Institut Universitaire de Technologie,
Aix-Marseille Université

RAPPORT DE STAGE
Diplôme Universitaire de Technologie
Spécialité Réseaux et Télécommunications

Stage de fin d'études

Paul CAZALS

Office Center

Responsable entreprise : Vincent CHARLES

Responsable académique : Sébastien SANCHEZ

2021

Table des matières

1 Introduction 1
2 Présentation de l'entreprise 2
2.1 Office Center 2
2.2 Organigramme 3
3 Missions réalisées 4
3.1 Refonte du LAN de l'entreprise. 4
3.1.1 Audit du réseau 4
3.1.2 Découverte de l'environnement ZyXEL 6
3.1.3 Découverte du Switch DLINK 7
3.1.4 Mise en place des VLANs 8
3.2 Optimisation du réseau WIFI. 13
3.2.1 Réalisation d'un Bot d'auto-configuration 14
3.3 Découverte du métier de Technicien 16
3.4 Réalisation annexe 18
3.4.1 Auto-installassions d'un logiciel Antivirus 18
3.4.2 Réalisation d'un Proxy de filtrage 19
3.4.3 Pré-Conclusion 20
4 Conclusion 21
5 Remerciements 23
6 Glossaire 24
7 Bibliographie 26

1 Introduction

Dans le cadre de mon Diplôme Universitaire Technologie en Réseaux et Télécommunication que j'effectue à Marseille sur le campus de Luminy, j'ai souhaité réaliser mon stage de fin d'études dans une entreprise au service des professionnelles. En effet, Office Center est un acteur majeur dans la gestion des infrastructures informatiques et réseaux des Alpes de Hautes Provence et Hautes Alpes. Le positionnement de l'entreprise et les différents domaines qu'elle traite était en parfaite adéquation avec mon projet professionnel.
L'informatique occupe aujourd'hui une place de plus en plus importante et, depuis la crise sanitaire, le télétravail s'est développé de manière exponentielle impliquant la mise en place de nouveaux services. J'ai donc pu évoluer pendant une période de 10 semaines sur différentes missions confiées au services techniques et en parallèle avancer sur mon projet de stage.

Au sein du service Technique de la société Office Center, j'ai pu découvrir le fonctionnement d'une équipe complète au service des différentes infrastructures informatiques. Grâce à mes compétences acquises à l'IUT, j'ai également pu traiter des demandes particulières de clients, faire des interventions plus ou moins complexes qui m'ont permis d'engranger de l'expérience pour poursuivre ma mission.
Le réseau de l'entreprise n'étant ni optimisé ni sécurisé, j'ai pu développer une solution permettant de corriger ces soucis principaux.

Tout au long de ce rapport, il sera expliqué le contexte de mon intervention, les différentes analyses des problèmes rencontrés et les démarches que j'ai pu réaliser en vue de l'amélioration du réseau local de l'entreprise.
Il sera également expliqué certaines de mes missions annexes qui m'ont été confié comme la mise en place d'une installation automatique d'antivirus, la configuration d'une solution de surveillance via un proxy puis via un logiciel et la gestion d'appel technique via le logiciel de l'entreprise.

2 Présentation de l'entreprise

2.1 Office Center

Figure 1 : Société Office Center

Office Center, située n°2 Parc Saint-Pierre au Chaffaut st-Jurson (04510) est une société à responsabilité limitée (SARL) de type PME créée en 1973. Elle dispose de locaux modernes et récents d'un capital social de 50 000 € et d'une clientèle assez importante.

En 1973, M. Yves Rispoli crée les « Etablissements Rispoli » devenus « Office Center Rispoli ». L'activité de l'entreprise a été reprise par la famille Raspail en février 2001.
Directeur technique, Sylvain Raspail devient alors co-gérant avec son fils Jérémy. Le 1er février 2005, le nouveau nom de l'entreprise « Office Center » prendra effet.

En 2014 ainsi qu'en 2015, le chiffre d'affaires de l'entreprise a atteint 930.000 € et bénéficie d'une augmentation d'année en année. Office Center est l'une des seules sociétés du département offrant cette diversité de services aux entreprises, elle n'a donc pas de concurrent direct. Elle dispose d'une clientèle de professionnels comme les Mairies, Hôtel, Restaurant, Médecin, Notaire, et différents types d'entreprises.

Les domaines de compétences de l'entreprise sont nombreux et sont surtout en corrélation avec la demande du marché en perpétuelle évolution. Ceux-ci vont de l'infogérance à l'assistance technique sur des infrastructures informatiques et réseaux en passant par le déploiement de solution cloud, de progiciel, la création de site web, d'audit* de sites déjà existants, en finissant par une partie reprographie et sécurité (mise en place de systèmes de vidéosurveillance). Office Center compte actuellement 8 salariés dont trois dans le service informatique où j'effectué mon stage.
Le chef d'entreprise, Jérémy Raspail, a réussi à mettre en place un système efficace de prestations de services permettant de faire évoluer l'entreprise et de la faire prospérer dans un lieu où la multimodalité, le volume d'offre d'emploi et la proportion d'habitant au mètre carré est faible.

2.2 Organigramme

Nous pouvons distinguer plusieurs services au sein de l'entreprise. Le service administratif pour gérer tous les aspects financiers, le service commercial ayant pour but de démarcher les nouveaux clients, d'accompagner les anciens dans la migration de leurs infrastructures ou encore d'informer la clientèle de nouvelles offres à pourvoir.
Le service technique qui gère la reprographie (pour certain des techniciens), l'informatique, la mise en place de caisse (monétique) ou de système de surveillance.

J'ai effectué mon stage dans ce service géré par mon tuteur Vincent Charles au côté des techniciens. Ce service a pour objectifs :

- D'effectuer l'infogérance des différentes infrastructures existantes
- La création, l'installation et la maintenance d'infrastructures
- L'Audit de parc informatique et l'optimisation des outils
- Le développement de logiciels professionnels spécifiques
- La création de site internet
- L'assistance technique

Le service est composé de deux techniciens « permanents » et d'un technicien alternant en licence Pro. Chaque technicien est plus ou moins qualifié dans un domaine, ce qui permet une diversité de compétences et une certaine efficacité à tous les niveaux.
La montée en compétence de tous est une valeur importante que prône l'entreprise. Dès que cela est possible, chaque personne peut être formé par une plus qualifiée pour évoluer et engranger de l'expérience.

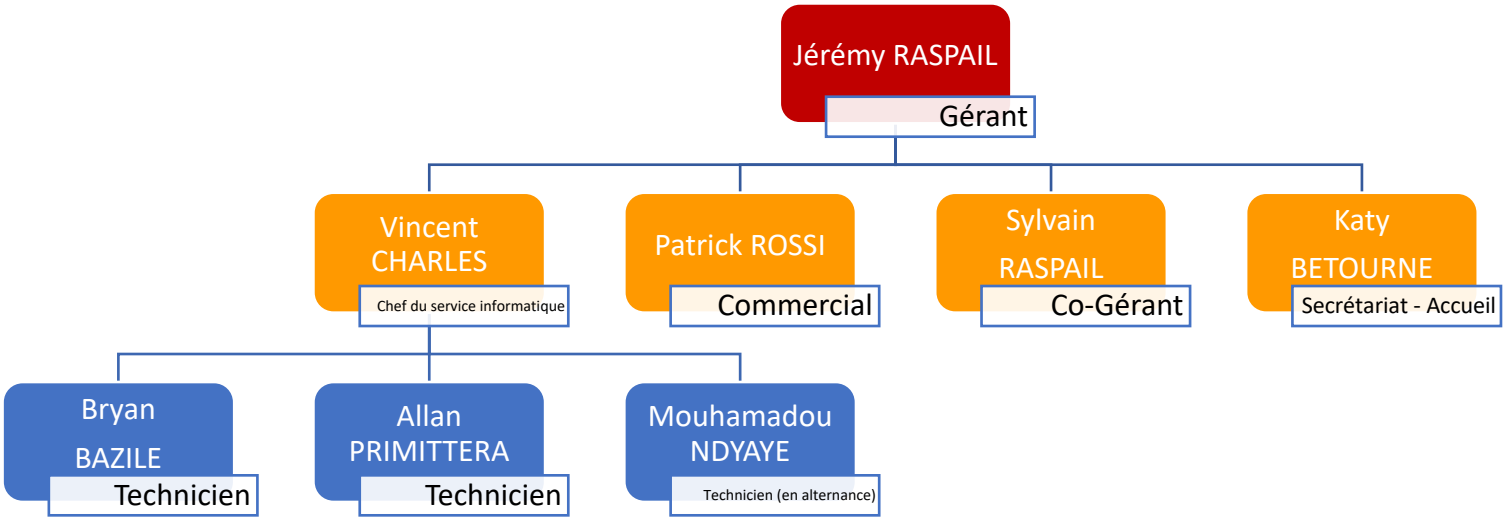


Figure 2 : Organigramme de la société

3 Missions réalisées

3.1 Refonte du LAN de l'entreprise.

Office Center comporte comme la plupart des PME un réseau informatique. Celui-ci était un réseau dit « simple ». Il n'était pas forcément optimisé ni sécurisé. J'ai œuvré avec l'aide de mon maitre de stage à la refonte de celui-ci. Cela s'est passé en plusieurs étapes. J'ai d'abord analysé l'infrastructure réseaux pour savoir ce qu'il était possible de faire en termes d'évolution.

3.1.1 Audit du réseau

Un réseau est configuré en 192.168.1.0 /24 et c'est un ZyXEL USG60W qui gère le routage.
Il est lui en 192.168.1.254 et est connecté à deux FAI*. Une Livebox en 128.1.1.1 /24 qui elle, permet l'accès à internet, la connexion externe via le VPN du ZyXEL et l'accès aux différents serveurs. Un deuxième routeur en 128.1.2.1 /24 est ici pour gérer la téléphonie OVH et permettre une redondance si le premier routeur internet tombe en panne.
Le ZyXEL est lui branché sur un switch administrable Dlink DGS 3100 de 48 et c'est ce switch qui s'occupe de l'interconnexion de tous les équipements.
Ci-dessous, un schéma du réseau que j'ai effectué pour y voir plus clair. Les équipements à la base du schéma ci-dessous, sont les équipements en IP fixes.

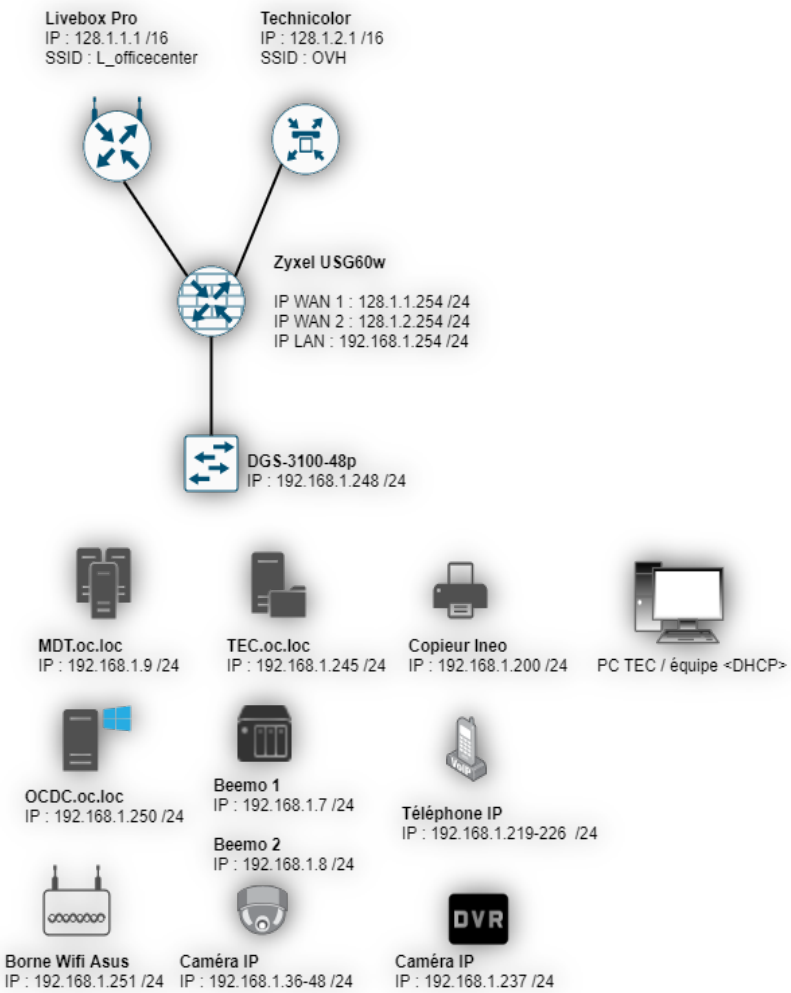


Figure 3 : Schéma du réseau avant

L'une des premières activités que j'ai effectués était de vérifier les équipements connectés sur le switch. En effet certains câbles arrivant dans la baie n'étaient pas identifiés. J'ai donc utilisé un testeur de câbles pour les identifier et ensuite référencer tous les équipements et toutes les prises mural RJ45. Nous en avons également profité pour remettre en ordre la baie de brassage. Cela était indispensable pour la continuité du projet.

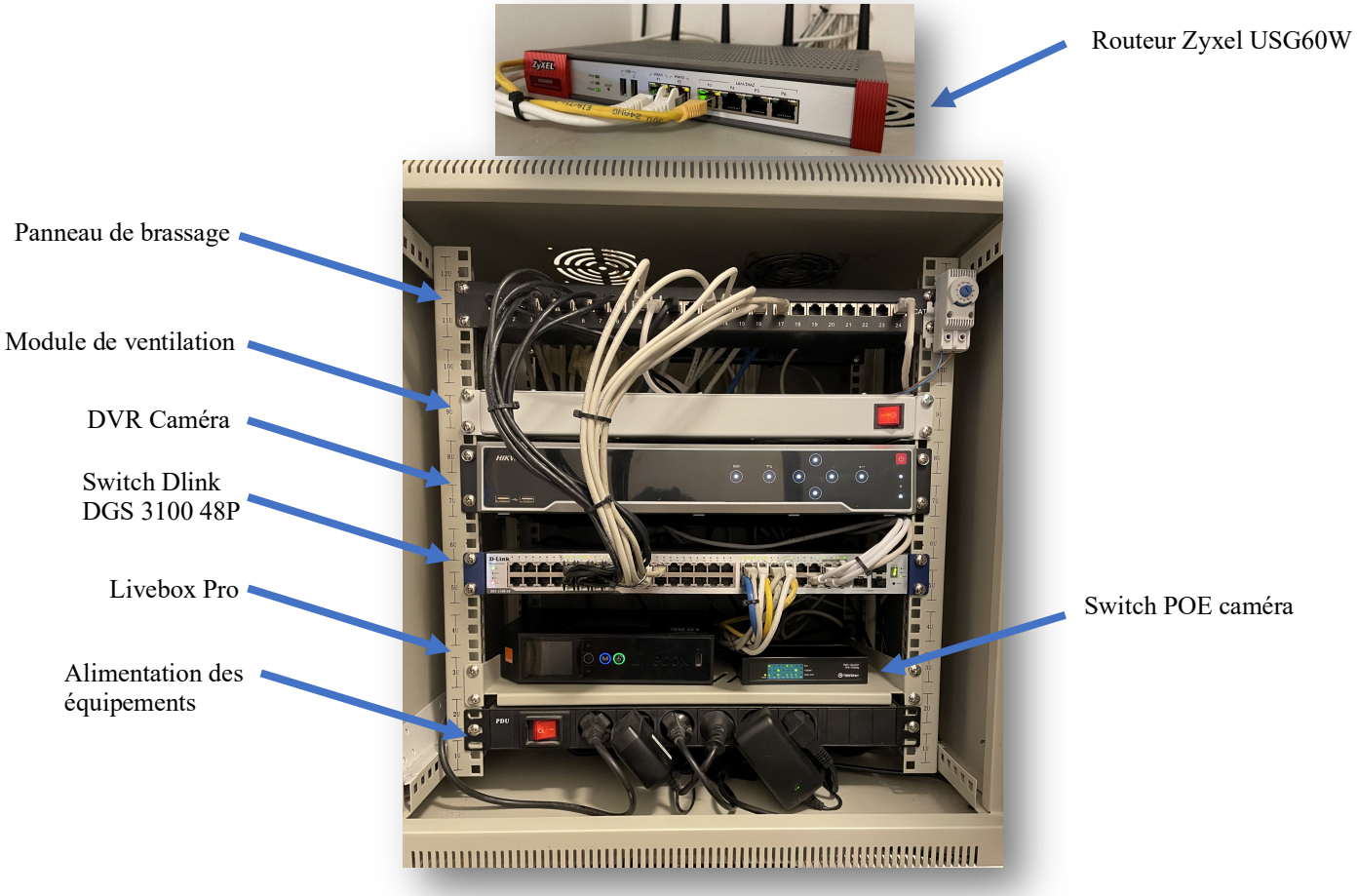


Figure 4 : Baie de brassage principal.

N° Port	Description	N° Port	Description
9	Salle de formation	33	Serveur TEC
10	Bureaux Vincent – PC	34	Serveur TEC
11	Atelier – SAV 4	35	Serveur OCDC
12	Caméra Couloir	36	Serveur OCDC
13	Atelier -SAV 5	37	Serveur Xen (Virtualisation)
14	Atelier – SAV 1	38	Serveur Xen (Virtualisation)
15	Switch Accueil	39	Beemo
16	Atelier – SAV 2	40	Zyxel USG60W
17	Bureaux Jérémy	41	
18	Salle de réunion étage	42	
19	Salle reprographie	43	Switch Allan (SAV 6)
20	Bureaux Patrick	44	Switch POE
21	Bureaux Vincent - Table	45	
22	Atelier - Allan	46	Table étage
23	Atelier SAV 3	47	Borne Wifi Asus
24		48	Salle reprographie 2

Figure 4 : Agrégation des ports

3.1.2 Découverte de l'environnement ZyXEL

Le réseau de l'entreprise est en grande partie géré par le routeur ZyXEL USG60W. Etant donné que je n'avais jamais travaillé avec ce type de matériel, j'ai d'abord cherché à me familiariser avec celui-ci.
Pour ne pas impacter les employées, j'ai travaillé sur un ZyXEL USG20, un peu plus ancien que celui utilisé par l'entreprise, mais avec le même mode de fonctionnement.
La gamme USG du constructeur permet à des PME* d'avoir un tout en un pour leur réseau. En effet, il est possible de configurer une connectivité VPN*, un firewall, un point d'accès Wifi et en parallèle gérer le routage et toutes les fonctions d'un routeur classique. De plus, cela reste du matériel accessible en termes de prix et de simplicité d'utilisation. Il est possible de se connecter en SSH*, telnet ou via le port console pour utiliser le routeur en CLI* mais il est également possible de s'y connecter via une interface graphique sur le WEB.
J'ai d'abord utilisé le routeur en CLI par habitude, les commandes sont ressemblantes à l'IOS* de Cisco mais demande un temps d'adaptation car elles doivent être écrites de manière « complète ».
J'ai ensuite utilisé l'interface Web intuitive qui m'a permis de réaliser une configuration avec un WAN* et deux LAN*, les faire communiquer, bloquer le trafic venant d'un réseau vers l'autre, créer des VLANs*, etc.
Avoir fait cette prise en main m'a permis de découvrir un nouvel environnement et d'éclaircir mes idées quand à ma méthode de réalisation du projet.

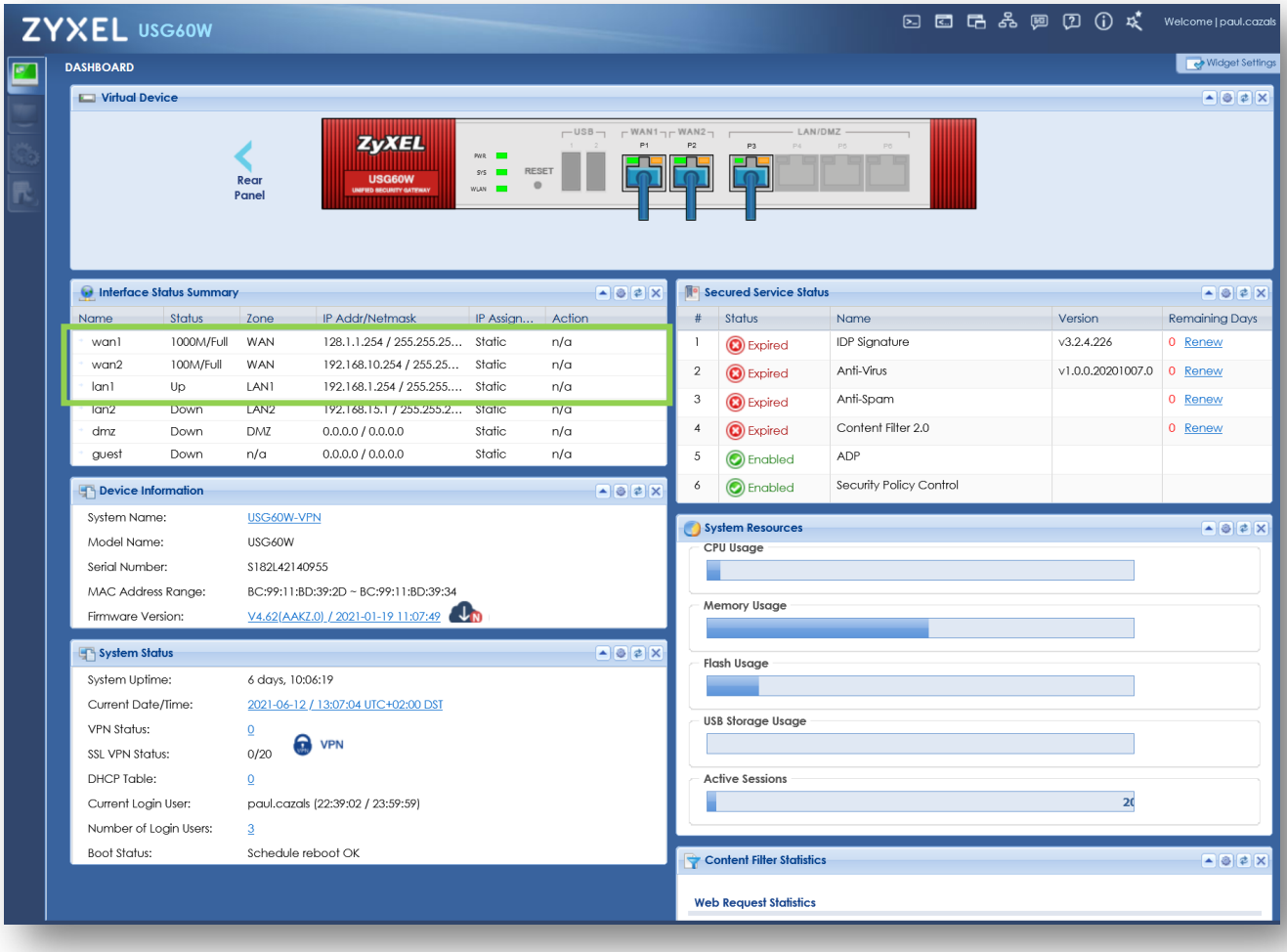


Figure 5 : Interface Web du ZyXEL USG60W

3.1.3 Découverte du Switch DLINK

Une fois la prise en main du routeur effectuée, le switch gérant l'interconnexion de tout l'équipement de l'entreprise était un équipement inconnu pour ma part.
Etant un Switch administrable, il fournit les fonctions les plus complètes pour un réseau : la mise en place de VLAN, la configuration en CLI, la gestion de SNMP, le routage IP, la QoS*, etc. Le switch de l'entreprise n'était pas configuré et fonctionnait en tant que switch non-administrable. Avant de commencer à manipuler le switch, je me suis renseigné avec la documentation du constructeur afin d'éviter toute fausse manipulation de ma part, pouvant provoquer une panne sur le réseau de l'entreprise et impacter les salariés.
Je lui ai donc premièrement assigné une adresse IP sur le réseau afin de permettre l'utilisation d'une connexion SSH/Telnet ou d'une connexion via la page Web de configuration. J'ai assigné la description des équipements connectés précédemment établis et je me suis ensuite appuyé sur la documentation afin de comprendre comment utiliser les VLANs avec ce switch. Cette partie sera développée de manière plus explicite à la suite de ce rapport.

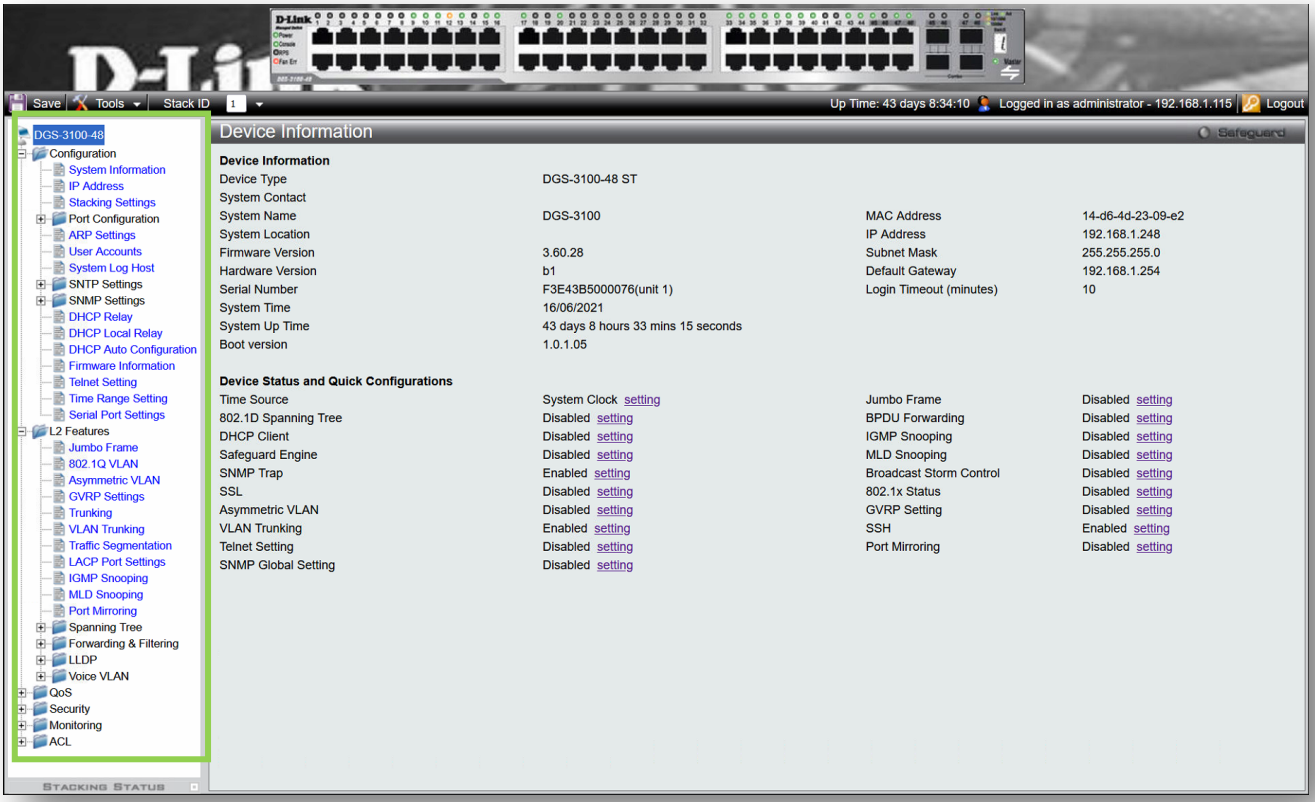


Figure 6 : Interface Web du D-Link DSG3100-48P

Nous pouvons voir sur la gauche les fonctions principales supportées par le Switch comme la configuration des ports, le SNMP* pour le monitoring, le menu « L2 Features » pour la gestion des VLAN, un menu « QoS » pour l'optimisation du réseau et différents menus pour la gestion de la sécurité (ACL*, SSL*, le protocole 802.1X, etc).

3.1.4 Mise en place des VLANs

Aujourd'hui dans le LAN de l'entreprise, tous les équipements peuvent communiquer entre eux puisqu'ils sont tous reliés de manière physique au switch. Cela n'est pas optimal, car dans la mesure où un appareil est compromis par un attaquant, il lui est très facile d'accéder aux autres appareils du réseau et ainsi le compromettre. Également, plus il y a d'équipements, plus le domaine de diffusion augmentera et plus il y a aura de latence (le domaine de diffusion étant l'ensemble des équipements interconnectés pouvant communiquer sans sortir du réseau).
Pour toutes ces raisons, nous avons décidé de séparer le réseau de l'entreprise en différents VLAN.

Les VLANs (**V**irtual **L**ocal **A**rea **N**etwork) sont des sous réseaux de niveaux 2 permettant de créer des réseaux logiques sur une seule infrastructure physique. Il est alors possible de « cloisonner » des réseaux facilement et de les sécuriser en y appliquant des règles d'accès (ACL par exemple). D'autre part, cela permet de baliser le domaine de broadcast auquel les machines appartiennent et donc rendre le trafic invisible aux machines n'appartenant pas aux mêmes VLANs.
Ainsi en cloisonnant les différents réseaux et en fonction de nos différents usages, cela garantie une meilleure rapidité. De plus, un réseau fractionné est bien plus simple à administrer.

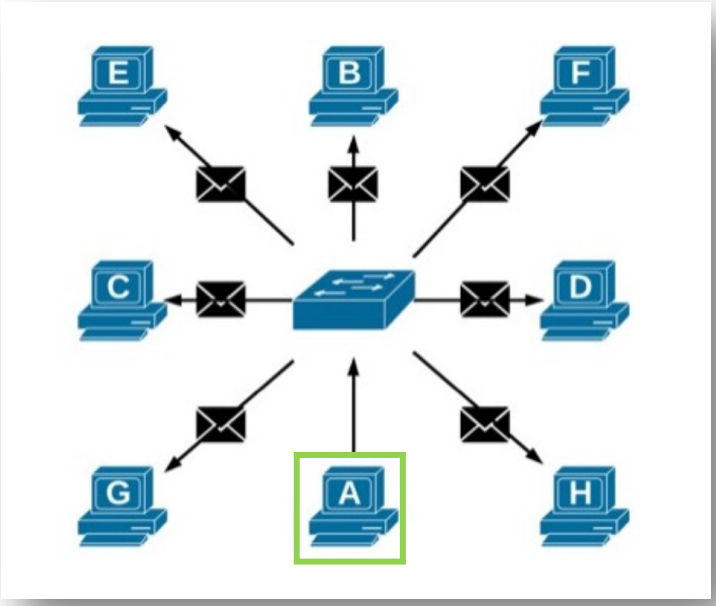


Figure 7 : Fonctionnement d'un Lan sans VLAN

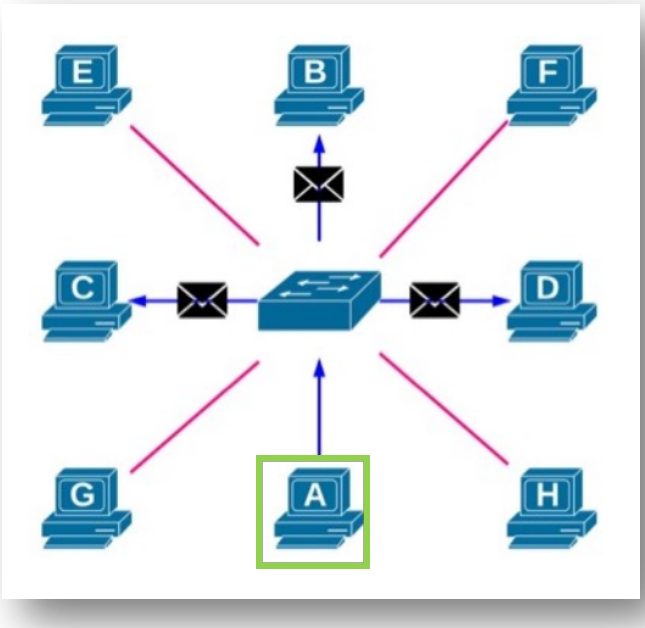


Figure 8 : Fonctionnement d'un Lan avec VLAN

Nous pouvons voir sur la figure 7 le fonctionnement d'un réseau local ne comportant pas de VLAN. Ce type de réseau possède un mode de transmission qui consiste à diffuser toutes les informations vers l'ensemble des équipements connectés à celui-ci. Ainsi, nous pouvons voir que le PC A émet du trafic à tous les équipements. Pour les raisons énumérées ci-dessus, cela n'est pas très optimal mais convient aux petites infrastructures comme les maisons et les petites entreprises.
Sur la figure 8, le PC A, B, C, et D sont dans le même VLAN, ainsi lorsque le PC A émet du trafic, seulement les équipements du même VLAN le reçoivent. Les PC E, F, G et H ne reçoivent aucun message de broadcast.

Nous allons donc découper le réseau existant en 4 VLANs. Le but étant de le sécuriser et l'optimiser un maximum. Nous allons procéder ainsi :

- Un VLAN « Privé » pour les employés de l'entreprise. Il comprendra les différents PC, les différents objets connectés (volets, alarme, lumière, robot nettoyant), les différents équipements utiles au bon fonctionnement des services (Wifi Perso, Copieur, Serveur de ressource, contrôleur de domaine, etc.). Pour des raisons de rapidité de mise en place et d'incompatibilité avec certains appareils (Alarme notamment) ce VLAN restera le VLAN par défaut et tous les autres appareils seront sur d'autre VLAN.
- Un VLAN « Public » sera utilisé pour le Wifi public (expliqué à la suite de ce rapport). Certaines prises Ethernet murales qui étaient utilisées pour des opérations de maintenance sur du matériel extérieur à l'entreprise, seront dans ce même VLAN. Cela permettra de bloquer l'accès aux différents serveurs stockant des données sensibles et plus généralement bloquer l'accès au réseau pour éviter une éventuelle attaque.
- Un VLAN « Téléphonie » sera mis en place pour la téléphonie IP. Il y a des gros soucis de ce côté-là du réseau, le placement de ce système dans un VLAN ne pourra qu'être bénéfique. Les données transmises sur ce VLAN seront seulement des données voix et pour toutes les raisons que nous avons données précédemment, cela améliorera le fonctionnement.
- Un VLAN « Caméra » dédié à la vidéosurveillance et au stockage des données de celle-ci.

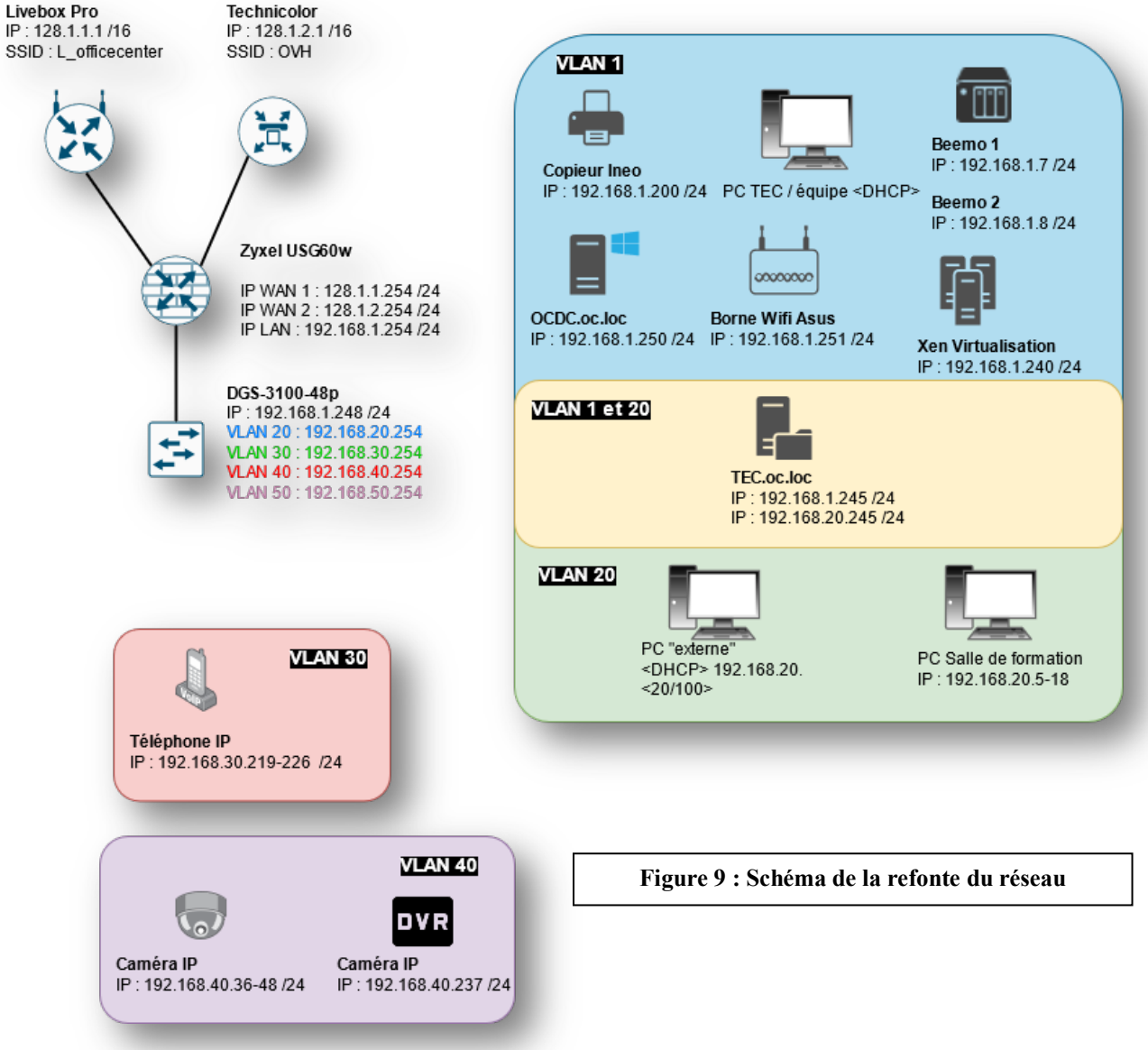
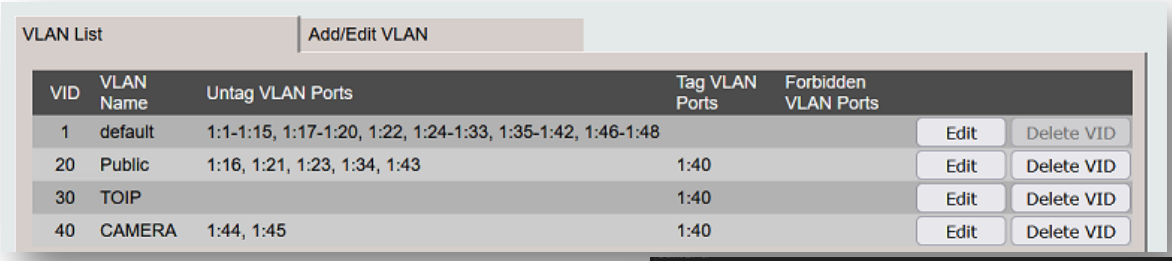


Figure 9 : Schéma de la refonte du réseau



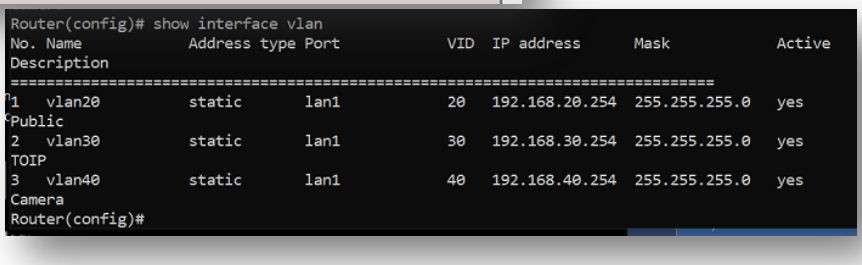


Figure 11 : Différentes interfaces des VLANS (sur le Switch et le routeur)

La volonté de diviser le réseau pour garantir une plus grande sécurité et une plus grande efficacité passe par différentes étapes comme la définition des différents besoins. Il a été validé que tous les appareils servant au bon fonctionnement de l'entreprise (serveurs contrôleur de domaine, serveurs de sauvegarde, serveur hébergeant les Progiciels* servant à la gestion des clients, etc…) devaient être séparés du réseau. Seul le serveur TEC, ayant pour but de stocker des données (tel que des outils utiles à la maintenance) et le serveur Xen utile à la virtualisation de système, devaient être accessible via les deux réseaux. Ainsi via des règles d'accès, l'accès du VLAN public vers le VLAN privé sera limité.
Pour l'assignation des adresses IP aux différents appareils, un serveur DHCP* était présent sur le

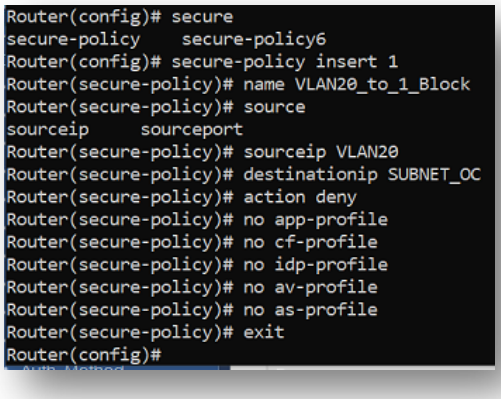


Figure 10 : Règle bloquant l'accès du VLAN Public au VLAN Privé

contrôleur de domaine. Ce serveur DHCP a été migré sur le serveur de données (serveur TEC) car celui-ci était doté de deux interfaces réseaux. Ainsi le serveur DHCP aura une « patte » dans chaque réseau et pourra continuer à fonctionner comme auparavant. Une mission de ce serveur étant notamment de faire du PXE* pour déployer des images systèmes, il a donc été migré avec l'aide de mon maitre de stage.
Les autres VLANs qui seront utilisés pour la téléphonie et les caméras ne bénéficieront pas de serveur DHCP. Les équipements ayant une IP fixe, cela n'a pas d'utilité.
Pour ceux qui est de la communication des VLANs avec internet, une opération de routage a également été faite pour permettre aux différents équipements dans les différents VLANs de fonctionner comme auparavant.
Pour la résolution DNS dans le VLAN 20 des différents appareils et notamment du serveur « TEC », une entrée dans la table du ZyXEL a été ajoutée.

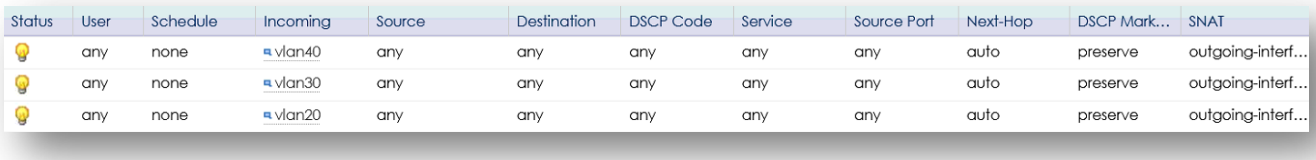


Figure 10 : règle de Routage pour permettre la communication des VLANs sur Internet

Une dernière chose sur les VLANs et l'utilisation des VLANs taggués. En effet une Trame Ethernet peut être taguée avec un numéro (numéro de Vlan) et ainsi être identifiée dans un VLAN. Cela peut être utile pour configurer plusieurs VLANs sur un même port. Nous l'avons utilisé sur le switch pour le port du routeur qui comporte plusieurs VLANs (voir figure 11). Le PC du Chef du service technique (mon maitre de stage) a également été taggué, permettant un accès à tous les réseaux virtuels.
Ainsi lorsque qu'un appareil communique avec le switch, il ajoutera un identifiant dans la trame (voir figure 12) et le Switch pourra alors faire le lien avec son VLAN et router correctement le trafic. Pour ce faire, les différents switches et les différents terminaux (Serveur / PC / etc…) devront être compatibles avec la norme IEEE 802.1Q Tag.

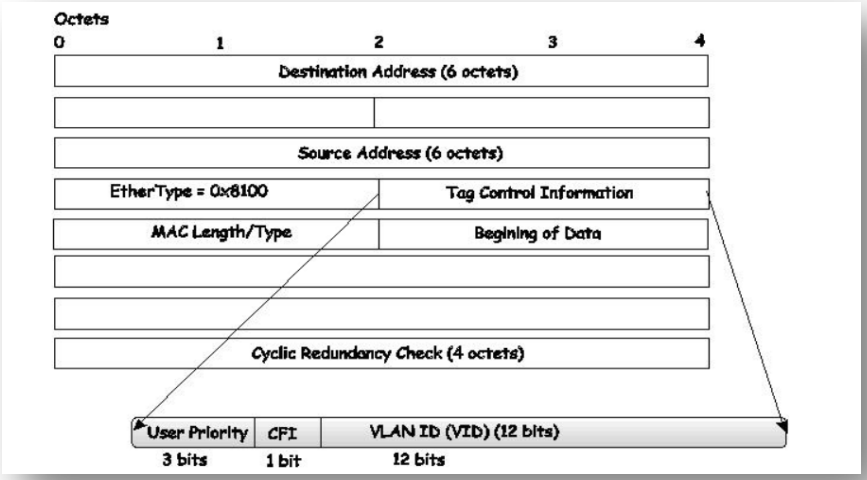


Figure 12 : Tag IEEE 802.1Q

La balise VLAN 802.1Q ci-dessus nous montre le fonctionnement des VLANs aggués. Quatre octets supplémentaires sont insérés après l'adresse MAC source.
Leur présence est indiquée par une valeur de 0x8100 dans le champ EtherType. Lorsque le champ EtherType d'un paquet est égal à 0x8100, le paquet porte la balise IEEE 802.1Q.
La balise est contenue dans les deux octets suivants et se compose de 3 bits de priorité, d'un bit d'identifiant de format canonique (CFI - utilisé pour encapsuler les paquets Token Ring* afin qu'ils puissent être transportés sur les dorsales Ethernet) et de 12 bits d'identifiant de VLAN (VID).
Les 3 bits de priorité utilisateur sont utilisés par la norme 802.1p. Le VID est l'identifiant du VLAN et est utilisé par la norme 802.1Q.
Comme le VID comporte 12 bits, 4094 VLAN uniques peuvent être identifiés. L'étiquette est insérée dans l'en-tête du paquet, ce qui rallonge le paquet de 4 octets. Toutes les informations contenues à l'origine dans le paquet sont conservées.

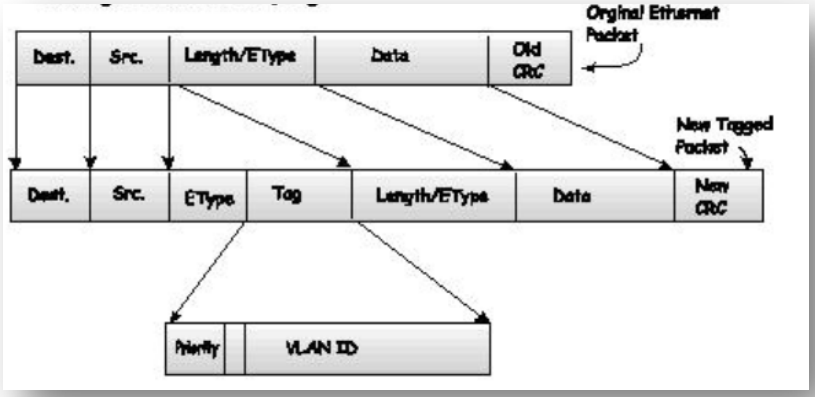


Figure 13 : Ajout d'un Tag sur une trame Ethernet

Si nous résumons, une partie des prises de l'atelier SAV 2, 3 et 6 sont désormais dans le VLAN 20. Sur ces prises, des switches standards sont connectés permettant de distribuer le réseau aux PCs externes se connectant. Les PCs de la salle de formation et le Wifi destiné au public le sont également. Grâce aux règles bloquant le trafic venant du VLAN 20 au VLAN Perso, il est impossible d'accéder aux données sensibles de l'entreprise. Seul le serveur « TEC » lié, au stockage des différents outils de maintenance, est accessible.
Une problématique que j'ai rencontrée lors de cette mise en place est qu'un switch était utilisé par le personnel et pour les PC externes. Ce switch-là n'étant pas un switch administrable et n'en ayant pas sous la main, nous avons pris la décision de tirer un nouveau câble que j'ai connecté sur le Switch administrable. J'ai donc pu de manière moins conventionnelle, séparer les deux réseaux.
Nous pouvons voir si dessous la répartition des différents VLANs en fonction des différents ports du Switch.

N° Port	Description	VID	N° Port	Description	VID
9	Salle de formation	1	33	Serveur TEC	1
10	Bureaux Vincent – PC	1	34	Serveur TEC	20
11	Atelier – SAV 4	1	35	Serveur OCDC	1
12	Caméra Couloir	1	36	Serveur OCDC	1
13	Atelier -SAV 5	1	37	Serveur Xen (Virtualisation)	1
14	Atelier – SAV 1	1	38	Serveur Xen (Virtualisation)	20
15	Switch Accueil	1	39	Beemo	1
16	Atelier – SAV 2	20	40	Zyxel USG60W	1, 20, 30, 40
17	Bureaux Jérémy	1	41		
18	Salle de réunion étage	1	42		
19	Salle reprographie	1	43	Switch Allan (SAV 6)	20
20	Bureaux Patrick	1	44	Switch POE Cam	40
21	Bureaux Vincent - Table	20	45	NVR	40
22	Atelier – Allan	1	46	Table étage	1
23	Atelier SAV 3	20	47	Borne Wifi Asus	1
24			48	Salle reprographie 2	1

En séparant le réseau de la sorte cela a permis de le gérer de manière plus efficace, donc améliorer les performances et d'augmenter les capacités d'évolutivité dans le temps.
Même si les objectifs principaux n'ont pas été atteints (une opération de QoS aurait été intéressante), cela aurait permis aux réseaux d'évoluer en fonction des futurs besoins de l'entreprise.

3.2 Optimisation du réseau WIFI.

Une mission qui m'a été confiée durant mon stage était d'optimiser l'utilisation et la performance des réseaux Wifi*. Il y a en effet trois réseaux Wifi dont un majoritairement utilisé. Les deux autres sont seulement présents pour d'éventuels tests de connexion aux différentes passerelles internet.

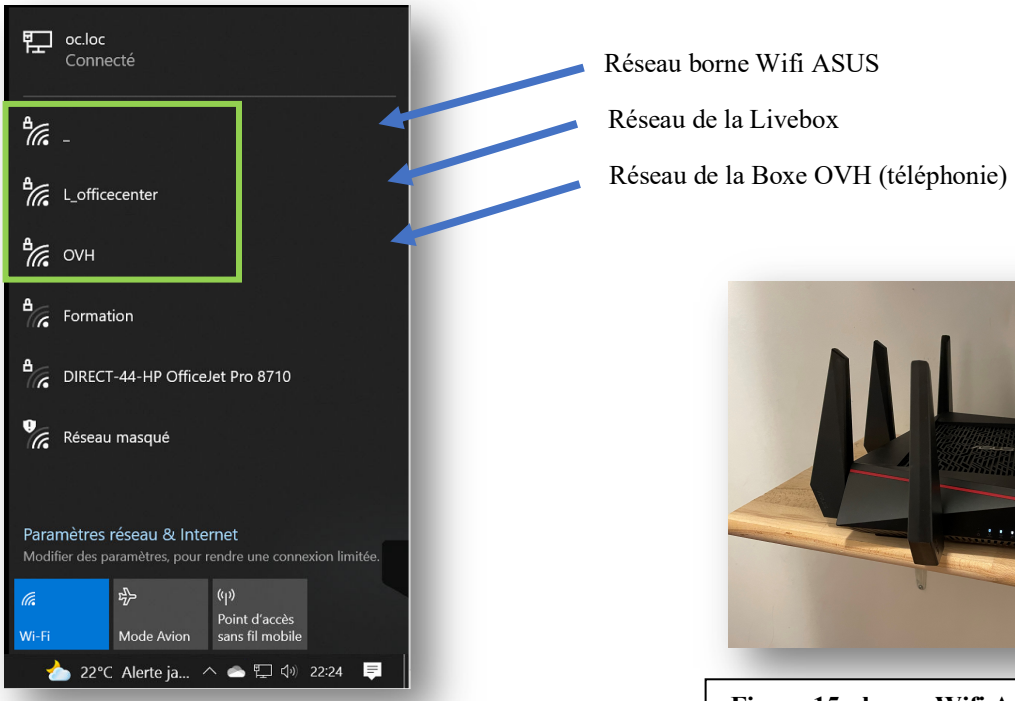


Figure 14 : SSID diffusé dans les locaux

Figure 15 : borne Wifi Asus ROG Rapture GT-AX11000

Le plus utilisé est celui portant le nom «_», que ce soit pour l'utilisation personnelle des salariés et la connexion de matériel externe à l'entreprise (PC en maintenance ou sur le banc de configuration). Il est diffusé par une borne Wifi gérant le wifi 6 (voir figure 15).
L'avantage de ce réseau wifi est qu'il est facilement accessible et permet de s'y connecter rapidement pour ne pas perdre temps. La clé de sécurité elle, n'avait pas changé depuis au moins 2016 (date à laquelle j'avais effectué mon précédent stage et ou la clé était identique).
La problématique était que lorsque les divers équipements revenaient à l'atelier pour des opérations de maintenance, ils se reconnectaient de manière autonome au réseau wifi et cela amputait de la bande passante. Également, si un équipement revenait infecté, il pouvait propager un virus facilement sur le réseau car tout y était accessible.
Le souhait de l'entreprise était alors d'avoir un réseau wifi restant accessible de manière simple et d'empêcher la reconnexion des équipements précédemment connectés. De plus, avec le travail réalisé sur la division du réseau avec les VLANs, un réseau wifi serait dans le VLAN « perso » et un autre dans le VLAN « public ». Cela aura permis de séparer les différents équipements.
Une solution d'authentification ou de portail captif aurait pu être envisageable mais nous aurions perdu l'aspect rapide et facile de la connexion.
J'ai donc pensé à changer le SSID et le mot de passe de façon hebdomadaire. Certain routeur propose cette fonction mais que ce soit le ZyXEL, les deux boxes internet ou la borne Wifi, ils n'en étaient pas dotés.
Pour cela j'ai alors réalisé un script d'auto-configuration se connectant à un équipement en SSH et envoyant des commandes à celui-ci. La borne Wifi Asus étant destinée au grand public et non destinée à un usage professionnel, elle ne comportait pas de connectivité SSH et d'interface CLI. J'ai donc opté pour que cette borne soit dans le VLAN « perso » et soit uniquement fait pour l'usage des équipements de l'entreprise.
Nous utiliserons le ZyXEL pour la diffusion du réseau présent dans le VLAN « public ».

3.2.1 Réalisation d'un Bot d'auto-configuration

Pour exécuter un script, il nous faut une machine exécutant un OS*. L'usage d'une machine virtuelle pour ce genre de chose est parfait. Je me suis naturellement tourné vers une machine virtuelle tournant sur Debian, un système d'exploitation libre et complet.
L'entreprise disposait d'un serveur de virtualisation (Xen Center) et j'ai pu l'utiliser pour réaliser mes tests. J'ai alors téléchargé un ISO* de Debian, compris le fonctionnement du serveur de virtualisation, installé une version minimale de Debian avec pas d'interface graphique, 512mo de RAM* et 4096Mo de ROM*. Cela permettra une utilisation minimale des ressources et une solution légère à mettre en place. Pour plus de simplicité, j'ai migré cette VM sur le contrôleur de domaine (OCDC.oc.loc) et elle est maintenant conteneurisée sous HyperV*.
Après mûre réflexion, nous avons opté pour changer le SSID et non le mot de passe qui restera le même, ce qui évitera d'aller le consulter à chaque fois.
Mon BOT* fonctionne de la sorte :
Chaque jour, une règle CRONTAB* exécute un script en Bash à 00H01 qui lui-même lance un autre script. Le premier est le script qui génère le SSID et le mot passe. Il l'envoie sur un serveur Discord et dans un fichier texte sur le serveur TEC (serveur MDT*/Ressource logiciel/Données). Le script génère également un QR Code d'auto-connexion au réseau wifi. En flashant ou en important le QR Code, cela permet une connexion immédiate (voir figure 16).
Le deuxième script lui, se connecte au routeur en SSH et envoie les commandes adéquates pour changer le SSID.
Pour le nom du réseau, j'ai choisi de le définir avec la date du jour + le nom « _WifiOC ». Ainsi les PC revenant en atelier pour de la maintenance connaitront seulement le SSID précédent et seront dans l'incapacité de s'y reconnecter. De plus, le réseau diffusé est dans le VLAN 20 ce qui permet de cantonner les différents utilisateurs à un seul réseau.

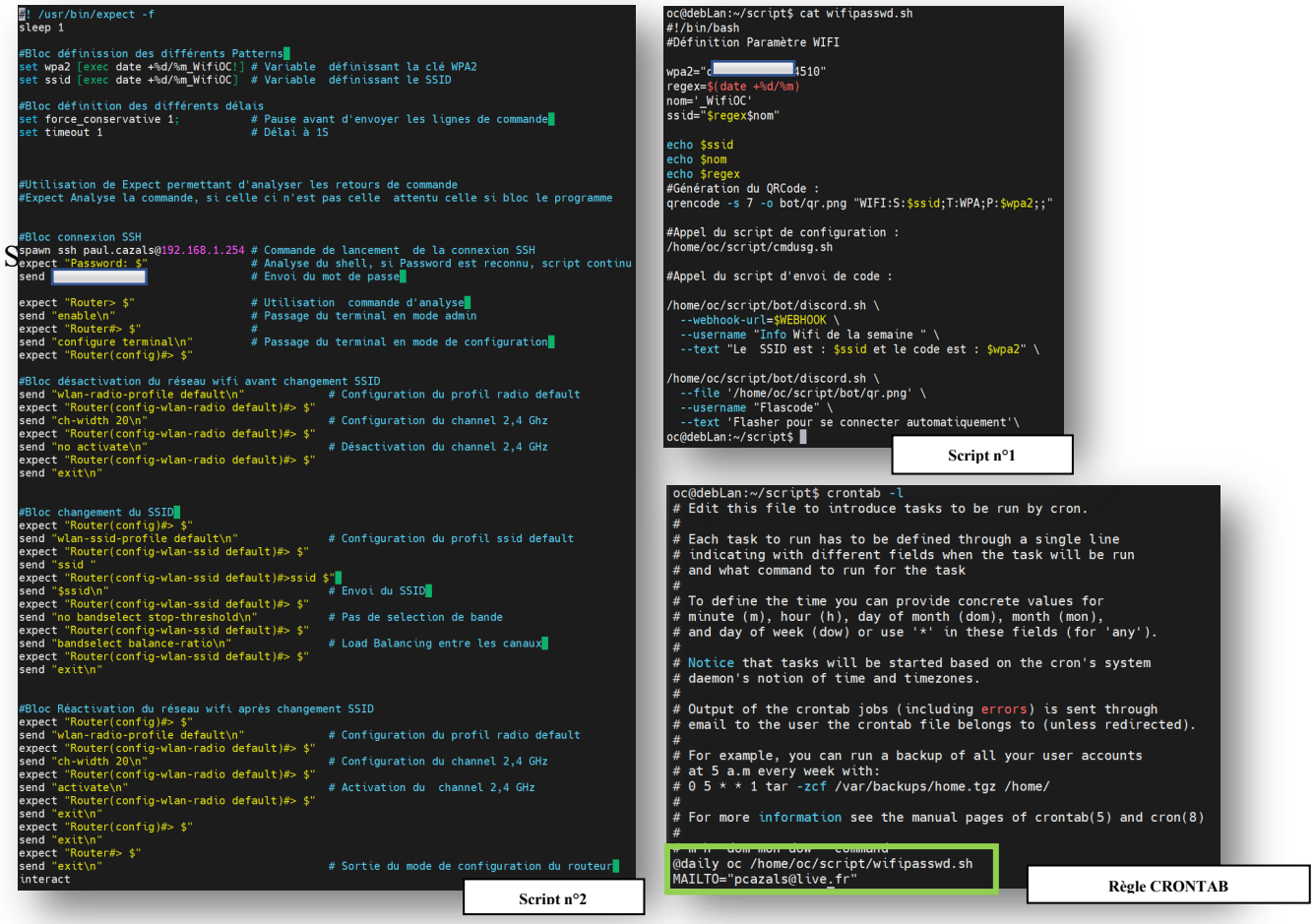


Figure 16 : Différents scripts permettant l'auto-configuration

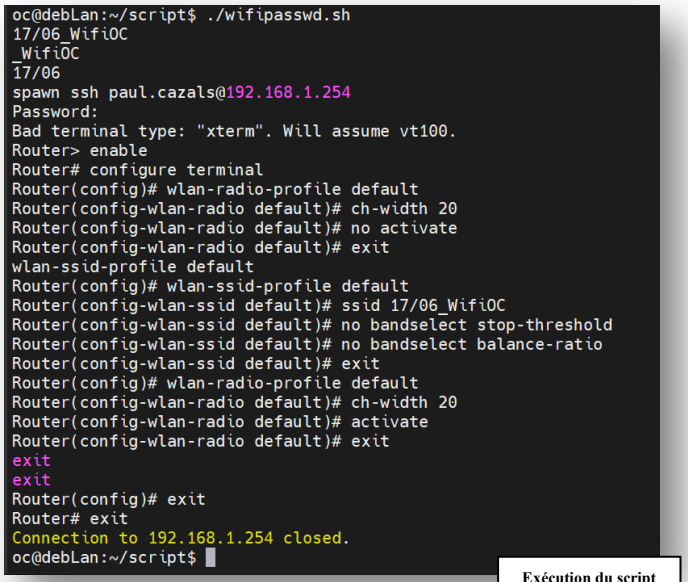
L'utilitaire que j'utilise pour lancer le script de manière autonome est Crontab. C'est un outil présent sur la plupart des systèmes Linux qui permet de lancer des applications de façon régulière.
Pour le configurer, il suffit d'ajouter des règles dans le fichier de configuration (`crontab -e`).
La syntaxe de la commande à ajouter est la suivante.

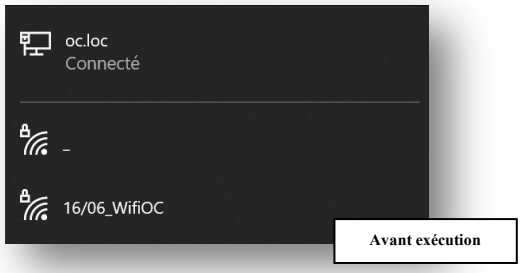
```
# Example of job definition:
# .---------------- minute (0 - 59)
# |  .------------- hour (0 - 23)
# |  |  .---------- day of month (1 - 31)
# |  |  |  .------- month (1 - 12) OR jan,feb,mar,apr ...
# |  |  |  |  .---
- day of week (0 - 6) (Sunday=0 or 7) OR sun,mon,tue,wed,thu,fri,sat
# |  |  |  |  |
# *  *  *  *  *  <user> <command to be executed>
```

Il faut commencer par définir la périodicité, ensuite définir quel utilisateur lance la commande puis pour finir quelle commande exécuter.
Dans notre cas, il est souhaitable que le script se lance tous les jours. Cela nous donnera donc la commande suivante (à voir également la figure 8).

```
# 1  0  *  *  *  oc ~/script/wifipasswd.sh
```

A noter que <`@daily`> peut remplacer <`1  0  *  *  *`>. Notre script se lance donc tous les jours à 00h01 et se charge des changements de manière autonome.





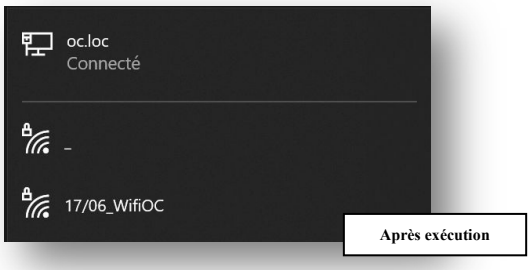


Figure 17 : Résultats des actions du BOT

3.3 Découverte du métier de Technicien

Une partie de mon stage qui a également été importante, était la découverte à part entière du métier de technicien. J'ai en effet, pris place dans l'atelier à côté des différents « Techs » comme ils sont appelés et après une petite semaine d'observation, j'ai pu comprendre leurs manières de travailler.

L'organisation de l'entreprise est simple et efficace. Le technico-commercial (Patrick ROSSI) vend différents packs de maintenance aux entreprises comprenant 50 heures, 100 heures, 1500 heures etc. Cela signifie que pour chaque intervention effectuée, mise en place du réseau, maintenance d'infrastructure, assistance sur les postes utilisateurs, mise en place de serveur, et bien d'autre ; le temps passé est compté à la minute prête et sera déduit du nombre total d'heures du pack de maintenance vendu. La même organisation est adoptée pour le service reprographie sous forme de « Contrat Copie ».
Au préalable de l'intervention, les entreprises contactent Office Center via le mail de contact ou directement en appelant le standard. Ensuite, la secrétaire crée une fiche d'appel sur le logiciel de Gestion « Gestco » qui est un logiciel « maison », développé et maintenu par le chef d'entreprise M. Raspail. Ce logiciel permet de suivre les différentes infrastructures installées chez les clients, facturer les appels, faire une récapitulation d'intervention et bien d'autres fonctions utiles à l'entreprise.

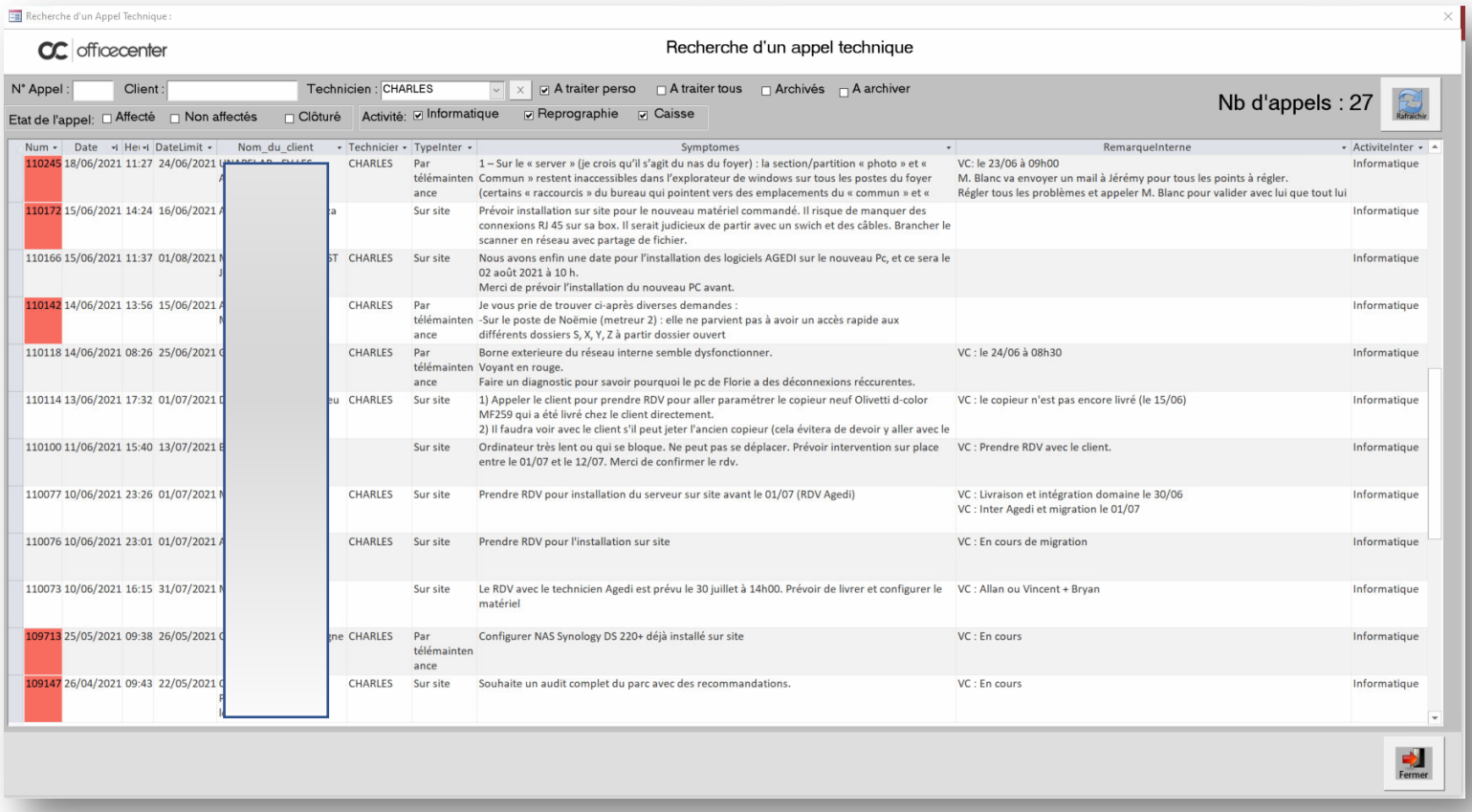


Figure 18 : Logiciel « Gestco » centralisant tous les appels

Selon le besoin du client, trois types d'intervention peuvent être mises en place. Soit les techniciens font une intervention en télémaintenance via différents logiciels tel que TeamViewer et Anydesk, soit le client emmène en atelier l'appareil sur lequel il a besoin d'une maintenance et les tâches à effectuer seront réalisées le plus tôt possible.
Un dernier type d'intervention au cas ou les deux premières ne sont pas possibles, sont les interventions sur site. Le technicien se déplace donc avec une des voitures de fonction sur le lieu de l'infrastructure en question.

Dans les trois cas d'intervention, un technicien qualifié doit intervenir. Il doit essayer de régler les problèmes dans les plus brefs délais. Les qualités requises sont donc efficacité, rapidité, communication et adaptation. Adaptation car lorsqu'il exerce dans une Société de Services Informatiques, il peut être alors amené à découvrir des domaines très différents au fil des missions.

Malgré la mise en place et la réalisation de ma mission de stage, nous avons jugé avec mon tuteur d'entreprise, qu'il serait également intéressant de me faire pratiquer le métier en effectuant différentes demandes des clients.
J'ai donc, lorsqu'il m'en était possible et que j'en avais les capacités pour réussir, effectué différentes interventions dans différents cas de figure. Au total, j'aurais réalisé une centaine d'interventions.
J'ai notamment pu me rendre sur différents sites de manière autonome, aller diagnostiquer des pannes et ensuite proposer une solution au client. Cet exercice était l'un des plus intéressants que j'ai pu pratiquer. Etant donné que je ne connaissais pas l'infrastructure existante, je devais analyser, comprendre le problème et essayer de le résoudre au mieux. Certaines interventions n'étaient vraiment pas compliquées, d'autres l'étaient un peu plus.
Ces types d'intervention m'ont beaucoup appris tant au niveau technique qu'humain. J'ai pu débloquer certaines personnes ne pouvant plus travailler et la reconnaissance acquise à la suite de mes actions n'est que plus réconfortante dans ma manière de travailler.

J'ai aussi pu assister et contribuer à différents Audit. Nous nous sommes rendus dans deux entreprises (Une Pharmacie et un Office de Tourisme) dans lesquels nous avons analysé toute l'infrastructure Informatique. Que ce soit la partie réseau avec la prise d'informations sur le FAI, le matériel utilisé, la configuration des équipements. Pour le matériel informatique, la configuration Hardware est relevée, l'utilisation de l'espace disque et le type de disque utilisé (SSD /HDD*), la taille de la messagerie, l'état de santé du serveur, etc. Tout cela permet ensuite de faire un rapport détaillé comprenant l'ensemble des relevés et l'ensemble des solutions d'amélioration qui pourraient être réalisées pour améliorer l'infrastructure tant au niveau des performances, de la sécurité et de la praticité. Tout est ensuite expliqué simplement de manière à ce que le client comprenne tous les points d'évolution et tous les choix technologiques les plus adéquats pouvant être fait sur son infrastructure.
Ainsi le client accepte (ou non) les propositions et une équipe de techniciens ira installer la nouvelle infrastructure rapidement.
Il m'a également été demandé de faire du rangement dans une baie réseau (en vue d'une évolution de celui-ci). Je suis donc allé sur site, ranger la baie, diagnostiquer les soucis qu'il y avait.
Le métier de technicien dans une petite entreprise comme celle-ci est vraiment très polyvalent et c'est ce qui m'a plu. Il faut être performant sur un nombre de points conséquents car les clients sont tous différents et n'ont pas les mêmes besoins. Tout type d'intervention est bonne à prendre pour évoluer dans ces compétences.

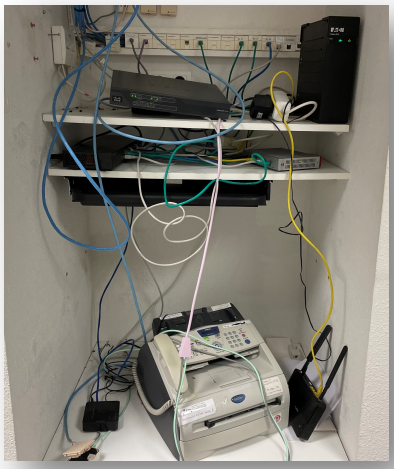


Figure 19 : Avant / Après de la baie réseau

3.4 Réalisation annexe

3.4.1 Auto-installation d'un logiciel Antivirus

Pour améliorer la rapidité d'exécution de certaines interventions techniques, mon maitre de stage m'a demandé de me pencher sur la réalisation d'un script permettant l'installation d'un logiciel antivirus de manière autonome. Ce logiciel en question, était plutôt fastidieux à installer et configurer, et faisait perdre un temp considérable aux différents techniciens. J'ai donc œuvré à la réalisation d'un script permettant une installation plus simple.

Pour ce faire, je me suis d'abord renseigné sur les différentes options d'installation. Une possibilité d'installation du logiciel ESET pouvait se faire en ligne de commande. Cela était très intéressant pour moi, car ces commandes pouvaient donc être utilisées pour configurer le logiciel à ma guise. Une autre possibilité était de le configurer en poussant des GPO* mais cela obligeait le PC à être intégrer dans un domaine.
Le souhait de l'entreprise était pour la configuration de :

- Ecraser l'installation si une précédente version est présente
- Configurer le logiciel en Français
- Désactiver le premier scan au démarrage
- Désactiver la solution de collecte des données du logiciel
- Activer le contrôle des applications
- Désactiver le scan d'antivirus sur les Disques Réseaux (pour éviter les ralentissements PC dans une infrastructure)
- Désactiver le contrôle des mises à jour Via Windows Update.
- Activer le logiciel avec la licence

Un but que je recherchais, était de pouvoir faire en un seul clic toute la configuration.
Il fallait donc que j'automatise :

- Le changement de répertoire pour aller trouver le fichier d'installation
- L'installation initiale du logiciel
- L'installation avancée du logiciel
- La suppression des différentes traces d'installation

J'ai donc peaufiné un premier script permettant de rapatrier le dossier d'installation sur le PC (cela était plus facile pour les droits d'exécution). En m'appuyant sur la documentation, j'ai pu déterminer la commande permettant de faire la configuration initiale.
Pour la configuration avancée, je n'ai pas trouvé de possibilité directe pour utiliser des commandes. Il fallait ouvrir le logiciel, aller dans les paramètres, puis dans les paramètres avancés, pour ensuite activer une fonctionne de paramétrage via une CLI. Cela n'avait donc plus aucun intérêt à mon sens. J'ai donc pris la décision d'installer une première fois le programme en manuel, exporter la configuration avancée pour ensuite réimporter cette configuration de manière autonome via un script envoyant des raccourcis clavier.
Pour ce faire j'ai utilisé un outil s'appelant SendKeys directement implanté dans les systèmes Windows (voir deuxième script dans les systèmes Windows). Il permet d'envoyer une ou plusieurs entrées clavier vers la fenêtre active comme si ces dernières étaient saisies depuis le clavier. Je me suis alors référencé à la documentation pour trouver les fonctions liées aux touches de navigation (Tabulation, Entrée et Espace majoritairement).
Cela semble dans un premier temps un peu barbare, mais cela fonctionne parfaitement après quelques réglages. Le logiciel s'installe et se configure donc de manière autonome et cela dans un laps de temps très court !

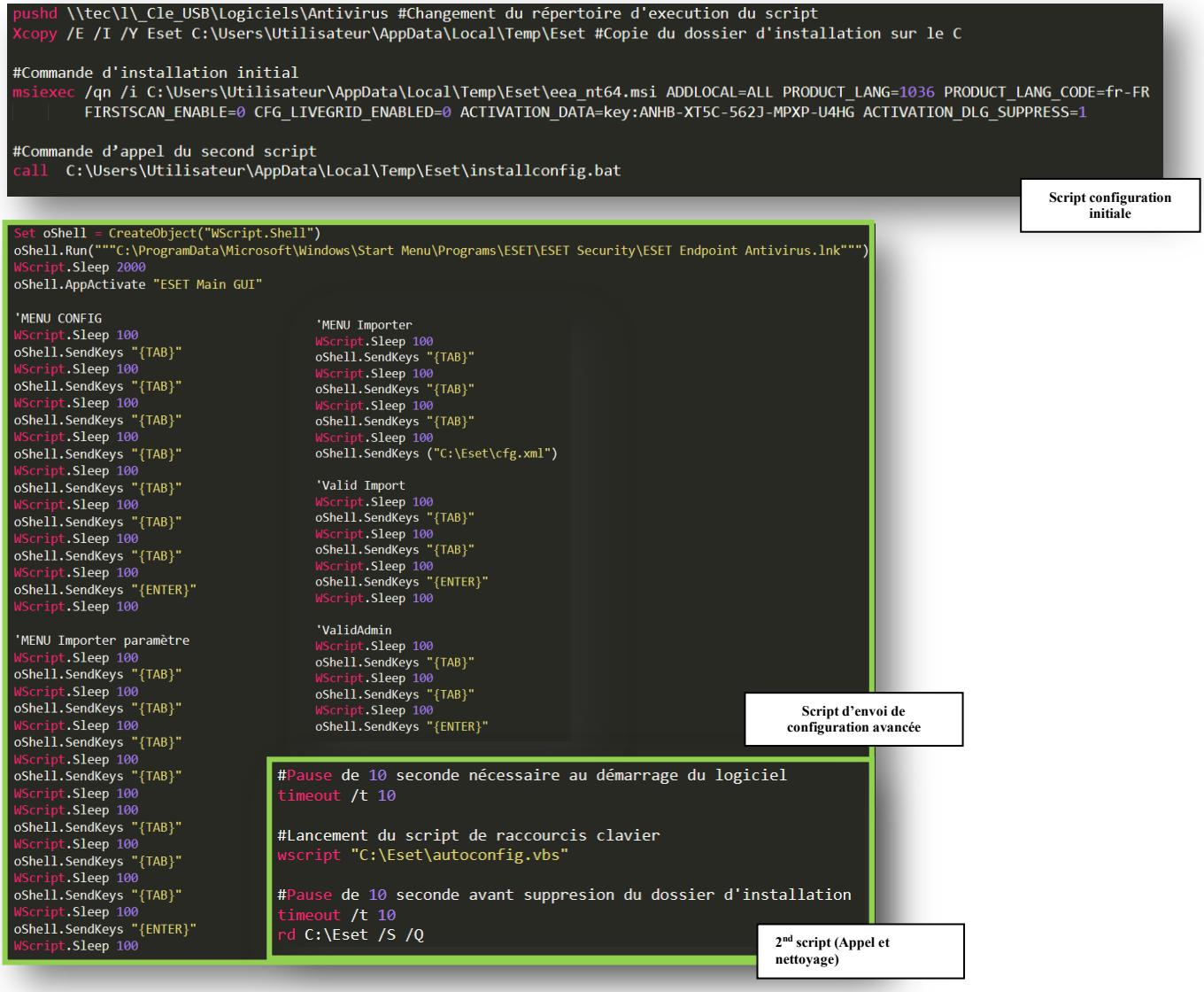


Figure 20 : Script d'auto-installation

3.4.2 Réalisation d'un Proxy de filtrage

Un client de l'entreprise avait une demande concernant la surveillance des activités informatique de ses employés. En effet, le personnel n'était pas productif car distrait par les outils de divertissements présents sur internet. Mon tuteur m'a demandé de me pencher dessus et m'a orienté sur la réalisation d'un proxy* de filtrage. Un proxy est un logiciel informatique qui joue un rôle d'intermédiaire en se plaçant entre deux hôtes pour faciliter et surveiller leurs échanges.
J'ai découvert la distribution linux pfSense qui n'est autre qu'un routeur/par-feu open source. Etant sous linux, il est possible d'installer des paquets externes et donc utiliser la distribution à sa guise.
J'ai découvert les paquets « Light Squid» et « Squid » permettant d'installer un proxy sur le réseau.
Il est donc possible de configurer ce proxy en mode transparent (ce que nous recherchions pour que la solution ne puisse pas être détectée par les employés), configurer des certificats d'autorité (obligatoires pour naviger sur des sites HTTPS) et une fonction s'appellant « SSL Man in the Middle* filtering » (littéralement filtre SSL en mode Homme du milleu), ce qui nous intéréssait particulièrement pour récupérer les données de navigation.

Après mettre appuyé sur la documentation et avoir fait une configuration correcte, nous avons pu relever sous forme de liste toutes les requêtes HTTP qui étaient faites sur le réseau. (voir figure 22).
Cependant, et malgré de nombreuses recherches, cette solution n'était pas viable. Les navigateurs, après contrôle du certificat, n'arrivaient pas à vérifier son authenticité et cela malgré le fait de placer le certificat dans les certificats d'autorité de confiance des paramètres de windows. Le navigateur avait donc conscience que le trafic était détourné vers un serveur (principe de l'attaque Man In The Middle) et bloquait la navigation. Nous avons donc pris la décision de ne pas poursuivre avec cette solution car elle aurait engendré beaucoup de souçis. Je me suis donc penché sur la mise en place d'un logiciel de surveillance et de contrôle à distance à la base destiné pour les salles informatiques des établissements scolaires. Cette solution était plus viable et permettait en plus, de surveiller les écrans à distance. Je me suis donc occupé de la mise en production de la solution, de la mini-formation au personnel concerné pour comprendre comment utiliser le logiciel. J'ai également expliqué l'utilisation et la configuration du logiciel adopté à mes cohéquipers, pour qu'en cas de soucis, les techniciens puissent comprendre d'où pourrait venir le problème. Cette rapide explication de mise en place se retrouvera dans l'annexe.

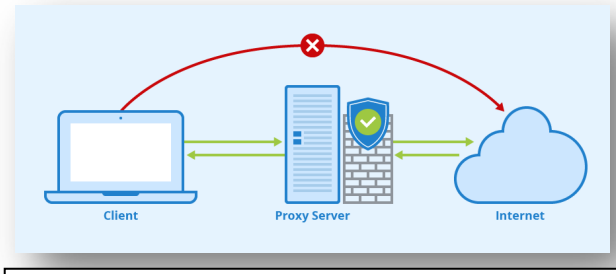


Figure 21 : Fonctionnement d'un Proxy

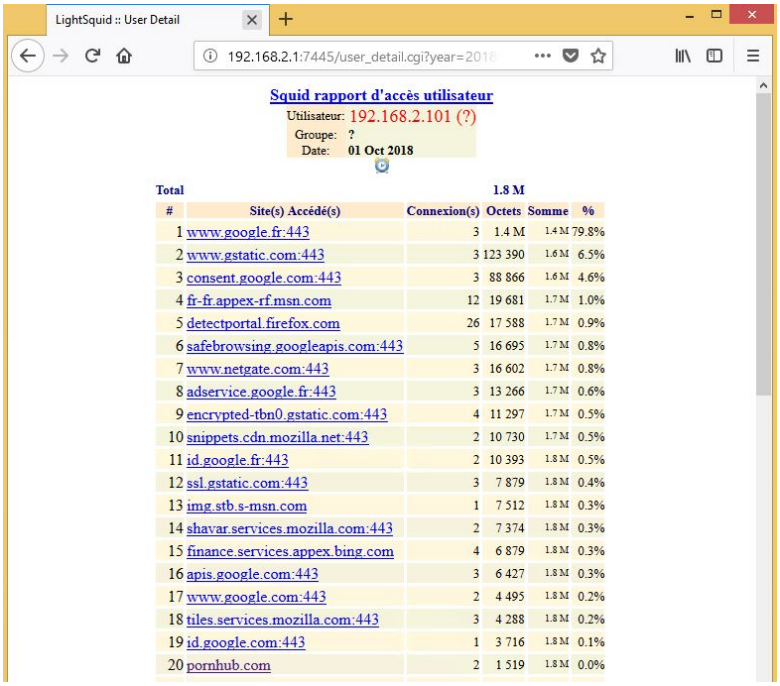


Figure 22 : Fenêtre de résultats des requêtes HTTPs en fonction des utilisateurs via le proxy pfSense

Vous retrouverez également en annexe un document que j'ai réalisé pour aider à la mise en place d'un serveur NAS*. La configuration devait permettre de sécuriser un maximum le NAS et de configurer des sauvegardes en fonction des besoins des clients.

3.4.3 Pré-Conclusion

J'ai pu réaliser de nombreuses interventions qui m'ont fait découvrir beaucoup de choses. Que ce soit la manière de travailler en autonomie, trouver des solutions en fonction des besoins des clients et par la sorte, acquérir de nouvelles compétences telle qu'apprendre et utiliser des nouveaux logiciels etc.
Je n'ai pas tout développé dans ce rapport car j'ai vraiment fait énormément de choses différentes, mais si je devais en mettre une seule en avant, ce serait la capacité de réflexion qu'il faut avoir pour aller au bon endroit et trouver les bonnes solutions. Le métier de technicien que j'ai découvert ces dernières semaines est un métier intéressant qui permet de faire évoluer ses compétences de jour en jour face aux nombreuses demandes et besoins des clients en termes de solution informatique.

4 Conclusion

Ce stage de fin d'études universitaires et technologiques a été très enrichissant sur de nombreux points. Sur le plan technique, j'ai pu améliorer mes connaissances et mes compétences dans le domaine de l'informatique et des réseaux, grâce notamment aux différentes interventions que j'ai pu effectuer et aux recherches permettant la réalisation de différents projets. Tout cela m'a également permis d'améliorer ma méthodologie de travail et d'être plus aguerri dans les actions que je mène.

Pour ce qui est du savoir être, le stage m'a donné de nombreuses occasions pour améliorer mon relationnel et ma capacité de travail en équipe. Le fait d'avoir été immergé dans l'équipe Office Center, d'avoir travaillé en tant que technicien, comprendre comment fonctionnait l'entreprise, travailler avec les autres services (administratif notamment) m'a beaucoup apporté.
J'ai également pu apporter des conseils et des compétences à certain technicien et ainsi s'entraider pour avancer.

Le plan professionnel a également été impacté de manière positive grâce à cette expérience. Les missions qui m'ont été données étaient très enrichissantes et passionnantes et n'ont fait qu'attiser mon souhait de poursuivre mes études en école d'ingénieur et pourquoi pas, un jour, gérer une équipe comme le fait mon maitre de stage aujourd'hui.

Même si toutes les missions initiales n'ont pas été abouties, le fait d'avoir pu activement participer à la vie de l'entreprise a été un gros plus pour moi. Cette expérience m'aura marqué et permis de progresser d'un point de vue scolaire, professionnel et humain, ce qui me servira sans aucun doute dans mes futurs projets qu'il soit professionnel ou personnel.

5 Remerciements

En tout premier lieu, je tiens à remercier mon responsable de stage Vincent CHARLES, le Chef d'entreprise Jérémy RASPAIL et toute l'équipe d'Office Center pour leur chaleureux accueil, pour m'avoir accepté en tant que stagiaire, m'avoir fait confiance sur la réalisation de projets et m'avoir fait partager pour chacun leurs expérience professionnelle et personnelle.

Je rapporte une nouvel fois mes remerciement à mon tuteur de stage et technicien en chef pour m'avoir guidé tout au long de ces semaines, m'avoir apporté des conseils pour ma vie professionnel et personnel tout en m'apportant de nouvelles compétences techniques.

Je tiens également à adresser mes remerciements à Allan PRIMITTERA pour sa bienveillance à mon égard et tous les conseils qu'il aura pu me transmettre.

Enfin, qu'il me soit permis d'adresser tous mes remerciements au corps enseignant pour m'avoir fait monter en compétence et permettre la réalisation de ce stage et en particulier remercier mon responsable académique pour les conseils et l'attention dont ils ont fait preuve à mon égard lors de la totalité de mon stage.

6 Glossaire

- **DUT,** Diplôme Universitaire de Technologie
- **SARL,** Société commerciale où la responsabilité des associés est limitée au montant de leurs apports.
- **AUDIT**, L'audit est une expertise professionnelle effectuée par un agent compétent et indépendant aboutissant à un jugement par rapport à une norme sur les états financiers, le contrôle interne, l'organisation, la procédure, ou une opération quelconque d'une entité.
- **FAI**, Fournisseur d'Accès à Internet
- **PME**, Petite Moyenne Entreprise
- **VPN**, Virtual Private Network : En informatique, un réseau privé virtuel ou réseau virtuel privé, plus communément abrégé en VPN, est un système permettant de créer un lien direct entre des ordinateurs distants, qui isole leurs échanges du reste du trafic se déroulant sur des réseaux de télécommunication publics
- **SSH**, Secure Shell est à la fois un programme informatique et un protocole de communication sécurisé. Le protocole de connexion impose un échange de clés de chiffrement en début de connexion. Par la suite, tous les segments TCP sont authentifiés et chiffrés.
- **CLI**, Une interface en ligne de commande ou CLI (Commande Line Information) est une interface homme-machine dans laquelle la communication entre l'utilisateur et l'ordinateur s'effectue en mode texte : l'utilisateur tape une ligne de commande, c'est-à-dire du texte au clavier pour demander à l'ordinateur d'effectuer une opération
- **IOS**, Cisco IOS, anciennement IOS, est le système d'exploitation produit par Cisco Systems et qui équipe la plupart de ses équipements
- **WAN**, Wide Area Network, Un réseau étendu, souvent désigné par son acronyme anglais WAN, est un réseau informatique ou un réseau de télécommunications couvrant une grande zone géographique, typiquement à l'échelle d'un pays, d'un continent, ou de la planète entière. Le plus grand WAN est le réseau Internet.
- **LAN**, Un réseau local, en anglais Local Area Network ou LAN, est un réseau informatique où les terminaux qui y participent s'envoient des trames au niveau de la couche de liaison sans utiliser d'accès à internet.
- **VLAN**, Virtual Local Area Network, Réseau local virtuel est un réseau informatique logique indépendant. De nombreux VLAN peuvent coexister sur un même commutateur réseau.
- **QoS,** Quality of services ou qualité de service est la capacité à véhiculer dans de bonnes conditions un type de trafic donné, en termes de disponibilité, débit, délais de transmission, gigue, taux de perte de paquets…

- **SNMP**, Simple Network Management Protocol, en français « protocole simple de gestion de réseau », est un protocole de communication qui permet aux administrateurs réseau de gérer les équipements du réseau, de superviser et de diagnostiquer des problèmes réseaux et matériels à distance.
- **ACL,** Access Control List, liste de contrôle d'accès en français — désigne traditionnellement deux choses en sécurité informatique : un système permettant de faire une gestion plus fine des droits d'accès aux fichiers que ne le permet la méthode employée par les systèmes UNIX.
- **SSL**, La Transport Layer Security ou « Sécurité de la couche de transport », et son prédécesseur la Secure Sockets Layer ou « Couche de sockets sécurisée », sont des protocoles de sécurisation des échanges par réseau informatique, notamment par Internet.
- **Progiciel,** Un progiciel, un logiciel professionnel standard ou parfois paquet logiciel est un terme commercial qui désigne un logiciel applicatif généraliste aux multiples fonctions, composé d'un ensemble de programmes paramétrables et destiné à être utilisé par une large clientèle
- **DHCP,** Dynamic Host Configuration Protocol est un protocole réseau dont le rôle est d'assurer la configuration automatique des paramètres IP d'une station ou d'une machine, notamment en lui attribuant automatiquement une adresse IP et un masque de sous-réseau.
- **PXE,** Preboot Exécution Environment, L'amorçage PXE permet à une station de travail de démarrer depuis le réseau en récupérant une image de système d'exploitation qui se trouve sur un serveur. L'image ainsi récupérée peut être le système d'exploitation brut ou bien le système d'exploitation personnalisé avec des composantes logicielles.
- **Token Ring,** le token ring ou anneau à jeton est une topologie de réseau associée à un protocole de réseau local qui fonctionne sur la couche « liaison » du modèle OSI
- **OS,** Opérating System ou Système d'exploitation, est un ensemble de programmes qui dirige l'utilisation des ressources d'un ordinateur par des logiciels applicatifs.
- **ISO,** Un ISO est une image disque proposant la copie conforme d'un disque.
- **RAM,** Random Access Memories et la mémoire mémoire vive d'un ordinateur
- **ROM,** Mémoire qui ne permet que la lecture des informations qu'elle contient (mémoire morte).
- **HyperV,** Hyper-V, également connu sous le nom de Windows Server Virtualisation, est un système de virtualisation basé sur un hyperviseur 64 bits de la version de Windows Server 2008
- **BOT,** Un bot informatique est un agent logiciel automatique ou semi-automatique qui interagit avec des serveurs informatiques.

- **CRONTAB,** cron est un programme qui permet aux utilisateurs des systèmes Unix d'exécuter automatiquement des scripts, des commandes ou des logiciels à une date et une heure spécifiée à l'avance, ou selon un cycle défini à l'avance
- **MDT,** Microsoft Deployment Toolkit, est la solution gratuite de déploiement de Microsoft. Elle repose sur le kit de déploiement Microsoft ADK. Cette solution permet l'automatisation de la création, de l'entretien et du déploiement de socle de système d'exploitation
- **SSD,** Solid State Drive, support de stockage numérique de données informatiques
- **HDD,** Hard Disk Drive, support de stockage physique de données informatiques
- **GPO,** Group Policy Object ou stratégies de groupe sont des fonctions de gestion centralisée de la famille Microsoft Windows. Elles permettent la gestion des ordinateurs et des utilisateurs dans un environnement Active Directory.
- **Proxy,** Un proxy est un composant logiciel informatique qui joue le rôle d'intermédiaire en se plaçant entre deux hôtes pour faciliter ou surveiller leurs échanges.
- **Man In The middle,** L'attaque de l'homme du milieu ou man-in-the-middle attack, parfois appelée attaque de l'intercepteur, est une attaque qui a pour but d'intercepter les communications entre deux parties, sans que ni l'une ni l'autre ne puisse se douter que le canal de communication entre elles a été compromis
- **NAS,** Un serveur de stockage en réseau, également appelé stockage en réseau NAS, est un serveur de fichiers autonome, relié à un réseau, dont la principale fonction est le stockage de données en un volume centralisé pour des clients réseau hétérogène

7 Bibliographie

Empson, S. (April 17, 2005). *CCNA Command Quick Reference (Cisco Networking Academy Program)* .

- Documentation officielle du Switch DLINK utilisé
http://files.dlink.com.au/Products/DGS-3100-48P/Manuals/DGS-3100_series_A1_User_Manual_v2.20.pdf

- Documentation officielle du Logiciel ESET pour les CLI
https://help.eset.com/eea/7/en-US/installation_command_line.html

- Documentation officielle de la commande SendKeys
https://docs.microsoft.com/fr-fr/dotnet/api/system.windows.forms.sendkeys?view=net-5.0

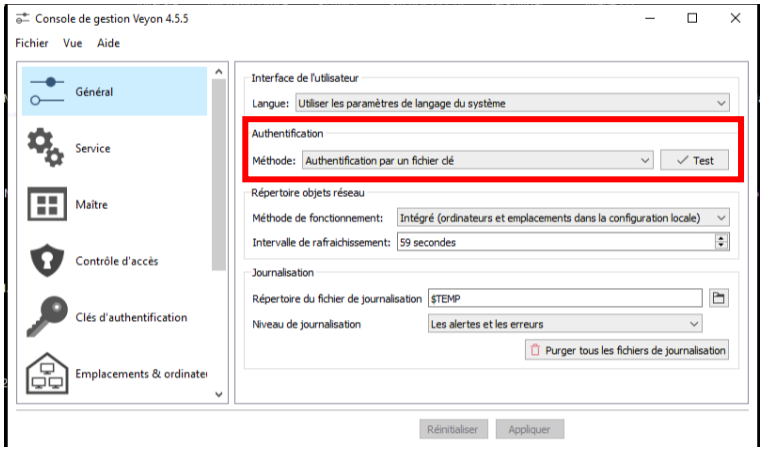
- Documentation officielle du logiciel SQUID
https://docs.diladele.com/faq/squid/dns_filtering_server.html

Annexe du Rapport de STAGE – Office Center – CAZALS Paul

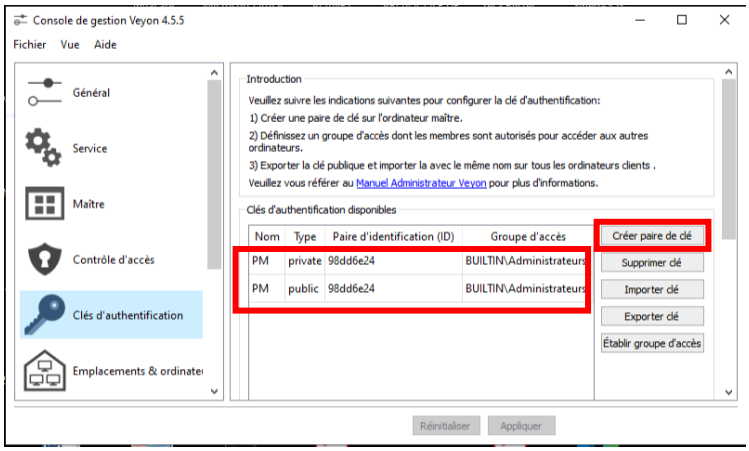
Logiciel Supervision écran PC

Le logiciel Veyon est un logiciel qui permet la supervision de PC à distance.
La version « master » du logiciel qui permet le contrôle et la supervision a été installé sur le Pc de Mr Christophe Gasser avec la configuration suivante :

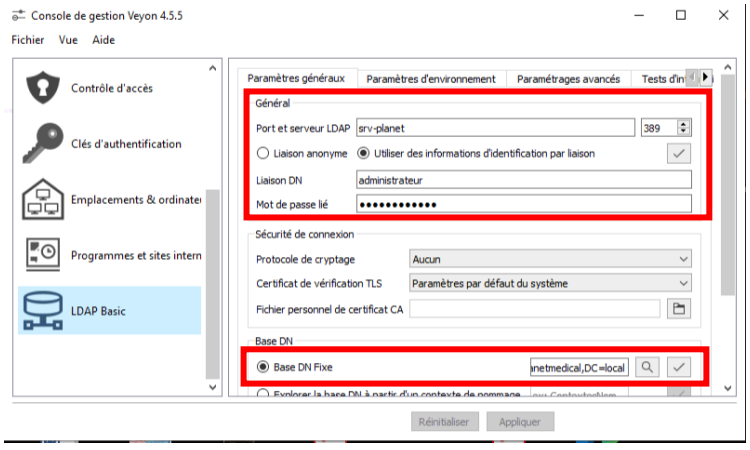
Dans Veyon Configurator :



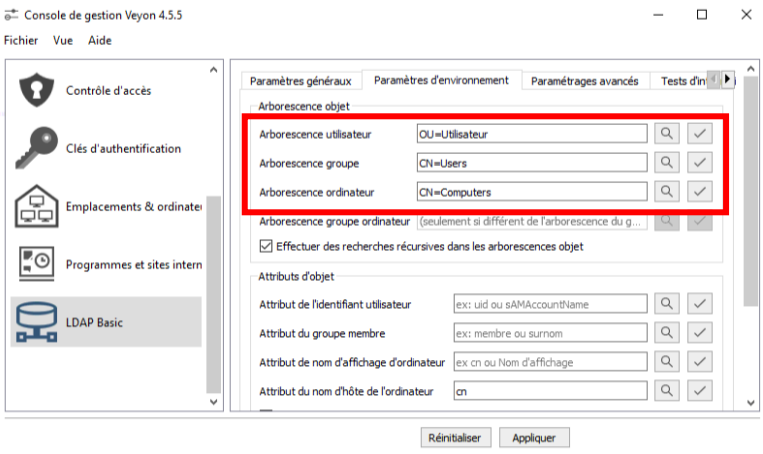
1. Changer le mode d'authentification en « authentification par un fichier clé »



2. Générer une paire de clé et exporter la clé publique.



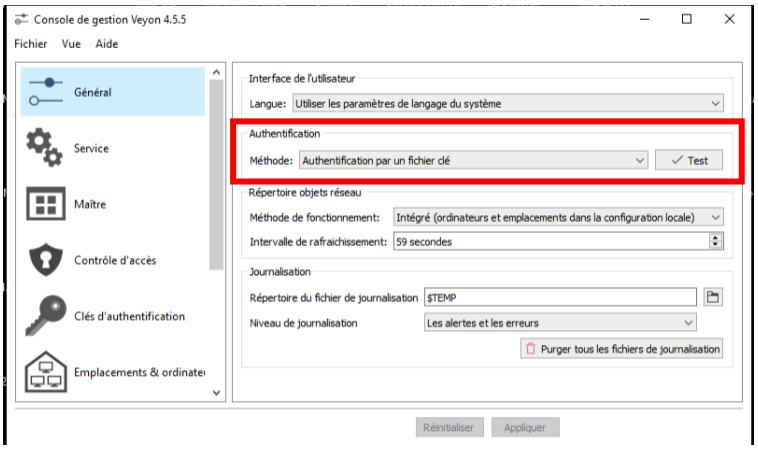
3. Configuration du serveur AD afin de récupérer le nom des postes de manière automatique



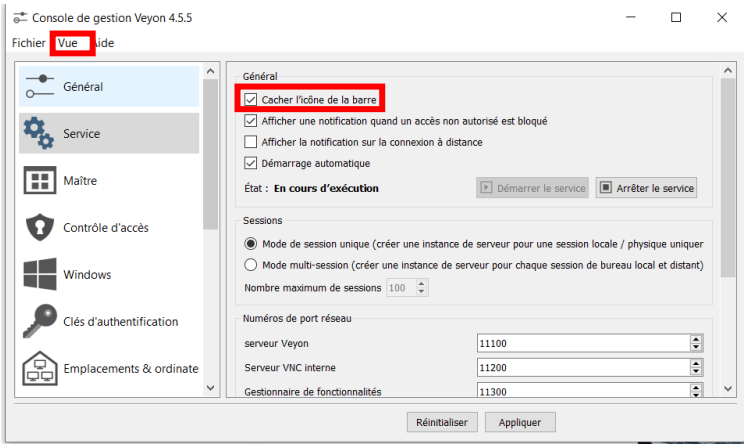
4. Adaptation des différentes arborescences dans les « paramètres d'environnement »

Tél. 04 92 31 39 75
Fax. 04 92 32 09 52
Courriel : contact@officecenter.fr
Bât. N°2, Parc d'activités St Pierre
04 510 Le Chaffaut/Saint-Jurson
SIRET 300 635 216 00058 - S.A.R.L. au capital de 50.000€

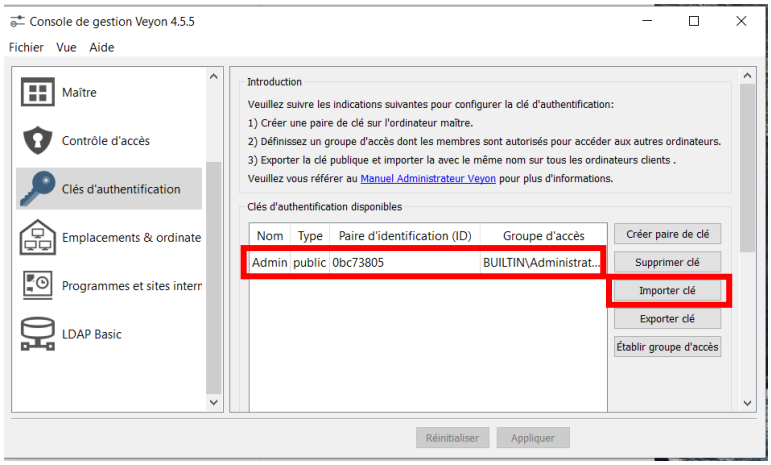
Concernant la configuration des Pcs surveillée (Veyon Configurator)



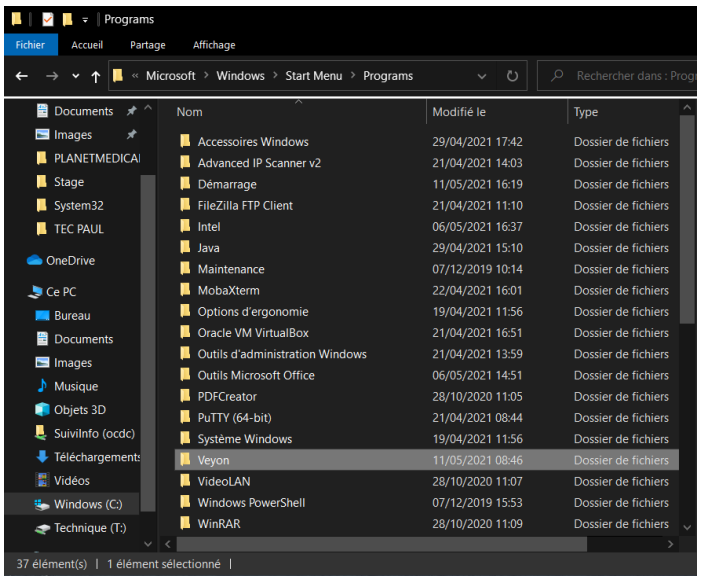
1. Changer le mode d'authentification en « authentification par un fichier clé »



2. Après avoir activé la vue confirmé (Menu Vue > confirmé), dans Service activer « Cacher l'icône de la barre)



3. Importer la clé publique précédemment importé.



4. Supprimer le raccourcis « Veyon » du menu démarrer (pour être un maximum transparent)

C:\ProgramData\Microsoft\Windows\Start Menu\Programs

Tél. 04 92 31 39 75
Fax. 04 92 32 09 52
Courriel : contact@officecenter.fr
Bât. N°2, Parc d'activités St Pierre
04 510 Le Chaffaut/Saint-Jurson
SIRET 300 635 216 00058 - S.A.R.L. au capital de 50.000€

Configuration NAS Synology

1. Premier démarrage

- ☐ Nom du serveur : NAS-Commun-<*Abréviation nom client ex : OC*>
- ☐ Compte Synology : Créer avec compte mail du client
- ☐ IP statique du NAS : 192.168.1.220 (Si disponible)
- ☐ Login : adminoc / mot de passe : Pa$$w0rd<*qqchose*>

2. Mise à jour du NAS

- ☐ Installation automatique des MaJ : Panneau de configuration **>** MaJ et restauration **>** Option de MaJ **>** Week-End

3. Notification

- ☐ Activer notification par Email : Panneau de conf **>** Notification **>** Email
    - Adresse électronique du destinataire : ###@officecenter.fr
    - Préfixe du sujet : NAS-Commun-<*Abréviation nom client ex : OC*>
    - Fournisseur de service : SMTP Personnalisé
    - Serveur SMTP : serveur smtp mail client
    - Port SMTP : port smtp mail client
    - Nom d'utilisateur : mail client
    - Mot de passe : mdp client
    - Connexion SSL : Coché
    - Nom de l'expéditeur : NAS-Commun-<*Abréviation nom client ex : OC*>-<*Usage : ex : Serveur/Backup/Slave*>
    - Adresse email de l'expéditeur : mail client

4. Sécurité

- ☐ Activer blocage automatique : Panneau de conf **>** Connectivité **>** Sécurité **>** Compte **>** Blocage auto
- ☐ Désactiver le compte Admin et Guest : Panneau de conf **>** Utilisateur **>** modifier compte admin **>** Désactiver ce compte
- ☐ Activer mot de passe fort : Panneau de conf **>** utilisateur **>** avancé **>** **Exclure mot de passe faible** et **inclure caractères spéciaux**.
- ☐ Activer la double authentification (pour compte admin)
    - Panneau de conf **>** Utilisateur **>** Avancé **>** Vérification en 2 étapes
    - Adresse mail : ###@officecenter.fr
    - Télécharger QRCODE + Récupérer la clé secrète
    - Télécharger Application Authy et ajouter QR CODE.
- ☐ Activer le pare-feu
    - Panneau de configuration **>** Sécurité **>** Pare-feu **>** Activer le pare-feu
        - Modifier les règles
        - Ajouter une règle autorisant le trafic venant des IP françaises (IP Source > Emplacement > France) et une règle autorisant le trafic venant du LAN (IP spécifique > plage d'ip > *par exemple : 192.168.1.1 à 192.168.1.254*)
- ☐ Activer HTTPS :
    - Panneau de configuration **>** Réseau **>** Paramètres DSM **>** Rediriger automatiquement les connexions http vers HTTPS pour le bureau DSM
- ☐ Changer le port HTTPS :
    - Panneau de configuration **>** Réseau **>** Paramètres DSM
        - HTTP : 8888
        - HTTPS : 8889
- ☐ Activer Protection DDOS
    - Panneau de configuration **>** Connectivité **>** Sécurité **>** Protection **>** Activer la protection DOS

5. Ajout de fonctionnalité

- ☐ Versionnage de fichier
  - Télécharger Synology Drive Server (**si le nas est serveur de fichier**) et/ou Active Backup for Business (**si le nas est le système de sauvegarde**)
  - Ouvrir dans le centre des paquets « console d'administration Synology Drive »
    - Dossier de l'équipe > <*Dossier à versionniser ex : commun/scan*> Activer > Activer le contrôle de version > OK
- ☐ Sauvegarde d'un serveur et/ou PC
  - Installer active backup for Business sur le NAS
    - Activer le compte avec : ###@officecenter.fr et mdp : Pa$$w0rdoc
  - Installer client active backup for bussiness sur les PCs (https://global.download.synology.com/download/Utility/ActiveBackupBusinessAgent/2.2.0-2070/Windows/x86_64/Synology%20Active%20Backup%20for%20Business%20Agent-2.2.0-2070-x64.msi?model=DS220%2B&bays=2&dsm_version=6.2.4&build_number=25556&_ga=2.199135471.1970811477.1624440770-1867119092.1621349682)
    - Adresse du serveur : IP du Nas
    - Login : adminoc
    - Mot de passe : Pa$$w0rd<*qqchose*>
    - Si erreur de certificat : Procéder quand même
  - Sur le NAS, ouvrir Active Backup for Business
  - Si le terminal à sauvegarder est un serveur : PC > Plus > Changer de type de périphérique > Oui
  - Pour sauvegarder
    - Créer une tâche > La nommer proprement (*Ex : sauv_<nom_PC>_quotidien*) > Suivant > Sélectionner Dossier > Suivant > Sélectionner les éléments à sauvegarder > Suivant > Sélectionner l'intervalle de sauvegarde > Appliquer les méthodes suivantes (Selon stockage disponible et volume de données à sauvegarder)
      - Conserver uniquement les dernières **3** versions
    - Appliquer
- ☐ Externaliser les sauvegardes sur HDD
  - Télécharger HyperBackup
  - Créer une tache de sauvegarde > Sélectionner le dossier de destination de la sauvegarde > Sélectionner les dossiers à sauvegarder (*Ex : Commun / SCAN*) > Ne pas sélectionner d'application à sauvegarder > Configurer les paramètres de la sauvegarde :
    - ACtover la notification des tâches
    - Compresser les données de sauvegarde
    - Calendrier de sauvegarde : Quotidienne à 01 :00 (voir selon besoin du client)
    - Vérification d'intégrité : Oui si le volume de données ne dépasse pas les 1 To
  - Paramètre de rotation
    - A partir des versions les plus anciennes