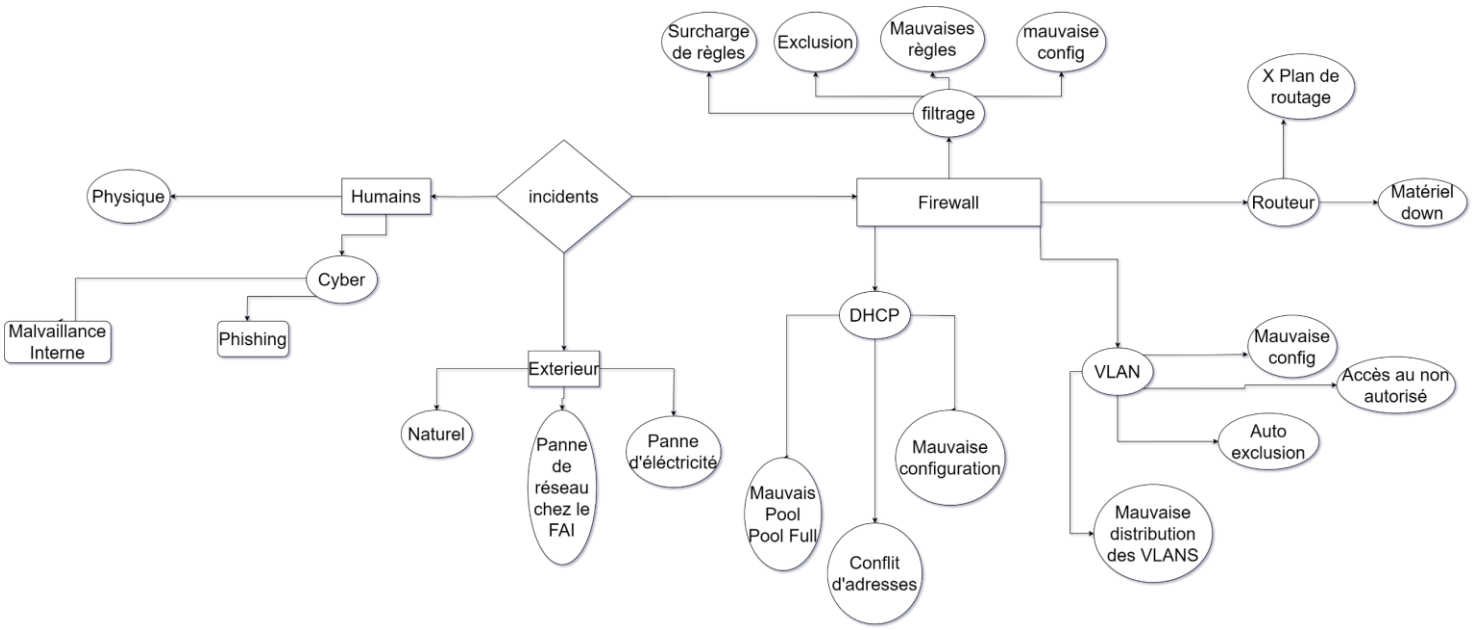


Figure 10 - Carte mentale des incidents possibles

Une fois la carte mentale réalisée, on nous a conseillé de nous concentrer sur l'élaboration d'un document de reprise de contrôle du firewall. Ce document regroupe les étapes à suivre en cas de panne du firewall, comme cela nous est arrivé, en utilisant un algorithme jusqu'à la résolution du problème. L'idée est qu'il soit interactif grâce à des renvois aux paragraphes correspondants dans le reste du document. Cela permet une meilleure efficacité dans le feu de l'action et de gagner du temps lors de la gestion des incidents.

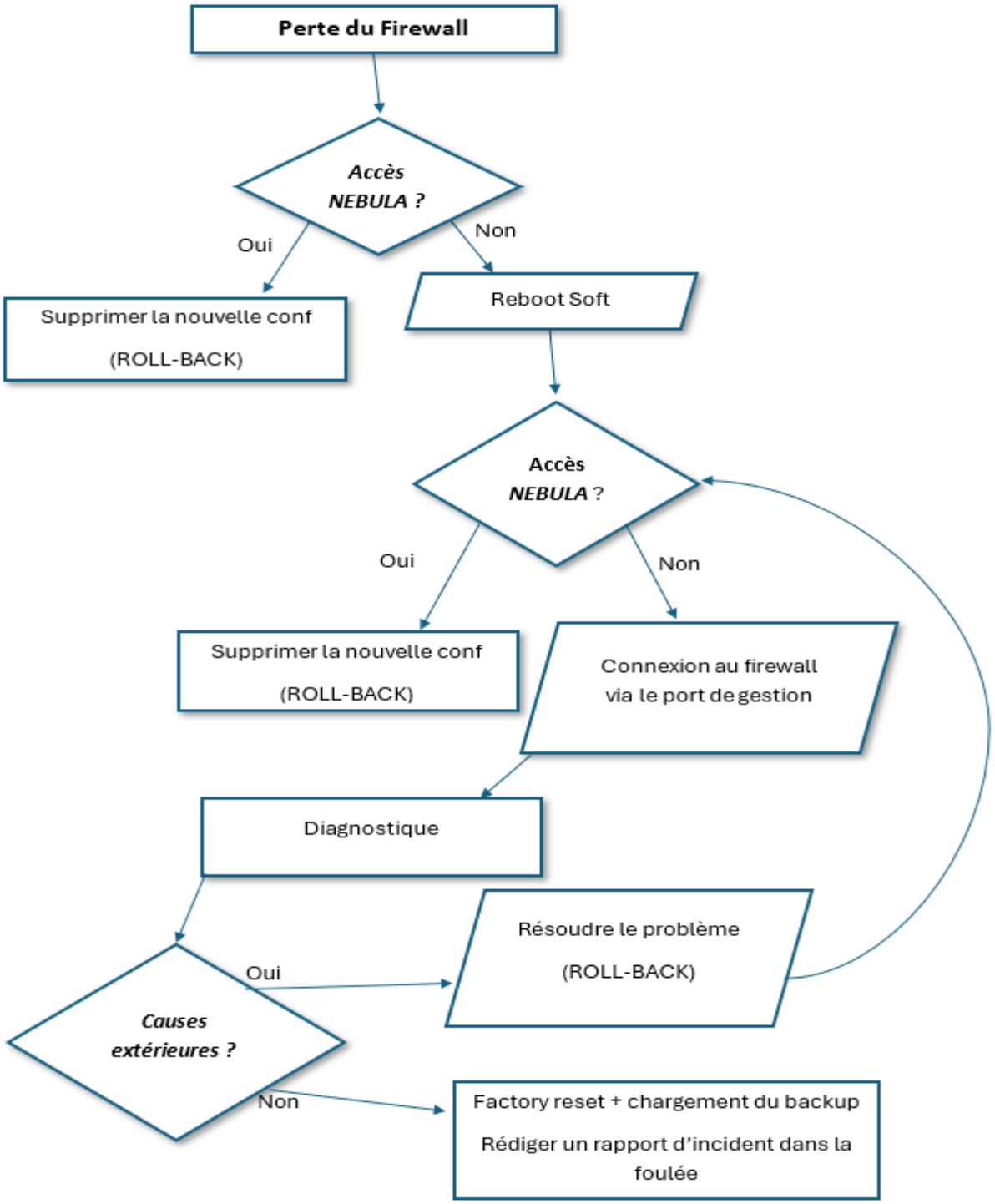


Figure 11 - algorigramme de reprise du firewall

3.7 Urbanisation

Après l'échec complet du précédent test, nous n'étions plus sereins pour la suite. Nous craignions qu'une nouvelle mauvaise interprétation des différents termes utilisés par ZyXEL nous perde et nous mène vers un nouvel incident. Nous avons alors réfléchi à une solution que nous avions rapidement écartée au début du projet. Nous avons pensé à changer le matériel sur lequel nous travaillons. Alors, pas tout bien sûr, mais en achetant un seul nouveau switch, il nous était possible de revoir toute l'architecture du réseau et de simplifier la mise en place de la segmentation.

L'idée était d'utiliser une architecture cœur de réseau avec en son centre un switch de couche 3 afin de pouvoir effectuer du routage entre les VLANs. Grâce à cela, nous n'aurions plus à gérer la configuration presque incompréhensible et souvent limitée des VLANs sur le firewall ZyXEL.

Malheureusement, ce changement de cap arrive seulement deux semaines avant la fin de notre stage mais il nous restait encore bien assez de temps pour creuser le sujet et laisser derrière nous une étude du réseau avec des perspectives d'évolution concrètes.

3.7.1 Etude de l'architecture réseau d'aujourd'hui.

Pour partir sur de bonnes bases, il nous a paru crucial de faire un état des lieux. Il s'agissait de savoir ce que nous avions, comment tout était branché et comment nous pourrions ensuite améliorer le système.

Nous avons donc commencé par la phase de reconnaissance. Il fallait identifier tous les appareils du réseau : le nombre de points d'accès (AP), de switches, de firewalls, de prises Ethernet et leurs numéros de brassage. Nous devions aussi nous assurer qu'il n'y avait pas d'autres appareils dont nous n'avions pas connaissance. Heureusement, la plupart de ce travail avait déjà été effectué en amont lors de la nomenclature. Nous savons qu'il y a 18 AP, 6 switches et un firewall. Nous savons même où les AP sont branchés sur les switches car nous les avons étiquetés dans la baie.

Les seules informations qu'il nous restait à connaître étaient l'emplacement de chaque port Ethernet. Après avoir compté plus de 110 câbles Ethernet, nous avons compris que retrouver, un par un, la localisation de chaque câble Ethernet dans la baie, alors que seulement une dizaine sont utilisés par les utilisateurs, n'était pas vraiment important. Nous avons donc laissé tomber cette partie, mais nous avons noté sur les switches tous les ports connectés aux câbles Ethernet. Même si nous ne savons pas où ils vont, nous savons qu'ils sont là.

Nous avons également identifié les appareils connectés aux switches dédiés à la sécurité du bâtiment, qui sont déjà dans un VLAN, le VLAN 8. Nous avons repéré les câbles connectés au système de caméras et au système de gestion des verrous des portes, OPTIMABOX.

Il ne nous restait alors plus qu'à documenter les appareils permettant d'accéder à Internet, à savoir une connexion en fibre et une borne 4G en redondance en cas de perte de la fibre. Les deux se connectent ensuite au firewall via le port destiné au Wide Area Network (WAN).

Une fois tout identifié, il ne nous restait plus qu'à organiser toutes ces informations sur un schéma grâce à l'outil draw.io. Nous pourrons ainsi avoir une vue d'ensemble de la façon dont est construit le réseau chez KLANIK HQ. Ce schéma est disponible en annexe page 29 (cf. Figure 17 - Architecture réseau actuel).

3.7.2 Réflexion sur le réseau et le besoin de KLANIK HQ

Le réseau de KLANIK HQ a évolué en parallèle des besoins de l'entreprise, sans une réflexion approfondie sur l'optimisation et la gestion des équipements. Il n'y a pas eu non plus beaucoup de documentation sur les différentes installations, ce qui nous manque aujourd'hui et nous bloque dans notre chemin vers un meilleur réseau. Cependant, on ne peut nier que jusqu'à présent, l'architecture du réseau a été efficace. Elle a très bien joué son rôle : fournir un accès à Internet à tout le monde chaque jour.

Il nous faut donc réfléchir à la façon dont nous voulons structurer le réseau de demain pour KLANIK. Tout d'abord, discutons des prises Ethernet. Tous ces câbles et prises inutilisés n'ont aucun sens d'être garder ainsi. Historiquement, les prises Ethernet étaient le principal moyen de connexion chez KLANIK. Chaque bureau et open space avait besoin d'une prise pour que les occupants puissent se connecter à Internet.

Cependant, aujourd'hui, KLANIK a évolué et a développé une couverture Wi-Fi très efficace dans tout le bâtiment, jusqu'au fond du jardin. L'ensemble des appareils étant désormais connectés au Wi-Fi, sauf pour certains irréductibles qui les utilisent encore, les 110 câbles n'ont plus vraiment de raison d'être. Il est donc tout à fait envisageable de réduire ce nombre.

Nous sommes arrivés à une solution qui nous paraît correcte : débrancher physiquement les câbles Ethernet non utilisés au niveau des switches, tout en les conservant sur le tableau de brassage pour pouvoir, à la demande ou en cas de besoin, les reconnecter facilement. Cette solution permet des économies de temps et d'énergie, car nous n'avons plus besoin d'autant de switches. Nous économisons ainsi un minimum de deux voire trois switches (48 ports chacun). De plus, une prise Ethernet accessible à tous représente une faille de sécurité en cas d'attaque physique, permettant à un attaquant de se connecter ou de connecter un petit ordinateur pour accéder au réseau depuis l'extérieur.

Maintenant que la question des prises Ethernet est gérée, nous pouvons nous concentrer sur la façon dont nous allons développer la nouvelle architecture. Comme nous l'avons dit plus tôt, nous souhaitons créer une architecture cœur de réseau avec, en son centre, un switch de couche 3. À partir de ce switch, tous nos autres switches seront connectés à lui.

Dans la salle réseau où se trouve la baie, il y aura donc le switch de sécurité, connecté au VLAN 8. Ce switch existe déjà et est déjà configuré, il n'y aura donc pas besoin d'y toucher. Ensuite, nous aurons un switch regroupant tous les AP, sauf ceux du deuxième étage, distribuant en mode trunk les différents VLAN via leurs SSID respectifs et des ports trunk. Le switch du jardin restera tel quel, pour des questions de distance et de contraintes, mais il fonctionnera de la même manière que le switch avec les AP.

Le switch du deuxième étage sera divisé : d'un côté, les ports serviront aux trois AP de l'étage et, de l'autre, il desservira, avec un VLAN attribué à chaque port, les accès aux prises Ethernet. Enfin, le dernier switch dans la salle serveur sera dédié aux câbles Ethernet, attribuant un VLAN aux trames qui passent par ses ports.

Cette configuration permettra une meilleure gestion du réseau, une isolation des différents segments pour la sécurité, et une simplification de la gestion et de la maintenance du réseau.

3.7.3 Le changement

On a beau savoir comment nous voulons refaire l'architecture, il nous reste encore à savoir avec quoi. Il nous faut choisir quel switch en cœur de réseau serait le plus adapté à nos besoins. Et pour cela, il y a deux solutions.

Soit nous choisissons de rester sur un écosystème ZyXEL avec un switch de couche 3 de chez eux. De cette manière nous gardons le confort de la gestion simplifiée de NEBULA et nous gardons aussi le support fournit par notre prestataire OCS qui ont l'habitude de l'interface ZyXEL et qui ont leurs contacts chez ZyXEL avec un accès aux informations rapidement. Mais nous gardons de notre côté aussi l'incompréhension de certains des termes utilisés par l'interface ZyXEL, le manque de documentation des équipements et aussi le prix, qui est assez important.

D'un autre côté nous avons la marque Mikrotik. Mikrotik est une entreprise lettone fondée en 1996, spécialisée dans les équipements réseau et les logiciels de routage. Elle est reconnue pour ses routeurs et switches performants et abordables, ainsi que pour son système d'exploitation avancé, Router OS, qui offre de nombreuses fonctionnalités pour la gestion réseau. Un switch Mikrotik serait alors une solution beaucoup plus abordable avec un rapport qualité prix imbattable face à ZyXEL. Doté de nombreuses fonctionnalités poussées, Mikrotik nous permettrait la création de notre segmentation comme nous l'imaginions. Mais nous perdrons alors l'expertise d'OCS sur ce matériel et il ne serait pas gérable depuis le cloud NEBULA. Cependant, les switches actuels ne l'étant déjà pas, ce n'est pas une contrainte. De plus, même si les appareils Mikrotik sont plutôt voué à être configuré en ligne de commande, il est possible d'utiliser l'interface graphique WinBox qui est très facile à comprendre et appréhender.

Nous avons pu en faire l'expérience grâce à un laboratoire virtuel sur le logiciel de virtualisation GSN3, dans lequel nous avons pu simuler un réseau avec des équipements Mikrotik. Ce qui d'ailleurs, est un autre bon point, car dans l'avenir, les tests comme ceux que nous avons faits plus tôt dans le stage, pourront être fait en virtuel sans impacter personne. Chose qui n'est pas faisable sur ZyXEL.

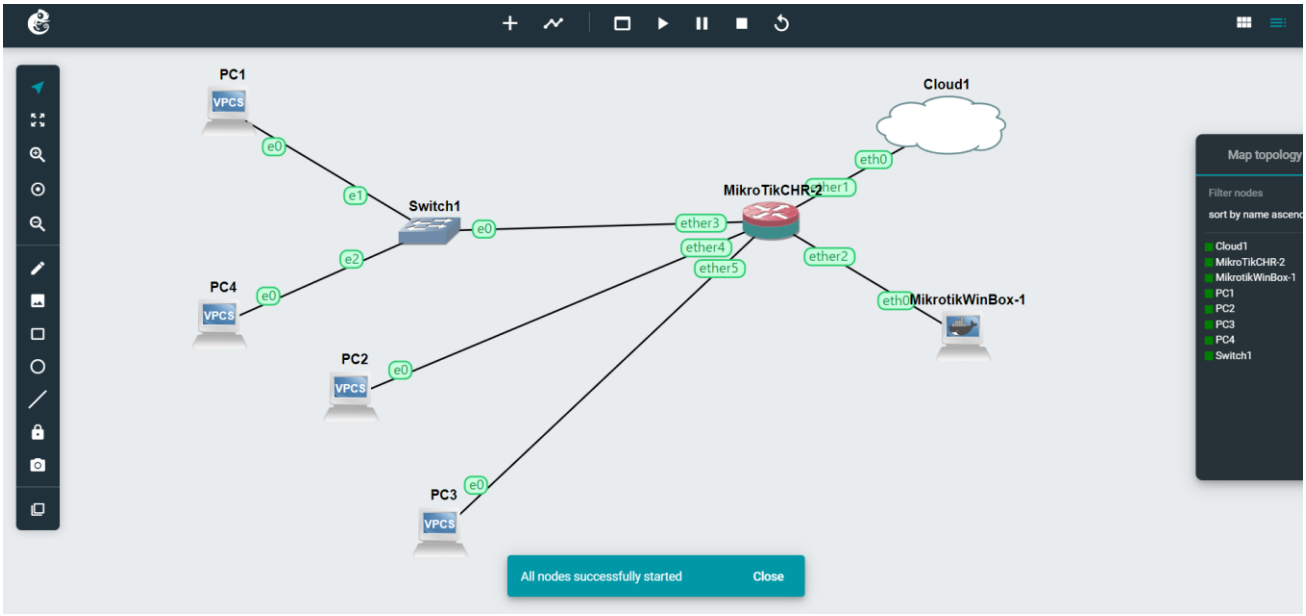


Figure 12 - laboratoire GNS3

Le routeur ici était configurable via le logiciel WinBox. Accessible via une connexion VNC au pc en bas à droite.

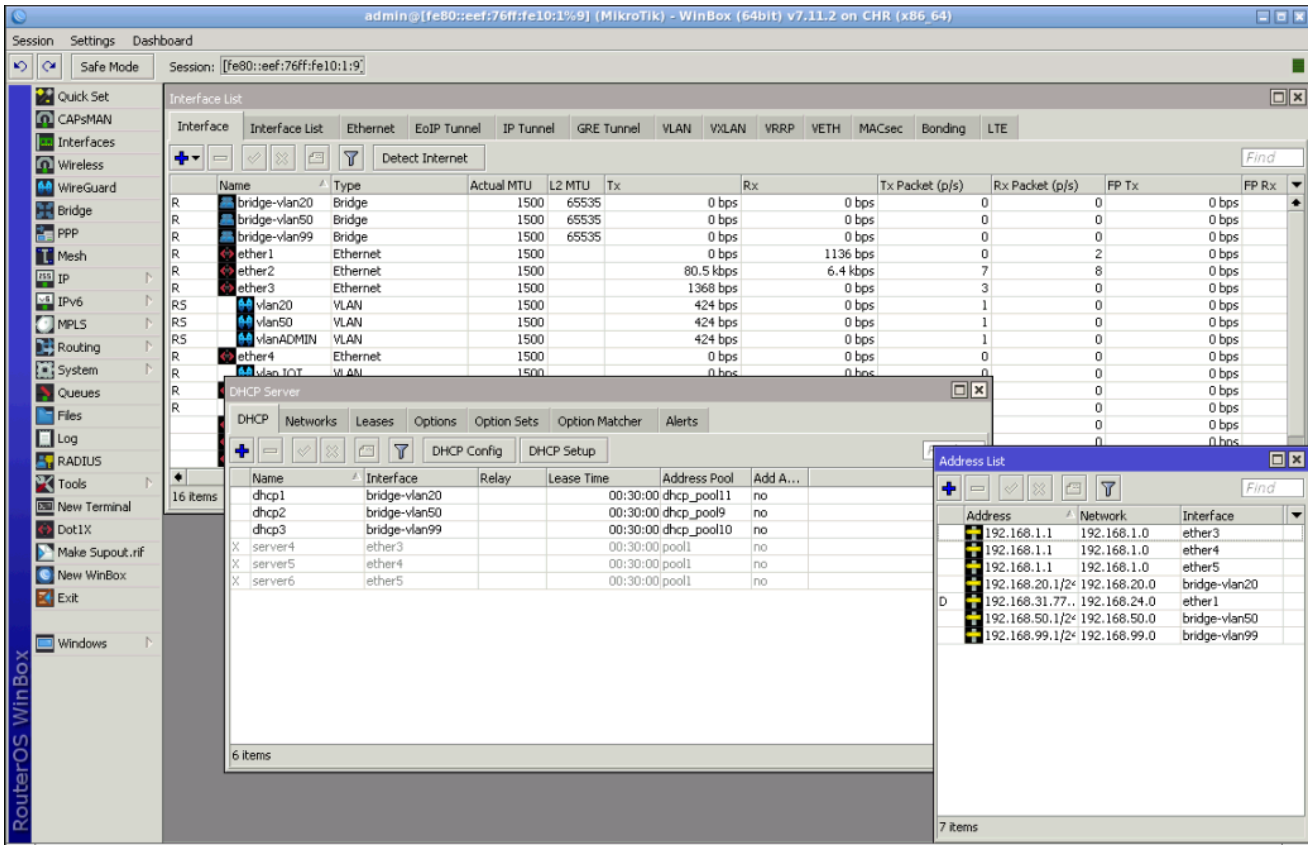


Figure 13 - interface WinBox

3.7.4 Un cahier des charges pour OCS

Nous avons nos idées et notre vision pour l'évolution de notre réseau. Malheureusement nous n'avons plus le temps de réaliser ce projet. Nous devons maintenant formaliser ces idées dans un cahier des charges destiné à notre prestataire, qui sera chargé de mettre en œuvre ces modifications. Ce document présentera le projet en détail et précisera nos attentes. Nous souhaitons également recueillir l'avis du prestataire sur les solutions proposées et obtenir son expertise sur le sujet.

Le cahier des charges développe toutes les idées mentionnées précédemment. Il détaille et explique les actions que nous souhaitons mener en interne, telles que la segmentation du réseau. Il précise également les tâches que nous déléguerons à One Computer Service (OCS), comme le recâblage des baies.

Grâce à ce document, OCS sera en mesure d'établir un devis pour nous informer du coût de cette opération. Cela inclura une évaluation détaillée des ressources nécessaires et des implications financières de chaque étape du projet. En ayant une vue d'ensemble claire et précise, nous pourrons assurer une collaboration efficace et une mise en œuvre réussie de notre nouvelle infrastructure réseau.

4 Avis personnel Clément DALIES

Cette opportunité de stage chez KLANIK était une réelle chance. J'ai découvert dans un premier temps le vrai monde de l'entreprise. Comment les différents services sont organisés et à quel point chaque personne à son impacte. L'exemple même, nous, simples stagiaires de 2 mois et demi, avons su impacter le quotidien de chacun des employés en provoquant une panne du réseau. Deux fois pour ma part. Mais la première n'était qu'un câble débranché par inadvertance. Et même si on peut le prendre à la légère aujourd'hui, ce n'était pas le cas à l'instant où cela s'est produit. Et là où d'autres responsable nous auraient passé un savon, Julien MONTROZIER et David CAUSSINUS ont quant à eux été très bienveillant et formateur sur cette erreur. Ils nous ont rassuré en nous rappelant que nous ne sommes que des stagiaires en apprentissage et que les erreurs sont faites par tout le monde tout le long d'une carrière. Et ils nous ont illustrés ça en nous parlant de leurs erreurs à eux, ce qui nous a bien fait tout relativiser et nous détendre après les trois quarts d'heure de tension pendant la panne.
Nous avons tout le long du stage travaillé à 3 dans une salle et on ne peut pas dire que la bonne humeur était absente. Nous avons beaucoup partagé sur beaucoup de sujets créant une atmosphère de travail très agréable. Chacun avait son avis, toujours dans le respect des uns et des autres et dans l'optique de progresser en groupe.
C'était aussi très intéressant de pouvoir discuter avec Julien MONTROZIER et David CAUSSINUS de leurs carrières et d'apprendre à leurs côtés.
En somme KLANIK était une très bonne expérience professionnelle et humaine. En espérant un jour recroiser les gens avec qui nous avons partagé notre première expérience professionnelle et qui m'ont redonné le goût et la passion pour l'informatique et l'innovation que j'avais pu perdre.

"L'éducation ne consiste pas à gaver, mais à donner faim." - Michel de Montaigne

5 Avis personnel de Aymane EL MOUTAOUAKKEL

Mon stage chez KLANIK a été une expérience incroyablement enrichissante et transformatrice. Entrer dans le monde de l'entreprise, qui m'était encore totalement inconnu, a été une immersion totale et fascinante.

L'une des choses les plus marquantes pour moi a été de constater à quel point chaque personne est importante, peu importe son rôle ou ses responsabilités. Chez KLANIK, j'ai vu que chaque membre de l'équipe contribue de manière significative au succès de l'entreprise. Cette réalité m'a permis de comprendre que l'effort collectif et la valorisation de chaque contribution sont essentiels dans un environnement professionnel.

Découvrir les méthodes de travail en entreprise a été une révélation. Elles sont bien différentes de celles utilisées dans le monde scolaire. En entreprise, l'accent est mis sur la collaboration, la communication efficace, et l'atteinte d'objectifs concrets. Comparé à l'approche académique souvent plus théorique et individuelle, cette immersion pratique fut très intéressante. Cela m'a permis de comprendre les dynamiques professionnelles et d'apprécier la richesse des interactions et des processus organisationnels.

Apprendre à adopter une méthode structurée et à rédiger des documents professionnels a également été très enrichissant. Chez KLANIK, j'ai développé des compétences essentielles telles que la rédaction de rapports, la gestion de projets, et la communication formelle. Ces compétences, bien qu'elles puissent sembler secondaires au premier abord, sont en réalité cruciales pour réussir dans le monde du travail.

Travailler aux côtés de Julien MONTROZIER, David CAUSSINUS et Hadji MOUIGNI a été un véritable privilège. Leurs côtés pédagogues et leurs volontés constantes de nous aider ont fait de cette expérience un véritable plaisir. Ils n'hésitaient jamais à partager leurs connaissances et à nous guider, ce qui a grandement facilité mon apprentissage et mon intégration dans l'équipe.

En conclusion, ce stage chez KLANIK a été une formidable aventure professionnelle et humaine. Il m'a permis de découvrir un monde nouveau, d'apprendre des méthodes de travail professionnelles, et de développer des compétences essentielles pour mon futur. Je suis reconnaissant d'avoir eu l'opportunité de vivre cette expérience et de travailler avec des professionnels aussi dévoués et inspirants.

6 Conclusion

Ce stage au sein de KLANIK a été une expérience riche et formatrice, marquée par des défis stimulants et des apprentissages précieux. La tâche qui nous a été confiée, la segmentation du réseau, nous a permis de mettre en pratique nos connaissances théoriques tout en développant de nouvelles compétences techniques et méthodologiques.

Nous avons commencé par une analyse approfondie des besoins et des infrastructures, suivi de la planification et de la mise en œuvre de diverses configurations réseau. Les tests réalisés, bien que ponctués de difficultés, ont été des occasions d'apprentissage exceptionnelles, nous permettant de comprendre l'importance de la rigueur, de la documentation et de la gestion proactive des incidents. L'épisode de la panne réseau nous a particulièrement marqué, soulignant la nécessité de plans de reprise d'activité bien structurés et de procédures claires pour gérer les crises.

L'expérience nous a également donné l'opportunité d'explorer et de comparer différents équipements réseau, notamment ceux de ZyXEL et Mikrotik. Cette comparaison nous a permis de proposer des solutions adaptées aux besoins spécifiques de KLANIK, en tenant compte des avantages et des inconvénients de chaque option.

Ce stage a solidifié notre passion pour les réseaux et la cybersécurité et nous a armés de compétences essentielles pour notre parcours professionnel. Nous sommes reconnaissants d’avoir eu l’opportunité de contribuer à un projet si significatif pour KLANIK, même si l’objectif du début de stage n’a pas pu être atteint, et espérons que notre travail continuera à bénéficier à l’entreprise dans ses futurs développements technologiques.

7 Remerciement

Nous tenons à exprimer notre profonde gratitude à Julien MONTROZIER et David CAUSSINUS, nos responsables en entreprise, pour leur encadrement et leurs conseils tout au long de ce projet. Leur soutien a été essentiel à la réussite de notre mission.

Un grand merci à Hadji MOUIGNI, qui a été notre tuteur officieux durant le stage. Il nous a guidés dans le monde de l'entreprise en nous montrant les ficelles du métier et de la communication avec la hiérarchie. Il nous a aussi introduit à son groupe de collège dans lequel nous avons vite été intégré.

Nous remercions également toute l'équipe de KLANIK et le prestataire OCS pour leur collaboration et leur aide précieuse. Cette expérience a été non seulement un tremplin professionnel, mais aussi une aventure humaine enrichissante, nous préparant efficacement à nos futures carrières dans le domaine des réseaux et télécommunications.

8 Glossaire

AP (Access Point) : Point d'accès. Dispositif permettant de connecter des appareils sans fil à un réseau filaire.

FW (Firewall) : Pare-feu. Dispositif de sécurité réseau qui contrôle le trafic entrant et sortant pour protéger un réseau interne contre les menaces externes.

BM (Business Manager) : Responsable des affaires. Personne en charge de la gestion des affaires commerciales et de la relation client.

CMD (Command Prompt) : Invite de commande. Interface en ligne de commande utilisée dans les systèmes d'exploitation Windows pour exécuter des commandes textuelles.

DHCP (Dynamic Host Configuration Protocol) : Protocole de configuration dynamique des hôtes. Protocole réseau qui permet d'attribuer automatiquement des adresses IP aux appareils connectés à un réseau.

DDOS (Distributed Denial of Service) : Attaque par déni de service distribué. Attaque visant à rendre un service indisponible en submergeant le réseau ou le serveur de requêtes.

ICMP (Internet Control Message Protocol) : Protocole de message de contrôle sur Internet. Utilisé pour envoyer des messages d'erreur et des requêtes de diagnostic à travers un réseau.

IT (Information Technology) : Technologie de l'information. Ensemble des techniques et équipements informatiques utilisés pour le traitement et la transmission des informations.

LAN (Local Area Network) : Réseau local. Réseau informatique qui interconnecte des ordinateurs sur une zone géographique limitée.

PRA (Plan de Reprise d'Activité) : Document décrivant les procédures à suivre pour restaurer les services et les opérations d'une entreprise après un incident majeur.

PRI (Procédure de Réaction à Incident) : Procédure décrivant les étapes à suivre en cas d'incident pour minimiser les impacts et restaurer les services.

SSID (Service Set Identifier) : Identifiant de l'ensemble de services. Nom attribué à un réseau Wi-Fi pour le distinguer des autres réseaux.

STP (Spanning Tree Protocol) : Protocole de l'arbre couvrant. Protocole réseau utilisé pour éviter les boucles dans les réseaux Ethernet.

SW (Switch) : Commutateur. Dispositif réseau qui connecte plusieurs appareils et dirige les données entre eux sur un réseau local.

VLAN (Virtual Local Area Network) : Réseau local virtuel. Sous-réseau logique créé au sein d'un réseau physique pour segmenter et isoler le trafic réseau.

WAN (Wide Area Network) : Réseau étendu. Réseau informatique couvrant une large zone géographique, souvent utilisé pour relier des réseaux locaux entre eux.

Wireshark : Outil logiciel de capture et d'analyse de paquets réseau. Utilisé pour diagnostiquer et analyser le trafic réseau en temps réel.

ZyXEL : Marque de matériel réseau. Fournisseur d'équipements tels que des switches, des points d'accès et des firewalls.

9 Bibliographie

- Admin Malin, s.d. Mise en place d'un serveur RADIUS sous Windows Server. [en ligne] Disponible à: https://www.adminmalin.fr/mise-en-place-dun-serveur-radius-sous-windows-server/ [Consulté le 19 juin 2024].

- Akamai, s.d. Qu'est-ce que la micro-segmentation ? [en ligne] Disponible à: https://www.akamai.com/fr/glossary/what-is-microsegmentation [Consulté le 19 juin 2024].

- Archives Factory, s.d. Qu'est-ce que la micro-segmentation ? Comment obtenir granulaire améliore la sécurité du réseau. [en ligne] Disponible à: https://www.archivesfactory.com/quest-ce-que-la-micro-segmentation-comment-obtenir-granulaire-ameliore-la-securite-du-reseau/ [Consulté le 19 juin 2024].

- Cloudflare, s.d. Qu'est-ce que la micro-segmentation ? [en ligne] Disponible à: https://www.cloudflare.com/fr-fr/learning/access-management/what-is-microsegmentation/ [Consulté le 19 juin 2024].

- CrowdStrike, s.d. Qu'est-ce que la segmentation du réseau ? [en ligne] Disponible à: https://www.crowdstrike.fr/cybersecurity-101/network-segmentation/ [Consulté le 19 juin 2024].

- FreeRADIUS, s.d. FreeRADIUS. [en ligne] Disponible à: https://freeradius.org/ [Consulté le 19 juin 2024].

- IT-Connect, s.d. Comment installer Proxmox VE 7.0 et créer sa première VM ? [en ligne] Disponible à: https://www.it-connect.fr/modules/au-coeur-de-lannuaire-active-directory/ [Consulté le 19 juin 2024].

- JumpCloud, s.d. Assignation dynamique de VLAN. [en ligne] Disponible à: https://jumpcloud.com/blog/dynamic-VLAN-assignment [Consulté le 19 juin 2024].

- Kong, s.d. Kong API Gateway. [en ligne] Disponible à: https://github.com/Kong/kong [Consulté le 19 juin 2024].

- Microsoft, s.d. Authentification RADIUS avec Microsoft Entra ID. [en ligne] Disponible à: https://learn.microsoft.com/en-us/entra/architecture/auth-radius [Consulté le 19 juin 2024].

- Network Life, 2010. Assignation dynamique de VLAN avec dot1x. [en ligne] Disponible à: https://www.networklife.net/2010/07/assignation-dynamique-de-VLAN-avec-dot1x/ [Consulté le 19 juin 2024].

- Oracle, s.d. Qu'est-ce qu'un SSO ? [en ligne] Disponible à: https://www.oracle.com/fr/security/qu-est-ce-qu-un-sso/ [Consulté le 19 juin 2024].

- Synexie, s.d. La segmentation réseau : pourquoi c'est important et comment la mettre en place. [en ligne] Disponible à: https://www.synexie.fr/la-segmentation-reseau-pourquoi-cest-important-et-comment-la-mettre-en-place/ [Consulté le 19 juin 2024].

- VMware, s.d. Micro-segmentation avec VMware NSX-T Data Center. [en ligne] Disponible à: https://docs.vmware.com/fr/VMware-NSX-T-Data-Center/3.0/installation/GUID-4CF407DD-734C-4B2B-B5AC-CF83B3BBB562.html [Consulté le 19 juin 2024].

- Wikipédia, s.d. Serveur de stockage en réseau. [en ligne] Disponible à: https://fr.wikipedia.org/wiki/Serveur_de_stockage_en_r%C3%A9seau [Consulté le 19 juin 2024].

- Zscaler, s.d. Qu'est-ce que le Zero Trust ? [en ligne] Disponible à: https://www.zscaler.fr/resources/security-terms-glossary/what-is-zero-

trust#:~:text=le%20Zero%20Trust%20%3F-,Qu'est%2Dce%20que%20le%20Zero%20Trust%20%3F,consid%C3%A9r%C3%A9e%20comme%20fiable%20par%20d%C3%A9faut [Consulté le 19 juin 2024].

- Zyxel Support, s.d. Configurer un serveur RADIUS pour l'assignation dynamique de VLAN. [en ligne] Disponible à: https://support.zyxel.eu/hc/en-us/articles/4453007504658-Switch-Dynamic-VLAN-Configure-RADIUS-Server-for-dynamic-VLAN-Assignment [Consulté le 19 juin 2024].

- Zyxel Support, s.d. NEBULA : Configurer les interfaces LAN/VLAN. [en ligne] Disponible à: https://support.zyxel.eu/hc/fr/articles/4412582220434-NEBULA-Configure-LAN-VLAN-interfaces [Consulté le 19 juin 2024].

- Zyxel, s.d. XGS2220-54HP User Guide. [pdf] Disponible à: https://download.zyxel.com/XGS2220-54HP/user_guide/XGS2220-54HP_V4.80_Ed4.pdf [Consulté le 19 juin 2024].

- Zyxel, s.d. 24/48-port GbE L3 Access Switch with 6 10G Uplink (XGS2220 series). [en ligne] Disponible à: https://www.zyxel.com/fr/fr/products/switch/24-48-port-gbe-l3-access-switch-with-6-10g-uplink-xgs2220-series/overview [Consulté le 19 juin 2024].

- Zyxel Community, s.d. How to configure VLAN trunk on GS1900. [en ligne] Disponible à: https://community.zyxel.com/en/discussion/19536/how-to-configure-VLAN-trunk-on-gs1900 [Consulté le 19 juin 2024].

- Zyxel Support, s.d. Download Center: USG FLEX 700. [en ligne] Disponible à: https://www.zyxel.com/fr/fr/support/download?model=usg-flex-700 [Consulté le 19 juin 2024].

ANNEXE

Figure 14 - Firewall ZyXEL USG FLEX 700

Figure 15 - Point d'accès ZyXEL NWA110AX

Figure 16 - Switch ZyXEL GS1920-24HP

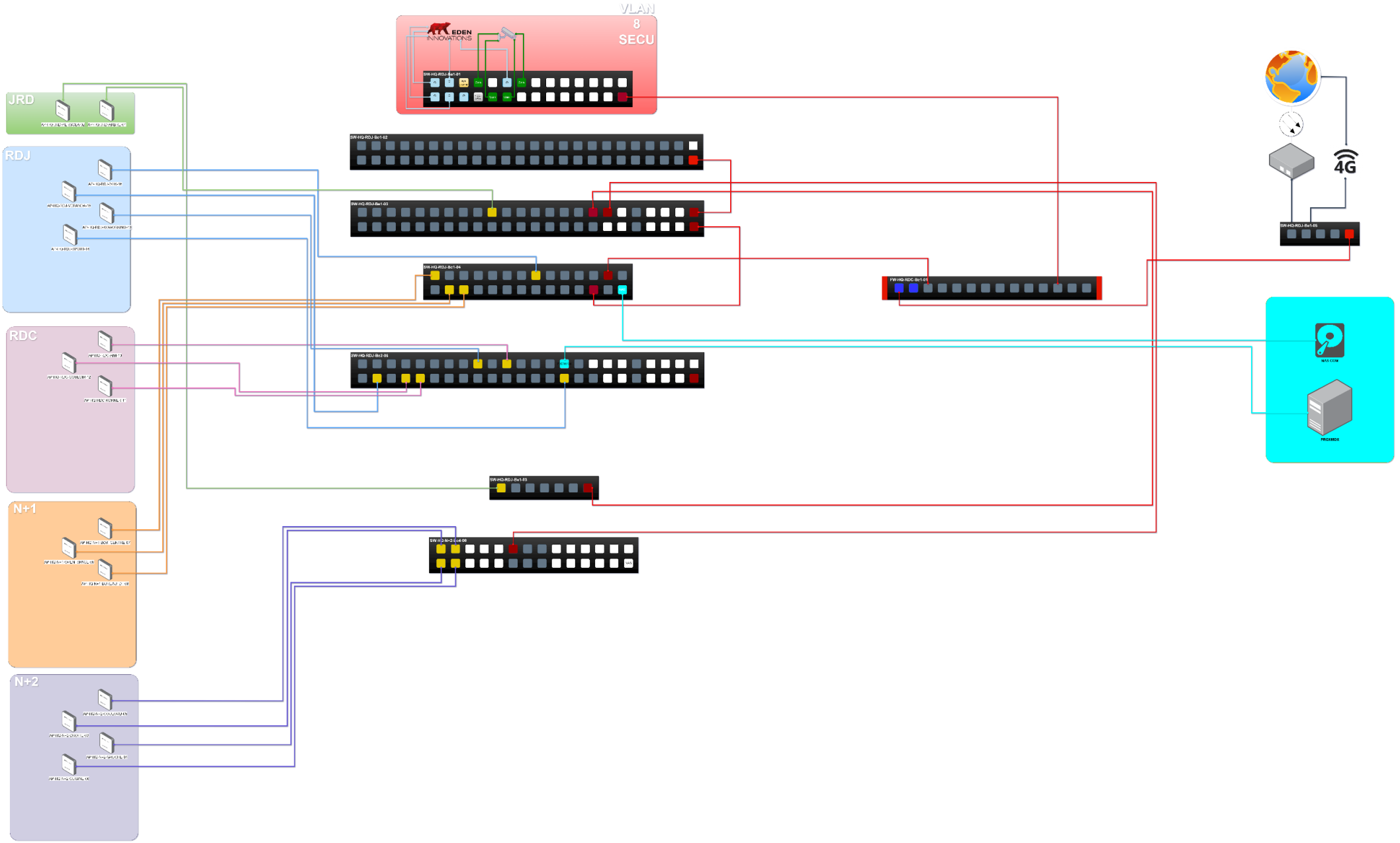


Figure 17 - Architecture réseau actuel

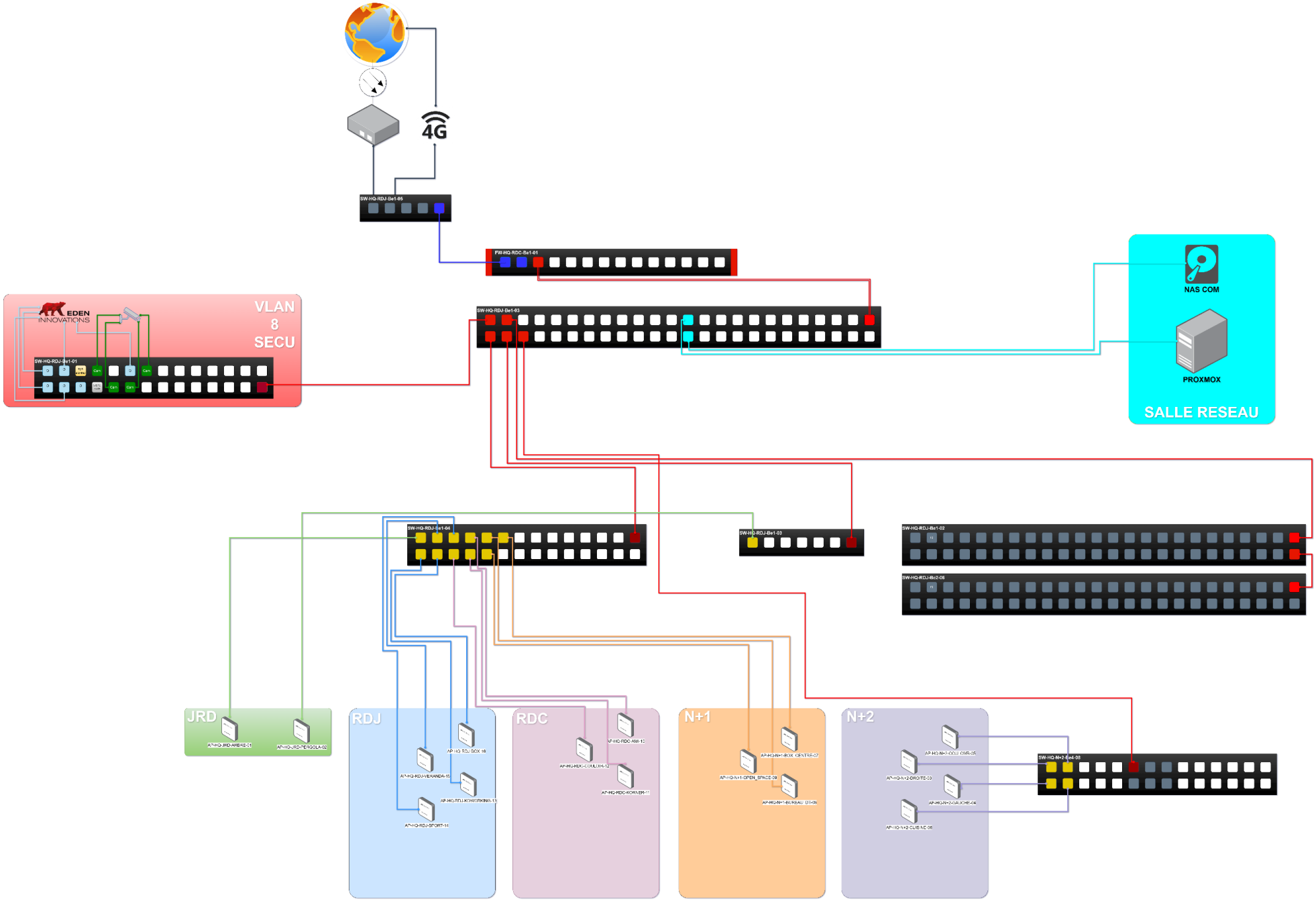


Figure 18 - Architecture réseau future sans SW C3

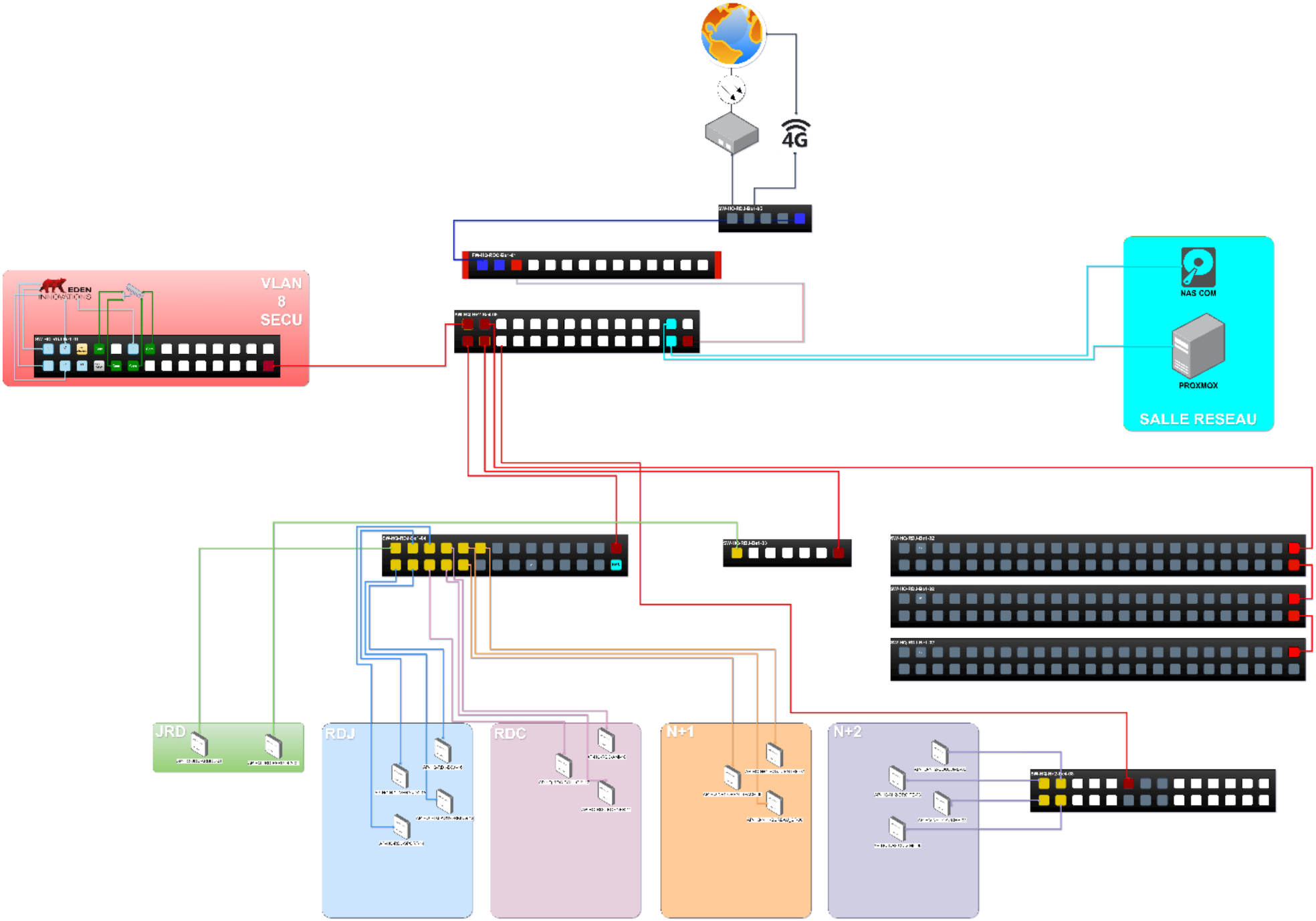


Figure 19 - Architecture réseau future avec un SW C3