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

MISE EN PLACE DE L'ANTIVIRUS ET DU NOUVEAU RESEAU

Eloïse BOCCHNO

SPIE Industrie

Responsable entreprise : Christophe WINCKLER

Responsable académique : Sébastien SANCHEZ

2024

Table des matières

1 Introduction

Mon stage s’est effectué à Aix-en-Provence dans la société SPIE Industrie, filiale de la société SPIE, Société Parisienne pour l’Industrie Électrique. J’ai travaillé au sein du service MCS soit la Cybersécurité.

L’objectif du stage consistait à la création et à la mise à jour de l’antivirus, des équipements réseau, et des serveurs, ainsi que la gestion de l'Active Directory et des services NTP. Elles incluaient également le bilan des correctifs via WSUS offline et la rédaction de procédures, avec un check et redémarrage de la solution ELK.

Ces missions se concentrent sur deux domaines, le réseau, avec la création d’un switch pour rectifier leur architecture réseau, la création et mise à jour du pare-feu ainsi que la création de GPO. Le second domaine est la cybersécurité, avec la création et la mise à jour d’antivirus, la sécurisation des mots de passe ainsi que de la création et modification des supports visuels.

2 SPIE Industrie, l'excellence pour maintenir l'exigence

2.1 Présentation Générale

En 1900, le baron Edouard Empain, industriel belge obtient la concession des travaux d'infrastructures électriques du Métro de Paris. Il crée à cet effet la Société Parisienne pour l'Industrie des Chemins de Fer et des Tramways Électriques qui sera connue sous le nom de SPIE. Cette société s'est développée dans l'alimentation électrique des réseaux ferrés, puis dans la production et la distribution d'électricité.

Nationalisée en 1946, avec ses activités d'électricité et de canalisation, SPIE se spécialise dans les équipements électriques des centrales nucléaires et en 1967, les activités pétrolières et gazières en France et en Afrique du Nord vont lui permettre d'accroître son chiffre d'affaires de près de 30 fois en 20 ans.

La société SPIE est devenue leader européen des services multi-techniques dans les domaines de l'énergie et des communications.

Figure 1 : Chiffres clés 2023

SPIE est présent dans 5 pays et a à présent 6 filiales dont SPIE Industrie créée en janvier 2023.

Cette filiale a de nombreux clients mais son client le plus important est un fournisseur d'énergie. Une plateforme lui est dédiée pour l'accompagner dans son réseau numérique, utilisant les outils spécifiques du fournisseur. SPIE lui fournit un service de maintenance corrective (MCO) qui inclue le patching soit la mise à jour des logiciels et est en communication permanente avec eux.

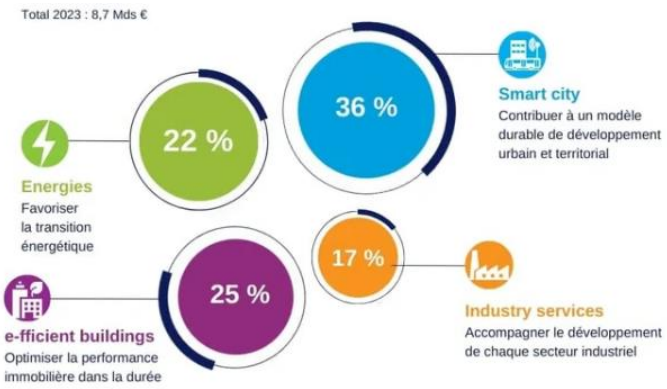


Figure 2 : 4 Marchés stratégiques

Les principales valeurs de SPIE sont la proximité, la performance, la responsabilité au cœur de notre culture d'entreprise.

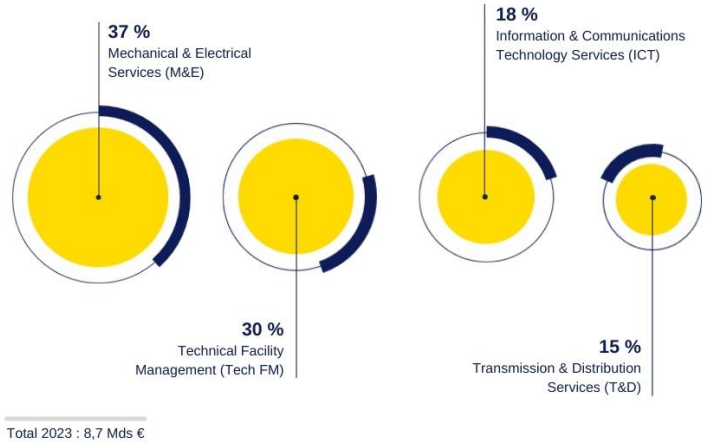


Figure 3 : Les 4 domaines d'excellence 2023

2.2 Présentation du service

Le service Cybersécurité est composé de 10 personnes dont mon tuteur, Christophe Winckler, qui est responsable d'activités informatiques et de cybersécurité et Valentin Olive, mon responsable, chef de projet cybersécurité.

Le service est composé de trois équipes, SUSIE, Système unifié de supervision et d'information d'exploitation, MESURAGE et MCS, Maintien en condition de sécurité. Les deux premières équipes effectuent principalement de la supervision, du déploiement, des automates et des calculatrices. J'ai donc effectué mon stage au sein de l'équipe cybersécurité, MCS.

Le MCO, Maintien en Condition Opérationnelle, utilisé par toutes les équipes est en liaison constante avec les clients pour effectuer du Patching donc des mises à jour pour le MCS et effectue des missions d'aide et de dépannage pour les clients.

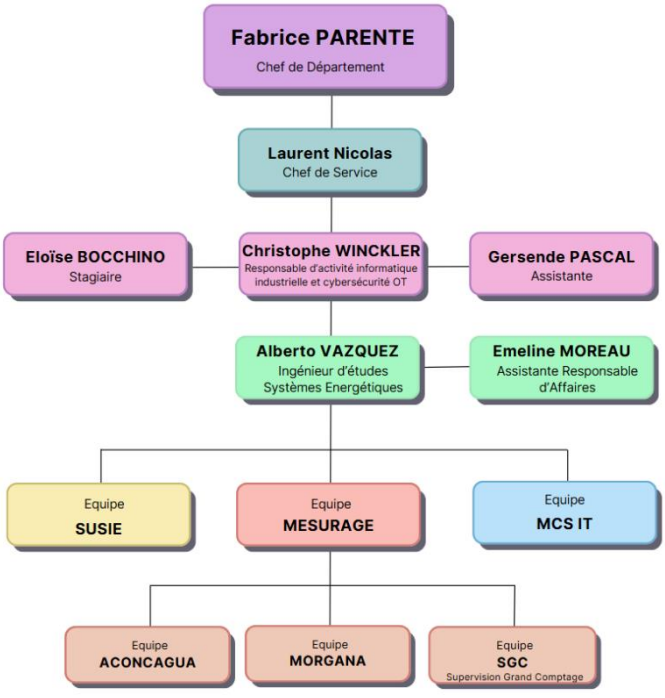


Figure 4 : Organigramme

2.3 Objectif du stage

L'objectif du stage est en priorité de mettre leur réseau à jour dans un premier temps, puis de créer un antivirus et d'effectuer sa mise à jour hebdomadaire. Une fois ces tâches achevées, je dois procéder à des correctifs, notamment au niveau de leur connexion. La liste des missions qui m'ont été confiées n'est pas exhaustive et certaines tâches m'ont été demandées par la suite, comme déverrouiller des sessions avec un mot de passe perdu, l'Active Directory et écrire des procédures.

3 Architecture Réseau

3.1 Configuration du switch

À mon arrivée, des câbles Ethernet étaient déjà mis en place. Il fallait donc faire une tête à chaque câble, soit joindre le câble à un connecteur RJ45.
3 câbles étaient tirés, un pour SPIE et les 2 autres pour des clients. J'ai donc relié les câbles aux connecteurs, en plaçant chaque câble dans les emplacements spécifiques du connecteur, selon les couleurs.

J'ai donc dénudé les câbles, puis j'ai mis les câbles dans les connecteurs RJ45 et j'ai pincé, ce qui permettait de trouer les câbles, afin de réussir la connexion.
Chaque extrémité de câble a été testée deux par deux afin de vérifier si toutes les broches fonctionnaient. Le test étant positif, j'ai fait un ping.

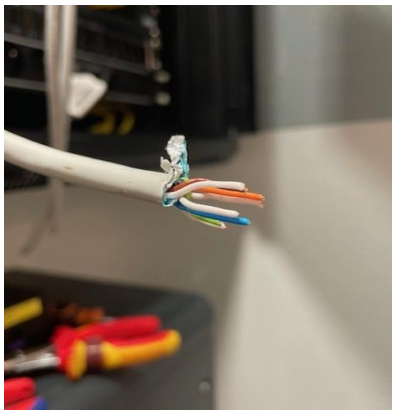


Figure 5 : Câble

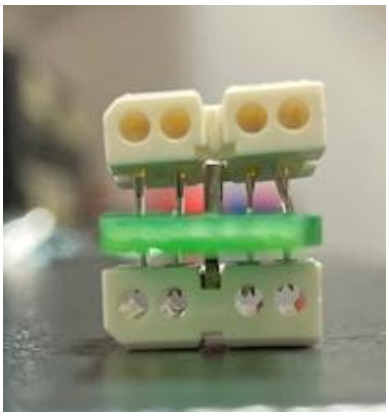


Figure 6 : Connecteur RJ45

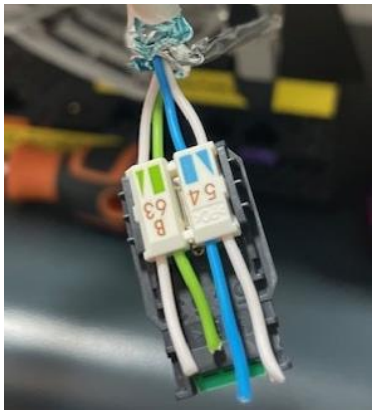
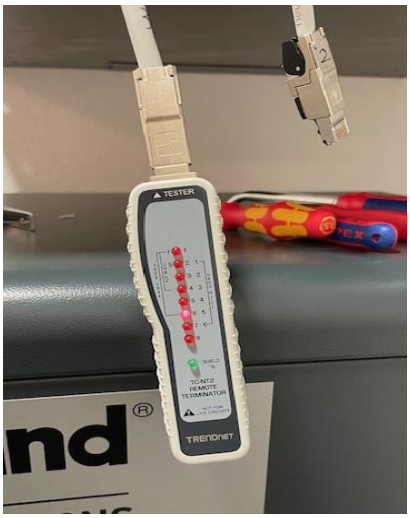


Figure 7 : Connexion par couleur

Lors du test, il faut brancher chaque extrémité du câble sur chacun des boîtiers testeurs de câble réseau. Chaque led sur les boitiers correspond à une broche.

Si c'est un câble droit, les deux leds de même niveau s'allument simultanément alors que si le câble est croisé, la première led sur le premier testeur s'allumera en même temps que la dernière led sur le second testeur.



Figures 8 et 9 : Testeurs de câbles réseaux

Auparavant, notre infrastructure réseau comprenait un switch Netgear qui commençait à être obsolète. Pour harmoniser notre parc de switchs et moderniser notre équipement, il a été décidé de le remplacer par un nouveau switch Aruba, identique à ceux déjà mis en place.

À la suite de cette mise à jour, j'ai entrepris une série de tâches pour assurer une transition fluide et efficace. Tout d'abord, j'ai dû changer temporairement la carte réseau de mon ordinateur afin d'accéder à l'interface web du nouveau switch, dont l'adresse IP était définie par défaut.
Une fois l'accès obtenu, j'ai créé un compte administrateur et attribué une nouvelle adresse IP au switch pour l'intégrer correctement à notre réseau. Cette opération a nécessité de faire un changement de l'adresse IP sur la carte réseau de mon ordinateur pour correspondre aux nouveaux paramètres du switch.

Ensuite, j'ai procédé à la configuration complète du switch Aruba. J'ai réglé l'horloge du switch pour synchroniser avec notre réseau (NTP), puis j'ai créé plusieurs VLANs pour segmenter le trafic. Le 1er VLAN a été configuré pour l'administration, tandis que les autres VLANs ont été créés pour les clients. Le 2ème VLAN a été assigné au câble Ethernet correspondant et le 3ème VLAN au câble Ethernet concordant. À chacun de ces VLANs, j'ai attribué des interfaces spécifiques pour garantir une gestion efficace du trafic réseau.

Après la configuration des VLANs, j'ai été chargée de tester chaque port du switch pour m'assurer qu'il obtenait la bonne adresse réseau en fonction du VLAN assigné. Pour ce faire, j'ai utilisé les commandes « ipconfig /release » et « ipconfig /renew » sur mon PC connecté aux différents ports. Ces tests ont permis de valider que chaque port était correctement configuré et que les adresses IP étaient correctement distribuées.

Pour assurer une connectivité fluide entre les différents équipements, il a fallu que je trouve un port libre sur le Switch de niveau 3 pour le relier au nouveau switch de niveau 2. J'ai ensuite effectué des tests de ping pour vérifier la correspondance et la communication entre les deux switchs. Des tests supplémentaires ont été réalisés pour s'assurer que la configuration fonctionnait correctement pour les différents postes du réseau.

Lors de l'analyse de l'ancienne configuration, j'ai remarqué que tous les ports de la salle MCO étaient configurés en mirroring, ce qui consommait inutilement de la bande passante. J'ai donc décidé de ne pas activer le mirroring sur le nouveau switch Aruba, afin d'augmenter le débit réseau.

Dans le cadre de la mise à jour et de l'optimisation de notre infrastructure réseau, il a été essentiel de procéder à une analyse approfondie de chaque port pour déterminer à quelle salle et à quel PC il correspondait.

Cette étape préliminaire a été cruciale pour garantir une transition fluide vers le nouveau switch Aruba. Une fois cette analyse terminée, j'ai entrepris le nouveau câblage.

Pour améliorer l'organisation et la gestion des câbles dans la baie de brassage, j'ai procédé à un câble management rigoureux. Cela consiste à l'identification des ports ayant accès à Internet dans la salle plateforme et l'annotation précise de ces informations tant dans la baie de brassage qu'au-dessus de chaque prise RJ45 de la plateforme.
Cette démarche vise à faciliter l'identification sur place et à éviter toute confusion future.

Par ailleurs, j'ai identifié les trois câbles réseau principaux pour savoir leur rôle spécifique et déterminer le PC administratif, garantissant ainsi une organisation optimale des câbles.

Parallèlement, il a été nécessaire de créer de nouvelles règles sur notre pare-feu Stormshield pour intégrer efficacement le nouveau switch dans notre infrastructure. J'ai rencontré un problème de connexion sur mon PC, ce qui m'a empêché d'accéder initialement au pare-feu.

Après avoir tenté diverses méthodes pour diagnostiquer la cause de cette interruption sans succès, j'ai finalement résolu le problème en redémarrant simplement la carte réseau. Cette action a rétabli la bonne configuration, me permettant d'accéder à l'interface graphique du pare-feu Stormshield. J'ai alors pu créer les règles nécessaires pour autoriser le flux de la nouvelle adresse IP.

Dans la salle cybersécurité, nous disposons de prises RJ45 distinctes pour le réseau client et celui des administrateurs. J'ai dû intervertir ces prises dans la baie ainsi que les câbles reliés à mon PC afin de maintenir une connexion stable. De plus, j'ai annoté au-dessus des prises pour indiquer clairement à quel réseau elles correspondaient. Ensuite, j'ai branché le pare-feu Stormshield au commutateur de niveau 3, assurant ainsi une connexion sécurisée et efficace.

Afin d'optimiser notre réseau, j'ai également retiré les box MCO et ADSL inutilisées. Cette action a permis de simplifier notre infrastructure et d'améliorer les performances globales du réseau.
Enfin, j'ai mis à jour les schémas Visio représentant l'architecture du réseau ainsi que le tableau Excel sur l’inventaire.
Cette mise à jour a impliqué la suppression des box obsolètes (MCO et ADSL), l'ajout de nouvelles prises Ethernet et l'intégration du nouveau switch avec ses connexions actualisées. Grâce à la documentation précise et mise à jour, la maintenance et les futures modifications de notre infrastructure réseau seront plus accessibles.

En somme, cette série d'actions et de modifications a non seulement permis de moderniser notre infrastructure réseau, mais a également renforcé sa sécurité, sa fiabilité et son efficacité, en veillant à maintenir une documentation précise et une organisation claire pour faciliter la compréhension du réseau à l'avenir.

Chaque étape, de l'analyse initiale des ports à la mise à jour des schémas Visio, a été réalisées avec précision pour avoir une bonne transition afin de ne pas affecter les divers services.

3.2 Firewall

L'une de mes premières missions a été de travailler sur le firewall.

J'ai commencé par effectuer une sauvegarde du firewall Fortinet. J'ai donc allumé le firewall, l'ai connecté au PC avec un câble console Fortinet et recherché sur le gestionnaire de périphériques sur quel COM se trouvait-il. Il m'a fallu ensuite lancer PuTTY, un émulateur de terminal me permettant d'accéder à l'invite de commande entre le PC et le firewall. Après avoir cliqué sur « Open » pour lancer la console, j'ai pu brancher la clé USB sur le firewall.
Il convient d'ouvrir la console et de faire « Enter ». On peut alors saisir le login et le password fournis. Le « # » en fin de commande m'a confirmé le mode administrateur.

Pour accélérer les commandes, il est possible d'écrire le début du mot puis de cliquer sur « Tab ». Lors de mon cursus, j'ai appris à rechercher les champs d'aide dans les commandes, avec le point d'interrogation.

À la fin de chaque commande, il suffit de mettre un « ? » et apparaît alors écrites toutes les situations possibles.

Pour effectuer une copie complète du firewall, c'est-à-dire créer une sauvegarde du fichier de configuration complète, y compris la configuration utilisateur et la configuration par défaut, la commande est celle-ci :

```
FortiGate-61F # execute backup full-config usb full_fw.conf
Please wait...

Copy config full_fw.conf to USB disk ...
Copy config file to USB disk OK.
```

Figure 10 : Commande de sauvegarde complète

Pour effectuer une copie du pare-feu, soit la sauvegarde de la configuration spécifiée par l'utilisateur sur un fichier texte, il est possible d'utiliser cette commande :

```
FortiGate-61F # execute backup config usb fw.conf
```

Figure 11 : Commande de sauvegarde spécifique

Une fois la sauvegarde effectuée, un contrôle sur la clé USB de la présence d'un fichier texte ou apparaît la configuration est conseillé.
J'ai noté chaque étape de la sauvegarde sur un document afin de créer une note de procédure.

La seconde étape consistait à nettoyer le firewall Stormshield à la suite de la suppression des box ADSL et MCO. En effet des objets réseaux et des objets machines existant dans le pare-feu étaient devenus inutiles. Certaines règles de filtrage pour ADSL étaient également présentes.
Grâce à ma certification Stormshield, acquise lors de ma 2ème année, j'avais déjà une idée des règles utilisées.

La dernière étape fut la mise à jour du pare-feu Stormshield.
Mon tuteur m'a communiqué une procédure existante chez SPIE. En suivant les instructions, j'ai noté le n° de série du pare-feu. Sur MyStormshield.eu, je suis allée dans les téléchargements pour télécharger la version du firmware désirée. Le fichier à télécharger a une extension « .maj ». Je suis allée ensuite sur un navigateur web, n'ayant pas d'accès internet.

Après connexion avec son adresse IP et indiqué le numéro d'identifiant et le mot de passe, il convient d'aller sur l'interface d'administration du firewall, de sélectionner le fichier de mise à jour dans la section maintenance puis de cliquer sur « mise à jour » pour effectuer l'installation.

3.3 Nas et Active Directory

Les ordinateurs de l'entreprise SPIE avaient initialement accès aux partages du NAS (Stockage en Réseau Attaché). Toutefois, il devenait impératif de restreindre cet accès pour des raisons de sécurité et de gestion.
Par conséquent, j'ai été chargé de mettre en place un PC en libre-service, accessible à tous les employés pour remplacer cet accès direct. Pour ce faire, j'ai commencé par rechercher une tour inutilisée ainsi qu'un écran, un clavier et une souris adéquats.

Ensuite, j'ai procédé à une analyse complète de la machine en question, en vérifiant sa puissance, sa capacité RAM, son espace de stockage et d'autres spécifications techniques essentielles. Après avoir déterminé que le PC répondait aux besoins requis, j'ai entrepris une remise à zéro du système pour m'assurer qu'il soit prêt pour une utilisation optimale et sécurisée.

Le projet incluait également la connexion de ce PC à l'Active Directory de l'entreprise.

Bien que l'Active Directory soit déjà présent avec un domaine et une Unité Organisationnelle (OU) créée, il n'était pas encore utilisé de manière optimale. Mon objectif était donc de structurer l'Active Directory en créant un utilisateur pour chaque employé de l'entreprise, en suivant le format "p.nom" pour les noms d'utilisateur comme vu en cours. Chaque employé s'est vu attribuer un mot de passe commun, qu'il sera obligé de changer lors de sa première connexion pour des raisons de sécurité.

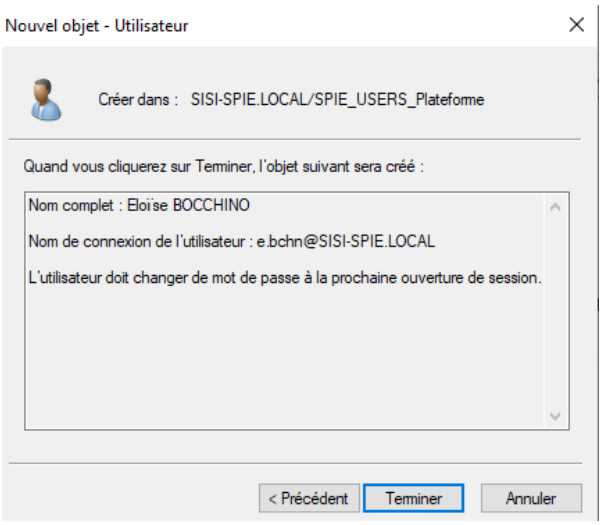


Figure 12 : Création d'un utilisateur

Par la suite, j'ai créé plusieurs GPO (Group Policy Objects) pour assurer une gestion cohérente et sécurisée de l'environnement utilisateur et de gérer efficacement les configurations système, les paramètres de sécurité et les accès au réseau au sein d'un domaine.

Lors de mes différents cours à l'IUT, nous avons vu que les GPO se créent dans la gestion de stratégie de groupe, une fois la stratégie créée et liée à l'OU il a fallu l'éditer.
Les quatre GPO principales mises en place comprenaient :

- **Fond d'écran commun** : J'ai configuré un fond d'écran standard pour toutes les sessions utilisateur, empêchant ainsi toute modification personnelle.

- **Extinction automatique** : Une GPO pour éteindre automatiquement les PC à 19h, garantissant que les machines ne restent pas inutilisées et allumées après les heures de travail.

- **Verrouillage de session** : Pour des raisons de sécurité, une GPO a été mise en place pour verrouiller la session utilisateur après 10 minutes d'inactivité.

- **Mapping réseau du NAS** : Un script relié à une GPO pour mapper automatiquement le réseau du NAS sur chaque session utilisateur, facilitant l'accès aux ressources nécessaires.

Enfin, j'ai dû relier l'Active Directory au NAS. Cette configuration permettrait une gestion centralisée des accès et des permissions, améliorant ainsi la sécurité et l'efficacité de l'administration réseau.

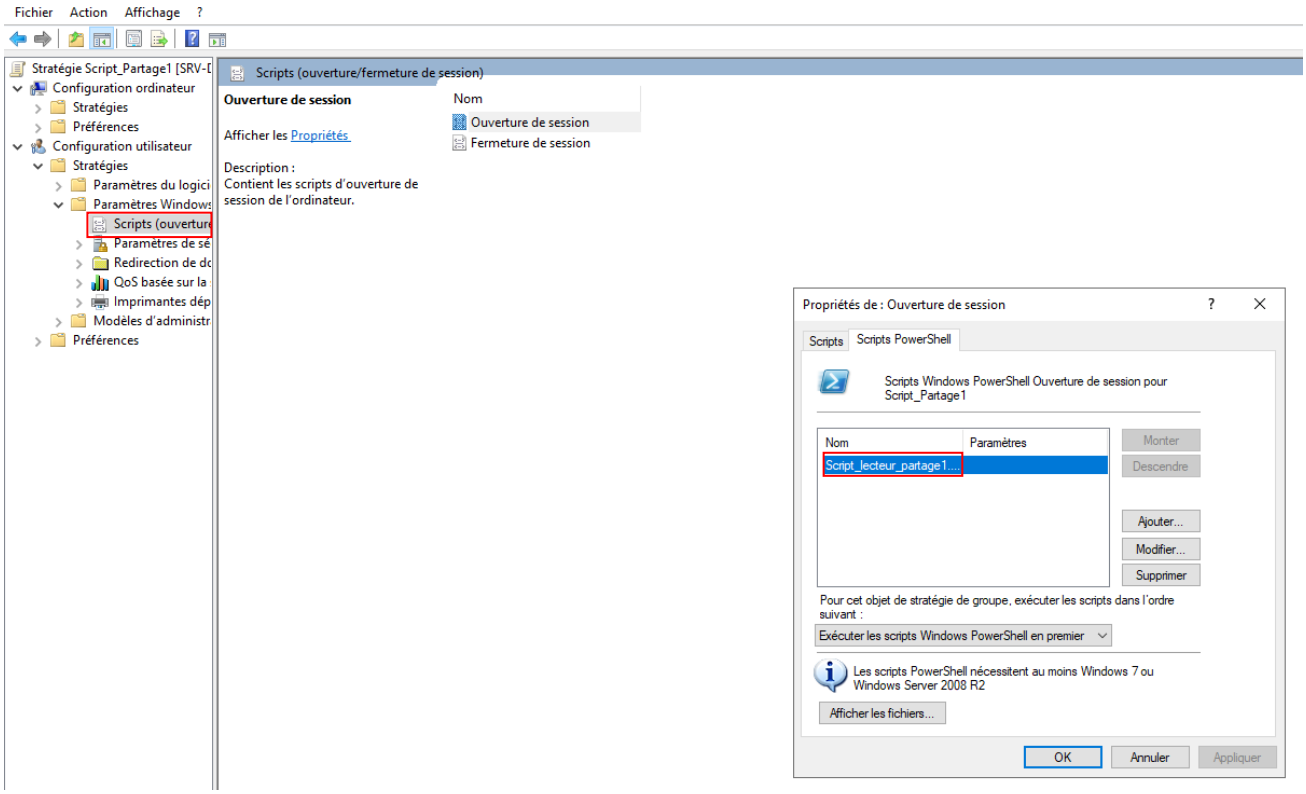


Figure 13 : Mappage réseau du NAS

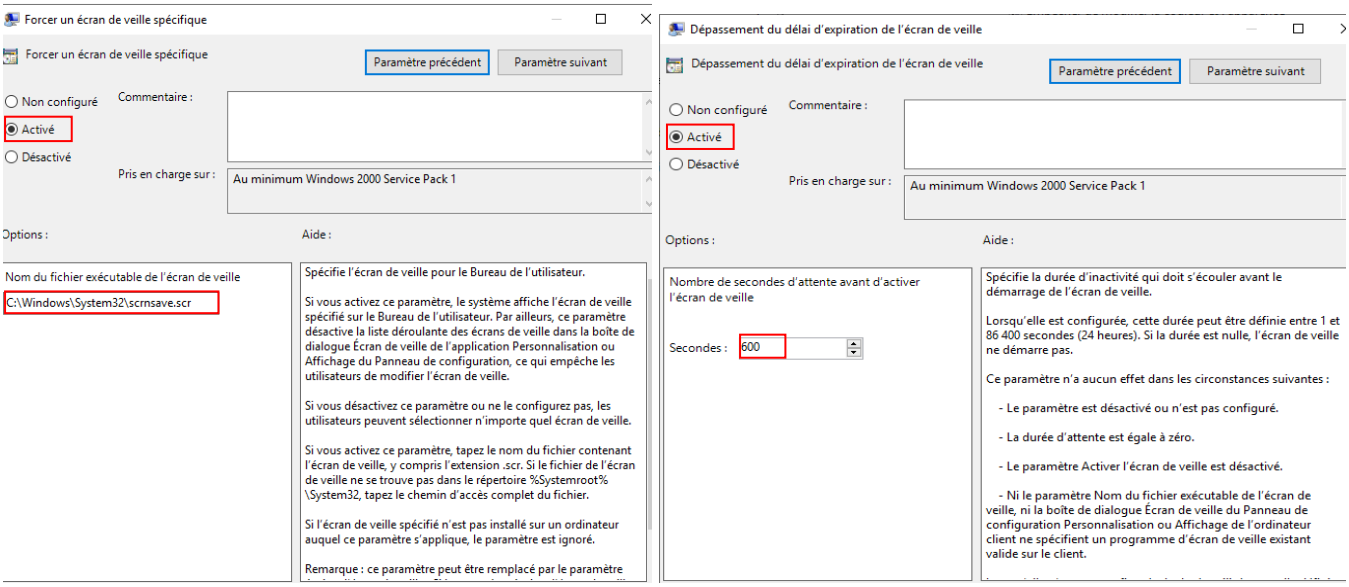


Figure 14 : Session verrouillage 10 minutes

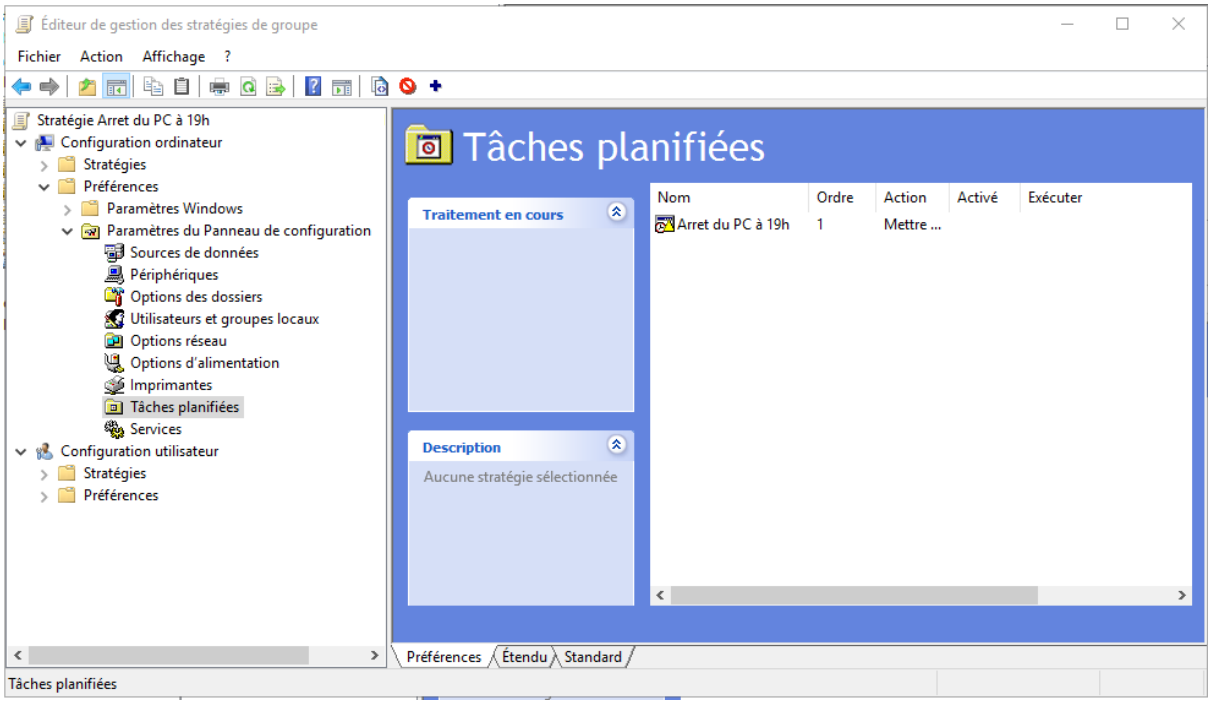


Figure 15 : Arrêt du PC à 19h

3.4 Missions transverses

3.4.1 Le câble management

Une de mes missions a été de faire du câble management et de remplacer un Hub par un Switch.
Le câble management est « l'organisation et la gestion des câbles et des cordons dans un environnement informatique ou électronique ».
J'ai branché le Switch cependant celui-ci faisant trop de bruit pour le personnel, j'ai dû l'enlever et remettre le Hub qui était déjà présent.

Il s’agissait donc pour moi de regrouper tous les câbles de manière ordonnée et de les attacher pour les placer correctement sous les bureaux dans le boîtier de rangement adapté, afin de les sécuriser.
Cela évite les enchevêtrements et les accidents. Le câble management est nécessaire pour un environnement de travail propre, une meilleure maintenance des équipements et pour faciliter les dépannages.
J’ai effectué cette mission dans une salle MCO, « Maintien en condition opérationnelle ». Il s’agit d’une salle dédiée au patching du client, soit effectuer des mises à jour pour le client et aux appels téléphoniques en cas de besoin.

C’est d’ailleurs dans une salle MCO que j’ai dû trouver des prises ou des connecteurs RJ45, qui sont utilisés pour les câbles Ethernet. Il fallait trouver où étaient les connecteurs pour savoir où ils sont reliés dans la baie de brassage.

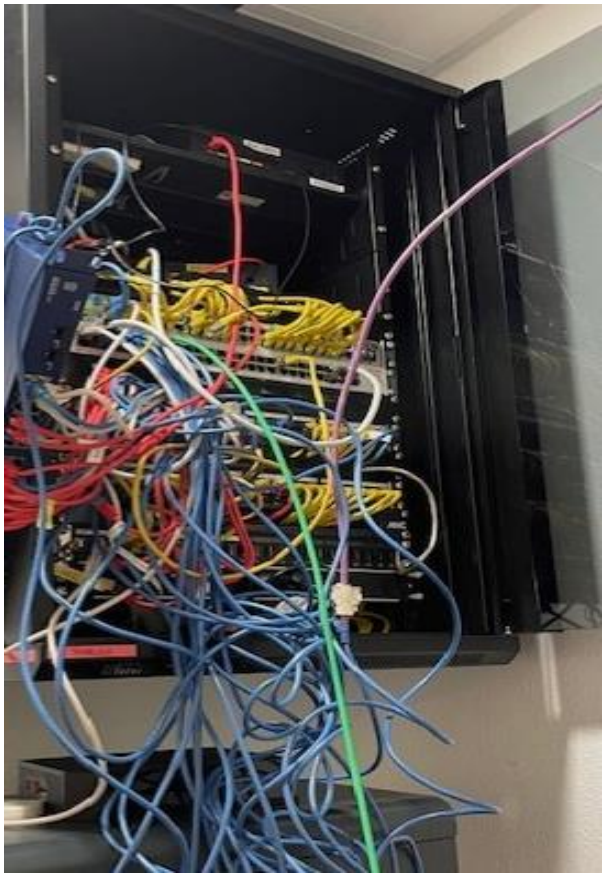


Figure 16 : Tests de configuration

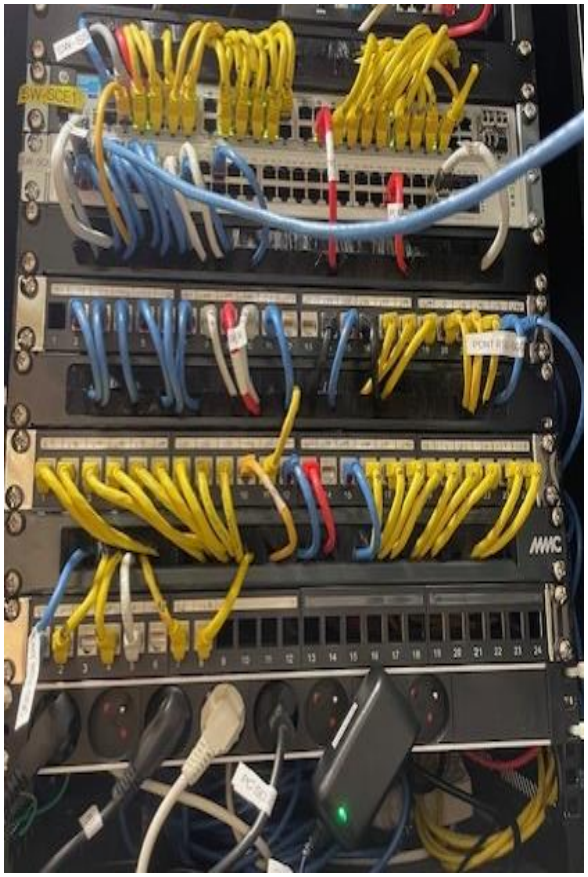


Figure 17 : Câble management du switch dans la baie

3.4.2 Linux

À la suite d’un changement de réseau, un de mes collègues a dû modifier l'adresse IP de sa machine virtuelle. Après avoir effectué les modifications nécessaires, il a constaté qu'il n'avait plus accès à Internet. Pour résoudre ce problème, nous avons entrepris une analyse approfondie de la configuration réseau de sa machine.

Notre investigation a révélé qu'il avait configuré un masque de réseau incorrect, utilisant /16 au lieu de /24. Après avoir analysé la situation, me rappelant ce que j’ai appris lors mon cursus, j'ai supposé que l'erreur provenait d'une saisie incorrecte de la commande « mask 255.255.255.0 » au lieu de « netmask 255.255.255.0 » dans le fichier /etc/network/interfaces.

J'ai alors corrigé ce fichier de configuration en ajustant le masque de réseau à /24. Malgré cette correction, l'accès à Internet n'était toujours pas rétabli. J'ai donc entrepris des recherches supplémentaires dans différents fichiers de configuration pour identifier la cause sous-jacente du problème.
J'ai vérifié les routes réseau en utilisant la commande « ip route » pour m'assurer que les chemins étaient correctement définis. J'ai également vérifié l'état de l'interface réseau pour voir si elle était active (« up ») ou inactive (« down »), ainsi que la passerelle par défaut à l'aide de la commande « ip route | grep default ».
Ensuite, j'ai examiné les paramètres DNS « Domain Name System », dans le fichier /etc/resolv.conf pour m'assurer qu'ils étaient correctement configurés. J'ai ajouté la ligne « nameserver 8.8.8.8 » dans ce fichier pour garantir que les requêtes DNS seraient résolues correctement.

Pour finir, j'ai redémarré le système avec la commande « systemctl reboot » et vérifié l'état des services réseau en utilisant la commande « systemctl status networking ». Cette vérification a confirmé que tout était correctement configuré. Après ces interventions, l'accès à Internet a été rétabli pour mon collègue, résolvant ainsi le problème de manière définitive. Il a alors pu faire les mises à jour de la machine virtuelle SURVI.

4 La cybersécurité

4.1 Création et mise à jour d'antivirus

Pour améliorer la sécurité de notre infrastructure, nous avons migré notre antivirus depuis un serveur Windows 2008 en RU4 vers Windows 2022 en RU6.
Cette mise à jour était essentielle étant donné la nécessité croissante de renforcer nos défenses contre les menaces informatiques. L'antivirus doit désormais être mis à jour chaque lundi pour garantir une protection optimale.

Pour héberger notre nouveau serveur de l'antivirus, choisi car leader sur le marché de solution de gestion de la sécurité, j'ai créé une machine virtuelle sur ESXi en local.
J'ai minutieusement installé Windows 2022 et ajusté divers paramètres tels que le nom de la machine, son adresse IP, les spécifications du processeur et les mots de passe pour optimiser ses performances. Utilisant l'accès Bureau à distance via l'adresse IP du serveur, j'ai facilité la gestion quotidienne du système.

Après avoir configuré l'environnement, j'ai installé la dernière version disponible de l'antivirus exploité, soigneusement choisie pour ses capacités de protection avancées. Pour sécuriser la machine, j'ai dû configurer manuellement toutes les règles du pare-feu et définir des exceptions spécifiques pour chaque groupe d'utilisateurs.

La création du package client s'est avérée être une étape critique, où j'ai dû choisir entre un fichier d'installation .exe complet et un package .msi nécessitant des fichiers externes. J'ai désactivé complètement la Politique Web et Cloud, conformément aux recommandations de sécurité, tout en intégrant le serveur de l'antivirus dans notre Active Directory et le retirant du DHCP « Dynamic Host Configuration Protocol » pour une gestion plus centralisée et sécurisée.
Sur chaque poste client, j'ai procédé à la désinstallation des versions précédentes de l'antivirus via le Panneau de configuration, ou en utilisant un outil de nettoyage spécialisé si nécessaire, avant de redémarrer chaque machine pour finaliser la transition.

Quant au NAS Synology, il joue un rôle crucial en tant que dispositif de stockage réseau permettant la centralisation, la gestion et la sécurisation des données, à la manière d'un dossier partagé accessible via une adresse IP dédiée.

J'ai configuré un dossier spécifique sur le NAS pour le logiciel de la société vendant le produit, incluant sa dernière version en .exe ainsi que l'outil de nettoyage.

Après avoir lancé et vérifié l'installation sur chaque ordinateur client, j'ai utilisé Angry IP Scanner pour auditer l'ensemble du réseau actif, assurant ainsi la mise à jour complète de chaque adresse IP et maintenant une documentation précise à jour dans un fichier Excel.

Pour assurer une sécurité continue, j'ai également dû ajuster les règles du pare-feu pour permettre exclusivement l'accès depuis l'adresse IP spécifique de notre serveur de l'antivirus, renforçant ainsi notre posture de sécurité globale.

Certaines fonctionnalités ne pouvaient pas être exploitées à la suite de mauvaises configurations de règles de firewall sur l'antivirus. Une fois les configurations modifiées, l'équipe exploitant l'antivirus a effectué des tests de bon fonctionnement mais également des tests de non-régression.

Ci-dessous, se trouve la liste des postes clients accompagnés de leur nom et adresse ip :

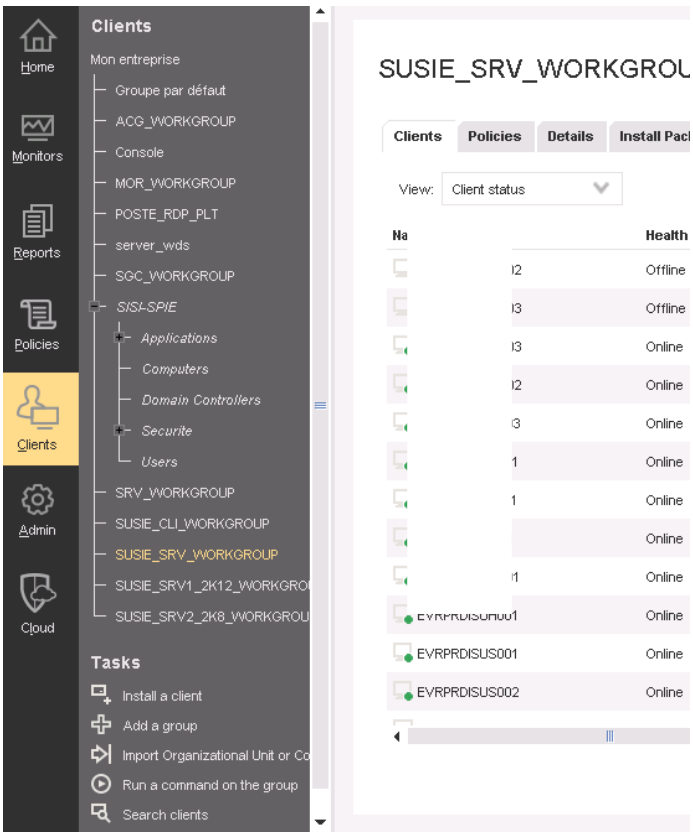


Figure 18 : Groupes de clients

Chaque groupe a ses propres exceptions, elles permettent de spécifier des fichiers ou des extensions de fichiers devant être exclus des analyses antivirus.

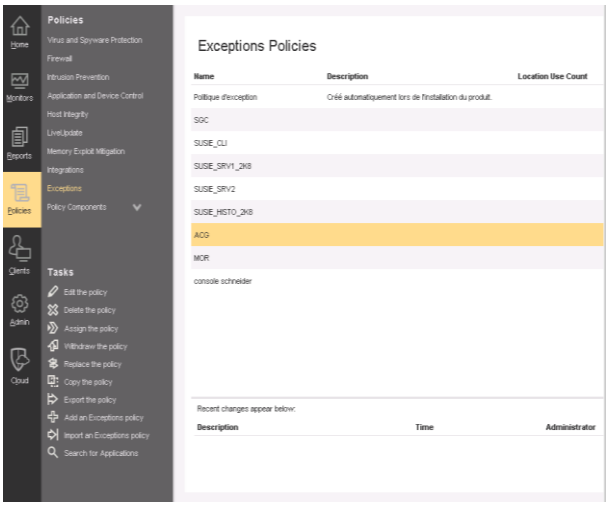


Figure 19 : Menu des exceptions

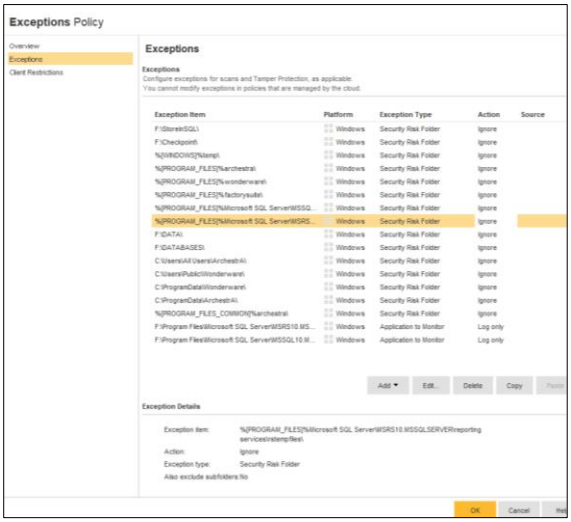


Figure 20 : Exemples d'exceptions

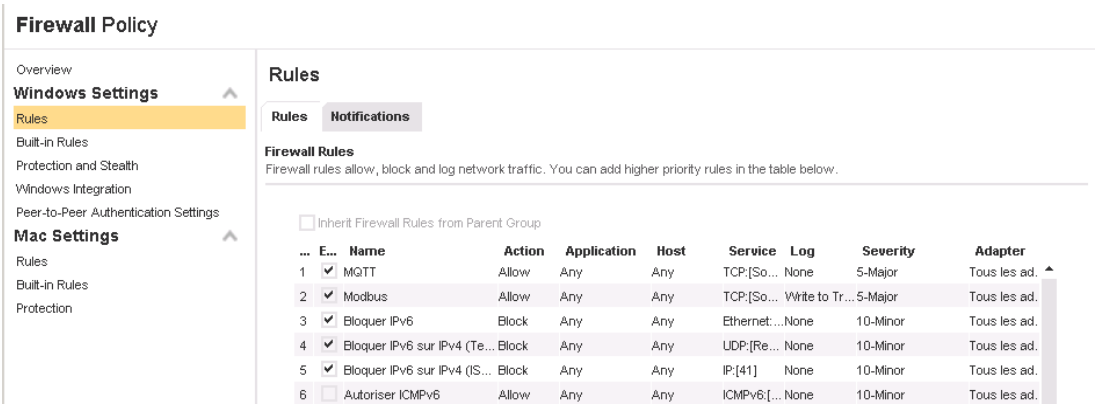


Figure 21 : Règles de firewall

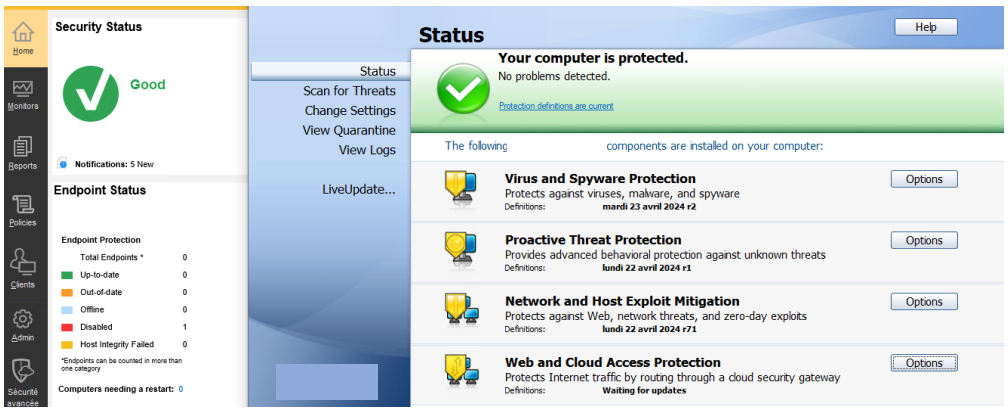


Figure 22 : Vérification de l'antivirus à jour

Sur cette tâche, j'ai rencontré un problème.

Après la mise en place, ma machine virtuelle s'éteignait sans cesse. À la suite de recherches dans les Log et autres, j'ai trouvé qu'elle s'éteignait parce qu'il y avait un problème de licence Windows qui avait expiré.

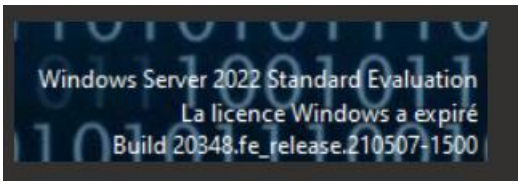


Figure 23 : Licence Windows expirée

Avec mon tuteur, nous avons recommandé une nouvelle licence. Mais cette nouvelle licence a été réceptionnée par erreur par la DSI de SPIE, qui a refusé de nous la rendre, alors qu'elle était budgétisée sur le service de Cybersécurité.
Après plusieurs semaines, une solution m'est apparue pour contourner le problème.

J'ai trouvé un site qui, à l'aide de quelques lignes de commande, permet de réactiver la licence Windows pour 10 jours. Cette démarche peut être effectuée plusieurs fois de suite.

Voici les commandes et ce qu'elle renvoie :

C:\Users\Administrateur>slmgr -dlv

Figure 24 : Nombres restants

C:\Users\Administrateur>slmgr -rearm

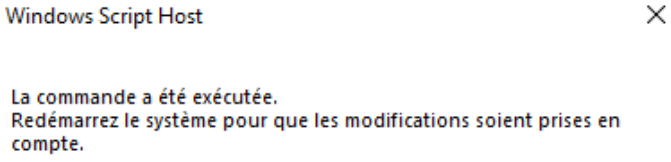


Figure 25 : Commande exécutée

C:\Users\Administrateur>slmgr -dli

Figure 26 : Temps restant

4.2 SURVI Supervision des équipements.

J'ai eu l'opportunité de travailler sur le développement de l'application web SURVI, un outil innovant conçu par SPIE.
SURVI a été spécialement développé pour garantir un suivi précis et efficace des alertes relatives aux vulnérabilités des produits utilisés par les clients. Ces produits sont organisés en profils clients, ce qui permet une gestion plus ciblée et personnalisée des alertes de sécurité.

Nous pouvons importer les failles manuellement dans l'application. Ce double système de récupération d'informations nous permet de ne rien laisser passer et d'assurer une surveillance continue et exhaustive des vulnérabilités potentielles.

Une fois toutes ces informations collectées et analysées, nous sommes en mesure de générer une liste de correctifs spécifiques pour les produits en fonction des vulnérabilités précédemment identifiées. Cela garantit que chaque produit est toujours à jour et protégé contre les menaces les plus récentes.

En ce qui concerne la gestion des données, le fichier Excel était déjà créé, j'ai donc dû faire des modifications pour organiser ces informations contient plusieurs colonnes essentielles :

1. **Identifiant** : Chaque vulnérabilité est répertoriée dans la base de données CVE (Common Vulnerabilities and Exposures) accessible par tous. Cela permet d'identifier une vulnérabilité.

2. **Score CVSS** : Le score CVSS (Common Vulnerability Scoring System) est une mesure standardisée de la gravité d'une vulnérabilité. Un score élevé indique que la vulnérabilité est critique et nécessite une attention immédiate.

   Des scores de vulnérabilité, supérieurs à 7 sur l'échelle du CVSS, indiquent des failles critiques qui peuvent représenter des risques significatifs pour la sécurité. Par conséquent, il est crucial de mettre à jour le firmware afin de protéger le matériel contre d'éventuelles exploitations de ces vulnérabilités.

3. **Vecteur CVSS** : Le vecteur CVSS fournit une description détaillée des caractéristiques spécifiques de la vulnérabilité qui ont été utilisées pour calculer le score CVSS. Il décompose la vulnérabilité en différentes composantes.

4.3 La sonde CISCO

La machine virtuelle (VM) de la sonde Cisco sert également à analyser les CVE (Common Vulnerabilities and Exposures) sur le réseau et le flux d'activité du réseau. Pour ce faire, il est nécessaire de créer un port mirroring. Je me suis donc connectée au switch de niveau 3, afin de configurer ce port mirroring.

Voici les étapes que j'ai suivies :
Je me suis connecté au switch via SSH et j'ai sélectionné le port 2, sachant qu'il était libre.
En mode configuration, j'ai saisi les commandes suivantes :
« mirror-port 2 »: pour désigner le port 2 comme port de mirroring.
J'ai spécifié les ports à surveiller, c'est-à-dire tous les ports sauf le port 2 : « interface 1 »
J'ai ensuite activé la surveillance avec la commande « monitor ».
Le port 2 était configuré pour être présent sur tous les VLANs.

Pour effectuer la surveillance, j'ai connecté un câble réseau au port 2 et un autre câble relié à un autre appareil. Mon PC était ainsi relié au réseau via deux câbles Ethernet, ce qui me permettait de capturer l'activité réseau.
Cependant, il a également été nécessaire de modifier la configuration réseau. Malgré mes efforts, cette tâche n'a pas abouti. Avec l'aide de mes coéquipiers, nous n'avons pas encore identifié la cause de ce problème.

4.4 Sécurisation des mots de passe

4.4.1 Réinitialisation de mots de passe

Ma première tâche en arrivant dans la société a été de déverrouiller une session d'ordinateur et de réinitialiser un mot de passe car un des collaborateurs ne se souvenait plus du sien. J'ai téléchargé le logiciel Lazesoft depuis leur site et l'ai configuré.

Ce logiciel permet de booter une clé USB, mais il faut être prudent car la clé, comme pour un formatage, est vidée de ses données. Cela n'a pas été mon cas car la clé était neuve.

Une clé USB bootable permet l'ouverture d'une session depuis cette clé et non depuis Windows.

Lors du redémarrage de l'ordinateur, j'ai appuyé sur la touche F12, qui permet d'accéder au menu du boot et ainsi accéder au compte de l'utilisateur impliqué pour supprimer tout mot de passe.
Un « ctrl + maj + suppr » permet ensuite de mettre un nouveau mot de passe.

4.4.2 BitLocker des clés

Lors de mon arrivée, j'ai compris que la sécurité des données est primordiale chez SPIE, l'utilisation de Bitlocker pour chiffrer les clés USB permet de garantir la confidentialité et la protection des informations sensibles. Toutes les clés USB sont chiffrées avec Bitlocker, il est donc impératif d'utiliser une clé protégée pour accéder aux données.

J'ai donc dû apprendre à utiliser Bitlocker pour sécuriser ma clé USB et ainsi pouvoir travailler.

Pour chiffrer ma clé USB, j'ai inséré une clé neuve dans l'ordinateur et j'ai suivi la procédure en faisant un clic droit dans le répertoire où est indiqué "Lecteur USB". J'ai ensuite choisi le mode de verrouillage par mot de passe, en créant un mot de passe complexe comprenant des majuscules, des minuscules, des chiffres et des symboles, avec un minimum de 12 caractères.
Une clé de récupération a alors été générée en cas de perte du mot de passe. Il est essentiel de conserver cette clé en lieu sûr, en la sauvegardant ou en l'imprimant.

Il est également possible de choisir entre le chiffrement de l'espace utilisé dans la clé ou de chiffrer l'intégralité du lecteur, cette dernière option prenant davantage de temps.

Le mode de chiffrement compatible permet d'accéder à la clé sur des versions antérieures de Windows, puis il suffit de lancer le chiffrement. Une fois ce processus terminé, j'ai procédé à un test en éjectant puis en réinsérant ma clé, et j'ai pu constater que le chiffrement avait été correctement effectué.

5 Les supports visuels

5.1 Les affiches

Le KUB sert à faire tester sa clé USB pour vérifier si elle est saine ou non. Les clés doivent être testées régulièrement et surtout avant d'aller sur le site d'un client. La station va analyser la clé.

Le résultat de l'analyse apparaît sur la station, mais également crée un fichier sur la clé et envoie un mail au service cybersécurité. Si la clé n'est pas saine, il convient d'aller impérativement auprès de l'équipe de cybersécurité.

Figure 27 : Méthode d'utilisation du Kub

J’ai également fait cette affiche ci-dessous pour l’appliquer sur la porte des baies de brassage, ou il y a également des compteurs électriques.

Figure 28 : Affiche de mise en garde

En amont, de la visite de certains clients, j’ai utilisé une borne non exploitée en temps normal, pour mettre un message de bienvenue pour nos clients. Cette tâche m’a été demandée personnellement car la borne se programme sous Linux.

J’ai donc mis le PowerPoint sur la borne pour que le message s’affiche, mais la borne ayant un écran tactile, plusieurs employés n’ont pu s’empêcher de toucher l’écran. J’ai donc dû refaire plusieurs fois la manipulation pour qu’à l’heure dite, le message de bienvenue soit prêt.

Figure 29 : Message de bienvenue sous Linux

5.2 Les procédures

Les procédures sont essentielles pour organiser le processus de création ou de mise à jour d'un outil ou d'un antivirus. Elles permettent de définir les étapes à suivre de façon claire et structurée. Celles-ci sont donc réalisées de la même manière à chaque fois, ce qui permet de garantir la cohérence et la qualité du produit final.
En suivant les procédures, chaque collaborateur sait ce qu'il doit faire et comment le faire et les nouveaux venus peuvent comprendre plus rapidement les processus de mise à jour.

La présence de procédures établies favorise l'optimisation du processus de création ou de mise à jour. Cela permet d'améliorer l'efficacité du travail et de gagner du temps.

Écrire des procédures faisait partie de mes missions. J'ai donc écrit la procédure de mise à jour de l'antivirus, celle concernant le NAS et la sauvegarde du Firewall.

Le détail de ces trois procédures figure dans l'annexe.

6 Conclusion

Ce stage m'a offert une opportunité d'appliquer mes connaissances théoriques acquises lors de mon cursus universitaire, de développer mes aptitudes et surtout d'acquérir de nouvelles compétences spécifiques, tant en réseau qu'en cybersécurité. J'ai également pu renforcer mes capacités d'analyse et de résolution de problèmes en faisant face à des situations complexes et en trouvant des solutions adaptées.
La gestion autonome de projets ambitieux gérés dans leur intégralité, m'a permis de développer ma confiance et mon efficacité.

J'ai vécu une expérience très enrichissante, ou la notion de culture d'entreprise a pris tout son sens mais surtout j'ai compris que le travail d'équipe, la collaboration et la communication sont essentiels dans le monde de l'informatique. L'ambiance positive et l'équipe sympathique chez SPIE ont renforcé ma motivation et mon désir de poursuivre dans ce domaine.

Je garderai un excellent souvenir de cette expérience enrichissante et j'espère avoir l'opportunité de travailler dans une équipe aussi dynamique à l'avenir.

7 Remerciements

Je tiens à remercier les équipes de SPIE Industrie, d'Aix la Duranne pour leur accueil au sein du groupe.

Je tiens à remercier Christophe Winckler, responsable d'activité pour m'avoir accordée sa confiance et permis d'effectuer mon stage dans cette société.

Je remercie tout particulièrement Valentin Olive, pour son accompagnement tout au long du stage. Son partage d'expériences et ses conseils me seront précieux pour mon avenir professionnel.

Mes remerciements vont également à toutes les personnes avec qui j'ai collaboré dans l'entreprise, à Dylan pour son aide, à Paul et à Sabri pour leur bienveillance à mon égard.

Enfin, je souhaite remercier l'ensemble du corps enseignant de l'IUT R&T de Luminy, pour la délivrance de leurs enseignements qui m'ont permis d'avoir les compétences nécessaires au bon déroulement de ce stage.

8 Glossaire

Active Directory
Service d'annuaire informatique développé par Microsoft, qui permet de stocker des informations relatives aux ressources et aux utilisateurs d'un réseau informatique.

Baie de brassage
Armoire technique où sont connectés les câbles de différents appareils réseau pour simplifier la gestion et la distribution des connexions réseau.

Connecteur RJ45
Utilisé principalement pour les câbles Ethernet dans les réseaux informatiques. Il permet de connecter des appareils comme des ordinateurs, des routeurs et des switchs pour la transmission de données à haut débit.

CVE
Identifiants uniques attribués à des vulnérabilités informatiques spécifiques. Les CVE sont utilisés pour identifier et suivre les vulnérabilités informatiques et sont largement utilisés dans les bases de données de vulnérabilités pour aider les organisations à gérer et à corriger les failles de sécurité de leurs systèmes informatiques.

DHCP
Protocole réseau qui assure la configuration IP automatique des clients dans un réseau.

DNS
Service informatique distribué qui associe les noms de domaine Internet avec leurs adresses IP

ESXI
Un système d'exploitation de type hyperviseur développé par VMware, utilisé pour la virtualisation des serveurs.

Firewall
Système de sécurité qui limite le trafic entrant et sortant à l'intérieur d'un réseau privé.

Firmware
Programme intégré dans un matériel informatique pour lui permettre de fonctionner.

Mirroring
Permet d'analyser le trafic réseau provenant de plusieurs ports et de le rediriger vers un port de surveillance spécifique.

Ping
Commande réseau utilisée pour tester la connectivité entre deux appareils en envoyant des paquets de données et en mesurant le temps de réponse.

Switch
Commutateur réseau permettant l'interconnexion d'appareils communicants tels que des ordinateurs.

Tests de non-régression
Type de test utilisé en développement logiciel pour vérifier si des modifications apportées à un logiciel n'ont pas introduit de nouveaux bugs ou n'ont pas altéré le comportement existant du logiciel.

VLAN « Virtual LAN »
Réseau informatique logique indépendant

9 Sitographie

Société SPIE Industrie
https://www.spie.com/fr/spie-industrie

GPO - Déployer un fond d'écran Windows en 10 minutes :
https://www.bing.com/videos/riverview/relatedvideo?q=comment+crrer+une+gpo+qui+mettrer+le+meme+fond+d%27ecran+peut+importe+la+session&mid=DED7CD45ED78089AF5C6DED7CD45ED78089AF5C6&FORM=VIRE

GPO : configurer le verrouillage automatique des sessions :
https://rdr-it.io/gpo-configurer-le-verrouillage-automatique-des-sessions/

GPO planification automatique de l'arrêt des postes:
Comment planifier un arrêt automatique de Windows par GPO ? (it-connect.fr)

Windows Server 2016/2019 : étendre la période d'évaluation:
https://www.it-connect.fr/windows-server-2016-2019-etendre-la-periode-devaluation/

Configuration port mirroring:
https://www.arubanetworks.com/techdocs/AOS-S/16.10/MCG/YAYB/content/common%20files/cnf-sou-swi-loc-mir-ses.htm