Institut Universitaire de Technologie,

Aix-Marseille Université

RAPPORT DE STAGE

Diplôme Universitaire de Technologie

Spécialité Réseaux et Télécommunications

Support réseau suite à l'incident de sécurité

Florent ESTRAT

Maison Méditerranéenne des Sciences de L'Homme

Responsable entreprise : Sophie BOUFFIER

Responsable académique : Anouch HOVSEPIAN

2021

Table des matières

1. Introduction

1.1 Présentation de l'entreprise :

L'entreprise qui m'a accueilli durant mon stage s'appelle la Maison Méditerranéenne des Sciences de l'Homme (que j'appellerai la MMSH durant la suite du rapport). C'est une composante d'Aix-Marseille Université appuyée sur une unité mixte de service de recherche du CNRS (USR 3125). Fondée en 1997 par Robert Ilbert elle est membre du Groupement d'Intérêt Scientifique « Réseau national des Maisons des Sciences de l'Homme » (GIS – RnMSH), qui est une infrastructure de recherche en sciences humaines et sociales. Structure de service et d'animation de la recherche, la MMSH regroupe 10 unités mixtes et accueille l'Ecole doctorale 355 « Espaces, Cultures, Sociétés ». Elle accompagne les activités scientifiques de ses unités associées par la mise à disposition d'équipements communs et d'outils mutualisés. Ses ressources documentaires sont rassemblées dans quatre grandes bibliothèques spécialisées.

Ses principales missions sont de :

- Soutenir l'émergence de programmes scientifiques renouvelant objets, terrains et approches dans le domaine des études méditerranéennes ;
- Favoriser les comparatismes et les dynamiques interdisciplinaires ;
- Développer des pôles de compétences techniques et des programmes transversaux ;
- Animer et coordonner des réseaux de recherche internationaux ;
- Construire des plateformes partagées et contribuer au déploiement territorial des Très Grandes Infrastructures de Recherche (TGIR).

La MMSH possède, pour ses recherches, 10 unités mixtes de recherche listées ci-dessous :

- CCJ
- CPAF
- IDEMEC
- IMAF
- IRAA
- IREMAM
- LA3M
- LAMPEA
- MESOPOLHIS

- TELEMME

Photographie 1 : Entrée de la MMSH

En ce qui concerne sa localisation, la MMSH est située dans la ville d'Aix-En -Provence, 5 Rue Château de l'Horloge, ce qui représentait pour moi environ 1h30 de trajet aller-retour quotidien.

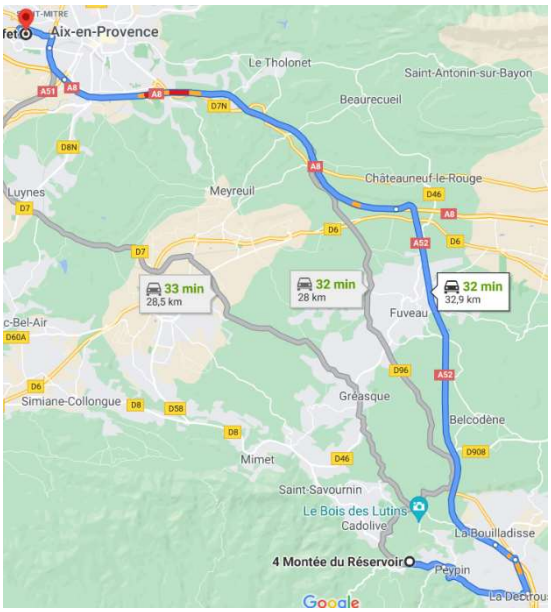

Figure 1 : Trajet domicile-MMSH

1.2 Présentation du service

Le service dans lequel j'ai été stagiaire ces 9 dernières semaines est le service informatique de la MSSH. Il est composé de Rémi SENOUQUE (AI-CNRS), Alberto SOTO (AI-CNRS), Pascal MARTEAU (TCE-CNRS) qui sont des membres du service et de Vincent BAYLE, (IR2-CNRS) qui le chef du service informatique. On peut voir sur le schéma ci-dessous l'organisation générale de la MMSH.

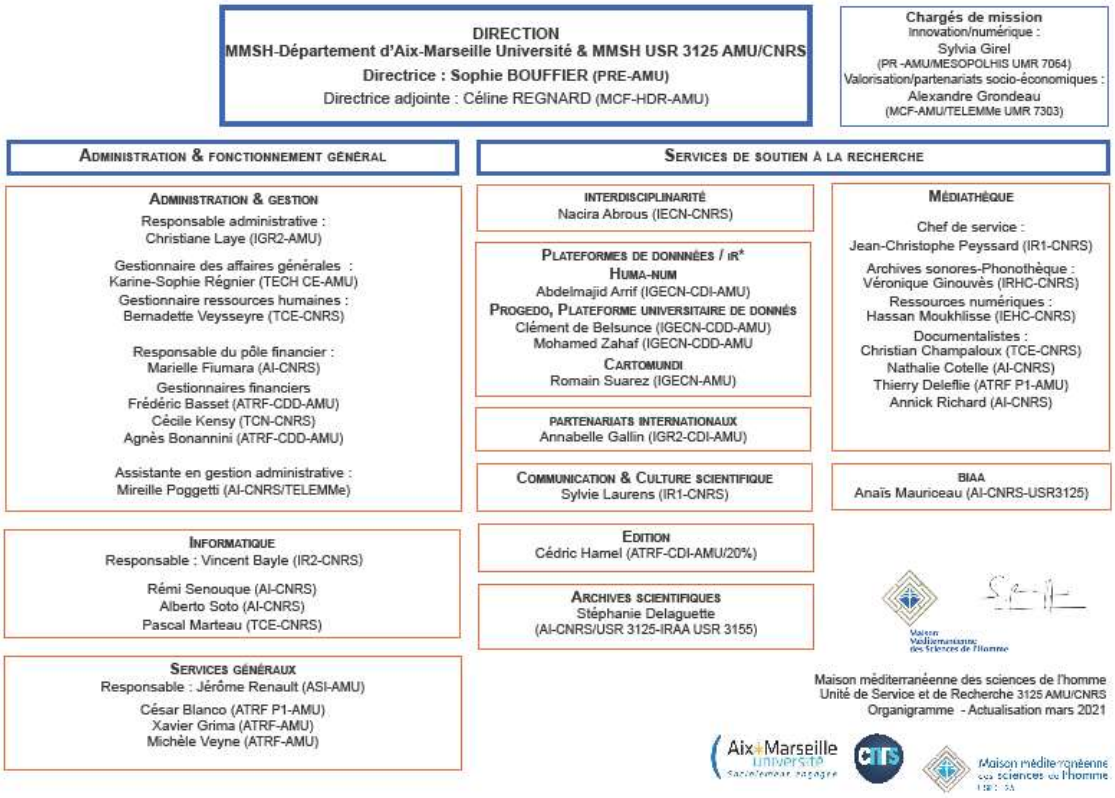

Figure 2 : Organigramme de la MMSH

2. Cadre Technique Général

2.1 Contexte

- J'ai effectué ce stage dans le cadre de ma 2ème année d'IUT Réseaux et Télécommunications, dont le cursus comprend la réalisation d'un stage en entreprise, dans l'objectif de valider mon diplôme. C'est dans ce but que j'ai effectué ce stage de 10 semaines à la MMSH qui a duré du lundi 16 Avril au vendredi 25 Juin. Le contexte du stage est assez particulier car, avant de débuter le stage, mon tuteur, Vincent BAYLE, m'avait fourni la liste des missions que j'aurais à effectuer durant le stage, détaillée ci-dessous :
- Mettre à jour la configuration de tous les switchs :
  - HPE Aruba 5120, 5130, petits, un switch 10G, mise en place et configuration de switchs Virtuels Windows avec des cartes 10G SFP+, configuration Linux / Proxmox, switchs Fabric de VRTX Dell
- Reconfigurer certains ports de switchs, pour les changer de VLANs. Il sera nécessaire d'effectuer des manipulations pour les adresses ip/mac, les vlans, etc.
- Manipuler les outils de gestion installés à la MMSH : Observium, Rancid, firewall Fortinet, via interface web mais aussi des manipulations de commandes CLI, et Unix
- En fonction de la facilité à développer, écrire une solution basique pour l'affichage, via un site web programmé en Django, en python, de la configuration des prises réseau

Cependant, lors de mon arrivée, le lundi 26 Avril, la MMSH est touchée par une attaque informatique, un crypto virus, qui a pour effet de crypter les serveurs Windows présents sur le parc informatique de l'entreprise. Le schéma ci-dessous montre les éléments touchés par cette cyberattaque (zone rayée en jaune) :

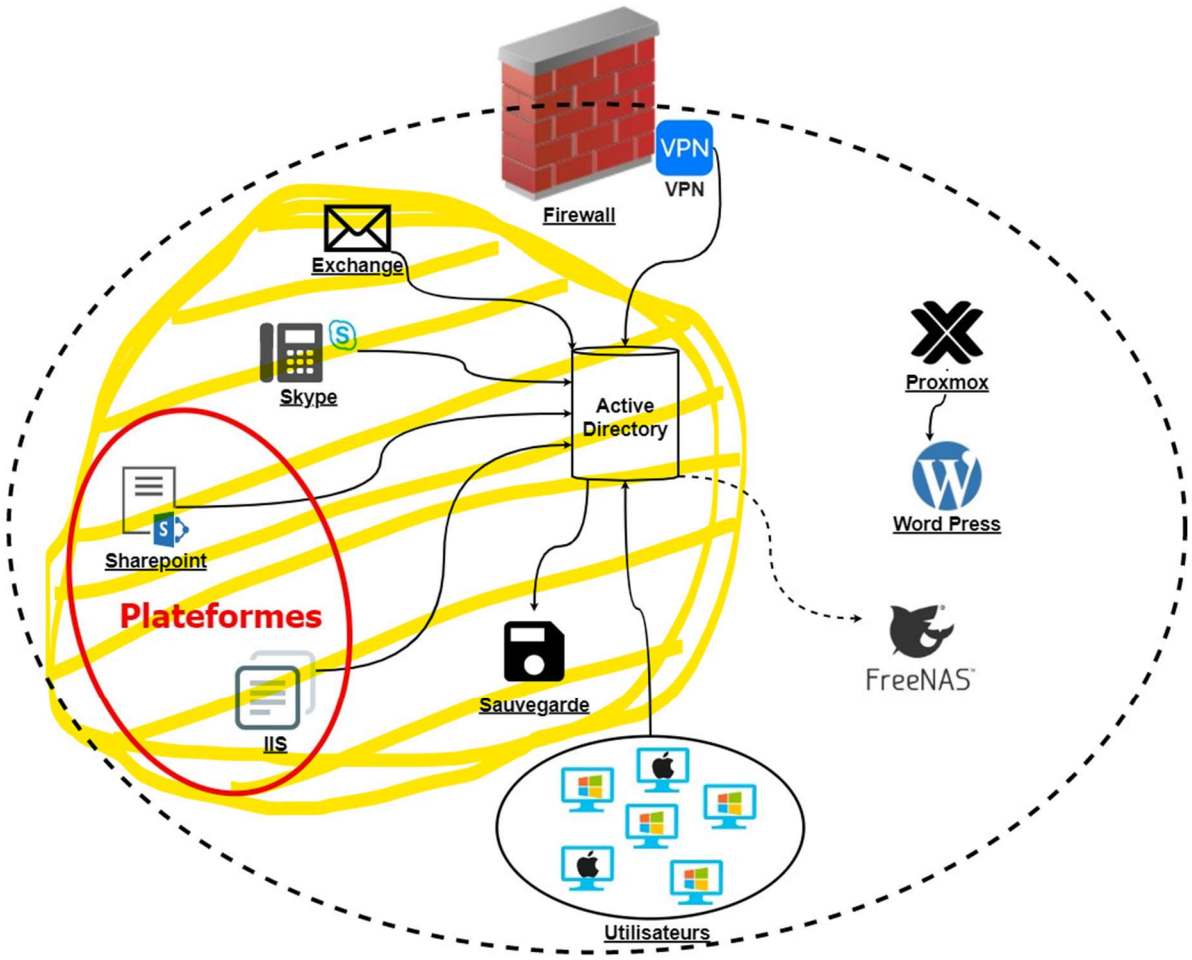

Figure 3 : Schéma attaque MMSH

Comme ont peut le voir sur le schéma, beaucoup d'éléments étaient dépendants de l'AD (Active directory), qui est malheureusement devenu inutilisable à la suite de l'attaque. En ce qui concerne le réseau, les machines des utilisateurs de la MMSH dépendaient de l'AD car il faisait office de serveur DHCP et de serveur DNS. Il y a aussi une action volontaire de la part du service informatique qui était d'interdire tout Traffic sortant sur le firewall pour pouvoir analyser l'état actuel du réseau de la MMSH.

2.2 Missions

À la suite de cet incident, il a fallu complétement revoir les missions initialement prévues pour le stage, car elles ne correspondaient plus du tout aux priorités actuelles. Mes nouvelles missions étaient donc :

- Dans un premier temps, rétablir un accès à internet aux membres de la MMSH, pour qu'ils puissent reprendre le travail, via la mise en place d'un vlan utilisateur, d'un serveur DHCP et d'un serveur DNS.

- Puis dans un second plan de reconstruire un réseau plus sécuriser, de manière à ne plus être vulnérable à ce genre d'attaques, notamment grâce au cloisonnement du réseau et la mise en place d'un serveur RADIUS.

2.3 Compétences requises

Pour le bon déroulement des ces missions, un BAC +2 ou une licence professionnelle dans le domaine des réseaux est obligatoire pour avoir les notions et les connaissances en réseau nécessaires.

3. Matériel Manipulé

3.1 Hardware

Durant ces semaines de stage et mes différentes interventions, j'ai été amené à manipuler différents terminaux et équipements réseau. Voici ci-dessous la liste des matériels que j'ai utilisés avec quelques mots sur leur utilité :

- Fortigate 200E :

Le FortiGate 200E est le pare-feu de la MMSH, c'est lui qui gère une grande partie de la sécurité sur le réseau.

- HPE 5820X-24XG-SFP+

Ce switch est muni de ports 10 gigabit Ethernet et il est le switch sur lequel sont reliés tous les switchs de tous les locaux, ce qui en fait un élément majeur du réseau de la MMSH.

- HPE 5120-48G-PoE+ EI

Ces switchs, car il y a plusieurs exemplaires de ce modèle dans les différent locaux, est utilisé pour apporter le réseau jusqu'aux prises présentes dans les bureaux

- HPE 5130-48G-PoE+ EI

Ces switchs, car il y a plusieurs exemplaires de ce modèle dans les différents locaux, est utilisé pour apporter le réseau jusqu'aux prises présentes dans les bureaux. C'est une version plus récente du 5120 au-dessus.

- Dell M6348

C'est le switch qui est présent à l'arrière des VRTX, châssis mini-lame, sur lequel j'ai pu activer la connexion par SSH, et sur lequel j'ai put faire les premières configurations, car il fonctionnait avec la configuration de base depuis sa mise en fonctionnement.

- Aruba 2530-8G-PoEP

Ce sont les petits switchs "manageables" présents dans les bureaux avec plusieurs ordinateurs.

L'accès à tout ses équipements se faisait par ssh, sauf pour le fortinet sur lequel je me connectais via l'interface web.

Pour ce qui est de la téléphonie, 2 références étaient disponibles dans le bâtiment de la MMSH :

- SNOM 710
- Polycom VVX 411

Ces téléphones sont de génération différente, les Polycom étant les plus récents, ils tendent à remplacer les Snom.

Pour terminer, en ce qui concerne la couverture sans fil dans le bâtiment, on peut y croiser 4 références de bornes :

- Aruba AP105
- Aruba AP115
- Aruba AP305
- Aruba AP315

3.2 Software

Après avoir présenté le matériel utilisé, voici les logiciels qui m'ont été utiles lors de me différentes interventions avec quelques mots sur leur fonctionnement :

- Netdisco

Netdisco est un outil de gestion de réseau adapté aux réseaux de petite à très grande taille. Les données relatives aux adresses IP et MAC sont collectées dans une base de données PostgreSQL à l'aide de requêtes SNMP, CLI ou des APIs des machines. Il permet aux administrateurs de réseau de localiser le port de switch de n'importe quel nœud connecté au réseau. La connexion à Netdsico se fait via son interface web.

- Observium

Observium est une plateforme de surveillance de réseau à faible maintenance et à découverte automatique qui prend en charge un large éventail de types de dispositifs, de plateformes et de systèmes d'exploitation, notamment Cisco, Windows, Linux, HP, Juniper, Dell, FreeBSD, Brocade, Netscaler, NetApp et bien d'autres. Observium s'engage à fournir une interface belle et puissante, mais simple et intuitive, pour le bon fonctionnement et l'état de votre réseau.

Développée et maintenue de manière professionnelle par une équipe d'ingénieurs réseau et d'administrateurs système expérimentés, Observium est une plateforme conçue et construite par ses utilisateurs. Il récupère ces informations grâce à des commandes qu'il exécute dans l'invite de commande des switchs. La connexion s'y fait par interface web mais on peut aussi récupérer des informations en se connectant via ssh sur la machine qui héberge observium.

- WiKi

Le service informatique de la MMSSH tient à jour un wiki qui leur sert de documentation et de base de connaissance général. Ce wiki m'a été utile par exemple pour mes connections ssh aux différents switchs et j'ai aussi pu apporter quelques modifications au wiki en y ajoutant une page concernant la démarche à suivre pour effectuer un diagnostic réseau.

- WSL

Windows Subsystem for Linux (WSL) est une couche de compatibilité permettant d'exécuter des exécutables binaires Linux (au format ELF) de manière native sur Windows 10 et Windows Server 2019. WSL m'a été utile durant toute la durée de mon stage notamment avec l'utilisation des alias, grâce auxquels la connexion aux switchs était bien plus rapide. WSL vient en remplacement d'un logiciel déjà utilisé lors de ma formation à l'IUT, PuTTy.

- FortiGate Web interface

Interface web du firewall de la MMSH sur laquelle je me connecte pour y effectuer des modifications.

4. Travaux Effectués

4.1 Plan Réseau de la MMSH

Lors de mon arrivé en tant que stagiaire à la MMSH, la première mission qui m'a été donnée était de faire un plan du réseau de la MMSH. Ce plan allait être utile pour l'ensemble du service informatique mais surtout pour moi-même car j'aurai à intervenir sur le réseau de nombreuses fois dans les semaines qui suivent. Ce schéma a pour objectif de se représenter facilement la topologie physique de l'ensemble du réseau de la MMSH et de pouvoir repérer rapidement les ports qui servent d'interconnexion entre les switchs, qui sont souvent l'origine des problèmes de réseau.

Pour réaliser ce schéma, j'ai eu besoin de Observium et du protocole LLDP. J'ai déjà expliqué ce qu'était Observium plus haut dans le rapport, mais pas LLDP.

LLDP signifie Link Layer Discovery Protocol. C'est un protocole normé dans les publications IEEE 802.1AB et IEEE 802.3 section 6 clause 79. Il sert à la découverte des topologies réseau de proche en proche, mais aussi à apporter des mécanismes d'échanges d'informations entre équipements réseaux et utilisateurs finaux.

Il tend à remplacer un bon nombre de protocoles propriétaires (Cisco CDP, Extreme EDP, etc.), pour de meilleurs échanges entre les équipements des différents constructeurs.

Ci-dessous, une photo de l'interface d'observium sur laquelle on peut voir les interfaces voisines au switch LTA1, grâce au protocole LLDP :

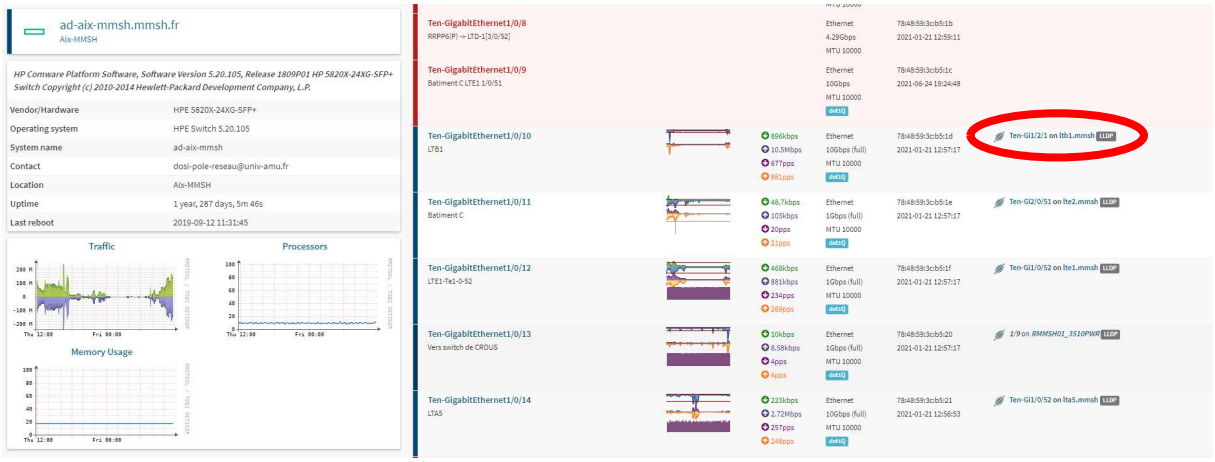

Figure 4 : Interface Observium

C'est grâce à ça que j'ai pu construire petit à petit le plan global du réseau de la MMSH sur lequel on peut voir le firewall, le switch au cœur du réseau, les switchs pour assurer la connexion vers les prises dans les bureaux ainsi que les petits switchs de bureau "manageable" :

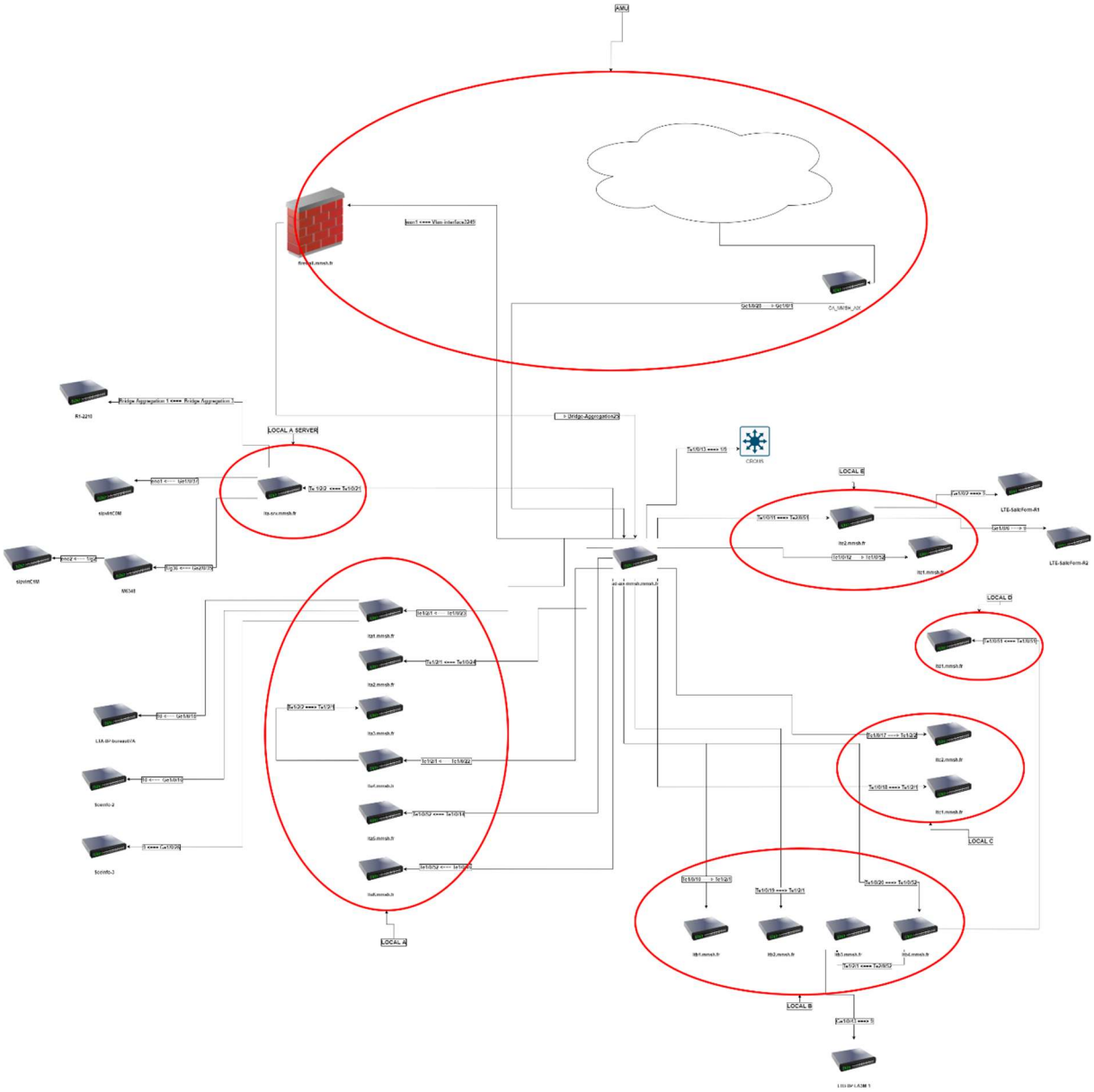

Figure 5 : Plan Réseau MMSH

4.2 Rétablissement du réseau

Après avoir fini le plan du réseau de la MMSH, il était important de rétablir un accès à internet pour les utilisateurs de la MMSH pour qu'ils puissent reprendre leur travail. En effet, l'AD de la MMSH est devenu inutilisable à la suite de l'attaque par cryptovirus. Étant donné qu'il faisait office de serveur DNS et de serveur DHCP, et que le trafic sortant avait été coupé manuellement sur le firewall, les utilisateurs n'avaient plus d'accès Internet.

Il a donc fallu mettre tous les utilisateurs dans un "vlan utilisateur" pour les isoler des serveurs vérolés, remettre en service un serveur DNS, remettre en place un service de DHCP puis autoriser le trafic à sortir sur internet.

Pour que les explications soient plus claires et compréhensibles, le schéma en-dessous illustre un exemple pour remettre l'accès à Internet à un utilisateur lambda, tout en sachant que les manipulations sont les mêmes pour le reste du parc.

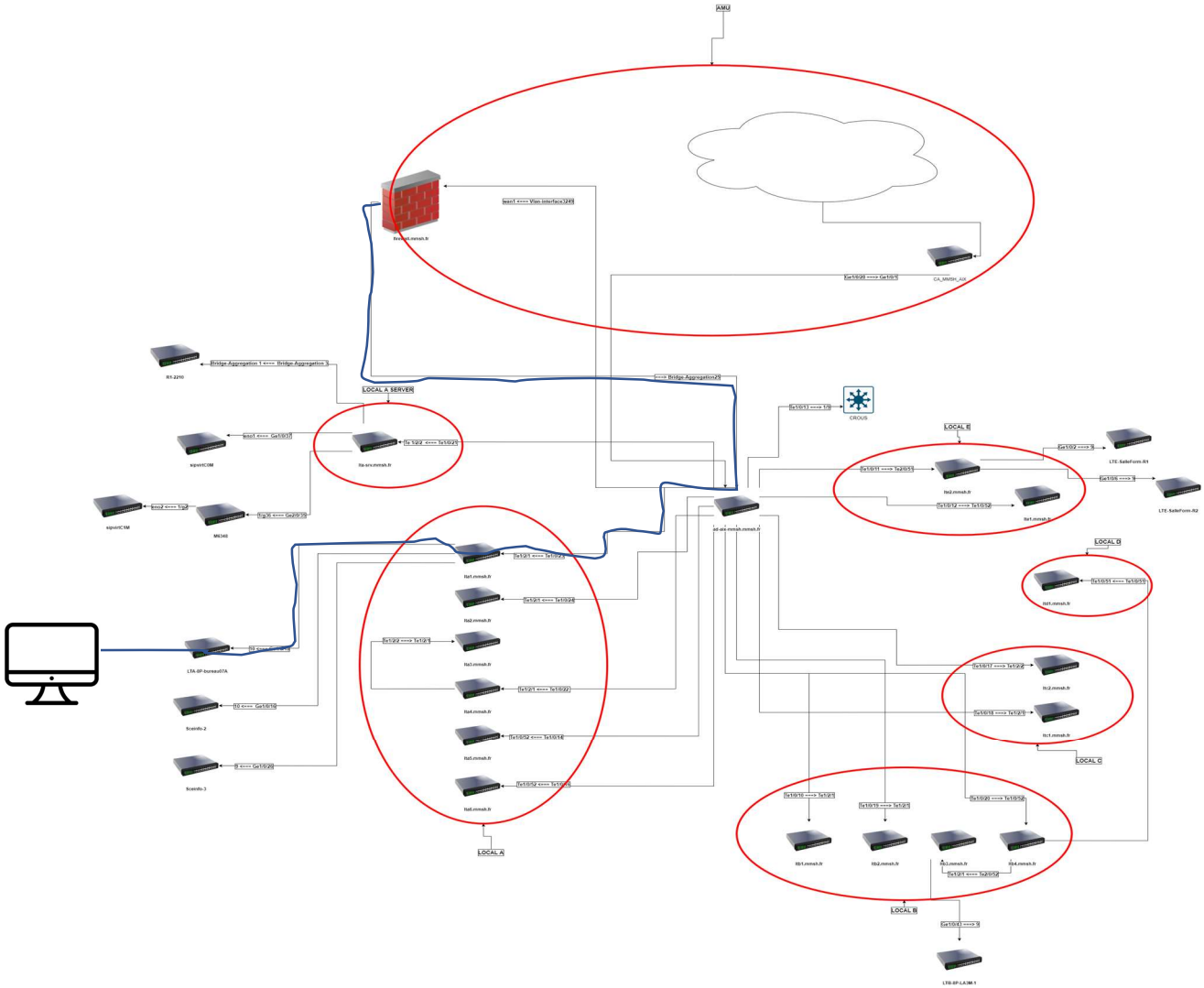

Figure 6 : Exemple pour un utilisateur

Ici, j'ai pris l'exemple d'un utilisateur lambda et j'ai tracé le chemin du post utilisateur jusqu'au firewall pour voir quels éléments il faut configurer pour que cet utilisateur ait un accès à internet.

J'ai aussi fait un schéma simplifié pour mieux comprendre et mieux voir le chemin entre le poste utilisateur et le pare-feu :

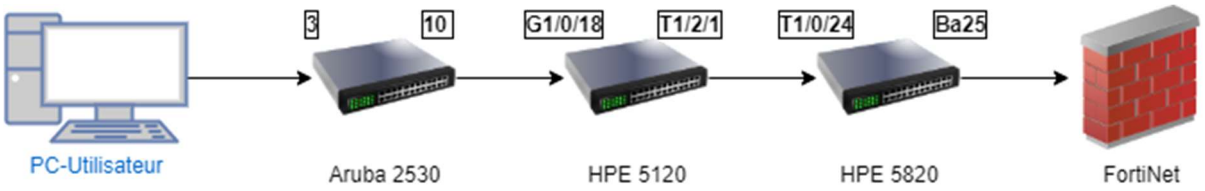

Figure 7 : Schéma simplifié

Pour ce qui concerne les vlan, la première chose à faire est de créer un vlan utilisateur afin d'isoler les postes des utilisateurs des servers vérolés, dans le but d'éviter une surcontamination. Pour cela, il va falloir passer sur tous les switchs présents sur le chemin entre l'utilisateur et les firewalls, pour déclarer ce vlan sur les switchs en utilisant les commandes suivantes :

- vlan 3
- name Utilisateurs

Maintenant que les vlan sont déclarés, il faut les assigner aux interfaces d'interconnections entre les switchs. Ici se pose un problème que je n'avais encore jamais rencontré auparavant, la syntaxe. En effet, sur le schéma présent Figure 7, on peut voir qu'il y a différentes versions de switchs, qui ont des syntaxes différentes l'un à l'autres et surtout des syntaxes différentes des switchs cisco sur lesquels j'ai pu travailler auparavant lors de ma formation.

Pour ça, on va déclarer le vlan Utilisateur en tant que vlan « Untagged » lorsque l'interface a en face d'elle un autre switch et en « Tagged » lorsqu'en face de l'interface ce trouve un ordinateur.

Maintenant, tout est bien configurer au niveau des switchs et le vlan 3 est bien présent du post utilisateur jusqu'au firewall.

Le reste de la configuration se fait désormais sur le Fortinet.

En effet, une fois sur le Fortinet, il faut créer une interface pour le vlan 3. Cette interface jouera le rôle de passerelle par défaut et de serveur DHCP pour les machines présentes sur le vlan Utilisateur. On peut le voir sur le schéma ci-dessous :

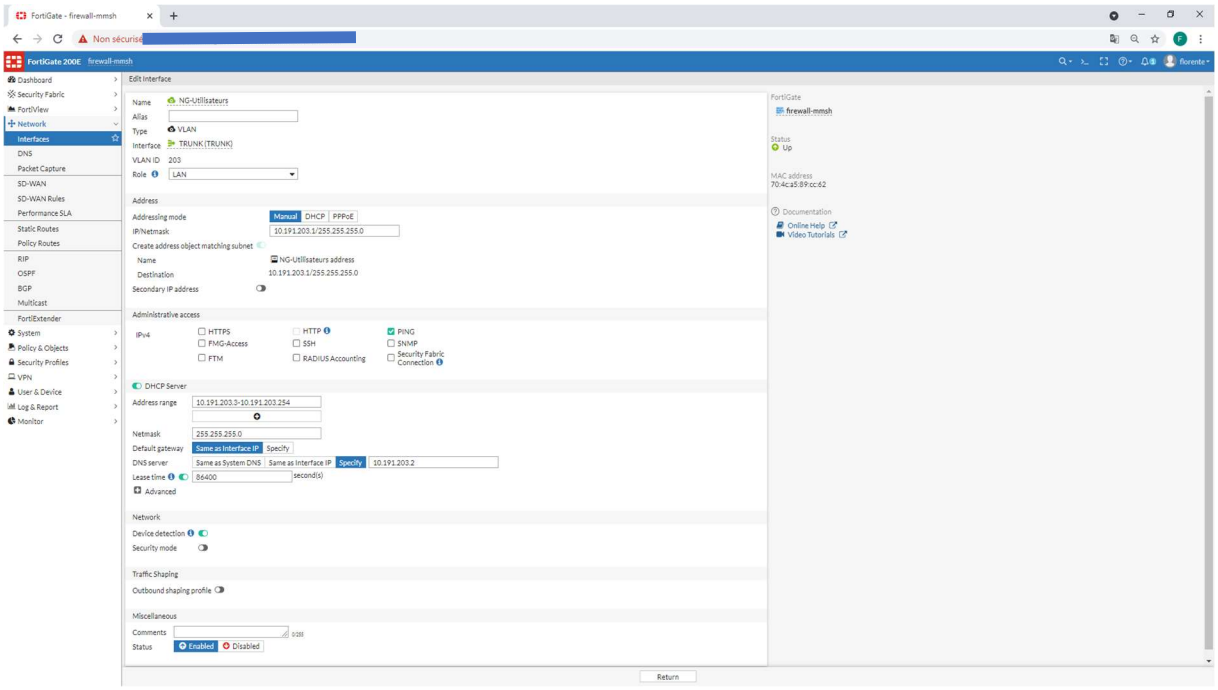

Figure 8 : Config interface Vlan Utilisateur

Maintenant, il ne reste plus qu'a créer une règle qui autorise le trafic venant de ce vlan vers l'extérieur, en autorisant que certains protocoles à sortir, pour les utilisateurs aient de nouveau accès à internet dan le bâtiment de la MMSH. En ce qui concerne le serveur DNS, il a aussi été mis en place mais je n'ai pas participer à sa mise en place donc je ne développerai pas son déploiement ici.

4.3 Réflexion sur la sécurisation du nouveau réseau

Maintenant que les utilisateurs ont accès à internet, il faut réfléchir comment reconstruire un nouveau réseau, mieux sécurisé, de manière à ne plus être vulnérable au type d'attaque subie.

En ce qui concerne la partie réseaux, voici les résolutions qui ont été misent en place :

- Le cloisonnement du réseau à l'aide de vlan, comme mettre chaque labo de recherche dans un vlan unique, isoler les switchs dans un autre vlan, ainsi que les serveurs etc.
- Le renforcement des règles sur le fortinet car auparavant, il était fréquent de trouver des règles qui autorisaient le trafic de n'importe quelle ip source vers n'importe quelle ip destination, en autorisant tous les protocoles.
- L'authentification des adresses mac des machines se connectant sur le réseau, grâce au déploiement d'un serveur RADIUS.

4.4 Serveur Radius

En effet, pour assurer une sécurité optimale sur le réseau, il a été décidé de mettre en place un serveur Radius qui, dans notre cas, va servir à l'authentification des machines se connectant sur le réseau par leur adresse MAC.

Le protocole RADIUS permet de faire la liaison entre des besoins d'identification et une base d'utilisateurs en assurant le transport des données d'authentification de façon normalisée. L'opération d'authentification est initiée par un client du service RADIUS, qui peut être un boîtier d'accès distant (NAS : Network Access Server), un point d'accès réseau sans fil, un pare-feu (firewall), un commutateur, un autre serveur. Le serveur la traite en accédant si nécessaire à une base externe : base de données SQL, annuaire LDAP, comptes d'utilisateur de machine ou de domaine ; un serveur Radius dispose pour cela d'un certain nombre d'interfaces ou méthodes.

Comme j'ai pu le dire au-dessus, dans notre cas, on utilisera la mac-based authentication qui se base sur les adresses mac des machines branchées sur le réseau pour les identifier.

Pour son fonctionnement, lorsqu'un utilisateur quelconque se branche sur le switch, le switch envoi une requête au server radius avec comme identifiant et mode de passe, l'adresse MAC de la machine en question. Si l'adresse MAC est reconnue, alors le serveur RADIUS renverra comme réponse le vlan qui a été renseigné dans le fichier de configuration des utilisateurs. Sinon, le server renverra comme réponse le vlan par défaut qui a été configuré. Une fois le port configuré avec le vlan renvoyé par le serveur RADIUS, la machine de l'utilisateur a accès à un serveur DHCP, présent sur la même machine que le serveur RADIUS, ce qui lui permet de récupérer une configuration réseau (passerelle par défaut, DNS, adresse ip). Ci-dessous un schéma pour mieux comprendre le fonctionnement de RADIUS.

Pour ce qui est du déploiement de RADIUS, on peut distinguer 2 parties :

- La partie système sur laquelle je ne suis pas intervenu, qui a été faite en collaboration avec Adrien MALGOYRE, ancien élève de l'IUT Réseaux et Télécommunications, actuellement Administrateur des systèmes informatiques, réseaux et télécommunications au CNRS. Cette partie comprend l'installation du serveur RADIUS et l'installation du serveur DHCP.

- La partie réseau, sur laquelle je suis intervenu qui comprend la configuration des switchs pour le bon fonctionnement du RADIUS.

Pour la configuration sur les switchs, il y a 2 grandes étapes. La première étape est la déclaration du RADIUS. Avec ces commandes, on va indiquer au switch l'adresse ip du serveur RADIUS, le mot de passe pour s'y connecter, le format à utiliser pour exporter les adresses MAC etc.

Voici un exemple de commandes à utiliser pour la déclaration du RADIUS :

```
radius scheme swmmsh
 primary authentication 10.191.192.93
 primary accounting 10.191.192.93
 key authentication simple [redacted]
 key accounting simple rad_[redacted]
 user-name-format without-domain


domain radius-mmsh
 authentication login local
 authorization login local
 accounting login local
 authentication default radius-scheme swmmsh
 authorization default radius-scheme swmmsh
 accounting default radius-scheme swmmsh

 mac-authentication
 mac-authentication domain radius-mmsh
 mac-authentication user-name-format mac-address without-hyphen uppercase
```

Figure 9 : Déclaration Radius

L'étape suivante est de configurer les ports des switchs pour leur dire d'utiliser le mac-based authentication. Voici ci-dessous l'exemple de configuration d'une interface qu'il faudra appliquer sur toutes les autres interfaces des switchs qui seront potentiellement reliées à des postes utilisateurs.

```
interface GigabitEthernet 1/0/1
default
port link-type hybrid
 undo port hybrid vlan 1
 port hybrid vlan 2400 tagged
 port hybrid vlan 203 untagged
 port hybrid pvid vlan 203
 undo voice vlan mode auto
 voice vlan 2400 enable
 mac-vlan enable
 poe enable
 mac-authentication max-user 10
 mac-authentication
 mac-authentication guest-vlan 203
```

Figure 10 : Config port pour RADIUS

Pour finir, il ne reste plus qu'a déclarer les machines voulus avec le vlan dans lequel on veut les affecter sur la machine RADIUS. Par exemple ici on veut affecter la machine avec comme adresse MAC c8:1f:66:ae:14:c7 dans le vlan 210 :

```
============================================================

nano etc/freeradius/3.0/mods-config/files/users_mmsh

# Nom machine : ED_FORM_14
C81F66AE14C7 956    ClearText-Password := "C81F66AE14C7"
        Tunnel-type = VLAN,
        Tunnel-Medium-Type = 6,
        Tunnel-private-Group-ID = '210'

============================================================
```

Figure 11 : Exemple config utilisateur

Puis, déclarer ce même utilisateur dans le fichier conf du DHCP pour lui assigner une adresse IP :

```
================================================

nano etc/dhcp/dhcpd.conf

host LAMES_COCHE5 {
        hardware ethernet c8:1f:66:ae:14:c7 ;
        fixed-address 10.191.210.13 ;
    }

================================================
```

Figure 12 : Exemple config DHCP

Maintenant, tous les éléments sont en places pour l'utilisation d'un serveur RADIUS.

5. Conclusion

Pour conclure sur ce stage, j'ai grandement apprécié participer à des projets variés comme la réalisation d'un plan de réseau ou le déploiement d'un serveur RADIUS. Le cahier des charges est bel est bien rempli même s'il reste encore quelques éléments à configurer pour compléter le travail réalisé. C'est pourquoi d'ailleurs, la MMSH a fait une demande de prolongation de mon stage, pour que je puisse finir de participer au projet de déploiement de ce serveur RADIUS. Ce stage a été pour moi très enrichissant du point de vue professionnel car il m'a permis de faire appel aux notions apprises sur le réseau pendant ma formation, de manière concrète. Cela m'a aussi obligé à faire appel à ma capacité d'adaptation, étant donné que les équipements que j'ai manipulé pendant ces semaines de stage étaient différents de ceux manipulés lors de mes différents TP à l'IUT, ce qui signifie une nouvelle syntaxe à apprendre et cela a renforcé mon envie de continuer à me former dans le domaine des réseaux.

6. Remerciements

Je tiens à remercier la MMSH, en particulier Sophie BOUFFIER, pour avoir accepté de me recevoir au sein de la MMSH. Je tiens aussi à remercier l'ensemble du service informatique pour leur confiance, leur gentillesse et leur encadrement qui a grandement participé au bon déroulement de ce stage. Je remercie aussi monsieur NGUYEN sans qui ce stage n'aurait jamais été possible.

7. Glossaire

MMSH, Maison Méditerranéenne des Sciences de l'Homme

RADIUS, Remote Authentication Dial-In User Service

DHCP, Dynamic Host Configuration Protocol

VLAN, Virtual Local Area Network

SNMP, Simple Network Management Protocol

8. Bibliographie

MMSH : https://www.mmsh.fr/

Netdisco : http://netdisco.org/

Observium : https://www.observium.org/