IUT Réseaux & Télécommunications
Campus de Luminy
13009, Marseille

ONET – Assistances Services
36 Bd de L'Océan
13009, Marseille

Institut Universitaire de Technologie,
Aix-Marseille Université

RAPPORT DE STAGE
Diplôme Universitaire de Technologie
Spécialité Réseaux et Télécommunications

Domaine Réseau & Téléphonie

Romain HAON

ONET GIE ASSISTANT SERVICES

Responsable entreprise : Mr Désire MOSUNALLEE
Responsable académique : Arnaud FEVRIER

2022

Remerciements…

Je souhaite adresser mes remerciements à mon tuteur de stage, Désiré MOSUNALLEE, qui m'a aiguillé lors de mon stage professionnel en entreprise.

J'aimerais également remercier :

- L'ensemble des ingénieurs de l'équipe Réseaux (Paul PARQUET, Pierre-Jean LE BIGOT et Dominique CARTELLA) avec qui j'ai beaucoup appris durant ces dix semaines

- Frédéric GERBAULT (**Responsable de domaine SI Métiers Exploitation**), pour son soutien et ses précieux conseils.

- Maxime NUNEZ, (**Alternant Poste de Travail)** et Maxime DESPRES (**Technicien Systèmes**), tous deux anciens étudiants issus du DUT et de la Licence R&T de Luminy, pour leur soutien, leurs conseils ainsi que leur bonne humeur

Introduction :

Dans le cadre de ma 2° année de mon DUT en Réseaux et Télécommunications, j'ai effectué mon stage, de 10 semaines du **11 avril 2022 au 17 juin 2022** au sein de la DSIN (Direction Systèmes d'Information et du Numérique), précisément dans l'équipe Réseaux et Téléphonie.

J'ai eu l'opportunité d'acquérir de nouvelles compétences dans le domaine des Réseaux avec les divers sujets que l'on m'a confiés. Parmi ces sujets : l'outil de supervision, configuration d'équipements réseaux.

Au-delà de l'aspect technique, ce stage au sein de la DSI m'a permis de m'insérer dans le monde de l'entreprise avec l'interaction au quotidien des différents services.

Table des matières

I / L'Entreprise ONET

A / ONET

L'entreprise ONET est une entreprise internationale comprenant plusieurs filières :

- **ONET Technologies**, *rassemble toutes les activités d'ONET liées à l'ingénierie et aux services pour le secteur du nucléaire et autres environnements industriels complexes*

- **ONET Sécurité**, *rassemble toutes les activités d'ONET liées à la sécurité, proposant des solutions de sécurités agiles*

- **ONET Accueil**, *offre des prestations qui ont une réelle utilité opérationnelle*

- **ONET Logistique**, *offre des prestations sur-mesure en logistique et manutention aux entreprises conscientes de l'importance de ces tâches dans leur fonctionnement quotidien*

- **ONET Airport Services**, *acteur français historique de l'assistance en escale depuis plus de 45 ans, contribue au développement et à l'attractivité des aéroports*

- **ONET Propreté et Services**, *acteur référant en France et en Europe de la propreté et des services associés*

Figure 1 : Filières rattachées au groupe ONET

B / Groupe ONET

Le siège social d'ONET se situe à Marseille, 36 Boulevard de l'Océan, dans le 9ème arrondissement. La gestion de différentes agences du groupe en France métropolitaine et l'étranger est gérée depuis le siège.

Le GIE s'occupe essentiellement des agences en France métropolitaine.

Figure 2 : Info ONET

Voici l'implantation nationale et internationale des sociétés du groupe ONET.

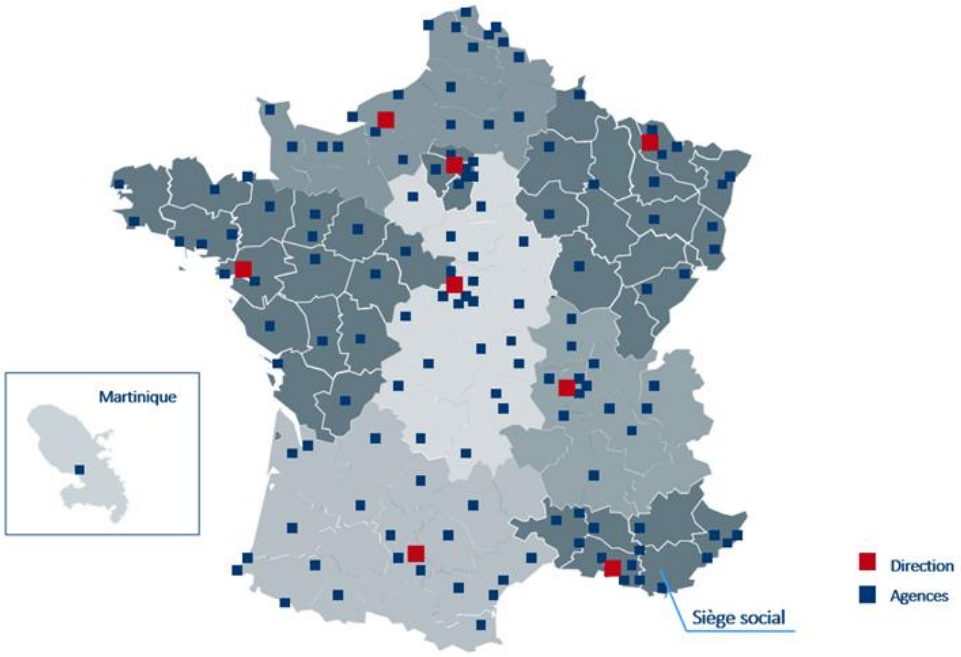

Figure 3 : Agences ONET en France

C / Organigramme

Le GIE (Groupe d'intérêt Économique) est le service fonction support qui est transverse à l'organisation du groupe. Ce service est constitué des pôles DSIN, Compta, Paie.

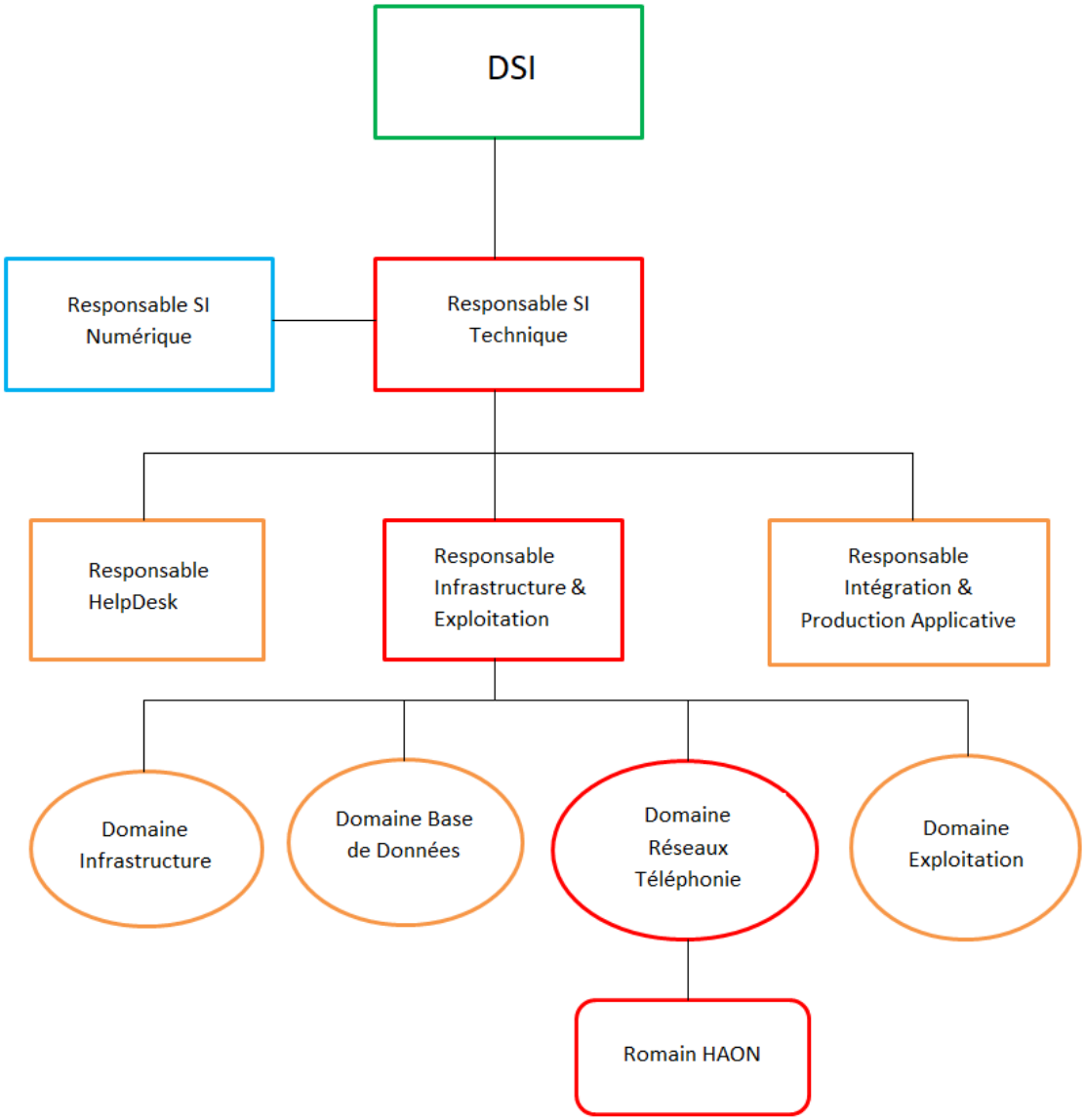

Figure 4 : Organigramme de la DSIN

Le service Infrastructure et Exploitation est composé de quatre domaines :

1. L'Infrastructure systèmes, qui est garante du bon fonctionnement de tous les serveurs, stockage, sauvegarde.

2. Bases de Données, qui gèrent les différentes bases de données servant pour les applications du groupe destinées aux utilisateurs (requêtes SQL…).

3. Exploitation, qui veille à la bonne exécution des tâches automatisées qui sont essentielles au fonctionnement de l'entreprise (ex : paie, applications...etc).

4. Réseaux-Téléphonie, qui s'occupe de l'infrastructure réseau, sécurité, téléphonie.

D / Domaine Réseau et Téléphonie

Le domaine réseau et téléphonie réalise quatre tâches principales :

- MCO (Maintien Conditionnel Opérationnel) : assure le bon fonctionnement des équipements composant l'infrastructure réseaux.
- MCS (Maintiens Conditionnel Sécurité) : mise à jour des équipements exposés aux failles de sécurité.
- RUN (Ticket d'incident, demande de service) : traitement des différents tickets via un outil de gestion « Easyvista »
- Projet Infra – Réseau (Evolution, architecture, obsolescence)

Figure 5 : Bureau de l'équipe Réseaux

II / Projets de Supervision

A / PRTG (Outil de Surveillance Réseaux)

L'objectif de ce projet est d'avoir à disposition un outil de supervision réseau et de pouvoir consulter une cartographie de l'architecture du réseau de l'entreprise.

A terme, suivant l'évolution de l'utilisation, l'équipe réseau souhaite afficher la cartographie sur une TV qui serait placée dans le bureau.

L'outil déjà en place au sein de l'équipe était PRTG (Paessler Router Traffic Grapher). La solution n'étant pas exploitée, j'ai eu l'occasion de travailler sans perturber la production.

PRTG est un logiciel commercial de supervision, il possède de nombreuses fonctionnalités très intéressantes telles que :

- ✓ Alertes Flexible (SMS, E-mail, Syslog…)
- ✓ Interface Utilisateur (WEB, Logiciel Bureau, IOS-Androïd)
- ✓ Carte, Tableau, Diagramme
- ✓ Surveillance (Sonde, WMI, SNMP…)
- ✓ Analyse Détaillée (Statistique (chiffre, pourcentage), graphique, rapport, log)
- ✓ Supervision LAN / WAN (Bande passante, WEB, CPU, Disk, Base de données, Mémoire…)

Les différentes étapes de configurations sont :

- ➢ Ajout d'équipements
- ➢ Mise en place de capteurs sur les équipements
- ➢ Notification d'équipement
- ➢ Cartographie du réseau

En premier lieu, l'ajout d'équipements à surveiller, pour cela il faut renseigner un nom, la version IP et l'IP.

Figure 6 : Ajout d'équipement PRTG

Durant toute la durée de mon stage j'ai pu intégrer de nombreux équipements :

- Cœur de réseau en datacenter
- Switch de distribution
- Pare-feu (Fortinet, Palo-Alto)
- F5 (Répartition de charge)
- VPN (Pulse)
- Proxy (Forcepoint)
- Wallix Bastion (Serveur de rebond)
- PerfVision (Logiciel d'analyse)
- Contrôleur WIFI

Une fois cela fait, on peut ajouter un ou plusieurs capteurs par équipements selon le besoin.

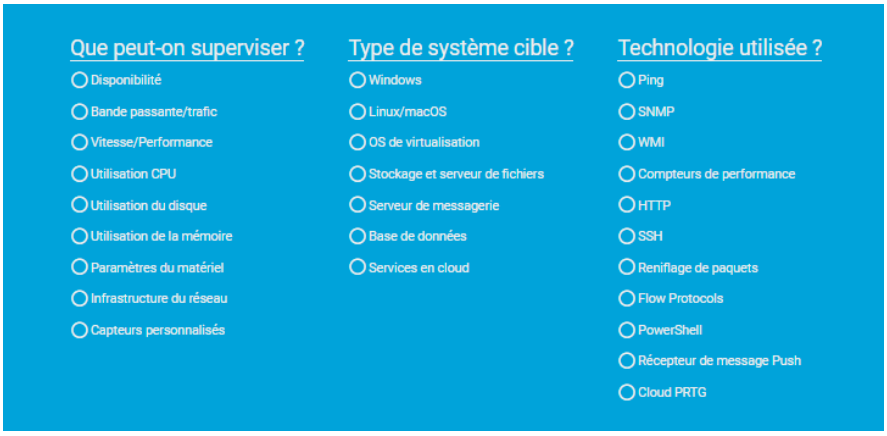

Figure 7 : Ajout de capteur PRTG

On obtient tout un panel de différents capteurs selon ce que l'on a coché.
Par exemple, pour « Utilisation CPU » et « WMI » de coché, voici les capteurs recommandés.

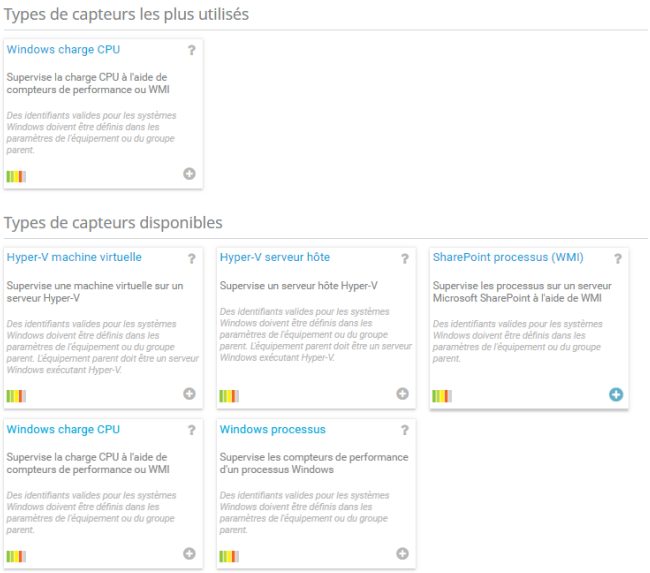

Figure 8 : Capteurs disponibles PRTG

Voici le rendu des données d'un capteur de trafic d'une interface d'un équipement :

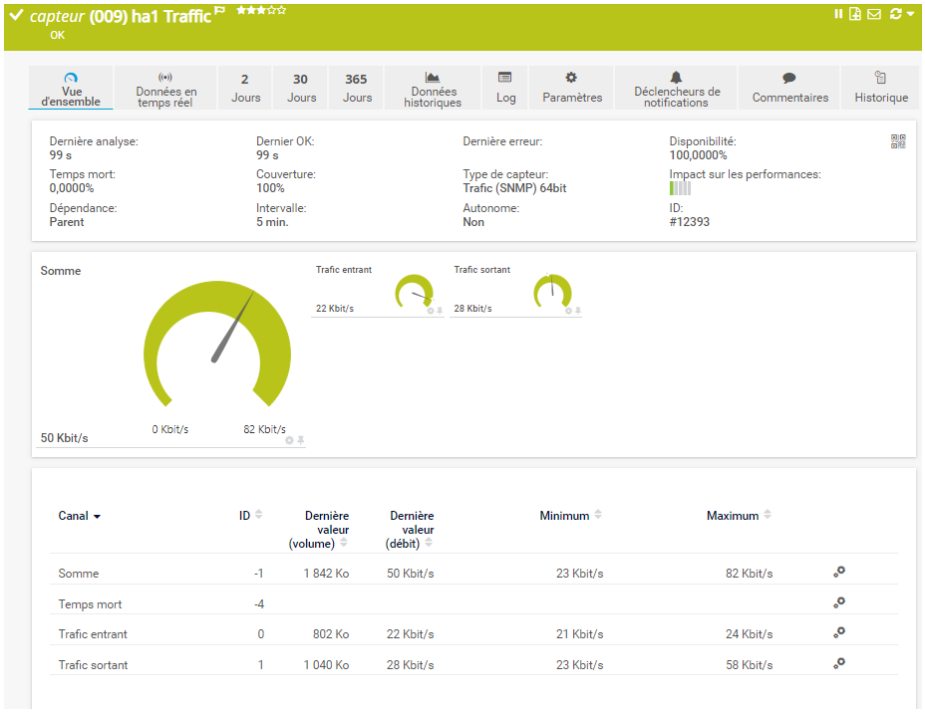

Figure 9 : Données d'un capteur PRTG

La grande majorité des capteurs que j'ai eu l'occasion de mettre en place fonctionnent grâce au protocole SNMP (Simple Network Management Protocol)
C'est un protocole de communication permettant la gestion, supervision ainsi que le diagnostic d'équipement réseau.

La configuration SNMP d'un équipement se réalise en 2 étapes :

- Configuration SNMP sur PRTG
- Configuration SNMP sur l'équipement ciblé

Pour l'ensemble des équipements, c'est la version 3 du protocole SNMP qui a été sélectionnée dû à l'obsolescence en termes de sécurité des versions antérieures.

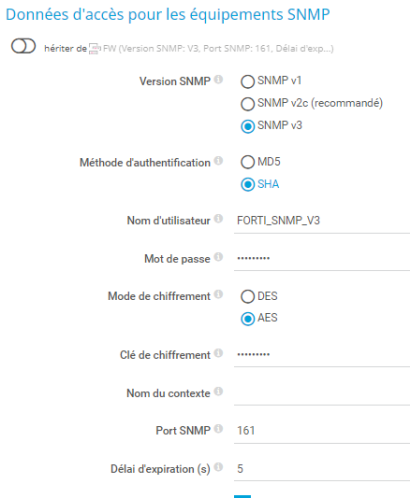

Figure 10 : Configuration SNMP sur PRTG

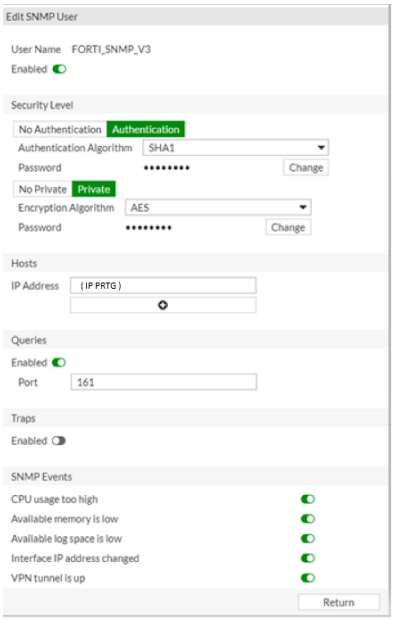

Figure 11 : Configuration SNMP sur un Fortinet

Les alertes permettent d'être notifiées selon différentes situations d'un équipement :

- L'état
- Vitesse
- Volume
- Seuil atteint
- Changement

Pour cela il y a différentes façons d'être notifiées :

- SMS
- E-mail
- Syslog
- PUSH
- SNMP TRAP
- Fichier audio

Enfin, la cartographie du réseau pour un rendu plus global et visuel

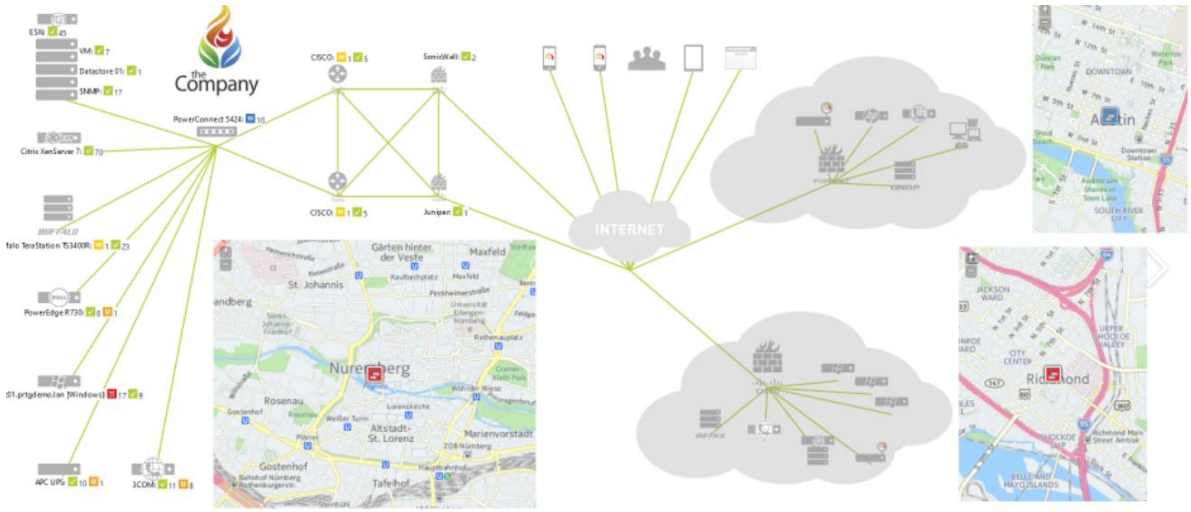

Figure 12 : Exemple Cartographie PRTG (pour cause de confidentialité)

Début Juin, j'ai pu réaliser une présentation à mon équipe réseau sur l'avancement de la configuration du logiciel PRTG.

B / IPAM (Gestionnaire d'adresse IP)

L'objectif du projet IPAM est de remplacer un fichier Excel contenant toutes les adresses IP du système d'information :

Qu'est-ce qu'un IPAM :

IPAM (Internet Protocol Address Management) est un gestionnaire d'adresses IP qui permet de faire :

- Du balayage d'IP (Supervision IP)
- De Suivi d'adresses IP (Est-il utilisé ou pas ?)
- De la Gestion d'IP (IP disponibles, réservation d'IP DHCP)
- Automatisation des tâches d'administration (enregistrement DNS, config DHCP)
- Découverte Automatique (IP, DNS)

La solution qui m'a été demandée est PHPIPAM et sur lequel j'ai travaillé en toute autonomie.

Ce dernier est une solution gratuite et Open Source, elles possèdent de nombreuses caractéristiques.

- ✓ Gestion d'adresse IPv4/IPv6
- ✓ Gestion des Sections/Sous-réseaux
- ✓ Affichage automatique de l'espace libre des sous-réseaux
- ✓ Affichage des sous-réseaux (diagramme)
- ✓ Scan automatique des sous-réseaux/ Verification du status IP
- ✓ Intégration PowerDNS
- ✓ Support NAT
- ✓ Gestion des baies d'urbanisation
- ✓ Domaine d'authentification (AD, LDAP)
- ✓ Permission section/sous-réseaux par groupe
- ✓ Appareil/Type d'appareil management
- ✓ Import de sous-réseaux RIPE
- ✓ Import de sous-réseaux par fichier XLS/CSV
- ✓ Module IP
- ✓ API REST
- ✓ Gestion VLAN
- ✓ Gestion VRF
- ✓ Calculateur IPv4/IPv6
- ✓ Recherche IP dans la base de données
- ✓ Notification par E-mail
- ✓ Support d'onglets personnalisé
- ✓ Traduction (plusieurs langages)
- ✓ Log

Ce projet est décomposé en quatre grandes étapes :

- Création d'une Machine Virtuelle
- Installation (Paquets PHP, MySQL, PHPIPAM, Apache)
- Mise à jour PHPIPAM
- Configuration / Import

1. Création d'une machine virtuelle

Phpipam est une solution fonctionnant uniquement sur le système d'exploitation « Linux » et l'outil « Virtual Box » propose de créer des machines virtuelles sous n'importe quel système d'exploitation.

J'ai donc combiné les deux afin de créer ma VM sous Linux (debian) dans le but de réaliser ce projet.

2. Installation

L'installation d'un logiciel comme celui-ci nécessite l'installation de divers outils et paquets tels que :

- Phpipam (outil phpipam web)
- MySQL (base de données)
- Apache (Serveur http Open-Source

3. Mise à jour

   Une fois le logiciel installé et fonctionnel, réaliser les mises à jour est nécessaire afin d'avoir accès aux dernières fonctionnalités de la solution ainsi que de résoudre les diverses erreurs et failles de sécurité des premières versions.

   Pour réaliser cette étape, il fallait :

- Récupérer les fichiers de MAJ sur le site de l'éditeur
- Intégrer le fichier de MAJ dans le répertoire local /var/www/html
- Intégrer le fichier « UPDATE.sql » dans la base de données (MySQL)
- Vérifier le bon fonctionnement de la montée de version

La version d'installation est la 1.0, le but était d'aller en 1.5, de plus il est nécessaire de savoir que les montées de version se font une par une.

Durant l'étape des montées de version, plusieurs problèmes ont été rencontrés issues de la base de données qui nécessitaient des analyses et corrections. La version finale qui a été atteinte est la 1.4 due à de divers problèmes d'affichage de la version 1.5.

En annexe l'installation détaille (Rapport d'installation et de MAJ en annexe)

4. Configuration / Import

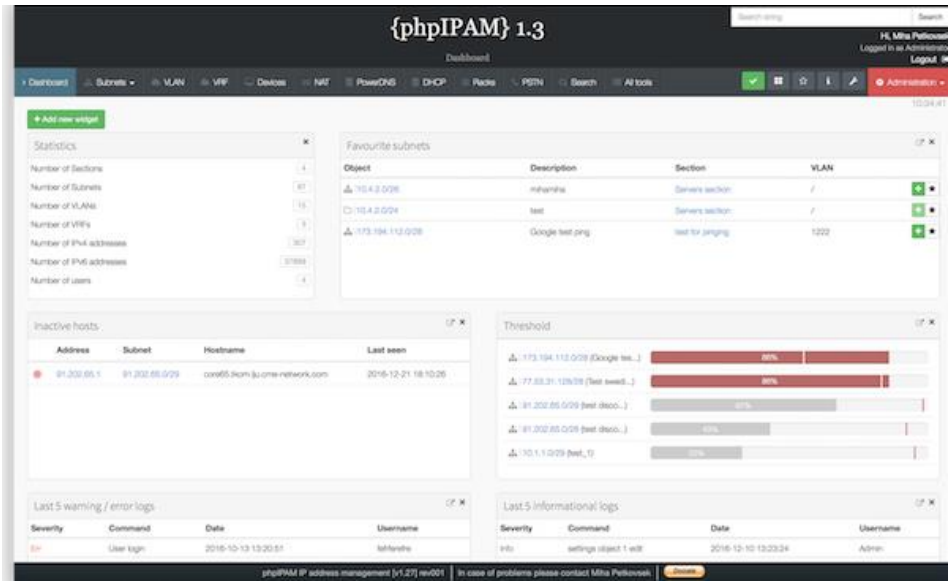

Figure 13 : Tableau de bord PHPIPAM

La configuration de l'outil PHPIPAM passe autant par des configurations générales telles que le langage du site, nom d'affichage, activation des modules nécessaires que par des configurations plus précises et personnelles, selon les cas d'usage comme la localisation, droits et authentification des utilisateurs, mise en place des différents réseaux et sous-réseaux.

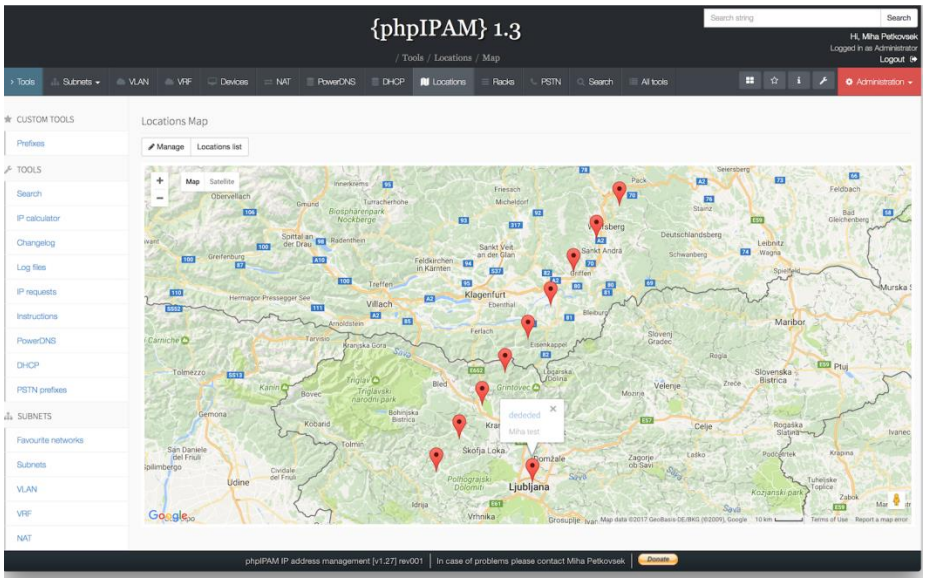

Figure 14 : Onglet de localisation

Enfin, l'import des données d'un fichier Excel de l'entreprise dans PHPIPAM. Pour cela, on m'a fourni un fichier contenant les différentes IP, VLAN, Sous-Réseaux, équipements de l'entreprise que j'ai adapté pour qu'il soit lisible par PHPIPAM (disposition des données, format du fichier)

Il est intéressant de savoir que les différentes options de PHPIPAM permettent aussi de faire de la supervision d'adresses IP.

Une fois la solution opérationnelle, j'ai eu l'occasion d'effectuer deux présentations :

- La première avec les membres de l'équipe réseaux, afin de leur exposer les possibilités de la solution, de répondre à leurs questions et de pouvoir m'aiguiller sur les points incompris pour que je puisse y faire des recherches.

- Puis j'ai eu l'opportunité de présenter cette solution aux différents responsables de chaque service de la DSI, dans le but de leur présenter la solution mais aussi afin de leur montrer l'un des différents sujets réalisés durant mon stage.

III / Mes Diverses Missions

A / Participation aux différents sujets en cours que traite l'équipe réseaux

J'ai eu la chance durant mon stage de participer à plusieurs réunions en visioconférences via l'outil « Teams »

- Avec des représentants de Fortinet pour nous présenter leurs produits ainsi que leurs solutions (2h)
- Présentation du concept « SD-WAN » (2h)
- L'entreprise RestorePoint, présentant une solution de sauvegarde de configuration d'équipement. Présentation en anglais (1h30)

Cela m'a permis d'élargir mes connaissances par le biais de nombreuses sessions de recherches afin d'approfondir mes sujets mais aussi de découvrir des concepts, constructeurs, équipements…

B / Switch Cisco 3750

L'objectif de ma première tâche était de réinitialiser 7 switch cisco 3750, afin qu'ils servent d'équipements de secours lors d'une maintenance électrique dans les locaux techniques.

Figure 15 : Switch Cisco 3750

La réalisation de cette tâche m'a permis de mettre en pratique les compétences acquises en TP.

Une fois connecté à l'équipement, voici les commandes à effectuer

- *« delete vlan.dat » (pour supprimer toutes les vlans car elles sont stockées dans la flash de l'équipement*
- *« Erase startup-config » (supprime la configuration de l'équipement)*
- *« reload »* (*redémarre* l'équipement et applique donc toute la réinitialisation)

C / Palo Alto (PA-220)

Les divers objectifs étaient :

- Mise en place de règles de sécurité
- Mise à jour de deux pare-feux.

Ces pare-feux sont destinés à remplacer deux autres pare-feux de la marque « Juniper ».

Figure 16 : Palo Alto, PA-220

Etape 1 : Réaliser une cinquantaine de règles de sécurité.

On se connecte sur internet via l'IP par défaut, puis une fois identifié, on arrive sur un tableau de bord

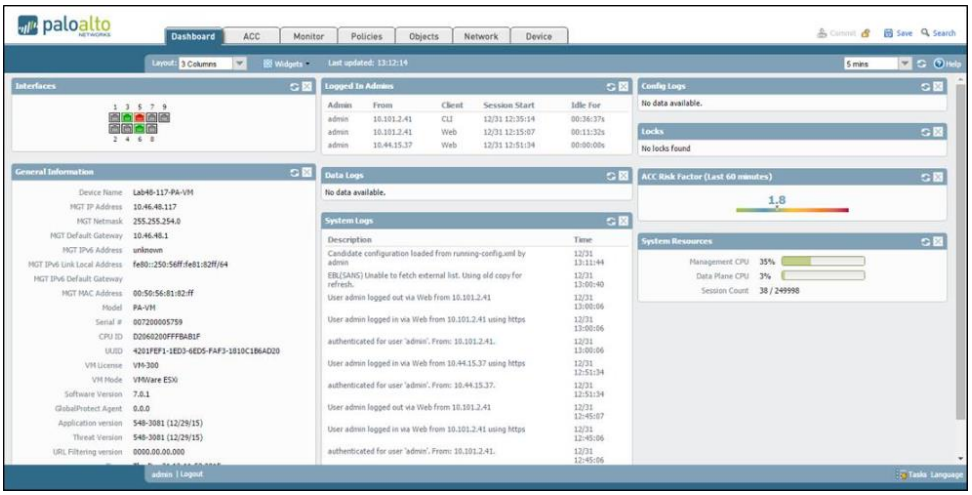

Figure 17 : Tableau de bord Palo-Alto

Ma mission était de configurer des règles de sécurité, pour cela j'avais accès à un fichier de règles de sécurité d'un autre équipement.

		Source				Destination				
Name	Tag	Zone	Address	User	HIP Profile	Zone	Address	Application	Service	Action
Trust-Untrust	Outbound	L3-Trust	any	any	any	L3-Untrust	any	any	any	✓
Any-Untrust	Outbound untrust	any	any	any	any	L3-Untrust	any	ssl web-browsing	any	✓
Untrust-Trust	Inbound	L3-Untrust	any	any	any	L3-Trust	Server_1	any	any	✓
Untrust-DMZ	Inbound	L3-Untrust	any	any	any	L3-DMZ	Server_DMZ	any	any	✓
Trust-DMZ	Intra-zone	L3-Trust	any	any	any	L3-DMZ	any	any	any	✓
DMZ-Trust	Intra-zone	L3-DMZ	any	any	any	L3-Trust	any	any	any	✓

Figure 18 : Tableau des règles de sécurité Palo Alto (exemple Internet)

Etape 2 : Réaliser les mises à jour sur les deux Palo Alto

Pour commencer, il est important de bien consulter et analyser quelle version choisir.

Cela nécessitait de prendre en compte plusieurs facteurs :

- Connaître les apports de chaque version
- Connaître les CVE (Common Vulnerabilities and Exposures) de chaque version
- Méthode à utiliser pour faire les montées de versions

Une fois les recherches terminées, il y avait trois méthodes disponibles :

- Avoir accès à internet sur le pare-feu et lancer les mises à jour directement dessus
- Récupérer les fichiers de mise à jour sur le site officiel de Palo Alto puis les importer sur le pare-feu et lancer les mises à jour
- Envoyer un mail au support de Palo Alto pour leur demander les fichiers pour une montée de version

Après avoir étudié le sujet, j'ai choisi la première méthode car c'est un bon moyen de prendre en main et comprendre l'équipement.

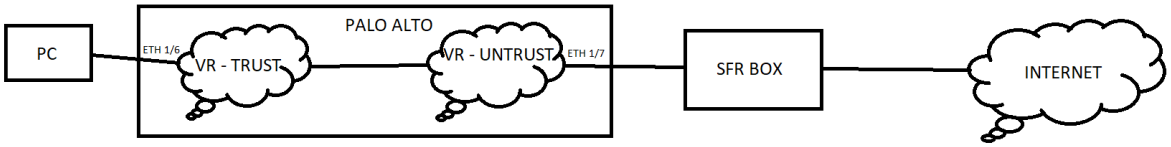

Figure 19 : Représentation de l'architecture mise en place pour obtenir internet

J’ai pris le temps de bien étudier l’équipement et j’ai découvert que la mise en place de cette tâche nécessitait quelques étapes :

- Comprendre le principe de zone TRUST et UNTRUST
- Configuration de l’interface qui a accès à internet
- Configuration de l’interface connectée à mon PC pour que j’ai accès à internet
- La/les route(s) des routeurs virtuels attribués aux interfaces
- Règle de sécurité à mettre en place à autoriser les différents flux à entrer/sortir du réseau
- NAT à réaliser pour autoriser le flux de la box internet à aller jusqu’à mon PC
- DNS à configurer
- Créer un profil Management à attribuer à chaque interface pour manager le palo Alto sur une autre interface que celle de management ainsi qu’autoriser le ping sur les interfaces.

Une fois effectué, il fallait réaliser la même chose avec le deuxième Palo-Alto, grâce à la fonction High Availability (Haute Disponibilité) qui permet la synchronisation entre les deux équipements, la configuration pour obtenir internet était déjà faite. Les mises à jour ont pu être réalisées plus vite sur le deuxième équipement du fait qu’il n’était pas nécessaire de tout reconfigurer.

Ces deux équipements n’auront pas été mis en production tout de suite après ma mission du fait qu’il fallait vérifier mes règles de sécurité et réaliser des configurations supplémentaires.

D / CISCO BE7000M UCS C240M5SX

Une autre tâche annexe étant d'aider un membre de l'équipe réseau à installer un UCS dans une des baies du siège ONET, cet UCS est un serveur permettant l'hébergement de machines virtuelles qui fournissent des services de TOIP.

Le but était d'alléger la charge de requête des deux autres serveurs TOIP déjà actif et d'avoir un serveur synchronisé avec les deux autres en y ajoutant un troisième.

Figure 20: CISCO BE7000M UCS C240M5SX

Dans cette tâche j'ai eu l'occasion de visiter le local Télécom du siège ONET

Figure 21 : Exemple de baie de brassage

IV / CONCLUSION

Ce stage de 10 semaines fut une expérience très enrichissante tant sur le plan professionnel que personnel.

Au niveau professionnel, j'ai pu appréhender les aspects du métier de Technicien réseau, notamment les règles de sécurité à respecter, les différentes procédures à suivre.

Sur le plan personnel, j'ai appris à adopter une attitude professionnelle en entreprise. Au travers des différents projets, l'autonomie est un point sur lequel il faut que je m'améliore, plus structurer mes plans d'action et surtout être plus à l'aise lors de présentations.

J'ai vécu une expérience réellement enrichissante au sein de l'équipe réseau qui me permet aujourd'hui d'avoir une vision plus claire du monde de l'entreprise.

En conclusion à l'issue de mon DUT, je compte continuer vers la licence professionnelle en alternance (alternance qui se fera probablement dans les équipes réseaux d'ONET).

V / Abréviation et Glossaire

- **CISCO SYSTEM** (Constructeur d'équipement réseau).
- **CVE** (Common Vulnerabilities and Exposures) Dictionnaire d'informations publiques relatives aux vulnérabilités de sécurité.
- **DNS** (Domain Name System) service informatique distribué utilisé qui traduit les noms de domaine Internet en adresse IP.
- **DSI** (Directeur des Systèmes d'informations).
- **DSIN** (Direction du système d'information et du numérique).
- **FORTINET** (Constructeur d'équipement, logiciel et services de cyber-sécurité).
- **GIE** (Groupe d'intérêt économique).
- **LAN** (Local area network) réseau situé dans une petite zone géographique, généralement dans le même bâtiment.
- **NAT** (Network Address Translation) transformation d'adresse IP en d'autre adresse IP.
- **Open Source :** Logiciel/Solution accessible à tous et tout le monde peut collaborer pour l'améliorer.
- **PALO ALTO** (Entreprise spécialisée dans les services de sécurité pour les réseaux et les ordinateurs).
- **PRTG** (Paessler Router Traffic Grapher) est un logiciel commercial de supervision.
- **SD-WAN** (*Software-Defined Wide Area Network)* réseau étendu à définition logicielle.
- **SNMP** (Simple Network Management Protocol) Protocole d'administration réseau de couche 7 du modèle OSI.
- **SUPERVISION** surveillance de manière continue de la disponibilité des services en ligne, du fonctionnement, des débits, de la sécurité mais également du contrôle des flux.
- **SWITCH** (Commutateur) équipements réseau.
- **TOIP** (Téléphony Over Internet Protocol) technologie informatique qui permet de transmettre la voix sur des réseaux compatibles IP**.**
- **UCS (**Cisco Unified Computing System) est une gamme de produits informatiques pour serveurs de centre de données composée de matériel de serveur, de prise en charge de la virtualisation, de matrice de commutation et de logiciels de gestion.
- **WAN** (Wide area network) réseau couvrant une zone géographique de grande envergure.

VI / Bibliographies

https://www.paessler.com (PRTG site official)

https://www.paloaltonetworks.com (Palo Alto Officiel)

https://security.paloaltonetworks.com/ (CVE Palo Alto)

https://oidref.com/ (MIB Equipements)

https://www.paessler.com/manuals/prtg/define_lookups#customizing
(Capteur personnalisé en XML)

https://phpipam.net (Site officiel de PHPIPAM)

https://fr.wikipedia.org/wiki/R%C3%A9seau_priv%C3%A9_virtuel (Doc VPN)

https://fr.wikipedia.org/wiki/Interface_de_programmation (Renseignement sur les API)

https://fr.wikipedia.org/wiki/Representational_state_transfer (Style d'architecture d'API)

https://fr.wikipedia.org/wiki/Proxy (Renseignement sur les Proxy)

https://fr.wikipedia.org/wiki/Multiprotocol_Label_Switching (Renseignement MPLS)