Institut Universitaire de Technologie,
Aix-Marseille Université

RAPPORT DE STAGE
Diplôme Universitaire de Technologie
Spécialité Réseaux et Télécommunications

Technicien de maintenance informatique - Réalisation d'un projet « Challenge LAB »

Florian ALLEMANN

SNS Solutions

Responsable entreprise : **Théo Maoual**

Responsable académique : **Jean-Luc Damoiseaux**

2022

Table des matières

Introduction

En vue de conclure mes deux années au sein du DUT* Réseaux et Télécommunications, il m'a été demandé de réaliser un stage en immersion au sein d'une entreprise professionnelle. Ce stage, d'une durée de 10 semaines, a pour principal objectif de nous confronter au monde de l'entreprise, mais également, d'appliquer nos compétences et connaissances théoriques acquises jusqu'alors.

C'est pourquoi j'ai pris contact avec l'équipe technique de SNS Solutions, qui me semblait être le meilleur profil d'entreprise pour travailler et perfectionner mes compétences dans tous les domaines de l'informatique possibles. Cette entreprise est spécialisée dans l'infogérance*, la maintenance informatique ainsi que dans la téléphonie, avec plus de 500 clients à son actif.

Au cours de mon stage, plusieurs missions m'ont été confiées par l'entreprise, et plus particulièrement par mon tuteur de stage, Théo Maoual, qui exerce le métier de technicien de maintenance informatique au sein de SNS. Ces missions se divisent en plusieurs étapes :

- Réception d'un appel de client, prise d'information (nom/tel/objet de la demande…)
- Création d'un ticket d'intervention avec ces informations.
- Prise en charge du ticket par un technicien.
- Traitement de l'intervention après contact avec le client.

J'ai également eu la chance que l'on m'attribue un projet technique à réaliser lors de mon stage. Ce dernier est un « Challenge-Lab » composé de plusieurs machines (physiques et virtuelles). Ce projet avait pour principal but de faire communiquer une borne Unifi (situé dans un réseau LAN*) à un contrôleur au travers d'un tunnel VPN IPSEC* (relié à un autre LAN).

Il m'est également arrivé d'accompagner des techniciens en intervention chez le client pour réaliser de la maintenance sur site.

Ce stage m'a permis de découvrir le monde de l'entreprise, ainsi que les différents types d'infrastructures d'entreprises-types (systèmes et réseaux). J'ai pu développer des compétences de communication vis-à-vis de la relation que j'ai pu entretenir avec les clients et leur prise en charge.

Je vais donc décrire l'entièreté de mon expérience au sein de chez SNS Solutions à travers ce rapport de stage, en commençant par présenter brièvement l'entreprise et son personnel, puis je continuerais en évoquant les outils de travail que nous utilisons pour traiter les demandes des clients. Je conclurai en prenant divers exemples d'interventions marquantes, et en décrivant la mise en place de mon Challenge Lab ainsi que les difficultés que j'ai pu rencontrer et les solutions que j'ai trouvées pour les contrer.

Un bilan global de ce stage ponctuera la fin de mon devoir en mettant en avant les compétences que j'ai acquises ou développées, et en établissant un lien avec l'apport de ce stage quant à mon projet professionnel.

I - Description de l'entreprise

1.1 Présentation

SNS Global Services, connue sous le nom de SNS SOLUTIONS, est une entreprise prestataire informatique fondée en 2004 par Olivier ETIENNE et Jean-Sébastien BIETTRON.
SNS Solutions fournit des prestations de services, du matériel, des liens d'accès, des solutions bureautiques, des logiciels métiers, de la téléphonie…

Alors en plein essor du secteur informatique, l'entreprise s'est très vite adaptée à ce dernier en adoptant les outils les plus performants pour exercer son activité principale : L'infogérance, où le contrôle de parcs informatiques d'entreprise. Le but initial étant de représenter la DSI* externalisée des utilisateurs clients, grâce à des outils propres à SNS.

L'évolution des technologies informatiques et logiciels ont rapidement convaincu SNS d'évoluer avec le marché. La première forte évolution de l'entreprise fut donc marquée par l'ajout des services liés à la téléphonie IP* en 2007, en adoptant des appareils MITEL (aujourd'hui fusionnées avec AASTRA), qui fut un pas majeur pour l'entreprise.

D'autres évolutions ont pu avoir lieu comme l'ajout d'une Branche de solutions sur la bureautique avec la demande grandissante d'intervention sur les imprimantes et scanners.
L'ouverture de cette branche donna suite à un panel de compétences plus évoluées, notamment sur les appareils Samsung, HP ou Canon.

Actuellement, on compte 5 agences réparties sur le territoire pour être au plus proche des clients : Marseille (Siège) / Toulouse / Sophia Antipolis / Monaco et Bordeaux.
Cette diversité de clientèles, d'environnements techniques, de prestations et de services permet une approche globale à même d'accompagner les clients sur l'ensemble de leurs problématiques IT*. Le plus petit client est un indépendant, tandis que le plus gros client possède plusieurs dizaines de sites, plusieurs centaines de machines, et des dizaines de serveurs.
Entre les deux, SNS maintient tous types de parcs techniques, de tailles différentes, en travaillant avec des administrations, des collectivités, des entreprises privées sur tous types de métiers (Industries, BtoC, BtoC, aide à la personne, Commerces, …)

L'entreprise est forte de ses 17 ans d'expériences accompagnés d'une croissance régulière et maitrisée, tout en restant à taille humaine ce qui donne une réactivité accrue face aux diverses situations.

Au fil de son évolution, l'activité de l'entreprise s'est grandement enrichie avec l'adoption de nouveaux outils et service logiciel. Les différents partenariats de SNS Solutions amènent l'entreprise à proposer des services personnalisés, allant de mise en place de serveurs (Cloud/TSE*/NAS*…), la gestion des services de messageries (Mail, Compte Exchange…), des propositions de matériels (PC*/Tablette/Périphériques divers…), etc.
Nous pouvons compter parmi les clients de SNS des entreprises comme Airbus Helicopters, Audition conseil ou encore les salles de sport Vita Liberté et bien d'autres, ce qui donne à la société ce rayonnement national.

1.2 Compétences et secteurs d'activités

SNS Solutions fournit un éventail de services adaptés aux TPE* / PME* :

RESEAUX

- Intégrateur de solutions de communications filaires (Allied et Cisco) et sans fils (Wifi – Aruba)
- Interconnexion de réseaux (Equipement de routage Bintec/Teldat/Allied/Zyxel/Ubiquiti)
- Certifié CISCO

SYSTEMES

- Partenaire Microsoft Certifié SMB (Tout OS Microsoft & Messagerie Exchange, Office 365)
- Partenaire Certifié Apple
- Virtualisation (VMWare & Microsoft Hyper-V)
- Partenaire Certifié DELL, LENOVO, VMWARE

SECURITE

- Sécurisation des réseaux informatiques (Firewalling Stormshield)
- Audit et sécurisation de réseaux filaires et sans fils
- Sécurisation des flux internet (Antivirus – Eset Nod, AntiSpam – Vaderetro, Tactical RMM)
- Certifié NETASQ/STORMSHIELD

DEVELOPPEMENT

- Développement applicatifs métiers sur mesure
- Développement applicatif sur appareils mobiles (tablettes, smartphone – IOS*,Android et Windows)
- Développement WEB

TELEPHONIE

- Partenaire premium 3CX (Téléphonie VoIP – Visioconférence – Softphone IOS Android) / Téléphonie Unifiée
- Construction de liens voix (LR, T0, T2), data (ADSL, VDSL, SDSL, Fibre) et Cloud(Centrex)
- Intégrateur de solutions Call Center
- Certifié MITEL, FUTUR, 3CX GOLD

BUREAUTIQUE

- Mise en place de solutions d'impression (A4, A3, traceur) avec maintenance
- Mise en place de solutions de GED (Gestion électronique de documents avec EUKLES)

CLOUD

- Infrastructure CLOUD
- Sauvegarde externalisée
- Mise en place de serveurs OVH

1.3 Partenariat et Clientèle

En quelques années, SNS Solutions a su forger des partenariats puissants avec des leaders du marché national et international. Cinq valeurs essentielles ont permis d'atteindre cet objectif : Disponibilité / Réactivité / Productivité / Performance / Adaptabilité.

Au fil des ans, le chiffre d'affaires évolue généralement à hauteur de 25 % à l'année, ce qui est propice à l'expansion de l'entreprise. La fiabilité de l'entreprise a permis d'ouvrir plusieurs agences dans une grande partie du Sud de la France comme l'agence de Monaco, Toulouse ou bien Sofia-Antipolis.

Cela signifie qu'avec une telle implantation, SNS Solutions peut exercer de la maintenance sur beaucoup d'agences différentes pour une même entreprise, mais également sur beaucoup de particuliers du secteur (Figure 1).

Figure 1 : Les principaux clients de SNS SOLUTIONS

Quant aux partenariats, ils sont nombreux (Figure 2). Les différents partenaires de SNS Solutions facilitent la mise en place de réseaux et de parcs informatiques fiables. Lorsqu'un client nécessite un nouveau besoin/service/appareil, nous lui recommandons une solution adaptée à ce qu'il recherche, en lui proposant des cotations (partie commerciale) pour un service qu'un de nos partenaires peut offrir.

Figure 2 : Les principaux Partenaires de SNS SOLUTIONS

1.4 Les membres de SNS Solutions

L'agence de Marseille représente le siège de toutes les agences de SNS (Figure 3). Elle est composée d'une équipe toujours plus grandissante et efficace. L'entreprise se veut être avant tout humaine en gardant cet esprit d'équipe et de cohésion. On trouve différents corps de métiers et de services, allant de l'aspect technique en contact avec les clients, à l'aspect commercial.

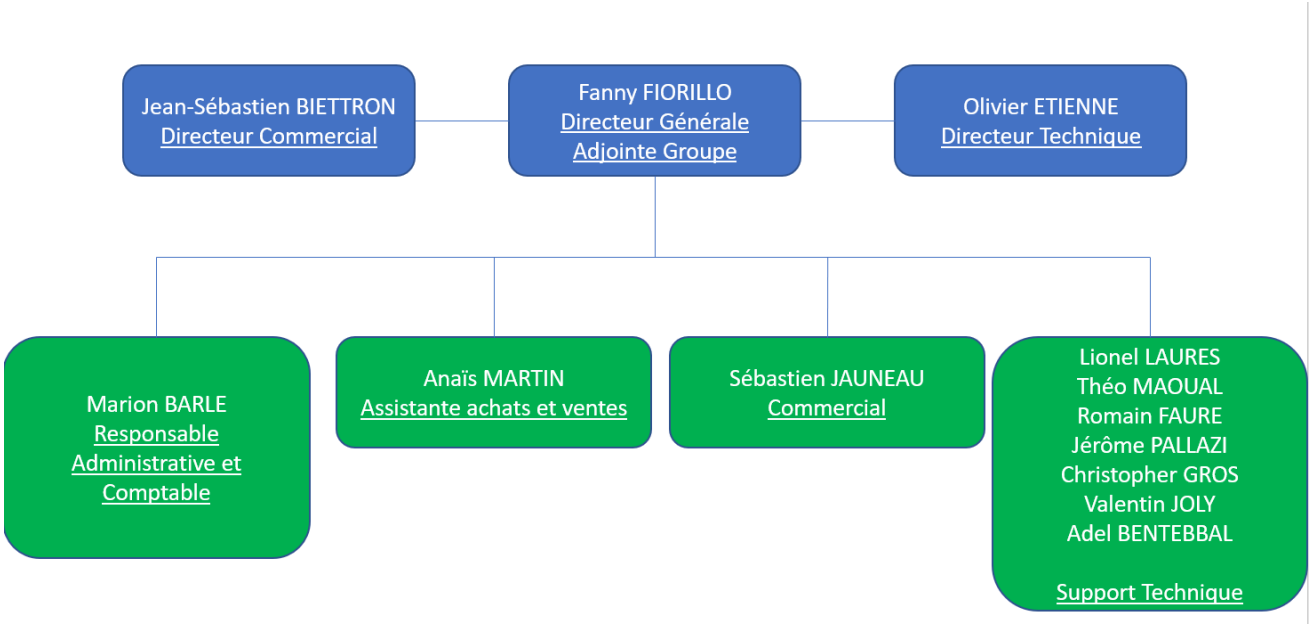

Figure 3 : Organigramme hiérarchique de SNS SOLUTIONS

II - Le Technicien de maintenance informatique

2.1 L'équipe Technique

Avec plus de 500 clients en infogérance, et 2400 clients actifs évalués au cours de l'année, les 5 agences de SNS Solutions ont pu réaliser plus de 15000 interventions par an. Cette performance est notamment justifiée par l'efficacité et la rapidité des équipes techniques de l'entreprise.

La majorité des interventions à réaliser sont des problèmes techniques ponctuels chez un client, classés selon la gravité d'un incident et la difficulté de ce dernier à être résolu. Les techniciens commencent en premier lieu par être contactés par le client (Mail ou téléphone), prennent alors un maximum d'informations sur le problème, et publient le ticket d'intervention sur la GPI*. L'Administrateur Systèmes et Réseaux se charge alors d'attribuer le ticket en fonction des paramètres vues précédemment. Cette manière de travailler se nomme la Télémaintenance.

La Télémaintenance, indispensable dans la gestion de parcs informatiques, désigne le contrôle à distance d'un appareil via un réseau de communication (Téléphone, Intranet ou Internet) dans le but de diagnostiquer, gérer et résoudre les problèmes de ce dernier. C'est donc logiquement la principale manière de travailler chez un prestataire informatique qui fait de l'infogérance.

Néanmoins, on compte aussi beaucoup d'interventions sur sites, ou de maintenances dites « permanentes » (visite hebdomadaire d'une entreprise cliente qui a opté pour le contrat adapté).

L'équipe Technique s'organise donc autour de l'Administrateur Systèmes et Réseaux qui distribue le travail, mais aussi en fonction du planning commun qui définit les interventions/événements de la semaine (Planning Outlook commun).

2.2 Les principaux outils de travail

2.2.1 3CX

L'outil de travail principal d'un membre de l'équipe technique de SNS Solutions est, sans nul doute, le plus indispensable de tous les outils : le Téléphone. En effet, la principale mission d'un technicien de maintenance informatique est de communiquer avec le client, que ce soit par la réception ou l'émission d'un appel. Il est donc plus qu'important de recueillir le maximum d'informations à chaque appel pour pouvoir résoudre un problème, et ceux, de la manière la plus efficace et rapide possible.

Outre cet aspect-là, le téléphone est également très important pour communiquer à distance avec nos collègues de l'équipe technique lorsque nous ne nous trouvons pas dans la même pièce que notre interlocuteur. C'est pourquoi SNS Solutions a opté pour une solution de téléphonie sur IP.

Les téléphones sont donc tous administrés par le standard téléphonique 3CX, qui permet d'émettre et recevoir des appels n'importe où avec nos smartphones, qui auront la même extension de bureau sur leur application 3CX. Au bureau, les téléphones 3CX sont des Yealink T46S.

2.2.2 La GPI

Ensuite, nous passons la majorité de notre temps sur notre poste informatique, notamment sur un outil propre à l'entreprise SNS : la GPI. Cet outil a été développé par Jean-Sébastien BIETTRON dans le but de répertorier les clients et les interventions en cours dans un même espace commun. Chaque client a sa propre fiche d'information, où on trouve absolument toutes les informations essentielles pour faire de la maintenance informatique (mots de passes utilisateurs, adresses IP, adresses électroniques, plans d'adressages, configurations, abonnements internet et téléphoniques…).

L'interface d'accueil de la GPI (Figure 4), permet déjà d'apercevoir beaucoup d'informations sur les tickets les plus récents en fonction du site d'exploitation (ici Marseille). On y trouve donc les tickets les plus récents, leur attribution, leur état et le degré d'urgence du ticket. Il y'a deux barres de recherche et un panneau déroulant permettant de filtrer les tickets selon l'intervenant afin de pouvoir filtrer au mieux ce que l'on recherche.
Enfin, on trouve de nombreuses statistiques comme le rapport tickets créés/résolus, où encore le nombres d'interventions et de temps passés par jour selon le technicien (tableau de classement en haut à droite). Attention, le type de contrat de maintenance (représenté par des couleurs) souscrit chez SNS Solutions influence le temps qu'un technicien doit mettre avant de commencer à traiter le ticket.

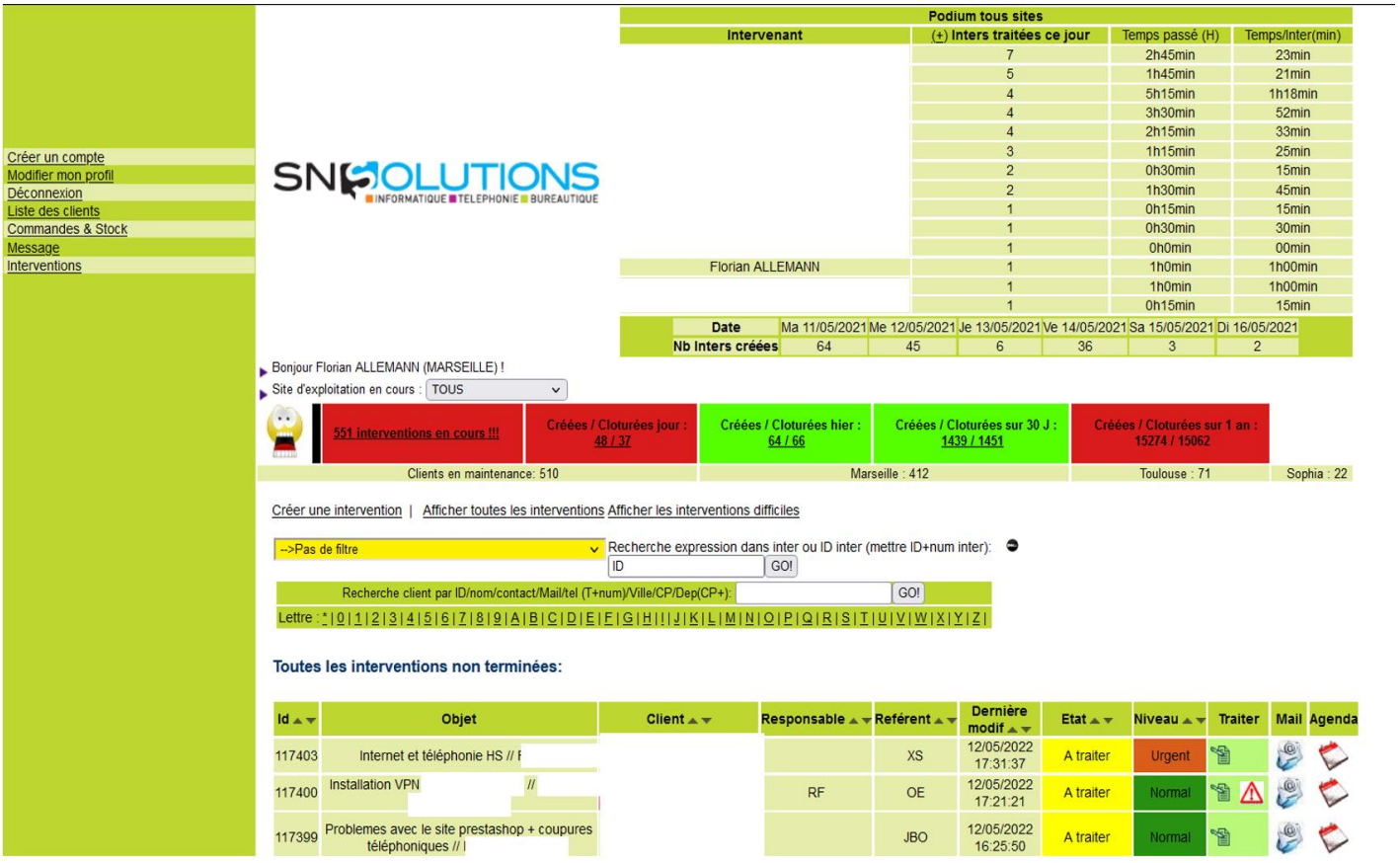

Figure 4 : Interface d'accueil de la GPI

Lorsque nous nous voyons attribuer un ticket à notre nom, nous pouvons évidemment obtenir plus de détails sur ce dernier en sélectionnant l'icone de papier dans la section « Traiter ». Nous obtenons alors les informations du ticket, classées par section selon l'interface propre des tickets de la GPI (Figure 5).

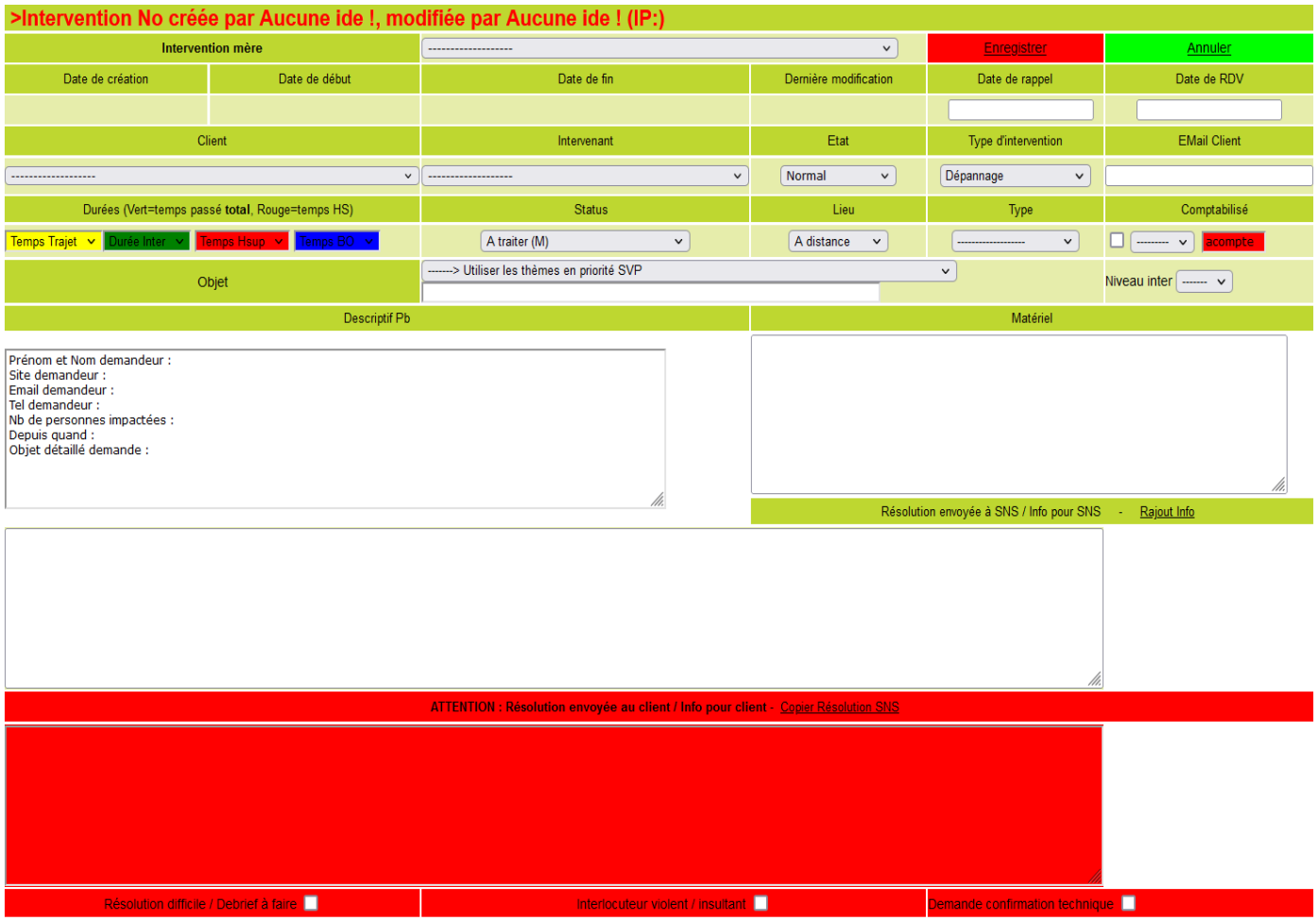

Figure 5 : Interface de création d'un ticket

Les informations à remplir par un technicien sont organisées par thèmes :

- La date et l'heure de la création du ticket, ou de la dernière modification de ce dernier (mais également des champs de date de rappel et de rendez-vous).
- L'entreprise cliente, l'intervenant en charge du ticket et les coordonnées de l'utilisateur ainsi que l'objet détaillé de sa demande.
- La durée passée sur le ticket au total (temps de trajet et ou d'heure sup…)
- Le statut du ticket (En cours, Terminé, Suspendu, RDV pris, Attente Rappel…)
- Un champ « Matériel », invisible pour le client où les techniciens partagent des informations entre eux.
- Un champ où nous allons décrire la manière dont on a procédé pour la résolution du problème. Chaque ligne ajoutée est datée afin de savoir précisément ce qui a été fait et surtout quand cela a été fait.

Actuellement, une nouvelle GPI (reprenant les mêmes fonctions que la précédente) est en développement, et j'ai eu la chance d'avoir un aperçu de ce à quoi elle devrait ressembler (Figure 6). Elle est fonctionnelle et d'ores et déjà utilisable par l'équipe technique. Cette dernière permettra d'accéder plus facilement et rapidement aux informations souhaitées.

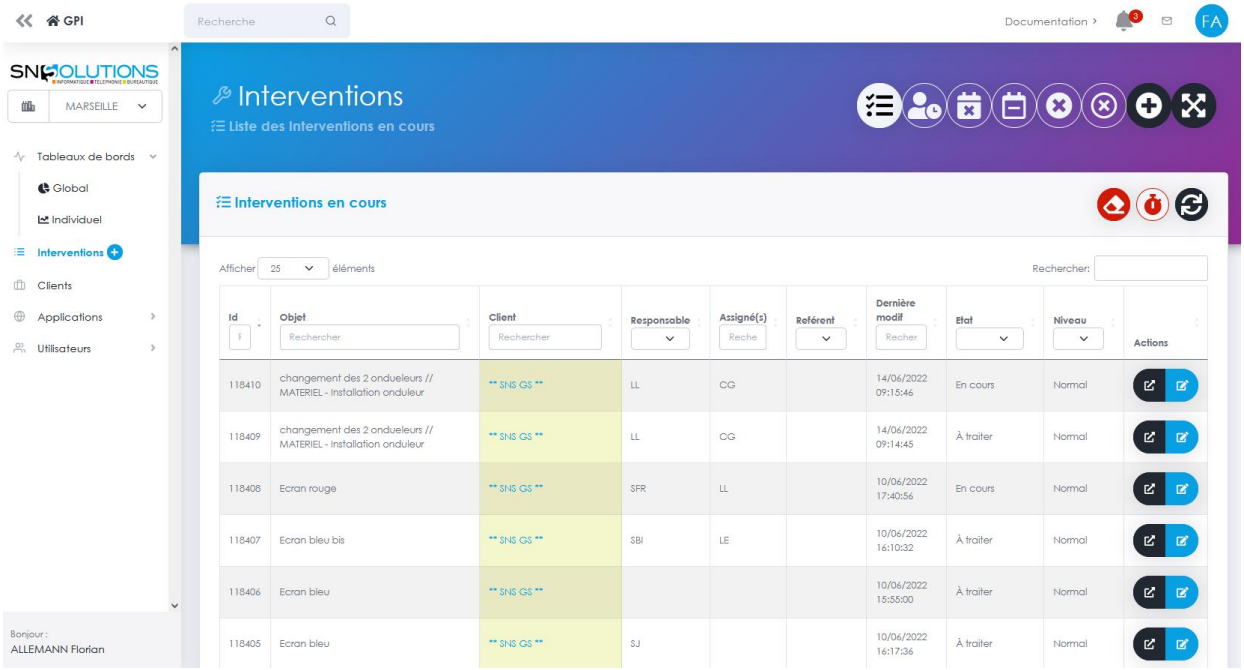

Figure 6 : GPI en développement

2.2.3 TeamViewer

Enfin, le dernier outil le plus utilisé chez SNS est le logiciel de maintenance TeamViewer (Figure 6). Ce logiciel d'infogérance permet de se connecter à la manière d'un bureau à distance sur un ordinateur client. Parfait pour faire de la maintenance informatique en allant directement régler le problème d'un utilisateur à distance. Cela représente un gain de temps considérable, car il permet de régler l'incident sans être sur place.

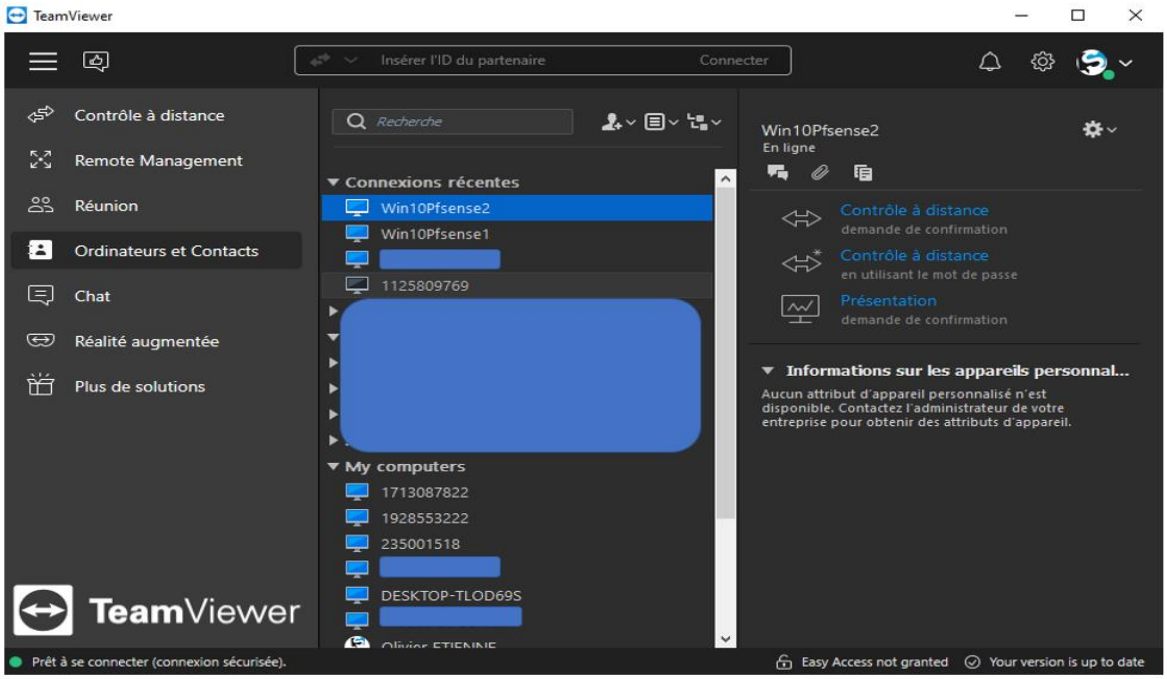

Figure 6 : Interface TeamViewer

III – Mon travail en tant que Technicien

3.1 Les tâches les plus récurrentes

Parmi les interventions que j'ai pu traiter, certaines étaient très similaires entre elles, et revenaient très souvent parmi bon nombre de clients…

3.1.1 Mot de passe oublié

Quel que soit la plateforme ou le logiciel possible, les utilisateurs ne sont pas des machines. Il arrive donc régulièrement que des utilisateurs nous appellent pour demander un mot de passe qu'il ne connait pas/plus. Parfois le mot de passe peut avoir expiré aussi. Quoiqu'il en soit, la procédure est toujours la même. Il faut commencer par vérifier si le mot de passe en question est présent sur la GPI. S'il faut réinitialiser le mot de passe, il faut passer par l'interface d'administration des mots de passes :

Exemples :

- Mot de passe session utilisateur (Figure 7)
- Mot de passe Office 365 (Figure 8)
- Etc….

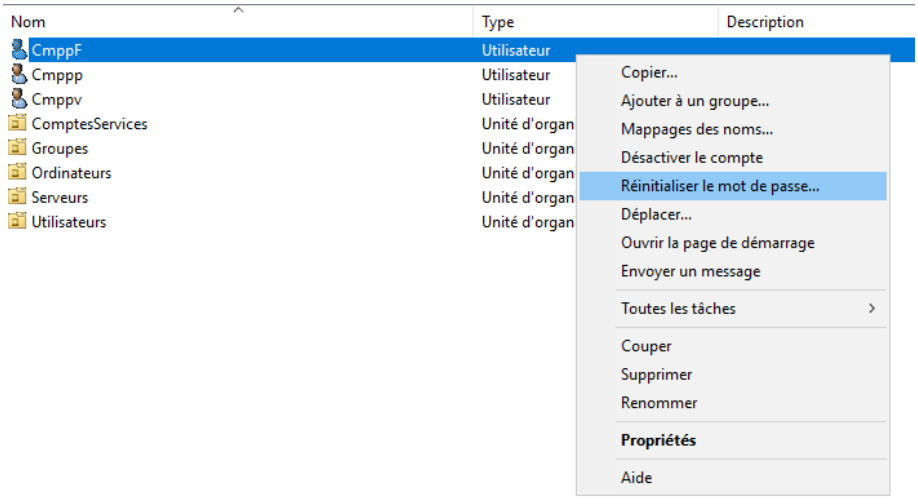

Figure 7 : Modification mot de passe utilisateur

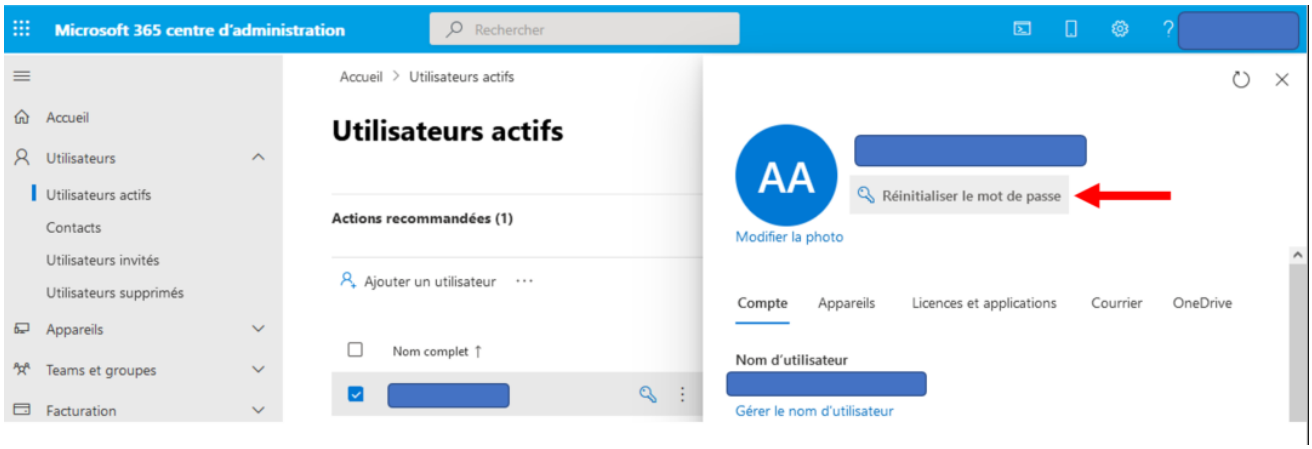

Figure 8 : Modification mot de passe compte Office 365

3.1.2 Dépannage d'imprimantes-scanners

Très souvent, les utilisateurs nous contactent pour un problème lié avec leur(s) imprimante(s). Cela peut être lié à l'imprimante elle-même (physiquement), à l'impression (impossible de communiquer avec l'appareil), ou bien un problème de Scan to Mail/Folder.

Il est donc important dans chaque cas de comprendre comment est (ou doit-être) installé l'appareil. Cela peut être installé sur un partage serveur (disponible pour les utilisateurs de tel(s) ou tel(s) groupe(s) selon les stratégies de groupes/GPO), ou localement sur le PC d'un utilisateur, ce qui est le cas le plus récurent (Figure 9).

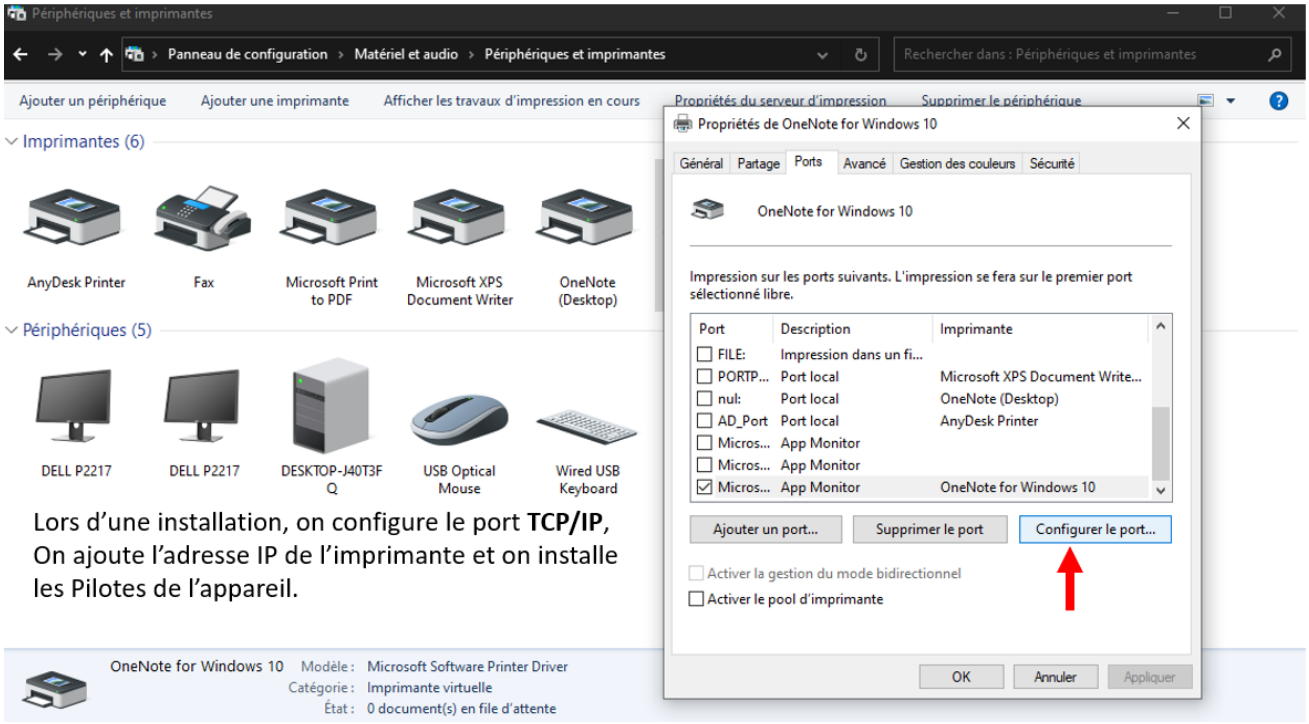

Figure 9 : Installation imprimante TCP/IP

3.1.3 Configuration VPN

Étant donné que SNS Solutions est partenaire avec l'entreprise **STORMSHIELD**, une grande partie de nos PME clientes (environ 40), sont équipés d'un Firewall* Stormshield.
En effet, en plus d'avoir une interface d'administration très complète et modifiable, les Pares-Feux Stormshield sont compatibles avec un client de VPN SSL Open Source très efficace : **Open VPN.**
Ce-dernier est très simple d'utilisation, et permet de se connecter avec n'importe quel IP source au site souhaité, si l'on possède le bon certificat d'utilisation.

On peut installer Open VPN depuis n'importe quel navigateur. En se connectant au portail captif **Client Utilisateur** (Figure 10), le firewall Stormshield peut s'avérer très utile car nous pouvons aller chercher le fichier de configuration d'Open VPN directement sur le portail. Il suffit alors de déposer le fichier de configuration du VPN sur Open VPN (Figure 11) pour pouvoir autoconfigurer le client en 2 clics (sans oublier de configurer le VPN avec TLS).

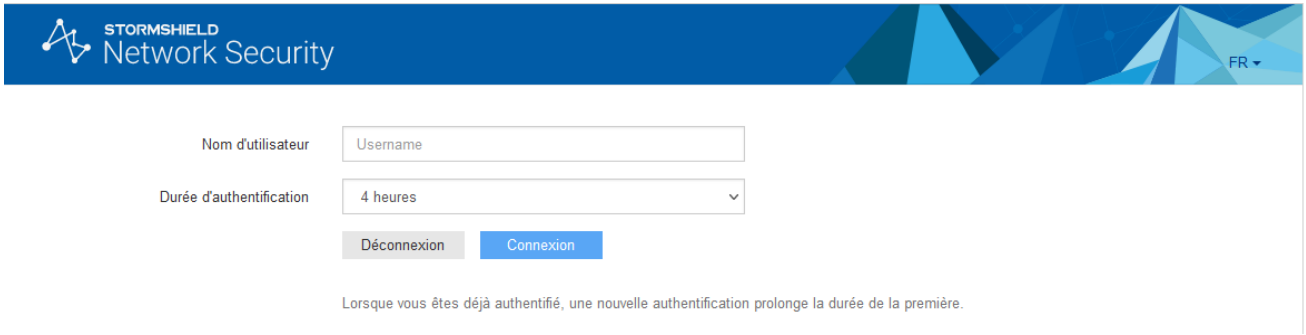

Figure 10 : Portail Captif utilisateur STORMSHIELD

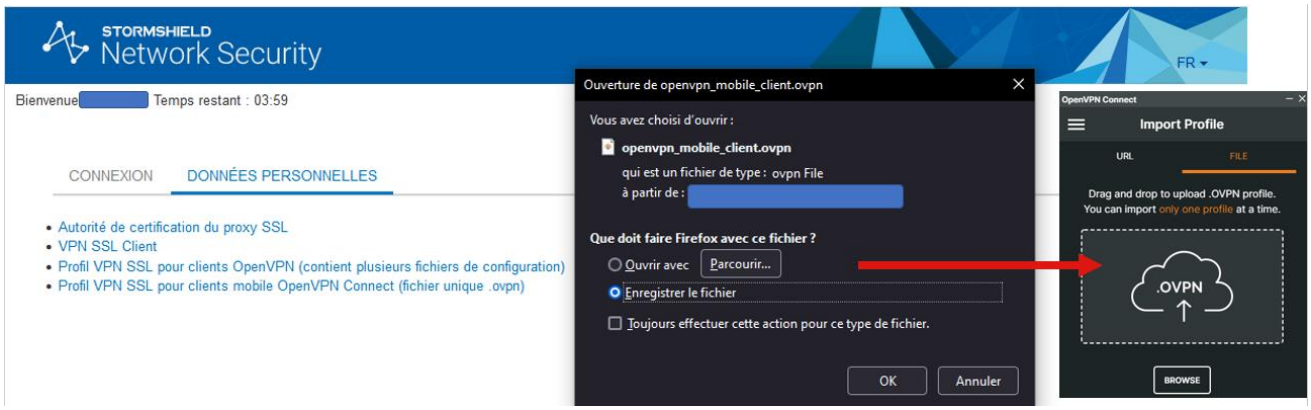

Figure 11 : Configuration Open VPN

3.1.4 Les interventions sur place

Au cours de mon stage, j'ai eu la chance de pouvoir accompagner mon tuteur de stage, Théo Maoual, dans ses interventions dîtes « permanentes » au sein de l'entreprise WIKO. C'est une visite de maintenance hebdomadaire, et qui permet de rencontrer les utilisateurs, et de dépanner chacun d'eux en fonction de ses besoins.
Ainsi, j'ai pu voir les locaux de l'entreprise de WIKO et mettre un visage sur des clients que j'ai pu entendre au téléphone.

L'expérience d'une permanence est très enrichissante et différente du temps normal. En effet, ce n'est pas forcément au client de faire le premier pas, mais à nous d'aller les voir afin de diagnostiquer un quelconque problème.

Pour ma part, j'ai configuré 5 PC portables Dell totalement neufs pour des utilisateurs WIKO afin de remplacer leurs PC actuels. J'ai commencé par boot les PC sur un WDS afin de préinstaller des logiciels de maintenance directement au premier démarrage (TeamViewer, Eset Antivirus, Tactical RMM…).
Il a fallu par la suite connecter les utilisateurs au Domaine de WIKO (wikomobile.local), installer des certificats « personnels » et pour les « Autorités de certification racine » (car ceux-ci sont obligatoires pour accéder aux services intranet de WIKO), configurer les paramétrages DNS, gérer les applications par défauts, connecter le compte Office…

IV – Projet « Challenge LAB »

4.1 Plan du projet

Environ deux semaines après le début de mon stage, et à la suite d'une discussion avec Théo MAOUAL et Olivier ETIENNE, ces derniers décident de m'attribuer un projet, assez complexe pour que je puisse le réaliser pendant toute la durée de mon stage. Ce projet est à la fois enrichissant pour mon stage, et utile pour eux car le but est de monter un LAB qui peut être maintenu.

L'objectif du projet est de déterminer s'il est possible, à travers un tunnel VPN IPSEC, de faire communiquer une borne UNIFI (Réseau LAN 1), à un contrôleur situé dans un réseau différent (Réseau LAN 2), le tout en passant à travers ce tunnel. Je vais donc vous présenter dans un premier temps le plan du projet et le matériel que j'ai utilisé, puis j'expliquerai par étapes comment je suis venu à bout de ce projet, et qu'elles ont été les difficultés rencontrées.

Tout d'abord, le plan Physique (Figure 12). Le matériel qui m'a été mis à disposition est le suivant :

- Deux routeurs 4G TP Link
- Un serveur de virtualisation DELL PowerEdge R200
- Un PC Dell
- Un Switch POE* (pour alimenter la borne UNIFI et la connecter au réseau)
- Une borne Wifi* UNIFI

Le but est donc de me servir des routeurs 4G pour créer deux réseaux WAN distincts indépendants, et de me servir des serveurs de virtualisation pour créer des machines virtuelles capable d'établir un tunnel VPN IPSEC.

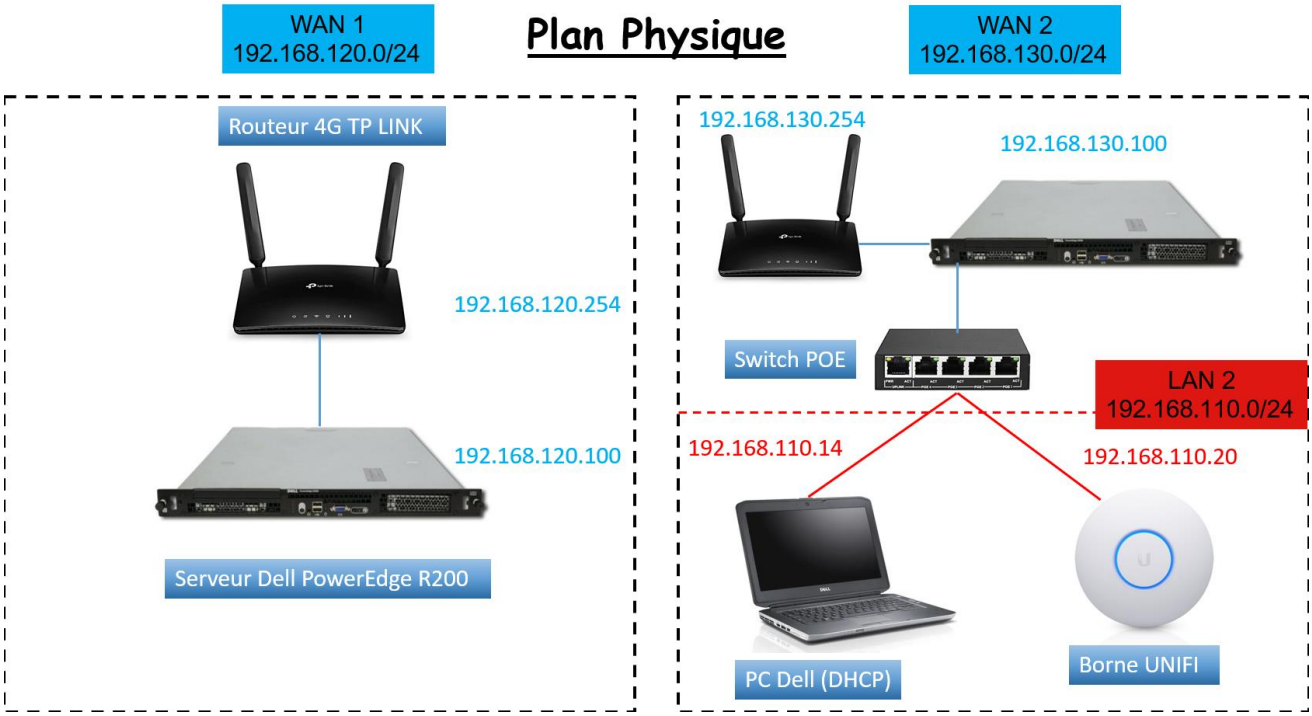

Figure 12 : Projet (Plan Physique)

À l'intérieur de ces deux WAN, on trouve dans chacun d'eux un réseau LAN qui lui est propre, et une DMZ* administré par le routeur 4G.

Passons maintenant sur le plan Logique (Figure 13) :

- Deux Serveurs ESXI (avec un switch virtuel intégré)
- Deux FW PFSense (responsable du VPN, DHCP*, routage, règles de trafic…)
- Deux Windows 10 (pour administrer les LAN/WAN avec TeamViewer)
- Une VM Debian 10
- Un contrôleur UNIFI (créé par la Debian)

Assurément, les machines virtuelles les plus importantes dans ce projet sont les deux Firewall PFSense, qui jouent un rôle majeur dans cette configuration.

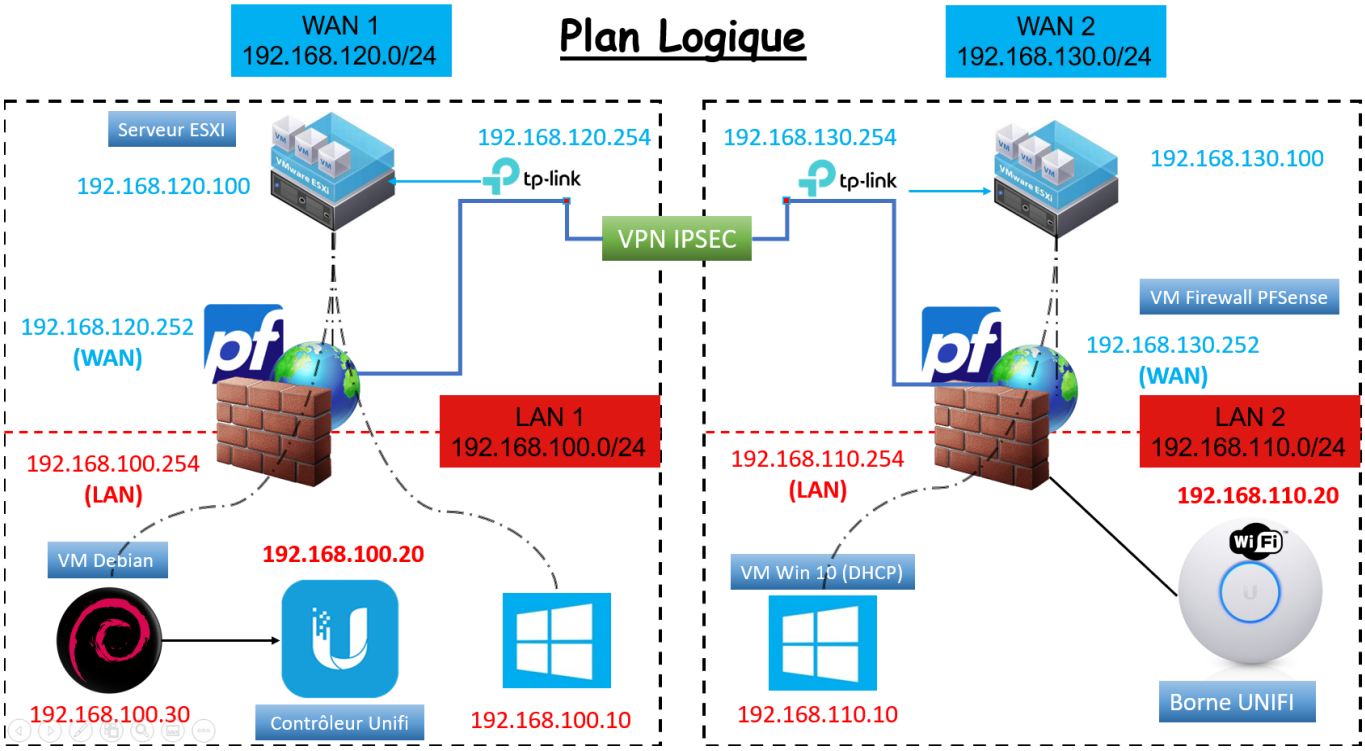

Figure 13 : Projet (Plan Logique)

4.2 Routeur, serveur ESXI et machines virtuelles

La première étape de mon projet était de configurer deux réseaux WAN à l'aide des routeurs 4G tp-link (Figure 14). Cette étape fut assez rapide, car l'interface WEB des routeurs est facilement accessible et personnalisable. J'ai donc monté deux réseaux WAN en [192.168.120-130.0/24].

Afin de pouvoir accéder au réseau des routeurs (situés dans la salle des serveurs) depuis mon bureau, j'ai dû effectuer un brassage sur le commutateur de l'entreprise afin que le réseau des tp-link passent par ma prise murale Ethernet, ce qui m'a permis de ne pas travailler hors de mon bureau, et ainsi pouvoir recevoir les appels des clients en parallèle.

J'ai également préparé une DMZ pour ma future interface de sortie WAN de mes firewalls à l'avance ([192.168.120-130.252]), afin de sécuriser mes infrastructures et faire fonctionner le future VPN IPSEC.

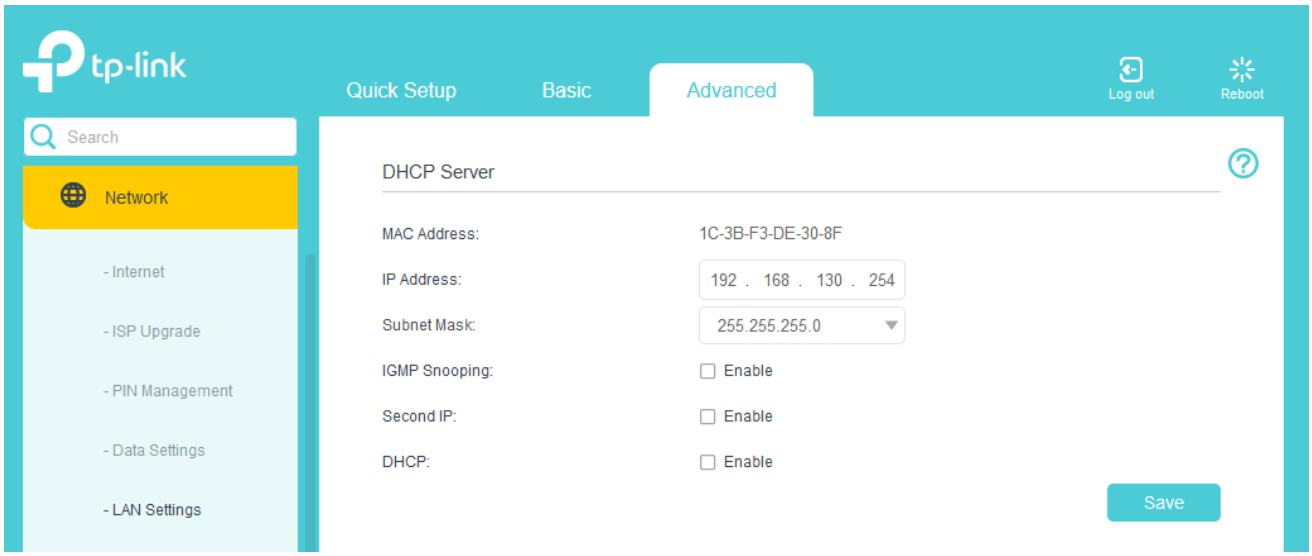

Figure 14: Interface Tp-link (LAN 2)

Par la suite, j'ai dû m'occuper des 2 serveurs de virtualisation. Ces derniers étaient totalement vierges, et il a fallu donc formater les disques durs, et démonter l'un des deux serveurs (car il manquait un HDD). J'ai donc appris à booter un appareil sur un OS depuis le BIOS, après avoir préparé une clé USB bootable via le logiciel Rufus. J'ai donc installé l'OS VMware ESXI (Figure 15) sur les 2 serveurs, en les ayant connectés à leur réseau WAN en amont.

VMware ESXi est un hyperviseur de type 1 indépendant des systèmes d'exploitation. Il repose lui-même sur le système d'exploitation VMkernel qui assure l'interface avec les agents dont il soutient l'exécution. Pour ma part, après avoir installé et configuré les deux serveurs, je me suis occupé de récupérer les ISO* des VM que je devais monter.

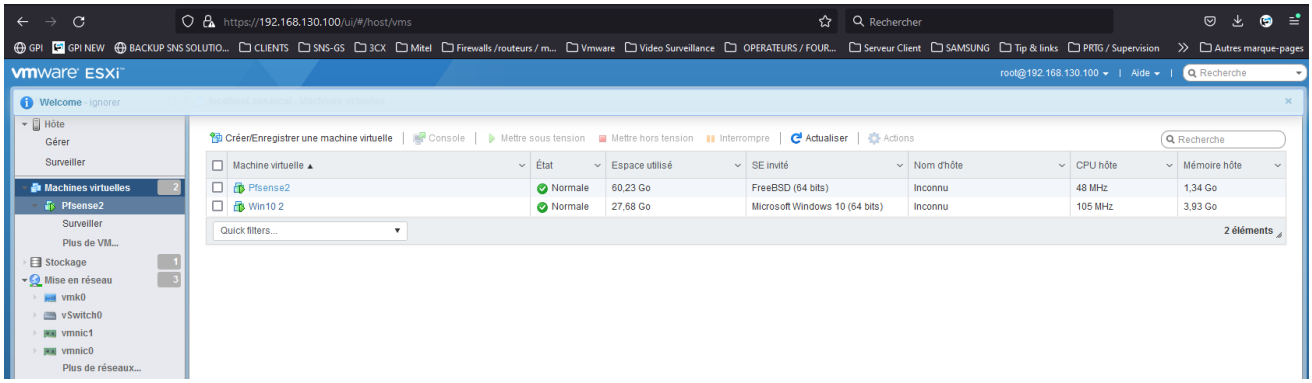

Figure 15 : Gestionnaire de VM ESXI

J'ai donc créé les machines virtuelles (cf. Figure 13), et j'ai commencé à les affecter sur leur interface respective (LAN ou WAN). Pour cela, j'ai utilisé le commutateur virtuel offert par ESXI 5 (Figure 16). Ce dernier fonctionne en parallèle avec mon PFSense, afin de placer dans un LAN les VM, et leur attribuer une adresse automatiquement, à l'aide du service de DHCP des PFSense. Attention, il ne faut pas oublier que **c'est le pare-feu qui doit délivrer le DHCP et non le routeur !** Cela pourrait entrainer des dysfonctionnements dans cette configuration car il pourrait y-avoir des problèmes d'adressages, ou de conflits d'adresses (problème que j'ai pu rencontrer).

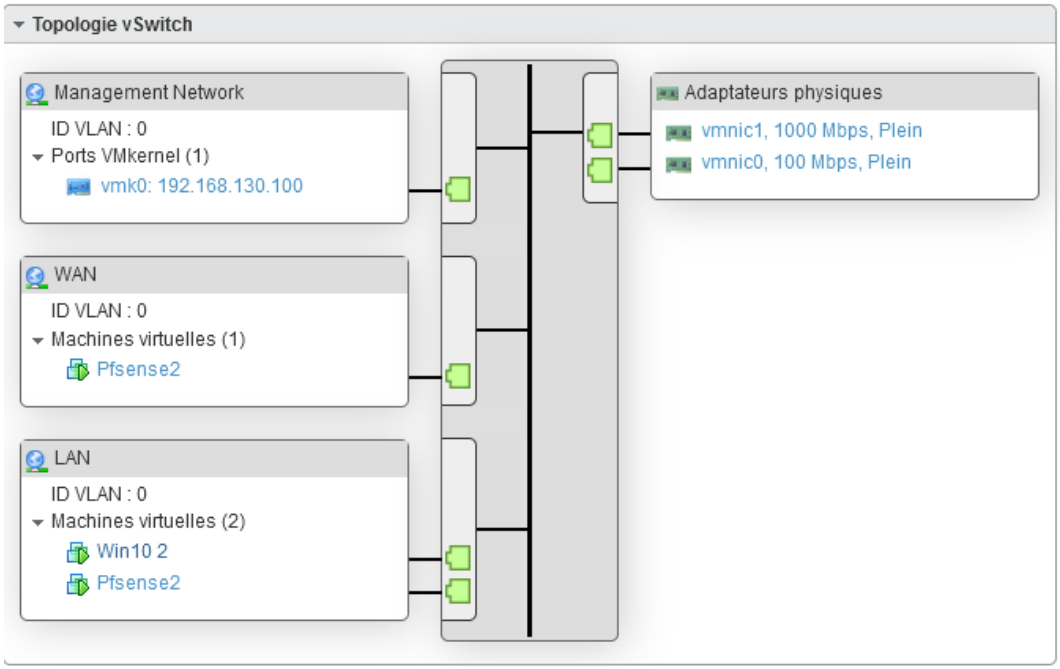

Figure 16: Switch Virtuelle VSwitch (LAN 2)

4.3 Configuration Firewall PFSense et VPN IPSEC

La partie la plus fastidieuse et difficile de mon projet fut sans nul doute l'accomplissement de l'objectif principal : l'établissement d'un VPN IP SEC sécurisé et fonctionnel. Pour cela, il a fallu dans un premier temps configurer les Firewall PFSense à partir du premier démarrage. Une fois fait, il a fallu que je créé les interfaces WAN et LAN des Firewall PFSense, en les attribuant aux deux cartes réseaux des serveurs de virtualisation. Cela a pris beaucoup de temps, car à cette étape, il fallait que je recommence à chaque problème, et ce depuis le début (or, l'entreprise à connu de nombreuses coupures de courant au cours de mon stage, due à des problèmes d'onduleurs).

Ensuite, j'ai configuré les serveurs DHCP des réseaux LAN, en prenant bien compte de choisir une range d'adresse large en cas de manque d'adresses (Figure 17).

Après cela, je me suis occupé d'établir des règles de trafic (Figure 18), afin d'autoriser les réseaux LAN à envoyer des requêtes à son homologue respectif, et à autoriser les paquets TCP (une liste de ports précis qui sont nécessaires pour faire fonctionner la communication entre la borne Unifi et le contrôleur). Dans un premier temps, les règles de trafic ont concerné les ports LAN et WAN. Au commencement du projet, et par besoin, j'ai mis des règles de PASS ALL* sur les deux firewalls, pour simplifier la communication et transmission des paquets lors du routage.

A partir de ce moment, j'ai commencé à faire des tests constamment depuis les VM Windows, afin de toujours vérifier que les infrastructures fonctionnent, que le DHCP assure ses fonctions, et qu'internet soit disponible.

La prochaine étape fut donc l'étape la plus difficile et longue du projet : la mise en place du VPN IP SEC (Figure 19). Cette étape à elle seule n'est pas compliquée, mais elle nécessite une parfaite connaissance des 2 réseaux (IP, masques, IP publiques, DNS…), mais également qu'il n'y ait aucun problème dans les deux réseaux, et que les règles de filtrages soient parfaites.

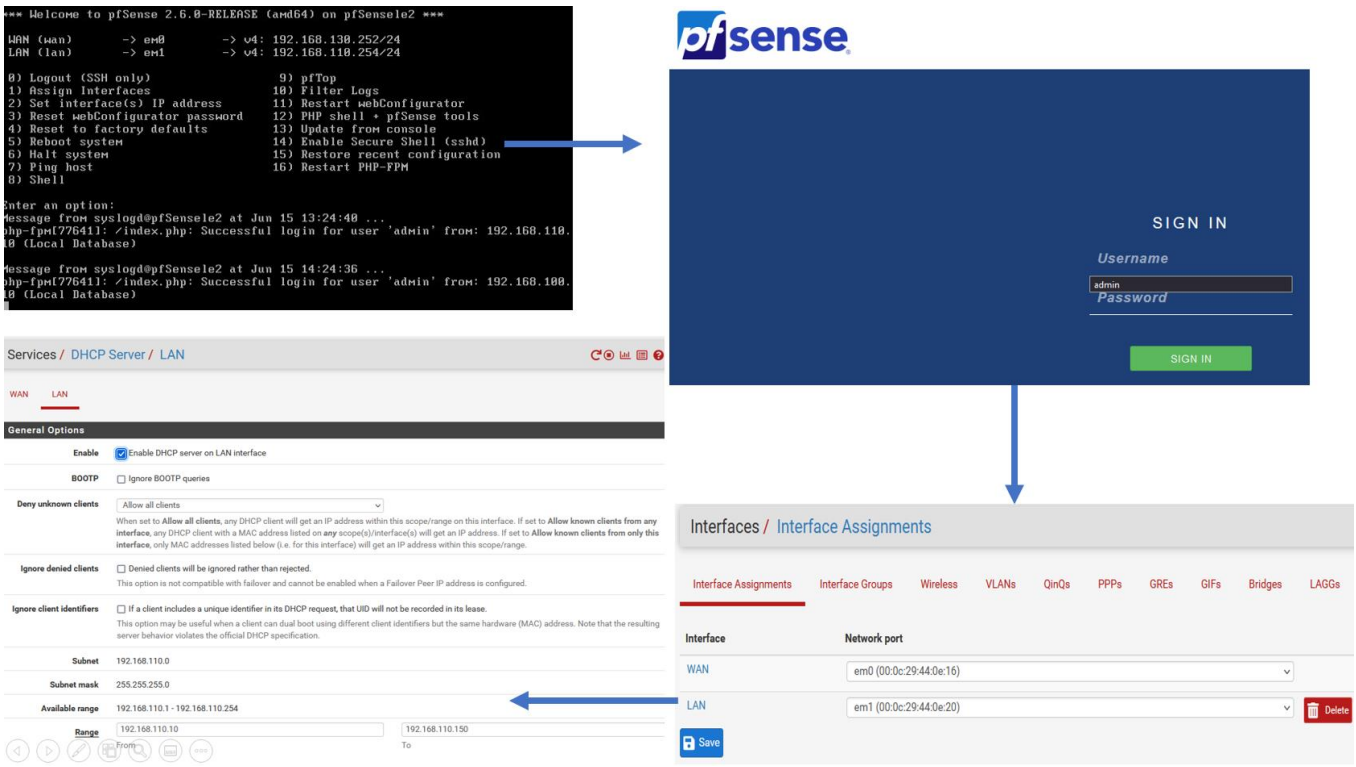

Figure 17 : Premiers pas sur le PFSense (WAN 2)

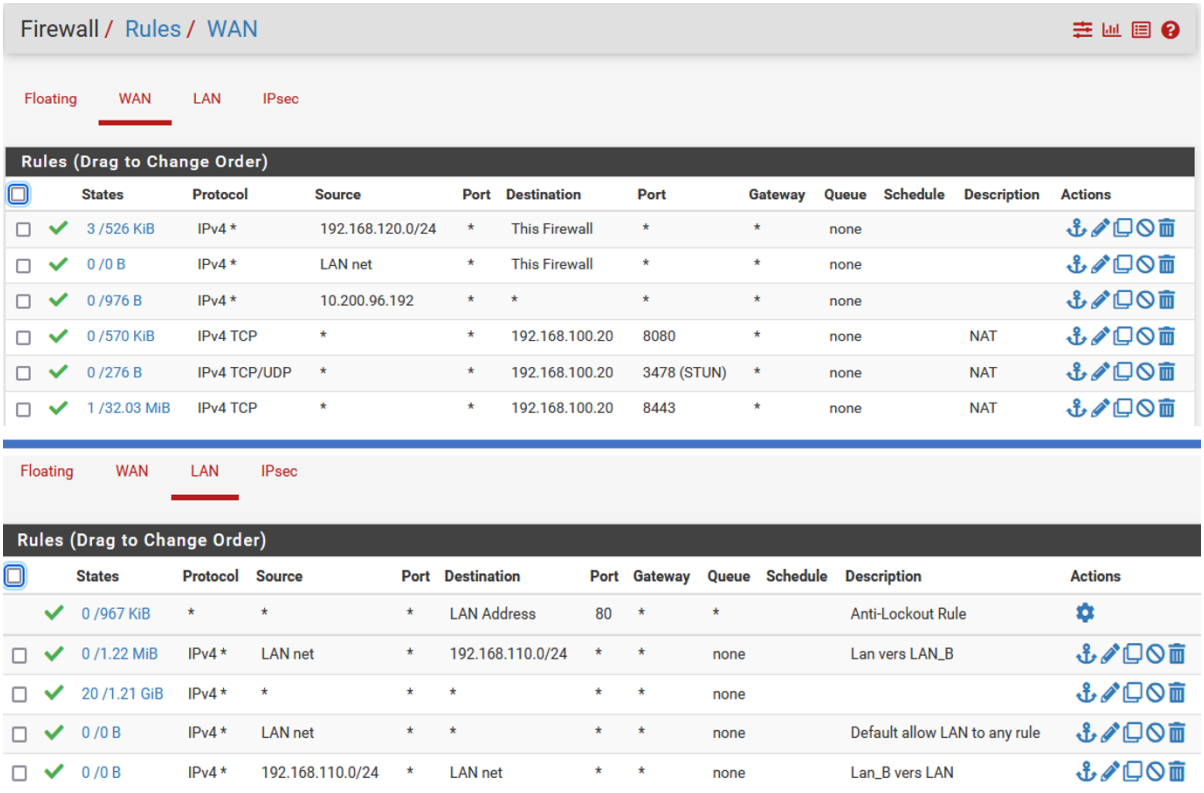

Figure 18 : Règles de Trafic PFSense (WAN 1)

Une fois mes règles faites, il ne me manquait plus qu'a établir le tunnel VPN sur les deux PFSense, en rentrant quasiment les mêmes informations dans les 2 pares-feux.

A partir du moment ou le statut du tunnel était en « Established », les deux LAN étaient capables de communiquer entre eux (requête ICMP). Il ne restait donc plus qu'une étape : faire communiquer la borne UNIFI et le contrôleur.

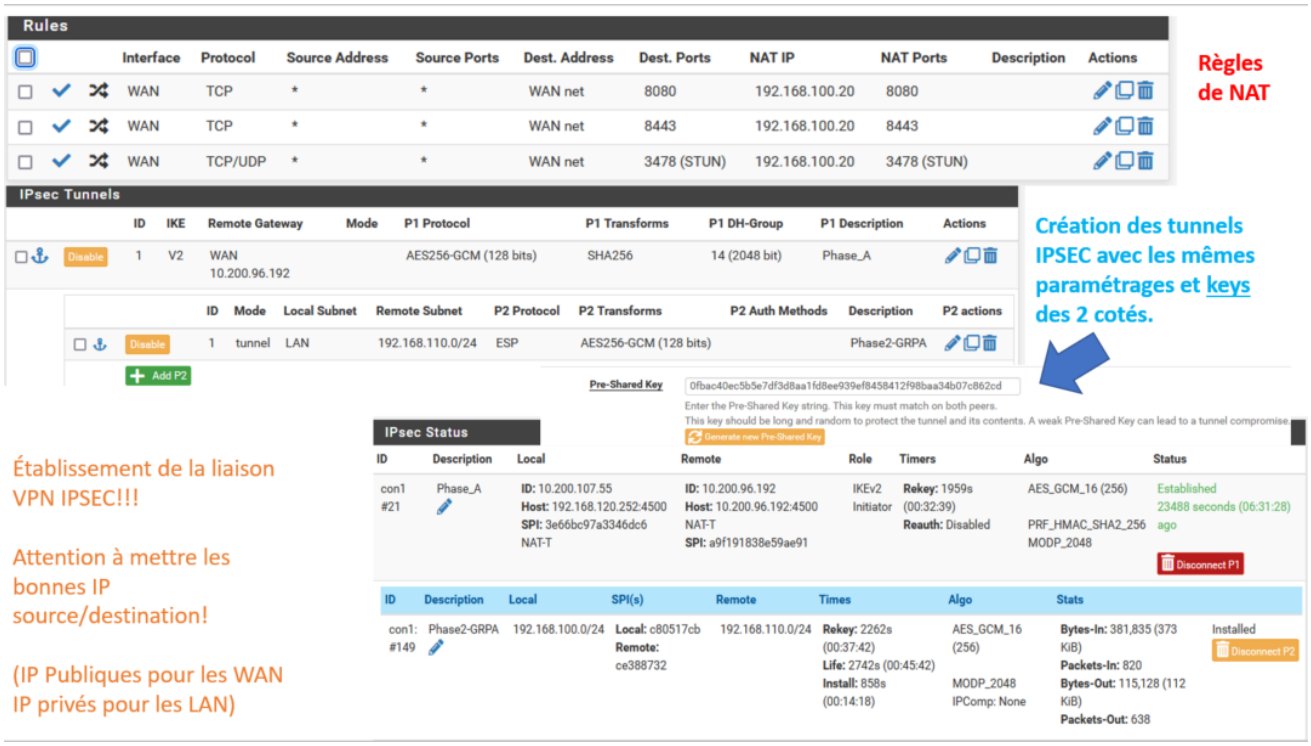

Figure 19 : VPN IPSEC (WAN 1)

4.4 Communication Borne Contrôleur et WIFI

Le tunnel VPN étant monté, il suffit de se connecter en SSH sur la borne UNIFI et de lui indiquer d'envoyer une requête à l'adresse du contrôleur [192.168.100.20] (Figure 20). J'ai pu ainsi terminer mon projet qui fut une très bonne expérience.

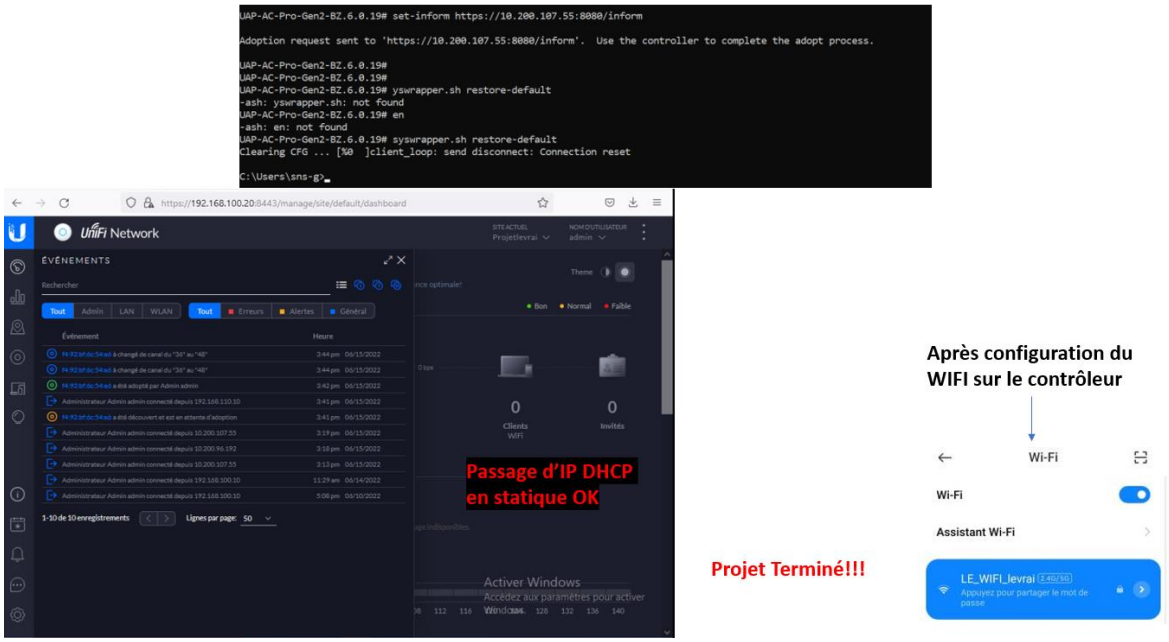

Figure 20 : Communication Borne Contrôleur UNIFI

Conclusion

Ainsi, j'ai effectué mon stage de fin d'étude du DUT R&T au sein de l'entreprise SNS Solutions en tant que technicien de maintenance informatique à Marseille.

Pendant ce stage de 10 semaines j'ai pu mettre en pratique mes connaissances théoriques acquises durant ma formation, en apprenant beaucoup grâce à des professionnels tout en étant confronté aux difficultés réelles du monde du travail. Les apports du stage sont nombreux. Au cours de ces dix semaines, j'ai beaucoup appris tant au niveau théorique que pratique, notamment avec mon projet.

Après une rapide intégration au sein de l'équipe technique, j'ai eu l'occasion de réaliser de nombreuses interventions qui ont constitué une mission de stage globale et chacune de ces missions, à distance ou chez le client, ont été utiles au bon fonctionnement de l'activité de l'entreprise.

Ce stage a été très enrichissant pour moi, d'une part il m'a permis de découvrir de manière plus technique et approfondie le domaine de l'infogérance, de connaître ses acteurs, d'appréhender ses contraintes, d'être réactif, d'apprendre à utiliser les logiciels pour le bon fonctionnement des appareils...

Je sors de cette période pleinement satisfait de l'expérience professionnelle valorisante acquise qui constitue une base pour mon avenir ainsi que de nouvelles compétences solides obtenue grâce aux bonnes conditions du déroulement du stage.

Mon projet professionnel étant d'exercer le métier d'administrateur systèmes et réseaux, cette première expérience va s'avérer plus que bénéfique en vue de mon insertion professionnelle car elle a permis d'approfondir mes connaissances dans l'administration système ce qui concorde parfaitement avec mon projet professionnel. C'est donc logiquement que je souhaite intégrer la Licence Pro ASUR au sein du même IUT*.

Enfin je ne peux qu'être satisfait après avoir pu travailler dans de bonnes conditions matérielles et un bon environnement de travail, des locaux modernes, une ambiance agréable et un personnel amical établissant ainsi une atmosphère de confiance solide.

Remerciements

Tout d'abord je tiens à remercier mon tuteur pédagogique, **Théo Maoual**, technicien au sein de l'entreprise SNS SOLUTIONS, pour m'avoir accompagné tout au long de mon stage, de m'avoir donné des responsabilités pendant la durée du stage, pour tous ses conseils, d'avoir été à l'écoute et d'avoir guidé ma démarche lors des projets.

Ensuite, je tenais à remercier particulièrement Messieurs **Jean-Sébastien BIETTRON** et **Olivier ETIENNE**, gérants de SNS Solutions, pour m'avoir accueilli et supervisé durant ces 10 semaines au sein de l'entreprise.

Je tiens à remercier de même toute l'équipe au service technique pour leur accueil, leur sympathie et surtout leur esprit d'équipe qui m'a vraiment conforté tout au long du stage. J'ai vraiment apprécié cet environnement de travail convivial et sérieux à la fois, qui est un peu la marque de fabrique de cette équipe de SNS SOLUTIONS.

Je tiens aussi à remercier l'ensemble de l'équipe commerciale pour son accueil, pour m'avoir aidé durant mon stage, mais également **Marion BARLE** pour la gestion administrative rigoureuse de mon stage.

Enfin, je tiens aussi à remercier mon tuteur académique, **Jean-Luc DAMOISEAUX**, pour son implication dans le bon déroulement de mon stage.

Glossaire

DHCP, Le protocole DHCP sert principalement à distribuer des adresses IP sur un réseau.

DMZ, zone démilitarisée

DUT, Diplôme Universitaire de Technologie.

DSI, Directeur des systèmes d'information.

Firewall, Pare-feu

Infogérance, Gestion de tâches informatiques confiées par une entreprise à un prestataire extérieur.

IP, Protocole internet.

IUT, Institut Universitaire de Technologie.

IT, Information Technology

GPI, Gestion Parc Informatique.

LAN, Local Area Network

NAS, périphérique de stockage intelligent connecté au réseau

PC, Personal Computer.

PME, Petites et moyennes entreprises.

POE, (Power Over Ethernet) Permet l'alimentation électrique à partir d'un équipement de niveau 2 (Switch).

TPE, Très petites entreprises

TSE, Terminal Server Edition.

VM, Machine virtuelle.

VPN IPSEC, connexion sécurisée et chiffrée entre deux réseaux ou entre un utilisateur individuel et un réseau par « tunneling ».

WAN, Wide Area Network

WIFI, Wireless Fidelity

Bibliographie

https://www.snsolutions.fr

https://www.vmware.com/fr/products/esxi-and-esx.html

https://community.ui.com

https://www.osnet.eu/fr/forum/4