BARTHELEMY Lilly-Rose
Terminale Baccalauréat Professionnel

Systèmes Numériques : option Réseaux Informatiques et Systèmes Communicants

Rapport d'activité en entreprise

Promo 2025

Maitre d'apprentissage et Tuteur : Christophe DOUET
Adresse de l'entreprise : 2E rue Abraham Lincoln 44110 Chateaubriant
Adresse du centre de Formation : 27 rue du Ballet – 44000 Nantes

Remerciements :

Je remercie l'entreprise Keysource, de m'avoir accueilli si chaleureusement et m'avoir formé avec patience durant ces deux années.

Je remercie aussi Mme TOCQUE qui m'a aidé à effectuer mes recherches d'entreprise et d'avoir contacté Keysource.

Merci à M. PERRIGAUD et M. DOUET de m'avoir acceptée en tant qu'alternante dans leur entreprise. Mais aussi d'avoir pris le temps de m'aider et de m'expliquer les points essentiels à certaines tâches qui m'ont été confiées.

Un grand merci à l'équipe de Keysource pour leur gentillesse et bienveillance envers moi et aussi pour cette bonne ambiance collective.

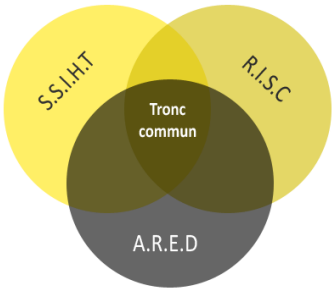
Merci à tous de m'avoir acceptée dans l'entreprise et de m'avoir intégrée avec patience et gentillesse.

Ensemble St Félix-La Salle
Nantes

Table des matières

1. Introduction

Le Bac professionnel Systèmes Numériques se décompose en 3 options distinctes :



- Sûreté et Sécurité des Infrastructures de l'Habitat et du Tertiaire (SSIHT) : tout ce qui est lié à la domotique liée à la gestion technique de maison et gestion intelligente des bâtiments.

- Audiovisuel, Réseaux et Equipements Domestiques (ARED) : tout ce qui est lié à l'éclairage et sonorisation ainsi que la domotique liée au confort.

- Réseaux Informatiques et Systèmes Communicants (RISC) : tout ce qui est lié aux télécommunications et réseaux ainsi que l'électronique industrielle et embarquée.

Etant en Bac Professionnel Systèmes numériques option RISC, mon lycée, Saint Félix La Salle, propose la continuité de ce parcours de baccalauréat en alternance avec une entreprise ayant un parc informatique.
Pour ma part, j'ai eu l'occasion de faire mon alternance, durant les deux dernières années, dans une entreprise nommée Keysource.

Ainsi, l'entreprise dans laquelle j'ai pu effectuer mon alternance est une Société de Services en Ingénierie Informatique, c'est-à-dire qu'elle est prestataire externe des entreprises pour le domaine informatique.

Pendant ces deux années, j'ai pu devenir technicienne systèmes et réseaux, qui est un des métiers qui m'intéresse le plus dans l'avenir.

Mon but dans cet apprentissage était d'en apprendre plus dans l'administration de réseau, dépanner des utilisateurs sur différents problèmes, liés par exemple à des problèmes logiciels ou problèmes matériels.

La suite de mon rapport sera constituée d'une présentation de l'entreprise dans laquelle j'ai travaillé durant deux ans. Puis, j'approfondirai sur quatre activités que j'ai effectuées durant ces 2 années, suivi de la présentation de la grande activité que j'ai choisie, et enfin ma conclusion sur ces années.

2. Présentation de l'entreprise

2.1. Histoire et lieu du siège

Keysource est née de la fusion de Keysource France créée à Paris en 2005, et MPI'nformatique créée à Châteaubriant, dans le siège actuel, en 1994.

C'est en 2008 qu'a lieu le rachat de MPI'nformatique par Keysource, entraînant le déménagement de cette dernière à Châteaubriant.

Mais ce n'est qu'en 2017 que les deux entités deviennent une seule entreprise : Keysource.

Enfin, en 2022, Keysource France est rachetée par les deux dirigeants actuels : Christophe DOUET et Frédéric PERRIGAUD.

Le siège de l'entreprise se trouve au sud-ouest de Châteaubriant, au 2E rue Abraham Lincoln.

2.2. Quelques chiffres clés

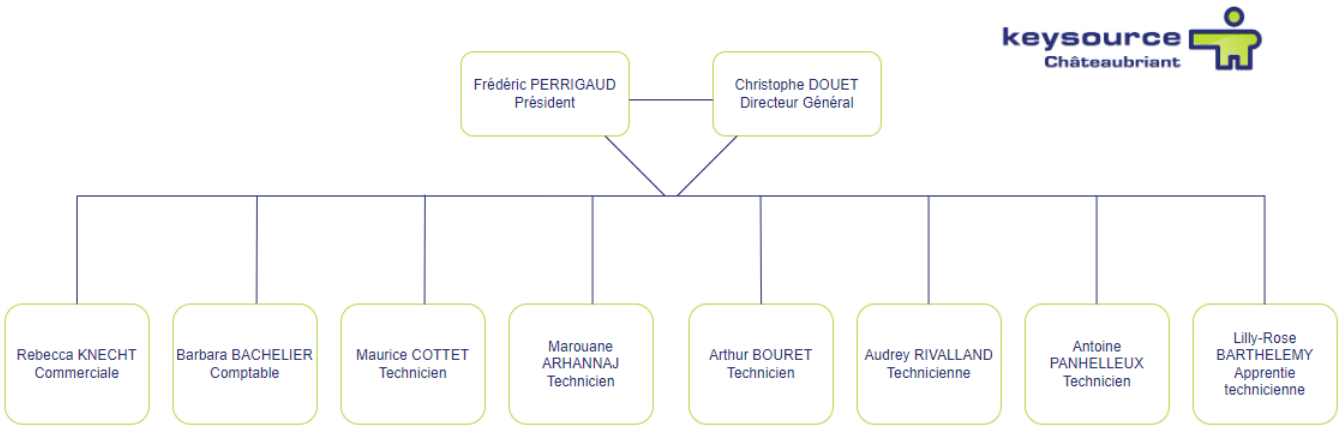
Avec désormais près de 18 ans d'expérience dans le domaine des réseaux informatiques, Keysource emploie un total de 10 salariés, alternants inclus.

Le chiffre d'affaires de Keysource est conséquent : en 2023, l'entreprise a réalisé un chiffre d'affaires de 1 525 000 € pour environ 1 658 tickets traités.

Nos clients sont principalement des professionnels, représentant près de 99 % de notre clientèle. Le dernier pour cent correspond donc à des particuliers.

2.3. L'organisation de Keysource

Voici entre autres l'organigramme de Keysource :



Il est constitué tout d'abord de Fréderic PERRIGAUD et Christophe DOUET, les dirigeants de Keysource, puis de tous les salariés, directement sous leur responsabilité.

Alors que la quasi-totalité des salariés sont des techniciens, certains se distinguent par des fonctions spécifiques, comme Rebecca KNECHT, commerciale et standardiste, ou Barbara BACHELIER, comptable de Keysource.

2.4. Les services proposés par Keysource

Keysource est une Société de Services en Ingénierie Informatique, autrement connue sous le nom de SS2I. Elle agit donc comme un prestataire externe pour ses clients.

Les services proposés par Keysource sont variés : supervision, infogérance, réseau, sécurité, téléphonie, et enfin, le service le plus important : l'hébergement en datacenter.

Tous ces services sont modulables selon les besoins des clients.

Au sein de Keysource, les administrateurs et techniciens gèrent les problèmes rencontrés par les clients bénéficiant d'un contrat de maintenance.

La majorité des clients sont des professionnels, les autres étant des clients particuliers de longue date.

On m'a installé à un bureau dans l'atelier pendant ces deux années, et on m'a attribué un téléphone IP ainsi qu'un PC portable, plus pratique pour les interventions.

Le téléphone est le moyen le plus courant pour signaler un problème. Ces problèmes peuvent varier : d'un simple dysfonctionnement logiciel à une panne complète du réseau de l'entreprise.

Sinon, pour les demandes spécifiques et les commandes, les clients passent par e-mail.

2.5. Les outils utilisés par Keysource

Pour intervenir à distance sur les postes des clients, nous utilisons un outil appelé **AnyDesk**. Celui-ci fonctionne avec un code que l'utilisateur doit fournir pour que nous puissions prendre la main sur son poste.

Toutefois, si le problème ne peut être résolu à distance, une intervention peut être envisagée sur le site du client, ou bien le poste concerné peut nous être apporté en atelier.

Chaque demande entraîne la création d'un ticket, qui peut être créé soit en interne, soit par un client disposant d'un accès à notre outil de gestion de tickets : **KSticket**.

Par ailleurs, pour prendre la main sur l'un des serveurs clients hébergés dans notre datacenter, nous utilisons un outil appelé **mRemote**. Il nous permet, entre autres, de nous connecter à toutes sortes de machines appartenant à nos clients.

Enfin, pour assurer le bon monitoring des serveurs, pare-feu, sauvegardes, et autres services clients, nous utilisons **Centreon**. Cet outil sera abordé plus en détail dans la partie relative à mes activités.

Des images de ces différentes interfaces sont disponibles en annexe 1.

3. Compte-rendu des activités

Pour information, pour des fins de sécurité, toutes les adresses IP, informations sensibles et noms de clients sont anonymisés à partir d'ici.

3.1. Préparation typique d'un poste

Avant toute chose, il faut savoir que l'un de nos partenaires principaux est le constructeur Dell. Ainsi, tous les postes destinés à nos clients proviennent de chez Dell, qu'il s'agisse de tours ou de PC portables.

Une préparation "typique" d'un poste débute à la suite d'une commande client. Bien sûr, chaque client a ses spécificités, notamment en ce qui concerne les applications à installer et les accès à configurer. Tout est précisé dans le bon de commande. Le poste est ensuite préparé à l'atelier chez Keysource.

3.1.1. Installation de Windows et mises à jour

La première étape consiste à installer Windows. Rien de très compliqué ici : il suffit d'allumer le poste, et le programme d'installation de Windows se lance automatiquement. On choisit alors « Français » pour la langue, le pays, et la disposition du clavier.

On connecte ensuite le poste au Wi-Fi du client, si celui-ci en possède un dans notre point d'accès Wifi, une étape importante pour la suite.

Après quelques mises à jour, vient la demande de connexion à un compte Microsoft. Comme nous n'en avons pas besoin, nous passons par les options avancées de « Compte professionnel ou scolaire » pour sélectionner « Joindre un domaine à la place ».

Une fois l'installation terminée, on se connecte avec le compte administrateur local, qui est alors créée durant l'installation de Windows, pour lancer les dernières mises à jour via Windows Update. On pense également à passer sur le site de Dell Support pour mettre à jour les drivers spécifiques au poste.

Le poste est maintenant à jour, on peut passer à l'étape suivante.

3.1.2 Désinstallation des applications par défaut et intégration dans le domaine

Chez Keysource, nous désinstallons systématiquement les applications par défaut de Dell, Office, et OneNote. Les applications Dell sont souvent sources de lenteurs, et de nombreuses langues inutiles sont installées avec Office comme l'allemand, l'italien, le néerlandais, et autres langues.

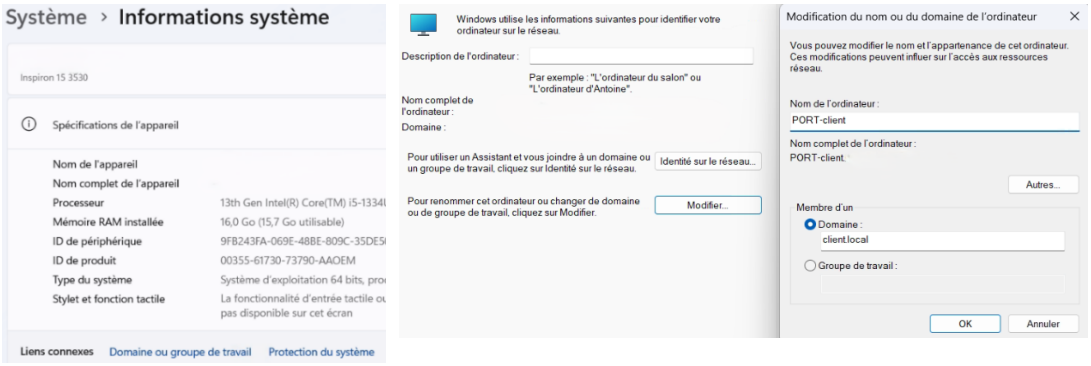
Pour une installation propre, nous retirons donc tout cela depuis le panneau de configuration via « Désinstaller un programme ». Une fois les logiciels superflus supprimés, on installe les outils essentiels :

- Google Chrome
- AnyDesk
- Foxit Reader

Vient ensuite l'intégration dans le domaine du client.

Pour cela, on va dans Paramètres > Système > Informations système > Domaine ou groupe de travail > Modifier.

Par défaut, le poste est dans le groupe de travail « WORKGROUP ». On sélectionne alors « Domaine » et on renseigne celui du client. Attention, il est essentiel à ce moment d'être connecté au bon Wi-Fi pour accéder au domaine.



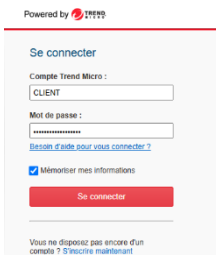
Une fenêtre s'ouvre pour saisir les identifiants de l'administrateur du domaine. Une fois la jonction faite, on peut continuer.

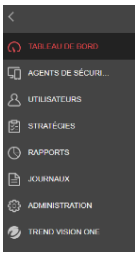
3.1.3. Installation de l'antivirus, du VPN et mise du raccourci RDS

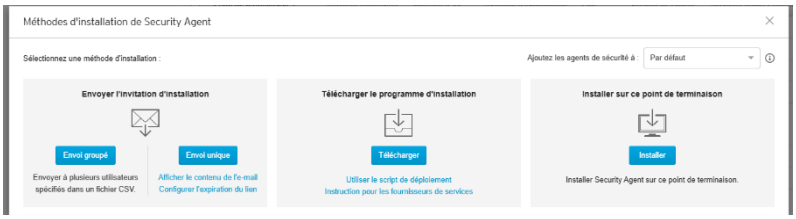
L'antivirus est essentiel. Celui de Windows est correct, mais nous utilisons Trend Micro, bien plus adapté à une gestion centralisée.

Chaque client possède sa propre console Trend Micro. On y accède via un tableau de bord affichant les licences, menaces détectées, etc.

Pour l'installation, on passe par « Agents de sécurité » > « Ajouter des agents de sécurité ».







Un menu s'ouvre, nous laissant 3 choix. Puisque pour l'instant nous n'avons pas configuré la session de notre client, et n'avons plus Office, nous ne pouvons pas lui envoyer par mail.

Aussi, cette manipulation n'étant faite sur le poste de l'installeur, nous n'allons pas choisir la dernière option. C'est donc celle du milieu que nous allons prendre.

Ensuite pour le mettre sur le poste en préparation, je le stocke dans ma clé USB.

Un RDS (Remote Desktop Services) est un service de Windows Server permettant à plusieurs clients d'une même entreprise d'avoir une session centralisée sur le serveur. Toutes les applications nécessaires y sont donc installées et maintenues à jour.

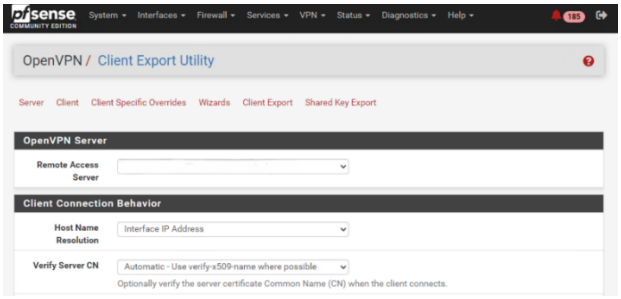
Ce fonctionnement réduit fortement les problèmes liés aux mises à jour des applications car elles sont toutes sur un serveur au lieu de chaque poste utilisateur de l'entreprise. Les utilisateurs sont donc connectés en bureau à distance sur leur serveur où ils retrouveront leurs logiciels métier.

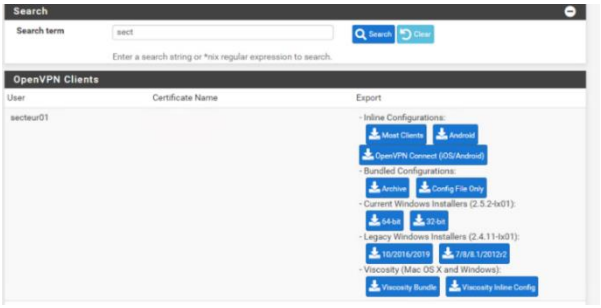
La majorité de nos clients possèdent au moins un RDS. Ceux possédant plus d'un serveur possèdent un serveur spécifique permettant de répartir la charge des utilisateurs sur les 2 ou 3 serveurs. Ce serveur est alors nommé Broker.

On ajoute alors le raccourci du serveur sur la clé USB avec le Trend.

Dernière étape : l'installation du VPN pour permettre une connexion à distance pour le télétravail ou les déplacements.

Pour ceci, on se connecte au firewall du client via mRemoteNG. Tous nos firewalls sont des pfSense.





On crée un utilisateur dans le User Manager, avec login/mot de passe identique à la session utilisateur, puis on coche « Create user certificate ».

Ensuite, dans OpenVPN > Client Export, on sélectionne le bon profil client et on génère un installeur Windows 64 bits, il est alors ajouté au dossier avec les autres.

On est prêt à les installer sur le poste.

3.1.4. Création de l'utilisateur dans l'Active Directory et configuration de la session.

Pendant que les installations s'effectuent, on se connecte au serveur Active Directory (AD) via mRemoteNG. Souvent, on copie un profil existant pour récupérer les bons groupes et permissions. Sinon, on crée le compte de zéro à partir des infos fournies par le client.

Une fois le compte créé, on se connecte avec cet utilisateur sur le poste et sur le RDS.

On termine la configuration :

- Navigateur Internet
- Mot de passe VPN enregistré
- Softphone (si nécessaire)
- Foxit en lecteur PDF par défaut
- Configuration imprimante
- Configuration des logiciels métier (base de données, etc.)

À ce stade, le poste est prêt à être livré au client.

3.2. Gestion de ticket (cas fusion boite mail)

Comme toute bonne SS2I, nous traitons les demandes de nos clients, ce qui génère des tickets. Je vais ici détailler l'un des tickets que j'ai dû gérer seule : un cas de fusion de boîtes mail. Cette demande faisait suite à une sur-création de boîtes mail pour les commerciaux, entraînant une sur-attribution de boîtes en archive.

Pour remédier à cette situation, le responsable de l'entreprise a décidé de ne conserver que deux boîtes mail : **Secteur01** et **Secteur02**.

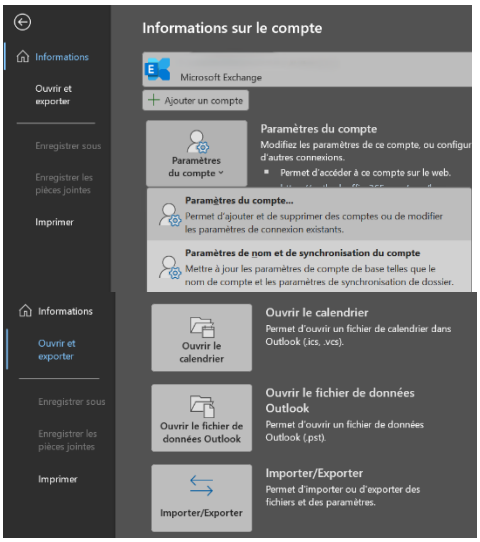
3.2.1. La recopie des mails

Les anciens commerciaux ayant quitté l'entreprise, leurs boîtes mail ont été transformées en boîtes partagées, attribuées à de nouveaux commerciaux. Maintenant que seules deux boîtes sont utilisées, il faut récupérer le contenu des anciennes.

Pour cela, on accède à la console Office 365 du client afin de déléguer les boîtes partagées à **Secteur01** ou **Secteur02**, selon les besoins.

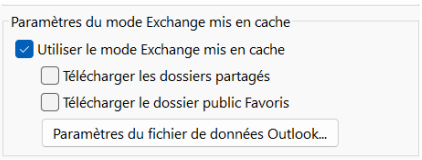
Dans notre cas :

- **Secteur01** récupère les mails de *commercial1*
- **Secteur02** récupère ceux de *commercial2* et *commercial3*



Une fois les délégations effectuées, on se connecte à Outlook avec le compte **Secteur01** ou **Secteur02**.

Avant de commencer la manipulation, un paramètre doit être ajusté pour garantir que l'intégralité de la boîte partagée soit visible. Il faut se rendre dans : **Fichier > Paramètres du compte > Paramètres du nom et de la synchronisation du compte > Paramètres supplémentaires > Avancé**, puis **décocher "Télécharger les dossiers partagés"**.



On suit ensuite le chemin suivant : **Fichier > Ouvrir et exporter > Importer/Exporter > Exporter des données vers un fichier > Fichier de données Outlook (.pst)**, puis on sélectionne la boîte mail à exporter.

Après avoir défini l'emplacement de l'export, Outlook effectue l'opération (ce qui peut prendre du temps).

Une fois l'export terminé, on revient dans le même menu, mais cette fois-ci pour **importer** le fichier .pst. On choisit : **Importer à partir d'un autre programme ou fichier > Fichier de données Outlook (.pst)**, puis on indique le chemin d'accès vers le fichier précédemment créé.

Après une nouvelle attente, tous les éléments de l'ancienne boîte sont désormais présents dans la nouvelle. Il suffit de répéter cette opération autant de fois que nécessaire. L'unique problème étant survenu était le fait que le compte du commercial3 était déjà supprimé et donc il était impossible de retrouver ses mails.

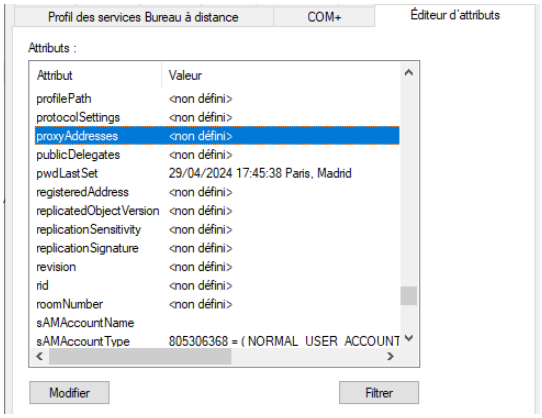
3.2.2. La mise en alias des comptes.

Les boîtes mail Microsoft 365 sont synchronisées avec l'Active Directory (AD) du client, qui gère le parc informatique.

Maintenant que les boîtes des anciens utilisateurs ne sont plus utilisées, nous devons créer des alias pour rediriger les mails vers les nouveaux comptes. Par exemple, *commercial1* doit devenir un alias de **Secteur01**.

Pour cela, il faut suivre plusieurs étapes afin d'éviter toute rupture de synchronisation avec l'AD :

1- **Renommer l'utilisateur** à mettre en alias par exemple : commercial1 devient commercial1old, puis forcer une synchronisation avec la commande PowerShell appropriée.



2- Une fois la modification visible dans la console Office 365, retourner dans l'AD sur le compte modifié (*commercial1*).

- Dans **Éditeur d'attributs**, si l'attribut **proxyAddresses** contient une valeur, modifier **SMTP:commercial1@domaine.com** en **SMTP:commercial1old@domaine.com**.
- Refaire une synchronisation.
- Si l'attribut est **<non défini>**, passer à l'étape suivante.

3- Désactiver le compte de l'utilisateur et le déplacer dans **Utilisateurs supprimés**.

Ensuite, sur le compte de destination (**Secteur01**), ouvrir l'**Éditeur d'attributs**, puis dans **proxyAddresses**, ajouter les valeurs suivantes :

- SMTP:Secteur01@domaine.local (adresse principale)
- smtp:commercial1@domaine.local (alias)

Après une dernière synchronisation, on peut vérifier dans la console Office 365 que l'adresse alias apparaît bien sur le compte **Secteur01**, confirmant que la fusion a réussi.

Il ne reste plus qu'à reproduire cette procédure pour **Secteur02**, et le ticket pourra être clôturé.

```
PS C:\Users\administrateur            Start-ADSyncSyncCycle -PolicyType Delta

 Result
 ------
Success
```

3.3. Préparation de téléphone pour client

Pour l'un de nos plus grands clients, un serveur de téléphonie basé sur **FreePBX** a été mis en place. Plusieurs numéros y sont configurés, correspondant aux différents sites utilisant la téléphonie IP.

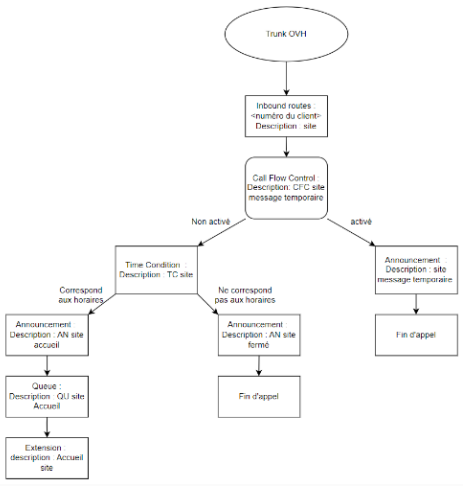
Cependant, le site de **Le Luart** n'en disposait pas encore. C'est à ce moment que **Keysource** est intervenu pour déployer la téléphonie sur ce site.

3.3.1. La structure du schéma téléphonique

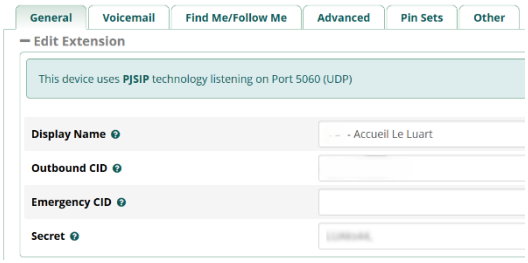
Le serveur étant déjà opérationnel, notre tâche a consisté à migrer leur numéro de téléphone sur OVH, configurer le scénario d'appel et préparer des téléphones fixes, des Grandstream GXP2140.

Dans un premier temps, mes collègues **M. Perrigaud** et **M. Douet** ont procédé à la migration du numéro principal du standard, depuis l'ancien opérateur vers **OVH**. Cette étape engendre un délai de quelques jours avant la bascule effective. Cela nous laisse donc ce temps de bascule pour faire la préparation.

Chez Keysource, afin de clarifier la configuration et les étapes à suivre, nous réalisons des schémas préalables définissant les objectifs avant toute intervention sur le serveur de téléphonie.



Nous abordons le schéma **de bas en haut**, en commençant par la création des postes téléphoniques, un pour l'accueil et l'autre pour les commerciaux. L'accueil étant le seul à devoir recevoir les appels entrants, c'est sur ce poste que nous allons nous concentrer ici.



Pour une gestion plus propre et évolutive, notamment en cas d'ajout futur de postes, nous créons une **Queue** (file d'attente) ne contenant que l'extension de l'accueil.

Ensuite, nous configurons les **Annoncements**, qui permettent de définir qui prend en charge les appels entrants. L'annonce principale **AN-accueil** redirige les appels vers la Queue, tout en diffusant un message d'accueil.

En parallèle, nous créons deux autres Annoncements :

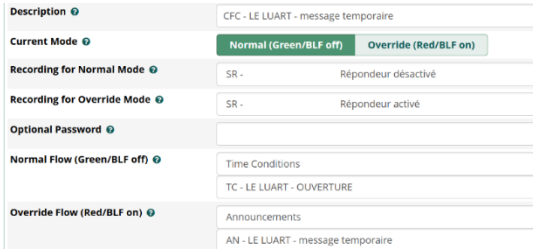
- **AN-fermé** : utilisé hors des heures d'ouverture, il raccroche automatiquement.
- **AN-message temporaire** : utilisé en cas d'absence exceptionnelle.

AN - LE LUART - ACCUEIL	Queues: 1420 QU - LE LUART ACCUEIL
AN - LE LUART - fermé	Terminate Call: Hangup
AN - LE LUART - message temporaire	Terminate Call: Hangup

Les appels passent ensuite par une **Condition horaire**, définie via un **Groupe de temps** précisant les heures d'ouverture :

- Du lundi au jeudi : **07h00–12h00** et **13h30–17h00**
- Le vendredi : fermeture à **16h30**

Pendant les horaires d'ouverture, les appels sont redirigés vers le téléphone de l'accueil via la Queue. En dehors de ces horaires, c'est l'annonce **AN-fermé** qui prend le relais.



Nous mettons également en place un **Call Flow Control**, permettant à l'utilisateur (par exemple, en cas de congé) de basculer manuellement tous les appels vers l'annonce **AN-message temporaire**, via un bouton préprogrammé.

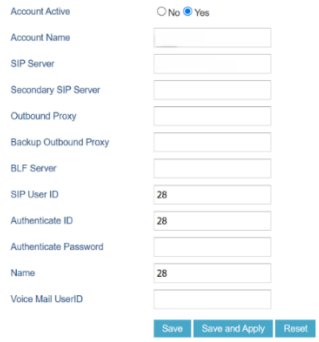
Enfin, nous créons une **Inbound Route**, correspondant au numéro de téléphone du site. Cette route est configurée pour rediriger les appels entrants vers le Call Flow Control.

La configuration du serveur de téléphonie étant achevée, deux étapes restent à effectuer la configuration des téléphones et la création des enregistrements d'accueil, de message temporaire et de fermeture pour les Annoncements.

3.3.2. La configuration des téléphones

Nous disposons de **deux téléphones Grandstream GXP2140** et d'un **extendeur** destiné au poste de l'accueil. L'extendeur est un module additionnel qui se connecte au téléphone, permettant, via des touches programmables, de lancer des appels ou de transférer vers des lignes définies.

Alors en préparation à l'atelier, nous allons les brancher sur le réseau administratif, ayant accès à leur serveur téléphonie de base.



Ensuite, via l'interface web des téléphones, nous procédons à la configuration :

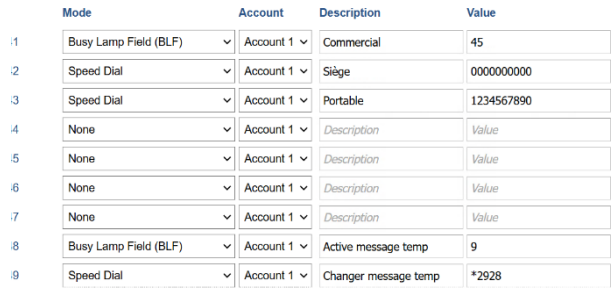
- **Account Name** : nom qui apparaîtra à l'écran du téléphone
- **SIP Server** : adresse IP du serveur FreePBX
- **SIP User ID**, **Authenticate ID** et **Name** : extension correspondante
- **Mot de passe** : celui défini dans l'extension sur le serveur

Cette procédure est répétée pour chacun des deux téléphones.

Nous allons faire cette manipulation deux fois.

Pour le poste de l'accueil, l'extendeur est ensuite installé et programmé avec les numéros et extensions les plus utiles, y compris :

- Un bouton pour **activer/désactiver le Call Flow Control**
- Un autre pour **modifier le message temporaire** associé à ce mode



En parlant de message, il est désormais temps de créer tous les enregistrements qui seront liés aux Annoncements. Pour cela, j'utilise Audacity.

Une musique est déjà attribuée par défaut au site, il me suffit de générer la voix IA et assembler les deux éléments pour créer les enregistrements pour l'accueil et le site fermé.

La mise en place de la téléphonie pour le site de **Le Luart** est ainsi finalisée. Après une brève formation de l'utilisatrice principale sur l'usage des téléphones et du Call Flow Control, le dossier peut être considéré comme **clôturé.**

3.4. Mise à jour Centreon

Centreon est une solution de supervision très utilisée dans les entreprises de type SS2I comme **Keysource**, ainsi que dans les structures possédant un vaste parc informatique.

Cette plateforme permet de **détecter rapidement les dysfonctionnements** afin que les techniciens puissent intervenir avant qu'ils ne deviennent critiques.

Des mises à jour majeures sont publiées deux fois par an : en **avril** et en **octobre**.

À ce jour, notre infrastructure est équipée de la version **24.04.6**, c'est-à-dire celle d'avril 2024. La version d'octobre étant disponible, une mise à jour est donc planifiée.

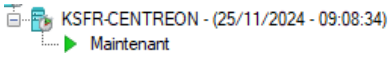
3.4.1. Mise à niveau de Debian 11 à Debian 12

Centreon ayant mis fin au support de **Debian 11**, nous devons mettre à niveau tous les serveurs Centreon (Central et Pollers) vers **Debian 12**.

- Étape 1 : Sauvegarde du serveur

Avant toute manipulation, une sauvegarde est indispensable.

Nos serveurs étant **virtualisés sous Hyper-V**, il suffit de créer un **point de contrôle** (snapshot) sur la VM Centreon Central. Cela nous permettra de revenir en arrière en cas de problème.



- Étape 2 : Préparation de Centreon

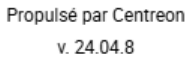
Une première tentative de mise à niveau via une procédure trouvée sur It-Connect a échoué. Elle provoquait la suppression de plusieurs paquets critiques de Centreon. Grâce au point de contrôle, nous avons pu restaurer le système.

Une procédure plus fiable a été trouvée sur le site **The Watch** , un sous-domaine officiel de Centreon.

La première étape consiste à **mettre à jour Centreon** dans sa **dernière version mineure** : 24.04.8.

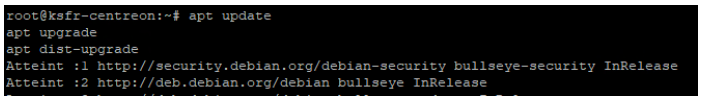
Pour cela, quelques commandes à passer comme : apt clean, qui efface tout ce qui est dans le cache des paquets, apt update, qui lui va nous permettre de générer des paquets « neufs », et enfin, celle qui nous permet de mettre à jour Centreon, apt install --only-upgrade centreon*.

L'interface web de Centreon guide l'utilisateur à travers les étapes de vérification. Une fois finalisé, le retour à la page de connexion confirme la version mise à jour.



Cette mise à jour vers la version mineure terminée, on peut maintenant commencer la montée de version du Debian.

- Étape 3 : Mise à jour de Debian.



Pour cela, on va tout d'abord mettre également à jour le Debian 11 dans sa dernière version mineure disponible grâce aux commandes apt update, apt upgrade, qui va permettre de lui appliquer les mises à jour trouvées par le apt update, et enfin apt dist-upgrade qui va mettre à jour dans la dernière version du Debian 11, qui est donc la distribution, d'où « dist » dans la commande.

Une fois fini, il faut alors à ce moment faire les commandes apt autoremove et apt autoclean qui vont supprimer les paquets obsolètes. Ensuite il faut le faire redémarrer grâce à la commande reboot.

Après le redémarrage, il y a une subtilité à faire pour que tous les paquets de Centreon, Maria DB et Sury-php et du système pour que ces derniers puissent se mettre à jour avec la nouvelle version. Ces commandes permettent de modifier dans ces fichiers le « bullseye » en « bookworm » :

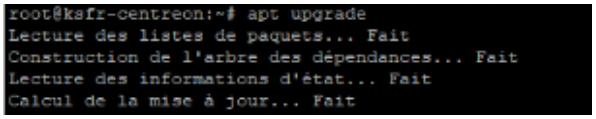
```
sed -i 's/bullseye/bookworm/g' /etc/apt/sources.list
sed -i 's/bullseye/bookworm/g' /etc/apt/sources.list.d/centreon*
sed -i 's/bullseye/bookworm/g' /etc/apt/sources.list.d/mariadb*
sed -i 's/bullseye/bookworm/g' /etc/apt/sources.list.d/sury-php*
```

Il faut donc maintenant régénérer les paquets avec cette nouvelle version au lieu de celle du Debian 11 grâce aux mêmes commandes que plus tôt : apt clean et apt update.

Les nouveaux paquets pré-téléchargés, on va donc mettre à jour les paquets déjà existants grâce à la commande apt upgrade --without-new-pkgs.

Cela fait, on va créer un fichier dans /etc/apt/preferences.d/centreon.pref qui va nous permettre de gérer les priorités des paquets lors de la mise à jour de Linux 11 à Linux 12 pour Centreon.

Une fois ce fichier créé et sauvegardé, on va pouvoir enfin commencer la mise à niveau vers Debian 12 avec la commande apt upgrade. Après un récapitulatif de tous les paquets qui vont être mis à jour, on peut maintenant accepter la mise à jour avec O et les paquets se mettent à jour.



La mise à jour terminée, on peut maintenant supprimer le fichier que nous avons créé peu de temps avant, puis nous allons désinstaller une partie des paquets de Perl pour par la suite réparer l'installation, pour cela, nous allons faire ce groupe de commande :

```
for package in $(dpkg-query -l | grep perl | grep -v centreon | awk -F " " '{print $2}')
do
dpkg -r --force-depends $package.
dpkg --purge --force-depends $package.
done
apt --fix-broken install
On peut maintenant installer pour de bon Debian 12 :
apt full-upgrade
apt autoremove
apt autoclean
reboot
```

Maintenant enfin en Debian 12, on peut passer à la mise à jour du Centreon.

3.4.2. Mise à jour Centreon Central

Le **Centreon Central** est le cœur de la supervision, récupérant toutes les données via les collecteurs et les présentant via une interface web.

Pour ajouter les dépôts de paquets de Centreon, il faut taper les commandes suivantes :

```
echo "deb https://packages.centreon.com/apt-standard-24.10-stable/ $(lsb_release -sc) main" | tee /etc/apt/sources.list.d/centreon.list.
echo "deb https://packages.centreon.com/apt-plugins-stable/ $(lsb_release -sc) main" | tee /etc/apt/sources.list.d/centreon-plugins.list.
Puis on va importer la clé du dépôt grâce à :
wget -O- https://apt-key.centreon.com | gpg --dearmor | tee /etc/apt/trusted.gpg.d/centreon.gpg > /dev/null 2>&1
apt update
```

Après avoir arrêté et désactivé le service php devenu obsolète, on peut maintenant arrêter le service Centreon Broker avec la commande

```
systemctl stop cbd.
```

Avant de lancer la commande pour mettre à jour Centreon, il faut supprimer les fichiers de rétention, c'est-à-dire les fichiers gardés en mémoire pour Centreon. Une fois fait, on va nettoyer une fois de plus le cache avant de mettre à jour Centreon avec la commande :

```
apt install –only-upgrade centreon
```

Une fois fait, il ne reste plus qu'à regarder quelques statuts sur Apache afin d'être sûr que tout soit en ordre puis on

```
apt autoremove
systemctl daemon-reload
systemctl stop php8.1-fpm
systemctl disable php8.1-fpm
systemctl enable php8.2-fpm
systemctl start php8.2-fpm
systemctl restart apache2.
```

va redémarrer les services nécessaires à Centreon :

Une fois ces commandes effectuées, on peut maintenant retourner sur la page web de Centreon et de nouveau faire les vérifications à la suite de la montée de version.

On peut maintenant passer à la suite et mettre à jour les pollers.

3.4.3. Mise à jour des pollers

Les **Pollers**, ou **collecteurs**, permettent de superviser des réseaux distants via des protocoles légers comme **SNMP (port 161)** et **ICMP (ping)**.

Cela permet de sécuriser les connexions en n'ouvrant que les ports nécessaires, plutôt que de donner un accès complet au réseau distant.

Après la mise à jour du Centreon Central, celui-ci ne pouvait plus interagir avec les Pollers, encore en Debian 11 et en version Centreon précédente. Une mise à jour est donc nécessaire. Pour cela, on peut se connecter en SSH sur les serveurs virtuels dédiés.

Après avoir passé les pollers aussi en Debian 12, on peut maintenant mettre à jour les paquets Centreon dessus. Les commandes sont différentes et plus rapides car les pollers sont uniquement des collecteurs d'informations, ils n'ont pas d'interface derrière et donc pas de serveur Apache. Il y a en tout 12 pollers à mettre à jour comme ceci.

Il faut donc mettre à jour les dépôts, comme pour le Central, avec les commandes :

```
echo "deb https://packages.centreon.com/apt-standard-24.10-stable/ $(lsb_release -sc) main" | tee /etc/apt/sources.list.d/centreon.list.
apt update
```

On peut ensuite vider le cache avec les mêmes commandes que précédemment : apt clean all && apt update. On peut maintenant mettre à jour la solution Centreon et redémarrer le service après ça :

```
apt install --only-upgrade centreon-poller
 systemctl restart centreon.
```

Maintenant, il suffit de répéter ces commandes sur les autres pollers et la solution Centreon est maintenant à jour.

4. Etude de Cas : Création d'un portail captif et supervision avec Centreon.

À la suite d'un projet n'ayant pas donné suite, j'ai été redirigé vers une nouvelle mission chez un autre client. Ce nouveau projet consiste à mettre en place un portail captif sur des points d'accès Wi-Fi (également appelés Access Points ou AP), avec une date de déploiement prévue au début du mois de mai.

Pour ce projet, je dois m'assurer que l'ensemble de l'infrastructure réseau soit opérationnelle et configurée en fonction des besoins du client. Cela comprend la configuration réseau, la gestion des VLANs, l'installation physique et logicielle des équipements, et l'intégration du portail captif.

⚠ À noter : Toutes les adresses IP et informations client ont été anonymisées afin de respecter la confidentialité.

4.1. Cahier des charges et planification

Comme dit dans la petite introduction, les délais sont serrés et le matériel arrive au fur et à mesure de la configuration. Nous sommes en mars pour le début de ce projet.

Voici donc un cahier de charges des choses que je dois faire :

- Configurer un pare-feu Pfsense
- Configurer un VPN pour le monitoring via Centreon
- Configurer un AccessLog permettant de faire un portail captif
- Créer 4 VLANs (FOYER, ADM, PRIVE et PUBLIC)
- Créer pour chaque VLAN un Wifi
- Intégrer au « WIFI-FOYER » le portail captif
- Configurer 4 switchs (3 de 28 ports et 1 de 10 ports)
- Configurer un Nuclias
- Configurer 19 points d'accès Wifi

J'ai donc défini un planning pour me préparer à ce que je dois faire avec les dates prévues pour chacune des phases :

Phase de Test (10/03 au 21/03) :

Tests de configuration de l'AccessLog (seul matériel arrivé au départ), avec un switch et un AP d'atelier.

Phase de préparation (à la réception du matériel)

Préparation des 4 switchs dès leur arrivée avec les différents VLANs.

Paramétrage de l'AccessLog en fonction des précédents tests.

Configuration des APs (renseignement des IPs dès leur arrivée)

Configuration du Nuclias et du profil pour les APs

Injecter la configuration dans les 19 APs grâce au Nuclias.

Phase d'installation (mai) :

Dans les locaux du client, mise en place du pare-feu, de l'AccessLog, des 4 switchs, du Nuclias et des 19 AP wifi, avec un ou plusieurs de mes collègues.

4.2. Phase de Test

Je vais donc pouvoir commencer l'essai de configuration de l'AccessLog mais surtout faire des tests. Le reste n'étant pas arrivé, je vais pouvoir essayer avec un AP et un switch qui sont disponibles en atelier. Je vais ainsi pouvoir visualiser le travail à effectuer sur les machines du client quand elles seront arrivées.

Le boîtier AccessLog, comme dit auparavant, permet de créer le portail captif, je vais donc faire quelques tests dessus car je n'en ai jamais manipulé un avant. Pour cela, je vais m'aider de la documentation de l'AccessLog qui va m'être très utile (https://accesslog.fr/documents/install-accesslog.pdf).

Pour mon premier test, j'ai voulu tester de créer sur notre pare-feu Pfsense un VLAN, Virtual Local Area Network qui permet de créer sur un port Ethernet plusieurs interfaces, on peut s'en servir pour séparer les services d'une entreprise avec des réseaux différents. On va donc en créer un seul et essayer de mettre le portail captif en place dessus.

Le VLAN ne semblait pas pouvoir traverser le boîtier d'AccessLog. Les tests n'étant pas concluant, j'ai découvert, avec l'aide de la documentation de l'AccessLog, que l'on pouvait créer des VLAN directement sur le boîtier. Nous avons donc les VLANs 211 ;212 ;213 et 214, sur lesquels nous avons déclaré une plage DHCP.

Paramètres Réseaux

Interface	DHCP	Adresse IP	Masque
Wan	✕		255.255.255.0 (24)
Wan vlan id			
Lan1	✕		255.255.255.0 (24)
Lan1 vlan id 211		172.23.211.254	255.255.255.0 (24)
Lan1 vlan id 212		172.23.212.254	255.255.255.0 (24)
Lan1 vlan id 213		172.23.213.254	255.255.255.0 (24)
Lan1 vlan id 214		172.23.214.254	255.255.255.0 (24)
Lan1 vlan id			
Lan2	✕		255.255.255.0 (24)
Lan2 vlan id			
Lan3	✕		255.255.255.0 (24)
Lan3 vlan id			

Services Réseaux

Interface	Service DHCP	IP Début	IP Fin	Accès	Enregistreur	DNS
Wan						
Lan1	✓	.50	.100	Libre	/ Log	✓
Lan1 vlan id 211	✓	172.23.211.50	172.23.211.250	Authentifié	/ Log	✓
Lan1 vlan id 212	✓	172.23.212.50	172.23.212.250	Libre	/ Log	✓
Lan1 vlan id 213	✓	172.23.213.50	172.23.213.250	Libre	/ Log	✓
Lan1 vlan id 214	✓	172.23.214.50	172.23.214.250	Authentifié	/ Log	✓
Lan2	✕			Inactif		✕
Lan3	✕			Inactif		✕

Une fois cette partie configurée, j'ai sorti un switch qui était en atelier, un switch niveau 3 D-Link DGS-1210-24P avec PoE, que j'ai configuré dans le réseau de mon LAN 1, INFRA.

Après avoir renseigné les VLANs dans le switch et, mon LAN 1 correspondant au VLAN 1 du switch, j'ai mis en « TAG » les VLANs sur les ports 2 et 24. Le « TAG » permettra aux autres VLAN de pouvoir communiquer à condition que le paquet lui soit destiné.

On aura donc le port 2 qui accueillera mon point d'accès de test et le 24 est mon lien vers l'AccessLog.

Cela donne donc cette configuration pour mon switch de test :

VID	VLAN Name	Untagged	Tagged
1	default	01-28	
211	FOYER		02, 24
212	ADM		02, 24
213	PRIVE		02, 24
214	PUBLIC		02, 24

Par la suite, je suis allée chercher un point d'accès Wifi, un DAP-3666, sur lequel j'ai configuré mes VLANs.

J'ai attribué à chaque VLANs un Service Set IDentifier, SSID, qui permet d'identifier une connexion sans fil grâce à un nom. Ce SSID, en fonction du VLAN auquel il est attribué, permettra à la personne voulant se connecter d'aller vers le réseau voulu.

Le SSID primaire fait donc parti du VLAN 211, correspondant au WIFI-FOYER. Ce Wifi n'aura pas de code de sécurité, c'est le portail captif qui va gérer l'accès.

Et pour le menu des SSID, on a activé le multi-SSID pour pouvoir en créer plusieurs, ce qui va accéder au réseau des VLANs précédemment configuré. La configuration des VLANs et des SSID va donc ressembler à ceci :

VLAN Status : Disable Enable Save
VLAN Mode : Static(2.4G), Static(5G)

VLAN List | Port List | Add/Edit VLAN | PVID Setting

VID	VLAN Name	Untag VLAN Ports	Tag VLAN Ports	Edit	Delete
1	default	Mgmt, LAN1, LAN2		Edit	Delete
211	FOYER	Primary(2.4G), Primary(5G)	Mgmt, LAN1, LAN2	Edit	Delete
212	ADM	S-1(2.4G), S-1(5G)	Mgmt, LAN1, LAN2	Edit	Delete
213	PRIVE	S-2(2.4G), S-2(5G)	Mgmt, LAN1, LAN2	Edit	Delete
214	PUBLIC	S-3(2.4G), S-3(5G)	Mgmt, LAN1, LAN2	Edit	Delete

Enable Multi-SSID Enable Priority

Index	SSID	Band	Authentication Method	Encryption Type	Delete
Primary SSID	WIFI-FOYER	2.4G Hz	No Authentication	No Encryption	
Multi-SSID1(Edit)	WIFI-ADM	2.4G Hz	WPA/WPA2-PSK	TKIP/AES Mixed Mode	Delete
Multi-SSID2(Edit)	WIFI-PRIVE	2.4G Hz	WPA2-PSK	TKIP/AES Mixed Mode	Delete
Multi-SSID3(Edit)	WIFI-PUBLIC	2.4G Hz	WPA2-PSK	TKIP/AES Mixed Mode	Delete

Une fois cela fait, on va pouvoir essayer de se connecter au Wifi, n'importe lequel mais de préférence sur celui possédant le portail captif : WIFI-FOYER.

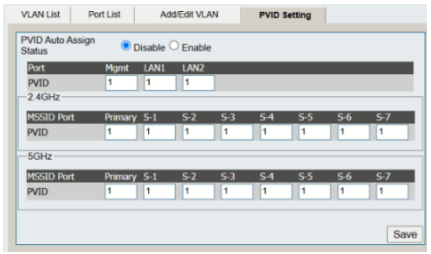
Pour l'essayer, je vais utiliser mon téléphone portable pour m'y connecter sans que je perturbe mon poste ou celui d'un de mes collègues pour s'y connecter.

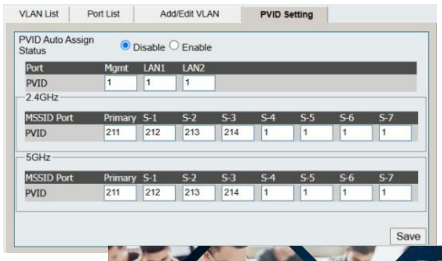
Cependant, alors que le téléphone semble vouloir se connecter, il a l'air impossible de récupérer une adresse IP avec le Wifi.
C'est le même résultat pour les autres wifi.

Il y a donc un problème dans la configuration. Je regarde de nouveau tous les menus et trouve dans le point d'accès wifi, le PVID. Le PVID veut dire Port Vlan ID, l'identifiant par port du VLAN. Il permet entre autres d'accéder au réseau du VLAN depuis le SSID.

Par défaut, tout est dans le VLAN 1.

C'est en regardant sur un AP qui se trouve à Keysource et possédant de multiples VLANs aussi que j'ai eu ma réponse. J'ai donc fait ces modifications :





Après la modification, le portail captif fonctionne et les Wifi aussi.

Il n'y aura plus qu'à configurer la même chose sur le matériel prévu pour eux et surtout étudier le fonctionnement du Nuclias quand il arrivera chez Keysource.

4.3. Configuration du matériel prévu

Effectivement, dans la configuration de test faite précédemment, j'ai pu configurer entièrement l'AccessLog mise à part quelques détails concernant le portail captif. Je vais donc voir avec le directeur du foyer pour voir ce qu'on fait.

Les 3 switchs de 24 ports et celui de 8 ports pour le foyer sont arrivés le 12/03 à Keysource. Je vais donc pouvoir les configurer de la même façon que j'ai fait celui de l'atelier. Il faut uniquement définir les ports sur lesquels il y aura les AP et le Nuclias pour la configuration des ports. Cela se fera au dernier moment, lors de l'installation sur le site.

Pour le moment, il faut donc que je configure les switchs avec les IPs définies avec M. PERRIGAUD et que je mette les VLANs dessus. Les switchs sont donc, en fonction de leur numéro attribués, en 172.23.210.250 jusqu'à 172.23.210.253, le 254 étant mon AccessLog.

Par la suite, je vais uniquement garder un switch allumé pour configurer l'adresse IP des 5 APs qui sont arrivés le 13/03 matin. 10 autres APs ont été réceptionnés le 14/03. AU fur et à mesure de leur arrivée, je leur ai défini un numéro, ce qui me mènera à leur IP. Nous avons donc la plage allant de 172.23.210.201 à 172.23.210.219, les derniers chiffres dépendant du numéro défini.

Maintenant que les derniers AP et le Nuclias sont arrivés le 17/03, on va pouvoir voir comment configurer le Nuclias. Tout d'abord, le Nuclias est une machine de la marque D-Link, comme les switchs et les APs, permettant de gérer à distance les équipements compatibles, comme les points d'accès et certains switchs. Il permet entre autres de créer des « profils » qui serviront de fichier de configuration que l'on pourra injecter dans les équipements. Afin de fonctionner, le Nuclias doit se situer dans le même réseau que les équipements qu'on veut lier.

Nous allons donc le lier pour notre part aux APs, les switchs sont compatibles mais après un petit test de ma part, je ne pouvais plus accéder à l'interface du switch et rien ne semblait fonctionner après ceci. Avec l'aide de mon tuteur, nous avons fini par réussir à le sortir du Nuclias.

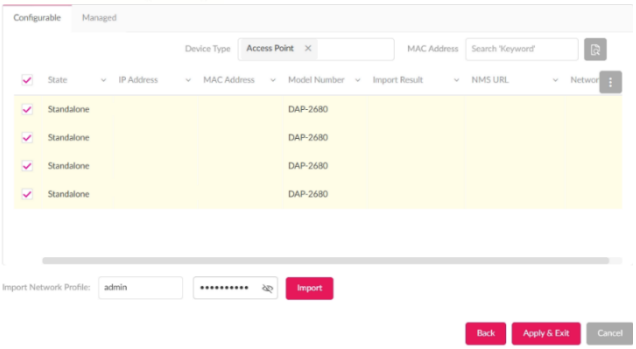
On va pouvoir commencer à configurer le Nuclias. On va tout d'abord lui renseigner son IP, étant donné qu'il contrôle les APs, on va lui mettre 172.23.210.200. On va pouvoir maintenant créer un profil uniquement pour les APs wifi, et renseigner l'équivalent de la configuration de l'AP dans la phase de test.

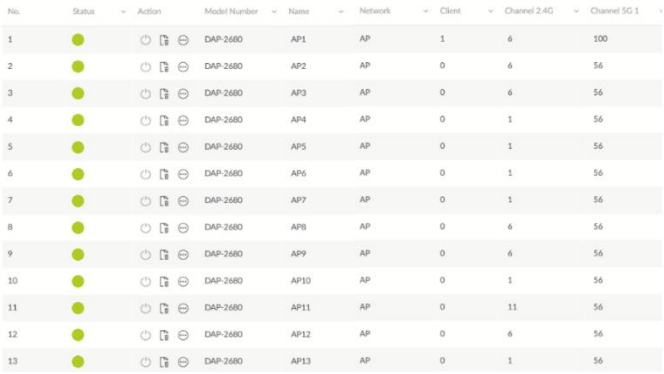
On va donc créer les 4 différents VLANs et les attribuer aux différents SSID, cette fois, on attribue bien les différents PVID aux VLANs en fonction de leur SSID et de quel réseau on veut que le client se connecte avec les SSID.

Une fois le profil créé, on va pouvoir injecter la configuration aux 19 APs différents. Pour cela, on va aller dans « Create profile » ; sur le profil qu'on vient de créer, on va cliquer sur la loupe « Discovery ».

On effectue une recherche par IP sur le réseau Infra. Les APs vont remonter ici en « Standalone », cela veut dire qu'il se gère lui-même.

On va donc cocher toutes les cases et faire « Import ». Quand le résultat est en « success », cela veut dire que la configuration s'est bien appliquée.

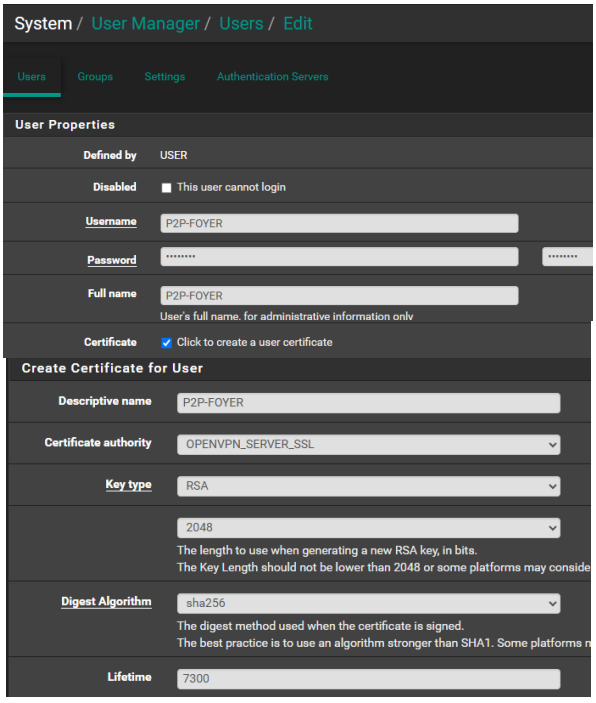




On peut alors aller voir dans « Monitor>Access Point> Access Point », tous les APs sont remontés dans cette interface, ce qui va nous permettre de les contrôler à distance.

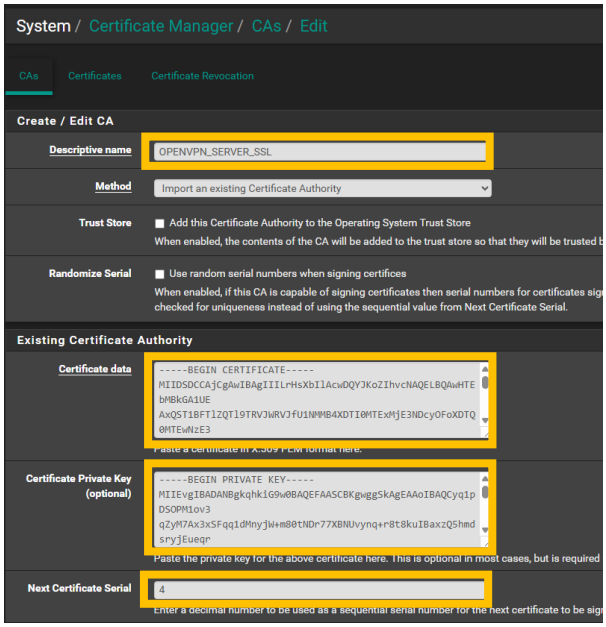
Passons à la configuration du pare-feu, sur lequel on va monter un VPN entre lui et notre Datacenter GAMMA. Ce VPN servira au monitoring du matériel depuis Keysource grâce à Centreon.

Pour la création du VPN, je vais suivre une procédure faite par M. DOUET. Cette procédure permet de créer le tunnel OpenVPN en Peer to Peer SSL. Nous utilisons uniquement OpenVPN



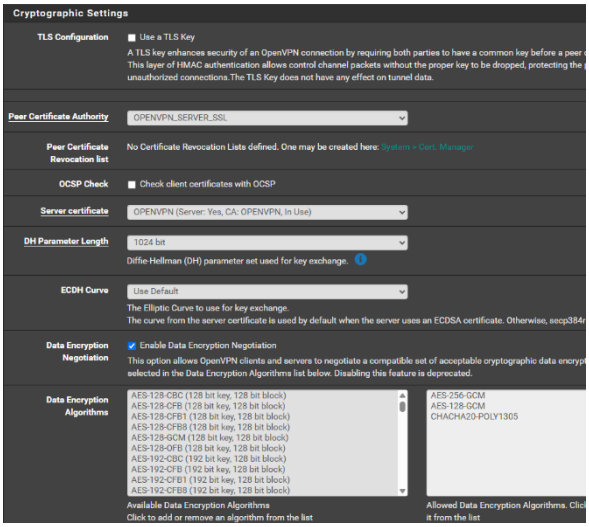
On va donc aller sur le pare-feu de notre datacenter GAMMA pour y créer un utilisateur comme ceci :

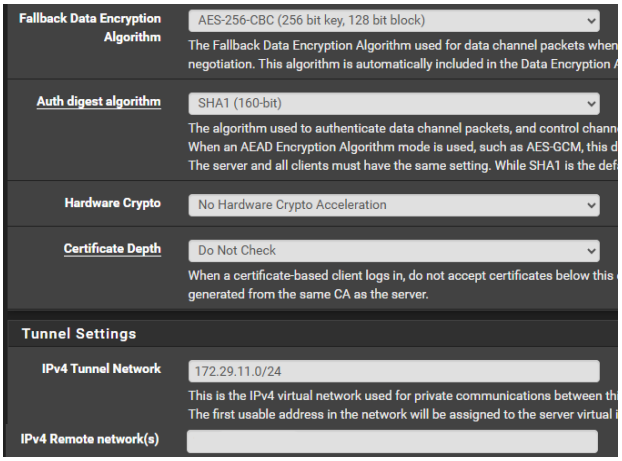
Une fois l'utilisateur créé, on va exporter les certificats du serveur OpenVPN, ici appelé « OPENVPN_SERVER_SSL ». On va donc copier les champs encadrés dans un document texte :



Et on va faire la même chose pour le certificat client qu'on vient de créer.

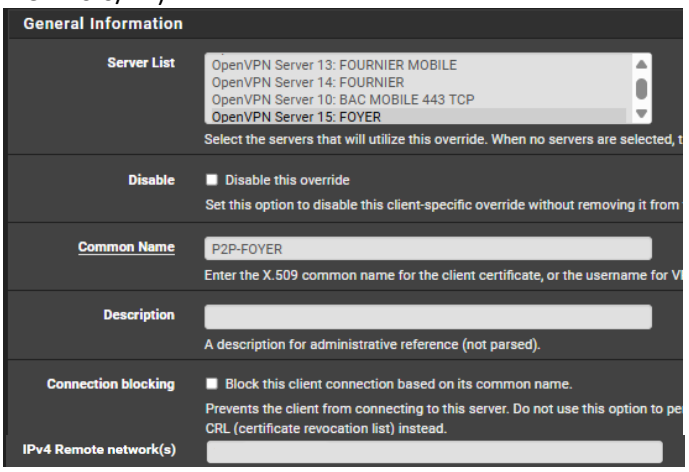
Une fois les certificats exportés, on va pouvoir créer le serveur OpenVPN, toujours sur le pare-feu GAMMA. On va donc dans le menu « VPN » puis « OpenVPN », et on va dans l'onglet « servers », puisqu'on va créer le côté du VPN serveur. Avant de le créer, il faut regarder les ports et les IP tunnel afin de voir quels sont ceux qu'on peut prendre. Ici, ce sera le port 1307 et l'IP tunnel 172.29.11.0/24. Cela mène donc à cette configuration :



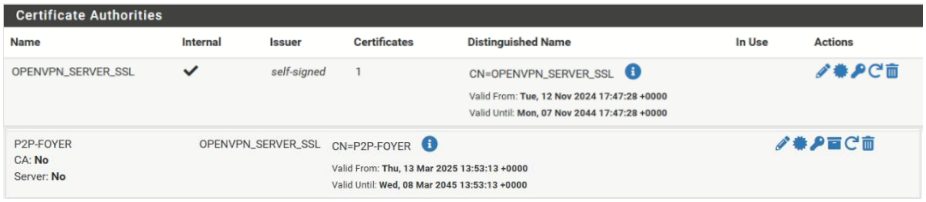


Une fois que le serveur OpenVPN est créé, on va aller dans l'onglet « Client Specific Overrides » et en ajouter un.

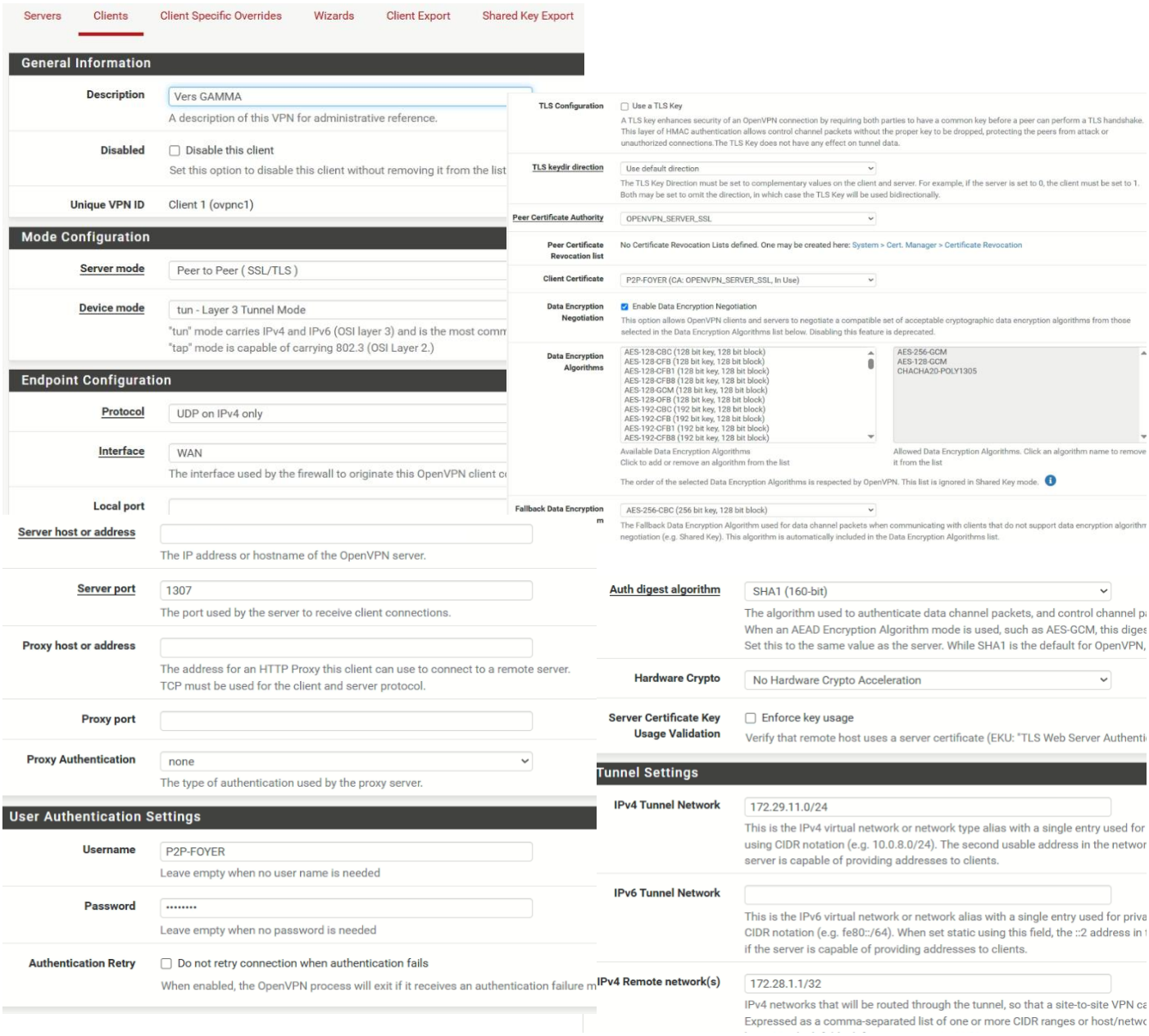
On va ici sélectionner le serveur OpenVPN qu'on vient de créer, renseigner le nom de l'utilisateur créé précédemment et l'IP du réseau à accéder depuis le datacenter GAMMA (172.23.210.0/24).



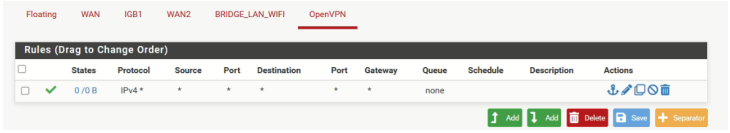
Maintenant, on peut aller sur le pare-feu client, on va tout d'abord importer les certificats client et serveur exportés précédemment. Pour cela, on va aller dans « System/Cert.Manager/CAs » pour le certificat serveur, cliquer sur « Add » et choisir dans « Method », « Import an existing Certificate Authority ». On va alors renseigner les champs avec les données exportées. On va faire la même chose pour le certificat client mais cette fois dans l'onglet « Certificates ».



Une fois fait, on va pouvoir créer le côté client du VPN :

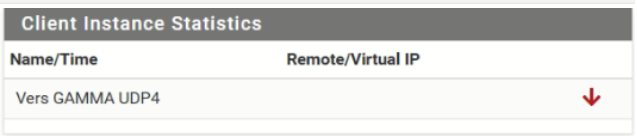


On va ensuite créer une règle de pare-feu autorisant les communications VPNs



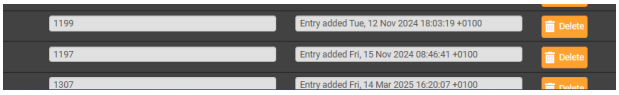
Puis on va aller activer le SNMP pour que le Centreon puisse accéder et contrôler les ressources du réseau.

On peut maintenant regarder l'état du VPN, ici, il n'est pas monté, cela veut dire qu'il y a un problème dans la configuration. Je rajoute donc un réseau dans ma configuration, c'est celle entre mon pare-feu et l'AccessLog.



Après un nouveau test, ça ne fonctionne toujours pas : TLS Handshake failed. Après de nombreuses vérifications et comparaison entre plusieurs autres VPN, je ne trouve toujours pas la cause de l'erreur.

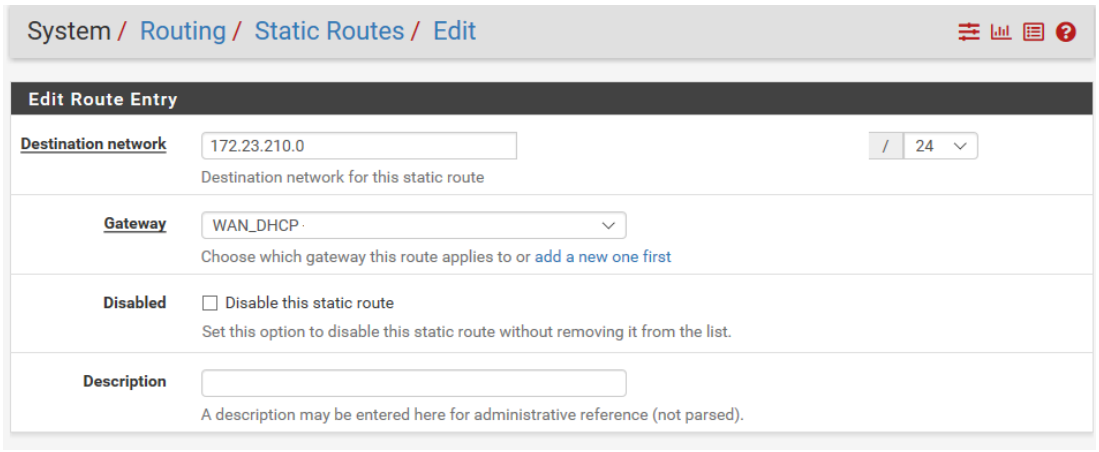
J'en parle donc à M. DOUET qui m'éclaire sur un point : une règle de pare-feu qui bloquait le port sur lequel j'essayais de monter mon lien OpenVPN, je l'ai donc ajouté dans l'alias :



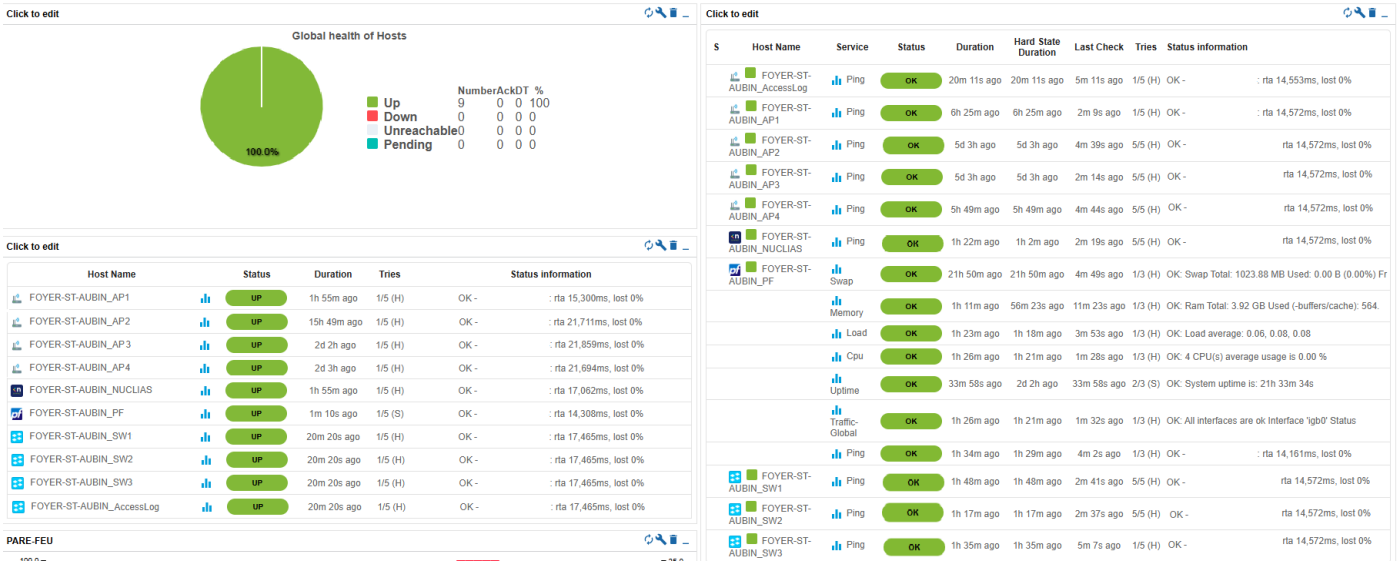
Après un nouveau test, le VPN ne monte toujours pas. Entre temps, M.DOUET est aller jeter un œil sur mon VPN et a trouvé le problème : mon certificat d'autorité n'était pas lié à mon certificat de serveur.

J'ai donc du créer un autre certificat de serveur, cette fois-ci lié au certificat d'autorité, puis après sa création, je l'ai changé dans mon VPN

Maintenant, on veut accéder au réseau après l'AccessLog, c'est-à-dire le 172.23.210.0/24, il faut donc tout d'abord que le pare feu soit capable d'accéder, pour cela, on doit créer une route statique, on crée donc une gateway entre l'interface WAN puis on crée la route statique dessus comme ceci :



Une fois fait, le pare-feu peux maintenant accéder on peut aller dans Centreon et créer les actions à faire pour chaque matériel,(Pare-feu, AccessLog, switchs, Nuclias et APs), principalement une requête ICMP pour voir s'ils répondent bien et qu'ils sont bien allumés. A la fin, le panneau correspondant à notre client donne ceci :



Comme à notre habitude chez Keysource, après la préparation d'un pare-feu, on lui fait lancer un script pour sauvegarder sa configuration dans notre serveur FTP. Ainsi, en cas d'incident avec le pare-feu en production, le client peut brancher celui préparé en secours. Il nous suffira alors de prendre la main sur le poste du client pour réinjecter la configuration de notre FTP.

Ce backup s'effectue toutes les nuits et fait l'objet d'une surveillance constante à Keysource, possédant ainsi son propre panneau de monitoring sur Centreon.

La configuration du backup s'effectue ainsi :

Aller dans «Diagnostics/ Edit File »

Taper : / et faire « Browse »

Si le fichier /backupconfig.sh existe alors cliquer dessus pour le modifier et s'assurer d'avoir le bon script.

Sinon, il faut créer un nouveau fichier appelé /backupconfig.sh et coller les lignes ci-dessous :

```
HOST='backupkeywall.keycloud.fr'
PORT='21'
USER='username'
PASSWD='password'

ftp -n -i -v $HOST $PORT <<END_SCRIPT
quote USER $USER
quote PASS $PASSWD
put /conf/config.xml /config.xml
quit

END_SCRIPT
```

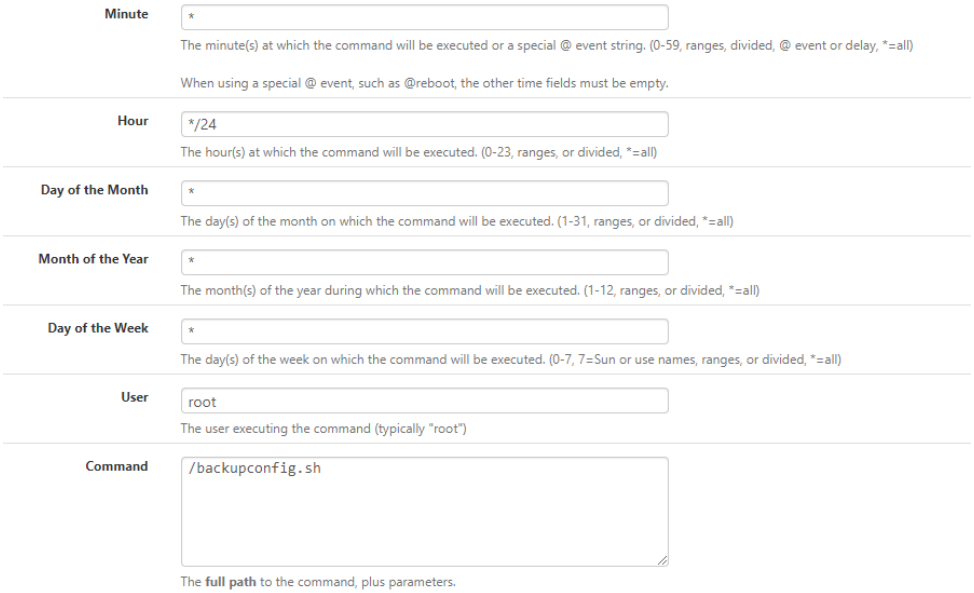
Il faut ensuite modifier le username et le password pour qu'ils correspondent au login du client sur le serveur FTP, créés précédemment. On peut ensuite aller dans « Diagnostics /Command Prompt » et taper les commandes suivantes :

```
Chmod +x /backupconfig.sh        #rends le script exécutable
/backupconfig.sh                 #exécute le script
```

Enfin, il faut créer un job de sauvegarde automatique, pour ça, on utilise Cron qui est accessible depuis « Services/ Cron ».

Si le service Cron n'est pas installé alors il faut aller dans « System/ Package Manager/ Available Packages » puis chercher Cron et l'installer. Une fois installé, il apparaîtra directement dans « Services/ Cron ».

Puis il faut ajouter un job en appuyant sur « Add » et renseigner les paramètres ci-joint :



Pour voir si la première sauvegarde s'est bien effectuée, on va sur le serveur FTP puis on va dans le répertoire dédié au client, si un fichier « config.xml » est présent, alors la configuration du script est bon

4.3. Mise en place sur site du client

A l'heure actuelle, la mise en place chez le client n'est pas encore faite. Tout l'équipement sera livré par nos soins du 28 au 30 avril. Cette mission sera effectuée par moi-même ainsi que 1 ou 2 de mes collègues, selon les disponibilités de chacun. Sur le terrain, nous aurons des petites configurations de dernières minutes concernant les VLANs sur les switchs à faire. Selon le matériel connecté sur les différents ports, la configuration peut différer.

4.4. Conclusion de l'étude de cas

Le but principal de l'étude de cas était de mettre en place sur un Wifi particulier un portail captif, avec l'aide du matériel AccessLog.

Ceci était une demande d'un client qui souhaitait différents Wifi dont un captif pour la connexion des jeunes étant au Foyer.

J'ai exploré le boîtier AccessLog, qui à ce moment était la seule partie arrivée, afin de comprendre son fonctionnement et mettre en œuvre une petite configuration pour mes tests avec du matériel d'atelier.

Alors que le matériel était censé arriver que fin mars, durant ma période de cours, par chance, tout est arrivé avant, entre le 12 et le 17 mars. J'ai donc pu le configurer au fur et à mesure des arrivées et paramétrer le tout ensemble.

Malgré quelques problèmes, la configuration était concluante, ne laissant que quelques détails derrière. J'ai passé en tout 2 semaines à travailler dessus en continu. Il ne manque plus que la mise en place, qui va se passer plus tard, dans les mois à suivre.

Ce projet m'a apporté des connaissances sur la mise en place de l'AccessLog avec la configuration et le fonctionnement d'un portail captif. Il m'a aussi permis de monter un VPN vers un de nos Datacenters, GAMMA, qui m'a par la suite permis de configurer le monitoring sur Centreon. Il était également intéressant de voir comment se configurait le Nuclias et voir comment gérer les points d'accès Wifi depuis cette interface.

5. Conclusion de l'alternance

Ces deux années d'alternance à Keysource m'ont permis de m'améliorer au point de vue social, mais aussi et surtout au point de vue Technique.

Apprendre au côté de professionnels comme M. DOUET et M. PERRIGAUD, qui m'ont fait confiance tout au long de ces deux ans sur des tâches toujours plus intéressantes les unes que les autres, m'a permis d'affirmer ma formation actuelle.

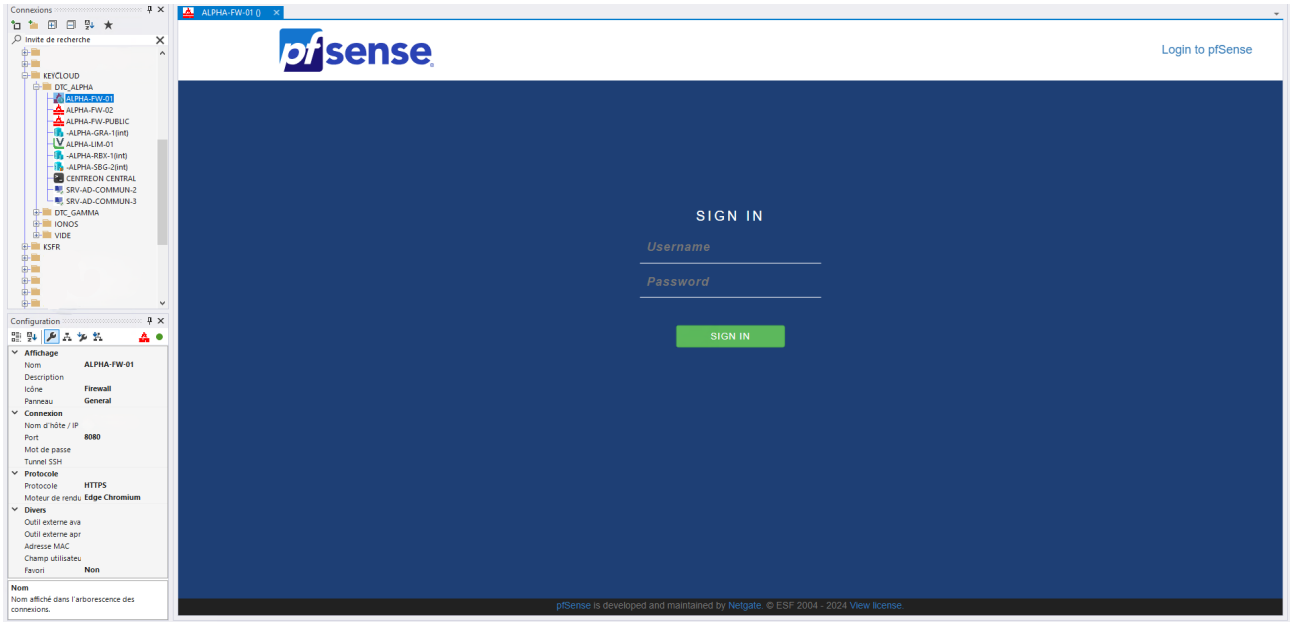
Leur patience et bonne humeur a vraiment été un plus dans cet apprentissage de métier. L'équipe de Keysource est formidable avec beaucoup de bonne entente et de rigolade avec mes collègues, mettant en place une bonne ambiance au sein de l'équipe.

C'est donc avec un immense plaisir que je vais continuer à leur côté une alternance pour mon BTS SIO à Saint Félix La Salle, afin de devenir une meilleure technicienne encore avec eux.

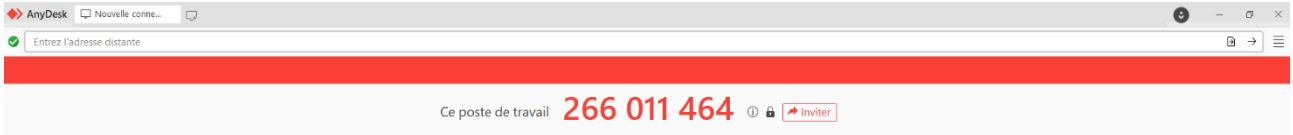
Sommaire des annexes

Annexe 1 : Les outils de Keysource

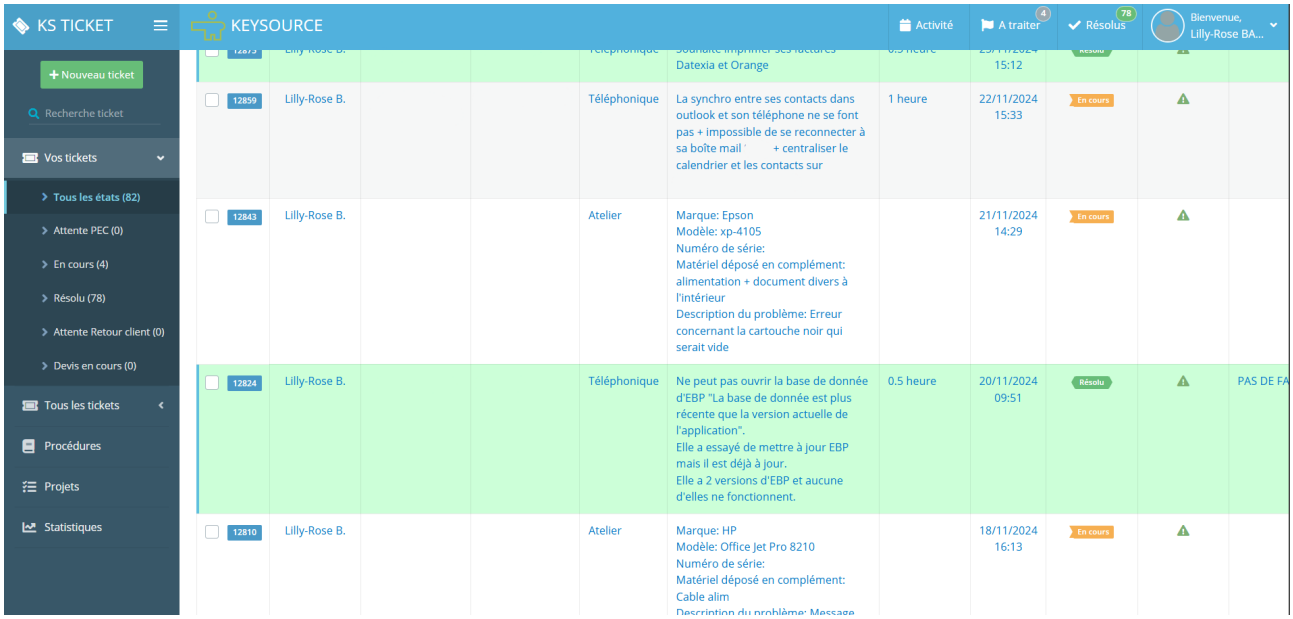
MRemote NG : Prise à distance sur les machines clients, ici, un firewall.



Anydesk : prise en main à distance sur les postes clients



KSticket : Outil de gestion de ticket



Annexe 2 : Le schéma réseau du Foyer