Institut Universitaire de Technologie,
Aix-Marseille Université

RAPPORT DE STAGE
Bachelor Universitaire de Technologie
Réseaux et Télécommunications

Support utilisateur, préparation de PC et installation conseil utilisateur

Hugo CARBONNIER

Xefi Informatique

Tuteur entreprise: Grégory FLAMENT

Tuteur Académique: Sébastien SANCHEZ

2024

Remerciements

Je tiens à remercier tout particulièrement et à témoigner toute ma reconnaissance aux personnes suivantes, pour l'expérience enrichissante et pleine d'intérêt qu'elles m'ont fait vivre durant ces dix semaines au sein de l'agence XEFI d'Aix-en-Provence Ouest.

Tout d'abord je tiens à remercier en particulier mon tuteur de stage Grégory FLAMENT pour l'accueil chaleureux qui m'a tout de suite permis de me sentir bien intégré..

Par ailleurs, je tiens également à remercier Maeva CACACE, Paul-Eric LALONDE et Pascal SIMON pour leur accueil et leurs aides techniques.

Je remercie également Sébastien SANCHEZ qui s'est assuré du bon déroulement de mon stage

Table des matières

Introduction

L'agence XEFI d'Aix-en-Provence m'a accueilli pour réaliser le stage de fin de deuxième année de BUT. Cette période de stage est l'opportunité pour chaque élève de pouvoir mettre en pratique les compétences qu'il aura acquises durant les deux premières années de formation et bénéficier d'une première expérience dans le milieu de l'entreprise.

Le groupe XEFI est une entreprise qui déploie des solutions informatiques pour des TPE/PME. Il gère également la maintenance du parc informatique de ses clients. Ces différentes missions permettent de rencontrer des problématiques différentes. A travers ces diverses activités j'ai pu avoir un aperçu des compétences requises dans ce domaine.

De nos jours, la gestion d'un parc informatique est essentielle à la vie d'une entreprise. L'informatique est omniprésente dans tous les domaines d'activité. Les avancées technologiques en la matière évoluent en continu. La gestion et l'utilisation de ces équipements font appel à un nombre important de professionnels spécialisés et de métiers différents.

Pour ma part, je compte me spécialiser dans les réseaux. Le fait de pouvoir acquérir tous les jours de nouvelles connaissances dans le domaine des réseaux, télécommunications ou encore cybersécurité, qui est selon moi un secteur très intéressant, me motive dans mon projet professionnel qui est de devenir, à la fin de mon cursus, Architecte réseaux.

J'ai été ravi d'effectuer ce stage dans cette entreprise. J'y ai vécu une expérience professionnelle et humaine enrichissante.

Présentation du Groupe Xefi

En 1997,Sacha Rosenthal crée la Société de Service en Informatique XEFI à Lyon (Auvergne-Rhônes-Alpes).

L'objectif est de se positionner sur le marché des services informatiques pour les PME/TPE.

XEFI intervient dans des domaines technologiques variés :

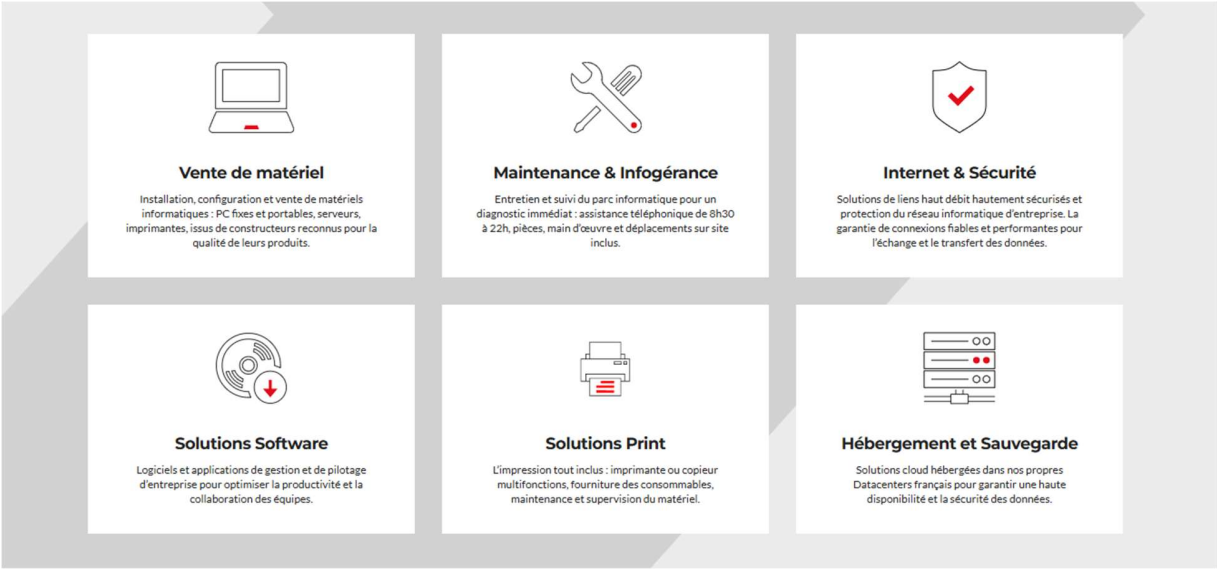


Figure 1 : Schéma des domaines traités par Xefi

Le groupe XEFI est composé d'environ 180 agences.
Chaque Agence gère ses propres clients mais il peut arriver que deux agences travaillent ensemble sur un projet ou une problématique.

XEFI travaille avec des partenaires récurrents pour la vente et la configuration d'équipements. Pour l'installation et la configuration de poste, ce sont des PC de la marque HP qui ont été choisis. En ce qui concerne la partie sécurité/réseaux, XEFI travaille avec le constructeur SOPHOS. Leurs antivirus, firewalls ou encore VPN sont déployés chez les clients XEFI.
Les switchs utilisés sont de la marque Aruba.
L'outil utilisé pour prendre la main sur le poste des clients est ISL.

Pour cela, le client doit entrer un code généré par le logiciel de prise en main dans le site accessible via l'URL support.xefi.fr

Interface client:

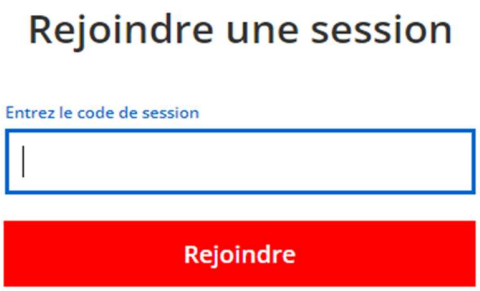


Figure 2: Interface client pour la prise en main

Interface technicien:

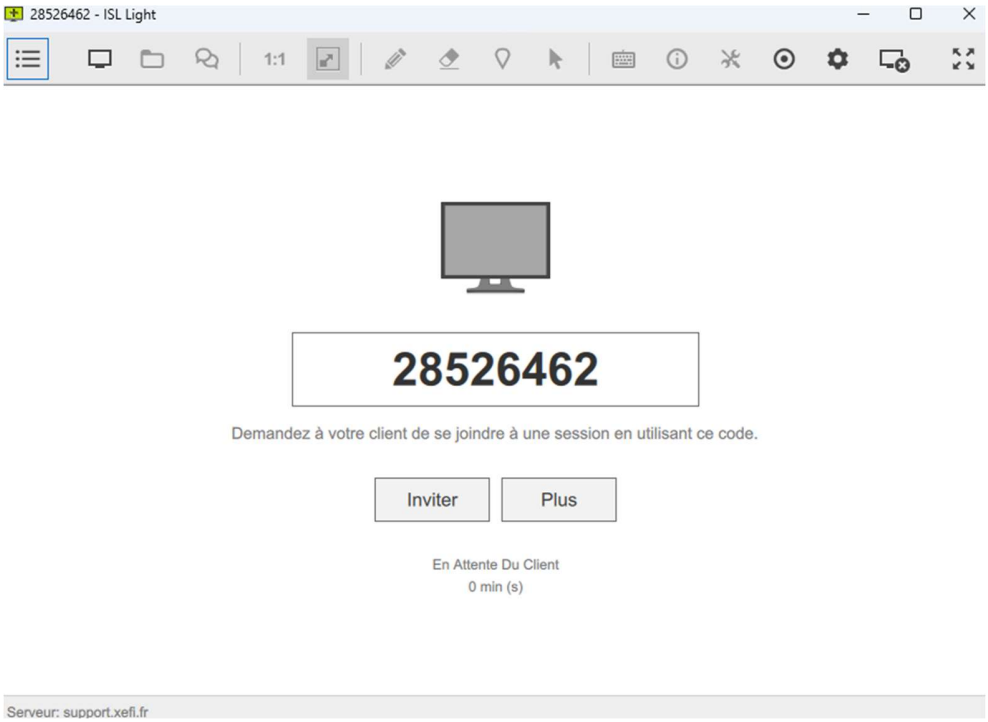


Figure 3: Interface technicien pour la prise en main

Pour les clients ayant souscrit à la maintenance, il y a la possibilité d'installer directement ISL sur leur poste. Grâce à quoi le PC sera enregistré sur l'outil de prise en main côté technicien pour qu'il puisse prendre la main sur le poste sans avoir à renseigner un code au client.

L'agence d'Aix-en-Provence Ouest

L'agence qui m'a accueilli pour mon stage (Agence d'Aix-en-Provence Ouest) est constituée de quatre personnes, les deux techniciens, Pascal et Paul-Eric avec qui je travaillais la plupart du temps, Maeva l'assistante commerciale et Grégory Flament Le gérant.

L'agence compte environ 270 clients acquis durant 13 années.

Les clients qui sont des TPE/PME proviennent de divers secteurs d'activité :

- Hôtels/Restaurants
- Cabinets d'avocats
- Agences Immobilières
- Médecins
- Administrations
- Entreprises BTP

Présentation générale du stage

Les objectifs

Objectifs personnels :

- Acquérir de nouvelles compétences liées au monde de l'entreprise
- Découvrir le monde du travail et me faire une première idée sur mon futur métier

Objectifs de l'entreprise :

- Me donner différentes missions afin de leur apporter un gain de temps
- Me faire découvrir de nouvelles notions qui me seront utiles dans le futur

Mes missions

J'ai pu réaliser différentes missions durant ces dix semaines de stage. Dans un premier temps, je vais vous présenter une mission qui s'apparente comme un projet. L'objectif consistait à installer une infrastructure de sécurité dans le cabinet d'un docteur.

J'enchainerai ensuite sur la résolution d'un problème d'accès à une adresse mail d'un client sur plusieurs jours. Ce problème l'empêchait de travailler correctement. Je vous détaillerai les solutions proposées dans un premier temps n'ayant pas abouties et le cheminement de pensée que l'on a eu avec l'équipe pour arriver à la solution finale.

Pour ces deux missions j'évoquerai ma première expérience de contact client. Effectivement, la compréhension des attentes des clients, la communication, expliquer de manière à se faire bien comprendre sont des postures qui ne sont pas si simples et cela s'apprend.

Je vous parlerai enfin des tâches plus petites mais tout de même récurrentes.

Savoir-Être

Curieux : Le métier de technicien nécessite d'être curieux car le domaine de l'informatique est en constante évolution, il est donc important de s'informer sur les nouveautés afin de proposer la meilleure solution possible aux clients.
Patient : Le métier de technicien nécessite d'être en contact avec le client, ce qui implique de faire preuve de patience face à des utilisateurs pas toujours très à l'aise avec les outils informatiques.
Ecoute : savoir écouter et entendre le client afin d'évaluer au mieux son problème, sa demande ou son projet.
Autonome : L'équipe étant pas mal occupée, je ne pouvais pas me permettre de leur demander de l'aide tout le temps. Il faut donc bien savoir se documenter, savoir où trouver les bonnes informations et savoir s'en servir à bon escient.

Savoir-Faire

- Connaissances dans les réseaux et sa sécurité (gestion de switch/Firewall.)
- Connaissances sur le système d'exploitation windows
- Gestion Microsoft/Google

Mise en place d’une nouvelle infrastructure de sécurité

Un médecin, client de XEFI, souhaitait renforcer la sécurité informatique de son cabinet médical tout en intégrant un point d'accès 4G de secours. Pour répondre à ce besoin, XEFI a recommandé et mis en œuvre une solution complète incluant l'installation d'un Firewall Sophos XGS, un switch Aruba 1930, ainsi qu'une borne 4G Huawei B535-232.
Cette configuration permet d'assurer une protection optimale des données sensibles du cabinet tout en garantissant une continuité de service en cas de défaillance du lien principal.

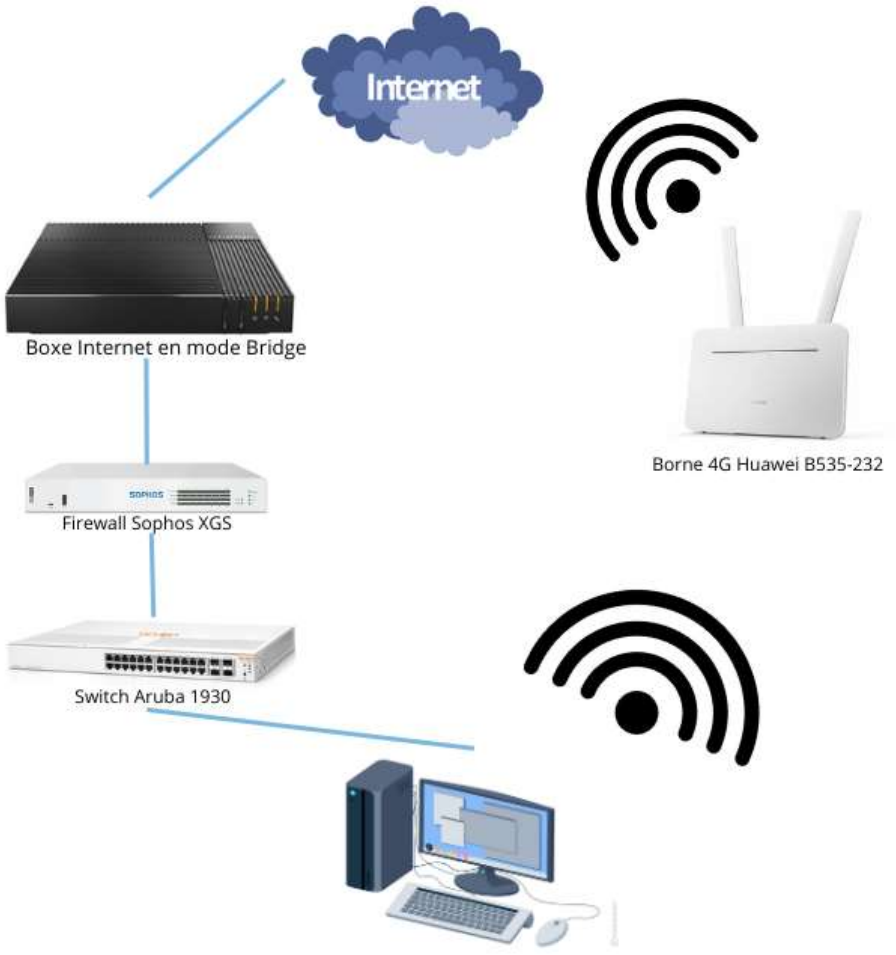


Figure 4: Schéma de l’infrastructure à mettre en place

Présentation du matériel

Firewall sophos XGS: Sophos est un constructeur d'équipements et d'applications de sécurité réseaux. Les équipements physiques (firewall) sont gérés depuis une interface web. Je vais vous présenter une configuration de base pour tous firewall Sophos, c'est en effet ce type de configuration que j'ai effectué pour les besoins du client.
Pour aider les techniciens à la configuration, le groupe XEFI met en place des documentations internes pour les équipements sophos et aruba.

Les possibilités offertes par le Firewall Sophos XGS sont nombreuses:

- Filtrage web
- Règle de pare-feu
- Création de VPN
- Blocage d'applications
- NAT
- Serveur DHCP
- Protection serveur WEB

Voici l'interface Web du Firewall Sophos XGS, Les onglets décrits ci-dessous sont ceux qui nous intéressent :

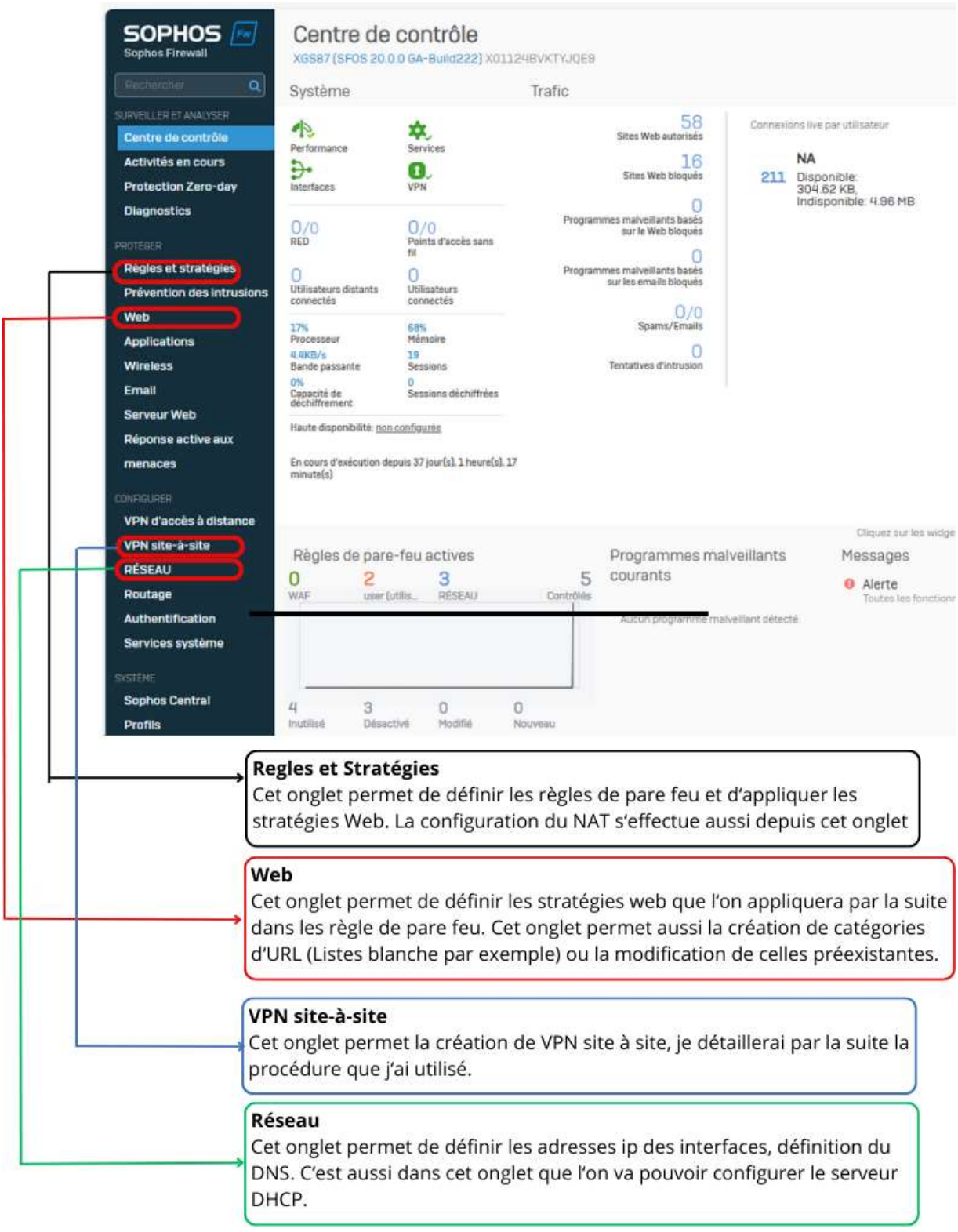


Figure 5: Explication de l'interface Sophos

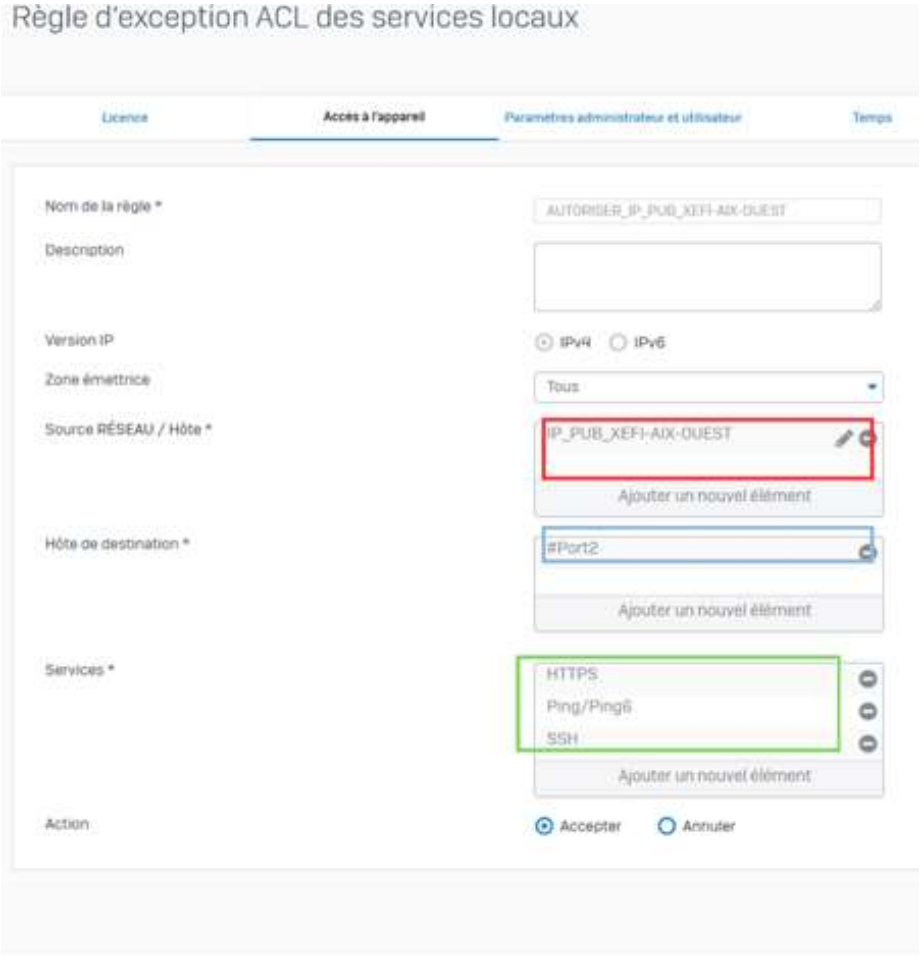
Configuration

Après avoir terminé la configuration de base (Création de mot de passe, connexion à internet, définition du fuseau horaire, définition de la plage DHCP, mises à jour), j'ai commencé à créer les premières règles.

Autorisations pour l'accès à distance

Les premières règles qu'il faut penser à créer sont des règles pour permettre l'accès à distance sur le Firewall. En effet, la configuration se fait en local mais il peut arriver qu'un technicien doit accéder au firewall à distance en cas d'incident.

C'est pour cela qu'une règle autorisant l'IP Publique de l'agence XEFI est créée comme ci-dessous:



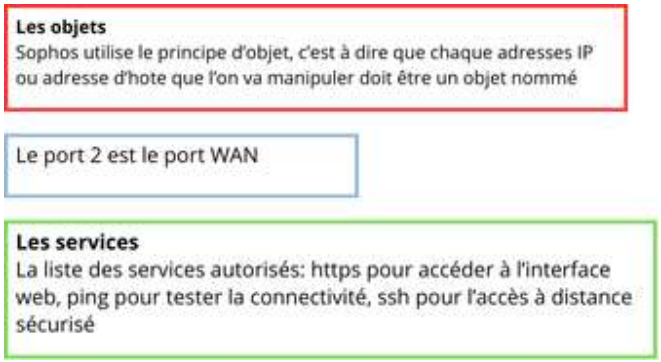


Figure 6: Explication création de règles

A noter que les règles d'accès à distance ne se font pas au même endroit que les règles de pare-feu classiques dont je vais parler plus tard.

Filtrage web

Pour le filtrage web, il y a plusieurs étapes à respecter.
La première est d'élaborer la stratégie dans la rubrique “Stratégies” de l’onglet “Web”
Chaque stratégie peut avoir plusieurs consignes. Les consignes sont l’autorisation ou le blocage de groupe d’URL. Comme dit précédemment ces groupes d’URL sont soit des groupes disponibles nativement sur le Firewall, soit des groupes d’URL personnalisés.
A noter qu’il n’est pas possible de voir le contenu des groupes d’URL natif mais l’ordre des consignes dans une stratégie est important. En effet, si un site est inaccessible car étant dans un groupe d’URL, il suffit d’inscrire cette URL dans une liste blanche que l’on placera en haut dans l’ordre des consignes. (**En annexe 01 une capture d’une stratégie web**)

La deuxième étape est d’utiliser la stratégie que l’on vient de créer dans une règle de pare-feu.

Pour créer notre règle, on doit définir une zone ainsi qu’un réseau d’origine. Dans ce cas, la zone émettrice est le port LAN, le réseau d’origine étant un objet contenant le réseau LAN.

On doit aussi définir une zone ainsi qu’un réseau de destination. Dans ce cas, la zone de destination est le port WAN et le réseau de destination est un objet contenant internet. Il faut aussi préciser les services utilisés. Notre règle concerne le filtrage web, les services concernés sont donc http et https. **(en annexe 02 l’interface pour la création des règles)**
C’est dans les options de la règle que je lie la stratégie web créée au préalable avec la règle de pare-feu.

Autres règles

Je viens de vous détailler la mise en place d’une règle web.
Les autres règles que j’ai dû mettre en place suivent le même principe car ce sont des règles “LAN TO WAN”. Les changements sont par rapport aux services autorisés (DNS, mail, ping…).
Comme je l’ai précisé plus haut, les firewall sophos utilisent le principe d’objet, même les services sont des objets avec un nom (généralement nom du service) et un port:

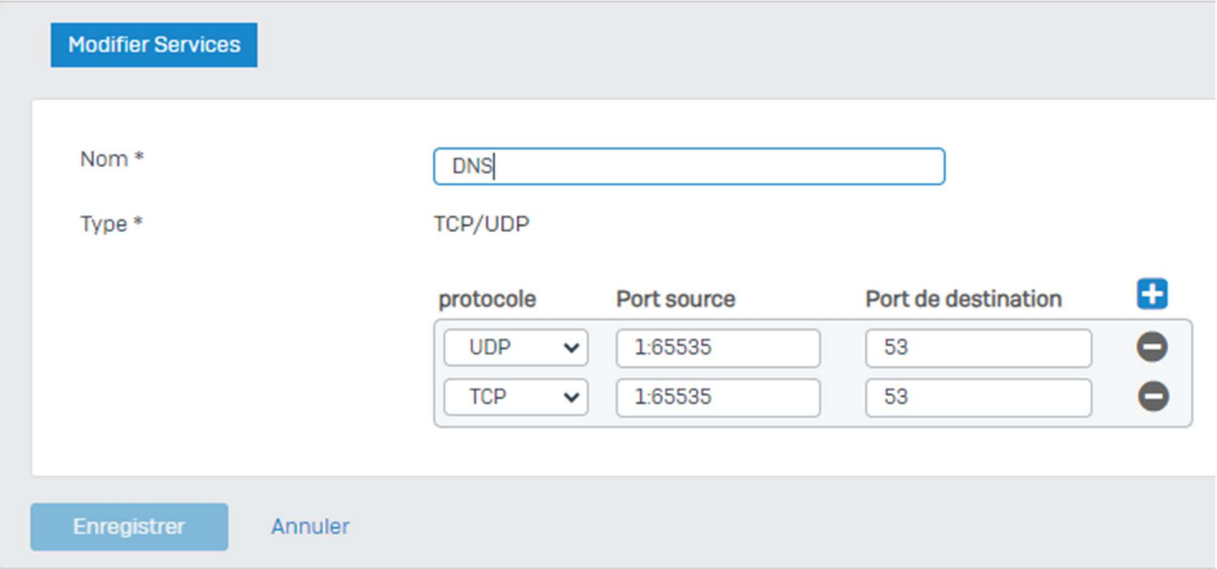


Figure 7: Création d'un objet service

A noter qu'une autre règle a dû être créée pour autoriser l'outil de prise en main ISL, il est en effet important de rappeler que tout ce qui n'est pas autorisé par le firewall est bloqué.

VPN site-à-site

Les avantages et objectifs d'un VPN site à site sont nombreux :

- Amélioration de la sécurité permettant le transfert de données entre deux sites dans un tunnel sécurisé de manière chiffrée
- La possibilité d'utiliser le même réseau local sur deux sites d'une entreprise
- En cas de panne ou de problèmes sur un site, les employés peuvent se connecter via un autre site du réseau VPN

Dans le cadre de mon stage j'ai donc dû mettre en place un VPN site-à-site (pour une autre entreprise et situation que la mise en place d'infrastructure pour le médecin mais je trouvais intéressant d'en parler). L'entreprise en question a deux sites différents en France et voulait étendre son réseau local, pour cela la mise en place d'un VPN site est la solution qui a été retenue.
XEFI proposait la solution suivante : Le montage d'un VPN entre chaque site et le Datacenter XEFI comme l'illustre le schéma suivant:

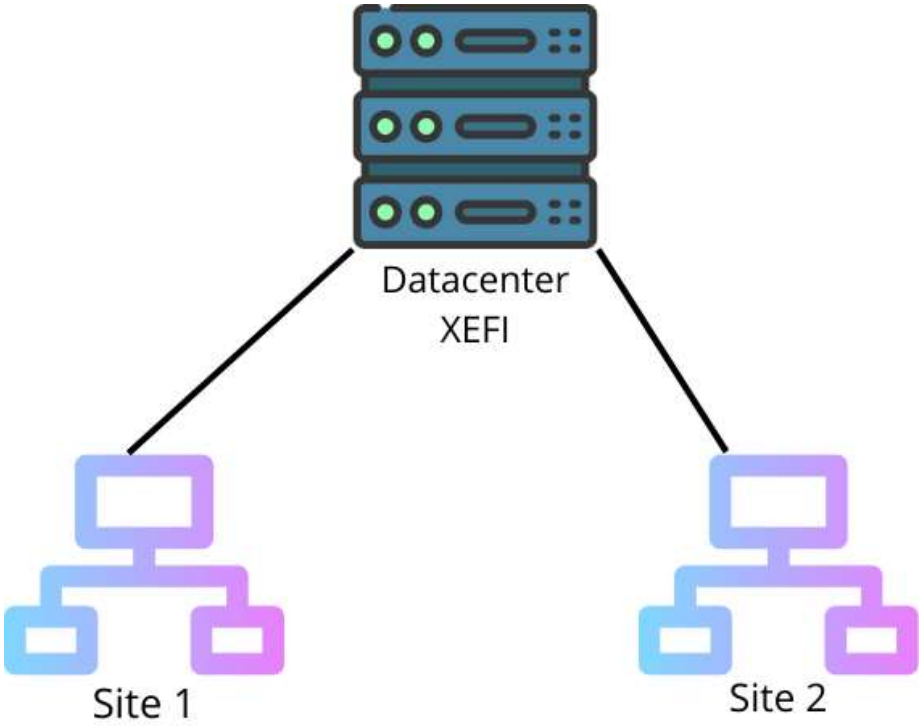


Figure 8: Schéma d'un vpn site-à-site

La configuration commence sur la plateforme XEFI:

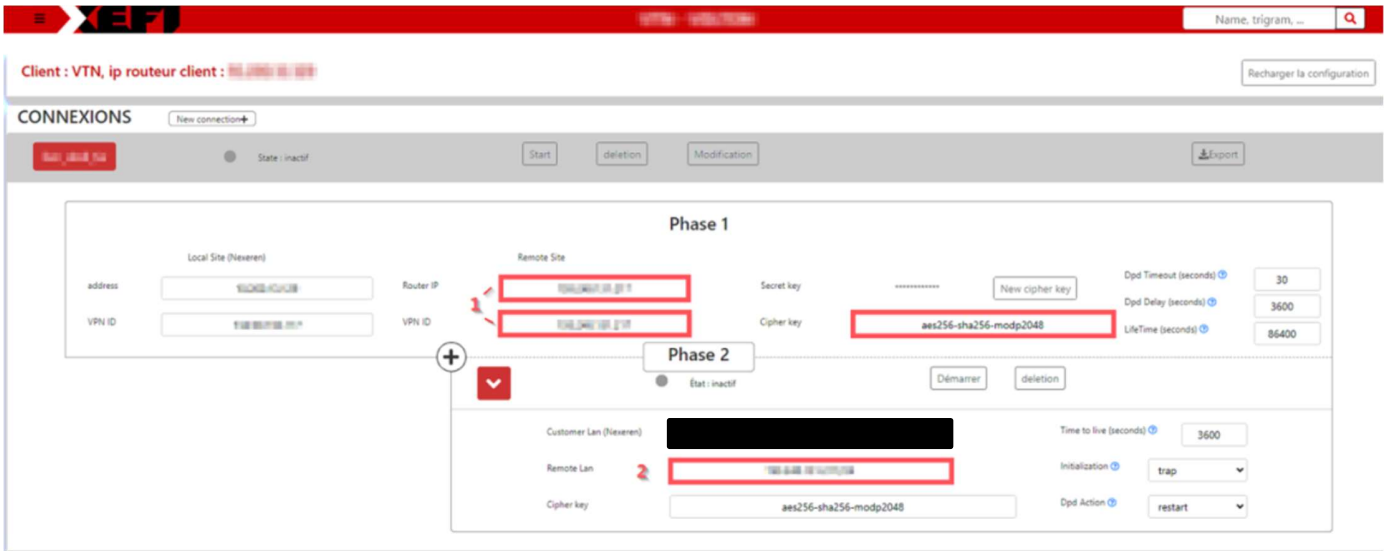


Figure 9: Configuration VPN sur la plateforme XEFI

Les cases importantes :
(1) “Remote site” représente l’IP public du firewall Sophos
aes256-sha256-modp2048 représente la suite de chiffrement utilisée pour le tunnel
(2) “Remote LAN” représente le LAN du client
“Secret key” sera important par la suite

On peut voir qu’il y a deux phases, la phase 1 sert à établir la sécurité du futur tunnel grâce à la suite de chiffrement aes256-sha256-modp2048
La phase 2 est l’établissement du tunnel sécurisé.

Côté Firewall,(**toute la configuration disponible en ANNEXE**) il faut créer un Profil IPSEC et renseigner la même suite de chiffrement que sur la plateforme XEFI et la “Secret key” qu’il y avait sur la plateforme XEFI.

Switch Aruba instant on 1930
La configuration de cet équipement a été très minimal étant donné les besoins du client qui était seulement d’étendre son domaine de diffusion.
Seul deux actions ont été effectuées : Établissement d’un serveur NTP et mises à jour.

Borne 4G Huawei
La configuration de cet équipement a aussi été très minime. En effet, cet équipement est vendu comme “plug and play”. La borne capte la 4G grâce à une carte SIM et un point d'accès est automatiquement remonté et détectable par les appareils aux alentours.
Le but de cet équipement est de fournir une connexion internet en cas de panne sur le Firewall.

Contact avec le fournisseur internet et le client

Avec le fournisseur internet

Pour pouvoir mettre en place le firewall, deux solutions s’offraient à nous, la première était de mettre en place une DMZ sur la boxe internet et la deuxième était de configurer la boxe internet en mode bridge. Dans les deux cas, l’objectif était que la box n’ait plus aucun rôle de filtrage, son seul rôle étant de fournir l'accès internet.

Pour prendre connaissance des possibilités, j’ai téléphoné à Orange en ayant préparé au préalable les informations client. Un technicien m’a dit qu’il n’était pas possible de faire une DMZ. Nous sommes donc partis sur la solution qui consiste à configurer la boxe en mode bridge.
Le technicien a pu me dire la démarche à suivre qui était d’acheter un pool d'adresses IP publiques (ce qui allait nous servir dans tous les cas).

Avec le client

Après avoir pris connaissance de ces informations, j'ai contacté le client afin qu'il puisse faire la démarche auprès d'Orange pour acheter le pool d'adresses IP publiques.
Je lui ai fait part du contenu de la conversation téléphonique avec le technicien d'Orange pour qu'il ait toutes les informations nécessaires.

L'installation

Après que le client ait fait les démarches nécessaires, un technicien d'Orange l'informe de la longueur de la procédure pour l'attribution du pool d'adresses IP (2 à 3 semaines) ce qui m'empêche de participer à l'installation physique étant donné que tant que la box n'est pas en mode bridge, nous ne pouvons pas installer le Firewall.

Suivi d'un incident "long"

Un chef d'agence web, client de XEFI, nous appelle pour un problème avec sa boîte mail, il ne peut plus l'ouvrir. Je prends donc la main grâce à l'outil ISL pour trouver des informations qui me permettraient de résoudre rapidement son problème. Lorsque je tente d'ouvrir sa boîte mail le message d'erreur suivant apparaît :

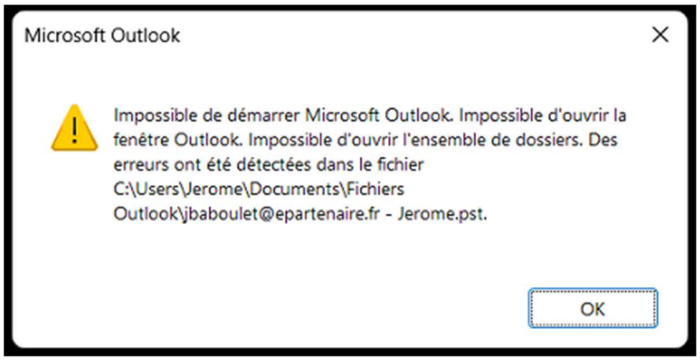


Figure 10 : Message d'erreur boite mail

Ce message m'a déjà permis de commencer à cibler l'origine du problème. Je vois qu'il s'agit d'un fichier PST (une fichier PST est un fichier de données qui contient des mails). La terminaison ".PST" m'indique que la boîte mail est une boîte mail de type POP ou IMAP.

Les trois types de boîtes mail

Pour bien comprendre l'origine du problème, il faut prendre connaissance des trois types de boîtes mail :

POP : Lorsqu'un client de messagerie (comme Outlook) utilise POP pour se connecter au serveur, il télécharge tous les e-mails dans la boîte de réception locale de l'utilisateur depuis le fichier PST.
Cela signifie que les e-mails ne sont accessibles que depuis l'ordinateur sur lequel ils ont été téléchargés, à moins que l'option de laisser une copie sur le serveur ne soit activée ou que le fichier PST soit conservé. Aussi l'état de la boîte de réception (dossier, affichage…) n'est pas synchronisé selon les ordinateurs.

IMAP : Contrairement à POP, IMAP stocke les e-mails sur le serveur et permet de synchroniser les messages entre plusieurs ordinateurs.
L'utilisation d'IMAP permet d'afficher une copie des e-mails sans les supprimer du serveur, ce qui permet à plusieurs dispositifs de voir le même état de la boîte de réception.

EXCHANGE : Exchange permet une synchronisation complète et en temps réel des e-mails, calendriers, contacts et tâches sur tous les appareils connectés avec l'adresse mail.
Ce type de boite mail permet aussi l'utilisation de fonctionnalités avancées de collaboration et de gestion (partage de calendriers, délégation d'accès, etc.).
Enfin exchange offre une sécurité renforcée avec des options de chiffrement et de contrôle d'accès.

En me renseignant auprès de l'équipe, j'ai su que le client avait une boîte mail en POP. En d'autres termes, cela signifie que tous ses mails sont stockés sur son ordinateur.
Il est important de noter que Outlook corrompt le fichier PST lorsque ce dernier dépasse 50 Go.
Je me suis rendu compte en allant chercher là où le fichier PST était censé être stocké que sa taille dépassait 50 Go. Il est donc corrompu (l'extension de fichier est renommé en .PST.corrupt).
Le problème final que cela génère est que Outlook ne trouve plus le fichier PST lié à l'adresse mail. C'est la cause du message d'erreur montré au début.

Maintenant que le problème est identifié, j'ai commencé à chercher des solutions, sachant que l'objectif était de réduire la taille du fichier.

Premières solutions n'ayant pas fonctionné

Grâce aux informations précédentes, j'ai conclu qu'il fallait trouver une solution pour réduire le volume du fichier PST.

En me renseignant auprès de l'équipe, j'ai tenter de tester deux solutions :

- Lancer une réparation avec l'exécutable SCANPST utilisé pour réparer un fichier PST.
- Utiliser une sauvegarde datant de quelques jours et supprimer manuellement quelques mails pour ensuite compresser le fichier.

SCANPST

Cet outil est un exécutable disponible nativement sur windows pour “réparer” un fichier PST.
Pour cela, le logiciel effectue les actions suivantes :

Reconstruction des liens brisés : Si des messages ne sont pas correctement liés à leurs dossiers respectifs, l'outil tente de reconstruire ces liens.
Correction des en-têtes : Les en-têtes de messages corrompus ou mal formés sont corrigés.
Suppression des données corrompues : Les parties irrécupérables ou gravement endommagées des données peuvent être supprimées pour permettre au reste du fichier de fonctionner correctement.
Reconstruction de l'index : Si l'index des messages est corrompu, scanPST.exe peut le reconstruire pour s'assurer que tous les messages sont accessibles.

Avant de procéder aux réparations, scanPST.exe crée une copie de sauvegarde du fichier d'origine. Cette copie est généralement nommée avec une extension .bak . Cela permet de restaurer le fichier d'origine en cas de problème pendant la réparation.

J’ai choisi cette solution en premier car elle est simple à mettre en place. Effectivement, il n’y a que le scan à lancer. Le désavantage de cette solution est que plus le fichier est lourd, plus le scan est long et que nous n’avons aucune certitude sur la réussite de la réparation. En effet, Ce scan a mis toute la journée pour s'effectuer sachant que le fichier PST qui posait problème pesait 50 Go.
J’ai donc pu retester à la fin de la journée et le message d’erreur montré au début du chapitre était toujours présent.

La réparation n’ayant pas fonctionné, j'ai dû me pencher sur d'autres solutions.

Exploitation d’une ancienne sauvegarde

Comme évoqué au début du rapport, XEFI propose des solutions de sauvegarde. Ce client ayant souscrit à ce service, nous avons donc récupéré son fichier PST non corrompu, le dernier avant la survenue de l’incident datant de plusieurs jours.
Nous avons en effet monté ce fichier sur un des PC de l’agence, pour faire des tests et avoir une vision sur la boîte mail.
L’objectif à ce moment était de réduire la taille du fichier PST d’au moins 10 Go pour le transférer sur le poste du client.

Ne pouvant pas prendre la responsabilité de supprimer des mails à la place du client, j'ai convenu avec lui pour qu'il se déplace à l'agence et supprime lui-même des mails ou crée des archives (Par chance les bureaux du clients se trouvaient à côté de l'agence).
Après avoir fait le ménage dans sa boite mail, je me suis rendu compte que la taille n'avait pas bougée. La taille du fichier n'avait pas réduit car sans une action manuelle pour le compresser, la taille du fichier ne rétrécit pas.
J'ai donc tenté de faire une compression manuelle. Malheureusement, cela n'a pas fonctionné. La taille du fichier n'était toujours pas réduite. De ce fait, le transfert du fichier sur le poste du client était impossible. J'ai donc dû me diriger vers une autre solution.

La solution finale pour résoudre le problème.

"Nettoyage"de la boîte aux lettres.
Après que les deux solutions précédentes aient échoué, j'ai tenté de rechercher d'autres possibilités, notamment sur le site microsoft.
J'ai donc trouvé la possibilité de "Nettoyer" la boîte mail grâce à une option Outlook

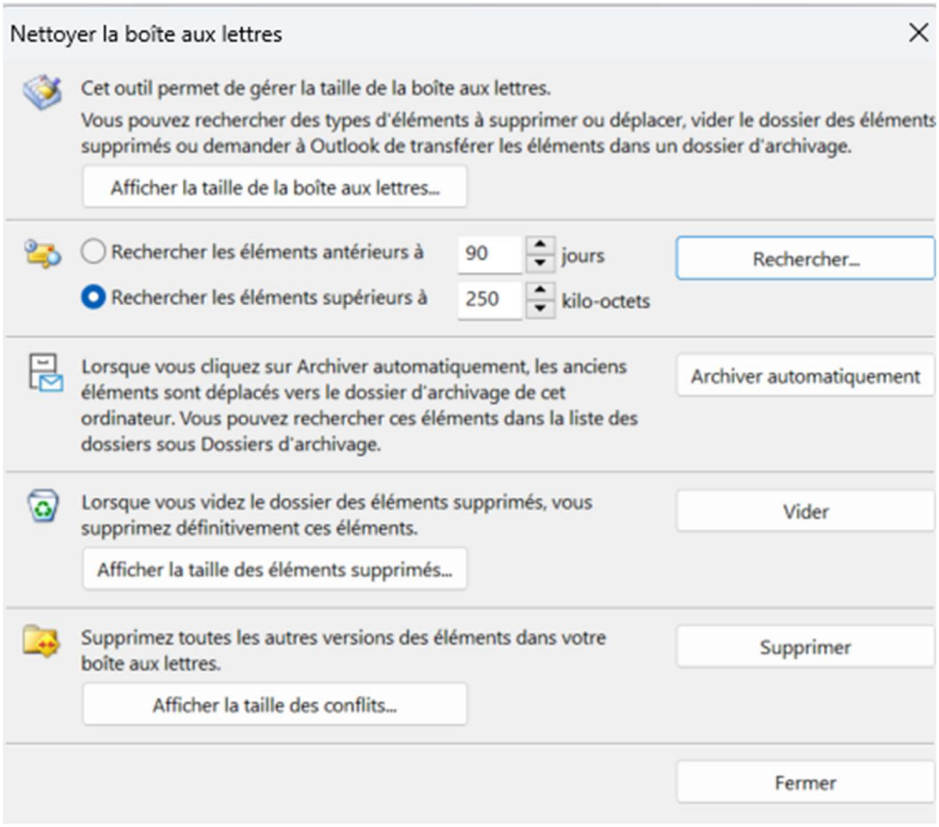


Figure 11: Paramètres pour le nettoyage de boite mail

Cette fonction permet aux utilisateurs de réduire la taille de leur boîte de réception en supprimant les messages redondants et en organisant les courriels de manière plus efficace.
L'inconvénient est aussi que ce processus a été lent à cause de la taille de la boîte mail.

Une fois le nettoyage effectué, j'ai une nouvelle fois compressé le fichier.
Cette opération terminée, j'ai bien constaté que la taille du fichier avait été réduite d'environ 20 Go. Les conditions étaient enfin réunies pour le transfert du fichier sur le poste du client.

Une fois le transfert effectué, le client a pu récupérer tous ses mails jusqu'à la dernière sauvegarde. L'inconvénient est que l'affichage auquel il était habitué n'a pas été sauvegardé et il a perdu quelques jours de mail.

Comment cet incident aurait pu être évité ?
Je rappelle que l'origine du problème est que le client avait son fichier de données Outlook stocké directement sur son poste et que ce fichier pesait plus de 50 Go.
Si le client avait créé des archives ou supprimé ses mails inutiles, son fichier n'aurait jamais atteint les 50 Go.
Des propositions d'évolution lui avait été faite auparavant, soit la migration vers une boîte mail exchange pour que les mails ne soit pas stockés directement sur ce poste mais sur les serveurs microsofts. Le client a souhaité jusqu'à présent rester sur le système actuel.

Contact avec le client

Cette expérience m'a permis d'appréhender les compétences relationnelles requises afin de gérer une situation stressante vécue par le client.
Il a fallu faire preuve de patience pour le rassurer, lui faire comprendre que tout était mis en œuvre pour un retour à la normal le plus vite possible et expliquer l'avancée des solutions mises en place. Ces désagréments informatiques sont une source d'énervement pour le client car de nos jours l'utilisation des mails est quotidienne. Il est difficile de s'en passer sans que cela ne génère une perte de temps et d'informations pouvant gêner le fonctionnement de l'entreprise de manière importante.
Je me suis efforcé de rester professionnel en gardant la tête froide et en persévérant dans la recherche de solutions malgré l'impatience du client et le fait qu'au début je ne maîtrisais pas tout.
Ma satisfaction a été d'aller chercher l'information qui me manquait dans une situation de stress.

Autres Tâches importantes

1. Configuration de postes (Procédure mise en place)
2. Intervention chez un client

Les deux missions que je viens de détailler ont été les plus formatrices. Toutefois, j'ai réalisé d'autres tâches moins longues et plus répétitives mais pas moins intéressantes.

Configuration de postes avec élaboration d’une procédure

Un des clients de l’agence est une entreprise qui embauche des médecins à travers toute la France pour des téléconsultations. Chaque fois qu'un médecin est embauché, un PC doit lui être configuré toujours de la même manière :

- Création de sa session
- Création de son compte google
- Création de son compte office et installation du pack office
- Installation de l’Antivirus
- Mise en place de l’outil de maintenance
- Mises à jour et nettoyage du poste

Pour mener à bien toutes ces tâches, j’ai mis en place une procédure partagée avec tous les membres de l’agence.

Pour le compte google et le compte microsoft, XEFI possède un compte avec les droits administrateurs, ce qui permet de créer, gérer et supprimer des comptes utilisateurs.
Le client envoie un mail à la partie commerciale de l’agence au préalable avec tous les prérequis pour l’ajout des comptes (noms des adresses mails, groupes…)
Dans le cas de cette entreprise, ce sont les outils google qui sont utilisés (mails, agenda, visio).
Le compte Microsoft est seulement utilisé pour le pack office.

Après la configuration, le médecin reçoit le PC et nous appelle pour que le fonctionnement du poste et l'écosystème de l’entreprise (mails, drive, fonctionnement des différentes applications) lui soient expliqués.

Intervention chez un client

Contexte de l'intervention

Dans le cadre de nos services de maintenance et d'optimisation des infrastructures informatiques, nous avons été sollicités par un hôtel, client de XEFI, pour remplacer un onduleur vieillissant. Cet onduleur était crucial car il assurait l'alimentation de secours pour le serveur principal, certains switchs (bien que tous ne pouvaient être connectés par manque de place) et le firewall. Au fil du temps, l'onduleur avait perdu en efficacité et ses ports disponibles n'étaient plus suffisants pour couvrir l'ensemble des équipements de l'hôtel.

Objectif de l'intervention

L'objectif principal de notre intervention était de remplacer l'onduleur défaillant par un modèle plus récent et mieux équipé: SMT3000RMI2UC - APC Smart-UPS (**Photo en Annexes 12**). Cette opération visait à garantir une alimentation de secours fiable pour l'ensemble des dispositifs essentiels, assurant ainsi la continuité des services informatiques de l'hôtel en cas de coupure de courant.

Planification et préparation

Afin de minimiser l'impact sur les activités de l'hôtel, nous avons planifié cette intervention avec soin. Il était impératif de procéder au remplacement de l'onduleur sans interruption de courant ou, si cela était inévitable, de limiter la coupure à une durée la plus courte possible. Cette contrainte demandait une coordination minutieuse et une préparation technique rigoureuse.

Déroulement de l'intervention

Le jour de l'intervention, nous étions deux techniciens présents sur le site. Cette double présence était nécessaire car l'onduleur à remplacer était lourd et son installation nécessitait la présence de deux personnes.

1. **Préparation du matériel :** Nous avons d'abord vérifié que le nouvel onduleur était pleinement opérationnel et compatible avec les équipements existants. Nous avons également préparé tous les outils nécessaires pour une installation rapide.
2. **Retrait de l'ancien onduleur :** Nous avons soigneusement déconnecté les équipements de l'ancien onduleur, en veillant à maintenir l'alimentation continue des dispositifs indispensables comme le serveur. Heureusement la plupart de ces équipements sont équipés d’une double alimentation.
3. **Installation du nouvel onduleur :** Une fois l'ancien onduleur retiré, nous avons installé le nouveau modèle. Nous avons connecté les équipements selon les priorités définies, en commençant par le serveur principal, suivi des switchs et du firewall.
4. **Tests et validation :** Après l'installation, nous avons effectué des tests complets pour nous assurer que le nouvel onduleur fonctionnait correctement et que tous les équipements recevaient une alimentation stable.

L'intervention s'est déroulée avec succès, sans interruption notable des services de l'hôtel. Grâce à la préparation minutieuse et à la coordination de l'équipe, nous avons pu remplacer l'onduleur de manière efficace et sécurisée. Le nouvel onduleur offre désormais une meilleure capacité et fiabilité, assurant ainsi la continuité des opérations informatiques de l'hôtel en cas de coupure de courant. (**photo de l'installation en annexe 13**)

Conclusion

Suivre les étapes de l'installation d'une infrastructure sécurisée m'a permis :

- D'observer le cheminement des différentes étapes de l'installation et saisir leurs utilités. J'ai aussi pu comprendre l'importance d'un Firewall au sein d'une entreprise et découvrir les possibilités d'un Firewall. Même s'il y a tellement de pistes à explorer que je n'ai pas pu, étant donnée la durée de mon stage tout voir et tout tester.
- De me donner une première expérience professionnelle avec les firewalls et en plus en découvrant un autre constructeur (ayant utilisé du sophos lors de mon stage et du Stormshiels lors du BUT. Cela m'a donc apporté un plus en termes de compétences.
- D'apprendre à corriger des erreurs, à les anticiper et à les contourner.
- D'avoir une première expérience dans le contact avec des clients notamment dans la réponse de ticket où dans la résolution de problèmes plus importants et plus stressants.
- J'ai pu donc pu vivre une première expérience dans une entreprise informatique et voir plusieurs aspects entre la résolution d'incidents et la proposition de solutions. Le monde du travail est complètement différent de l'école et il important de savoir s'adapter en entreprise.

Ce stage m'a permis de développer des compétences dans le domaine des réseaux notamment sur l'aspect sécurité. Je suis maintenant capable de mettre en place une infrastructure réseau sécurisée pour une petite entreprise. Ce stage m'a aussi permis de savoir où me diriger en cas d'incidents majeurs.

Ce stage m'a confirmé que le domaine des réseaux est celui qui me correspond le mieux. Cela m'a conforté dans mon choix d'orientation, soit devenir ingénieur réseau/systeme.