Institut Universitaire de Technologie,
Aix-Marseille Université

RAPPORT DE STAGE de fin de deuxième année

Bachelor Universitaire de Technologie

Spécialité Réseaux et Télécommunications

parcours cybersécurité

Création d'un nouveau réseau WIFILAIRE et Scripting Python

Hatim SBAI

Institut de Neurosciences de la Timone

Responsable entreprise : Arnaud CRUZEL

Responsable académique : Éric SOCCORCI

2023

Sommaire :

1 Introduction :

Durant ce stage j'ai eu 2 missions principales, l'étude et le déploiement d'un réseau nommé WIFILAIRE et l'amélioration d'un script Python de gestion des utilisateurs. En parallèle, j'ai également été impliqué dans la résolution de tickets informatiques. J'ai effectué ce stage au sein du laboratoire de neurosciences de la Timone, plus précisément au sein de l'équipe informatique du NIT.

Ce stage dans le laboratoire de neurosciences de la Timone a été une expérience essentielle dans mon parcours de formation, me permettant d'appliquer mes connaissances théoriques à des problématiques réelles et de développer des compétences techniques et professionnelles.

Dans les lignes qui suivent, je vais en premier lieu présenter l'institut de neurosciences de la Timone tout en mettant l'accent sur le service proposé par le NIT. Je présenterai les différentes missions que j'ai réalisées au cours de mon stage, en mettant l'accent sur l'étude et le déploiement du réseau WIFILAIRE, ainsi que sur l'amélioration du script Python.

2 Présentation de l'entreprise et environnement

2.1 L'INT

L'Institut de Neurosciences de la Timone (INT) est une unité mixte de recherche affiliée au CNRS et à Aix-Marseille Université. Il est situé sur le Campus Timone de la Faculté de Médecine, au cœur de Marseille (figure 1).

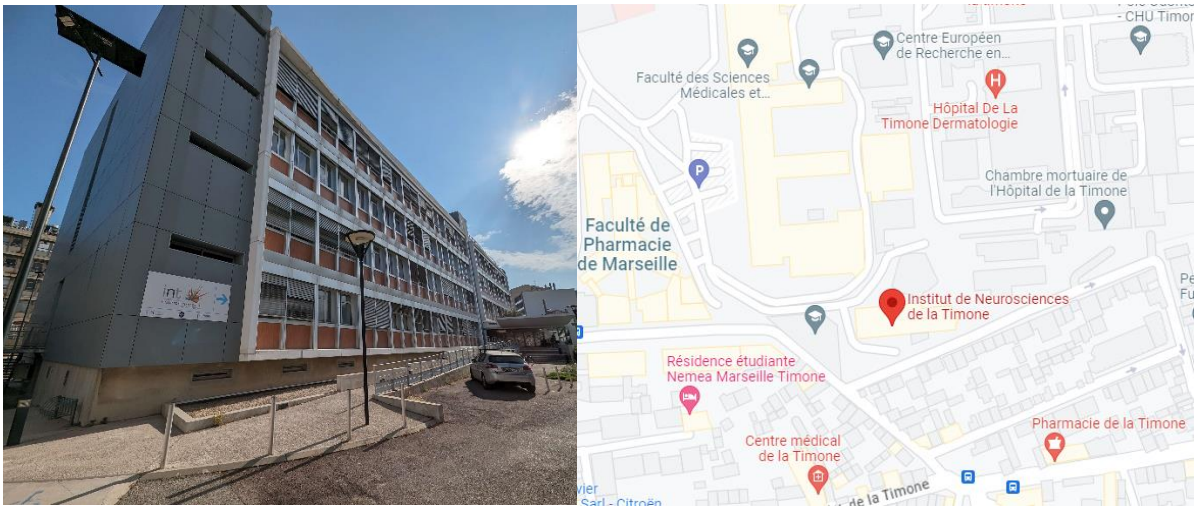

Figure 1. Bâtiment de l'INT et emplacement géographique.

L'INT a été créé en mettant en place deux principes fondamentaux : les équipes de recherche et les services communs ou plateformes. Les équipes de recherche, au nombre de 14 en 2022, regroupent des chercheurs, des enseignants-chercheurs, des étudiants, des postdoctorants, ainsi que parfois des ingénieurs et des techniciens. Ces équipes constituent le socle de l'INT, favorisant les interactions scientifiques quotidiennes et la collaboration interdisciplinaire. Elles sont évaluées et renouvelées tous les 5 ans, tout en ayant la possibilité de créer ou de fermer des équipes en fonction des besoins. La mobilité entre les équipes est également encouragée.

Figure 2. Institut de Neurosciences de la Timone.

Depuis sa création en 2012, l'INT occupe un bâtiment (figure 1) entier de 4500m2 sur le Campus de la Faculté de Médecine. Ce bâtiment a été entièrement rénové pour accueillir le laboratoire.

2.2 les Plateformes de l'INT

En 2022, l'INT comporte 6 plateformes technologiques. L'une d'entre elles est une structure dédiée à la recherche sur l'animal et fonctionne comme une Unité de service indépendante, le Centre de Primatologie de la Méditerranée (MPRC, UAR2018, CNRS Aix-Marseille Université).

Neuro-Bio-Tools (NBT) est une plateforme AMU soutenant la recherche en neurobiologie. Elle est formée de 4 services déployant des outils de biologie moléculaire et cellulaire et d'histologie. Elle est accessible par https://iris.science-it.ch/Landing/Provider/1329.

Human Investigation Platform (HIP) est une structure dédiée au soutien à la recherche clinique et fondamentale, conduite chez des volontaire sains et chez des patients. Les missions de HIP sont triples :

–> Animer la recherche clinique et fondamentale chez l'Homme

–> Accompagner le montage et le suivi des projets

–> Mettre en place des outils communs pour la recherche clinique

Plateforme de Neuroimagerie Photonique in vivo et in vitro (INPHIM) organise les moyens technologiques d'imagerie photonique in vivo et in vitro. Le parc instrumental compte actuellement sept microscopes optiques, deux systèmes d'imagerie à grand champ (macroscopes), un poste pour la visualisation et l'analyse d'image avec le logiciel Arivis Vision4D.

Centre d'Imagerie par Résonance Magnétique (IRM-INT) est une plateforme de recherche gérée par l'Institut de Neurosciences de la Timone (UMR 7289). Son rôle est de soutenir la communauté scientifique, médicale, locale, nationale et internationale, publique et privée, dans la réalisation de recherches en neurosciences fondamentales, cliniques et en psychologie cognitive.

Service de Prototypage et d'Instrumentation Mécanique et Electronique (S-PrIME) conçoit et construit des prototypes mécaniques ou électroniques pour les différents systèmes expérimentaux utilisés en imagerie, neurobiologie, neurophysiologie ou encore en psychologie expérimentale.

Neuroinformatics and Information Technology (NIT) est composé d'une cellule « Données et Calcul Scientifique » et d'une cellule « Infrastructure Système, Réseau, et Calcul Haute Performance ». Comme les autres plateformes de l'INT, la direction du NIT est double, avec un responsable scientifique (O Coulon, DR) et un responsable technique (S Takerkart, IR).

2.3 Organigramme de l'INT

Ci-dessous (figure 3) l'organigramme qui détaille la structure organisationnelle et hiérarchique au sein de l'INT :

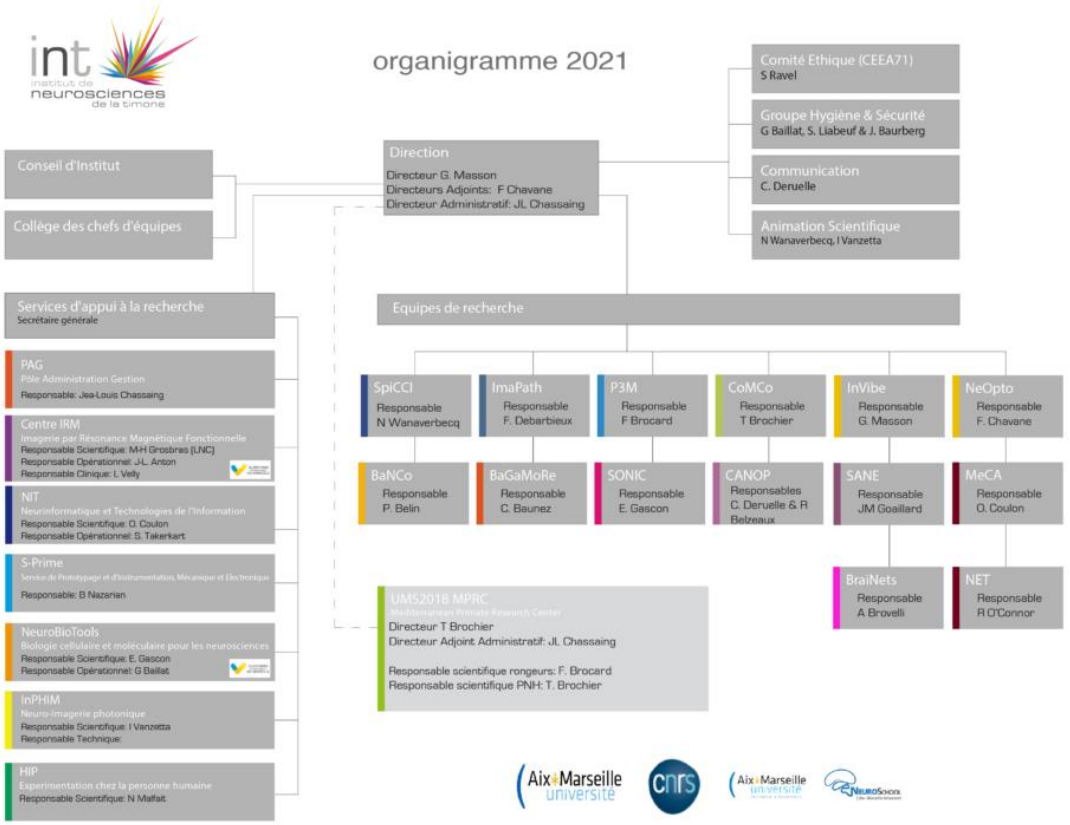

Figure 3. Organigramme de l'INT.

2.4 Le NIT :

L'INT accueille 14 équipes de recherche avec 6 services communs, comprenant le service informatique NIT (Neuroinformatics and Information Technology).

Le NIT, est la plateforme dédiée à tout ce qui concerne l'informatique. Il propose et met en œuvre la stratégie de l'Institut en matière de télécommunication, de système d'information, de sécurité informatique, de développement et gestion du parc informatique et d'électronique. Il a pour mission aussi d'assurer l'administration et l'exploitation de l'ensemble des moyens informatiques du laboratoire, d'administrer les moyens et les procédures pour garantir les performances, la disponibilité du système d'information et la sécurité de l'infrastructure. Il vise aussi à apporter des outils informatiques innovants et performants pour tous les utilisateurs.

L'équipe de travail est composée de 9 personnes qui assurent le bon fonctionnement du NIT, elle a à sa tête M. COULON Olivier (DR CNRS), responsable scientifique et M. TAKERKART Sylvain (IRHC CNRS) responsable opérationnel, ils dirigent une équipe dont les membres sont M. CRUZEL Arnaud (IE CNRS) mon tuteur en entreprise « qui s'occupe de tout ce qui est administration système et réseau, ensuite M. BACHAR Dipankar (IRCN CNRS), M. MEUNIER David (IRCN CRNS), Mme SPRENGER Julia (IR CDD)…

2.4.1 Organigramme de l'équipe NIT

Ci-dessous (figure 4) représente l'organigramme, qui détaille la structure organisationnelle de l'équipe NIT :

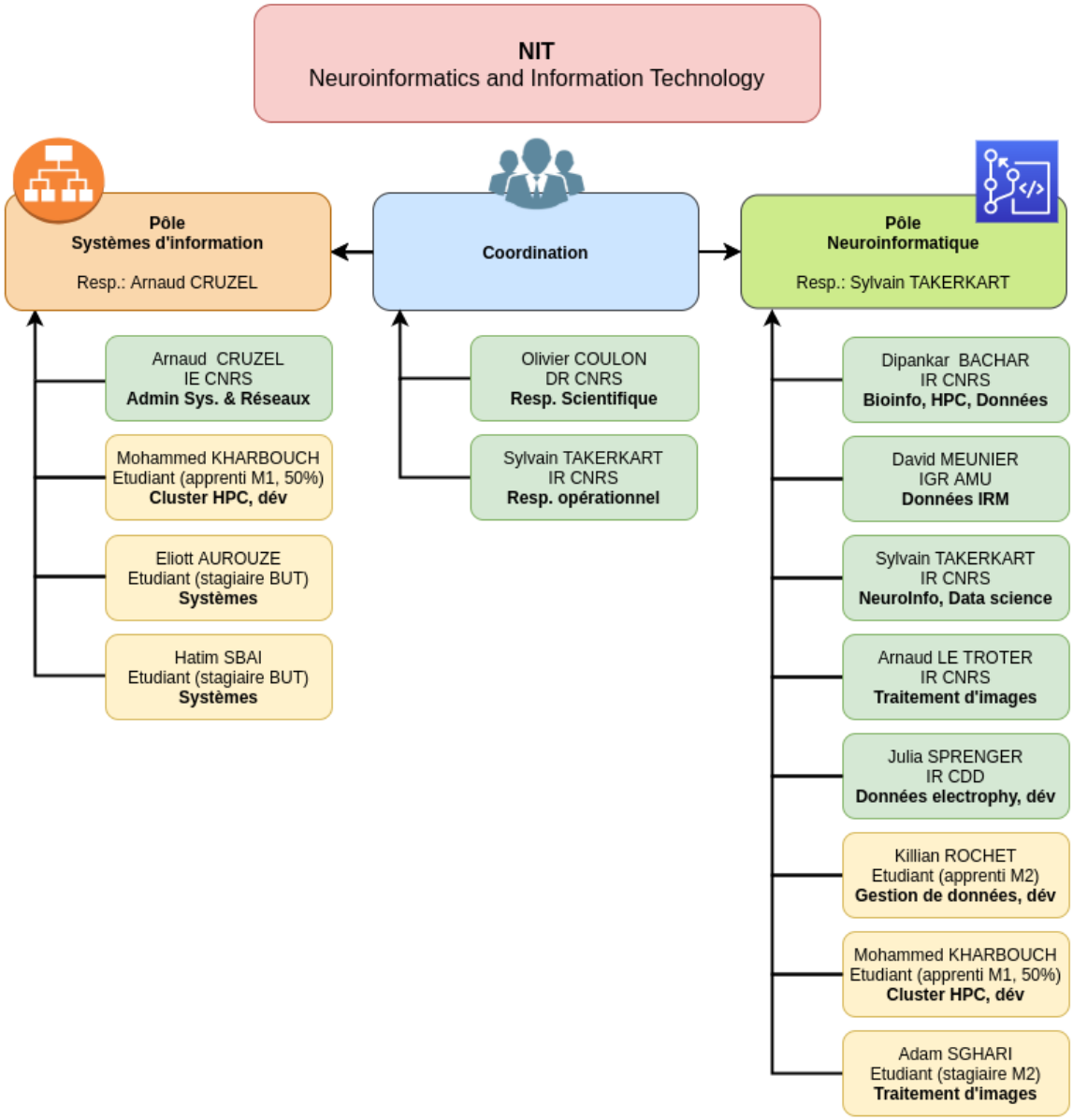

Figure 4. Organigramme du NIT.

L'équipe à laquelle je suis intégré est dédiée à l'administration systèmes et réseaux informatique. Mon travail est donc dirigé par M. CRUZEL Arnaud.

3 Présentation du sujet de stage :

3.1 Contexte :

L'INT est composé de plusieurs équipes de recherche qui utilise chacun du matériel/logiciel différent. Dans le cadre de leurs expérimentations ils sont amenés à utiliser des PC qui peuvent posséder différentes caractéristiques telles que, des versions de système d'exploitation spécifiques ainsi que certains droits administrateur en fonctions du matériel piloter comme des microscopes, laser … Néanmoins cela ne s'accorde pas avec la politique de sécurité que propose le NIT, car des PC ayant les droits administrateur ou avec des versions de système d'exploitation obsolète sont de potentielles failles dans le réseau.

3.2 Objectif du stage :

Durant mes dix semaines au sein du NIT j'ai donc travaillé sur une solution pour proposer à tous les utilisateurs ayant un compte avec des droits administrateur un accès à Internet tout en les isolant du reste de l'infrastructure. Ma mission était donc de développer un nouveau réseau nommé WIFILAIRE qui permettrait cela sans pour autant ouvrir de faille dans le réseau de l'INT.

En second lieu j'ai procédé à l'amélioration d'un script python servant à la gestion des utilisateurs en créant une fonction qui permettrait de modifier les informations des utilisateurs de l'Active Directory basé sur le protocole LDAP. J'ai en parallèle de mes missions principales effectué des résolutions de tickets qui consistaient par exemple à remplacer des disques de stockage HDD, installer des logiciels nécessitant les droits administrateur…

3.3 Aperçus du matériel utilisé

Un switch ou commutateur, est un dispositif de réseau qui permet de connecter plusieurs appareils ensemble, en acheminant efficacement les données vers leur destination respective. Il améliore les performances et la sécurité du réseau en isolant le trafic vers les appareils concernés.

J'ai travaillé sur des switches HP et plus précisément les modèles HP2510G, HP2910, HP5406, HP5700 (figure 5) et HP5710.

Figure 5. Switch HP5700.

La différence entre ces switches est les performances qui sont chacune dédiées à un besoin spécifique, par exemple le modèle HP2510G est taillé pour les petites entreprises ou les réseaux de bureaux de taille moyenne contrairement au HP5700 qui est conçu pour les Datacenters et qui permet de gérer de hauts débits.

Je ne présenterais pas ici les spécificités de chaque switch, car je n'ai utilisé que des fonctionnalités qu'ils ont en commun : création/ajout de VLAN, tagging de port.

Un firewall, ou pare-feu, est un dispositif de sécurité informatique conçu pour surveiller et contrôler le trafic réseau. Il agit comme une barrière entre un réseau privé et les réseaux externes, telle qu'Internet, en filtrant les données qui entrent et sortent du réseau. Son rôle est de détecter et de bloquer les tentatives non autorisées d'accès ou de transmission de données, fournissant ainsi une protection contre les menaces et les attaques informatiques.

Dans le cadre de mon stage j'ai utilisé le modèle 600E de FortiGate (figure 6), il me permettra de filtrer le trafic du réseau WIFILAIRE afin d'éviter toute intrusion venant de l'extérieur (d'Internet). Et en parallèle de router (rediriger) le trafic entre les différents réseaux du laboratoire et Internet.

Figure 6. Firewall FortiGate-600E.

3.4 Problématique

L'INT dispose actuellement de deux réseaux pour ses utilisateurs.

Le premier nommé USERS est destiné aux chercheurs possédant un compte utilisateur sans privilège (droit administrateur) avec des machines à jour et sécurisées. Ils disposent d'un accès à internet ainsi qu'un accès aux services internes.

Le deuxième XPRIMENT est destiné aux chercheurs et plus précisément à ceux utilisant des machines d'expérimentation comme des microscopes, des lasers… Les comptes de ces derniers sont dotés des droits administrateurs et certains PC disposent de vieilles versions de système d'exploitation comme Windows XP qui ne sont plus maintenues par l'éditeur (Microsoft) et donc vulnérables à de grosses failles informatiques. Pour cette raison tous les PC dans ce réseau sont isolés d'Internet et ont uniquement accès à un serveur de stockage de données.

Le problème ici est que certains chercheurs des PC du réseau XPRIMENT ont par moment besoin d'Internet pour leurs travaux, mais comme dit plutôt, les PC de ce réseau sont souvent sujets à de grosses failles de sécurité.

Il faut donc trouver le moyen de proposer un nouveau réseau qui permettrait à ces utilisateurs d'accéder à Internet, mais tout en bloquant leur accès aux services internes de l'INT pour éviter toute intrusion et propagation dans le réseau interne. Bien sûr l'accès à ce nouveau réseau ne sera autorisé qu'à condition de disposer de la dernière version de Windows soutenu par l'éditeur, car sinon cela ouvrira beaucoup trop de failles de sécurité.

4 Projet WIFILAIRE

4.1 Le réseau de l'INT :

Le réseau actuel de l'INT est composé d'un réseau de serveurs qui contient un cluster Proxmox qui rassemble l'ensemble des services à disposition des utilisateurs et qui est destiné au bon fonctionnement du système d'information au travers de machines virtuelles.

Dans le réseau INT, il y aura tous les services internes de l'INT accessibles depuis l'extérieur (internet) par n'importe qui comme le wiki, la page web…

On retrouvera les deux réseaux USERS et XPRIMENT.

Tous ces réseaux sont reliés au firewall FORTINET le FortiGate 600E qui permet de filtrer et sécuriser le trafic.

Les réseaux restants comme le TOIP (Téléphonie sur IP) qui servent à la téléphonie du laboratoire et les serveurs de Saint-Jérôme sont directement connectés à CISCAM qui est le cœur du réseau de Aix-Marseille Université. Juste après CISCAM on retrouve INTERNET. Ces réseaux ne sont donc pas gérés par le NIT.

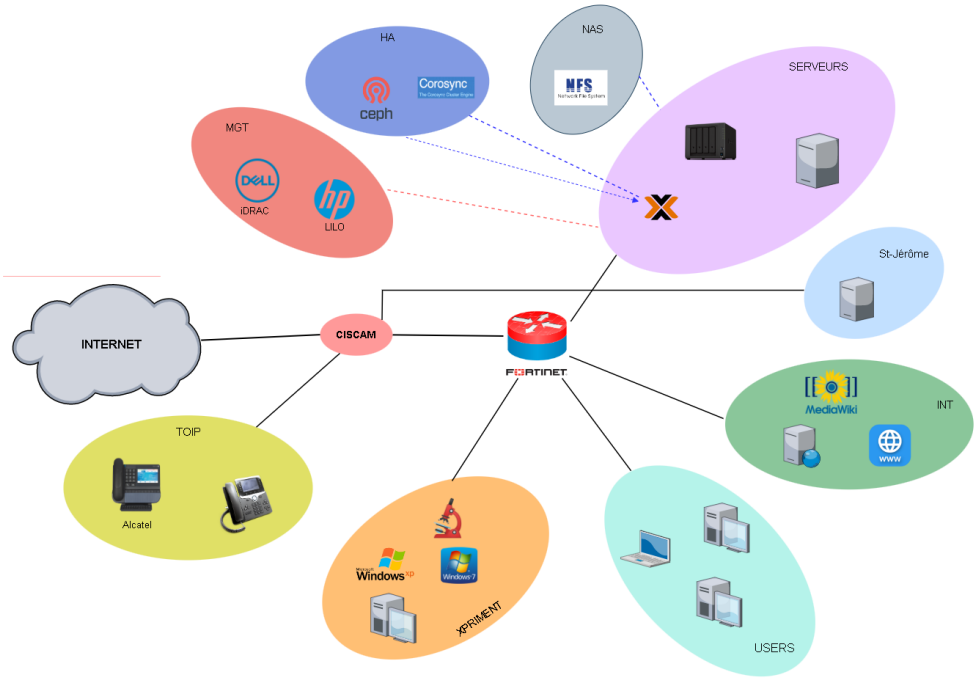

Figure 7. Schéma logique du réseau de l'INT

Comme il est observé (figure 7), la partie du réseau interne est configurée pour passer par le FORTINET, qui agit en tant que point de filtrage avant d'envoyer le trafic vers CISCAM qui le redirige vers INTERNET.

4.1.1 Emplacement visé :

Par rapport au réseau interne de l'INT, le réseau WIFILAIRE doit être placé derrière le FORTINET (figure 8) ce qui donnerait le résultat suivant :

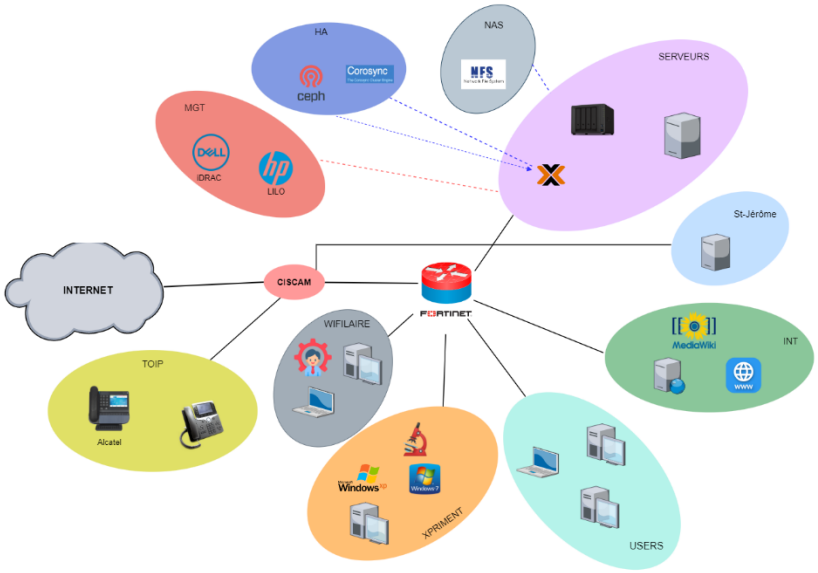

Figure 8. Schéma logique du réseau avec le réseau WIFILAIRE.

4.2 Les réseaux utilisateurs

Tout d'abord, voyons un comparatif (Figure 9) des trois réseaux qui comprend le nouveau réseau WIFILAIRE pour bien visualiser les différences et les objectifs à atteindre :

Figure 9. Type de réseaux de l'INT

On peut observer qu'ici le réseau WIFILAIRE autorisera les comptes avec droit administrateur, mais uniquement si les machines disposent des dernières mises à jour. L'accès aux services internes est quant à lui totalement bloqué sauf sous autorisation spécial de l'administrateur réseau (cas d'utilisation de VPN) qui permettra d'accéder aux services internes.

4.3 Procédure de déploiement

Il faut savoir que dans notre architecture il y a du matériel qui est géré par une entité supérieure la DIRNUM qui gère le réseau de l'université dans lequel s'intègre l'INT, le matériel en question comprend 2 stacks de switch, l'un est situé à côté de notre firewall au R-1 (c'est lui qui fait la liaison entre le firewall et CISCAM) et le second au R+2. Vu que je n'ai pas les droits d'accès sur ce matériel il faudra que je contacte la DIRNUM en leur indiquant les ports à tagger pour le déploiement du VLAN WIFILAIRE.

Il faudra ensuite :

- Créer et configurer le VLAN WIFILAIRE sur le firewall FortiGate et les switches
- Tagger les ports sur les switches concernés pour le VLAN WIFILAIRE

4.4 Création et configuration du VLAN WIFILAIRE sur Firewall

Les VLANs (Virtual Local Area Network) sont des segments logiques de réseau qui permettent de diviser un réseau local physique en plusieurs sous-réseaux virtuels. Chaque VLAN fonctionne indépendamment, avec ses propres paramètres de configuration et de sécurité. Les VLANs offrent une meilleure gestion des réseaux en regroupant des périphériques en fonction de critères spécifiques, tels que les départements ou les équipes. Ils améliorent également les performances en limitant la diffusion du trafic uniquement aux utilisateurs concernés. Les VLANs renforcent la sécurité en isolant le trafic entre les segments, empêchant ainsi les accès non autorisés ainsi que la propagation de logiciels malveillants dans le réseau.

Il faut donc créer le VLAN WIFILAIRE sur le FortiGate. Pour cela il nous faudra renseigner :

- L'adresse IP du réseau
- Le nom de l'interface
- Le nom du VLAN
- L'ID **(**identifiant**)** du VLAN
- Son Interface de Base
- Le type d'interface

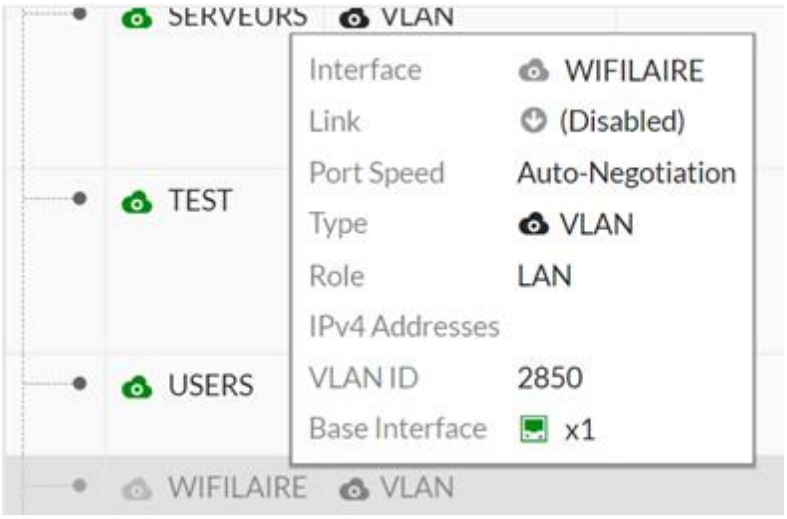

Figure 10. Configuration VLAN WIFILAIRE sur FortiGate.

Une fois le VLAN créé on se rend sur la page « Edit Interface » (figure 11) de WIFILAIRE pour spécifier le serveur DNS (Domain Name System) qui fait le lien entre l'IP et le nom de domaine des sites de l'INT et donc permet de rediriger correctement les utilisateurs vers ces sites, ainsi que le NTP (Network Time Protocol) qui permet de synchroniser l'heure de tous les PC qui seront dans ce réseau.

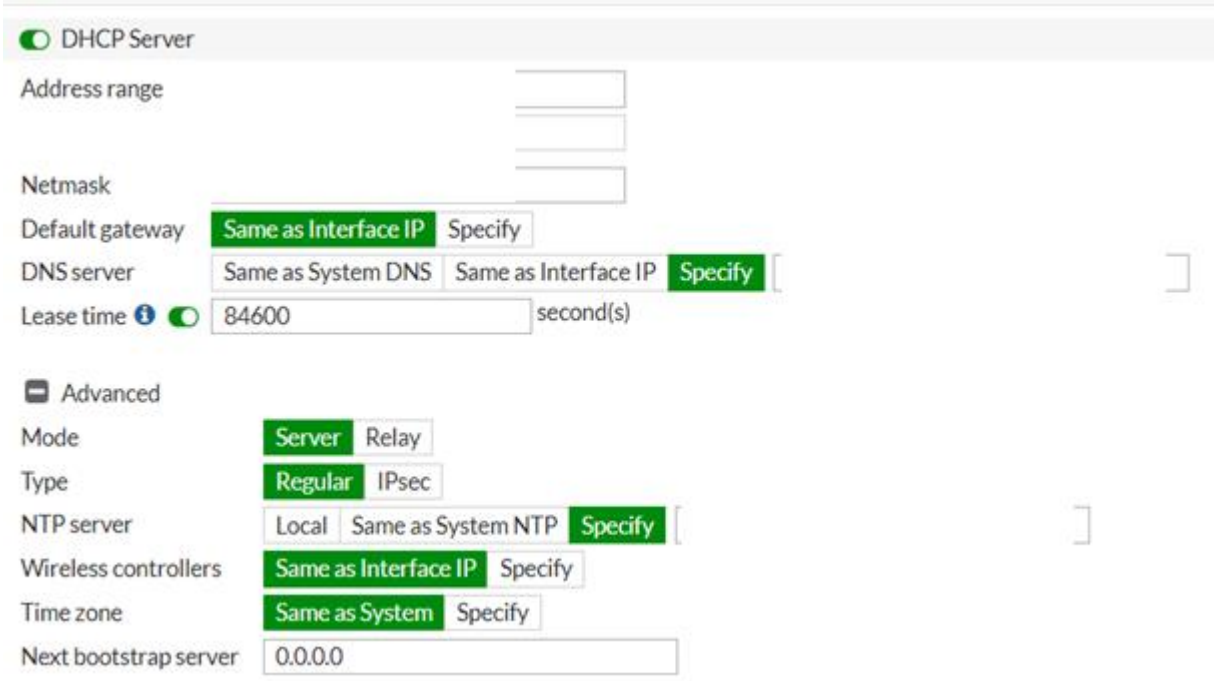

Figure 11. Édition de l'interface VLAN WIFILAIRE.

Il faudra ensuite créer l'objet « Reseau_WIFILAIRE » (figure 12) pour permettre de créer nos règles de filtrage. Il faudra spécifier l'IP du réseau, dans notre cas celui de WIFILAIRE, ainsi que sélectionner l'interface qui sera liée qui sera ici celle de WIFILAIRE.

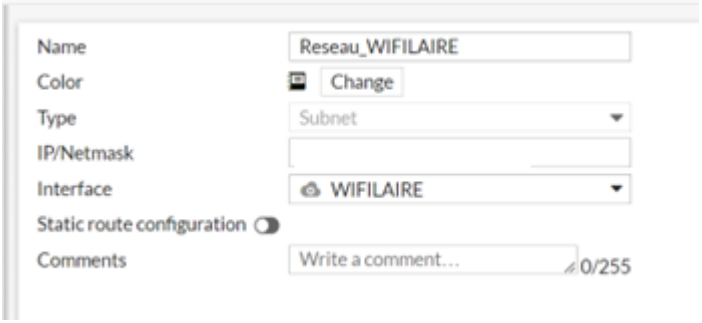

Figure 12. Création de l'objet Reseau_WIFILAIRE.

Grâce aux cours sur les firewalls j'ai trouvé cet environnement de configuration assez similaire à celui des firewalls Stormshield que j'ai étudier avec M. DAMOISEAU.

Règle de filtrage :

Maintenant que j'ai créé le VLAN il faut établir les règles de filtrage qui permettront de contrôler le trafic et de sécuriser la connexion sur le réseau WIFILAIRE. Pour cela il faut aller dans l'onglet « Policy » qui va nous permettre de rajouter ces règles.

Pour l'exemple, prenons le groupe de règles qui autorise le trafic depuis WIFILAIRE vers CISCAM (figure 13). À l'intérieur on va retrouver la règle qui autorise la connexion depuis WIFILAIRE vers INTERNET, si on regarde à droite on peut apercevoir les protocoles autorisés qui sont HTTP, HTTPS qui correspondent à un trafic web « normal ». En faisant cela, je bloque tous les autres protocoles qui ne sont pas utiles à la navigation sur Internet ce qui permet d'éviter déjà une partie des intrusions malveillantes sur le réseau interne. On retrouve également la règle qui autorisera la connexion VPN et permettra aux utilisateurs d'accéder aux services internes c'est pour cette raison que j'ai tout autorisé. En parallèle cela permet aussi de séparer les logs et de mieux administrer le trafic.

Figure 13. Règle de filtrage du groupe WIFILAIRE -> CISCAM.

4.5 Déploiement sur switch

Avant de pouvoir déployer notre nouveau réseau, il faut savoir à quel endroit tagger le port pour qu'il soit bien accessible dans toute l'infrastructure de l'INT.

Le tagging de ports sur un switch permet de segmenter et de contrôler le trafic réseau. En utilisant des entêtes VLAN, vous pouvez configurer des ports sur le switch pour appartenir à des groupes de VLAN différents. Lorsqu'un port est configuré en mode trunk, il peut transporter plusieurs VLAN à travers le même câble, en ajoutant des entêtes VLAN aux trames réseau. Cette technique est appelée VLAN tagging.

Pour tagger les bons ports, il faudra regarder du côté du schéma physique du réseau (figure 14). Par exemple sur les 2 switches en bas à gauche il va falloir tagger les ports 47-48 ce qui permettra si un utilisateur se branche à une prise connectée à ce port de pouvoir se connecter au réseau du VLAN WIFILAIRE.

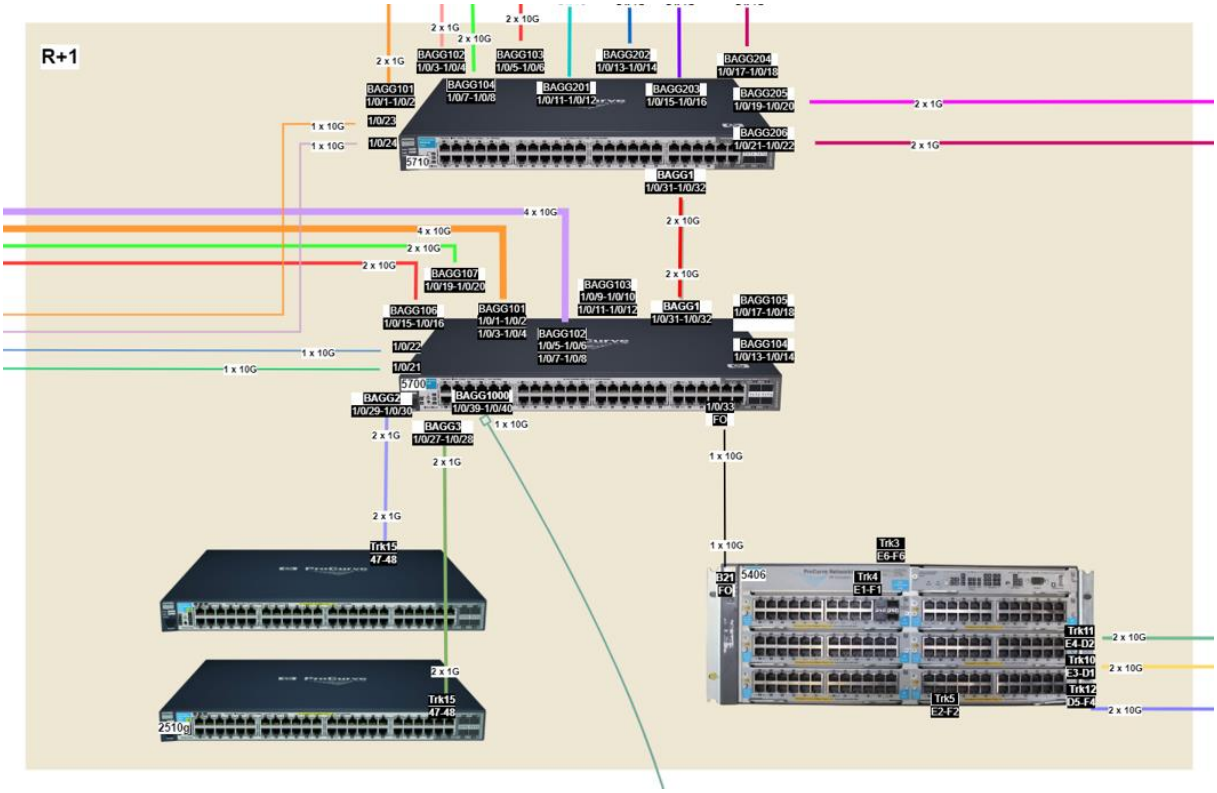

Figure 14. Schéma physique du réseau R+1.

Une fois tous les ports repérés et listés, il faut déployer les changements dans les configurations sur chaque switch HP. Pour tagger un port sur un switch HP2510G on utilise la commande suivante :

```
vlan 2850
   name "WIFILAIRE"
   tagged Trk1
   exit
```

Trk1 comprend les interfaces 47-48

Cette commande ne fonctionne pas par exemple sur un switch HP5700 qui n'utilise pas exactement le même langage, voici comment tagger un port pour le VLAN WIFILAIRE sur ce switch.

On définit d'abord le VLAN :

```
vlan 2850
 name WIFILAIRE
```

On ajoute ensuite ce vlan à l'interface du port souhaité :

```
interface Bridge-Aggregation101
 port link-type hybrid
 port hybrid vlan 1 2000 2010 2020 2030 2040 2850 2881 3004 to 3005 tagged
 port hybrid vlan 2081 untagged
 port hybrid pvid vlan 2081
 link-aggregation mode dynamic
```

On peut voir que j'ai ajouté le VLAN 2850 qui correspond à celui de WIFILAIRE dans la liste de VLAN.

4.6 Phase de déploiement

Avant le déploiement, il était nécessaire de préparer une procédure de test afin de vérifier le bon fonctionnement du nouveau réseau WIFILAIRE.

Pour cela, j'ai proposé de demander à la DIRNUM de retirer le tag d'un port. Contrairement au port tagué, le fait de retirer le tag d'un port avec un VLAN spécifique permettra de faire passer uniquement un seul VLAN. À la différence du port tagué, où le switch détecte automatiquement et redirige les appareils vers le VLAN approprié, le mode untagged nécessite une configuration manuelle du PC connecté au port pour lui attribuer le VLAN correspondant.

Dans ce cas, au lieu d'utiliser une véritable machine physique, j'utiliserai une machine virtuelle sur le serveur Proxmox et je modifierai ses paramètres réseau (figure 15) pour lui assigner le VLAN WIFILAIRE.

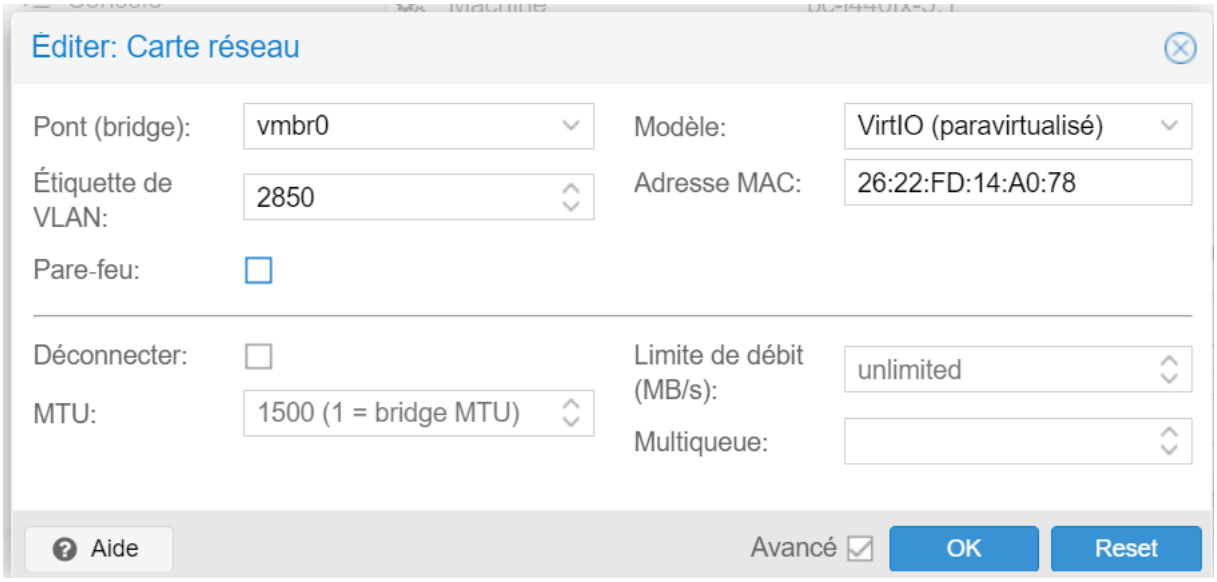

Figure 15. Édition de carte réseau VM Proxmox.

4.7 Résultat :

Malheureusement, le projet WIFILAIRE a dû être suspendu en raison d'un changement majeur dans l'infrastructure réseau de la DIRNUM. Cette évolution a pour objectif l'arrêt de l'usage du NAT dans les unités de recherche et la migration vers des réseaux gérés entièrement par la DIRNUM.

Le NAT et le VLAN sont deux concepts distincts, donc la suppression du NAT ne nous empêche pas d'utiliser le VLAN. Jusqu'à présent, nous avons créé des VLAN derrière notre pare-feu, ce qui permettait au NIT de les gérer. Cependant, avec la suppression du NAT, les VLANs seront désormais créés par la DIRNUM et gérés par eux, sans passer par notre routeur pare-feu FortiGate 600E.

5 Script Python createnituser.py :

5.1 Introduction du script python :

Les informations et comptes des utilisateurs sont gérés par une base de données LDAP qui tourne sur un Active Directory sous Samba (figure 16). Pour ajouter un utilisateur, il faut se connecter directement à ce serveur et taper à la main les commandes ce qui est très long surtout quand on a beaucoup d'utilisateurs à inscrire dans cette dernière.

Voici un exemple de base de données LDAP :

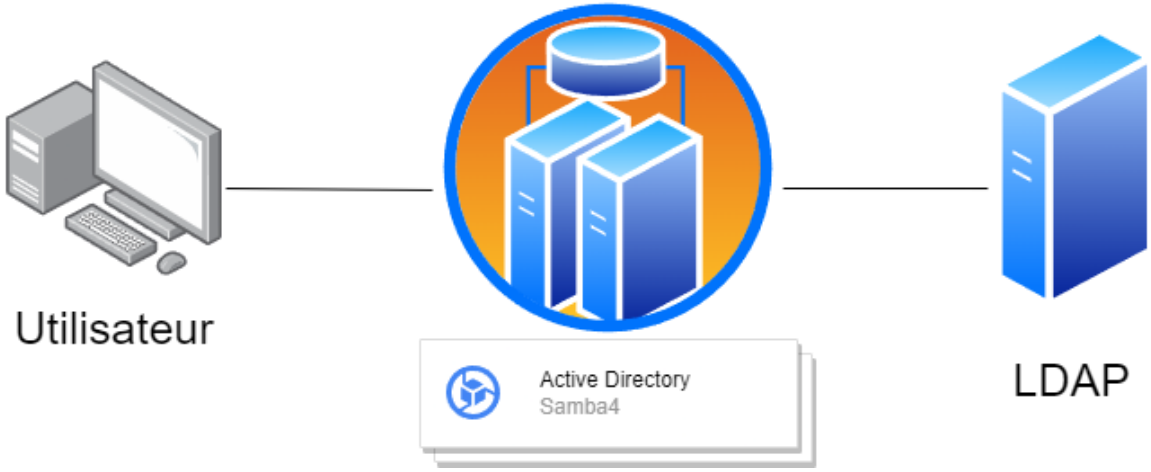

Figure 16. Représentation de l'accès au serveur LDAP

C'est pour cela que mon tuteur Arnaud CRUZEL à développer un script Python qui permet via une interface CLI Python d'inscrire un utilisateur dans la base LDAP sans pour autant devoir entrer les longues commandes complexes d'ajout, ici il suffit d'entrer les informations de l'utilisateur comme son nom, prénom… et le programme s'occupe de convertir et transférer les infos au serveur avec les bonnes syntaxes et commandes.

Le problème ici est qu'il y a par moment besoin de changer certaines informations d'un utilisateur comme la date d'expiration de son compte, son grade, sa fonction… Et pour ces cas spécifiques, il n'y a pas de fonctionnalité qui effectue cela dans le script.

J'ai donc été chargé d'implémenter cette fonctionnalité à ce dernier.

5.2 Fonctionnement du script Python :

Il m'a fallu dans un premier temps étudier les principes généraux de LDAP, la manière dont les données d'un utilisateur sont formatées, et les fonctions des librairies Python qui permettent d'interagir avec la base LDAP. Dans un deuxième temps, comprendre comment le script arrive-t-il à convertir les données entrées et les envoyer à la base de données du serveur. Pour cela j'ai observé ce que le programme fait quand on crée un utilisateur.

```
#ajout du responsable
if args.responsable:
#création du fichier ldif a envoyer au serveur LDAP
        ldif_data_resp = """dn: %(d)s
changetype: modify
add: manager
manager: %(r)s
""" % {'d': get_adattr( args.username, 'dn' ),
        'r': get_adattr( args.responsable, 'dn')}
        verboseprint("Modifications apporté à l'utilisateur %(u)s :\n%(l)s" %
{'u': args.username, 'l': ldif_data_resp})
        samdb.modify_ldif(ldif_data_resp)
```

Voici une partie du code qui permet de créer l'utilisateur dans le serveur LDAP ce que l'on peut observer ici c'est que le programme crée un fichier texte qu'il stocke dans la variable ldif_data_resp. À l'intérieur on retrouve le Distinguished Name (DN) c'est le format utilisé dans les annuaires LDAP pour identifier de manière unique une entrée dans la structure hiérarchique de l'Active directory. L'Active directory est un annuaire qui répertorie tous les appareils est les utilisateurs d'un domaine on appelle cela des objets, dans l'active directory tout est un objet que ça soit un utilisateur, une imprimante ou encore un PC.

Pour mieux comprendre, voici un exemple, nous avons un DN qui représente l'entrée d'un utilisateur nommé John Doe dans l'unité organisationnelle "Employees" du domaine "example.com". Le DN est composé des composants suivants :

CN (Common Name) : John Doe, qui est le nom commun de l'utilisateur.

OU (Organizational Unit) : Employees, qui est l'unité organisationnelle à laquelle appartient l'utilisateur.

DC (Domain Component) : example.com, qui est le domaine dans lequel se trouve l'utilisateur.

Pour « changetype : modify » il définit le type d'opération à effectuer qui est dans ce cas « modifier », "add: manager" indique quant à lui l'intention d'ajouter une valeur à l'attribut "manager" de l'entrée LDAP spécifiée. Cela signifie qu'on souhaite ajouter une relation de gestionnaire (manager) à cette entrée. Enfin "manager" va correspondre à l'attribut qui sera modifié ici la valeur est %(r)s elle correspond à la variable « r » qui stocke la valeur entrée par l'utilisateur.

5.3 Création de la fonction modify_nit_user :

Maintenant que je sais comment communiquer avec le serveur LDAP je n'ai plus qu'à créer la fonction qui permettra de récupérer les modifications et de les envoyer au bon format vers le serveur LDAP.

Pour cela j'ai récupéré un menu déjà fait dans le script puis j'ai commencé la partie la plus importante c'est-à-dire la modification des données. Pour cela deux choix s'offraient à moi, soit je crée une variable de modification pour chaque option soit je fais une boucle qui s'adapte en fonction de l'option choisie. Bien sûr dupliquer ce code 8 fois prendrait déjà une place colossale dans le script, mais aussi rendrait le programme plus « lourd ». Pour faire ma boucle « for » je dois repérer les zones variables du fichier à générer « ldif_data ». On a donc le DN qui sert à localiser l'emplacement de l'utilisateur dans la base de données LDAP, « replace » où on doit spécifier l'objet à remplacer et la dernière ligne ou l'on doit spécifier l'attribut et sa nouvelle valeur :

```
 # Ajouter les modifications confirmées au LDIF
            for attribute, new_value in changes_dict.items():
                if new_value!=None:
                    ldif_data = "dn: {}\n".format(get_adattr(args.username,
'dn'))
                    ldif_data += "changetype: modify\n"
                    ldif_data += "replace: {}\n".format(attribute)
                    ldif_data += "{}: {}\n".format(attribute, new_value)
                else :
                    ldif_data = "dn: {}\n".format(get_adattr(args.username,
'dn'))
                    ldif_data += "changetype: modify\n"
                    ldif_data += "add: {}\n".format(attribute)
                    ldif_data += "{}: {}\n".format(attribute, new_value)
                samdb.modify_ldif(ldif_data)
```

On a donc :
- le « DN » qui sert à localiser l'emplacement de l'utilisateur
- le « replace » qui indique que l'attribut spécifié sera remplacé
- la dernière ligne qui spécifie l'attribut (attribute) et sa nouvelle valeur (new_value)

Il faut donc réussir à récupérer l'attribut à modifier ainsi que sa nouvelle valeur entrée par l'utilisateur. Pour faire cela il faut stocker dans un dictionnaire qui contiendra l'attribut qui correspondra à la clé ainsi que sa valeur ce qui donne {clé : valeur} voici comment je récupère donc les informations dans ce dernier :

```
    changes_dict = {}
    change_group = {}

    #dès qu'on détecte une modif on l'ajoute dans le bon dictionnaire
    if pgivename != ogivename:
        changes_dict['givenName'] = ngivename
```

Par exemple pour le prénom, je compare le nouveau prénom à modifier, qui lui est stocké dans la variable pgivename avec la variable actuelle qui est dans ogivename. S'il est différent alors cela signifie qu'on doit l'ajouter à notre dictionnaire ce qui donnera {ngivename ; nouveau_prénom}.

Grâce à ce dictionnaire, je vais pouvoir créer ma boucle « for » qui va itérer en fonction de mon dictionnaire c'est-à-dire qu'à chaque tour de boucle elle passera à la combinaison clé/valeur suivante en envoyant le ldif_data pour effectuer les modifications à chaque fin de boucle jusqu'à ce que le dictionnaire qui contient les modifications souhaitées soit vide.

Modifier la date d'expiration d'un compte :

Ici on doit aussi pouvoir modifier la date d'expiration d'un compte pour cela il faut regarder la fonction qui est déjà disponible et qui permet de leur en attribuer une à la création de leur compte :

```
    # Convertion de la date d'expiration en seconde depuis "now"
      Y = int(args.expire.split("-")[2])
      M = int(args.expire.split("-")[1])
      D = int(args.expire.split("-")[0])
      verboseprint("jour",D," mois",M," année",Y)
      exp_date = datetime.datetime(Y, M, D)
      verboseprint(exp_date)
      exp_date += datetime.timedelta(days=1)
      verboseprint(exp_date)
      diff_nowtoexp = (exp_date - datetime.datetime.today())
      args.expire = str(diff_nowtoexp.total_seconds()).split(".")[0]
      return args.expire
```

Pour modifier la date, nous utilisons un format en secondes qui est stocké dans le serveur LDAP. Ainsi, pour effectuer la modification, nous devons convertir le format classique de date (jour-mois-année) saisi par l'utilisateur en un format en secondes, plus précisément un timestamp Microsoft. Ce timestamp est basé sur « l'epoch » (la date de référence) qui est le 1er janvier 1601 à minuit chez Microsoft. Une fois convertie, nous transmettons directement cette valeur au serveur LDAP.

Par exemple, si nous utilisons la fonction pour convertir la date du "31-12-2023" en secondes, le résultat sera 1672521600.

J'ai donc pu l'optimiser pour qu'elle soit plus courte et efficace, voici ci-dessous la fonction complète. La première partie convertit le timestamp en date lisible pour l'utilisateur et la seconde convertit la date donnée en format timestamp :

```
# Convertir la date en date lisible ou calcule la date d'expiration en seconde
def ad_timestamp(timestamp=None, expireinsec=True):
    if not expireinsec:
        if timestamp != 0:
            value = datetime.datetime(1601, 1, 1) +
datetime.timedelta(seconds=int(str(timestamp))/10000000)
            return value.strftime('%d-%m-%Y')
        return None
    else:
        exp_date = datetime.datetime.strptime(args.expire, "%d-%m-%Y")
        exp_date += datetime.timedelta(days=1)
        exp_date -= datetime.datetime(1601, 1, 1)
        filetime = int((exp_date.total_seconds() * 10**7) // 1)
        return filetime
```

5.4 Mise en production de la fonction modify_nit_user :

Après avoir terminé la fonction qui permet de modifier les utilisateurs dans la base de données LDAP, le code a été testée puis mis en production en utilisant Git pour le transférer sur le serveur. Voici un exemple de modification sur un utilisateur (figure 17) :

```
Nous allons modifier le compte pour titi ojdojf avec les données suivantes :
        Username                    : toto.t
        Adresse mail                : titi@gmail.com -> toto@gmail.com
        Fonction                     : Stagiaire
        Grade                   : IE
        Responsable                 : cruzel.a -> sbai.h
        Date d'expiration du compte : 28-06-2023
        Groupe primaire             : nit
        Groupe d'appartenance       : ['niolon', 'mprc', 'comco']
        Unité d'organisation        : CN=Users,DC=intlocal,DC=univ-amu,DC=fr


1: Prénom                               4: Fonction                             7: Date d'expiration du compte
2: Nom                                  5: Grade                                8: Groupe primaire (NE FONCTIONNE PAS)
3: Adresse Mail                         6: Responsable                          9: Groupe d'appartenance

Quel élément voulez-vous modifier (c pour valider les changements) ?
: c
Il y a des changements
{'mail': 'toto@gmail.com', 'manager': Dn('CN=sbai.h,CN=Users,DC=intlocal,DC=univ-amu,DC=fr')}
Voulez-vous appliquer ces modifications ?  (o/n):
```

Figure 17. Modification du prénom et du mail de l'utilisateur Toto.

5 Conclusion

Au cours de mon stage au laboratoire de neurosciences de la Timone, j'ai été confronté à de nombreux aspects de l'informatique, notamment à travers mes missions de déploiement du réseau WIFILAIRE et d'amélioration du script de gestion des utilisateurs LDAP. Ces expériences ont été extrêmement enrichissantes et gratifiantes, car j'ai pu constater l'impact concret de mon travail sur l'efficacité et la facilité d'utilisation des systèmes.

Pendant mon stage, j'ai eu l'opportunité d'observer et de participer à des interventions sur le terrain comme des résolutions de tickets et des déploiements de nouveau matériel, notamment dans les laboratoires de l'INT. J'ai ainsi pris conscience que le métier d'administrateur réseau ne se limite pas à l'aspect purement informatique, mais qu'il englobe également la gestion de l'infrastructure physique, le diagnostic des problèmes de câblage et la coordination avec des entreprises externes pour les installations et la maintenance.

Bien que le projet WIFILAIRE ait été annulé en raison des changements dans l'infrastructure réseau de la DIRNUM et de leur volonté de supprimer le NAT, j'ai néanmoins pu acquérir des compétences précieuses en matière de planification, de configuration et d'optimisation des réseaux. Cela m'a également permis de prendre en compte les contraintes administratives et hiérarchiques dans une entreprise.

En effet, grâce à mes efforts et à ma collaboration avec l'équipe informatique du NIT, j'ai pu apporter des améliorations significatives au script existant, permettant ainsi une gestion plus efficace et précise des utilisateurs dans la base de données LDAP. Ce succès a été particulièrement gratifiant, car il a été accueilli positivement par les utilisateurs du système, simplifiant leur expérience et facilitant leur travail au quotidien.

Ce stage a été une expérience professionnelle stimulante et diversifiée, me permettant d'explorer de multiples aspects des métiers du réseau et de l'informatique en général. La formation solide que j'ai reçue au BUT m'a fourni les bases nécessaires pour relever les défis qui m'ont été confiés tout au long du stage. Cette expérience a conforté ma volonté de poursuivre dans la voie de l'ingénierie informatique et des réseaux, un domaine qui m'inspire et me pousse constamment à me dépasser.

6 Remerciements

Je tiens à exprimer ma sincère reconnaissance à mon tuteur de stage, Arnaud CRUZEL, pour son soutien continu et ses précieuses explications tout au long de mon parcours. Sa grande expertise et sa disponibilité ont été d'une importance capitale dans le développement de mes projets. Ses conseils éclairés et sa patience ont été essentiels pour résoudre les défis techniques auxquels j'ai été confronté.

Je tiens également à remercier chaleureusement l'équipe du NIT pour son accueil bienveillant. Leur engagement envers l'excellence scientifique et leur esprit d'équipe m'ont inspiré et motivé tout au long de mon stage. Je suis reconnaissant d'avoir pu travailler avec des professionnels aussi talentueux et passionnés.

Enfin, je souhaite exprimer ma gratitude envers toutes les personnes qui ont contribué au succès de mon stage. Que ce soit en m'apportant leur aide technique, en me prodiguant des conseils précieux ou en m'offrant un environnement de travail stimulant.

Je tiens à remercier une fois de plus mon tuteur de stage, Arnaud CRUZEL, pour la relecture de mon rapport et pour les multiples conseils qu'il m'a donnés.

7 Glossaire

BUT : Bachelor Universitaire de Technologie

LDAP: Lightweight Directory Access Protocol

Wiki: What I Know Is

TOIP : Téléphonie sur IP

VPN : Virtual Private Network réseau privé virtuel qui permet de créer une connexion sécurisée et chiffrée entre un utilisateur et un réseau distant via Internet.

DIRNUM : Direction des Ressources Numériques

IP : Internet Protocol

ID : Identification

NAT : Network Address Translation est un protocole de translation d'adresses

Timestamp : Un timestamp est une valeur numérique qui représente un instant précis dans le temps.

Cluster : Un cluster est un groupe ou un ensemble de composants, d'ordinateurs, de serveurs ou de nœuds interconnectés qui travaillent ensemble pour fournir des ressources informatiques.

Machine virtuelle : Une machine virtuelle (VM) est un environnement informatique isolé et autonome qui fonctionne sur un ordinateur physique. Elle est créée par un logiciel appelé hyperviseur, qui permet à plusieurs machines virtuelles de s'exécuter simultanément sur un seul ordinateur hôte.

Proxmox : Proxmox est une plateforme de virtualisation open-source basée sur la technologie de conteneurisation et de virtualisation KVM, offrant la possibilité de gérer et de déployer des machines virtuelles et des conteneurs dans un environnement centralisé.

Log : Un log est un enregistrement des événements et des actions d'un système informatique.

CLI : Command Line Interface

HTTP : Hypertext Transfer Protocol protocole de communication utilisé pour le transfert de données sur le Web

HTTPS : Hypertext Transfer Protocol Secure version sécurisée du protocole HTTP qui utilise le chiffrement SSL/TLS pour garantir la confidentialité et l'intégrité des données échangés¨

Python : Langage de programmation interprété, qui est largement utilisé pour le développement de logiciels, l'automatisation de tâches, l'analyse de données et le développement web.

Git : Git est un système de contrôle de version qui permet de suivre et de gérer les modifications dans un projet de manière collaborative.

8 Sitographie

FortiGate 600E (8 mai 2023) https://docs.fortinet.com/document/fortiadc-e-series/hardware/fortiadc600equickstart

FortiOs (8 mai 2023) https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/954635/getting-started

Site de l'INT (17 avril 2023) https://www.int.univ-amu.fr/institut

Sambadb (5 juin 2023) https://samba.tranquil.it/doc/fr/samba_advanced_methods/samba_python_samdb.html

Proxmox (29 mai 2023) https://fr.wikipedia.org/wiki/Proxmox_VE