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

Technicien informatique et réseau

Frederico CARVALHO GAMA

STCE PROVENCE

Responsable entreprise : Damien PIERRE

Responsable académique : Éric WURBEL

2024

Table des matières

1 Introduction

En stage chez STCE Provence en tant que technicien informatique et réseau, entreprise spécialisée dans l'informatique, les réseaux et la téléphonie, ils assurent un accompagnement complet des clients, STCE fait partie du groupe RESADIA, réseau de prestataires informatiques et d'opérateurs télécom en France au service des organismes privés et publics. Lors de mon premier entretien à l'entreprise je me suis senti concerné par les services et le travail fourni par STCE, ils ont aussi montré leur soutien vers une alternance et une poursuite d'études et cela correspond avec mon envie de poursuivre mes études avec un Master en réseau et cyber sécurité. Ce sont ses raisons qui m'ont poussé à faire mon stage chez eux.

Concrètement, j'ai apporté un support aux équipes techniques en accomplissent des tâches en lien avec l'informatique et le réseau, mes missions étaient très variées, le travail pouvait se faire la fois en bureau et sur le terrain, chez les clients. Cette chance de faire beaucoup de déplacements m'as permis de voir et comprendre comment marchent réellement les infrastructures informatiques dans le monde professionnel, cela m'a aussi permis de créer des liens avec les clients, une fois que je les ai rencontrés c'était bien plus simple pour moi d'interagir avec eux lors d'interventions et j'ai pu commencer à créer mon réseau de connaissances dans ce milieu.

Dans ce rapport, je vais vous faire part de mon expérience durant le stage en commençant par l'environnent de l'entreprise, montrent le cadre de vie de tous les jours, l'esprit et les stratégies de l'entreprise, ensuite je vous présenterais le cadre technique dans lequel j'ai travaillé, les logiciels et technologies utilisés, suivi de mon travail réalisé durant le stage, les tâches que j'ai réalisées, les techniques et les solutions que j'ai pu faire et trouver. Puis le lien entre académie et monde professionnel que j'ai pu constater, avant de conclure en abordent ce que je vais retenir de cette première expérience professionnelle dans le monde des réseaux et de l'informatique.

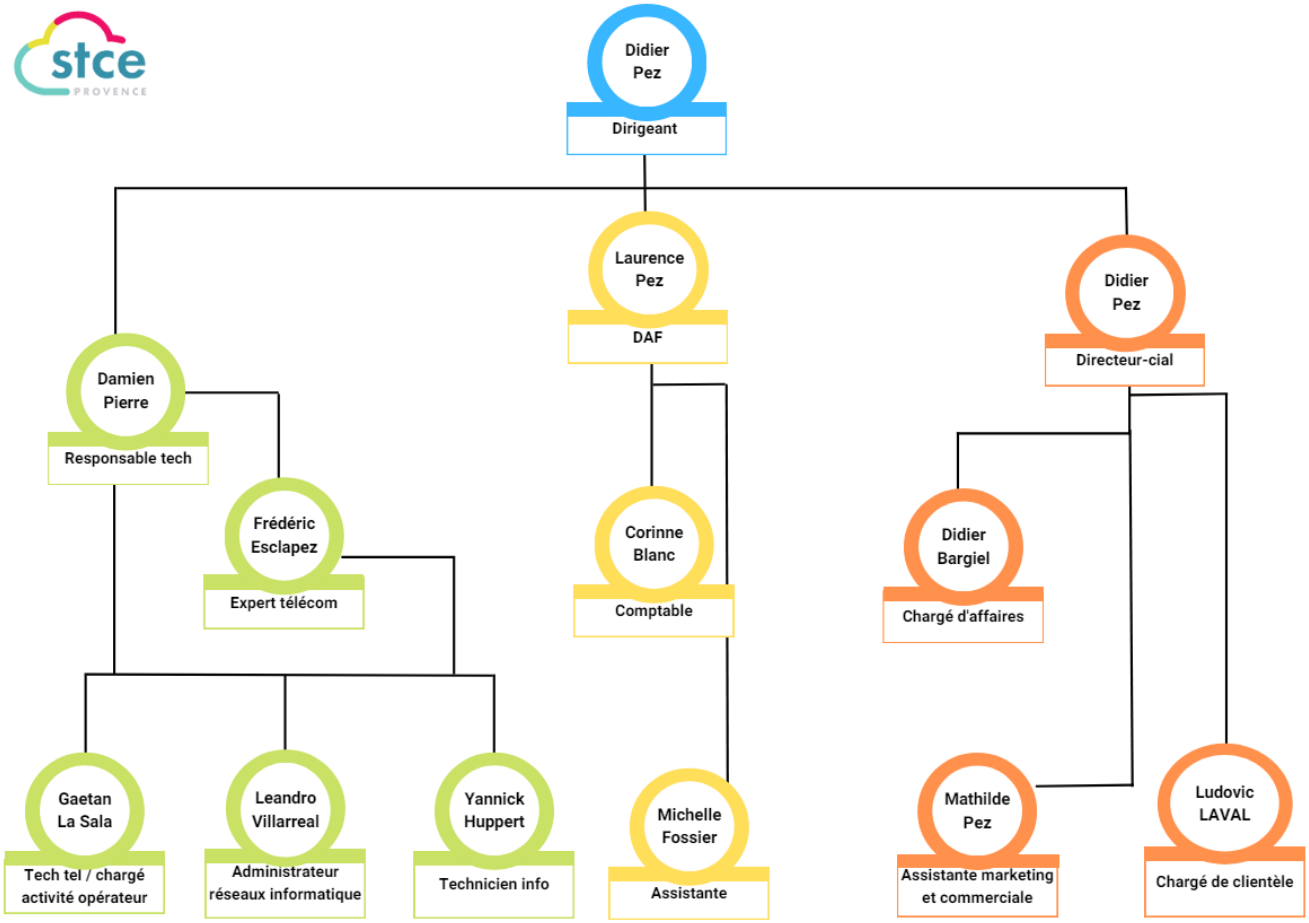
2 Environnement de l'entreprise

STCE Provence est une entreprise à taille humaine aux activités variées, elle offre à ses clients une externalisation des services informatiques, télécom, opérateur, réseaux et sécurité, cela peut se faire dès l'installation d'un parc informatique ou téléphonique, ensuite ils proposent des services de gestion, surveillance et maintenance. Aussi, une des stratégies de STCE est d'offrir le service le plus adapté et satisfactoire possible, en travaillent en liens étroits avec ses clients, pour cela elle travaille le plus souvent avec des **TPE (Très petites entreprises)** et **des PME (Petites et moyennes entreprises)** .

Les équipes techniques sont divisées en deux, une équipe de deux personnes qui s'occupe de la partie opérateur télécom et une autre de quatre personnes dont moi qui travaille du côté informatique et réseaux, cependant les équipes s'entraident régulièrement. Cette collaboration inter-équipes favorise le partage d'expérience et de points de vue, enrichissant ainsi les compétences de chacun.

Il est important de citer que l'entreprise crée une atmosphère de travail conviviale et collaborative. Les relations entre collègues sont renforcées par des activités de team-building et des espaces de travail conçus pour encourager les échanges.

Voici en dessous l'organigramme de l'entreprise en détails.



Organigramme de l'entreprise

3 Cadre technique

L'objectif de mon stage été d'apporter une assistance aux équipes techniques pour les tâches liées à l'informatiques et le réseau, pour cela j'ai dû m'adapter aux techniques utilisées, le contexte et les compétences nécessaires.

À STCE Provence, le support informatique occupe une grande partie des missions, elles sont très variées. Les clients peuvent solliciter de l'aide via des tickets sur un **PGI (Progiciel de Gestion Intégré)** appelé ARTIS, le technicien pourra donc résoudre le problème à distance grâce au logiciel TeamViewer ou le **RMM (Remote Monitoring and Menagement)** appelé N-SIGNT, le RMM utilisé permet de surveiller et gérer un parc informatique à distance. Bien que le PGI et le RMM soient les principaux outils et nous permettent de gérer les demandes clients à distance, nous nous rendons également chez les clients pour intervenir si besoin.

Voici les fonctionnalités que proposent les logiciels utilisés par STCE pour gérer les services en informatique :

- ARTIS permet aux techniciens de gérer plusieurs choses comme les tickets clients, de gérer leur planning en fonctions des déplacements et des demandes clients, de s'informer sur les matériels pris en charge selon le contrat du client, c'est un outil très utile et adapté aux nécessités informatiques proposées par STCE.

- N-SIGHT est un outil qui permet aux techniciens de gérer tout le parc informatique des clients en mettent en place des vérifications automatisés, en prenant la main sur le matériel à distance, cela permet d'avoir une surveillance active sur les réseaux de nos clients, pour que le poste soit présent sur le RMM, il est nécessaire d'installer notre agent de surveillance sur le poste.

- TEAMVIWER est un logiciel qui permet également de prendre la main à distance sur les postes clients, mais il est nécessaire d'être en possession d'un ID et d'un mot de passe fourni par le poste client, ce qui n'est pas le cas sur le RMM.

Le support réseau proposée par STCE est complet, il peut se faire dès l'installation du matériel, comme l'arrivage de fibre, puis de la maintenance des ordinateurs et de tout type de serveur, la sécurité du réseau et aussi garantie par STCE. C'est une partie extrêmement importante car si le client à un problème, il peut avoir des pertes financières, paralysie de l'activité et un déclin de la réputation. Les équipement et logiciels choisis par STCE sont des FORTINET (pare-feu, anti-virus, systèmes de prévention d'intrusion et de sécurité des terminaux).

Logos des technologies utilisées

4 Le travail réalisé

Dans cette rubrique, je vais présenter le travail que j'ai pu réaliser durant mon stage, la manière que je me suis pris pour accomplir les tâches qu'on m'a soumis en informatique et en réseau, les techniques et méthodes utilisées, les analyses et les solutions adoptées.

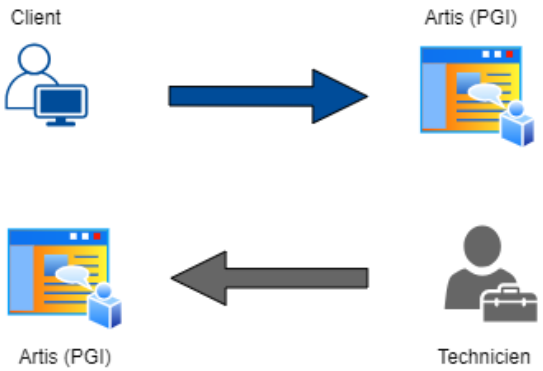
4.1 Support informatique

Je me suis occupé de diverses tâches informatiques, comme gérer des tickets clients en prennent la main sur le matériel à distance, j'ai aussi fait des entretiens d'ordinateurs, en faisant des mises à jour, installent/désinstallent des logiciels, gèrent l'espace de stockage, des migrations de systèmes d'exploitation via l'utilisation de masterisations **WDS (Windows Deployment Services)** et j'ai aussi effectué des réparations et analyses des systèmes. Le tout pour rendre plus simple, efficace et sécurisé l'infrastructure informatique du client.

4.1.1 Tickets

L'objectif de gérer des tickets est de répondre aux besoins et apporter une aide aux clients, le plus souvent en informatique.

Le client soumet un ticket via le PGI, permettant ainsi au technicien de prendre connaissance de sa demande. Une fois la solution trouvée, le technicien l'applique et rédige ensuite un rapport détaillant l'assistance fournie et les étapes effectuées.



Comment s'organise la gestion des tickets ?

- Priorité aux tickets plus urgents,anciens aux plus récents
- Adaptation selon la complexité du ticket

Le nombre de tickets à gérer par jour varie, cela dépend évidemment des besoins clients mais aussi de la complexité des tickets.

J'ai géré divers tickets nécessitant des capacités informatiques très variées, cela m'a permis d'acquérir des compétences en résolution de problèmes techniques, en communication avec les clients pour comprendre leurs besoins et en collaboration avec d'autres membres de l'équipe pour trouver des solutions efficaces et adaptées. Ce processus m'a également aidé à développer ma capacité à prioriser les tâches en fonction de leur urgence et de leur complexité, tout en maintenant un niveau élevé de service clientèle et en assurant la satisfaction des utilisateurs finaux.

Voici l'ensemble des techniques informatiques que j'ai le plus traités lors de la gestion de tickets :

- Gestion des droits utilisateurs/groupes
  Exemple : Un client se plein qu'il n'as pas accès aux ressources dans le serveur, la solution était de l'ajouter au bon groupe (Administratif) dans l'active directory.

- Gestion d'espace de stockage
  Exemple : Un client n'arriver plus à imprimer, après vérification le serveur avez plus d'espace de stockage, après la suppression d'un dossier de 50 Giga-octets qui n'avais plus aucune importance, la connexion avec l'imprimante s'est rétabli.

- Gestion de logiciels office 365
  Exemple : Un client m'a demandé de synchroniser sa boîte Outlook avec celle d'un ancien employé. Pour ce faire, j'ai attribué les autorisations nécessaires via le compte administrateur d'office 365 de l'entreprise.

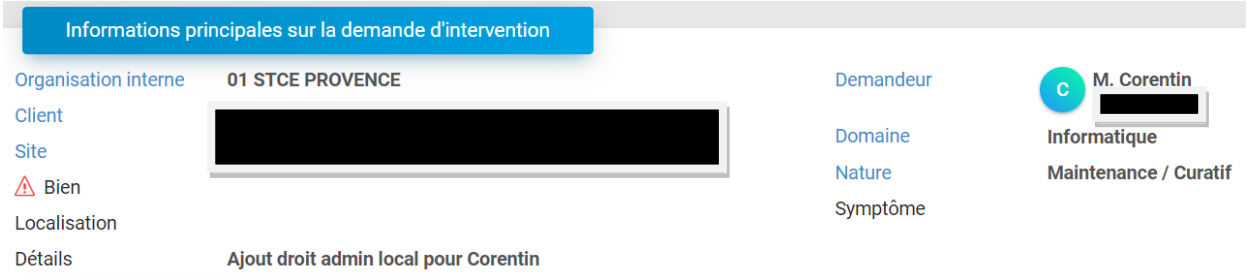
- Gestion dossiers/fichiers supprimés
  Exemple : Un client a supprimer un dossier de son ordinateur par erreur, je l'ai récupérer grâce aux snapshots qui sont programmés sur le serveur des dossiers partagés de l'entreprise.

- Mise à jour du système et des logiciels
  Exemple : Un client n'arrive plus à se connecter via **VPN (Virtual ptivate network),** au réseau de son entreprise, il suffisait de mettre à jour le logiciel utilisé pour cette connexion.

- Informer les clients
  Exemple : il est courant que des utilisateurs oublient leur mot de passe, j'ai donc à plusieurs reprises réinitialisé ou retransmis ses informations aux clients suite à leur demandes.

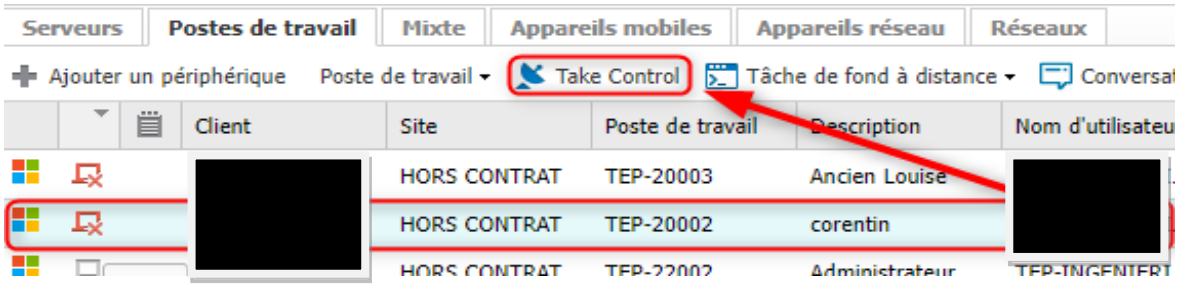
Voici en dessous, l'exemple en images d'un ticket que j'ai résolu durant mon stage.

La demande du client été d'ajouter les droits admin local pour Corentin sur son pc.



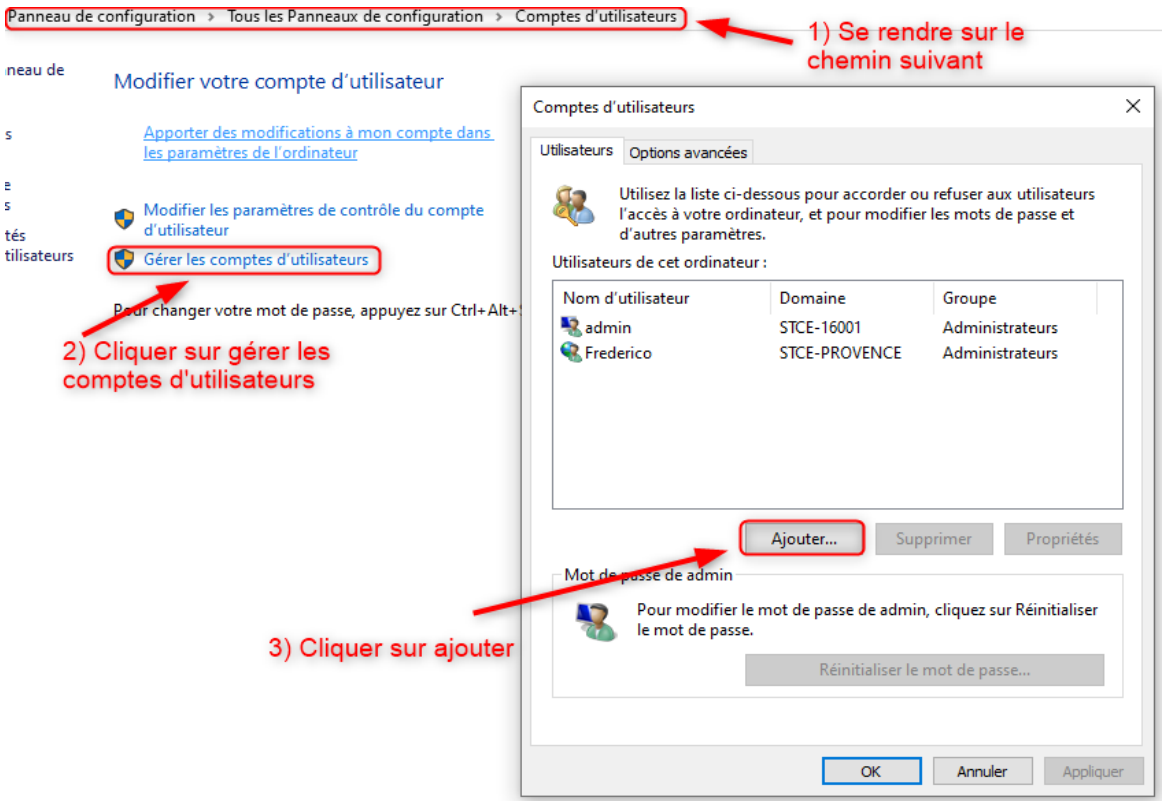
interface du PGI ARTIS et la demande du client

Ensuite, j'appelle le client pour qu'il me donne l'autorisation de prendre la main à distance sur son pc, ce ne pas une étape technique mais étique, puis je me rends sur le RMM pour prendre la main a distance sur son pc.



Interface du RMM N-SIGHT pour prendre la main sur le pc du client

Une fois que j'ai la main sur le pc du client je peux effectuer des tests et des analyses, pour ce ticket les démarches à suivre sont les suivantes :



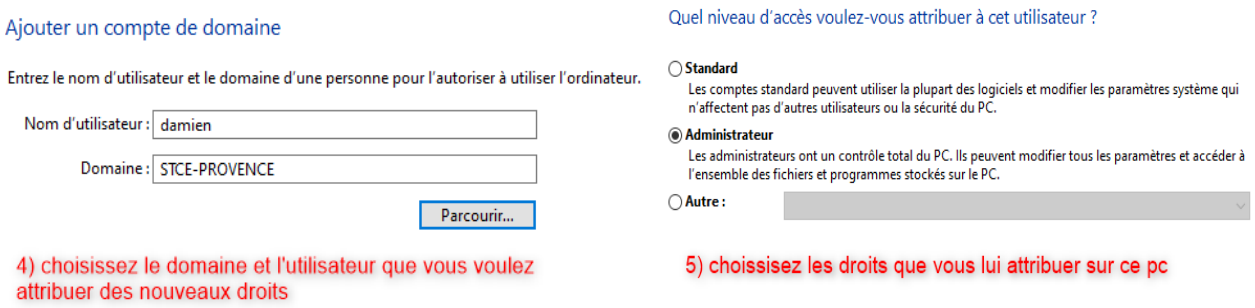
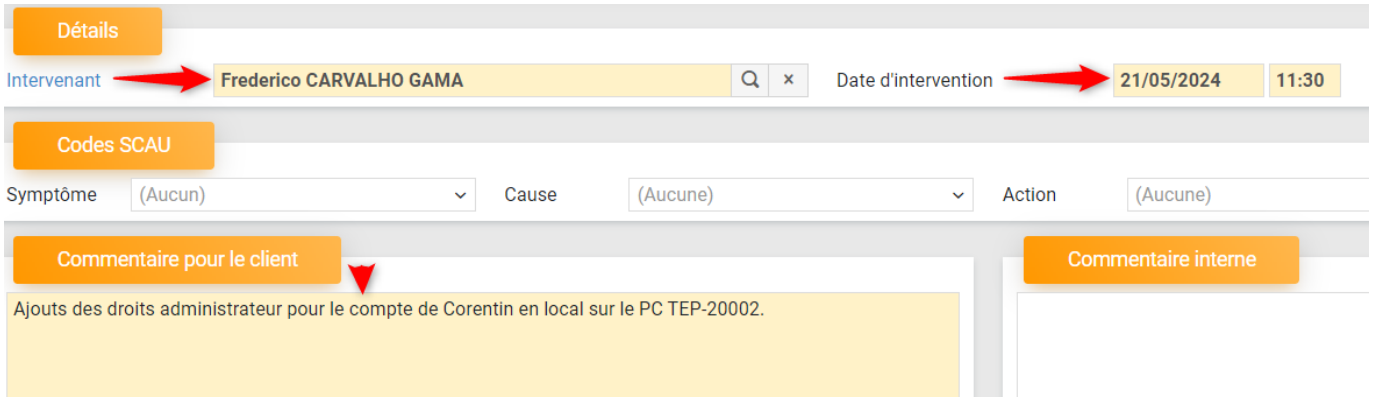


illustration des étapes pour ajouter un compte admin en local

Si tout c'est bien passé, il suffit de se reconnecter avec le compte local pour mettre à jour les droits de l'utilisateur.

Ici nous avons répondu au besoin du client, il manque plus qu'à fermer le ticket et soumettre le bilan.



Bilan sur le travail effectué déposé sur le PGI ARTIS

L'ensemble des tickets vues durant le stage m'ont apporté du savoir-faire en informatique, une certaine façon de réfléchir et d'appliquer les solutions, j'ai pu évoluer en tant que technicien informatique tout au long du stage.

4.1.2 Entretien d'ordinateurs

Cette partie du travail permet aux clients de maintenir leur environnement informatique à jour, assurant ainsi une performance optimale et une sécurité renforcée pour leurs systèmes et logiciels.

Voici les tâches d'entretien d'ordinateurs que j'ai réalisé :

Mises à jour des systèmes : Permettent de prévenir les failles de sécurité, améliorer les performances et assurer la compatibilité avec les dernières technologies et logiciel, toutes les mises à jour effectués étaient des mises à jour Windows.

Gestion du stockage : Cela commence par l'organisation des dossiers et des logiciels sur l'ordinateur, et peut également inclure l'ajout ou le remplacement d'un disque dur en fonction des besoins du client. Par exemple, un client se plaignait que son ordinateur était trop lent, nous avons donc fait le déplacement sur place, là-bas nous avons changé le disque de stockage de l'ordinateur, en mettant un disque **SSD (Solid Stade Drive)** car les SSD sont jusqu'à cent fois plus rapides que les disques durs, nous avons aussi migré son ordinateur vers Windows 10.

Changement de disque dur vers disque SDD

Remise d'ordinateurs aux clients : Lors que nous devons remettre un ordinateur au client, qu'il soit neuf ou pas, il y a plusieurs étapes à réaliser, l'installation des logiciels nécessaires pour le client et pour notre gestion, comme l'agent de surveillance, aussi nous devons faire toutes les mises à jour disponibles. Selon la situation nous devons aussi ajouter l'utilisateur dans le domaine de son entreprise, l'ajouter aux bons groupes **GPO (Group Policy Objects)**, créer ses comptes mails et donner accès aux licences utilisées par l'entreprise.

Masterisation WDS : Cette technique offre la possibilité d'installer automatiquement des postes de travail via le réseau de manière automatisée sur un ou plusieurs ordinateurs simultanément. Cette automatisation a optimisé le processus de déploiement en réduisant le temps et les efforts nécessaires. Au lieu de passer par une installation manuelle sur chaque poste de travail, la masterisation WDS permet une mise en service rapide et efficace. Cette découverte m'a permis d'appréhender les avantages de l'automatisation dans le domaine de l'informatique d'entreprise, renforçant ainsi ma compréhension des processus de déploiement et ma capacité à proposer des solutions innovantes pour répondre aux besoins des entreprises.

Comment marche réellement la masterisation WDS ?

Dans le cadre que j'ai travaillé, nous avons un serveur virtuel qui a pour rôle de fournir un service de WDS, pour que WDS fonctionne il a besoin d'un serveur **DHCP (Dynamic Host Configuration Protocol)** celui si doit être bien programmer avec des stratégies DHCP car quand une machine client démarre en **PXE (Pre-boot eXecution Environment),** il y a deux modes, le BIOS ET LE UEFI et selon le mode la configuration à mettre en place n'est pas la même. Dans le serveur WDS on a deux types d'images celles de démarrage qui permettant au client de charger l'image d'installation via le réseau, puis les images d'installation déployant le système d'exploitation via le réseau sur l'ordinateur du client, Il faut aussi configurer plusieurs paramètres tels que à qui le serveur doit répondre lors qu'il reçois une demande en PXE, la version du système d'exploitation à installer, ici Windows 10 version 22H2 et Windows 11 version 23H2, l'installations de logiciels comme TEAMVIEWER, FORTICLIENT qui est un logiciel pour les connexions **VPN (Vitual Private Network)**, les pilotes nécessaires pour les installations, l'utilisateur qui sera créé et d'autres paramètres. C'est une configuration complexe mais très utile une fois mise en place.

J’ai aussi effectué des réparations et analyses systèmes lorsqu’un client avait un problème dans son ordinateur, en identifiant la source des dysfonctionnements, en effectuant les corrections nécessaires et en veillant à ce que le système fonctionne de manière optimale. Les outils utilisés étaient les suivantes :

- chkdsk, et chkdsk /F/X/R, outil de ligne de commande permettant de vérifier s’il y a une erreur d'intégrité des systèmes de fichiers et des disques et de les réparer le cas échéant. Si la commande chkdsk détecte une erreur alors on lance la commande ckdsk /F/X/R.
    - L'option /F indique à chkdsk de réparer les erreurs trouvées sur le disque. Elle corrige les erreurs logiques dans le système de fichiers, telles que les entrées incorrectes dans la table de fichiers principale (MFT) ou les index de fichiers.
    - L’option /X force le démontage du volume avant que le scan ne commence. Cela permet à chkdsk d'avoir un accès exclusif au disque, ce qui est nécessaire pour corriger certaines erreurs. C'est utile pour les disques qui sont en cours d'utilisation ou verrouillés par d'autres processus.
    - L’option /R En plus de réparer les erreurs, cette option localise les secteurs défectueux sur le disque et tente de récupérer les informations lisibles. Cela signifie que chkdsk /R effectue toutes les tâches de /F, mais ajoute une analyse physique des secteurs du disque, ce qui peut prendre plus de temps.

- Dism /Online /Cleanup-Image /Restorehealth suivis de sfc /scannow. Dism est un outil de ligne de commande utilisé pour la maintenance et la préparation des images de système Windows. Il peut être utilisé pour monter et gérer des images Windows avant le déploiement, ainsi que pour réparer et gérer une installation Windows en cours d'exécution. Puis sfc /scannow viens comparer les fichiers actuels du système avec ceux téléchargés par Dism, cela permet de vérifier s’il y a des manques de fichiers nécessaires pour le bon fonctionnement du système.

- Bootrec.exe, utilitaire de ligne de commande, utilisé dans les environnements Windows pour réparer le MBR (Master Boot Record), le BCD (Boot Configuration Data), et d'autres problèmes liés au démarrage du système d'exploitation. Il est particulièrement utile lorsque Windows ne démarre pas correctement ou que des erreurs de démarrage surviennent. Ces commandes sont généralement exécutées à partir de l'Environnement de récupération Windows (WinRE), accessible via un disque d'installation de Windows ou une clé USB bootable. Voici un aperçu de ses principales commandes et de leur utilité :
    - Bootrec /fixmbr, cette commande répare le MBR du disque système. Elle est souvent utilisée pour résoudre les problèmes causés par les virus ou les erreurs dans le MBR.
    - Bootrec /fixboot, cette commande écrit un nouveau secteur de démarrage sur la partition système. Elle est utile lorsque le secteur de démarrage est endommagé ou manquant.
    - Bootrec /rebuildbcd, cette commande reconstruit le Boot Configuration Data (BCD). Elle est utilisée lorsque le BCD est corrompu ou absent, ce qui empêche le système d'exploitation de démarrer correctement.

- DriversCloud, service en ligne gratuit qui permet aux utilisateurs de scanner leur ordinateur à la recherche de pilotes matériels obsolètes ou manquants, puis de télécharger et d'installer les pilotes mis à jour depuis une base de données en ligne.

En effectuant des tâches telles que les mises à jour système, la gestion du stockage, la remise d'ordinateurs aux clients, la configuration de la masterisation WDS, ainsi que les réparations et analyses systèmes, j'ai pu contribuer à l'efficacité opérationnelle et à la fiabilité des infrastructures informatiques des entreprises.

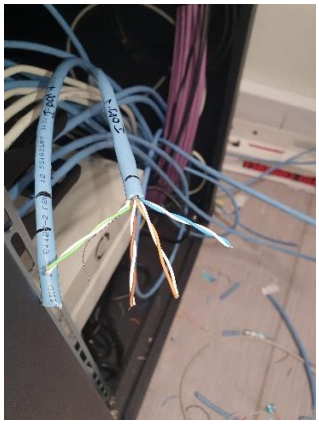
4.2 Support réseau

Mon support en réseau durant mon stage m'a permis d'apprendre beaucoup de nouvelles choses comme la mise en place de panneaux de brassage, la conception de plans réseaux professionnels, la mise en place de vérifications automatisées, la configuration de matériels Fortinet, l'intérêt d'utiliser un EDR **(Endpoint detection and response)** ou encore des interfaces comme Vade for M365 qui permet de contrôler et superviser le trafic d'emails.

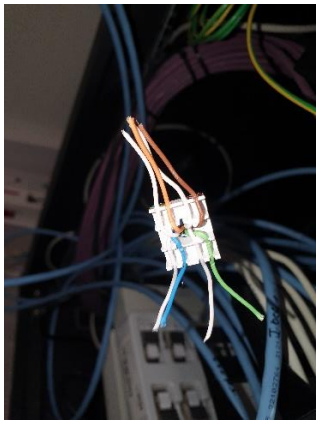
4.2.1 Couche physique

Lors de mes déplacements chez les clients, j'ai eu l'occasion d'installer physiquement du matériel réseau comme des câbles RJ-45, des commutateurs et des panneaux de brassage. Pour cette partie, les modules **R105 Supports de transmission pour les réseaux** et **R306 Fibres optiques et propagation**, vue en académie m'ont aidé car j'avais déjà une base sur comment faire et tester du matériel réseau.

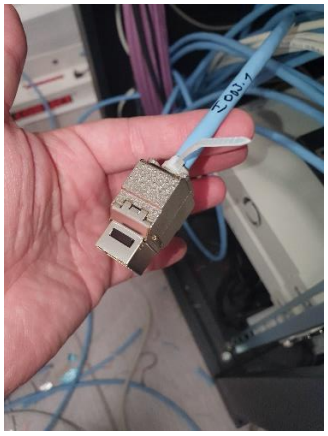
Voici en dessous des images lors de l'installation d'un panneaux de brassage chez un client.



Organisation des fils



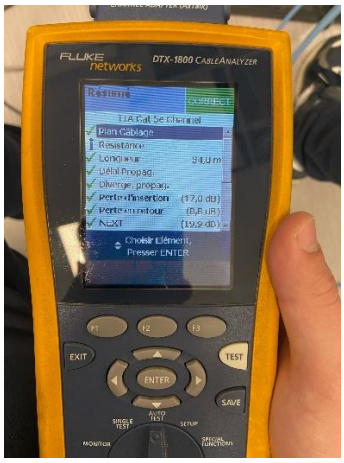
Placement des fils



Placement embout récepteur

Installation des câbles par ordre

Résultat test échec



Résultat test correct

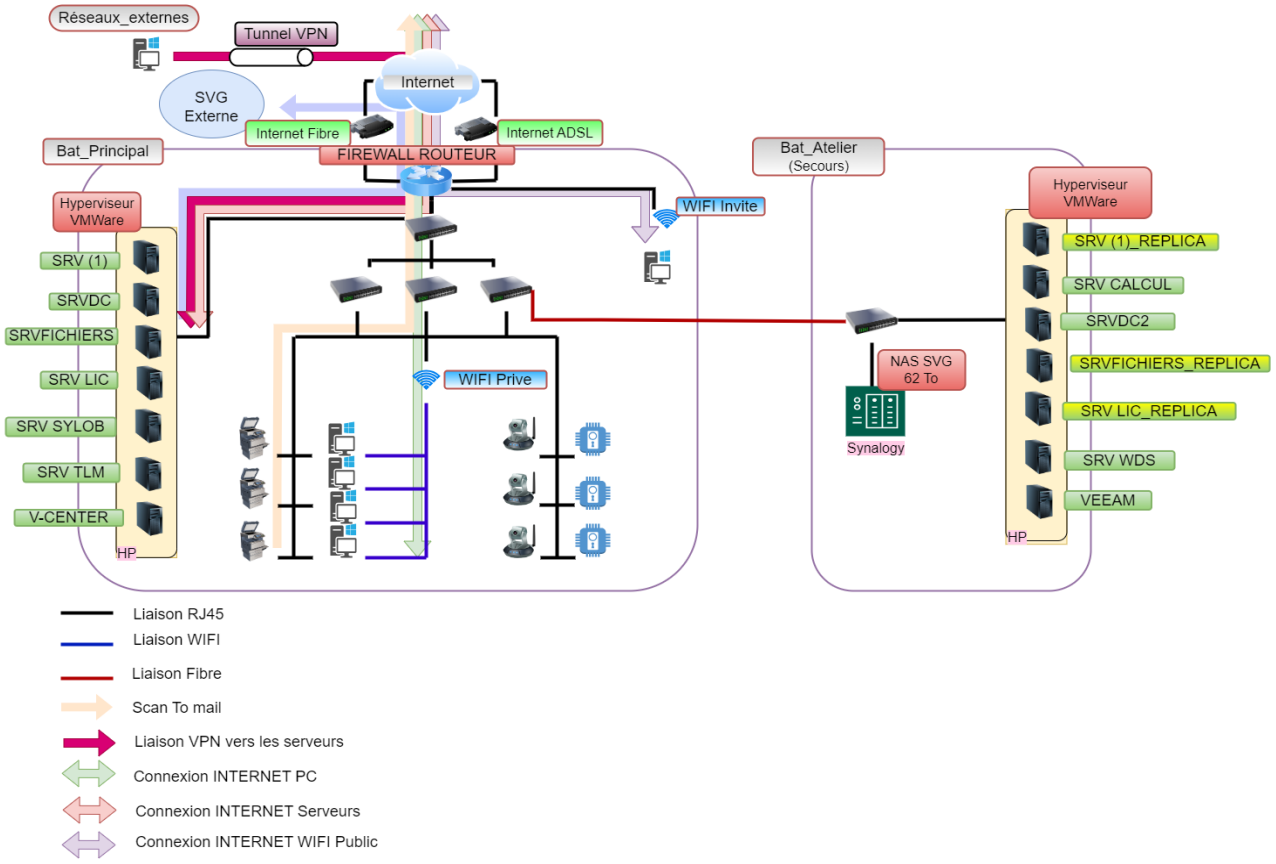
Le testeur de réseau est un outil indispensable pour assurer la qualité et la fiabilité de l'installation du matériel réseau. En effectuant des tests sur les câbles et les connexions, nous pouvons obtenir des résultats précis sur l'état de l'infrastructure. Les résultats des tests nous permettent de savoir si tout est bien câblé ou, en cas d'erreur, où elle se trouve et quel type d'erreur il s'agit.

Cette partie m'a permis d'approfondir les connaissances que j'avais déjà, mais cela a aussi renforcé la pratique et ma confiance en mes compétences techniques.

J'ai appris à identifier rapidement les problèmes de câblage, à utiliser efficacement les outils de test, et à résoudre les erreurs de manière autonome. De plus, j'ai amélioré mes compétences en organisation et en gestion de projets en assurant une installation propre et efficace du matériel, ce qui est essentiel pour garantir la fiabilité et la performance du réseau.

4.2.2 Plan logique d'un réseau

À la suite d'une visite chez un client et l'ajout de matériel réseau tel que des bornes WI-FI et des commutateurs sur son réseau, j'ai eu la tâche de faire une conception de plan logique de l'infrastructure réseau, le plan ci-dessous permet d'avoir une vision plus nette des technologies utilisées, du mode de fonctionnement du réseau, des liaisons et des moyens de communication utilisées.



Plan logique infrastructure réseau client

Ce type de plan est très utile pour plusieurs raisons. Il permet de vérifier si le réseau répond à tous les besoins du client, comme la capacité de bande passante, la redondance, la sécurité et l'accès à distance. En visualisant le plan, il devient plus facile de détecter des incohérences et de mieux comprendre l'évolutivité du réseau, en identifiant les composants pouvant être mis à niveau.

Le plan sert également d'outil de communication entre les équipes techniques et non techniques, facilitant la compréhension des aspects complexes du réseau. De plus, il fournit une documentation précieuse pour les administrateurs et techniciens de maintenance, aidant aux interventions futures, dépannages et mises à jour.

Enfin, le plan aide à identifier les points vulnérables et à mettre en place des mesures de sécurité appropriées. En résumé, un plan logique d'infrastructure réseau est essentiel pour garantir un réseau bien conçu, évolutif et capable de répondre aux exigences actuelles et futures du client, contribuant à une gestion plus efficace et proactive.

Voici les différentes technologies et techniques que STCE a mis en disposition en s'adaptent aux besoins du client :

- Arrivage d'internet : Nous avons deux moyens d'accès à internet, un arrivage via fibre et un arrivage **ADSL (Asymmetric Digital Subscriber Line)** une technologie de transmission de données qui utilise les lignes téléphoniques existant pour fournir une connexion Internet à haut débit aux utilisateurs, ce sont deux technologies différentes qui ajoutent de la redondance au réseau, si une ligne viens à tomber en panne, le réseau reste connecté.

- Firewall : Permet de filtrer le trafic entrant et sortant du réseau, en appliquant des règles de sécurité pour autoriser ou bloquer les connexions selon des critères prédéfinis.

- Tunnel VPN : Permet aux membres travaillant en externe ou dans d'autres sites de l'entreprise de se connecter de manière sécurisée et chiffrée aux serveurs et ont accès aux données disponibles sur les serveurs.

- WI-FI : Utilise des ondes radio pour transmettre des données entre un routeur ou un point d'accès et les appareils compatibles, comme les ordinateurs et les smartphones. Ici nous avons un WI-FI privé, qui permet seulement aux membres de la boîte de se connecter sur le réseau local via un mot de passe, puis un WI-FI public qui permet aux invités de se connecter sur internet mais ils ne se connectent pas sur le réseau local, c'est un réseau à part.

- Serveurs : Les serveurs jouent un rôle crucial dans une entreprise en centralisant la gestion des ressources, des données et des services.

    - SRV (1) : Serveur hébergent l'ancien PGI du client. Le PGI en question n'est plus utilisé mais les données du serveur son encore nécessaires pour le client.

    - SRVDC : Serveur contrôleur de domaine et **DCHP (Dynamic Host Configuration Protocol)**, son rôle de contrôleur de domaine inclut l'authentification des utilisateurs et le contrôle des accès en gérant les permissions selon les politiques de sécurité. Il applique les politiques de groupe pour contrôler les configurations et les permissions, maintient une base de données centralisée (Active Directory) avec des informations sur les utilisateurs, les ordinateurs, les groupes, et autres objets réseau, et assure la réplication des données entre plusieurs contrôleurs de domaine pour garantir la cohérence et la disponibilité des informations. Son rôle de DHCP inclut l'attribution automatique des adresses IP aux appareils du réseau, Il configure également d'autres paramètres réseau, tels que le masque de sous-réseau, la passerelle par défaut et les serveurs DNS, facilitant la communication et l'accès aux ressources réseau.

    - SRVFICHIERS : Serveur qui stocke et partage les fichiers importants, facilitant la collaboration entre les utilisateurs. Il gère les permissions d'accès, assure l'intégrité des données et offre une récupération rapide en cas de besoin.

    - SRV LIC : Serveur qui gère les licences flottantes, ce sont des licences qui sont prises dès qu'elles sont utilisées par un utilisateur, puis libérer une fois le logiciel fermé. Ici par exemple il stocke des licences comme SOLIDWORKS entre autres.

    - SYLOB : c'est un serveur qui héberge le logiciel SYLOB, qui est le PGI utilisé pour les entreprises manufacturières, les aidant à gérer efficacement leur production, leurs stocks, leurs ressources et leurs coûts.

- SRV TLM : Serveur de télémaintenance, mis en service à la suite de la demande du client.
- V-CENTER : Serveur de gestion centralisée pour VMware, utilisé pour gérer les machines virtuelles.
- SRV CALCUL : Serveur conçu pour exécuter des tâches de calcul intensifs, dans ce cas utilisé pour exécuter des simulations, des modélisations numériques, des analyses de données massives et d'autres tâches qui nécessitent une puissance de calcul élevée.
- SRV DC2 : Serveur de secours qui en cas de perte de communication entre le réseau et SRV DC, prend le rôle de fournir des tâches de contrôleur de domaine et DHCP. Cependant, ce n'est pas une copie du SRV DC.
- SRV WDS : Serveur qui permet un déploiement automatisé et centralisé des systèmes d'exploitation Windows sur les ordinateurs du réseau, en prenant compte des paramètres spécifiques de l'entreprise, simplifiant ainsi le processus d'installation et de gestion des images système.
- VEEAM : logiciel de gestion de sauvegarde et de récupération des données spécialisé dans les environnements virtualisés. Il permet d'automatiser la sauvegarde des machines virtuelles ainsi que toutes les données qu'elles contiennent. Lors de la sauvegarde, VEEAM copie les données vers un serveur **NAS (Network Attached Storage)**, dans ce cas, le serveur NAS SVG. Cette automatisation permet de garantir que les données sont régulièrement sauvegardées sans intervention manuelle, réduisant ainsi le risque de perte de données en cas de panne ou d'incident. De plus, VEEAM offre des fonctionnalités avancées telles que la déduplication des données, la compression, et la vérification des sauvegardes, assurant non seulement l'efficacité du processus de sauvegarde, mais aussi l'intégrité et la rapidité de la restauration des données en cas de besoin.
- NAS SVG : Le serveur vient stocker les données de sauvegarde, c'est un serveur internalisé, installé dans un autre bâtiment, il est utilisé en cas de besoin de récupération des données d'un des serveurs.
- Serveur répliques : SRV (1), SRV FICHIERS, SRV LIC ont tous les 3 des copies sur le réseau, en cas de panne ou de perte de communication, les copies de ces serveurs garantissent la disponibilité des données et des services essentiels, assurant ainsi une reprise rapide et efficace des opérations, minimisant ainsi les temps d'arrêt et préservant la productivité de l'entreprise.

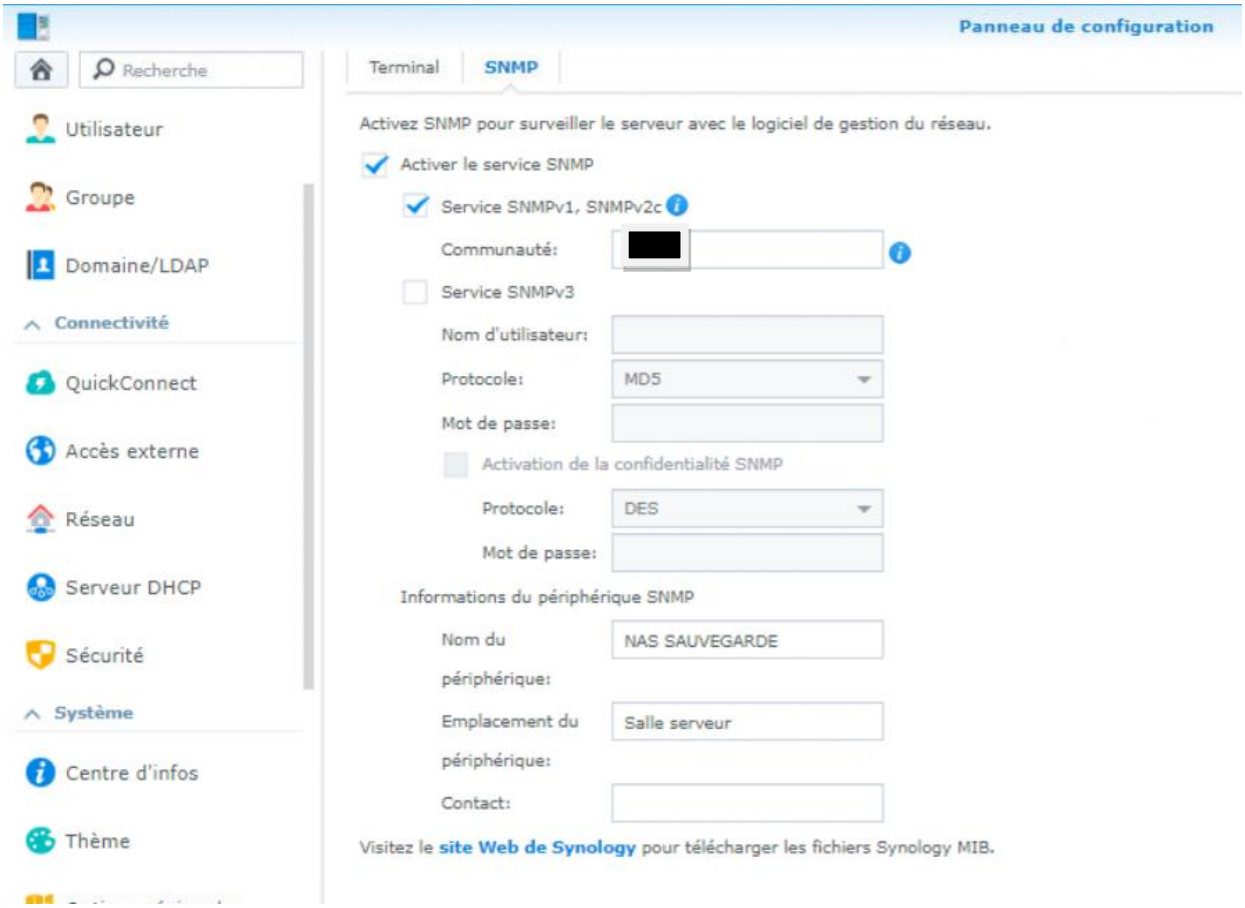
Même avec toutes les technologies déjà mises en place, il y a quand même des améliorations à apporter au sein du réseau, ce site en question est à court d'adresses IPv4 disponibles, il est nécessaire de mettre en place des VLAN, cela augmentera la plage d'adresses disponibles mais aussi la sécurité du réseau en isolant les différents types de trafic et d'utilisateurs. Ce problème est connu par notre équipe et sera traité dans un futur proche.

4.2.3 Automatisation et vérifications

Une de mes missions était de configurer des tâches d'automatisation, via le protocole **SNMP (Simple Network Management Protocol).** Grâce à SNMP, j'ai pu configurer des alertes automatiques pour détecter les anomalies, générer des rapports de performance et optimiser la gestion des ressources du réseau. Ces tâches d'automatisation permettent d'améliorer l'efficacité de la gestion réseau et une intervention plus rapide en cas de problème.

Voici en dessous les étapes d'une configuration SNMP mise en place selon les besoins du client sur un serveur Synology.

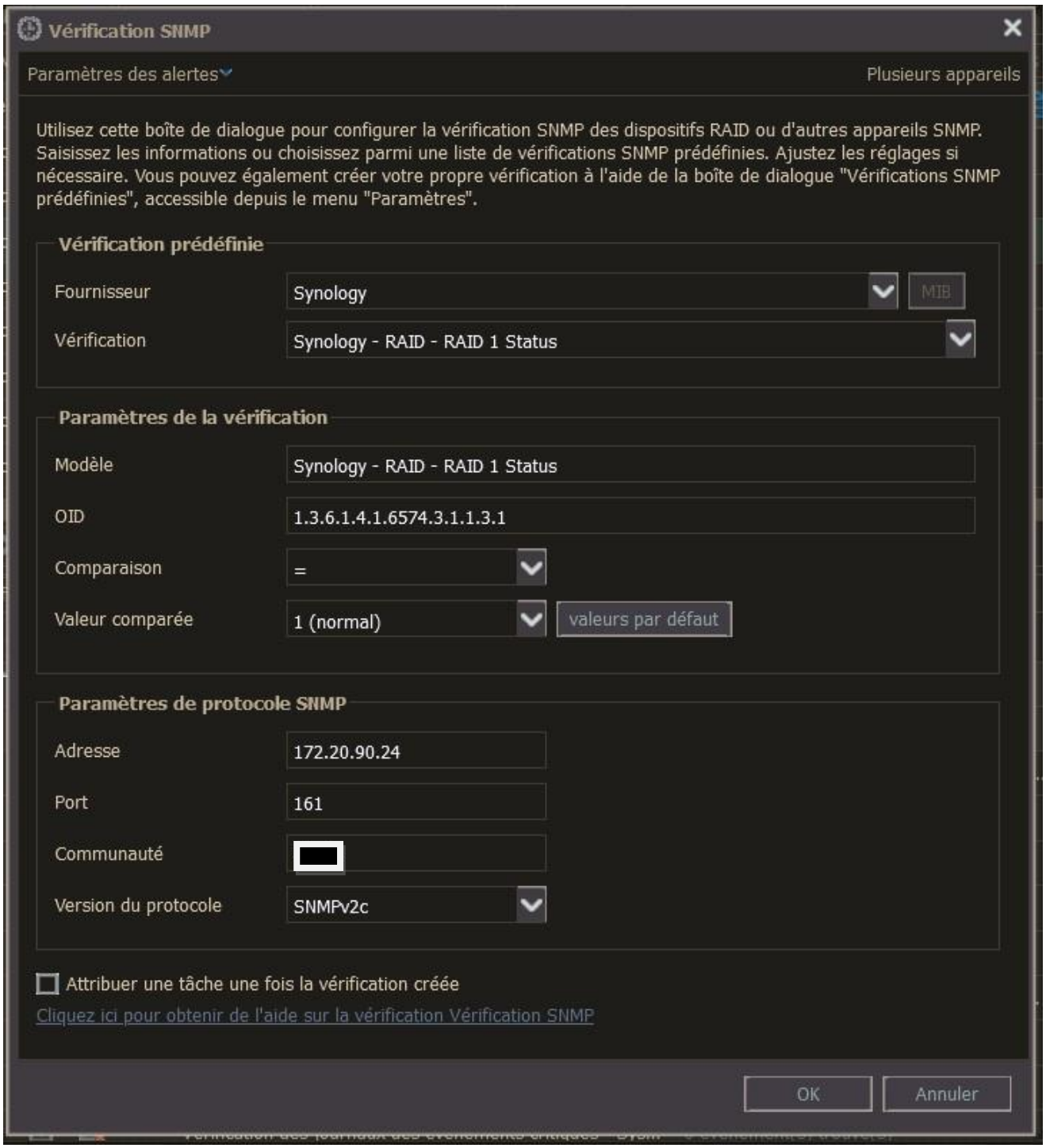
D'abord on se connecte à l'interface web du serveur grâce à son adresse IP, puis on s'identifie en tant qu'administrateur pour pouvoir modifier la configuration, ensuite nous pourrons activer SNMP et ajuter les paramètres nécessaires.



Interface web serveur Synology

Une fois le service activé sur le serveur, nous devons ajouter les règles de supervision utilisant SNMP sur le RMM, cela nous permettra de recevoir des alertes sur le logiciel et avoir une meilleure supervision.

Voici l’exemple d’une règle mise en place pour but de vérifier le statut du RAID du serveur.

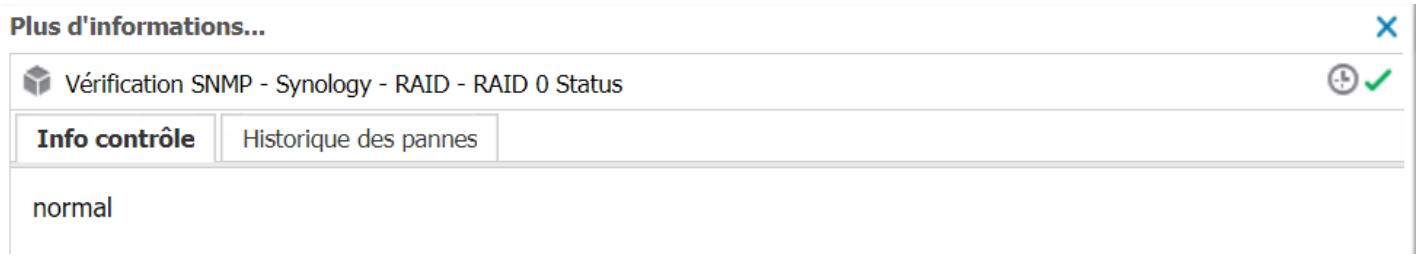


Règle ajoutée sur le RMM pour recevoir les alertes SNMP.

Pour cette configuration, on peut constater une adaptation au niveau de la version du protocole, le serveur Synology nous propose une version SNMPv3 qui est plus sécurisée car elle ajoute la cryptographie à SNMP, mais le RMM nous propose seulement des règles SNMPv2.

En sensibilisant le support du logiciel RMM à l'importance de cette mise à jour, nous pourrions améliorer la sécurité de notre système de gestion et assurer une meilleure protection de nos données et de notre infrastructure contre les menaces potentielles, mais en attendant nous devons s’adapter et mettre en place les meilleures solutions à notre disposition.

Ensuite nous pouvons vérifier si la règle a été prise en compte et le statut de la règle en question.



Règle prise en compte et statut

Nous constatons que la règle a bien été prise en compte car elle est maintenant visible sur le RMM et que son statut est "normal". Il existe 12 statuts de vérification du RAID possibles, allant du niveau de risques le plus faible au plus élevé, permettant au technicien d'agir selon l'anomalie détectée. Les voici :

1. **Normal** : Toutes les unités de disque fonctionnent normalement et aucune action corrective n'est requise.
2. **Repairing** : Ce statut indique que le RAID est en train de réparer une défaillance sur l'une de ses unités de disque et que le RAID reconstruit les données perdues ou endommagées.
3. **Migrating** : Ce statut indique que le RAID est en train de migrer vers un nouveau niveau ou vers de nouveaux disques. Cela peut être nécessaire pour étendre la capacité du RAID ou améliorer ses performances.
4. **Expanding** : Ce statut indique que le RAID est en cours d'extension pour inclure de nouveaux disques. Cela permet d'augmenter la capacité de stockage du RAID sans perdre les données existantes.
5. **Deleting** : Ce statut indique que le RAID est en cours de suppression. Toutes les données seront effacées.
6. **Creating** : Ce statut indique que le RAID est en cours de création.
7. **RaidSyncing** : Ce statut indique que le RAID est en train de synchroniser les données entre les disques pour assurer la cohérence et l'intégrité des données.
8. **RaidParityChecking** : Ce statut indique que le RAID est en train de vérifier la parité des données pour détecter les erreurs éventuelles.
9. **RaidAssembling** : Ce statut indique que le RAID est en cours d'assemblage, ce qui peut se produire après l'ajout de nouveaux disques ou après une réparation du RAID.
10. **Canceling** : Ce statut indique que l'opération en cours sur le RAID a été annulée. Cela peut se produire si une erreur est détectée ou si l'utilisateur décide d'annuler une opération en cours.
11. **Degrade** : Ce statut indique que le RAID est dégradé, ce qui signifie qu'au moins une unité de disque a échoué ou est en train de dysfonctionner.
12. **Crashed** : Ce statut indique que le RAID a subi une défaillance critique et ne fonctionne plus. Toutes les données stockées sur le RAID peuvent être perdues.

La mise en place des vérifications nous permet d'ajuster la surveillance selon les besoins du client et les besoins des techniciens, ce qui est très utile quand vous avez un grand nombre de périphériques informatiques à gérer.

J’ai aussi configuré une automatisation d’alertes sur des firewalls Fortinet, l’objectif était de recevoir une notification par mail à chaque connexion.

Pour cela j’ai configuré les firewalls en ajoutant la configuration suivante :

```
config system automation-trigger
    edit "Admin Login"
        set description "A FortiOS event with specified log ID has occurred."
        set event-type event-log
        set logid 32001
    next
end

config system automation-action
    edit "Email Notification"
        set description "Send a custom email notification to the FortiCare email address registered on this device."
        set action-type email
        set email-to ‘ADRESSE MAIL QUI RECEVRA LES ALERTES’
        set email-subject "FORTI_’NOM DU CLIENT’ _%%log.logdesc%%"
    next
end

config system automation-stitch
    edit "supervision_admin_login"
        set trigger "Admin Login"
        config actions
            edit 1
                set action "Email Notification"
                set required enable
            next
        end
    next
end
```

Après la saisie de ce script voici ce que reçois l’administrateur par mail quand il y a une connexion ou tentative de connexion sur le routeur :

date=2024-05-21 time=10:45:20 devid="FG100FTK21053022" devname=[redacted]
eventtime=1716281120348213400 tz="+0200" logid="0100032001" type="event" subtype="system" level="information"
vd="root" logdesc="Admin login successful" sn=[redacted] user="admin" ui="https([redacted]" method="https"
srcip=[redacted] dstip=[redacted] 37 action="login" status="success" reason="none" profile="super_admin"
msg="Administrator admin logged in successfully from https[redacted]"

Dans cette alerte, nous pouvons apercevoir des informations importantes lors de la connexion, la date et l’heure, le nom du routeur, les droits de l’utilisateur qui se connecte, son adresse IP, si la connexion à abouti ou pas.

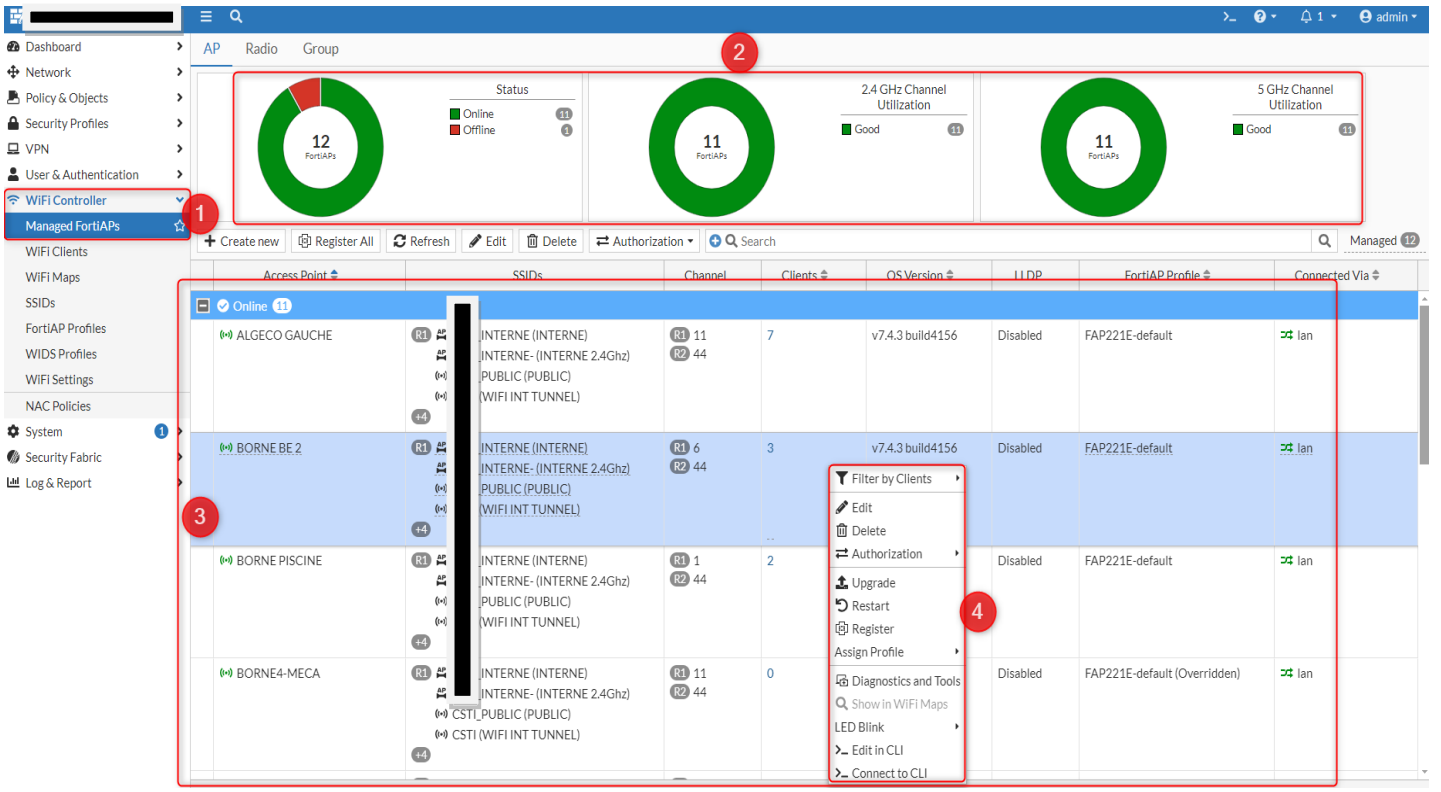
Ces données offrent à l'administrateur une vision exhaustive des connexions sur le routeur, lui permettant d'anticiper les risques et de préserver la sûreté du réseau. Cette surveillance renforce l'autonomie et la sécurité du système, assurant une défense efficace contre les cybers attaques et autres dangers.

4.2.4 Configuration et manipulation de matériel réseau

J'ai configuré et manipulé des routeurs Fortinet, ça a été pour moi une nouvelle compétence à apprendre car jusqu'à présent je connaissais seulement les matériels de chez CISCO. Cette expérience m'a permis de diversifier mes compétences en matière de configuration et de gestion de routeurs, en me familiarisant avec les interfaces, les fonctionnalités et les protocoles spécifiques aux équipements Fortinet.

Un travail que j'ai dû réaliser plusieurs fois c'est la mise à jour, la supervision et la configuration de bornes WI-FI via l'interface WEB des routeurs Fortinet.

Voici un exemple en image de l'interface WEB d'un routeur Fortinet que j'ai dû mettre à jour les bornes WI-FI et surveiller son état de fonctionnement.



Interface WEB d'un Firewall Fortinet

1. Endroit où il faut se rendre pour avoir cette page WEB dans là qu'elle nous avons accès sur toutes les bornes du le réseau local.

2. Résumé sur l'état des bornes Wi-Fi et on peut aussi voir leurs fréquences de transmissions.

3. Ici nous avons plus d'informations comme les noms des bornes, la version de l'OS des bornes, leur état, leurs SSIDS, leurs canaux, combien de personnes sont connectées à la borne, par quel réseau elles sont connectées au Firewall et si le protocole LLDP est activé ou pas. Toutes ses informations sont utiles et nécessaires pour surveiller et garder une bonne gestion du réseau.

4. En cliquant avec le bouton droit sur une borne, nous pouvons voir les possibilités de configuration suivantes : filtré les clients de la borne, la supprimer, éditer les autorisations, la mettre à jour mais pour cela il est nécessaire d'avoir à disposition le fichier de l'OS, on peut aussi ouvrir un terminal de la borne pour l'éditer via ligne de commandes directement depuis le firewall.

Durant mon stage, il y a eu un problème sur une certaine version des OS des bornes WI-FI la 7.2.0, elles se déconnectaient sans raison du réseau, j'ai donc mis beaucoup de bornes à jour vers une version 7.4.3 qui règle le problème.

Une des manipulations importantes que j'ai effectuées sur les Firewalls Fortinet concerne la redirection du trafic internet en cas de panne du lien principal. Lorsqu'un lien principal vers Internet devient défaillant, il est crucial de rediriger tout le trafic réseau vers une connexion de secours. Cette connexion de secours peut varier d'un client à l'autre et inclure des options comme l'ADSL, la 4G ou d'autres types de connexions internet. Pour rediriger le trafic, il faut ajuster les routes utilisées par le firewall. Cela se fait en modifiant les priorités des routes. Plus la priorité d'une route est basse, plus cette route est privilégiée pour le trafic réseau. Ainsi, lorsque le lien principal tombe en panne, on augmente la priorité de cette route pour qu'elle soit supérieure à celle de la route de secours. De cette manière, le trafic est automatiquement redirigé vers la connexion de secours. Une fois que le lien principal est réparé, il suffit de rétablir sa priorité en la réduisant à son niveau initial. Ainsi, le lien principal reprend son rôle de route par défaut pour le trafic internet du réseau.

Voici des schémas expliquant le principe des priorités et de route principal route secours :

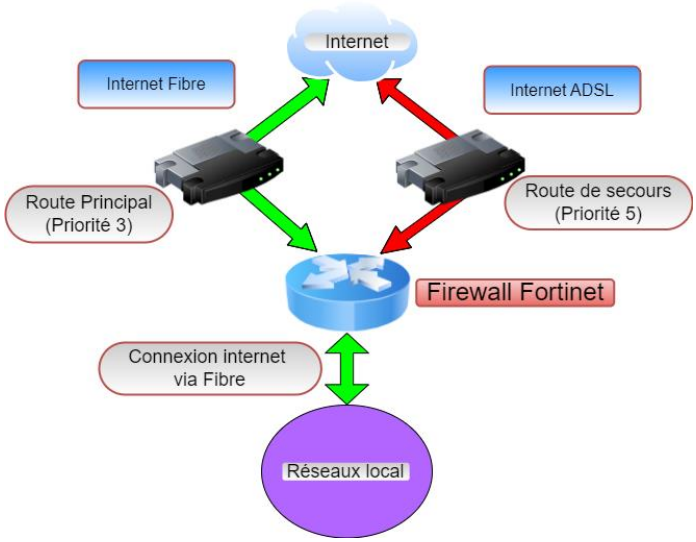


Schéma fonctionnement normal du réseau

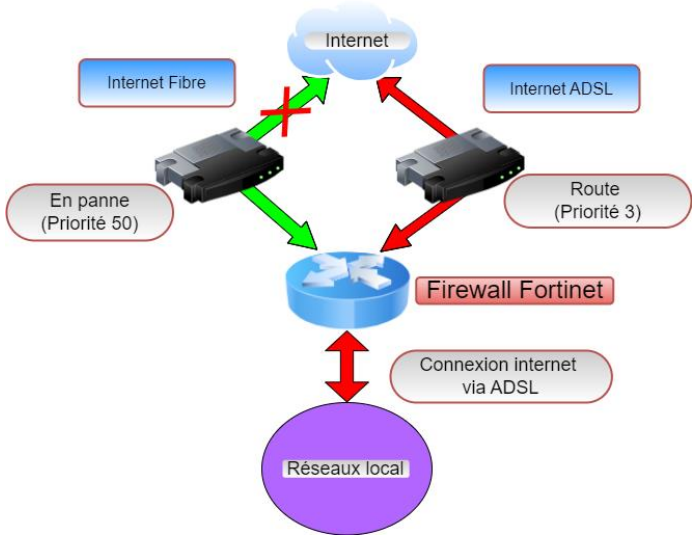
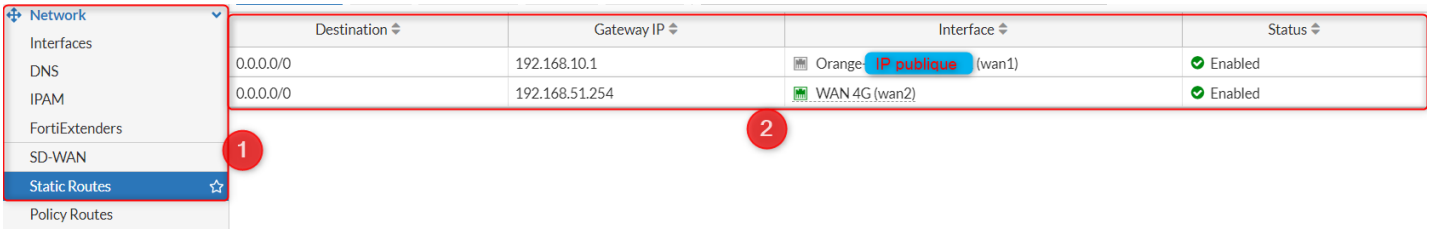


Schéma fonctionnement route principal en panne

Sur les firewalls Fortinet, nous pouvons changer les priorités des routes de manière simple, voici l'interface et les étapes pour changer la priorité des routes :

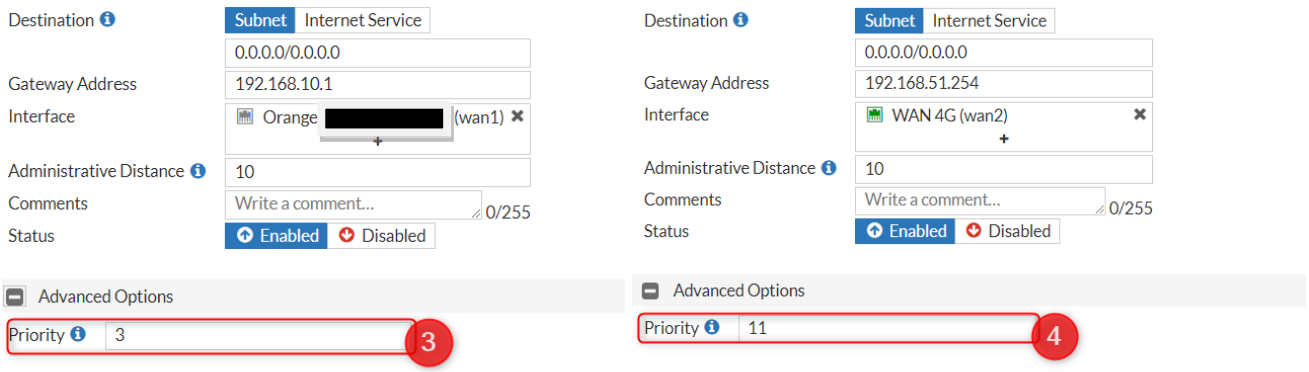


Interface Firewall

1. C'est ici qu'il faut se rendre pour voir toutes les routes statiques configurées sur le Firewall

2. Nous pouvons voir les deux routes statiques et quelques informations comme leur destination, ici 0.0.0.0 représente internet, par quelle adresse IP il faudra passer pour joindre internet, le nom de l'interface sur laquelle la règle est montée et son statut.

Puis en double cliquant sur une des routes nous pouvons modifier et voir la configuration des routes statiques.



Interface Firewall

3. La route Orange à 3 de priorité

4. La route WAN 4G à 11 de priorité

Nous pouvons donc conclure que la route principale est la route Orange, est que si elle devenait défaillante, il faudrait monter sa priorité de sorte qu'elle soit supérieure à 11 pour que le réseau de l'entreprise en question reste connecté à internet.

Ces expériences m'ont non seulement renforcé mes compétences techniques en administration de réseaux, mais elles m'ont également permis de mieux comprendre les défis liés à la résilience et à la redondance des infrastructures réseau. Travailler sur les routeurs Fortinet et gérer les changements de routes en cas de panne m'a fourni une perspective pratique sur l'importance de la continuité de service et de la réactivité en situation de crise. Grâce à ces tâches, j'ai pu développer une approche méthodique pour résoudre des problèmes.

4.2.5 La cyber sécurité chez STCE

Chez STCE Provence la sécurité dans l'ensemble de l'infrastructure réseau et informatique de ses clients est très importante, c'est une partie complexe et cela demande beaucoup de temps et de travail, j'ai pu constater que STCE met en œuvre plusieurs étapes lors du déploiement de l'infrastructure réseau pour sécuriser les réseaux de ses clients, j'ai donc participé à la mise en fonction des technologies suivantes :

La gestion des droits utilisateurs dans l'Active Directory ou dans d'autres services comme Microsoft Office est cruciale. En gérant efficacement les droits et les permissions des utilisateurs, nous nous assurons que seules les personnes autorisées ont accès aux ressources sensibles. Cela inclut la création et la gestion des groupes de sécurité, la définition des politiques de mots de passe et l'implémentation de règles strictes pour l'accès aux données.

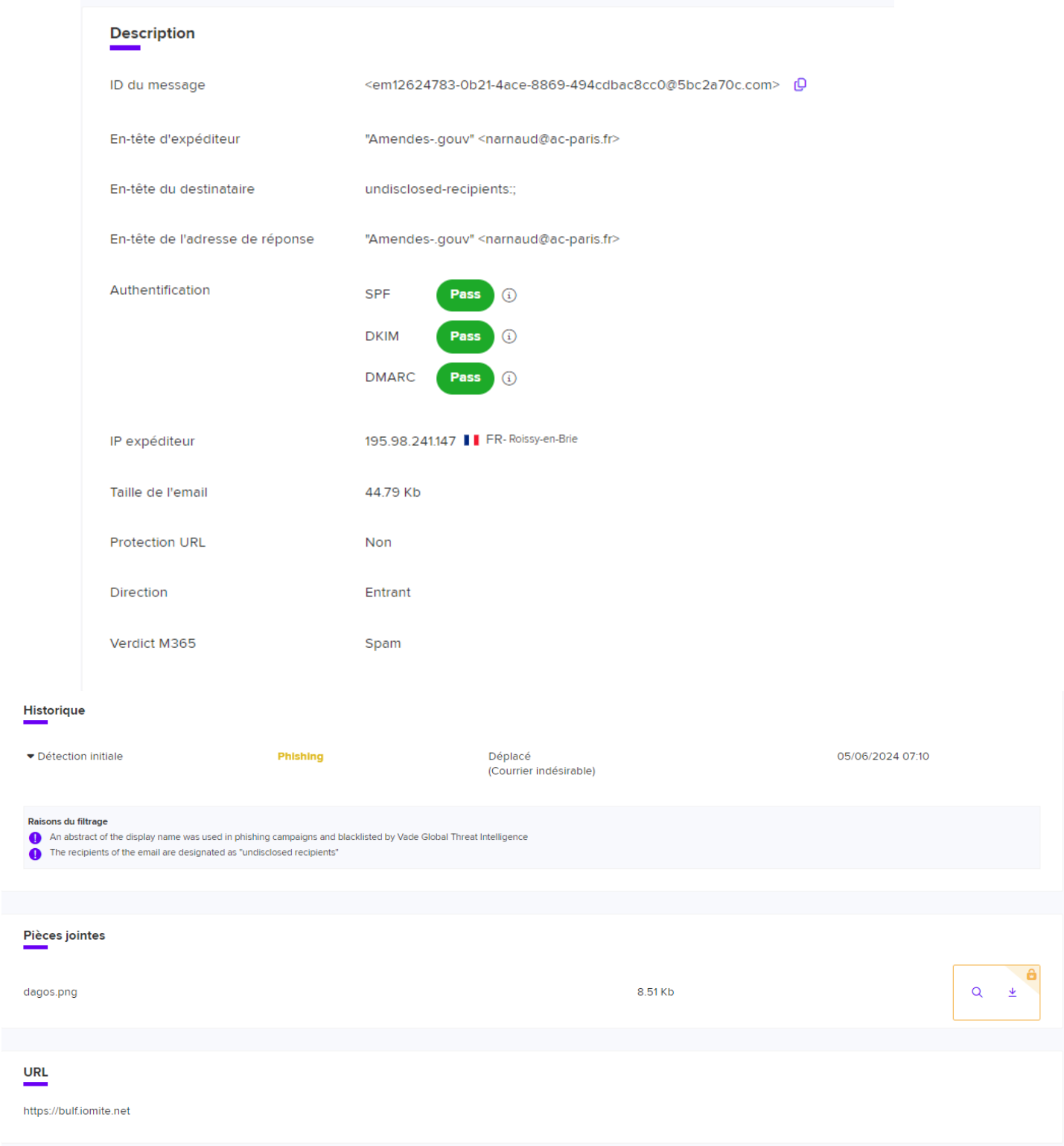
- Pour m'a part, à chaque création d'utilisateur, ou de type d'objet qui doit avoir certains droits, j'ai dû me renseigner et bien comprendre les demandes du client car chaque client à une infrastructure différente qui fonctionne d'une manière particulière, et donc ce qui est sécurisé pour l'un peut ne pas l'être pour l'autre.

Pour sécuriser les ordinateurs des clients, la technologie le mieux adapté à déployer sont les EDR. Les EDR offrent une protection avancée en détectant et en répondant aux menaces en temps réel. Ils surveillent continuellement les activités des terminaux pour identifier les comportements suspects, ce qui permet de prévenir les attaques avant qu'elles ne causent des dommages. En plus de la détection, les EDR fournissent des capacités de réponse automatisée pour isoler et neutraliser les menaces, assurant ainsi une protection robuste et réactivent des systèmes informatiques des clients.

- J'ai participé à la mise en fonction chez un client de l'EDR choisi par STCE, le SentinelOne, nous nous sommes déplacés sur place, nous avons désinstallé les anciens anti-virus puis installés l'EDR sur chaque poste.

Une des cybers attaques auxquelles les entreprises sont le plus affrontés est le phishing, selon le Rapport sur les violations de données de Verizon de 2022, les escroqueries de phishing représentent près de 36 % de toutes les violations de données. De plus, une étude de Proofpoint, entreprise américaine spécialisée dans la sécurité informatique, révèle que 83 % de toutes les entreprises ont été victimes d'une attaque de phishing en 2021. C'est une technique utilisée pour obtenir des informations sensibles, en se faisant passer pour une entité de confiance dans une communication électronique. Les attaquants envoient souvent des courriels ou des messages instantanés qui semblent provenir de sources légitimes, comme des banques ou des entreprises, incitant les destinataires à fournir leurs informations personnelles ou à cliquer sur des liens malveillants, durant mon stage j'ai constaté à quel point cette technique est utilisée de nos jours.

- Pour protéger ses clients, STCE utilisé un outil appelé Vade for M365 du groupe VADESECURE. Cet outil qui filtre, analyse et bloque les courriels suspects avant qu'ils n'atteignent la boîte de réception des utilisateurs, Vade for M365 utilise des techniques avancées de détection des menaces, telles que l'intelligence artificielle et l'apprentissage automatique. J'ai pu analyser des phishings envoyés à nos clients et détectés par VADE for M365, nous pouvons les effacer des boîtes mails, les mettre en quarantaine ou encore voire qui à cliquer sur un lien malveillant, Voici un exemple d'un phishing détecté par VADE for M365 :



Images et détails sur phishing détecté

Nous pouvons voir des détails sur l'incident, par exemple l'en-tête qu'à utilise l'expéditeur, son adresse IP, la taille du courriel, le verdict de M365 et encore plein de descriptions comme les liens URL, ou encore les pièces jointes qui ont été envoyé.

Le domaine de la cyber sécurité est gigantesque, en réalité chez STCE il y a d'autres techniques et technologies qui favorisent la sécurité dans le réseau, ici j'ai détaillé les techniques que j'ai le plus travaillé dessus, mais il y en a d'autres comme l'utilisation de la double authentification, chez nous et chez les clients, les règles de filtrage dans les Firewalls Fortinet, la sensibilisation sur le cyber attaques chez nos clients ou encore le fait de maintenir tout le temps à jours les appareils informatiques. Tout cela renforce la sécurité du réseau et de nos jours on est constamment entrain de renforcer nos réseaux sans forcément se rendre compte car les attaques évoluent elles aussi.

5 Lien entre académie et monde professionnel

Pour moi, le lien entre l'académie et le monde professionnel s'est manifesté dans la compréhension et l'aboutissement du travail à faire sans trop de difficulté. Comprendre les infrastructures réseaux des clients, le fonctionnement des outils qu'ont utilisé ou encore les règles de filtrage qui sont en place sur les firewalls Fortinet, n'étaient pas compliquées car les principes vus en académie répondaient à toutes les éventuelles questions que j'aurais pu me poser.

Mes deux premières années en académie m'ont apporté des connaissances en informatique et réseaux et une façon de faire qui m'ont été fondamentaux durant mon stage, toute la partie théorique ou même pratique via les **TP (Travaux Pratiques**) fait en cours m'ont été utile pour les tâches que je devais accomplir, les certificats **CCNA (Cisco Certified Network Associate)** de Cisco et le **CSNA (Certified Stormshield Network Administrator)** de Stormshield m'ont aussi apporté des bonnes connaissances dans ce milieu.

C'est pendant le stage que certains concepts prennent véritablement vie et que l'on comprend leur application concrète. Par exemple, la gestion des incidents en temps réel, la prise de décisions rapides sous pression, et l'adaptation aux besoins spécifiques de chaque client sont des aspects qui ne peuvent être pleinement appréhendés qu'en entreprise même si on nous prépare à ce genre de situation en académie.

6 Conclusion

Le stage chez STCE m'a permis d'acquérir et de renforcer des compétences techniques essentielles en administration réseau et informatique, avec un travail très diversifié, en faisant des tâches simples comme des mises à jour sur des PC clients, ou encore renseigner les clients de leurs identifiants, puis des tâches plus complexes jusqu'à configurer des firewalls Fortinet, mettre en place des taches de vérification automatisées, et maîtriser des outils avancés de surveillance et de sécurité comme Vade for M365.

Avec tout le travail réalisé, j'ai eu l'opportunité de m'impliquer non seulement aux compétences techniques, mais aussi au contact client, l'analyse et l'écoute de leurs besoins, l'autonomie des fonctions et à l'adoption d'une approche méthodique et rigoureuse. Ce qui est important dans le domaine que je souhaite m'expertiser, la cyber sécurité.

Aussi, STCE m'a offert une perspective précieuse sur les réalités du monde professionnel et m'a préparé à faire face à des situations variées avec confiance et compétence, pour une première expérience professionnelle dans le domaine des réseaux et l'informatique j'en garde une bonne impression et une base solide pour ma future carrière.

Finalement, mon stage chez STCE Provence m'a ouvert les portes vers une alternance au sein de l'entreprise, et ils m'ont fait part d'un avis favorable en ce qui concerne ma poursuite d'étude après cette formation.

7 Remerciements

Je tiens à exprimer ma gratitude envers mon tuteur de stage, Damien PIERRE, pour sa confiance, les responsabilités qu'il m'a confiées durant le stage, ainsi que pour tous ses précieux conseils.

Je remercie également Yannick HUPPERT et Leandro VILLARREAL de l'équipe technique pour leur accueil chaleureux, leurs nombreux conseils, leur écoute attentive face à mes questions, et surtout pour leurs réponses et leur aide précieuse.

Je suis également reconnaissant envers tout le personnel de STCE Provence pour m'avoir si gentiment accueilli et intégré au sein de l'entreprise.

Enfin, je souhaite remercier l'ensemble du corps enseignant, en particulier mon tuteur académique Éric WURBEL, pour leurs conseils et l'attention qu'ils m'ont accordés au cours de ces deux années, et plus spécialement durant ce stage.

8 Glossaire

Ticket, enregistre une tâche effectuée (ou qui doit être effectuée) par un système de support informatique afin de rectifier le ou les problèmes, résoudre les demandes des clients et exploiter l'environnement technologique.

Agent de surveillance, logiciel installé sur un système informatique pour surveiller son activité, ses performances, ou d'autres aspects liés à la sécurité. Ces agents sont souvent utilisés dans un contexte de gestion des systèmes informatiques, de sécurité informatique ou de surveillance réseau.

Masterisation, c'est un processus sophistiqué de création et de gestion d'une image système standardisé pour les ordinateurs de bureau et portables.

Snapshot, une sauvegarde locale de l'état d'un système à un instant donné.

Disque SSD, technologie de stockage pour ordinateur récente. Ils utilisent de la mémoire flash pour lire et écrire numériquement les données.

Raid, ensemble de techniques de virtualisation du stockage permettant de répartir des données sur plusieurs disques durs afin d'améliorer soit les performances, soit la sécurité ou la tolérance aux pannes de l'ensemble du ou des systèmes.

VPN, Permet une connexion chiffrée à distance entre deux points finaux.

Cryptographie, technique d'écriture où un message chiffré est écrit à l'aide de codes secrets ou de clés de chiffrement.

9 Bibliographie

Microsoft, 2023 "DISM Operating System Package Servicing Command-Line Options." Microsoft Docs

Microsoft. "How to Use the Chkdsk Tool." Microsoft Support.

Cybermalveillance.gouv,2021 "Qu’est-ce que le phishing ou hameçonnage ? " Phishing

Cisco Systems. "CCNA Certification and Training." Cisco Learning Network.

Stormshield. "CSNA Certification Overview." CSNA Certification.

Fortinet. "FortiGate: Next-Generation Firewall." Fortinet Documentation.