Institut Universitaire de Technologie,
Aix-Marseille Université

ANNEXES
Bachelor Universitaire de Technologie
Spécialité Réseaux et Télécommunications
parcours cybersécurité

Expérience Professionnelle en Réseaux et Cybersécurité

Ethan AMEVET

REGION SUD

Responsable entreprise : Emmanuelle ROME

Responsable académique : Rabah IGUERNAISSI

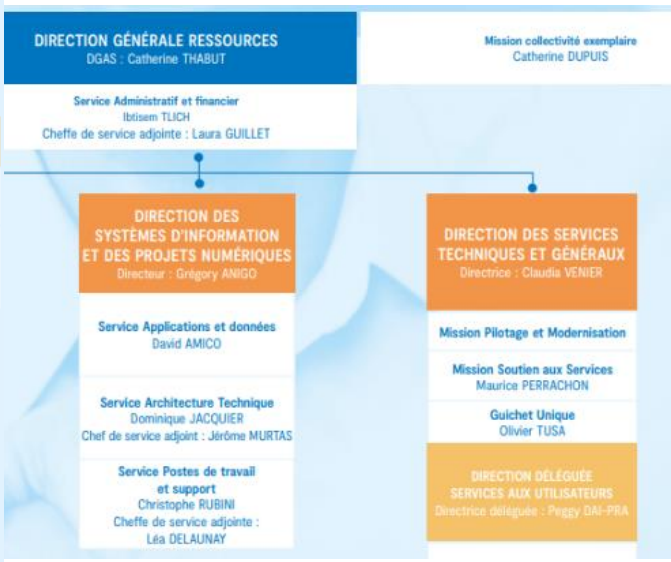
2023

Table des matières

1 Introduction

Ce document rassemble toutes les annexes, apportant des informations supplémentaires afin d'approfondir mon rapport de stage. Il reprend des éléments déjà abordés dans le rapport initial par ordre d'apparition.

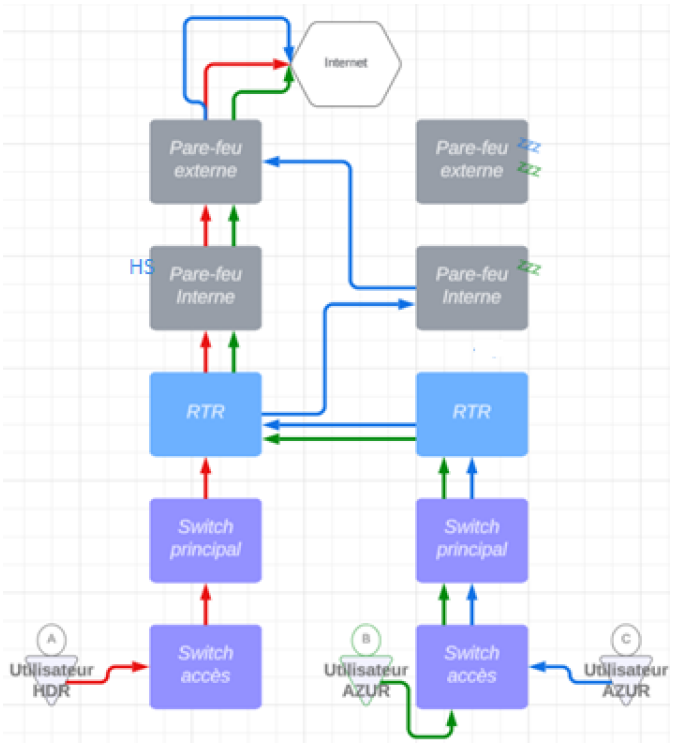
1.1 Le cadre du travail



Pour mieux comprendre le fonctionnement de cette architecture, on peut la découper en 3 parties ;
-la partie routeur
Chaque bâtiment possède un routeur, appelé cœur de réseau. Ils permettent de se connecter aux autre bâtiments. La liaison entre les bâtiments est sous-traitée et redondée. C'est-à-dire que c'est une entreprise privée qui s'est occupée a faire la connexion et que cette dernière est sécurisée par différentes voies de communication (fibre, technologies hertzienne…) au cas où une se coupe. Pour se connecter à Internet, il faut passer par un commutateur, appelé « commutateur principal ».
Les routeurs communiquent ensemble avec le protocole MPLS. Cette solution permet de diffuser leurs VLANs. De cette façon, elles sont mises en commun.
-la partie serveur
Connecté au commutateur principal, cette partie rassemble toutes les VLAN ainsi que les serveurs qui font tourner les applications. Les pares-feux sont des applications, c'est pourquoi ils sont dans cette partie. De plus, ils sont dans des VLANs, les bâtiments Azur et Alpes utilisent les pares-feux du bâtiment HDR.
-la partie utilisateur
Cette partie représente tous les commutateurs qui font fonctionner les équipements physiques des agents tel que les ordinateurs, les téléphones, les imprimantes… A chaque étage se trouvent une baie qui dessert le réseau.

Un seul bâtiment est capable de prendre en charge l'ensemble des connexions. HDR est celui qui les prends pour le moment. Si HDR est totalement ou partiellement inaccessible, Azur peut prendre le relais, puis Alpes.

Voici un schéma logique des routes emprunté par différents utilisateurs dans différents contextes :



Utilisateur A

L'utilisateur A, situé dans le bâtiment HDR, suit le chemin standard lorsqu'il accède au réseau. La séquence de passage est la suivante :

-Switch d'accès de son étage.
-Switch principal du datacenter HDR.
-Routeur.
-Pare-feu interne et externe.

Tous les équipements étant opérationnels, le trafic suit le chemin prévu sans interruption.

Utilisateur B

L'utilisateur B, situé dans le bâtiment Azur, utilise les VLANs partagés via MPLS, permettant l'accès aux ressources du bâtiment HDR. Les pare-feu du bâtiment Azur sont en mode **passif**, tandis que ceux de HDR sont **actifs**. Le trafic suit le chemin suivant :

Switch d'accès de son étage dans le bâtiment Azur.
Switch principal du datacenter HDR (via MPLS).
Routeur de HDR.
Pare-feu interne et externe de HDR.

Le RTR de HDR ne différencie pas les pare-feu des différents bâtiments, assurant ainsi une continuité de service.

Utilisateur C

L'utilisateur C, également dans le bâtiment Azur, est affecté par une panne du pare-feu interne de HDR. En cas de défaillance, le pare-feu interne passif du bâtiment Azur devient actif en conservant l'adresse IP du pare-feu défaillant. Le chemin du trafic devient alors :

Switch d'accès de son étage dans le bâtiment Azur.
Switch principal du datacenter Azur.
Routeur (RTR) de HDR.
Pare-feu interne du bâtiment Azur.

Le routeur de HDR redirige le trafic vers le pare-feu interne d'Azur sans être conscient du changement, maintenant ainsi la connexion active.

1.2 Déployer l’application en ligne

Fonctionnement des requêtes

Dans cette partie je viens expliciter le fonctionnement des requêtes sur le réseau afin de mieux comprendre les manipulations que j’ai mené

Lorsqu'un utilisateur entre un nom de domaine dans son navigateur, le DNS traduit ce nom en une adresse IP associée à un port spécifique. Par exemple, google.com deviendra 8.8.8.8. Le DNS est un serveur présent dans le datacenter. Il contient des centaines de traductions pour toutes les applications disponibles.
La requête est alors envoyée l’adresse IP récemment traduite, qui pointe d'abord vers le pare-feu externe (FWe). Le FWe filtre le trafic entrant et transmet la requête au Reverse Proxy. Un routeur permet également de filtrer, mais le pare-feu sera capable de détecter des cyber attaques, avoir des règles de filtrages plus avancées ou encore d’inspecter au niveau applicatif les paquets, tandis que le

routeur ne peut inspecter que jusqu'à la couche 3. Le Reverse proxy est un serveur intermédiaire qui gère les requêtes des clients et les dirige vers le serveur approprié. Le Reverse Proxy envoie ensuite la requête au pare-feu interne (FWi), qui sécurise et filtre les requêtes avant qu'elles n'atteignent l'application. Enfin, après avoir traversé le FWi, la requête atteint l'application, qui répond à l'utilisateur.

En utilisant le DNS pour la traduction des adresses, les pares-feux pour la sécurité, et le reverse proxy pour la gestion des requêtes, l'application peut être rendue accessible sur Internet tout en assurant une protection et une gestion adéquates des données et des flux de trafic.

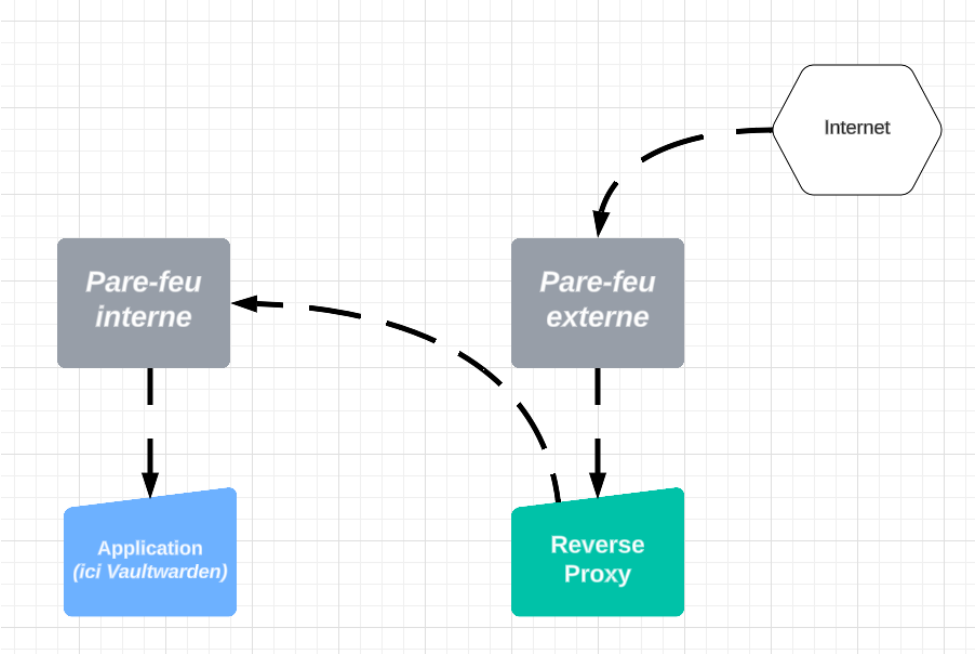


Figure 1 : Schéma du chemin d'une requête

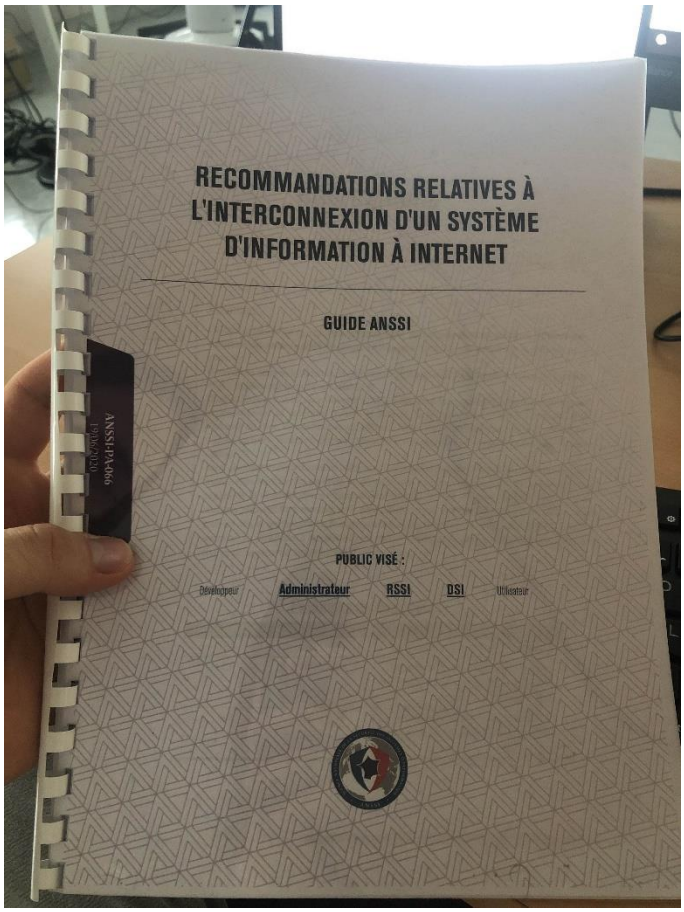


Figure 2 : Guide de l'ANSII qu'on m'a offert pour approfondir les réponses qu'on donnait à mes questions

On m'a également présenté des organigrammes sur les protocoles de sécurité et d'acheminement des paquets. Chaque élément sur la figure 3 peuvent être déroulés et présentent plus en détails les technologies utilisées

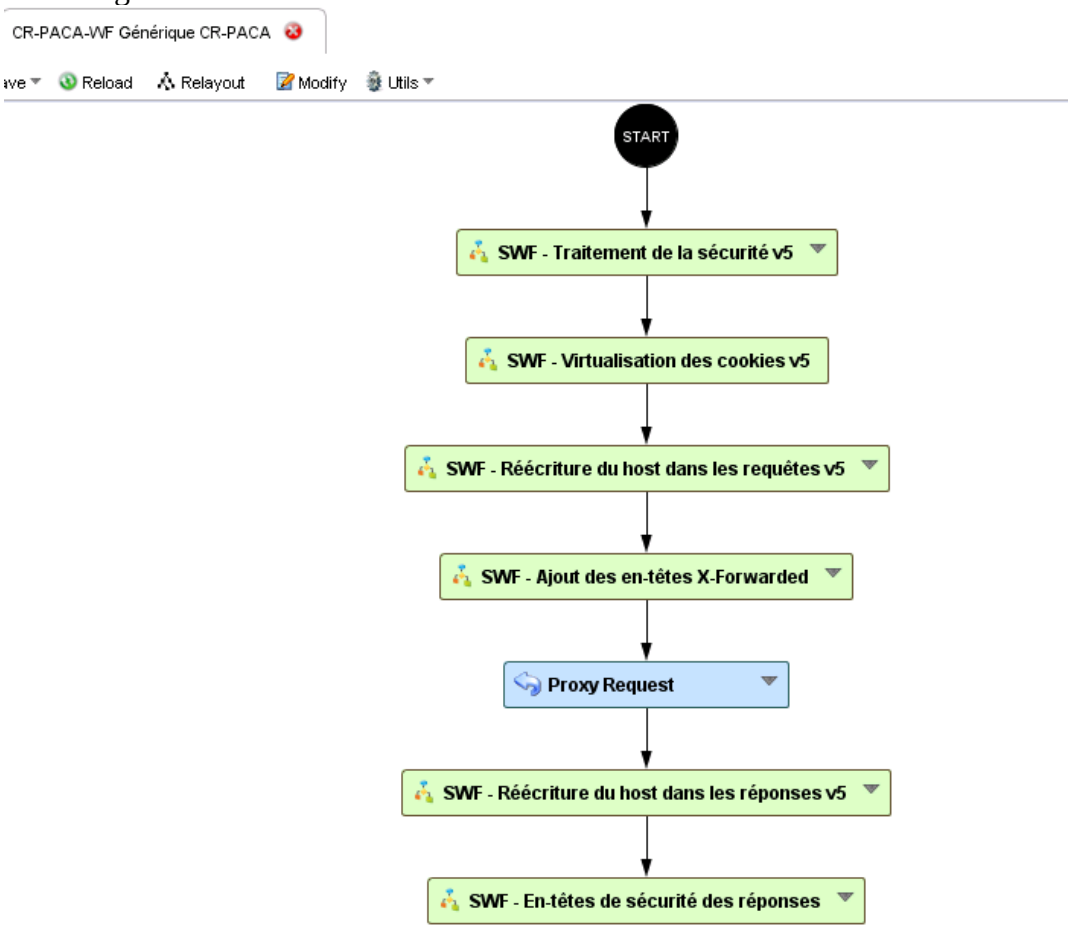


Figure 3 : Comment les paquets sont traités

2 Missions complémentaires

2.1 Missions réseaux

2.1.2 Déploiement Wifi

Plus de 200 bornes Wifi sont disposées aux quatre coins des bâtiments de la région. On utilise des bornes Cisco, les « points d'accès Cisco Catalyst 9100 » (figure 2). Elles sont appréciées pour leur déploiement rapide. Il arrive que certaine tombe en panne. Pour surveiller l'état des bornes en temps réel, nous utilisons un Cisco Wireless LAN Controller (WLC). Il est crucial de savoir les remplacer rapidement et efficacement. Cela fait partie d'une mission que j'ai menée.

Figure 4 : Point d'accès Cisco Catalyst 9100

Installation du point d'accès

Tout d'abord, il faut commencer par noter et retrouver la borne à remplacer. On peut les trouver souvent dans le faux-plafond (figure 3) avec une étiquette.
Par la suite, on débranche l'ancienne qu'on remplace avec une borne neuve. Seul un câble est nécessaire car c'est un câble **PoE**.

Figure 3 :Exemple d'étiquette

Configuration

Le DHCP envoie en broadcast « l'option 43 » (figure 4). Cette option permet d'échanger les informations de configuration, notamment l'IP du contrôleur Wifi. Une fois branchée, la borne reçois ce message. La borne y répond pour ce faire enregistrer. Le point d'accès fonctionne, mais il lui manque un nom personnalisé et l'adresse du contrôleur passif (celui qui prends le relai en cas de panne du premier). On entre ces informations à l'aide du client léger du contrôleur.

```
ip dhcp pool <pool name>
network <ip network> <netmask>
default-router <IP address>
dns-server <dns server IP address>
option 43 hex <hexadecimal string>
```

Figure 4 : Exemple de configuration DHCP pour l'attribution automatique des paramètres réseau aux bornes Wifi Cisco, y compris l'option 43

Vérification

Une fois le déploiement finis, on vérifie si la borne émet le bon signal wifi à l'aide d'un « Wifi Analyzer ». Un Wifi Analyzer est un outil qui scanne et analyse les réseaux Wifi pour fournir des informations sur les différents signaux qu'il reçoit. C'est un outil important pour la gestion d'une infrastructure wifi que j'ai découvert à l'aide de cette mission.

Sur la capture d’écran ci jointe, on peut voir une fréquence élevée qui est apparu et qui porte le nom du point d’accès récemment ajouté. La borne est fonctionnelle.

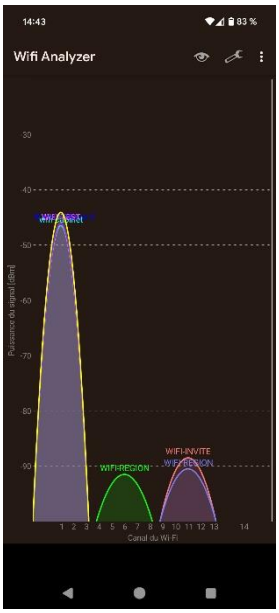


Figure 5 : Capture d’écran du Wifi Analyser

2.2 Observation Cybersécurité

2.2.1 Test d’intrusion Orange

Voici explications approfondis des techniques que j’ai pu observer durant cette experience.

Password spraying : Le password spraying (attaque par pulvérisation de mots de passe) est une méthode de bruteforce (« force brute »). Après avoir récupéré l’ensemble des noms d’utilisateurs à l’aide d’un outil de reconnaissance active, les intrus vont essayer de se connecter avec des mots de passe communs sur l’ensemble des comptes. Cela permet d’éviter le blocage automatique en cas d’erreurs répétés sur le même compte, car il y avait un délai de 30 minutes entre chaque tentative, tout en permettant d’automatiser un nombre de requêtes inhumain. Un compte à être vérolé, à l’aide notamment de social engineering, ou ingénierie sociale. En effet, au détour d’une discussion, un des prestataires a réussi à récupérer le mot de passe par défaut des comptes, et a tenter de rentrer un mot de passe similaire pour piéger un utilisateur qui manquerait de vigilance (si Region2023 aurait été le mot de passe par défaut, le prestaire aurait tenté Region2023!). Cette intrusion a permis aux ingénieurs d’accéder à certains fichiers, notamment aux répertoire « Partagés » qui met en commun des fichiers et des répertoires avec d’autre utilisateur.

Responder est un outil utilisé pour les attaques de type man-in-the-middle sur les réseaux locaux. Man-in-the-middle, ou l’homme du milieu, est un type d’attaque très fréquent qui a pour but d’intercepter des communications entre deux acteurs qui communiquent entre eux. Responder exploite les protocoles de diffusion comme LLMNR et NBT-NS pour intercepter les requêtes de résolution de noms de domaine. En répondant à ces requêtes, il redirige le trafic vers l'ordinateur de l'attaquant, permettant de capturer et les mots de passe qui circulent. Cela facilite l'accès aux comptes sans nécessiter d'attaque bruteforce directe, rendant l'attaque plus discrète. Cette technique n’a cependant pas fonctionné.

Netexec permet d'exécuter des commandes à distance sur des systèmes via le réseau, en utilisant des protocoles comme SMB. Avec des identifiants valides (qui peuvent être obtenu à l'aide des deux techniques précédentes), Netexec se connecte aux systèmes cibles et exécute des commandes. Ces commandes étaient préalablement préparées puis modifiées sur mesure afin d'extraire des données ou installer de logiciels malveillants comme des backdoor (accès secret à la machine). Certaines données récupérées étaient sensibles (cartes d'identités, permis de conduire, documents de la Région potentiellement confidentiel), il fallait faire preuve de professionnalisme et ni les regarder, ni les sauvegarder. Cela reviendrait a enfreindre le contrat qui stipule une stricte confidentialité et intégrité des informations