Institut Universitaire de Technologie,
Aix-Marseille Université

RAPPORT DE STAGE
Diplôme Universitaire de Technologie
Spécialité Réseaux et Télécommunications

ASSISTANT Responsable Sécurité Informatique

Loïc MAURER

THEMYS

Responsable entreprise : Christophe Clément

Responsable académique : Anouch Hovsepian

2019

Table des matières

1 Introduction

L'informatique occupe une place de plus en plus importante dans le domaine maritime, c'est dans ce contexte que j'ai pu intégrer l'entreprise Themys pour mon stage de deuxième année DUT Réseaux & Télécommunications. Au cours de ce stage, j'ai participé aux différentes missions confiées au service informatique. Nous présenterons dans ce rapport, le secteur d'activité dans lequel j'ai évolué, et la position de Themys sur ce marché. Nous détaillerons également les différentes missions qui m'ont été confiées. Nous analyserons aussi les contraintes liées au contexte maritime de notre activité et finirons par un résumé de cette expérience très enrichissante dans cette société.

2 Themys

2.1 L'entreprise

Située à Roquevaire, Themys est une PME de trente employés spécialisés dans les équipements de communication et de navigation maritimes. Créée dans les années 90, la société devient leader dans la fourniture des systèmes de communications réglementaires pour les navires (SMDSM). Elle devient ensuite premier centre de formation en France pour les équipages, et pour les inspecteurs de l'ANFR. La société se spécialisera également dans la vente et l'installation d'antennes marines motorisées (VSAT, TV-SAT) puis dans les équipements de navigation.
Cette entreprise intervient dans les secteurs du yachting, des navires de commerce et passagers, de l'offshore et du militaire. Chaque type de navire a ses propres contraintes, ainsi la réglementation pour un navire à passager ne sera pas la même que pour un navire militaire. De même les impératifs opérationnels d'un navire militaire sont très différents d'un navire civil. Les équipements et solutions déployés contiennent de plus en plus de composants informatiques et les problématiques cybers liés à ces équipements deviennent critiques. La société s'est donc préparée à ce changement majeur pour les années à venir, ce qui lui permet d'être considérée comme une référence dans son domaine d'activité.
NB : Nous aurons l'occasion d'étudier quelques équipements de communication dans les tâches qui me seront confiées.

2.2 Organigramme

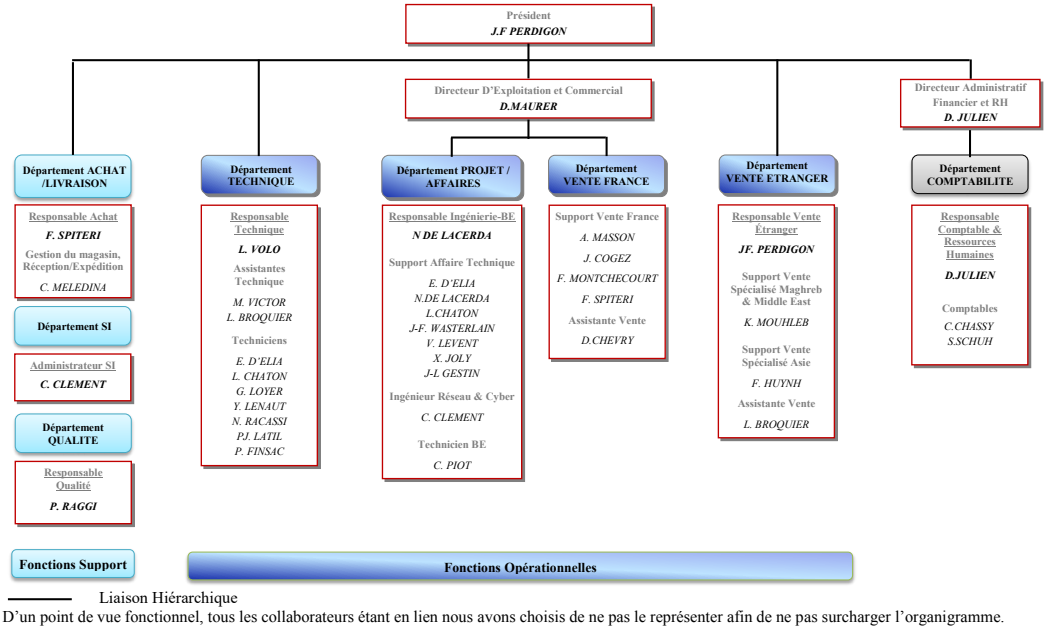

Figure 1 : Organigramme

Voir annexe 1 : cartographie des processus mettant en évidence les liens entre les services.

2.3 Le service informatique

Le service informatique ne compte actuellement qu'une personne. Ma mission était de l'assister pour assurer la maintenance et la migration de l'infrastructure Themys, et auprès du service projet/affaire traiter les sujets liés à l'informatique dans nos solutions matérielles. Etant dans une PME, les missions se sont avérées aussi diverses que variées. En effet ce service s'occupe de l'infra réseau et système de l'entreprise et en assure la sécurité. Il participe également activement aux projets techniques pour les clients. L'infrastructure réseau de l'entreprise est la suivante (figure 2) :

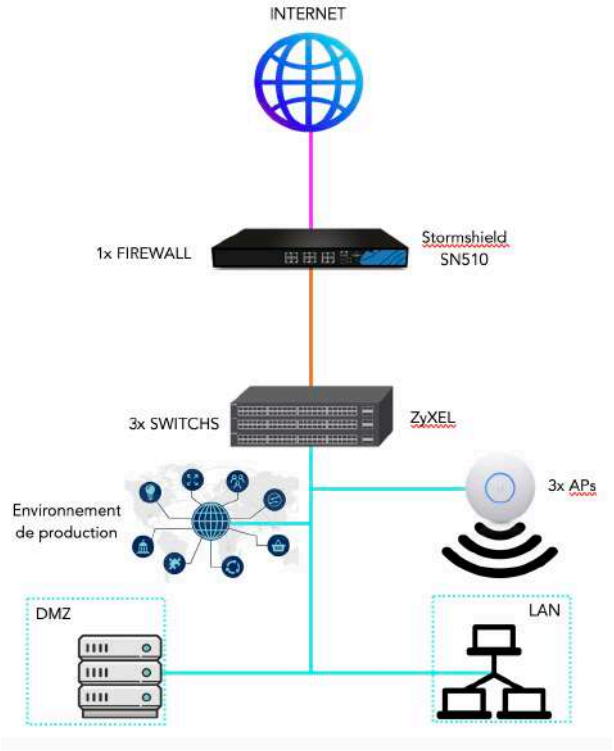

Figure 2 : Infrastructure réseaux Themys

3 Assistant Responsable Sécurité Informatique

En tant qu'assistant du RSI (Responsable Sécurité Informatique), j'ai eu l'opportunité de développer de nouvelles compétences et découvrir un milieu qui ne m'était pas familier. Tout au long de ce stage j'ai pu effectuer diverses missions, cependant je vais me concentrer sur trois projets qui ont constitué le cœur même de mon stage et nous finirons par diverses tâches que j'ai eu à effectuer.

3.1 Projet VPN

3.1.1 Contexte

Dans le cadre d'un projet internet à l'entreprise afin d'élaborer une solution pour des clients j'ai été amené à mettre en place une connexion sécurisée entre l'entreprise et un navire. L'objectif de ce projet est la maintenance de l'équipement de communication radio VHF (Very High Frequency) afin d'éviter des déplacements et des frais de mobilités. Dans la mise en place cette connexion j'ai dû étudier l'infrastructure réseaux de l'entreprise afin de mieux comprendre les paramètres à utiliser. Dans mon cas deux paramètres rentrent en compte : le premier étant que la connexion à internet au sein de l'entreprise est assurée via une box internet SFR, le deuxième étant que la connexion internet sur le navire se fait via un satellite et l'allocation d'adresses IP se fait dynamiquement.

Après une analyse du réseau on obtient la topologie suivante (figure 3) :

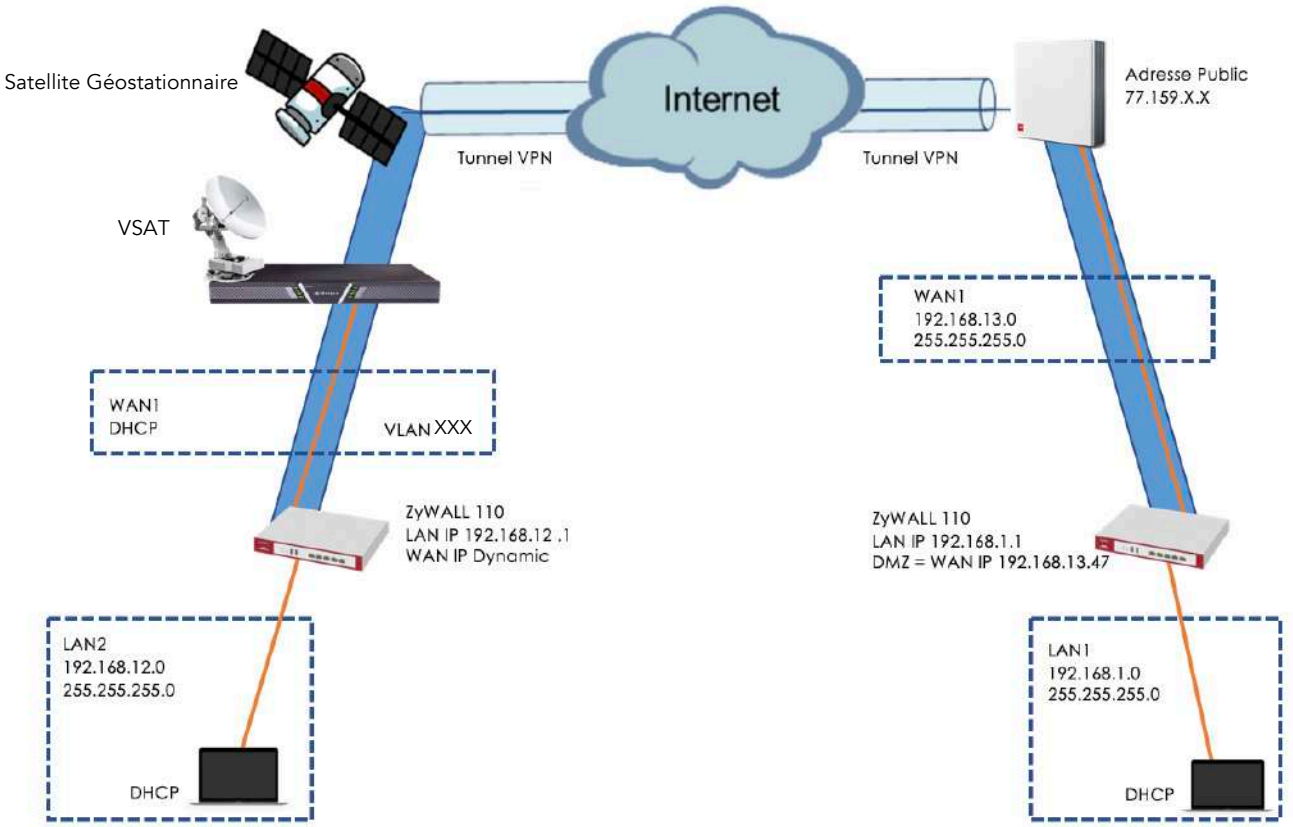

Figure 3 : Topologie réseaux

La figure ci-dessus représente donc la structure développée du réseau sur lequel nous allons travailler. Cependant, j'ai pu la simplifier afin de pouvoir garder les éléments essentiels à la configuration du VPN.

On obtient donc une structure simplifiée (figure 4) :

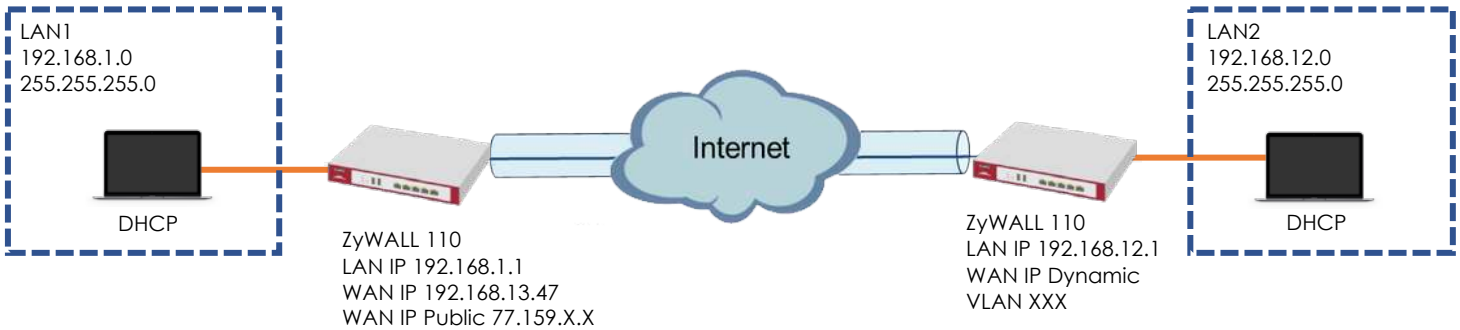

Figure 4 : Topologie simplifiée

3.1.2 Les équipements

Dans cette partie nous allons voir les principaux équipements utilisés qui m'ont permis de configurer le VPN et de communiquer.

ZyXEL ZyWALL 110 VPN Firewall

Le ZyXEL est un routeur-firewall permettant ainsi de fixer des règles de sécurité tout en assurant le routage vers internet. L'interface du ZyXEL reste simple mais complète (figure 5) :

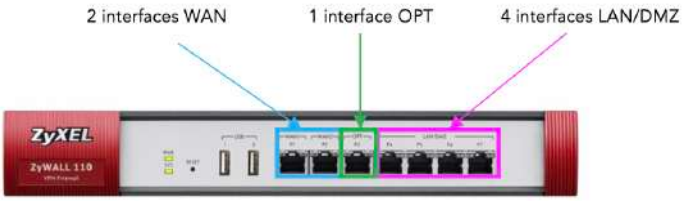

Figure 5 : Face avant firewall

WAN : Wide Area Network – Permet de se connecter à internet ou à des sites distants. L'adresse IP sur les WAN est une adresse IP publique.

LAN : Local Area Network – Réseau local où les utilisateurs d'une même zone restreinte sont connectés. L'adresse IP est privée.

OPT : Ce port désigne un port optionnel, il est très flexible et peut-être configuré comme un port LAN, WAN, DMZ.

Models	 ZyWALL 110	ZyWALL 310	ZyWALL 1100
Hardware Specifications			
Interfaces	4 x LAN/DMZ, 2 x WAN, 1 x OPT	8 (configurable)	8 (configurable)
USB ports	2	2	2
Console port	Yes (DB9)	Yes (DB9)	Yes (DB9)
Rack-mountable	Yes	Yes	Yes
Key Features			
VPN	IKEv2, IPSec, SSL, L2TP/IPSec	IKEv2, IPSec, SSL, L2TP/IPSec	IKEv2, IPSec, SSL, L2TP/IPSec
SSL (HTTPS) inspection	Yes	Yes	Yes
Hotspot Management*7	Yes	Yes	Yes
Ticket printer support*10 / Support Q'ty (max.)	Yes (SP350E) / 10	Yes (SP350E) / 10	Yes (SP350E) / 10
Amazon VPC	Yes	Yes	Yes
Facebook Wi-Fi	Yes	Yes	Yes
Device HA Pro	Yes*6	Yes*6	Yes, Activate once registered
Link Aggregation (LAG)	-	Yes	Yes

Figure 6 : Caractéristique techniques ZyXEL

D'après la fiche technique (figure 6) des différents modèles proposés par ZyXEL, les différences majeures se trouvent au niveau des interfaces qui peuvent être configurables ou non et au niveau de l'agrégation de lien qui lui n'est pas présent sur le modèle utilisé.

Les paramètres qui nous intéressent le plus ici sont les protocoles VPN disponibles. Pour les trois modèles les protocoles VPN disponibles sont identiques et nous verrons plus tard lequel nous allons utiliser.

Satellite

Dans le cadre du projet le satellite utilisé est un satellite géostationnaire. Il existe deux types de satellite : le satellite géostationnaire mais aussi le satellite à défilement. Nous allons voir leurs caractéristiques générales mais aussi leurs principales utilisations.

Le **satellite géostationnaire** se trouve sur une orbite géostationnaire. Ce satellite se déplace de façon synchrone avec la planète en restant constamment au-dessus du même point de la surface. Ce satellite se situe à une distance d'environ 36 000 km d'altitude avec comme période de révolution la même que celle de la Terre. De par son altitude élevée ce satellite couvre environ un tiers de la planète ; il ne suffit donc que de trois satellites afin d'assurer une couverture complète. Ce type de satellite est utilisé dans les télécommunications, télédiffusion mais aussi pour l'observation. Etant principalement utilisé pour des télécommunications, le principal défaut de ce type de satellite est la résolution qui est faible dûe à la distance et le temps de transmission qui lui est nettement plus perceptible (0,2 secondes environ) entre la Terre et le satellite.

Le **satellite à défilement** connu plus souvent sous le nom de satellite météorologique est lui sur une orbite polaire ce qui signifie qu'il est héliosynchrone (axe de rotation perpendiculaire à celui de la Terre). Il se situe à une altitude d'environ 800 km permettant d'avoir une plus grande résolution que les satellites géostationnaires qui sont eux beaucoup plus éloignés. C'est le seul type des deux types de satellite à obtenir des images polaires. De plus, son synchronisme avec le soleil lui permet d'être totalement autonome, mais aussi d'obtenir des images dans les mêmes conditions d'éclairage pour les surfaces observées.

VSAT

Maintenant que nous savons qu'il existe deux types de satellite nous allons voir comment j'ai pu m'y connecter. La connexion Terre-satellite se fait via des antennes, on sait qu'il existe plusieurs types d'antennes cependant celles-ci sont bien particulières. En effet sachant que le satellite géostationnaire (celui qui est utilisé dans le cadre de mon projet) semble depuis la Terre être immobile, cependant il ne faut pas oublier que cette installation sera faite à bord d'un navire qui lui est en mouvement. L'antenne utilisée est donc une antenne VSAT (Very Small Aperture Terminal) motorisée (figure 7), ce type d'antenne permet de s'orienter automatiquement afin de toujours être aligné avec le satellite. Comme son nom l'indique son ouverture est très petite (1°) ce qui avec la distance séparant le navire du satellite peut engendrer une perte de connexion causée par un désalignement de l'antenne avec le satellite.

Figure 7 : Antenne VSAT & contrôleur

iDirect

Dans le cadre du projet l'iDirect (figure 8) permet le routage des données reçus par le satellite. L'iDirect peut donc être comparé à un routeur. Il faut savoir qu'afin d'obtenir une connexion internet via satellite l'iDirect ne suffit pas, il faut en plus un contrôleur permettant de gérer l'orientation du VSAT, Very Small Aperture Terminal, afin d'être aligné avec le satellite et récupérer les informations. *Voir annexe 8 : Caractéristiques techniques*

Figure 8 : iDirect X7 Routeur Satellite

Radio VHF

La radio VHF, Very High Frequency (figure 9) fonctionne sur la bande de fréquence maritime 156-163 Mhz. Ce type de radio est obligatoire sur les navires à partir de la zone semi-hauturière se situant entre 6 et 60 milles qui correspondent respectivement à 9,66 et 96,56 km d'un abri. Elle est utilisée pour communiquer avec les abris côtiers mais aussi les navires à proximité ; de plus cette radio permet d'envoyer ou recevoir un appel de détresse en ASN (Appel Selectif Numérique). Les messages audios utilisent le canal 16 de la bande marine VHF, qui est le canal reservé à cet effet. Sa portée est inférieure à 60 km. Chaque radio VHF est équipée d'une fonction ASNpermettant de produire automatiquement des alertes de détresse en format numérique. Le MMSI (Maritime Mobile Service Identity) est une série de neuf chiffres transmis par ondes électromagnétiques afin d'identifier de manière unique les stations radioélectriques. Celui-ci facilite l'identification du navire et du propriétaire en la rendant plus sûre et rapide. Il est de la forme suivante MID XXX XXX avec le MID (Maritime Identification Digits) étant composé de trois chiffres et permettant d'identifier le pays d'origine du navire.

Figure 9 : Interface Radio VHF

3.1.3 Protocole VPN

Comme nous avons pu le voir dans la fiche technique du ZyXEL il existe différent protocole VPN afin de crypter les données et d'assurer la sécurité de notre VPN.

J'ai dû étudier deux protocoles VPN afin de déterminer lequel serait le plus adapté à notre contexte : SSL/TLS et IPsec.

SSL/TLS : Secure **S**ocket **L**ayer / **T**ransport **L**ayer **S**ecurity

Ce protocole permet d'assurer la sécurité de la couche transport dans le modèle OSI. TLS est l'évolution de SSL. Cependant ce protocole reste encore beaucoup utilisé d'où le nom SSL/TLS.

Ce protocole fonctionne sur un modèle **client-serveur** assurant :

- L'**authentification** service permettant d'assurer qu'une donnée provient bien de l'origine de laquelle elle est censée provenir du serveur
- Le **chiffrement** service consistant à rendre impossible l'interprétation de données si on n'en est pas le destinataire.
- L'**intégrité** service qui consiste à s'assurer qu'une donnée n'a pas été altérée accidentellement ou frauduleusement.

Ce protocole est majoritairement utilisé pour des transactions ou des échanges de données confidentielles sur des sites web. Son point fort est une mise en place relativement facile par le fait que les protocoles de couches applications (ex : http) n'ont pas à être profondément modifiés pour utiliser une connexion sécurisée (ce qui a donné https).

IPsec : Internet **P**rotocol **S**ecurity

Il assure les mêmes services que ceux proposés par SSL/TLS avec deux services supplémentaires :

- **Protection contre le rejeu** : service qui permet d'empêcher les attaques consistant à envoyer de nouveau un paquet valide intercepté précédemment sur le réseau pour obtenir la même autorisation que ce paquet à entrer dans le réseau. Ce service est assuré par la présence d'un numéro de séquence.
- **Gestion des clés** : mécanisme de négociation de la longueur des clés de chiffrement entre deux éléments IPSEC et d'échange de ces clés.

Ce protocole est défini comme un standard pour assurer des communications privées et protégées sur des réseaux IP. La particularité de ce protocole est qu'il n'est pas limité à une seule méthode d'authentification ou d'algorithme. Nous allons maintenant voir les différents mécanismes de sécurité :

AH : Authentification **H**eader
Le protocole AH assure l'intégrité des données en mode non connecté et l'authentification de l'origine des datagrammes IP sans chiffrement des données. Son principe est d'ajouter un bloc au datagramme IP. Une partie de ce bloc servira à l'authentification, tandis qu'une autre partie, contenant un numéro de séquence, assurera la protection contre le rejeu.

ESP : Encapsulation **S**ecurity **P**ayload
Le protocole ESP assure, en plus des fonctions réalisées par AH, la confidentialité des données et la protection partielle contre l'analyse du trafic, dans le cas du mode tunnel. C'est pour ces raisons que ce protocole est le plus largement employé.

Les modes de fonctionnement :

Dans le mode transport (figure 10), IPsec ne se situe pas sur la couche réseau du modèle OSI mais bien évidemment sur la couche transport ; ce sont uniquement les données transférées (la partie payload du paquet IP) qui sont chiffrées et/ou authentifiées. Le reste du paquet IP est inchangé et de ce fait le routage des paquets n'est pas modifié. Néanmoins, les adresses IP ne pouvant pas être modifiées par le NAT sans corrompre le hash de l'en-tête AH généré par IPsec, AH ne peut pas être utilisé dans un environnement nécessitant ces modifications d'en-tête. En revanche, il est possible d'avoir recours à l'encapsulation NAT-T pour encapsuler IPSec ESP. Le mode transport est utilisé pour les communications dites hôte à hôte (Host-to-Host).

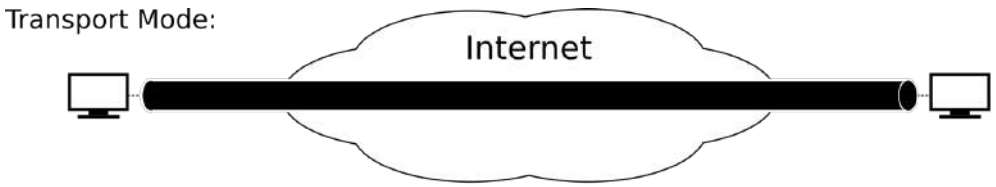

Figure 10 : Mode transport

En mode tunnel (figure 11), c'est la totalité du paquet IP qui est chiffré et/ou authentifié. Le paquet est ensuite encapsulé dans un nouveau paquet IP avec un nouvel en-tête IP. Au contraire du mode transport, ce mode supporte donc bien la traversée de NAT quand le protocole ESP est utilisé. Le mode tunnel est utilisé pour créer des réseaux privés virtuels (VPN) permettant la communication de réseau à réseau (c.à.d. entre deux sites distants), d'hôte à réseau (accès à distance d'un utilisateur) ou bien d'hôte à hôte (messagerie privée).

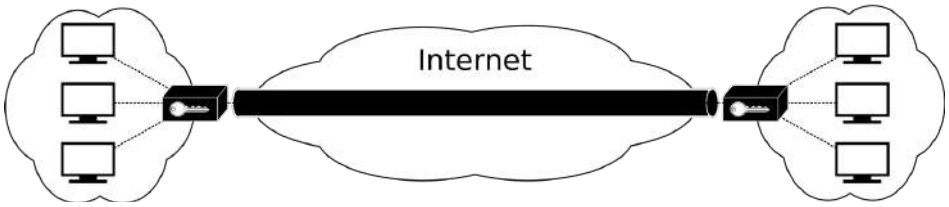

Figure 11 : Mode tunnel

3.1.4 Configuration

Une fois les protocoles étudiés, j'ai pu déterminer lequel correspond le mieux à mon projet. Pour rappel je me situais dans un contexte où depuis un équipement interne je devais pouvoir établir une connexion sécurisée afin de paramétrer une radio VHF située sur un navire. Sachant que SSL/TLS est plus adapté pour un modèle client-serveur (ce qui n'est pas mon cas) j'ai pu en déduire que le protocole IPsec serait le plus adapté pour un VPN entre réseaux IP. Nous avons à présent tous les éléments nécessaires à la configuration de notre VPN.

La configuration des deux ZyXEL se fait à travers une interface WEB. Pour avoir accès à cette interface il faut se câbler sur une des interfaces LAN du Firewall. La première connexion se fait avec le login de base (annexe 9).

Une fois le branchement effectué entre l'ordinateur et le port LAN du Firewall il suffit d'entrer l'adresse IP de l'interface LAN à laquelle nous sommes branchés (annexe 10).

Une fois la connexion effectuée on obtient l'interface suivante (figure 12) :

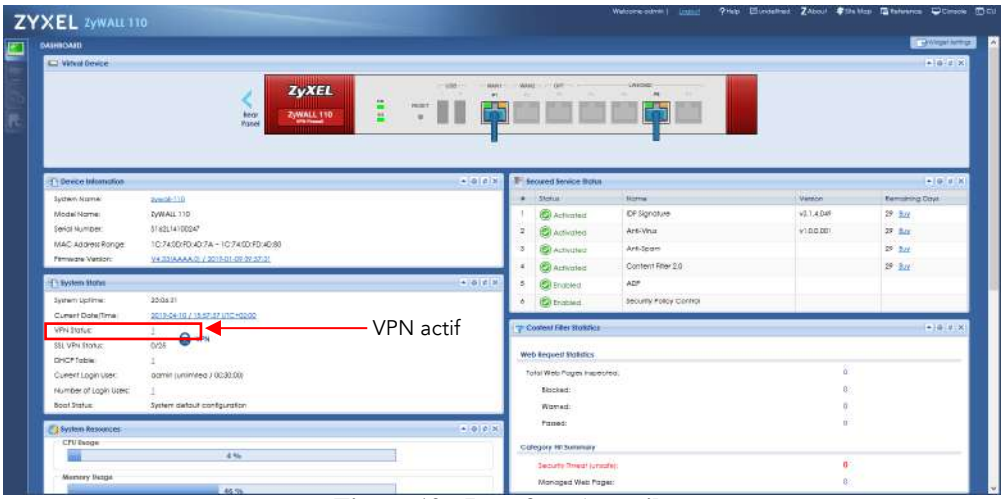

Figure 12 : Interface Accueil

Sur cette interface on obtient de multiples informations généralistes sur la configuration de notre équipement. L'information qui nous intéresse principalement est celle du VPN statuts. En effet elle me permettra de voir à la fin de configuration si notre VPN a bien été mis en place.

Statut interfaces :

Sur cette interface (figure 13) nous retrouverons toutes les informations concernant la configuration de nos interfaces (@IP, masque, active/inactive, attribution d'interface aux LAN…)

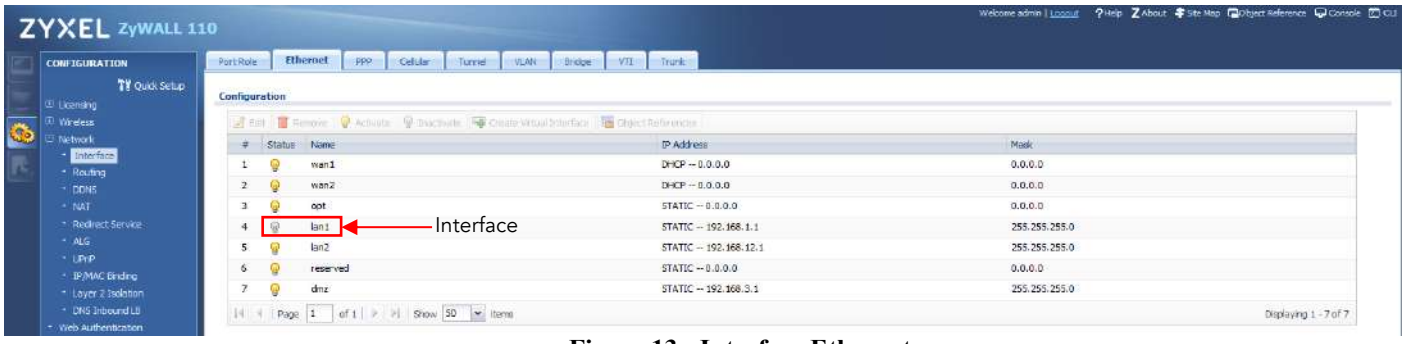

Figure 13 : Interface Ethernet

Afin de mieux mettre en évidence la connexion VPN entre les deux réseaux j'ai décidé de désactiver le LAN 1 sur le Firewall car chaque ZyXEL a la même configuration de base donc le même plan d'adressage pour chaque LAN ce qui ne correspond pas au but premier d'un VPN qui est la mise en place d'une liaison sécurisée entre des réseaux différents n'ayant donc pas le même plan d'adressage.

Figure 14 : Rôle des ports

Sur cette interface (figure 14) il est possible de configurer les ports et plus précisément qu'elle sera l'adresse ainsi que la fonctionnalité de l'interface. En effet une interface n'a pas la même fonctionnalité s'il agit d'une DMZ, LAN, WAN.
Il est recommandé de ne pas changer le rôle d'une interface si l'on est directement branché dessus pour la configuration.

Vlan :

C'est sur cette interface (figure 15) qu'il est possible de configurer des vlan.

Figure 15 : Création Vlan

Dans le contexte de mon projet un vlan a été mis en place comme nous avons pu le voir plus haut. Il a donc fallu que je configure ce vlan (figure 16) seulement sur le Firewall du navire qui sera directement relié à l'iDirect.

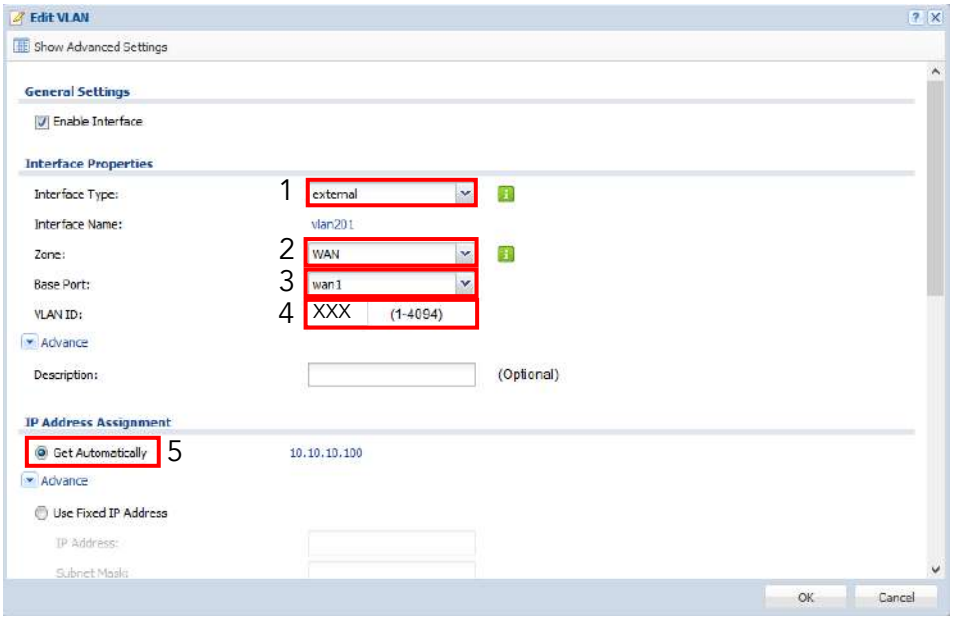

Figure 16 : Configuration Vlan navire

La configuration ci-dessus est celle du navire. En effet comme nous avons pu le voir afin d'avoir une connexion interne le Firewall doit se connecter au Vlan XXX pour avoir l'accès à l'iDirect.

Nous allons à présent l'étudier :

Il y a deux options possibles **« 1 »**, internal et external. Sachant que nous sommes dans la configuration du firewall du navire et que nous voulons accéder à internet via un vlan nous passerons donc par une interface externe. L'interface étant externe la zone sera donc WAN **« 2 »** et plus précisément l'interface wan1 **« 3 »** que nous avons reliée à l'iDirect. Il ne manque donc plus qu'à configurer le numéro du vlan qui doit correspondre à celui de l'iDirect **« 4 »** ainsi que l'adresse IP attribuée via un DHCP **« 5 »**.

Une fois la configuration terminée le vlan créé doit automatiquement récupérer une adresse IP. Une fois cette étape terminée il ne manque plus qu'à configurer le VPN.

VPN :

La configuration du VPN doit se faire en deux étapes :

VPN Gateway : c'est là où j'ai configuré l'interface du VPN ainsi que la route par défaut.
VPN Connexion : c'est là où j'ai défini le type de scénario (site-to-site, site-to-site with Dynamic Peer) et établi la connexion entre les deux Firewall.

C'est deux étapes sont plus communément appelées phase 1 et phase 2. La phase 1 vise à établir un canal sécurisé entre les deux équipements (firewall) avant de pouvoir échanger des paquets IPsec. La phase 2 permet l'échange de paramètres via le canal sécurisé (phase 1) afin de se mettre en accord sur les paramètres IPsec tel que l'authentification, le crypgtage et le type d'échange de clé. Nous verrons ci-dessous la configuration du VPN que j'ai effectuée sur les deux Firewall (figure 17 à 21).

VPN Gateway :

Attention : Il est très important que les paramètres d'authentification, de cryptage ainsi que les clés de chiffrement correspondent entre les deux VPN.

Firewall Terrestre Firewall Navire

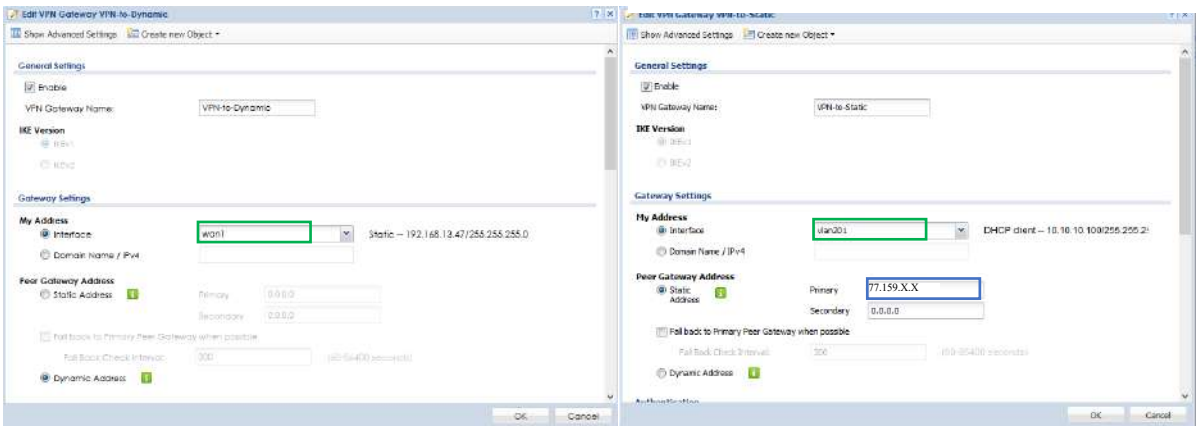

Figure 17 : VPN Gateway 1

Il faut choisir les interfaces connectant les deux bouts de notre VPN. De plus pour le firewall connecté au satellite il est important de configurer l'adresse IP public à atteindre du firewall de la société.

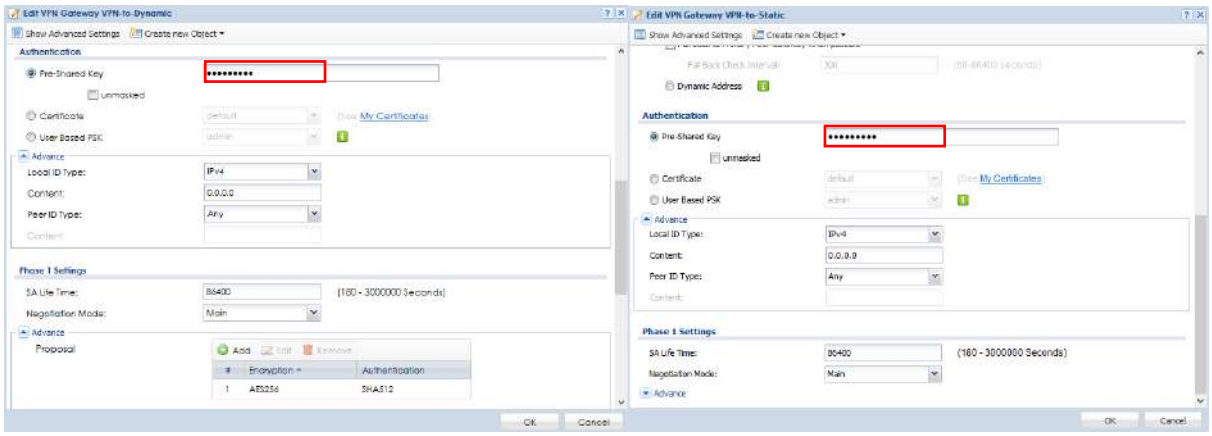

Figure 18 : VPN Gateway 2

Il est impératif de mettre la même clé partagée afin que les deux firewalls puissent établir une liaison.

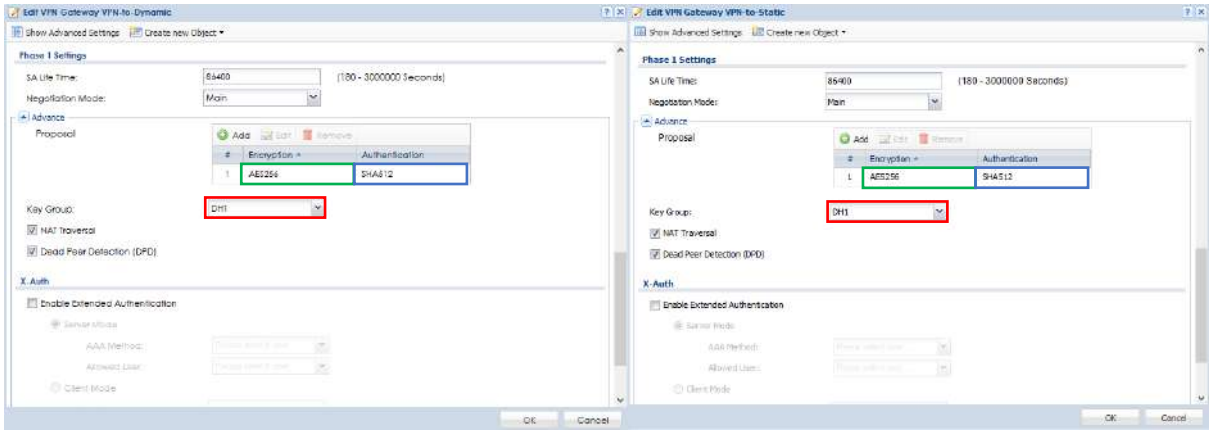

Figure 19 : VPN Gateway 3

DH1 : Algorithme Diffie-Hellman, c'est l'algorithme le plus utilisé dans l'échange de clé privée. Cet algorithme assure la confidentialité persistante (PFS, Perfect Forward Secrecy), cela veut dire que même si la clé privée est interceptée il reste des valeurs inconnues afin de pouvoir déchiffrer les messages. Cependant cet algorithme a ses limites, en effet il n'est pas possible de savoir au début de l'échange de clé si nous communiquons avec la bonne personne. L'algorithme est donc sensible à l'attaque dite « Man in the middle ». Le schéma illustrant cet algorithme se trouve en annexe 11.

AES-256 bits : Advanced Encryption Standard est un standard dans le chiffrement de données.

SHA-512 bits : Secure Hash Algorithm est une fonction de l'algorithme de cryptographie SHA-2 évolution de SHA-1. Cet algorithme se base sur des fonctions de hachage visant à transformer une valeur d'entrée aléatoire en une valeur fixe. Il faut savoir que cela marche à sens unique ; il n'est pas possible d'obtenir la valeur d'entrée à partir de la valeur fixe.

VPN Connexion :

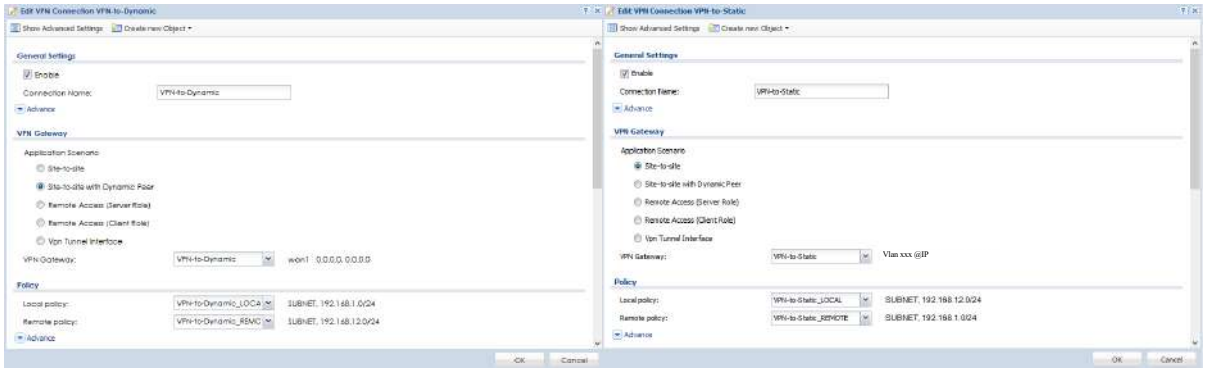

Figure 20 : VPN Connexion 1

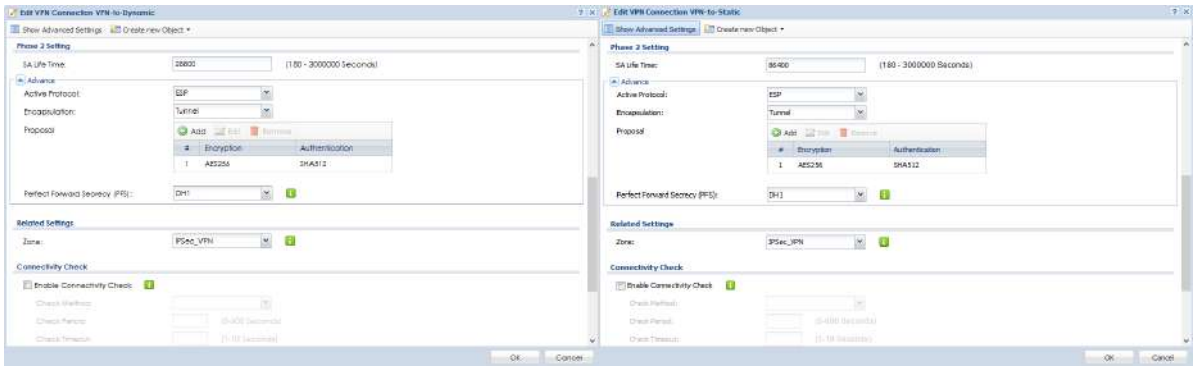

Figure 21 : VPN Connexion 2

Vérifications

La vérification de la connexion du VPN se fait via l'interface monitor IPsec (figure 22) qui affiche toutes les informations sur l'état de notre connexion VPN.

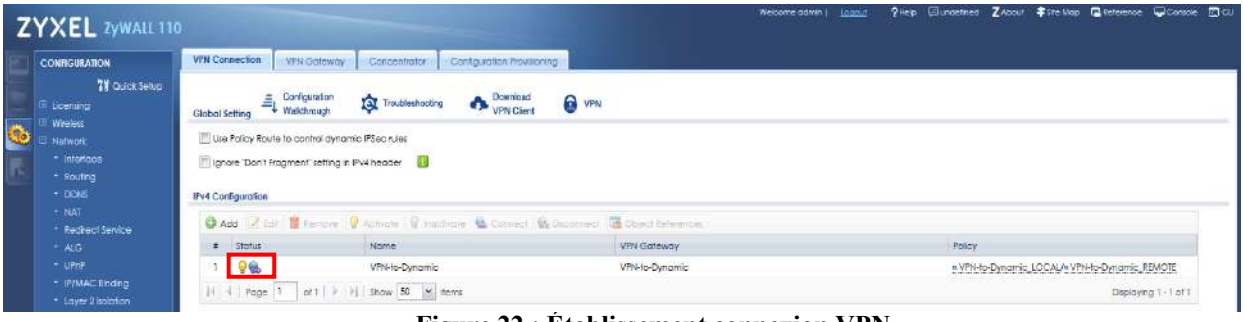

Figure 22 : Établissement connexion VPN

De plus la meilleure solution pour vérifier la connexion VPN reste de la tester soi-même en essayant de se connecter à l'interface LAN de l'autre Firewall à l'aide de son adresse IP. Une fois la connexion VPN établie la connexion est sécurisée, il ne manque plus qu'à configurer la radio VHF à distance.

3.1.5 Configuration VHF

Le service projet/affaire a développé un logiciel ProjectVHF (figure 23) permettant de contrôler différents paramètres d'une radio VHF une fois connecté à celle-ci. Les paramètres restent assez limités pour éviter tout problème de sécurité lié à une connexion malveillante. Dans le cas de mon projet le but premier est le changement de MMSI permettant un gain de temps et d'argent important.

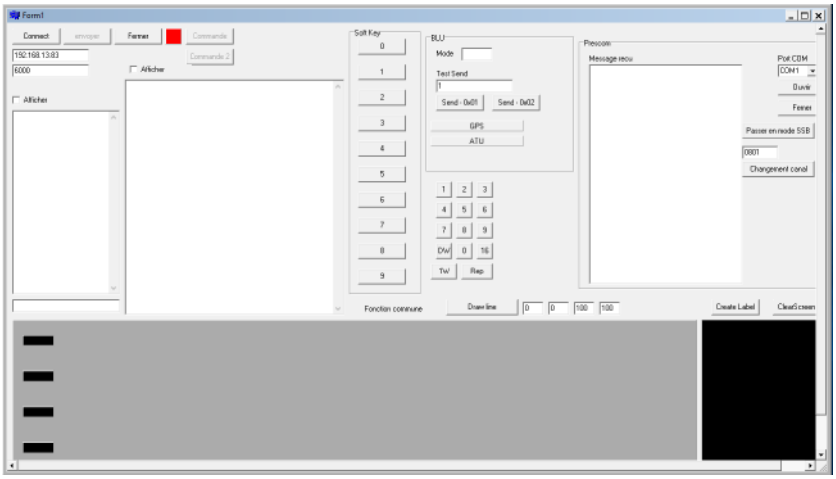

Figure 23 : Application ProjectVHF

L'interface permet d'émuler les différents boutons présents physiquement sur la radio VHF afin de pouvoir tester les ASN mais aussi paramétrer l'adresse IP ainsi que les journaux d'évènement. Ceci permettant d'analyser à distance l'origine du problème s'il est identifiable et de pouvoir corriger ce problème très rapidement.

3.2 Projet Wifi

3.2.1 Cahier des charges

Dans le cadre du projet de renouvellement de l'infrastructure du réseau Themys, il a été décidé de mettre en place un accès wifi afin d'obtenir une infrastructure complète autant pour les utilisateurs internes que les intervenants externes.

Les différentes contraintes sont les suivantes :

- Couverture wifi dans tout le bâtiment.
- Mise en place de deux réseaux wifi dans des vlan différents : un pour les employés et l'autre pour les intervenants externes sur une courte durée (stagiaires, rendez-vous professionnels).
- De plus il faut que les utilisateurs puissent se connecter simultanément aux bornes wifi afin d'avoir un temps d'attente réduit et un meilleur débit.
- La borne wifi doit-être discrète.

Afin de mieux comprendre nos choix lors de cette installation wifi nous allons voir les équipements choisis, leurs caractéristiques ainsi que leurs configurations.

3.2.2 Unifi Ubiquiti

Pour l'installation wifi, mon tuteur de stage a fait le choix d'utiliser des bornes wifi Unifi nanoHD de Ubiquiti (annexe 12).

L'Unifi nanoHD est une borne wifi créée par Ubiquiti Networks, société qui connaît une croissance importante depuis ces dernières années. Ubiquiti vend aussi de nombreux équipements réseaux tels que

des amplificateurs, des switches, des routeurs mais aussi des téléphones et caméras IP. En effet cette entreprise veut fournir les meilleures performances pour des prix attractifs (annexe 13).

Après une étude des besoins de l'entreprise, mon tuteur a décidé de nous orienter vers ce type de borne wifi de par son prix attractif sur un marché relativement cher mais aussi de par ses caractéristiques techniques (figure 24) correspondant à nos besoins.

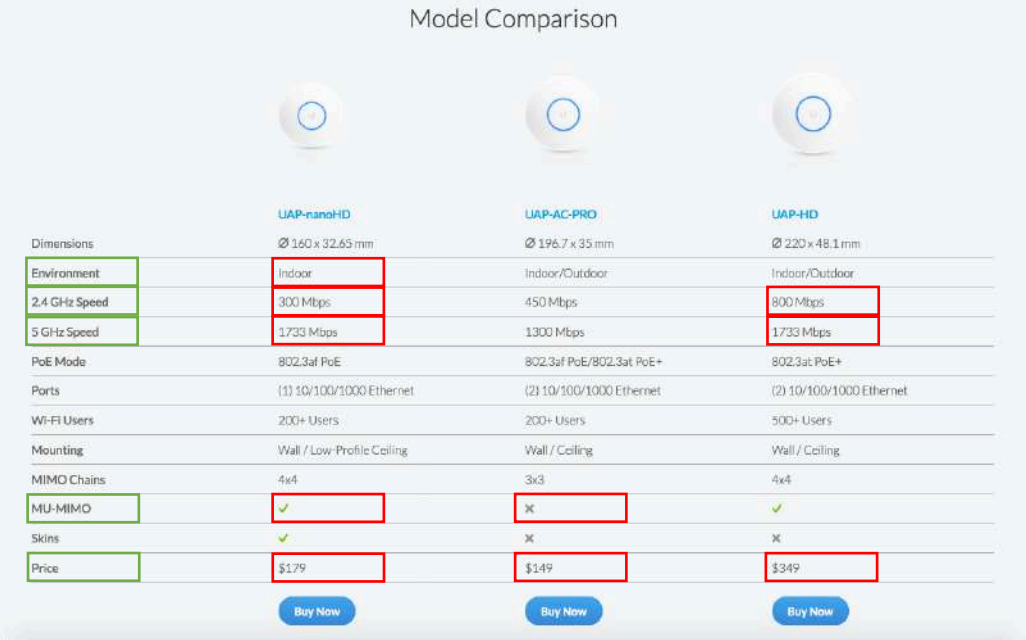

Figure 24 : Comparaison des modèles

Nous ne nous sommes pas orientés vers le produit UAP-AC-PRO malgré son prix légèrement plus bas car l'option MU-MIMO (Multi utilisateurs – Multi Input, Multi Ouput) n'est pas présente et cela ne correspond pas au cahier des charges. De plus, le modèle choisi est adapté à un environnement Indoor proposant le même débit en 5G que le modèle le plus cher.

L'apparence était un critère faisant partie du cahier des charges, et cette solution permettait un montage facile est discret (annexe 14 à 16).

3.2.3 Interface

Dans cette partie, nous allons voir et détailler l'interface afin de pouvoir ensuite étudier la configuration que j'ai effectuée avec l'aide de mon tuteur de stage.

NB : Nous détaillons l'interface pour le logiciel Unifi Controller Linux. En effet le contrôleur de borne wifi est une machine virtuelle et non un contrôleur physique.

Une fois le logiciel téléchargé et lancé nous sommes arrivés sur le menu d'authentification (annexe 17).

Les identifiants sont ceux que nous avons créés au préalable. Une fois la connexion établie l'interface de bienvenue s'affiche mettant en avant les différentes fonctionnalités proposées par la marque.

Une fois le menu de bienvenue terminé nous sommes arrivés sur le tableau de bord. Nous allons voir en détails les paramètres disponibles.

Le tableau de bord (figure 25) est l'endroit permettant d'afficher toutes les informations générales sur notre configuration et l'utilisation wifi.

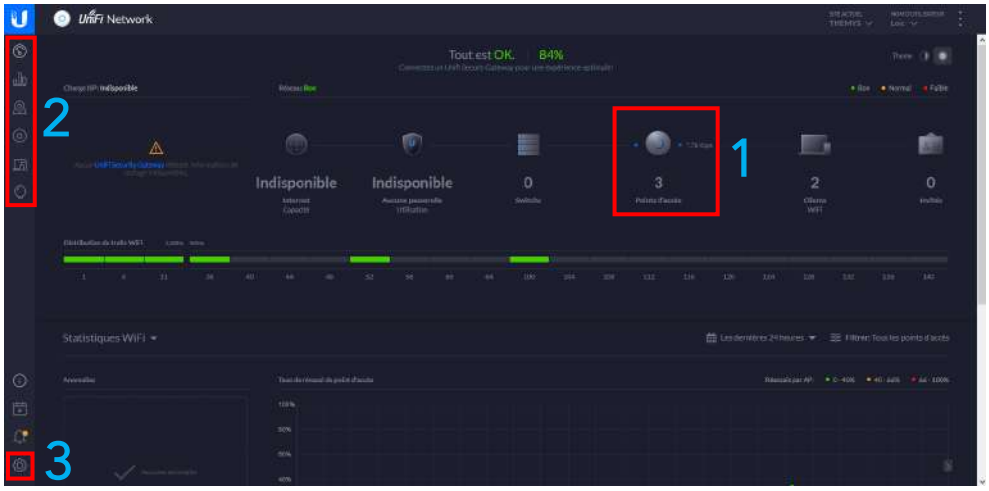

Figure 25 : Tableau de bord

Sur cette interface les paramètres qui nous intéressent le plus afin de configurer sont les suivants :

1 – Nombres de bornes wifi en marche.
2 – Barre latérale : de nombreux paramètres sur l'état de notre configuration sont disponibles.
3 – Paramètres : c'est là où l'on va configurer les paramètres réseaux.

Nous allons à présent étudier de plus près les paramètres disponibles sur la barre latérale.

Cette barre permet plus précisément la maintenance de notre réseau, de nos bornes ainsi que des clients connectés.

Statistiques : Dans ce menu (annexe 18) seront listés le nombre de clients connectés ainsi que le nombre total des données utilisées par chaque borne.

Carte : Ce menu (annexe 19) permet d'obtenir le plan de l'entreprise avec le placement de nos bornes wifi ainsi que les recouvrements et les rayons d'émissions. Dans notre cas nous n'avons pas encore configuré cette partie.

Equipements : Liste les équipements (bornes wifi, routeurs, switches, etc…) ainsi que leurs paramètres (annexe 20).

Clients : Liste les clients (annexe 21), la qualité de leur connexion mais aussi leurs activités (données utilisées).

Aperçu : Les bornes wifi nanoHD sont capables de détecter les réseaux wifi à proximité. Tous ces réseaux apparaissent dans le menu « aperçu » (annexe 22).

Evenements : Liste (annexe 23) toutes les connexions et déconnexions aux réseaux wifi à une date et heure précise ainsi que l'ID de l'objet connecté.

Durant l'étude de l'interface et des paramètres de configuration disponibles pour les bornes, nous avons remarqué un problème. Ces bornes ne fournissent pas de journaux d'événement précis sur le trafic mais seulement sur les connexions. Il faut donc passer par un service tiers ou si le trafic de notre borne passe par le routeur-firewall de l'entreprise, nous pouvons identifier le trafic émis depuis la borne en direction d'internet afin d'être conforme à la LCEN de 2004.

3.2.4 Configuration

Tout au long de cette partie, nous allons voir la configuration des trois bornes wifi. Après une étude rapide du bâtiment fait au préalable par mon tuteur de stage, trois c'est le nombre qu'il faut afin d'assurer un accès wifi à l'ensemble du bâtiment sur les deux étages. Nous les nommerons :

- Etage Réunion
- Etage Technique
- RDC accueil

Il existe plusieurs moyens de configurer ces bornes wifi. En effet, vous pouvez télécharger le logiciel Unifi Controller pour ordinateur ou l'application pour mobile. Il faut savoir que ces deux méthodes ne fournissent pas les mêmes fonctionnalités :

- Ordinateur : toutes les options de configuration sont disponibles
- Mobile : seulement les options de bases sont disponibles

Une fois sur le menu de configuration depuis un ordinateur il est possible de configurer une adresse IP permettant d'accéder au menu de configuration depuis un navigateur web.

Environnement radio

Dans le cas de nos bornes wifi il y a deux environnements radio disponibles en même temps, la 2GHz et 5GHz. J'ai dû étudier dans un premier temps les deux environnements (figure 26) :

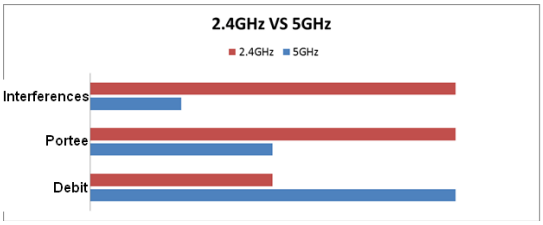

Figure 26 : 2.4GHz VS 5GHz

La première remarque est que l'environnement 2GHz correspond plus précisément à 2.4GHz. Là où un environnement 5G assure une stabilité avec un débit maximum à courte portée la 2G, elle fait face à des interférences beaucoup plus importantes dûes aux nombreux équipements utilisant cette même fréquence mais couvrant de plus grandes distances.

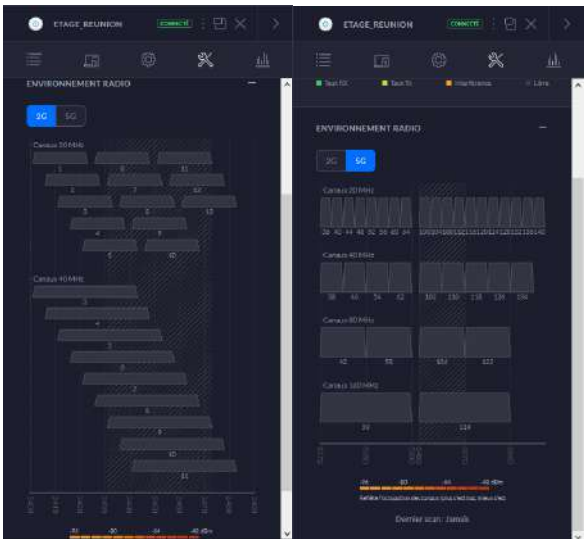

Figure 27 : Environnement 2G/5G

Sur cette interface (figure 27) nous pouvons voir les différentes canaux disponibles ou utilisés ainsi que leur occupation pour chaque environnement radio en dBm.

Avant de configurer l'environnement radio de nos bornes wifi il nous a fallu étudier les réseaux wifi environnants afin de choisir la meilleure configuration.

Pour cela j'ai décidé d'utiliser l'application Wifi Scanner disponible sur macOS. Voici un aperçu (figure 28) :

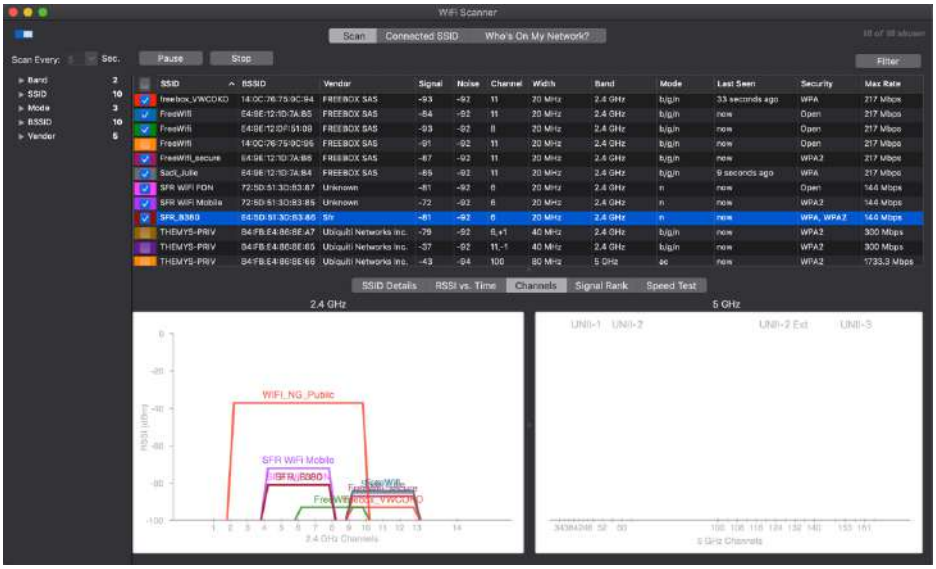

Figure 28 : Wifi Scanner

Cette application permet de lister toutes les informations concernant les réseaux wifi alentour telles que la qualité, la puissance du signal RSSI (Received Signal Strength Indication), etc…

Configuration radio

Après avoir étudié le réseau et sachant qu'en 2.4GHz les canaux 1/6/11 ne se recouvrent pas, nous avons fait le choix d'attribuer à chaque borne un canal différent avec une largeur de bande de 40MHz. Il faut savoir que plus la largeur de bande allouée est grande plus le nombre de canaux diminue. Pour le 5GHz comme aucun réseau à proximité n'utilise cette fréquence nous avions le choix entre 19 canaux. Nous avons donc fait le choix de prendre comme largeur de bande 80MHz avec comme canaux pour les bornes 36/52/100 (figure 29).

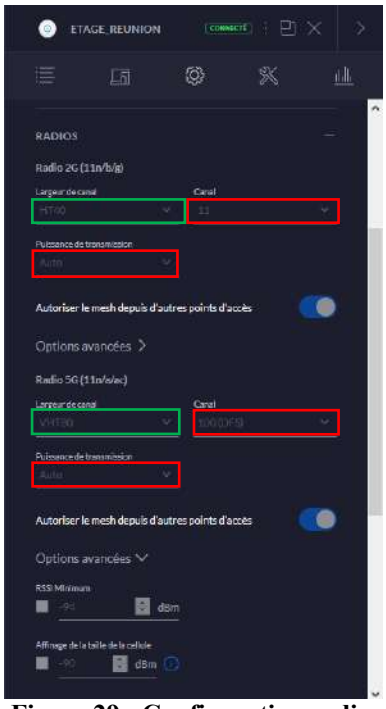

Figure 29 : Configuration radio

Une fois la configuration terminée j'ai relancé le scan et j'ai obtenu (figure 30) :

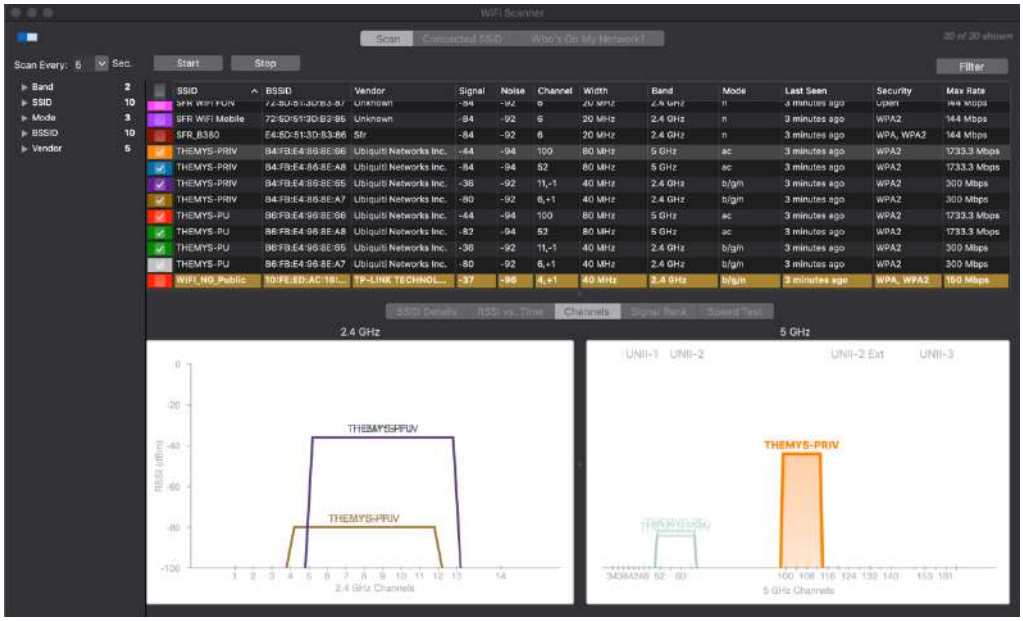

Figure 30 : Scanner Themys

Configuration réseaux

Une fois l'environnement des bornes wifi configuré j'ai configuré le site (annexe 24), le réseau ainsi que la gestion des invités.

Dans le menu « Réseaux sans-fil » (figure 31) nous pouvons créer de nombreux réseaux wifi ainsi que gérer la sécurité et la planification :

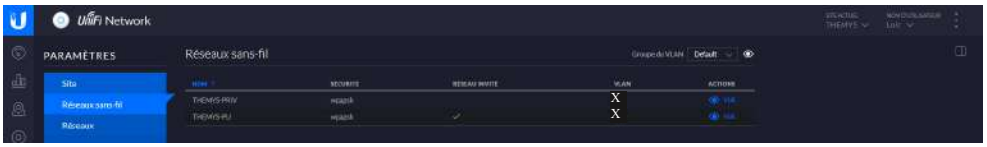

Figure 31 : Création réseaux wifi

Pour ce qui est de la sécurité nous avons mis en place deux vlan. Un pour le wifi public accessible par les intervenants externes et un pour les employés.
Afin de renforcer la sécurité il faut aussi choisir le WPA ainsi que le cryptage. Nous avons choisi WPA2 (Wi-fi Protected Access 2) ainsi que AES (Authentification Encryption Standard) des valeurs sûres dans le domaine de la protection.

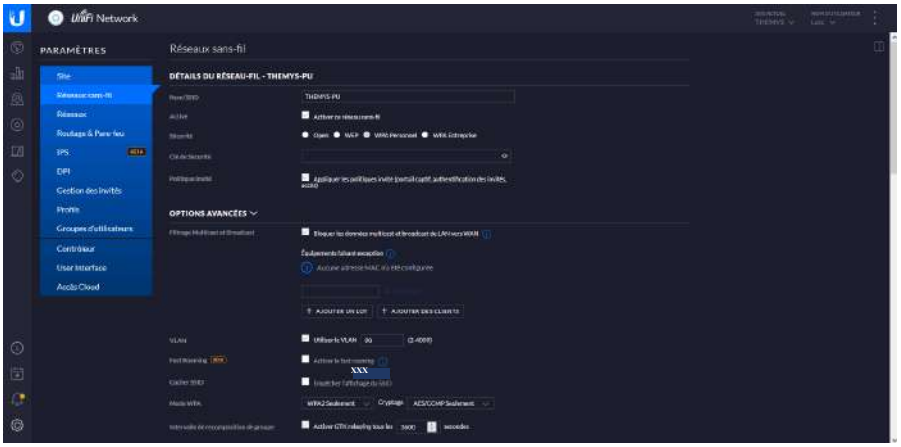

Figure 32 : Vlan et sécurité

Nous voulions activer les bornes wifi seulement lors des heures de travail c'est pour cela que la planification des bornes wifi fut un paramètre très utile (annexe 25).

Gestion des invités

Une fois la configuration globale des bornes wifi effectuée il ne nous restait plus qu'à mettre en place la gestion des invités sur le réseau public : THEMYS-PU.
En effet comme ce réseau est accessible aux intervenants externes il est donc nécessaire de mettre en place une gestion des accès sur des durées définies avec des certains contrôles.

Nous avons donc mis en place une authentification sur un portail captif configurable (figure 33) :

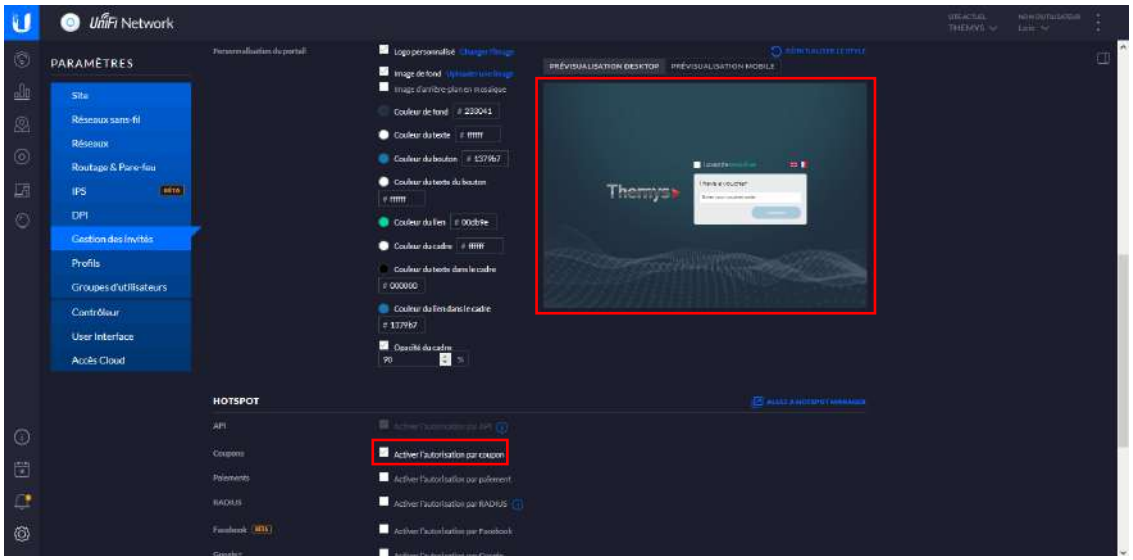

Figure 33 : Portail Captif

De plus, de nombreux paramètres sont disponibles afin d'assurer une meilleure gestion de ses invités. En effet la solution que nous avons décidé de mettre en place est celle d'authentification par coupon avec une durée d'utilisation variable en fonction de la durée de la présence de l'intervenant (figure 34).

Figure 34 : Authentification

La configuration du réseau wifi est donc opérationnelle. Cependant mon tuteur de stage et moi-même n'avons pas eu le temps matériel pour finaliser certains paramètres (facilité d'accès pour les utilisateurs internes, meilleure gestion des autorisations de connexion et d'accès à certains sites) car des missions urgentes nous ont été confiées.

3.3 Nouvelle infrastructure réseaux Themys

3.3.1 Contexte

Suite à l'expiration des garanties sur les équipements de l'infrastructure réseau de l'entreprise Themys un choix a été fait en interne afin d'analyser le besoin et l'opportunité d'un changement d'équipements et une refonte de cette infrastructure. Malgré une probabilité de panne faible de celle-ci, grâce à la redondance des équipements, le choix a été fait de changer l'ensemble des équipements, pour que ceux-ci soient sous contrat de maintenance (garantie étendue), mais également pour bénéficier des dernières évolutions disponibles.

Mon tuteur de stage a donc fait un inventaire des quelques équipements pouvant être conservés. Nous allons porter notre attention sur les nouveaux équipements qui ont été sélectionnés pour la nouvelle infrastructure Themys.

3.3.2 Les nouveaux équipements

Les principaux éléments qui ont été changés sont la baie de stockage, les serveurs, un LTO (Linear Tape Open) ainsi que l'ajout d'un nouvel onduleur. En effet, en plus du remplacement de certains équipements d'autres viennent se rajouter tel qu'un switch Cisco. Nous allons voir les principaux équipements que j'ai pu installer.

NB : Il faut savoir que les serveurs DELL présentés ci-dessous ont été achetés avec des licences Windows Server 2016. De plus la configuration d'une interface iDRAC (integrated Dell Remote Access Control) présente sur chaque équipement nécessite l'achat d'une licence supplémentaire.

1x Baie de stockage DELLEMC (annexe 26)

La différence majeure de cette baie de stockage avec l'ancienne est l'espace de stockage totale passant de 2 To à 9 To avec comme type de support des disques SSD.

2x Serveur PowerEdge R640 (annexe 27)
Ces nouveaux serveurs remplaceront les anciens en assurant une plus grande rapidité d'accès grâce aux nouveaux composants.

1x PowerVault LTO-8 lecteur de bande externe (annexe 28)

La particularité de ce modèle comparé à l'ancien (LTO-6) est sa capacité native de 12 To de stockage qui peut atteindre jusqu'à 30 To en compression contre 2,5 To de capacité native pour le LTO-6.

Ces équipements DELL ont été achetés avec une garantie Prosupport d'une durée de 5 ans assurant une intervention sous 24h. C'est un des critères très importants pour la nouvelle infrastructure.

1x Switch Cisco SG350XG annexe 29

Ce nouveau switch permet l'interconnexion entre les nouveaux serveurs et les anciens équipements déjà mis en place.

3.3.3 Nouvelles solutions logicielles

En plus d'une évolution matérielle il a été fait le choix d'une évolution logicielle. En effet les licences logicielles représentent plus en termes de coût que le matériel. Chaque ordinateur doit avoir une licence unique valable à vie allant des outils de collaborations jusqu'aux outils métiers. Une infrastructure réseau a donc besoin de nombreuses licences afin d'assurer le fonctionnement de chaque outil, de plus on peut constater une réduction de la présence d'équipements physiques au profit de la virtualisation. Maintenant un serveur physique équivaut à de nombreux serveurs virtuels tels que serveur de messagerie, serveur web, serveur de stockage et bien d'autres. Nous allons maintenant voir les choix logiciels qui ont été faits.

VEEAM

Comme nous venons de le voir la virtualisation est en pleine croissance et toute bonne infrastructure réseau doit avoir une solution de backup en cas de problème. Cette solution de sauvegarde était le logiciel ARCserve. Celui-ci permettait d'assurer la sauvegarde des différentes VM (Virtual Machine) allant de la VM entière jusqu'à la restauration de partition précise. Le nouveau logiciel de sauvegarde

choisi est VEEAM. Les critères qui ont amené à choisir VEEAM sont le prix de la licence, un support plus efficace et la possibilité de restaurer un fichier spécifique dans une partition. De plus VEEAM est certifié QoreStor, logiciel de sauvegarde tiers venant compléter VEEAM.

QoreStor

De nos jours les flux de données ne cessent d'augmenter et par conséquent le stockage aussi. Les sauvegardes prennent donc de plus en plus de place et de temps. C'est là que QoreStor présente un intérêt, cette solution vient en complément de VEEAM afin d'améliorer les performances de sauvegarde et réduire considérablement les besoins de stockage. En effet, QoreStor permet la déduplication ; il s'agit, en informatique, d'une technique de stockage de données, consistant à factoriser des séquences de données identiques afin d'économiser l'espace utilisé. La première sauvegarde est effectuée entièrement et représente donc une grande quantité de données, alors que les futures sauvegardes compareront les données afin de ne conserver que les changements permettant un gain de place énorme ainsi qu'une sauvegarde beaucoup plus rapide.

NB : Il faut savoir que QoreStor doit être installé et configuré sur une machine Linux.

Exchange Server 2019

Mise à niveau de Exchange Server 2016 vers 2019 pour les différentes mises à jour assurant :

- **Sécurité**
  - Un déploiement sur une surface réduite (Windows Server Core) réduisant la surface pouvant être attaquée.
  - Possibilité de blocage d'accès externe facilitant la gestion et la complexité des règles d'accès.

- **Performance**
  - Une meilleure indexation et recherche de fichiers assurant une plus grande accessibilité et rapidité.
  - Modification rapide et fiable entre les serveurs.
  - Prend en charge de nouveaux composants matériels modernes

- **Fonctionnalités** facilitant l'utilisation du logiciel pour les différents utilisateurs mais aussi en assurant une meilleure intégrité des plugins.

3.3.4 Mise en place et migration

Afin de pouvoir mettre en place ces nouveaux équipements j'ai participé aux montages des baies ainsi qu'à leurs installations dans la salle informatique. Dans un premier temps, j'ai effectué l'identification ainsi que le marquage des câbles (annexe 30 à 31) afin de pouvoir décâbler et recâbler facilement. Cette partie de la migration a dû se faire durant les horaires où les employés n'étaient pas là car toutes l'infrastructure devait être éteinte.

Voici les deux baies avant le décâblage (figure 35) :

Figure 35 : Ancienne baie

L'objectif principal de la mise en place de nouvelles baies était d'avoir un câblage le plus organisé et accessible possible. Cela nous a pris du temps, en effet afin d'obtenir le résultat souhaité (figure 36) nous avons été obligés de dé-câbler et re-câbler à de multiples reprises. En démontant les différents équipements j'ai pu mieux comprendre leurs connexions et ainsi avoir une vision et une compression plus large de l'architecture réseau mise en place.

Figure 36 : Baie finale

3.3.5 Configuration et future mission

Une fois l'installation matérielle terminée j'ai pu participer à la configuration du switch Cisco SG350XG avec le paramétrage des interfaces IP ainsi que leurs VLAN. De plus, afin d'avoir une infrastructure avec une gestion plus simple, mon tuteur a décidé de reconfigurer totalement le firewall StormShield SN510 (annexe 34 à 35) afin de simplifier les règles de filtrages. J'ai de mon côté mis en place un firewall virtuel StormShield ce qui m'as permis de me familiariser avec VMWare WorkStation comme outil de virtualisation ainsi que l'interface du firewall (annexe 36 à 37) afin d'ajouter l'Active Directory et paramétrer quelques règles de filtrages.

Par manque de temps, je n'ai pu participer qu'à l'installation d'une seule nouvelle baie et à la configuration de deux serveurs DELL. En effet, en rajoutant de nouveaux équipements, une intervention technique afin d'adapter le tableau électrique est nécessaire pour mettre en marche la nouvelle infrastructure. Or, cette intervention est programmée à la suite de mon départ. Estimant que ce projet est une opportunité afin de pouvoir comprendre au mieux les contraintes d'une infrastructure ainsi que son architecture il m'a semblé évident de demander à revenir à la suite de mon DUT afin de

pouvoir terminer cette installation et configuration qui sauront m'apporter de nombreuses connaissances théoriques et techniques.

3.4 Autres missions avec le service projet/affaire

Le service projet/affaire dispose de ressources affectées dédiées aux études pour les projets complexes en phase d'offre et à la réalisation des affaires signées.
Ces ressources sont :

- Personnel technique compétent et spécialisé sur les équipements proposés
- Matériels de tests et de validation des solutions sur plateforme
- Equipements de mesure (banc de test, ordinateurs, logiciels, etc…)

L'informatique étant de plus en plus présente, le responsable du service informatique est également rattaché au service projet/affaire pour les prestations le concernant.

3.4.1 Navire Yersin

Le Yersin est un navire océanographique appartenant à M. François Fiat. Il a vocation a être loué pour des missions scientifiques ou d'explorations sur toutes les mers du globe, y compris les zones polaires. Son installation informatique est importante et complexe et il s'avère que l'équipage ne dispose pas des compétences permettant d'en assurer la maintenance. La société Themys ayant fourni les équipements de communication par satellite (VSAT), il nous a été demandé de prendre en charge cette partie informatique.

Suite à une installation de bornes wifi Cisco faites depuis plusieurs années au sein du navire, le personnel a rencontré de nombreux problèmes de connexion. Moi-même ainsi que mon tuteur de stage avons donc dû faire une intervention afin d'identifier la source du problème ainsi que le corriger. Une fois sur place et après analyse de la configuration des bornes nous avons identifié rapidement la source du problème. Le contrôleur wifi Cisco avait perdu toutes ses licences ainsi que sa configuration. Après une estimation des coûts, il était préférable d'acheter un nouveau contrôleur wifi dernière génération sous licence plutôt que de renouveler les licences expirées sur l'ancien contrôleur. Nous avons donc assuré la remise en marche ainsi que la configuration du nouveau contrôleur Cisco pour la connexion wifi du Yersin.

Vous retrouverez en annexe (section 5) toutes les photos prises au sein du Yersin.

3.4.2 Problème de coupure diffusion TV sur réseau

Des solutions de diffusion IP TV sont déployées sur les navires. Ces solutions de distraction doivent cohabiter avec les systèmes réglementaires marine. Lors de la diffusion d'un message sur les hauts parleurs du navire, la diffusion TV doit s'arrêter pour permettre à l'équipage d'écouter ce message. Le système installé coupe la fibre optique de diffusion en sortie de baie IP-TV. Cela a pour conséquence de faire redémarrer les postes TV avec IP box intégrée. Le temps de redémarrage étant considéré par le client comme trop long il nous a demandé de trouver une solution.
Nous avons réfléchi à une solution qui permettrait d'éviter ce redémarrage du poste TV. En discutant ensemble nous avons compris que la coupure du flux IP était à l'origine de ce comportement. Nous avons donc eu l'idée de séparer les flux audio/vidéo et de contrôle logiciel. L'idée étant de ne couper que le flux audio/vidéo et de conserver le flux de contrôle opérationnel. La solution pressentie était de créer deux VLAN séparés mais transportés sur le même câble réseau. J'ai été chargé de réaliser les tests sur un switch identique à celui utilisé à bord (Switch HP ARUBA) afin de valider la configuration applicable. Les tests ont été satisfaisants et seront présentés prochainement au client.

3.4.3 Etude de projets externes

Configuration Switch Cisco (Naval Group)

J'ai aussi pu participer à différents projets externes. En effet de multiples projets sont en cours concernant une partie de l'infrastructure réseau de différents navires. L'un des plus gros clients de la société (Naval Group) nous a demandé de tester et corriger une configuration sur un switch Cisco 4221 faite au préalable dans le cadre d'un projet militaire. Je ne peux donc pas transmettre la configuration ainsi que les différents documents qui sont classés confidentiels. Ayant eu une formation spécialisée sur les équipements Cisco à l'IUT cela me fut d'une grande aide afin de comprendre la configuration au mieux et encore une fois pouvoir me spécialiser un peu plus dans ce type d'équipement. L'objectif principal était d'autoriser un LAN à communiquer avec le Serveur ainsi que les autres LAN alors que les autres LAN ne sont autorisés qu'à communiquer entre eux sans passer par le serveur.
Lors de ce projet j'ai rencontré un problème au tout début, lors du lancement du switch, il m'était impossible de rentrer dans le mode de configuration globale. Après de longues recherches j'ai trouvé que le problème venait de l'OS installé par défaut sur le switch Cisco. Il m'a donc fallu télécharger un OS approprié à notre configuration et ainsi booter (démarrer) le switch sur une clé USB contenant l'OS afin de l'installer proprement et pouvoir le configurer.

Clonezilla

Le personnel présent sur des navires privés est la plupart du temps non qualifié pour, gérer le réseau du navire les obligeants donc à passer par des intervenants externes tels que Themys assurant la mise en place ainsi que la maintenance des équipements réseaux présents sur leur navire. Cependant certaines tâches telles que des sauvegardes doivent être effectuées régulièrement même en mer ce qui rend donc une intervention impossible. Afin de faciliter et réduire les coûts d'interventions pour le client, j'ai rédigé une documentation sur le logiciel Clonezilla. C'est un logiciel libre de restauration de données qui permet d'effectuer des Ghosts (sauvegarde complète de chaque partition) afin de les restaurer en cas de nécessité. Cette documentation a dû être rédigée dans des délais courts avec un maximum d'informations dans le but d'être compris par un novice.

Etude document CyberSécurité (Naval Group)

Au cours de mon stage j'ai eu la chance de pouvoir étudier brièvement des documents confidentiels sur des matrices de conformités concernant les journaux d'évènements de différents équipements. Il était demandé de faire des tests sur nos équipements internes afin d'établir un fichier répertoriant les différents logs (journaux) pour différents types de requêtes pouvant être parfois très simples comme pour une autorisation d'accès. Ce mini projet m'a permis d'avoir une première approche de la cybersécurité ainsi que des compétences et connaissances à avoir et à développer sans arrêt de par l'évolution constance de l'informatique et de ces équipements.

4 Conclusion

Cette expérience enrichissante fut pour moi une première expérience professionnelle qui m'a permis de découvrir le monde de l'entreprise ainsi qu'un cadre de travail différent. De plus, mon stage s'est déroulé dans un milieu qui ne m'était pas familier, le secteur maritime. En effet, au cours de ces deux ans d'IUT nous avons étudié et développé des compétences dans les réseaux et télécommunications qui m'ont été très utiles dans le cadre de mon stage. Cependant, le secteur maritime avec ses contraintes était pour moi tout nouveau. De plus pouvoir évoluer dans un milieu tel que celui-ci m'a permis de découvrir différents équipements maritimes ainsi que l'importance des réseaux dans les télécommunications. Avoir la chance d'intégrer une petite équipe et ainsi avoir des tâches variées allant de la couche cœur de réseaux à l'accès, jusqu'à la mise en place de l'environnement de production avec la configuration des serveurs, des logiciels nécessaires aux différents corps de métier, mais aussi à la sécurité est une chance qui m'a permis de mieux appréhender les contraintes ainsi que le fonctionnement d'une infrastructure réseau. Les différents projets qui m'ont été confiés m'ont permis de mettre en pratique mes compétences mais aussi de redécouvrir et d'approfondir mes connaissances concernant la sécurisation d'une liaison, la configuration d'un environnement wifi mais surtout sur les différents équipements constituant une infrastructure réseau tout en découvrant le monde des télécommunications maritimes.

5 Remerciements

Je tiens à remercier toutes les personnes qui ont contribué au succès de mon stage et qui m'ont aidé lors de la rédaction de ce rapport.

Je veux tout d'abord adresser mes remerciements à mon tuteur de stage **Christophe CLÉMENT**, responsable sécurité informatique qui est au final bien plus que cela. En effet il s'occupe de tous les aspects ainsi que la configuration de l'infrastructure du réseau au sein de l'entreprise mais aussi dans des projets externes. Il a su partager son expertise, me consacrer du temps et m'a permis de découvrir et d'évoluer dans le milieu maritime mais surtout dans le monde de l'entreprise.

Je remercie également **Cyril PIOT** ainsi que **Nicolas DELACERDA** du service projet/affaire pour leur accueil mais aussi pour l'intérêt porter à mon stage en me faisant découvrir d'autres aspects du réseau et plus précisément les télécommunications.

6 Glossaire

ANFR, Agence Nationale des Fréquences

DMZ, Demilitarized Zone

LAN, Local Area Network

LCEN, Loi pour la Confiance dans l'Économie Numérique

LTO, Linear Tape Open

OS, Operating System

SMDSM, Système Mondiale de Détresse et de Sécurité en Mer

SSD, Solid-State Drive

TV-SAT, Système de réception TV par satellite

UHF, Ultra Haute Fréquence

VHF, Very High Frequency

VLAN, Virtual Local Area Network

VM, Virtual Machine

VPN, Virtual Private Network

VSAT, Very Small Aperture Terminal (équipement de communication par satellite)

WAN, Wide Area Network

7 Sitographie

Themys [en ligne]. Consulté tout au long du stage, disponible sur https://www.themys-sa.com/themys/

Wikipedia [en ligne]. Consulté tout au long du stage, disponible sur https://www.wikipedia.org/

Documentation ZYXEL [en ligne]. Consulté tout au long du projet VPN, disponible sur https://www.zyxel.com/support/KnowledgebaseLandingSR.shtml?c=gb&l=en&md=&s=1

Le VPN [en ligne]. Consulté lors du projet VPN, disponible sur https://www.le-vpn.com/fr/protocoles-le-vpn/

Documentation StormShield [en ligne]. Consulté lors de la migration de l'infrastructure réseau, disponible sur https://www.stormshield.com/fr/documentation/

Radio marine [en ligne]. Consulté lors de l'étude d'équipements maritimes, disponible sur http://seme.cer.free.fr/plaisance/radio-marine.php

Configuration Unifi [en ligne]. Consulté lors de la configuration des bornes wifi Unifi, disponible sur https://help.ubnt.com/hc/en-us/articles/219051528-UniFi-Setting-Up-UniFi-for-Beginners

ANFR [en ligne]. Consulté pour le projet wifi, disponible sur https://www.anfr.fr/international/negociations/grands-dossiers-dactualite/wifi-5ghz/