LYCÉE CABANIS

PLANQUE CLÉMENT

DOSSIER DE SYNTHÈSE

2017 - 2020

Remerciements :

Dans le cadre de ma formation professionnelle au lycée Georges Cabanis, j'ai eu l'opportunité d'effectuer trois périodes de stages au sein de différentes entreprises.

C’est pourquoi, j’aimerais remercier l’équipe pédagogique professionnelle et l’équipe pédagogique des matières générales du lycée. J’aimerais aussi remercier mes tuteurs ainsi que les employés des entreprises qui m’ont accueilli.

Ces stages m’ont permis non seulement d’appliquer ce que j’avais appris en cours mais aussi d’acquérir de nouvelles connaissances et de découvrir le monde professionnel.

Présentation Personnelle :

Depuis toujours, je suis passionné d'informatique, je m'en sers du divertissement au traitement de texte en passant par la programmation et le montage photo / vidéo. J'aime bien analyser le fonctionnement de logiciels ou de sites internet car ça me permet de comprendre comment l'informatique qui nous entoure interprète les choses. J'ai alors choisi de vivre de ma passion. Après mûres réflexions, j'ai décidé de devenir Technicien réseau. Cela me plairait beaucoup étant donné qu'il faut principalement analyser la situation afin de comprendre ce qui ne va pas. Par exemple, si un routeur ne fonctionne plus, on commence par vérifier le branchement et l'état des câbles puis si ce n'est pas le problème, on vérifie le routeur. C'est pour le côté réflexion, que j'ai décidé d'aller en Bac professionnel SN (Systèmes Numériques) afin de me spécialiser sur la section RISC (Réseaux Informatiques et Systèmes Communicants).

Lors de mon cursus, je devais réaliser plusieurs Périodes de Formations en Milieux Professionnels en entreprise chaque année. Lors de ces formations, j'ai pu découvrir plusieurs types d'entreprises, à savoir, les entreprises publiques, qui dépannent pour les particuliers, les magasins ainsi que les entreprises privées qui s'occupent uniquement des professionnels.

Ces différentes entreprises m'ont permis de découvrir le Monde du travail et m'ont appris énormément de choses sur l'informatique et le réseau.

Planque Clément

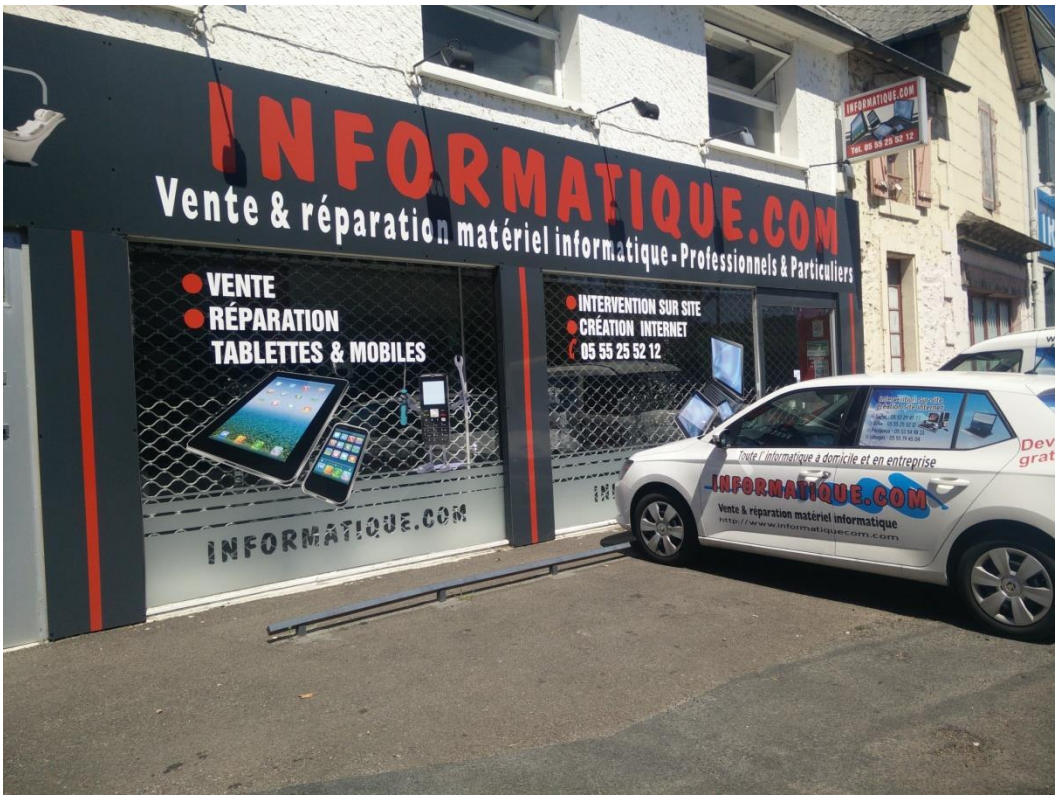
Seconde SN

Lycée Cabanis

Période de stage : du 04/06/18 au 06/07/18

Entreprise : ***INFORMATIQUE.COM***

112 bis Avenue Jean Abbe Alvitre 19100 Brive



Sommaire de la PFMP 1 :

Présentation de l'Entreprise :

- **En quelques lignes :**

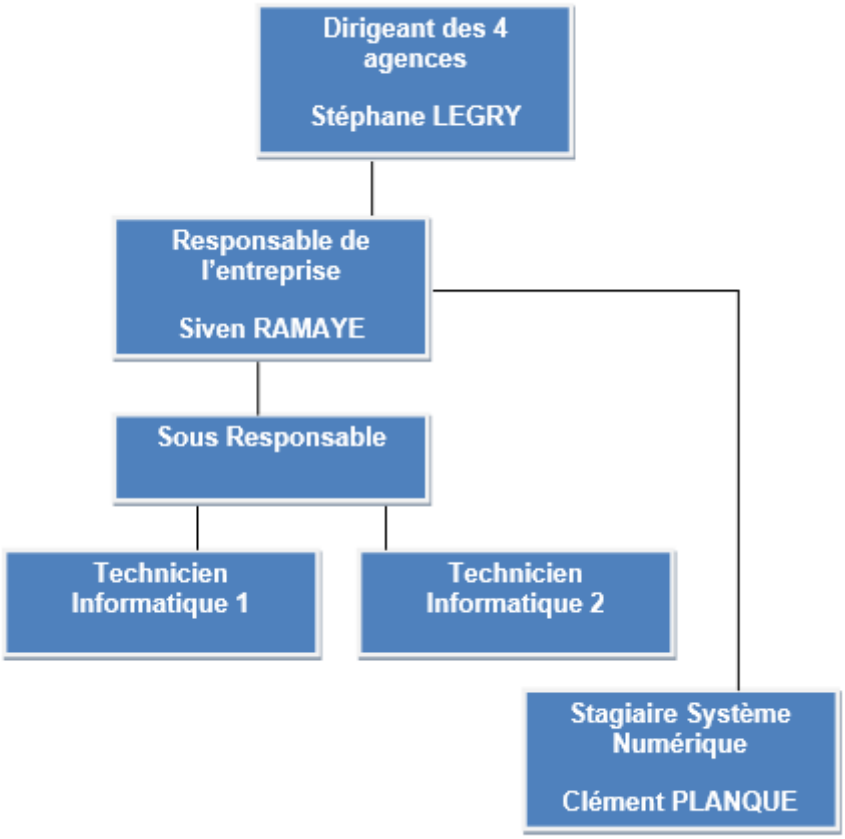
INFORMATIQUE.COM est un réseau d'agences de dépannages à domicile, pour les particuliers et les professionnels, qui intervient sur les zones de Sarlat, Brive, Périgueux et Limoges.

Ces agences disposent chacune d'un magasin proposant la vente de matériels informatique, de l'ordinateur fixe au portable en passant par la tablette ; mais aussi de matériel et fournitures de bureautique.

Elles se composent également chacune d'une équipe de techniciens spécialisés, qui réalisent des prestations très variées allant du dépannage en informatique aux installations de connexion internet, en passant par la création de sites internet, de la maintenance et même de la formation.

Enfin, ces agences travaillent en sous-traitance pour certains fournisseurs d'accès internet et opérateurs de téléphonie mobile.

Organigramme de l'entreprise de Brive dans laquelle j'ai effectué mon stage :



- **<u>Activité en Entreprise</u> :**

Durant ma PFMF, j'ai principalement réalisé des réparations d'ordinateur, de tablettes et de téléphones de tous types. J'ai aussi effectué des interventions chez des particuliers. Dans ces interventions, je testais des lignes ADSL afin de vérifier si les problèmes vis-à-vis d'internet venaient d'une cause extérieure ou s'ils venaient de chez le client.

Pour cela, j'utilisais un Voltmètre, et un appareil conçu pour tester la ligne ADSL. Ces éléments seront développés dans l'étude de cas.

Pour les téléphones, il fallait souvent remplacer le bloc LCD et la vitre tactile. Cette opération est très délicate car les composants du téléphone sont très fragiles et de petites tailles. Sur certains téléphones, il fallait chauffer l'écran afin de le décoller pour cela, on utilisait un décapeur thermique.

Décapeur thermique et bloc LCD neuf

Pour les iPhones récents, il y avait un problème avec la mise à jour vers IOS 11 et le téléphone se retrouvait bloqué au démarrage. Afin de régler ce problème, il fallait faire une restauration du système via ITunes mais cela engendrait une perte de données. En effet cette opération entraine un retour aux réglages d'usine, c'est-à-dire l'état du téléphone lors de l'achat par le client, donc sans toutes les données qu'il a pu ensuite rajoutées : photos, applications, contacts etc … Or il était impossible techniquement de procéder à une sauvegarde des données en amont du dépannage.

Pour finir, de temps en temps, je devais vérifier les stocks des routeurs. Il faut savoir que les techniciens travaillent avec une dizaine de marques de routeurs et que chaque marque propose plusieurs modèles de routeurs. Je m'assurais donc que ce qui était écrit sur la fiche des stocks, correspondait avec ce qu'on avait en magasin. Cette fiche se trouvait sur le réseau intra de la boutique. Cette mission était très longue et très difficile car il fallait rester concentré tout le long sous peine de devoir recommencer.

- **<u>Conclusion personnelle</u> :**

Cette PFMP m'a beaucoup intéressé car j'ai appris des choses qu'on ne traitait pas en cours tel que la vérification de ligne ADSL. J'ai aussi eu l'occasion, grâce aux employés qui se sont occupés de moi, d'observer la méthodologie à adopter. Par exemple, pour démonter un ordinateur portable, il faut mettre une mousse en dessous afin de ne pas le rayer.

J'ai bien aimé les réparations d'ordinateur car il fallait adopter tout une procédure de diagnostiques afin de déterminer la source du problème et le corriger. J'ai aussi apprécié les interventions SFR.

Par contre, je n'aime pas du tout faire les stocks car cela ne m'a pas intéressé. Je suis bien conscient que cela permet de savoir rapidement où sont les routeurs et combien il en reste. Pourtant j'ai trouvé fastidieux de le faire trois fois par semaines.

Photo de l'atelier.

Derrière le comptoir se trouve des cartons. Ceux-ci contiennent des routeurs. Sur le comptoir nous apercevons des routeurs prêts à être chargés dans les véhicules d'intervention.

Etude de cas :

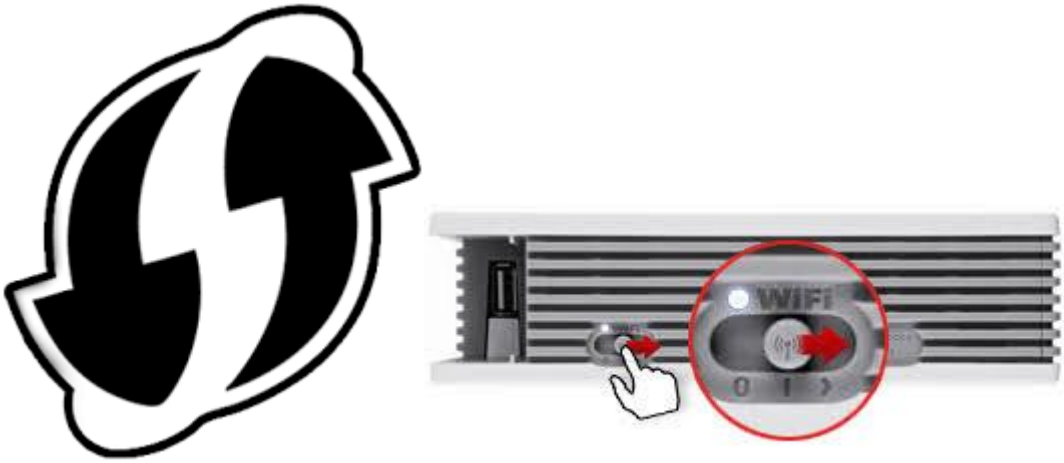
L'étude de cas que je vais traiter sera une intervention à domicile sur un problème de connexion internet avec pour opérateur SFR. J'ai choisi cette intervention car tout d'abord elle nécessite d'intervenir sur le réseau internet et que mon projet professionnel est de faire du dépannage internet mais aussi de l'installation. De plus cette intervention a été plus longue que les autres interventions que j'avais faites auparavant.

Nous avons donc suivi **le protocole d'intervention suivant :**

1ère étape :

Pour commencer, nous devons vérifier si ce que dit le client est vrai. Pour cela, nous accédons à la box SFR qui était dans son bureau et nous nous y connectons avec la fonction WPS (Wifi Protected Setup). Cette fonction permet de se connecter à un réseau Wifi sans avoir besoin du mot de passe.

Box SFR du client



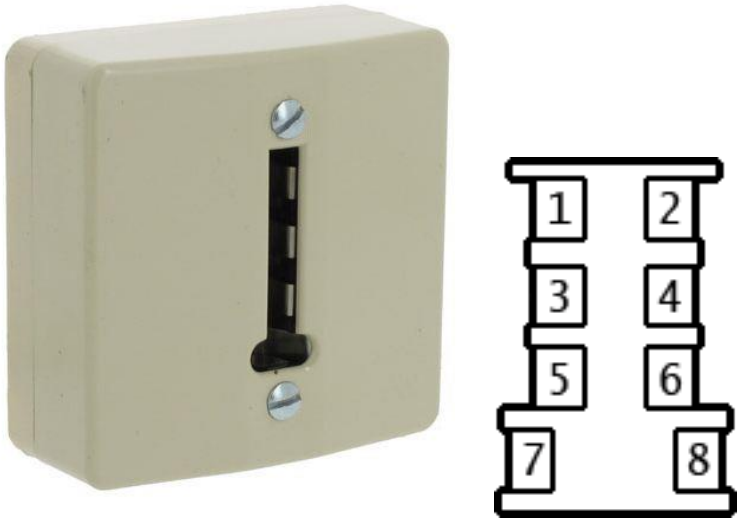
Icône représentant la fonction WPS. Nous pouvons le trouver sur toutes les box SFR hormis celle-ci ou il faut pousser le bouton wifi vers la droite

2nd étape :

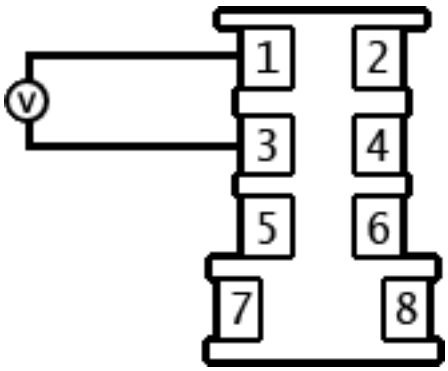
Internet ne fonctionnant pas, mon collègue et moi, devons chercher la 1ère prise ADSL de la maison. Pour cela, nous demandons au client ou sinon nous suivons le câble. Ici, le client nous avait indiqué son emplacement.

Après y avoir accédé, nous l'ouvrons et nous y connectons deux sondes à un multimètre afin de vérifier s'il y a un courant qui traverse la prise ADSL. Il suffisait de placer les sondes sur les vis.

Le courant doit avoisiner les 50V en continu. Celui-ci était de 48.7V alors il n'y avait aucun problème à ce niveau-là.



Prise ADSL + Schéma simplifié de l'intérieur



Multimètre + Branchement à la prise ADSL

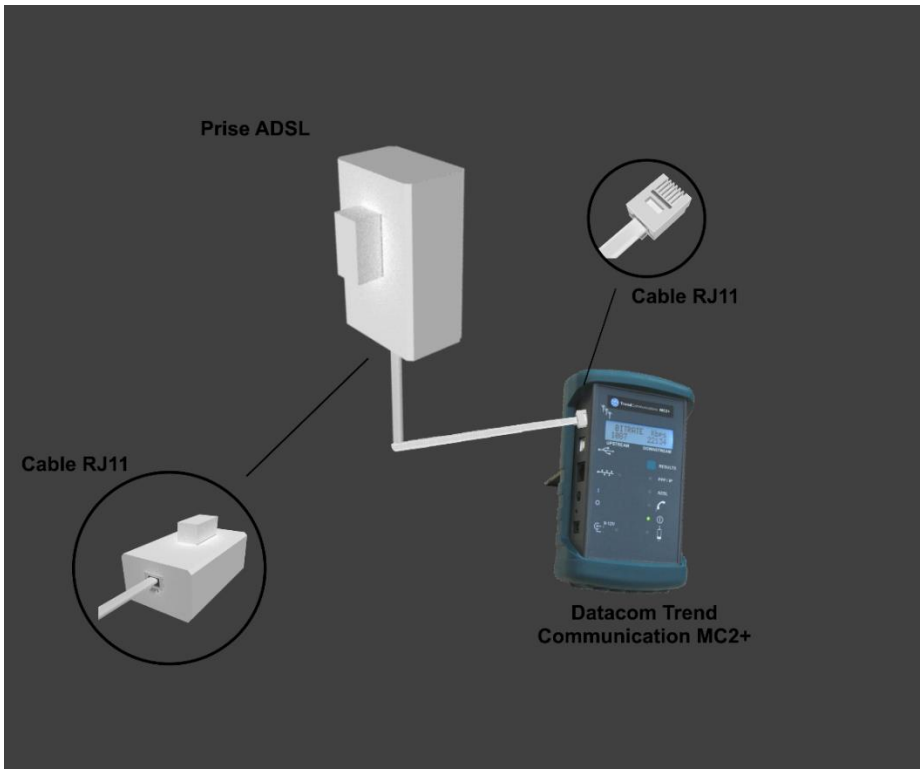
3ème étape :

Ensuite, nous utilisons un appareil conçu pour la vérification des lignes ADSL. Cet appareil est un « Datacom Trend Communications MC2+ ».

Photo d'un Datacom. Il permet de tester les lignes ADSL.

Il affiche actuellement la mesure du débit en Kbps.

Nous le connectons à la prise ADSL via un adaptateur.



Voici un schéma que j'ai conçu afin que vous compreniez comment on a procédé. Afin de réaliser ce schéma, j'ai moi-même modélisé les éléments avec un logiciel de modélisation 3D.

Après avoir attendu environ une minute, une LED s'allume au niveau de l'indication ADSL. Celle-ci indique que nous avons un signal et que l'ADSL est fonctionnelle. Mais, nous devons tout de même noter les mesures. Nous avons constaté que le débit ascendant et le débit descendant étaient tous deux supérieurs à la moyenne.

Le débit descendant était de 16.3Mo/s et le débit ascendant était de 12.1Mo/s. Il n'y avait donc aucune erreur sur la ligne.

Nous appelons une erreur, le fait de ne pas recevoir correctement une information suite à une perte de signal.

4ème étape :

Le problème venait donc d'une source intérieure. Alors nous avons refait les mesures sur la prise où est connectée la box.

Cette prise venait d'une rallonge ADSL étant donné qu'elle était par terre et reliée à une bobine de fil qui partait vers la première prise. Le débit et le voltage étaient très faible et il y avait plus de 20 000 erreurs.

Le problème venait alors de la rallonge que le client avait installée. Les rallonges ADSL sont pratiques sauf qu'il faut s'en servir uniquement pour le téléphone car le câble n'est pas adapté pour une communication internet. Alors, celui-ci peut fonctionner pendant quelques années mais à un moment donné il faudra le remplacer.

Pour conclure, nous avons conseillé au client de faire passer un électricien afin qu'il installe un câble qui sera certes plus cher, mais celui-ci sera adapté et de meilleure qualité.

En fait **INFORMATIQUE.COM** dans ce cas-là est mandaté pour identifier le problème, trouver une solution à celui-ci mais pas pour mettre en œuvre cette solution.

Conclusion :

Pour cette intervention, le client n'avait plus accès à internet depuis une semaine. Nous avons alors suivi le protocole pas à pas. Cette intervention a duré une quinzaine de minutes.

Celle-ci m'a beaucoup plu car j'ai pu découvrir les différentes causes d'un problème internet étant donné que nous avons contrôlé la quasi-totalité du réseau.

Ici, un câble Ethernet était défectueux. Nous avons alors proposé au client de faire venir un électricien pour en installer un nouveau. Le client s'est montré compréhensif.

Conclusion de l’étude de Cas :

Pour cette intervention, le client n’avait plus accès à internet depuis une semaine. Nous avons alors suivi le protocole pas à pas. Cette intervention a duré une quinzaine de minutes.

Celle-ci m’a beaucoup plu car j’ai pu découvrir les différentes causes d’un problème internet étant donné que nous avons contrôlé la quasi-totalité du réseau.

Ici, un câble Ethernet était défectueux. Nous avons alors proposé au client de faire venir un électricien pour en installer un nouveau. Le client s’est montré compréhensif.

Planque Clément

Première SN

Lycée Cabanis

Période de stage : du 04/02/19 au 12/04/19

Entreprise : ***PC19***

La Barriere de Saint Laurent - 19240 ALLASSAC

RAPPORT PFMP2 :

Sommaire de la PFMP 2 :

Présentation de l'Entreprise :

- **En quelques lignes :**

PC19 est une entreprise de dépannages à distance et sur site, pour les professionnels, qui intervient sur les zones de Brive, Périgueux et Limoges.

Cette entreprise de trois employés habituellement est dirigée par Thomas Blanchard. Celui-ci s'occupe principalement des logiciels de paye et de la comptabilité.

Tandis que Nicolas Quintanel, le second employé est plus dirigé vers le réseau et vers la virtualisation (utiliser un serveur afin d'avoir plusieurs ordinateurs accessibles à distance, d'une puissance variable selon les besoins).

Et pour finir, Flavien Crozes travaille principalement dans le dépannage informatique en général. Il travaille le plus possible à distance et quand cela n'est pas possible, il intervient directement sur site.

- **Partenaires :**

PC19 a pour partenaires :

- HP, qui fournit tous leurs équipements réseaux, ordinateurs, platines (petits ordinateurs tournant sous linux permettant de se connecter à distance sur un « vrai » ordinateur) …
- Les logiciels SAGE, pour la comptabilité
- Les TPE et PME

Etude de Cas :

L'étude de cas de cette seconde année de mon cursus sera l'installation et la configuration d'un pare-feu pfSense.

Présentation générale d'un pare-feu :

Un pare-feu est un équipement réseau permettant de contrôler le flux internet d'un réseau. Cela est très utile en entreprise car il peut, par exemple, éviter la propagation d'un virus informatique.

Pourquoi avoir choisi un pare-feu pfSense et non un Stormshield ?

pfSense est un système d'exploitation « open source » qui possède plusieurs avantages :

- Il peut s'installer sur toutes les machines suite à son faible volume
- Il dispose d'un large choix de configuration
- Il peut être monitoré* très facilement
- Il est régulièrement mis à jour
- Il est modifiable à souhait
- Il dispose d'une interface graphique simple d'utilisation
- Il est capable de faire une liaison VPN entre deux réseaux
- Il est possible d'avoir plusieurs interfaces WAN

*** Monitorer : Permet d'obtenir facilement l'état matériel et système de la machine et de la centraliser dans un logiciel comme PRTG.**

Explication des termes utilisés dans cette étude de cas :

- **VPN (Virtual Private Network) :** Permet d'accéder aux machines d'un autre réseau via son adresse IP privée
- **LAN :** Réseau Local
- **WAN :** Réseau étendu (souvent connexion avec internet)
- **DHCP (Dynamic Host Configuration Protocol) :** Configure les paramètres IP de la machine de façon automatique
- **dynDNS :** Permet d'avoir un nom de domaine fixe

Installation de pfSense :

Le pfSense que j'ai utilisé est préinstallé sur la machine mais il faut savoir que c'est plutôt simple d'installation.

Pour installer un pfSense, tout d'abord, il faut aller sur le site web officiel et aller dans la section « téléchargement ». https://www.pfsense.org/download/
Ensuite sélectionner l'architecture de la machine, le format CD Image (ISO) et appuyer sur « télécharger ».

Une fois le fichier téléchargé (328Mo), il faut le décompresser avec un logiciel comme Winrar ou 7zip et installer l'iso sur une clé usb avec Rufus.

Une fois terminé, il suffit de démarrer l'ordinateur souhaité sur la clé usb et de toujours appuyer sur « entrer ». Il est tout de même préférable de l'installer sur un équipement qui a au moins deux interfaces réseaux.

Voici ce à quoi ressemble le nôtre :

Comme vous pouvez le voir, il possède 4 interfaces réseaux, des ports usb pour le clavier, un port console afin de le configurer via PuTTY et des antennes wifi que nous n'utiliserons pas.

Configuration de pfSense afin d'accéder à une interface graphique :

Tout d'abord, il est conseillé de mettre le clavier en azerty. Pour cela, il faut entrer en mode Shell (similaire à l'invite de commande de Windows) en appuyant sur la touche « 8 » et sur « Entrer ».

Ensuite, il faut entrer cette commande :
kbdcontrol -l /usr/share/syscons/keymaps/fr.iso.kbd
kbdcontrol -l /usr/shqre/syscons/key,qps/fr.iso.kbd (si vous avez du mal avec le qwerty)

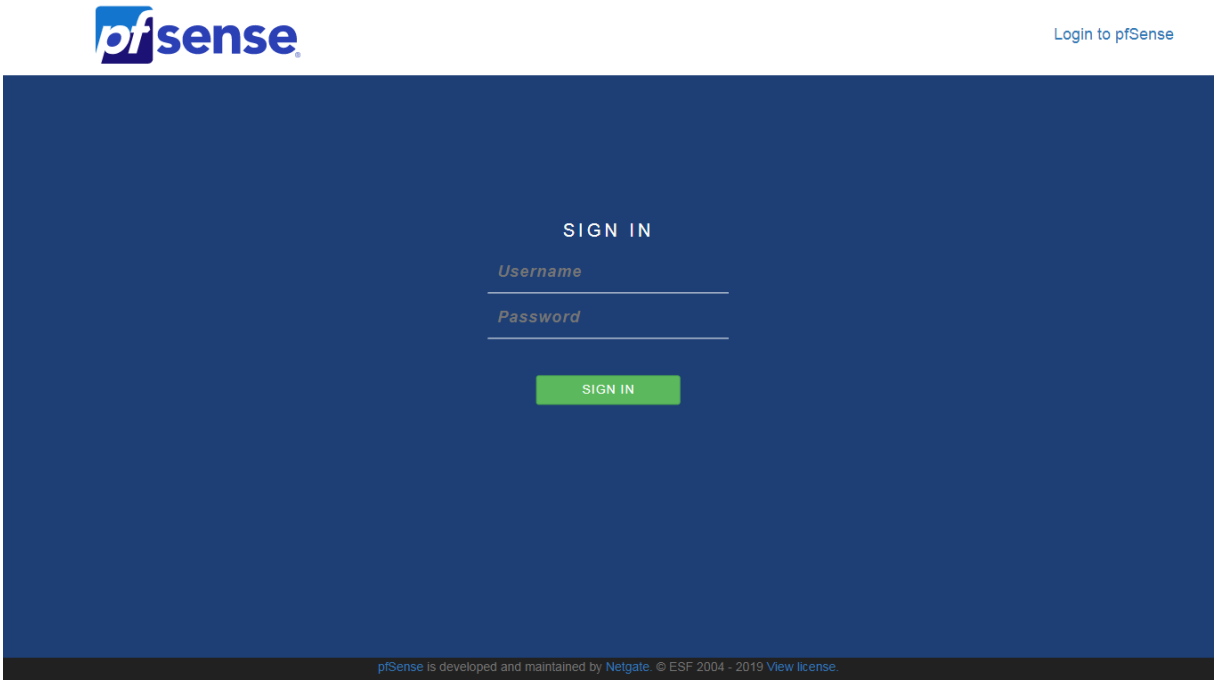
Maintenant, afin de nous faciliter la tâche, nous allons activer l'accès à l'interface web depuis l'interface WAN en entrant cette commande :
pfSsh.php playback enableallowallwan

Le pfSense est presque configuré, il suffit de sortir de ce mode en tapant « exit » et nous allons garder la configuration des interfaces par défaut.

Configuration de pfSense depuis l'interface graphique :

Pour commencer, il faut brancher le pare-feu dans votre réseau via une prise murale ou un switch sur la 1ère interface qui est le WAN.
Cela aura pour effet de récupérer l'adresse IP via DHCP.

Il ne reste plus qu'à se connecter au pfSense avec un navigateur internet avec l'IP écrite en haut.



Cela vous donnera une page de connexion pour accéder à la suite, il faut entrer les identifiants suivants :

Username : admin
Password : pfsense

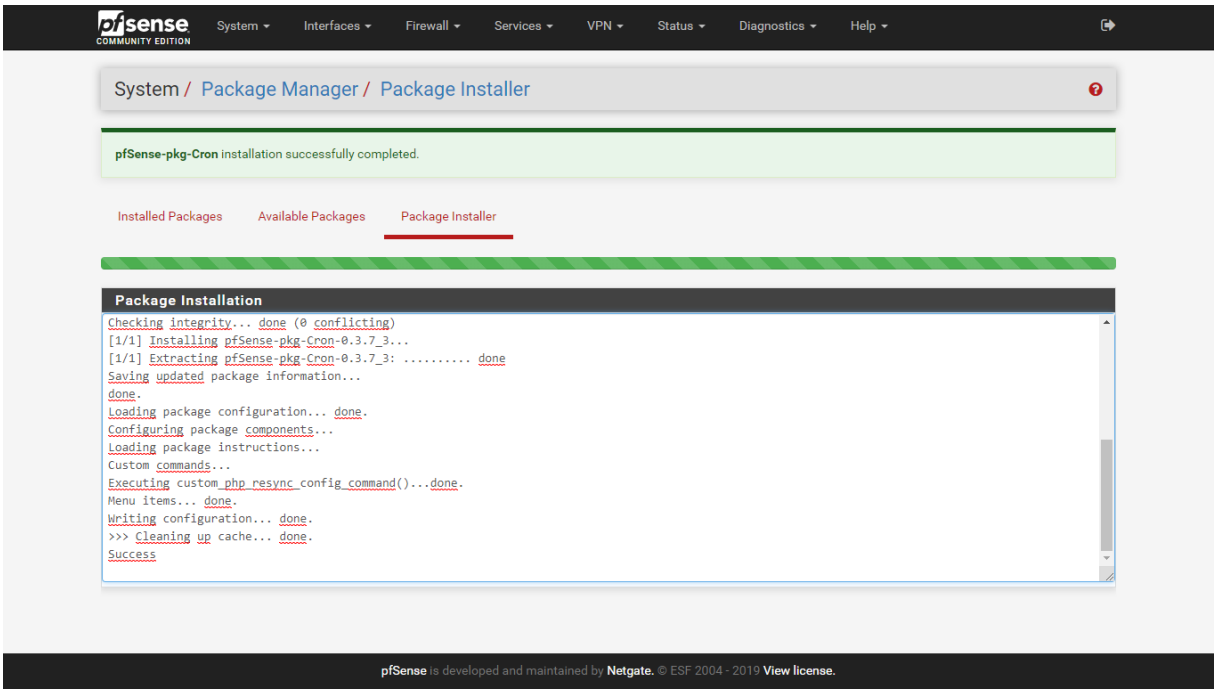
La page de première configuration s'affiche, on règle ici le fuseau horaire, le nouveau mot de passe et on laisse le reste tel quel.

Pour cette activité, on m'a demandé de configurer :

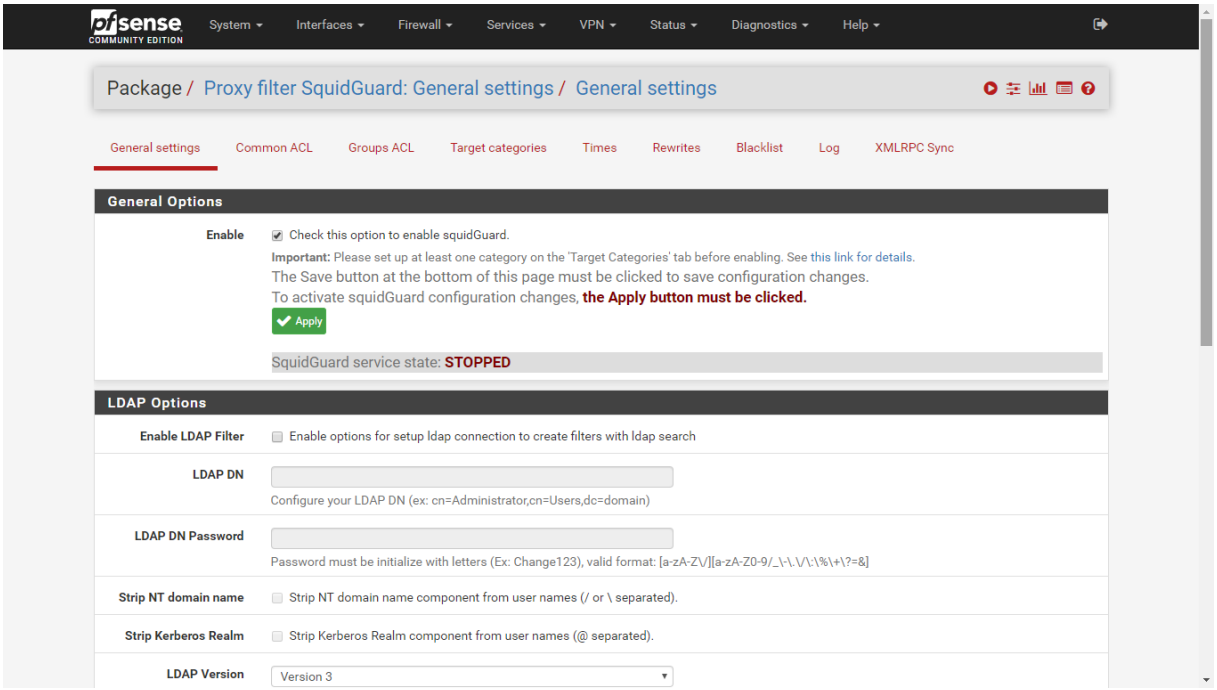
- Un filtrage URL
- Se connecter avec deux interfaces WAN en même temps
- Mettre en place un VPN afin d'être connecté sur un réseau distant
- Faire en sorte que le VPN fonctionne même en cas de redémarrage du routeur 4G (ce qui engendre un changement d'adresse IP publique)

Pour commencer, nous allons installer les modules complémentaires que vous avons besoin. Afin de faire cela, il faut aller dans la section « System » et ensuite dans « Package Manager » et d'installer les modules suivants :

- Cron (Tâches planifiées)
- Squid (Serveur Proxy)
- SquidGuard (Filtrage)



Une fois réalisé, nous avons tout ce dont nous avons besoin. Maintenant, nous allons configurer le filtrage URL. Pour cela, il faut aller dans la section « Services » et dans « SquidGuard Proxy Filtrer » et vous tomberez sur cette page :

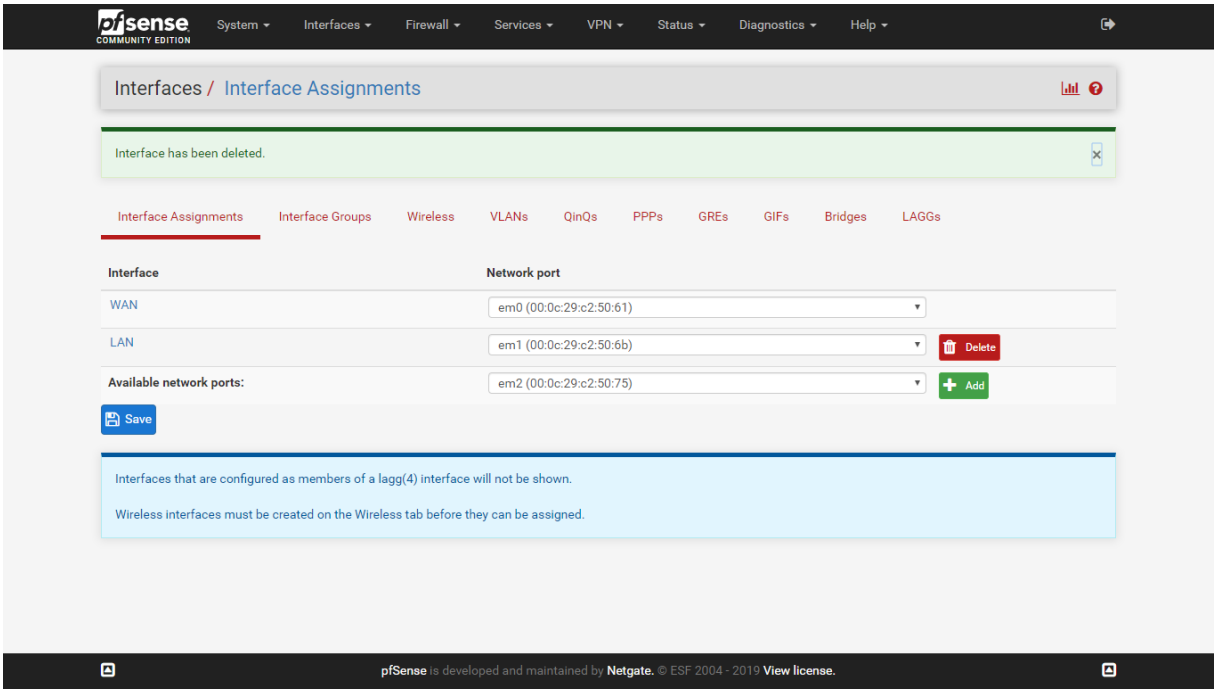


Il faudra cocher la case « Check this option to enable squidGuard » et cliquer sur « Apply ».

Ensuite, il faut aller dans « Blacklist » et écrire l'URL ci-dessous et appuyer sur « Download ».
http://dsi.ut-capitole.fr/blacklists/download/blacklists_for_pfsense.tar.gz

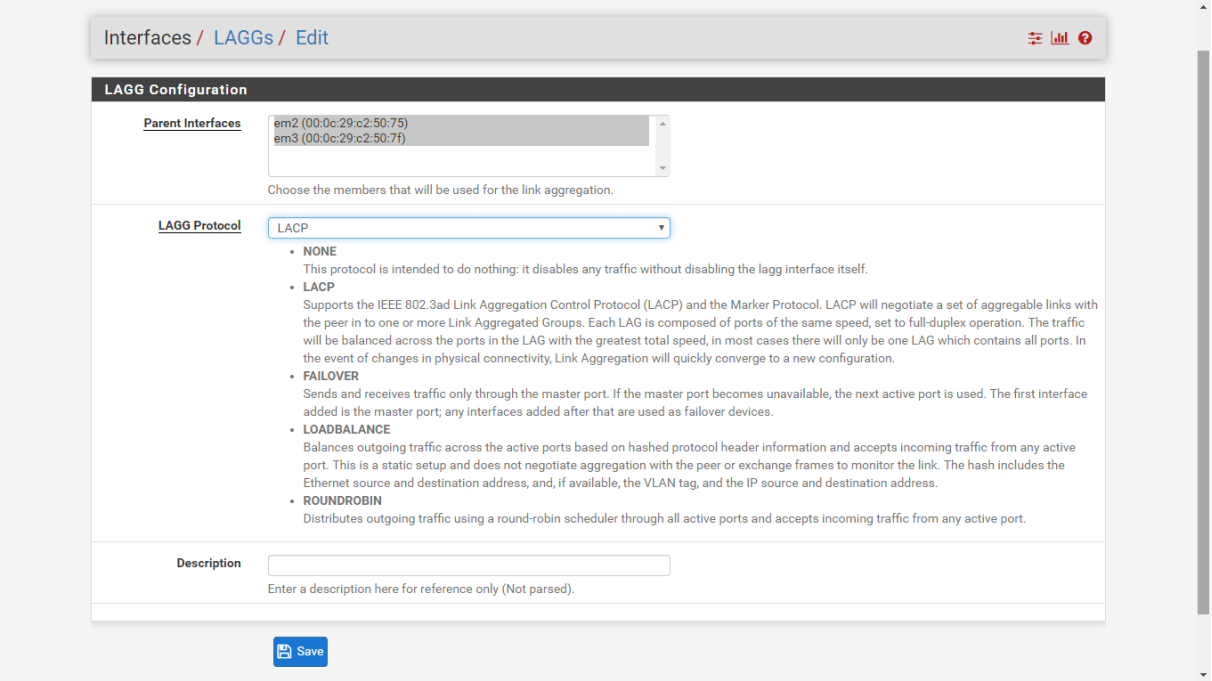
Une fois la synchronisation terminée, il suffit d'aller dans « Common ACL », cliquer sur le « + » et choisir les catégories que l'on ne souhaite pas voir dans notre réseau. Par exemple, les jeux vidéo, les réseaux sociaux…

Désormais, nous allons passer à la création de deux interfaces WAN qui fonctionneront ensemble. Pour cela, il faut aller dans la section « Interfaces » et dans « Assignments » puis, supprimer l'affectation des deux interfaces voulues. Attention, si vous êtes connecté à l'interface web via cette interface, cela aura pour effet de vous déconnecter.



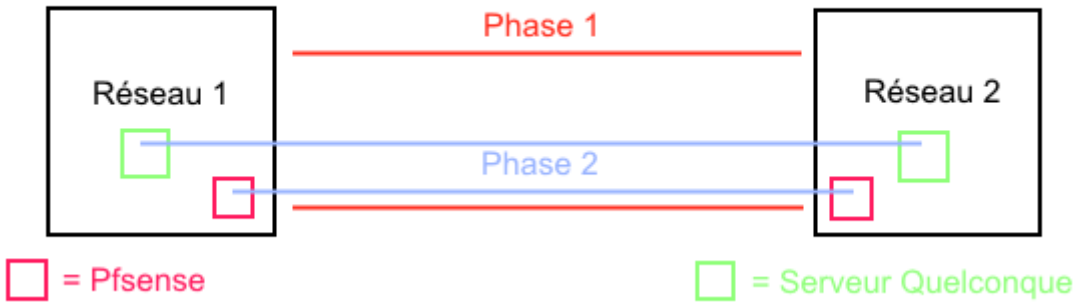
Ensuite, il faut aller dans « LAGGs » et ajouter une interface qui englobe les deux interfaces souhaitées avec le protocole LACP. Voilà, vos interfaces ne font maintenant qu'une. Cela est très pratique lorsque vous avez une ligne ADSL et une ligne 4G car cela double votre débit actuel et permet d'assurer une connexion internet même en cas de coupure d'une des lignes.

Maintenant, il suffit d'aller sur la page précédente (Assignments) et remplacer l'interface WAN (ici em0) par l'interface crée (LAGG0).



Pour mettre en place un VPN, il faut aller dans la section « VPN » et dans IPsec. Mais avant de le configurer, il faut comprendre comment fonctionne un VPN.

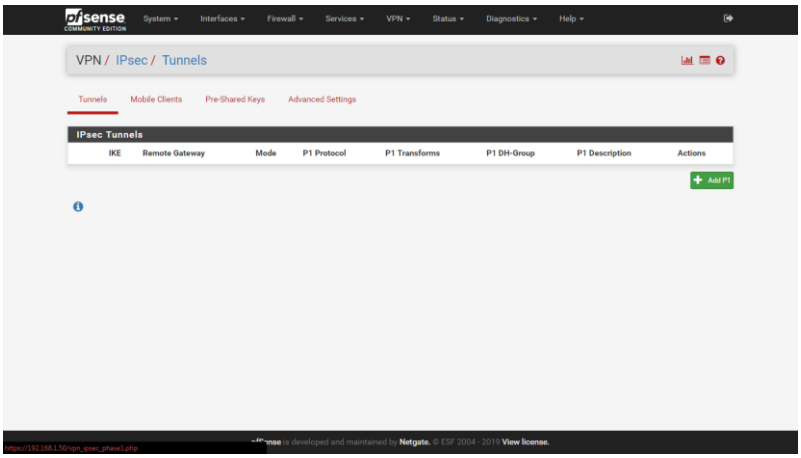
Un VPN est constitué d'une phase 1 et d'une ou plusieurs phase 2.
Une phase 1 sert à créer le lien entre les deux réseaux. Tandis qu'une phase 2 permet de relier deux appareils qui ne sont pas dans le même réseau. Voilà à quoi ça ressemble :



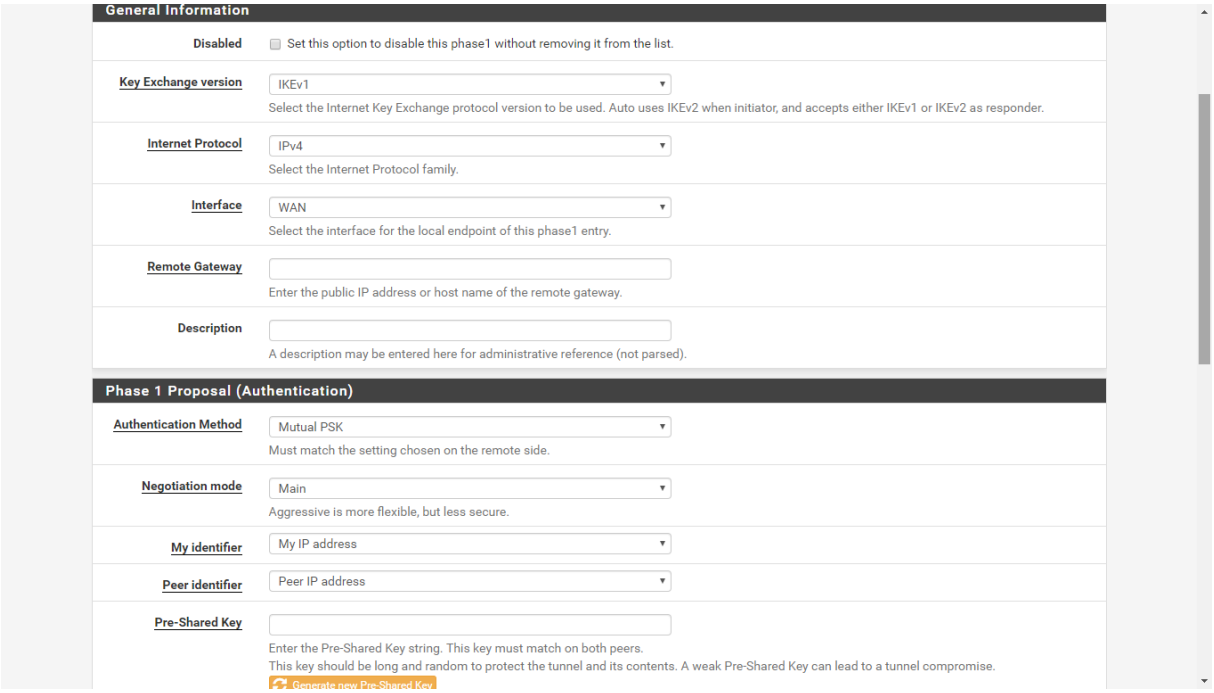
Pour schématiser un peu, la phase 1 pourrait se comparer à une gaine et la phase 2 serait le câble. Dans notre cas, la phase 1 se fait entre deux pfSense.

Pour qu'un VPN soit fonctionnel, il faut avoir exactement les mêmes réglages entre les deux appareils, que ce soit la phase 1 comme la phase 2.
Dans notre cas, le VPN sera crypté par une clé partagée et un double algorithme d'encryptions.

Dans pfSense, pour créer un VPN, c'est très simple mais il ne faut pas se perdre. Pour commencer, il faut créer une Phase 1 pour cela, il faut cliquer sur « Add P1 ».

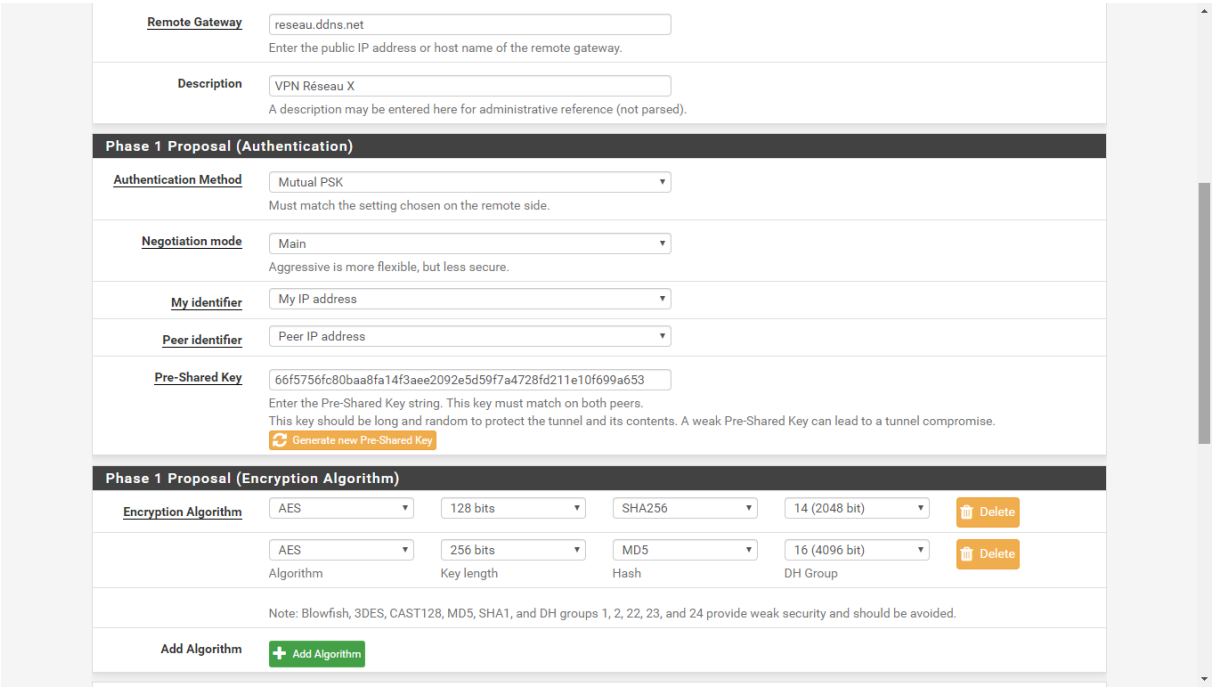


Et vous tomberez sur cette page :



Dans la case « Remote Gateway », il faudra indiquer l'adresse IP publique ou le dynDNS du réseau distant et dans « Pre-Shared Key », il faut mettre un mot de passe compliqué qui sera identique aux deux configurations (configuration réseau 1 et réseau 2). Ce mot de passe sera la clé partagée qui permettra le chiffrement des données.

Maintenant, il faut déterminer quel cryptage sera utilisé pour les communications. Il n'y a pas de meilleure façon de crypter, dans notre exemple, j'ai décidé de mettre deux cryptages différents (un en MD5, 256 bits et un en SHA256, 128 bits).
Voici à quoi ça ressemble.

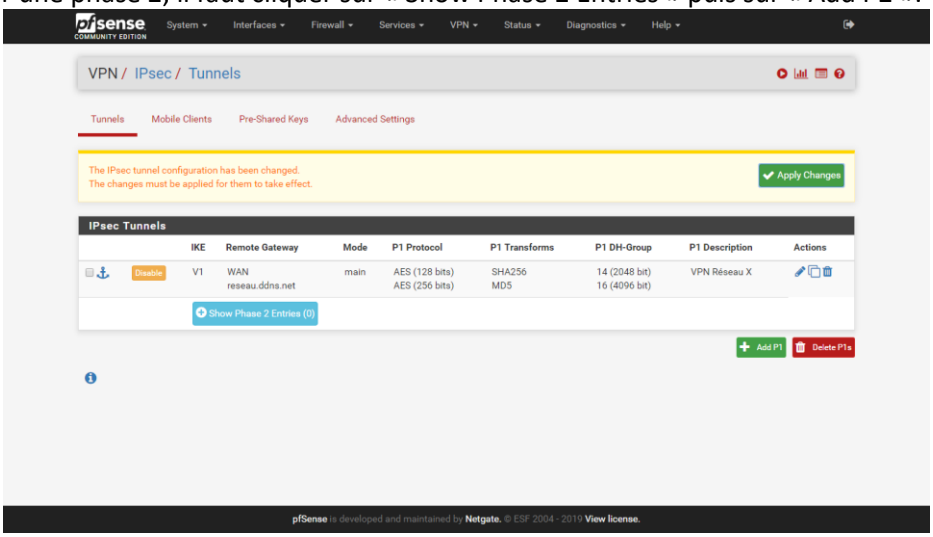


Maintenant, nous allons créer une phase 2 entre :

- Un serveur du réseau 1 : 192.168.10.49
- Un serveur du réseau 2 : 192.168.20.146

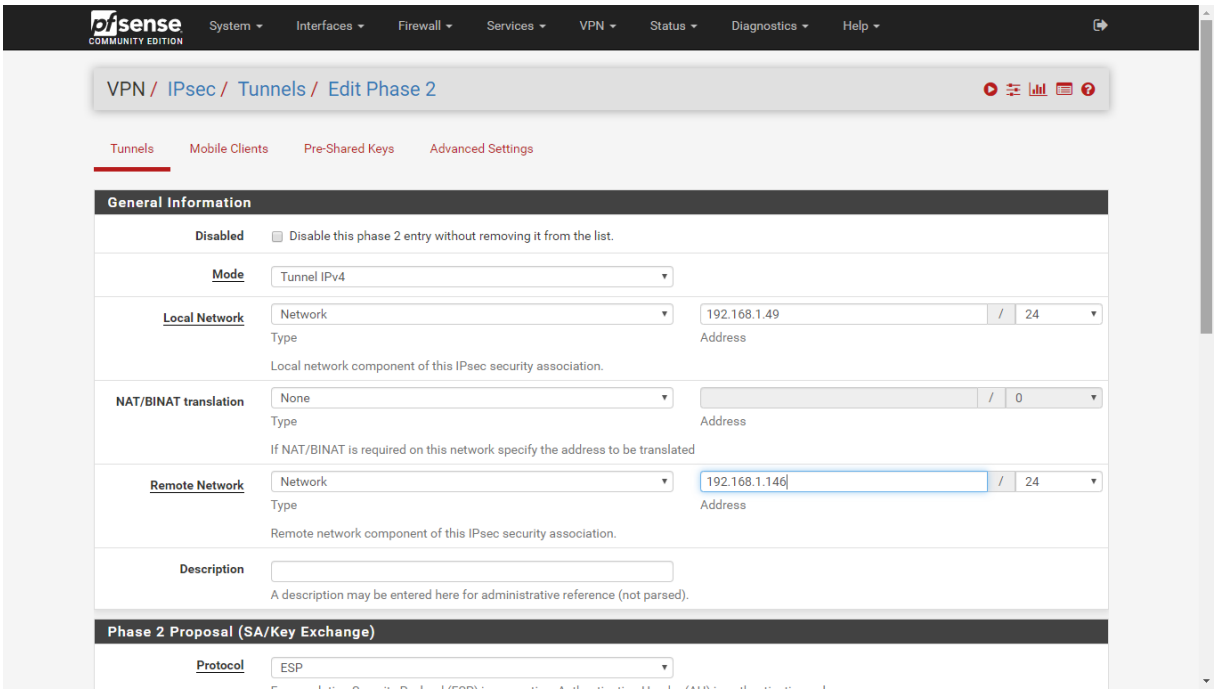
Tous les réglages seront effectués sur le réseau 1, il faudra faire de même sur le réseau 2 mais il faudra faire attention à inverser les IPs.

Pour ajouter une phase 2, il faut cliquer sur « Show Phase 2 Entries » puis sur « Add P2 ».



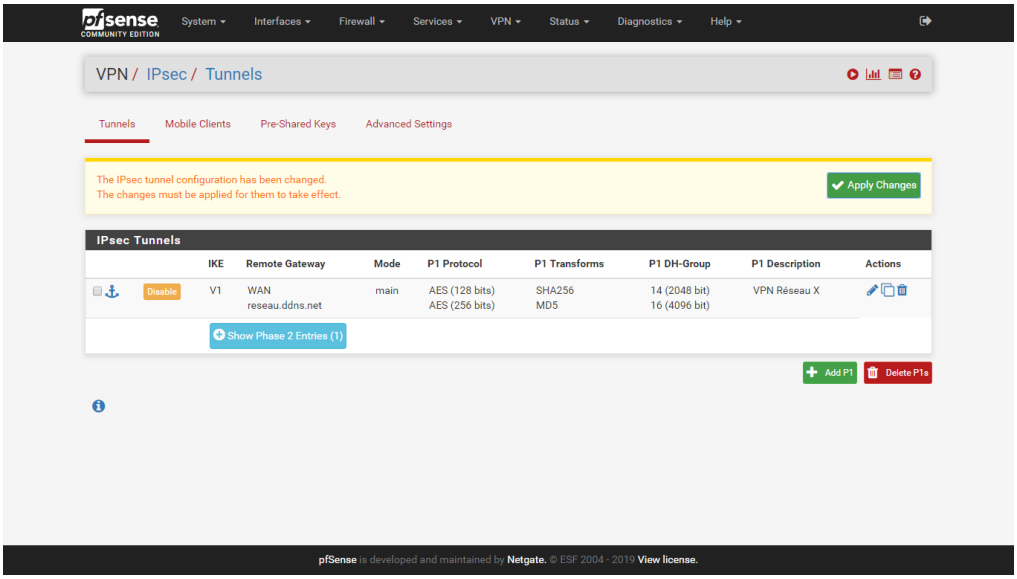
Il faudra renseigner l'adresse IP du serveur local (réseau 1) dans la section « Local Network ». Pour cela, vous devez cliquer sur le menu déroulant et mettre « Network » puis mettre l'IP du serveur à droite et son masque de sous réseau en bit.

Il faudra faire de même dans la section « Remote Network » mais cette fois-ci, il faudra mettre l'IP du serveur distant (réseau 2).
Une fois fait, cela devrait ressembler à ça :

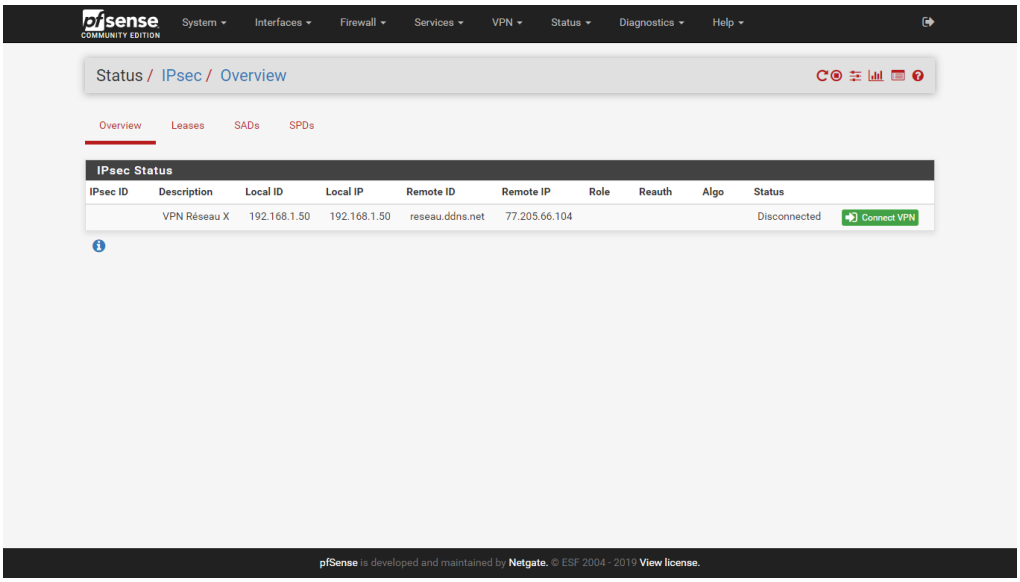


A ce stade-là, il manque plus que la méthode de cryptage, c'est le même principe qu'au-dessus. Je conseille quand même de laisser les réglages par défaut.

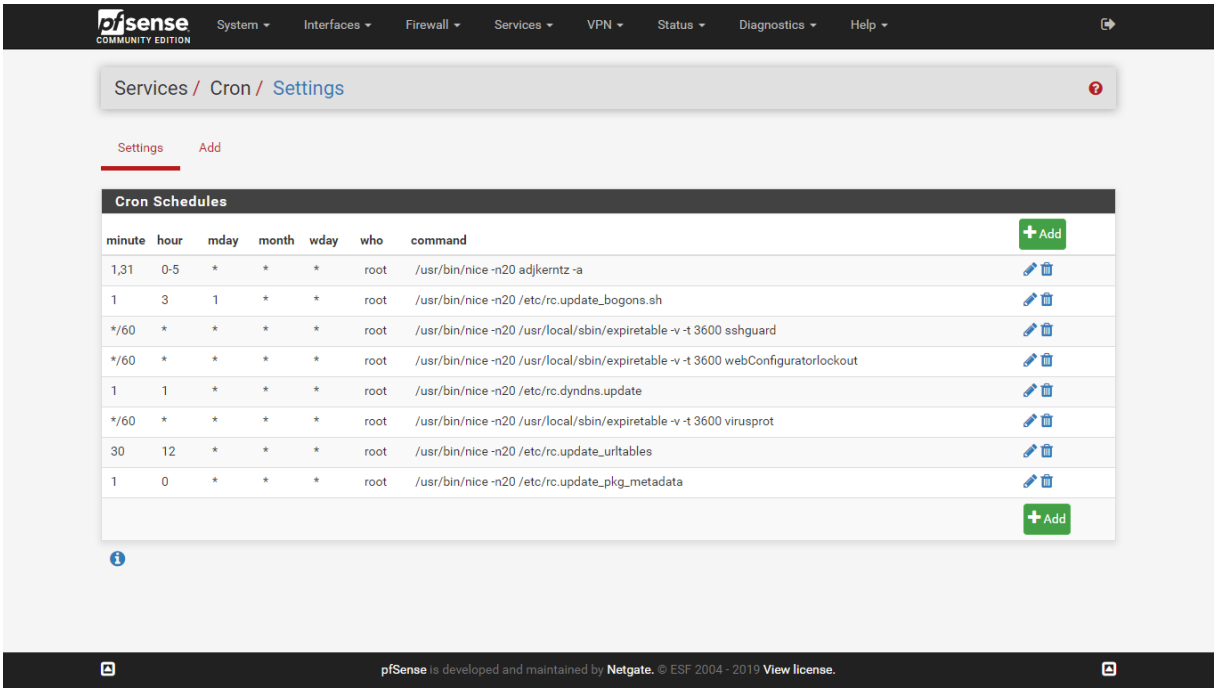
Une fois les configurations terminées et avoir appuyé sur « Save » il faudra appuyer sur le bouton vert « Apply Changes » afin de sauvegarder les changements.



Il ne reste qu'une seule étape afin que votre VPN soit actif. Pour cela, il faut aller dans la section « Status » puis dans « IPsec » et de cliquer sur « Connect VPN ».



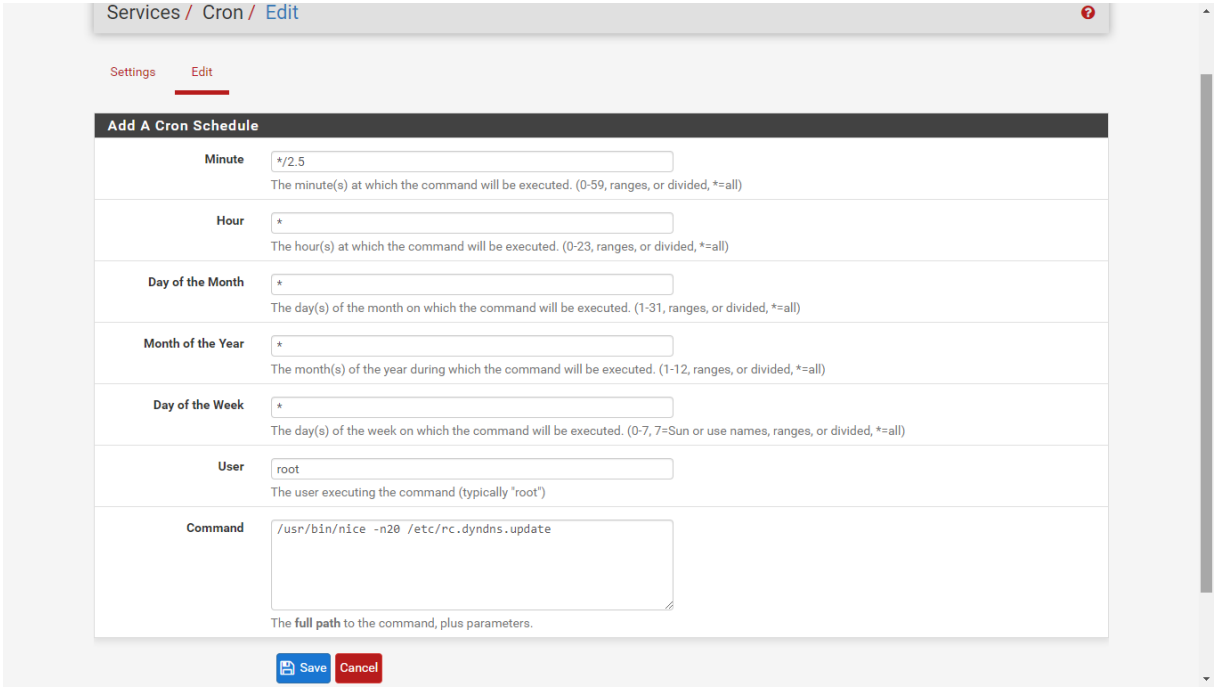
Pour finir il faut configurer la reconnexion automatique du VPN. Pour cela, il faut aller dans la section « Services » puis dans « Cron ». Cela vous mènera à cette page :



Et il faudra modifier la ligne : /usr/bin/nice-n20/etc/rc.dyndns.update
Et mettre dans la case « Minute » la valeur « */2.5 » qui pourrait se traduire par « Toutes les 2.5 minutes ». Pour les heures, mettez la valeur « * » ceci fera une mise à jour toutes les heures. Le reste, laissez-le tel quel et cliquez sur « Save ».

Les réglages sont finis, j'ai décidé de mettre la recherche toutes les 2.5 minutes car après quelques tests, cela s'avère être le plus optimisé.

Une fois les réglages effectués, la page devrait ressembler à cela :


Services / Cron / Edit
Settings
Edit
Add A Cron Schedule
Minute
*/2.5
The minute(s) at which the command will be executed. (0-59, ranges, or divided, *=all)
Hour
*
The hour(s) at which the command will be executed. (0-23, ranges, or divided, *=all)
Day of the Month
*
The day(s) of the month on which the command will be executed. (1-31, ranges, or divided, *=all)
Month of the Year
*
The month(s) of the year during which the command will be executed. (1-12, ranges, or divided, *=all)
Day of the Week
*
The day(s) of the week on which the command will be executed. (0-7, 7=Sun or use names, ranges, or divided, *=all)
User
root
The user executing the command (typically "root")
Command
/usr/bin/nice -n20 /etc/rc.dyndns.update
The full path to the command, plus parameters.
Save
Cancel

Conclusion de l'étude de Cas :

Durant cette activité, j'ai appris à me servir d'un pfSense et le fonctionnement d'un VPN en IPsec. J'ai réalisé cette activité en deux jours en me renseignant sur l'intégralité de celle-ci.

Mon maitre de stage m'avait confié cette activité dans le but d'élargir les possibilités du pfSense (dans ce qu'il m'avait demandé, il ne savait faire que la configuration d'un VPN).

J'ai trouvé cette activité très intéressante car j'ai pu travailler en autonomie complète durant ces deux jours et ça m'a permis de connaitre ce modèle de pare-feu alors que je ne connaissais que Stormshield et Cisco.

J'ai aussi pu me renseigner sur le système d'exploitation de pfSense (FreeBSD) qui est une sorte de Linux où toutes les commandes les plus importantes changent voire sont supprimées.

Planque Clément

Terminale SN

Lycée Cabanis

Période de stage : du 12/11/19 au 17/01/20

Entreprise : ***ACS'IT***

9 Avenue de la Libération, 19360 Malemort-sur-Corrèze

Sommaire de la PFMP 3 :

Présentation de l'Entreprise :

- **En quelques lignes :**

ACS'IT est intégrateur de solutions voix - données - images, pour les professionnels.

Cette société de 20 employés est dirigée par M. Claude GENIER. Son siège social est à Limoges, et une seconde agence est basée à Malemort. Portée sur les domaines de la téléphonie, les réseaux, la sécurité et la mobilité, cette société intervient sur la France entière.

- **Partenaires :**

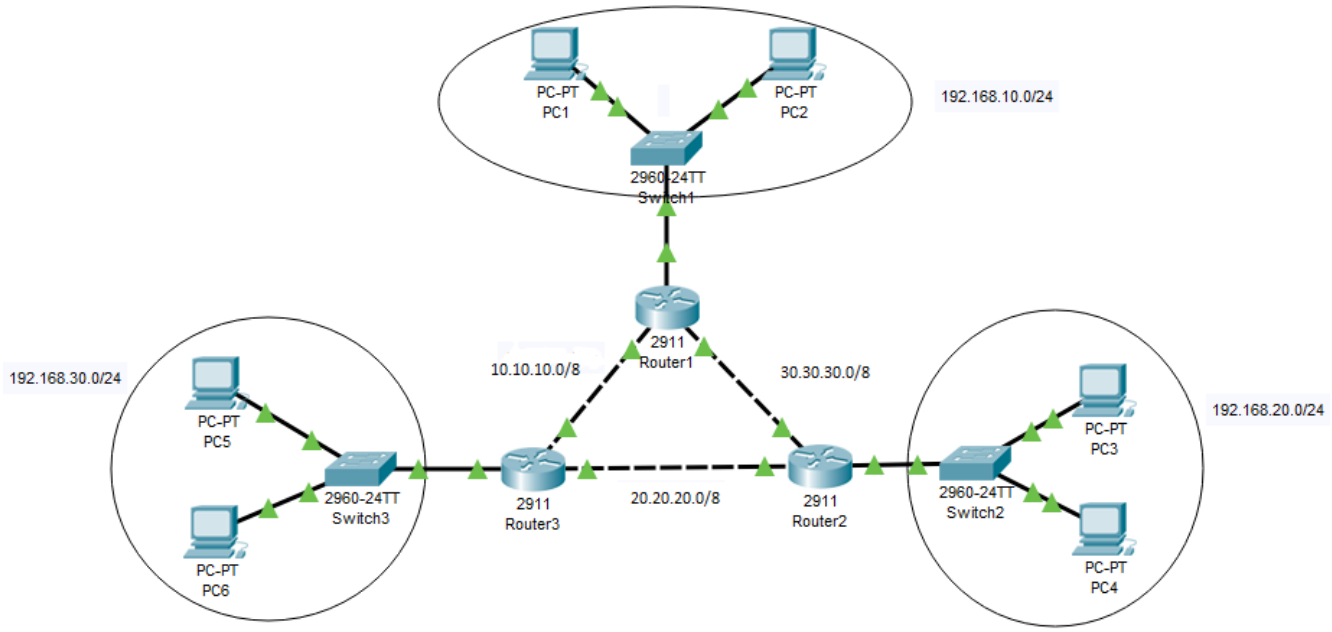
ACS'IT a pour partenaires :

ALIPTIC Association Limousine des Professionnels des Technologies de l'Information et de la Communication	Association Limousine des Professionnels des Technologies de l'Information et de la Communication
RÉSEAU EURABIS INFORMATIQUE & SERVICES	Groupement de revendeurs en informatique
cpme CONFÉDÉRATION DES PME	Confédération des Petites et Moyennes Entreprises, est une organisation patronale interprofessionnelle, privée et indépendante
FEDERATION EBEN ENTREPRISES DU BUREAU ET DU NUMÉRIQUE	La Fédération EBEN rassemble les entreprises de distribution de produits et services pour l'environnement de travail
BNI®	BNI est un réseau d'affaires professionnel basé sur la recommandation mutuelle

Etude de Cas :

L'étude de cas de ma terminale de lycée se portera sur la réalisation d'un réseau étendu avec routage OSPF avec des VLANS.

Définition :
Routage OSPF : Routage dynamique, souvent utilisé pour les grands réseaux. Celui-ci requiert un réseau différent afin d'établir le lien entre les différents routeurs. Les routeurs sont reliés par un câble RJ45 et on peut utiliser des interfaces FastEthernet ou GigabyteEthernet. Si un équipement vient à tomber, la route entre eux se désactive. Si la connexion entre les deux routeurs revient, alors la route se réactive automatiquement.



Voici une maquette du réseau. Dans chaque réseau, il y a les VLANs suivants :

- 10 : TEL
- 20 : DATA
- 30 : CAM
- 50 : ADMIN

Les VLANs ne peuvent communiquer entre eux, excepté le VLAN ADMIN qui lui, peut communiquer entre tout le monde.

Lors de la configuration du routage, les routeurs ont besoin d'un identifiant « router-id » afin de pouvoir se reconnaître entre eux. Celui-ci est unique à chaque routeur. Généralement, on attribue les identifiants suivants : 1.1.1.1 ; 2.2.2.2 ; 3.3.3.3 … Il faut aussi que les routeurs aient une IP dans le même réseau.

Pour conclure, le routage OSPF est rapide à mettre en place et très efficace. Cela peut s'avérer assez utile pour les réseaux d'entreprise.

Conclusion générale :

Mes années de lycée en systèmes numériques m'ont permis de découvrir ce que je voulais faire vraiment, à savoir le réseau. J'ai pu découvrir l'électronique, qui m'intéresse peu, le réseau ainsi que l'informatique en général qui sera pour moi un plan de secours si je n'arrive pas à suivre dans les études supérieures ou si le réseau ne m'intéresse plus.

Ces trois Périodes de Formation en Milieu Professionnel m'ont beaucoup appris, que ce soit en technique ou en méthodologie. J'ai aussi pu découvrir différents types d'entreprises, avec une gestion différente des affaires et des tickets ainsi qu'une manière différente de travailler.

Cette formation sera porteuse de mon suivi de cursus, j'envisage d'aller en école d'ingénieur et de faire le maximum de certifications Cisco possibles afin de partir au Japon, pays où les diplômes européens ne sont pas tenus en compte, mais les certifications sont reconnues internationalement.

Je tiens à remercier une seconde fois l'équipe pédagogique professionnelle et l'équipe pédagogique des matières générales du lycée ainsi que mes tuteurs ainsi que les employés des entreprises qui m'ont accueilli.