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

Administrateur des systèmes réseaux

Yanis ROUAINIA

Effective Yellow

Responsable entreprise : Frédéric VILANOVA

Responsable académique : Ivan MADJAROV

2023

Table des matières

1 Présentation de l'entreprise

1.1 *Historique*

Effective Yellow, fondée en 2014, est une entreprise dont le siège social est établi à Martigues. Composée d'une équipe d'environ dix experts, elle compte également deux collaborateurs permanents sur son site de Gardanne, où j'ai réalisé mon stage. L'entreprise s'investit activement dans diverses associations telles que ESCP Business School, ISACA, et IFACI.

1.2 *Activités*

Effective Yellow est une entreprise spécialisée dans la cybersécurité, dédiée à apporter sérénité et lucidité aux dirigeants à travers une gouvernance et un management expertisés.
Elle offre un large éventail de compétences, incluant l'expertise en tests d'intrusion (Pentesting), l'accompagnement en conformité RGPD, et la restructuration des fonctions d'audit interne.

L'entreprise développe également des solutions logicielles qui aident les organisations à gagner en maturité et en autonomie sur des sujets complexes. Leurs activités se répartissent en quatre axes principaux : accompagner, comprendre, conseiller et concevoir.

1.3 Missions

Lors de ce stage, j'ai effectué plusieurs type de missions.
Tout d'abord, je devais mettre en place un réseau wifi pour le bureau de l'entreprise.
Ainsi que la configuration d'un firewall, pour la sécurisation du réseau.
J'ai créé un guide d'utilisation pour le patron puisse modifie ou refaire les installations.
En dernière étape, exporter le matériel pour l'installer au siège de l'entreprise.

2 Présentation du travail réalisé

2.1 *Administration et maintenance d'une borne wifi*

2.1.1 Sécurisation du réseau wifi

2.1.1.2 Gestionnaire de mot de passe chiffré

Pour sécurise toutes les données sensible comme les mots de passe pour configurer la borne wifi, les adresses MAC des ordinateurs ou encore automatiser des connexions avec des lies, j'ai dus utilise un gestionnaire de mot de passe chiffré qui se nomme KeeePassXC..

Par exemple si on veut créer une base de données pour des mots de passe : Premièrement créer une nouvelle base de données -> Identifiant de la base de données → mettre un mot de passe fort → qui vas permettre de vous connecter à votre base de données -> Ajouter une nouvelle entrée → remplir les informations.

De plus le logiciel KeePassXC est Open Source est bien validé par L'ANSSI. Très pratique car il y a plusieurs fonctionnalités comme s'identifier automatiquement juste avec un lien (Netflix , Auchan…) ou écrire des notes, mettre des adresses MAC ,IP … .

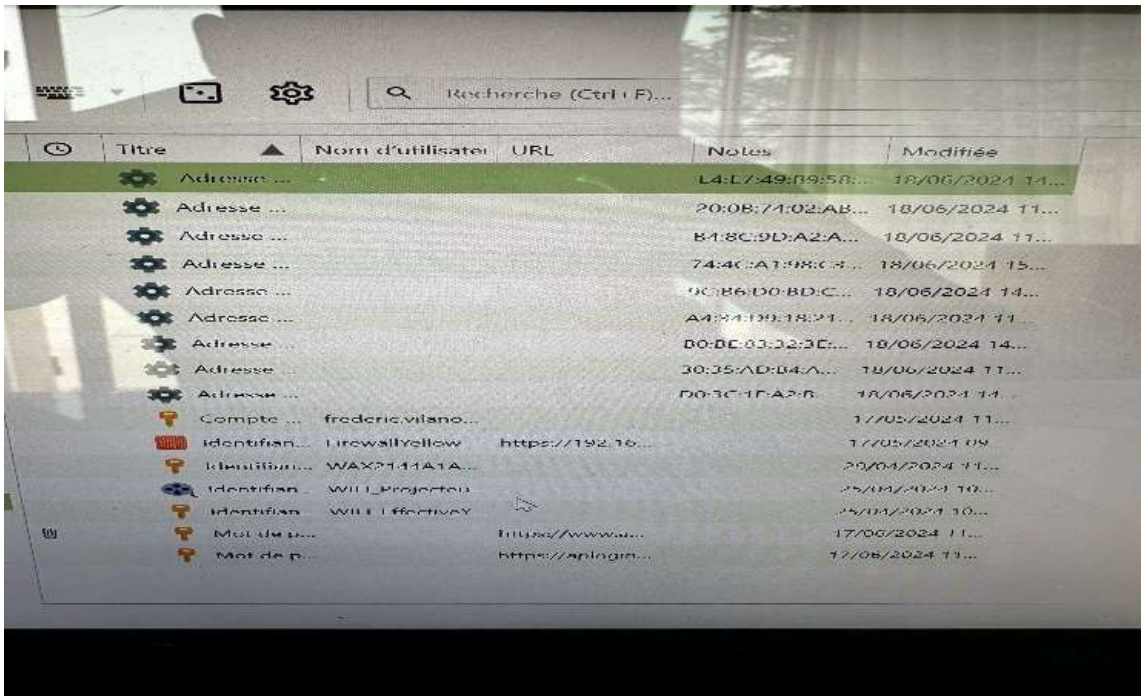

Figure 1 : Page de la base de donnée

2.1.1.3 SSID

J'ai caché le SSID qui est le nom du réseau wifi qui apparait lors de la connexion, grâce à cette fonctionnalité on voit apparaître ' Réseaux Masqué' et pour ce connecté à celui-ci on doit connaître le SSID dans un premier temps puis la clé de sécurité.
Qui ajoute une première couche de sécurité.

2.1.1.4 Chiffrement et protocole d'accès

Pour le protocole d'accès j'ai opté pour le WPA2/WPA3 qui permet de mixer les caractéristiques de sécurité. Tels qu'avoir une sécurité renforcée par rapport à WPA2 sûr (attaque brute force, chiffrement de données individuel) .

Mais aussi la compatibilité des équipements moins récent avec WPA2.

Pour le protocole de chiffrement j'ai mis du AES avec une taille de clé de 128 bits qui est la recommander par L'ANSSI.

2.1.1.4 Filtrage MAC

Le filtrage par adresse MAC est très important car c'est lui qui va autoriser ou non un périphérique à se connecter aux réseaux wifi, on peut aussi noter que celle qu'on interdit sur le réseau. Pour trouver l'adresse MAC de la machine il suffit d'aller dans le Terminal du PC faire la commande ipconfig /all descendre jusqu'à Carte réseaux sans fil Wifi → Adresse physique. Cette sécurité était bien pour cette entreprise car elle avait que quelque périphérique a ajouter et pas beaucoup de passage de nouveau périphérique car pour les grandes entreprises ce n'est pas pareils.

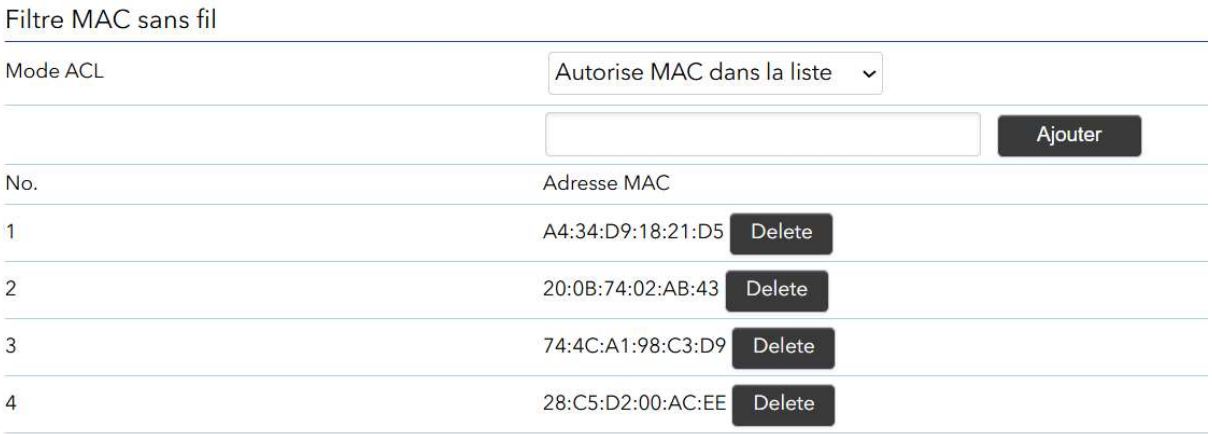

Figure 2 :Interface de modification des adresses MAC

2.1.1.5 Planification Wifi

Le but de cette fonctionnalité est de réguler les moments ou le wifi est activé. Je me suis basé sur les horaires et les souhaits du responsable, qui permet de ne pas laisser le réseau disponible sans aucune utilité. Ceci-ci peut-être modulable sur chaque réseau wifi distinct en fonction des utilisations.

Tableau annexe

Semaine	disponibles	Durée
Dimanche	indisponible	00 : 00 ~ 24 : 00
Lundi	indisponible	00 : 00 ~ 05 : 00
Mardi	indisponible	00 : 00 ~ 05 : 00
Mercredi	indisponible	00 : 00 ~ 05 : 00
Jeudi	indisponible	00 : 00 ~ 05 : 00
Vendredi	indisponible	00 : 00 ~ 05 : 00
Samedi	indisponible	00 : 00 ~ 24 : 00

Figure 3 : Page de modification des horaires

2.1.2 Matériels utilisés

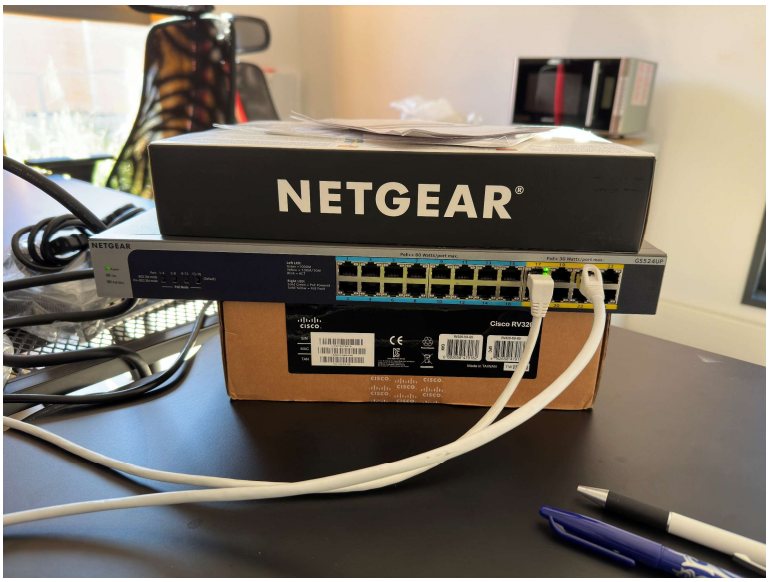

Figure 4 : Switch NETGEAR 24 ports (GS524UP)

Se switch est de la marque NETGAER munit de 24 ports dont 8 en POE+ /30 watts et 12 POE++.
La particularité de se switch qu'il permet de transférer des données et aussi alimenter en électricité des périphériques par câble Ethernet .
Ce qui plus pratique, car il y a moins de câbles donc être plus flexible et moins coûte, une puissance délivré plus grande de 30 watts pour les ports jaune ou 60 watts pour les ports bleu pour alimenter par exemple des cameras IP de haute qualité.

Figure 5 : Borne wifi NETGEAR (WIFI 6 AX1800 Dual-band Access Point with PoE WAX214V2)

La borne Wi-Fi NETGEAR WAX214V2 est un point d'accès sans fil conçu pour offrir une connectivité rapide, fiable et efficace dans divers environnements, tels que les petites entreprises, simple a installer, munit d'une des dernières performance le Wifi 6 qui offre une vitesse élevées et une gestion simple garce a son interface de configuration.

Figure 6 : 2 câbles RJ45

Un câble RJ45, souvent appelé simplement câble Ethernet, est un type de câble réseau utilisé pour connecter divers dispositifs dans un réseau local (LAN).
Garanti une fiabilité car moins sensible à l'interférence sans fil, facile a installer et une sécurité plus importante que les signaux sans fil.

Figure 7 : Vidéo projecteur WiFi Bluetooth, 20000L 700ANSI Rétroprojecteur 4K Supporte, Jimveo 1080P Full HD

Le vidéoprojecteur "Jimveo 1080P Full HD" est un appareil polyvalent conçu pour offrir une expérience de projection de haute qualité, adapté à une utilisation domestique ou professionnelle, il est muni d'une installation flexible une connectivité polyvalente ou Wifi ou Bluetooth

Figure 8 : Imprimante HP Office Jett Pro 9020

C’est une imprimante multifonction conçue pour les petites et moyennes entreprises ainsi que pour les utilisateurs à domicile ayant besoin de fonctionnalités de bureau complètes.
Elle est conçue pour offrir des impressions de haute qualité, des vitesses rapides, et une gamme de fonctionnalités qui simplifient la gestion des documents avec une connectivité et interface WIFI,Ethernet,USB…

2.1.2 Imprimante

2.1.3.1 HP Smart

HP Smart est un logiciel développé par HP pour gérer facilement les imprimantes de la marque. Il permet d'installer et configurer des imprimantes, de scanner, copier et imprimer directement depuis un ordinateur ou un appareil mobile. En plus, il offre des fonctionnalités avancées comme l'accès à l'impression depuis le cloud et la gestion des niveaux d'encre.

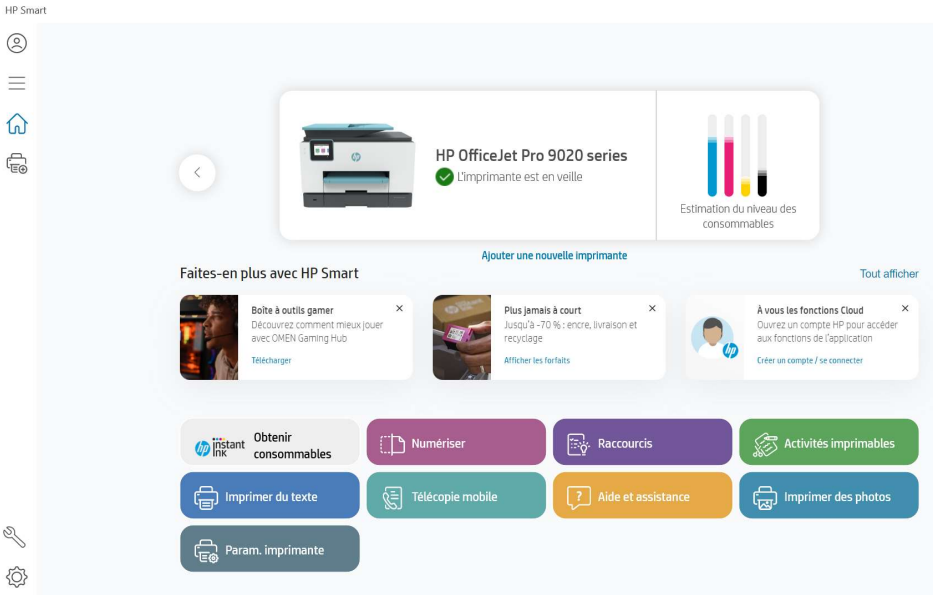

Figure 9 : Page d’accueil

2.1.3.2 Problématique de sécurité

Wi-Fi Direct est une fonctionnalité permettant à deux appareils de se connecter sans passer par un routeur, facilitant ainsi le transfert de fichiers, l'impression.
Cette technologie est utile pour des interactions sans fil simples et rapides entre smartphones, imprimantes, et autres périphériques.
Je me suis aperçu d'un très gros problème de sécurité avec le mot de passe par défaut qui ne respecter aucune règle (longueur, caractère spéciaux, majuscule, minuscule, nombre…) donner par L'ANSSI.
Je l'ai donc ajouté sur le réseau de l'entreprise qui est lui sécuriser.

2.1.3.3 Étude de cas

Dans le rapport pour le responsable, j'ai noté les problèmes ou les astuces pour que l'imprimante fonctionne correctement.
Par exemple :
-Vérifier si l'imprimante a bien était ajouter à « Imprimante & Scanners », si on veut imprimer
- Si il y a un message d'erreur ou noter « impression en attente » en bas à droite de l'écran, cela veut dire qu'il faut réimporter l'imprimante.
Mais aussi si l'on veut imprimer directement depuis (Word,Libre Office…) vérifier que la bonne imprimante sois bien sélectionner.

2.1.4 Vidéo projecteur

2.1.4.1 Dans quel but

Pour ce projet, il fallait réussir à mettre un réseau wifi sécurisé sur le vidéo projecteur.
Car à chaque utilisation, la personne qui voulait utiliser le vidéo projeteur , devait déplacer tous son matériel pour se brancher par câble Ethernet.

2.1.4.2 Sécurité

Tout d'abord, j'ai fait plusieurs tests, j'en ai conclu que la meilleure solution est de créer un nouveau réseau "WIFI_ProjecteurYellow", spécialement pour le vidéo projecteur.
Avec comme bande de fréquence 5Ghz, car la borne wifi est à proximité donc on priorise la puissance et performance du débit envoyé.

J'ai mis en place l'isolement des clients qui consiste à bloquer leurs communications entre eux sur le même SSID car le réseau est conçu uniquement pour le vidéo projecteur.
J'ai caché le SSID mais je n'ai pas pu mettre le filtrage d'adresse MAC car cela n'est pas compatible avec le vidéo projeteur.

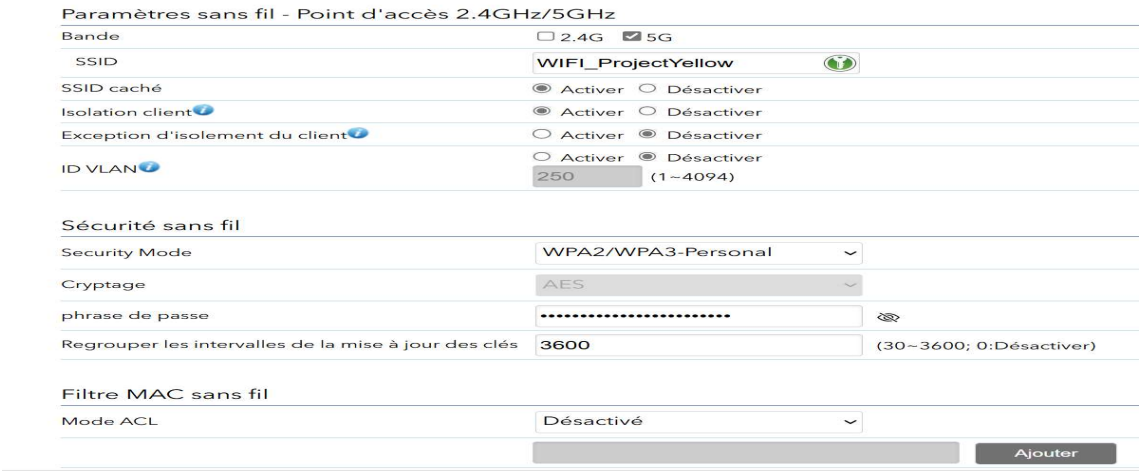

Figure 10 : Fenêtre de paramétrage du réseau wifi

2.1.4.3 Problématique

Une des solutions aurait était d'utiliser le wifi administrateur qui permet la configuration de la borne, sachant, qu'il devient inactif au bout de 15 minutes.
Ce qui est intéressant pour le vidéo projecteur qui n'est pas souvent en fonction.
Cependant, pour faire redevenir le réseau actif, il faut redémarrer la borne wifi ce qui n'est pas pratique et pose un problème pour les collaborateurs.
De plus on ne peut pas cacher le SSID sur réseau administrateur donc tout le monde pourra le voir à n'importe quel moment.

2.2 Configuration et installation d'un firewall

2.2.1 Introduction d'un firewall

2.2.1.1 Quel intérêt

Installer un Firewall dans une entreprise est crucial pour sécuriser le réseau en filtrant le trafic et en bloquant les menaces externes comme les virus et les cyberattaques. Il contrôle l'accès aux ressources internes, assurant que seules les entités autorisées peuvent interagir avec les données sensibles. De plus, il surveille et enregistre l'activité réseau, aidant à identifier et à répondre aux anomalies, tout en optimisant la performance du réseau.

2.2.2 Tunnel VPN

2.2.2.1 Les différents type de tunnel VPN

Il y a deux types de Tunnel VPN :

Passerelle-à-Passerelle
Où
Client-à-Passerelle.

Passerelle-à-Passerelle (site a site) :
Deux réseaux locaux séparé géographiquement qui sont interconnectés via une connexion sécurisée.

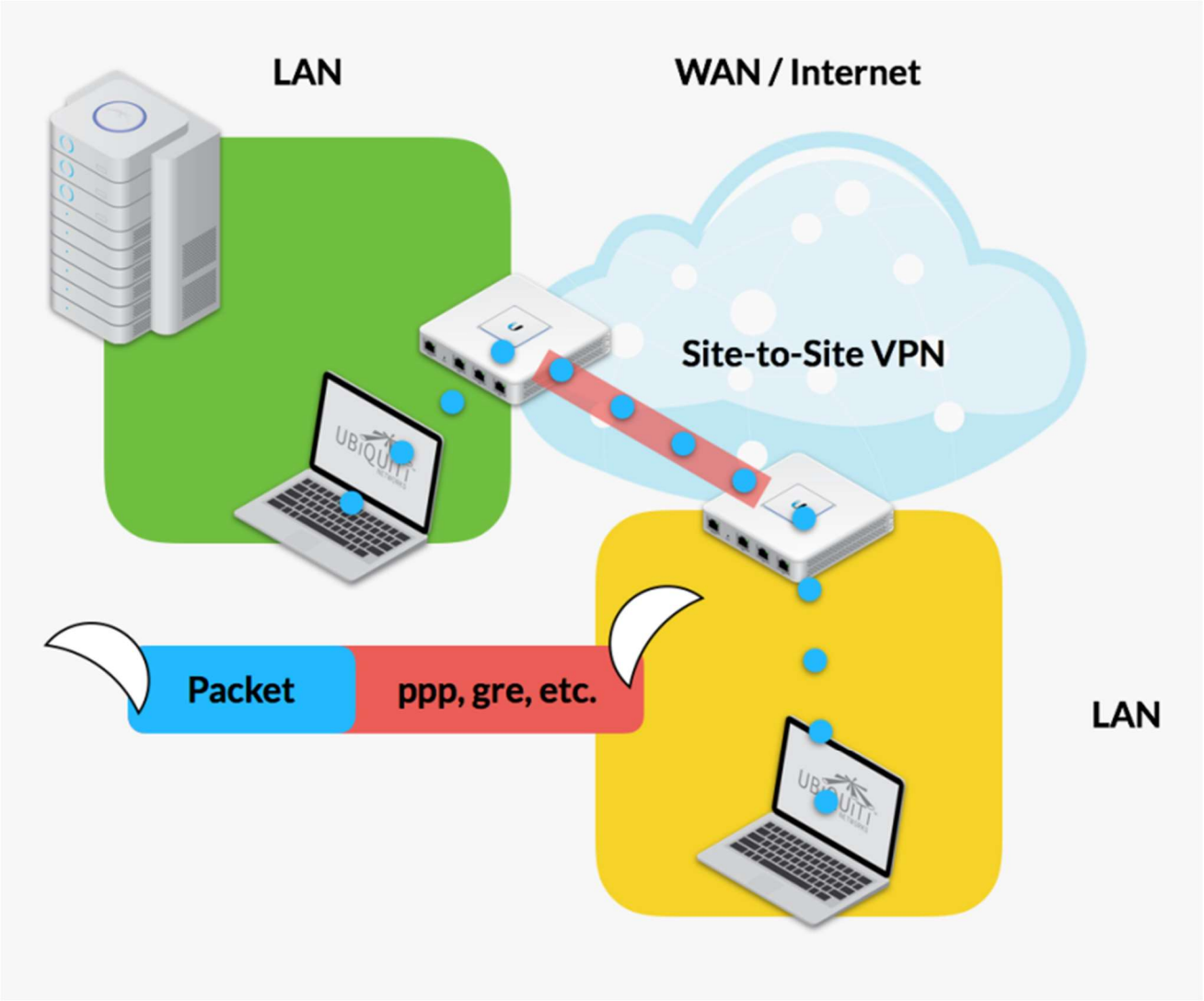

Figure 11 : Schéma Tunnel VPN Site-to-Site

Client-à-passerelle (point a site) :
Un réseaux privé virtuel dans lesquels les clients se connecter individuellement de manière sécurisée aux réseaux prive distant via Internet. De plus il est souvent utilisé pour les utilisateurs en télétravaille.

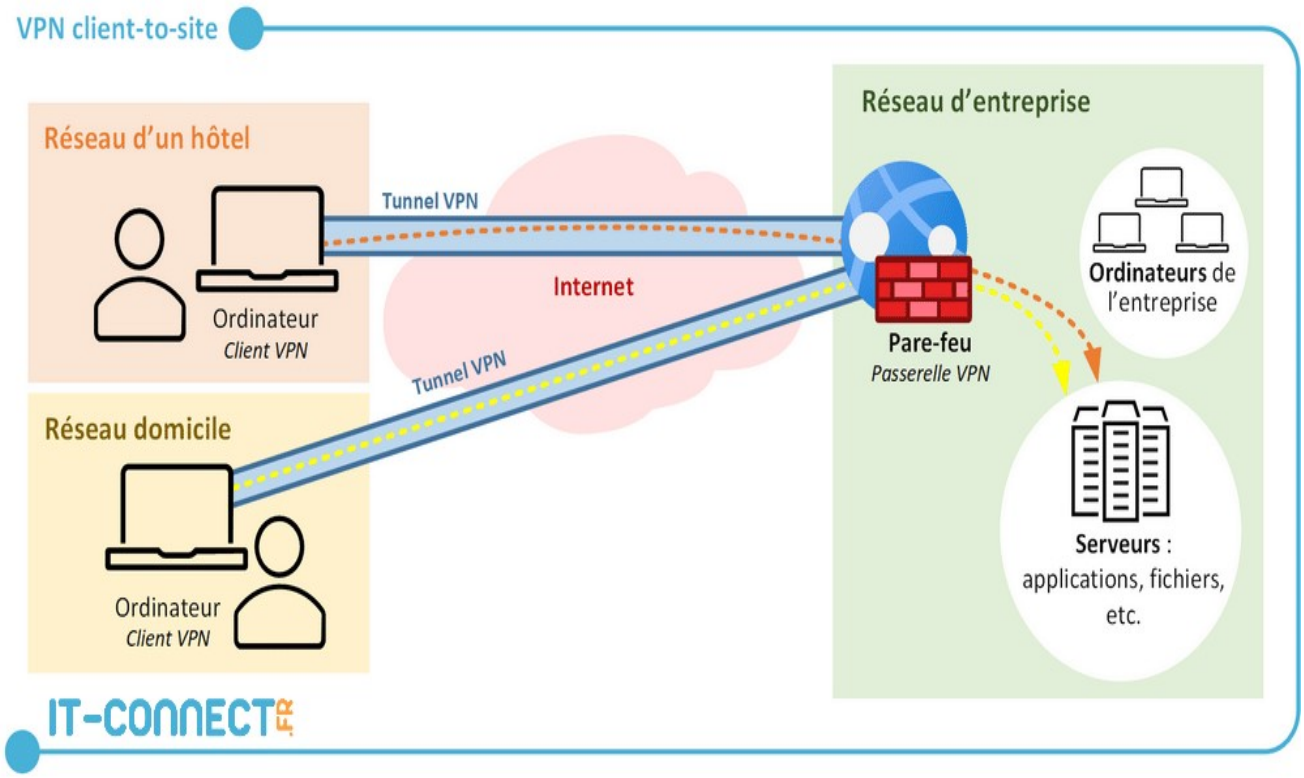

Figure 12 : Schéma Tunnel VPN Client-to-Site

2.2.2.2 Les options VPN

Tunnel VPN :

Un tunnel qui établit une connexion sécurisée entre un utilisateur et un réseau distant, en chiffrant les données échangées pour garantir la confidentialité.
Cette connexion traverse l'Internet public, mais reste isolée et protégée, permettant un accès sécurisé aux ressources du réseau comme si l'utilisateur était physiquement présent sur ce réseau.

VPN de Groupe :

Un VPN de groupe permet à plusieurs utilisateurs de se connecter simultanément à un réseau privé à travers une connexion chiffrée partagée.
Ce type de VPN centralise les connexions, facilitant l'accès sécurisé aux ressources du réseau pour des groupes d'utilisateurs, comme les employés d'une entreprise, tout en simplifiant la gestion et l'administration des connexions.

EASY VPN :

Une solution simplifiée pour la gestion, le déploiement et la sécurité des VPN développé par Cisco Systems.
Qui consiste à installer une application « VPN client Cisco » mais arrêté à cause de sa vulnérabilité. Remplacer par AnyConnect, grâce à cette application il suffit juste d'identifier le client avec un mot de passe, adresse IP … pour prendre le tunnel.
Il y a 2 options important ou l'on décide comment passe le trafic.

Le Tunnel Split consiste à ne pas laisser le trafic Internet passer mais que les paquets à destination du réseau privé.
Ce qui permet de réduire la charge du réseau.
Au contraire, le Full tunnel permet de faire passer l'ensemble du trafic même si celui-là n'est pas lié, tous en étant chiffré, on a donc une plus grande sécurité.

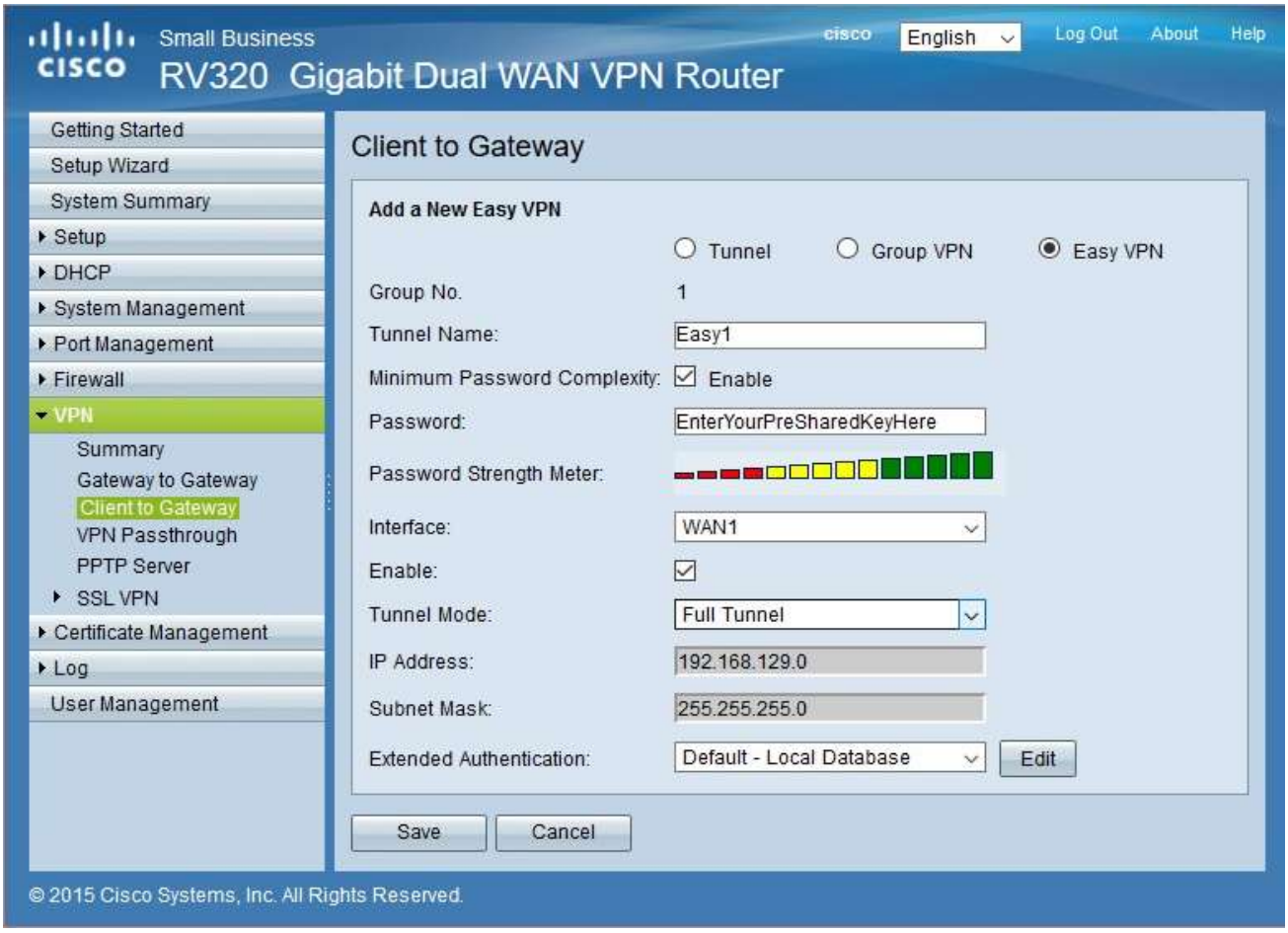

Figure 13 : Page de configuration tunnel EASY VPN

2.2.3 Les sécurisations mise en place

2.2.3.1 Gestions/États des ports

J'ai dû désactiver des ports qui était inutiles, comme le port LAN 2 , 3 ,4 et le WAN 2.
Sur les ports restants, j'ai activé le EEE qui permet de rendre les ports rapide et réactif, ainsi que de réduire la consommation d'énergie, pouvant être en veille.

Pour leur état, il y avait plusieurs possibilités :
-la première, mettre en Semi-Duplex qui permet de recevoir ou d'envoyé les données tout en utilisant un protocole de contrôle de flux pour éviter les collisions sur le réseau.
- la deuxième, est l'Intégral (Full Duplex) permet de recevoir ou d'envoyé des données en simultané.

J'ai préféré mettre du Full Duplex car il est largement préférable dans les réseaux modernes pour sa capacité à éliminer les collisions et à offrir une performance maximale en permettant la communication bidirectionnelle simultanée.

Table Ethernet

ID du port	Type	État de la liaison	Activité du port	Priorité	État du débit	État du duplex	Négociation automatiqu
LAN1	10Base-T/100Base-TX/1000Base-T	Actif	Activé	Normal	1000Mbit/s	Intégral	Activé
LAN2	10Base-T/100Base-TX/1000Base-T	Inactif	Désactivé	Normal	10Mbit/s	Semi-duplex	Activé
LAN3	10Base-T/100Base-TX/1000Base-T	Inactif	Désactivé	Normal	10Mbit/s	Semi-duplex	Activé
LAN4	10Base-T/100Base-TX/1000Base-T	Inactif	Désactivé	Normal	10Mbit/s	Semi-duplex	Activé
WAN1	10Base-T/100Base-TX/1000Base-T	Actif	Activé	Normal	1000Mbit/s	Intégral	Activé
WAN2	10Base-T/100Base-TX/1000Base-T	Inactif	Désactivé	Normal	10Mbit/s	Semi-duplex	Activé

Figure 13 : Table Ethernet

2.2.3.2 Règles d'accès

Les règles d'accès sur un Firewall, sont très importante car c'est là où l'on Autorise/Interdit un trafic sur notre réseau.
Il y a certains protocoles qui ne sont pas sécurisé comme HTTP car les données sont transférées en texte brut.
Mais aussi, le protocole TELNET car nous pouvons accéder à distance et il transmet toute ses données en texte clair même les mots de passe.
Ou encore FTP, car il n'est pas sécurisé par défaut et en plus les données sont transférées en texte clair y compris les informations d'identification, le seul autorisé est HTTPS car lui a une couche de chiffrement SSL/TLS.
Sans oublier le 'ANY ANY'qui permet d'interdire tout le trafic qui n'est pas spécifiquement Autoriser.

Table des règles d'accès — Éléments 1-10 de 13 — 10 par page

	Priorité	Activer	Action	Service	Interface source	Source	Destination	Heure	Jour
○	1	☑	Refuser	HTTP [80]	LAN	192.168.8.1 ~ 192.168.8.254	8.8.8.8 ~ 8.8.8.8	Toujours	
○	2	☑	Refuser	HTTP Secondary [8080]	LAN	192.168.8.1 ~ 192.168.8.254	8.8.8.8 ~ 8.8.8.8	Toujours	
○	3	☑	Autoriser	HTTPS [443]	LAN	192.168.8.1 ~ 192.168.8.254	8.8.8.8 ~ 8.8.8.8	Toujours	
○	4	☑	Refuser	TELNET SSL [992]	LAN	192.168.8.1 ~ 192.168.8.254	Tout	Toujours	
○	5	☑	Refuser	TELNET Secondary [8023]	LAN	192.168.8.1 ~ 192.168.8.254	Tout	Toujours	
○	6	☑	Refuser	TELNET [23]	LAN	192.168.8.1 ~ 192.168.8.254	Tout	Toujours	
○	7	☑	Refuser	SMTP [25]	LAN	192.168.8.1 ~ 192.168.8.254	8.8.8.8 ~ 8.8.8.8	Toujours	
○	8	☑	Refuser	FTP [21]	LAN	192.168.8.1 ~ 192.168.8.254	Tout	Toujours	
○		☑	Autoriser	Tout le trafic [1]	LAN	192.168.8.1/255.255.255.0	Tout	Toujours	
○		☑	Refuser	Tout le trafic [1]	USB1	Tout	Tout	Toujours	

Table des règles d'accès — Éléments 11-13 de 13 — 10 par page

	Priorité	Activer	Action	Service	Interface source	Source	Destination	Heure	Jour
○		☑	Refuser	Tout le trafic [1]	USB2	Tout	Tout	Toujours	
○		☑	Refuser	Tout le trafic [1]	WAN1	Tout	Tout	Toujours	
○		☑	Refuser	Tout le trafic [1]	WAN2	Tout	Tout	Toujours	

Ajouter | Modifier | Supprimer | Restaurer les règles par défaut | Gestion des services... | Page 2 de 2

Figure 14 : Table des règles d'accès

2.2.4 Faille ZERO-DAY Cisco

2.2.4.1 Définition

Une faille ZERO-DAY est une faille qui vient d'être découverte et qui n'est pas connue par le développeur ou le fabricant.
Elles sont très dangereuses car elles peuvent être exploitées pour compromettre des systèmes informatiques.
Le seul moyen pour se protéger contre elles et de garder les systèmes à jour et d'avoir un Firewall et des antivirus, mais aussi une vielle technologique pour rester à jour.

2.2.4.2 Une récentes ZERO-DAY Cisco

L'une des dernières découverte qui cible les Firewall Cisco dans le monde, consiste une fois entrée dans la machine à injecter " Line Runner et Line Dancer".

- ***Line Dancer*** est un implant mémoire qui exécute des charges utiles de shellcode, désactive syslog, exécute des commandes, provoque des redémarrages d'appareils, échappant à l'analyse.

- ***Line Runner*** est un web shell persistant. Il peut télécharger et exécuter des scripts Lua, qui sont comme des instructions spéciales.

Ce qui montre qui la veille technologique est très important peu importe le matériel ou la marque du produit.

2.3 Installation du matériel dans le siège

2.3.1 Contrainte environnementale

Pour l'installation au siège social de l'entreprise, j'ai dû penser et prendre en compte des nouveaux paramètres et règles de sécurité.

Sachant qu'une imprimante était présente, j'ai dû la rajouter dans le réseau de l'entreprise donc récupérer son adresse MAC, car les attaques se font par tous ce qui est connecté à un réseau (Camera IP, Imprimante, Scanners Webcams).

J'ai demandé aux employés et au responsable, si il avait des ordinateurs qu'il utilisé pour le travail pour eux aussi les intégrés au réseau.

Suite à ça, il fallait changer les horaires de planification du wifi, j'ai donc laissé le wifi tourné non-stop car le responsable la souhaité. Déplacer le matériel a cote de la box et des câbles Ethernet disponible.

3 Conclusion

Au terme de ce stage, j'ai pu enrichir significativement mes compétences en matière de technologies de l'information et de la communication.

Mon expérience a été marquée par l'installation d'une borne Wi-Fi, la configuration d'une imprimante réseau et la mise en place d'un firewall, autant de tâches qui ont renforcé mon savoir-faire technique.

L'installation de la borne Wi-Fi m'a permis de renforcer mes connaissances sur les principes de base du déploiement de réseaux sans fil, notamment la sélection de l'emplacement optimal pour maximiser la couverture et la qualité du signal. J'ai également découvert l'importance de sécuriser le réseau contre les accès non autorisés, ce qui m'a initié aux protocoles de sécurité comme le WPA2/WPA3.

La configuration du firewall a été l'une des tâches les plus cruciales de mon stage. J'ai appris à identifier et à gérer les menaces potentielles qui peuvent compromettre la sécurité d'un réseau. Ce processus a renforcé ma compréhension des concepts de sécurité informatique, tels que la définition de règles de filtrage, la gestion des ports et la surveillance des journaux d'activité.

Un aspect fondamental que j'ai appris à travers ces missions est l'importance de la documentation et de la planification préalables. Avant d'entamer toute intervention, il est essentiel de se documenter minutieusement pour comprendre les implications techniques et organisationnelles de chaque action. Cela m'a permis d'anticiper les problèmes potentiels et de concevoir des solutions robustes et durables.

Enfin, cette expérience m'a enseigné à évaluer les impacts de mes modifications sur l'ensemble du réseau. Chaque ajustement, même mineur, peut avoir des conséquences significatives sur la performance et la sécurité du système.

Cette prise de conscience est cruciale pour quiconque travaille dans le domaine des technologies de l'information, où la précision et la prévoyance sont essentielles.

En conclusion, ce stage a non seulement développé mes compétences techniques, mais a également enrichi ma compréhension de l'importance des bonnes pratiques en matière de gestion des systèmes d'information. Il a renforcé ma capacité à analyser les situations, à planifier des interventions efficaces et à garantir la continuité opérationnelle tout en assurant la sécurité du réseau.

Je suis reconnaissant pour cette opportunité d'apprentissage pratique et je suis convaincu que ces compétences me seront inestimables dans ma future carrière professionnelle.

4 Remerciements

Je souhaite exprimer ma gratitude à Mr Frédéric Vilanova, mon responsable de stage et directeur de la société Effective Yellow, pour m'avoir accueillie en tant que stagiaire au sein de son entreprise.

Je tiens également à remercier Louis Brouardelle pour le soutien qu'il m'a apporté au sein de l'entreprise.

Je remercie aussi l'ensemble de l'équipe d'Effective Yellow pour l'intérêt qu'ils ont porté à mon travail durant mon stage, ainsi que pour leur aide et leurs précieux enseignements.

Enfin, je remercie sincèrement mon tuteur de stage pour son encadrement et ses conseils tout au long de cette période.

5 Glossaire

POE+ (Power Over Ethernet)
C’est une technologie réseaux permettant de transfert des données et alimente en électricité des périphériques par Ethernet. (+) apporte plut de puissant en termes de Consommation énergique fournis ou consommation reçue.

WPA (Wi-Fi Protected Access)
Norme de sécurité pour les réseaux sans fil, conçue pour sécuriser les connexions Wi-Fi en protégeant les données transmises entre les appareils connectés.

SSID (Service Set Identifier)
utilisé dans les réseaux sans fil pour désigner le nom unique d'un réseau Wi-Fi.
EEE (Energy Efficient Ethernet) norme réseau qui réduit la consommation d'énergie des équipements Ethernet lorsqu'ils sont peu sollicités ou inactifs.

Les failles ZERO-DAY
une vulnérabilité de sécurité dans un logiciel ou un système informatique qui est découverte par des acteurs malveillants avant qu'un correctif ou une solution de contournement ne soit disponible pour les protéger .

L’ANSSI (Agence nationale de la sécurité des systèmes d’information)

MAC (Media Access control)
Adresse physique d’une périphérique.

AES (Advanced Encryption Standard)

LAN (Local Area Network)
Le réseau local.

VPN (Virtual Private Network)
Crée une connexion réseau sécurisée et privée sur une infrastructure publique comme Internet.

HTTP ((HyperText Transfer Protocol)
Protocole de communication utilisé pour le transfert de données sur le World Wide Web.

HTTPS ((HyperText Transfer Protocol Secure)

SSL/TLS (Secure Sockets Layer / Transport Layer Security)
Pour chiffrer les données échangées entre le navigateur web (client) et le serveur web.

FTP (File Transfert Protocole)
Protocole de transfert des fichiers entre clients.

6 Bibliographie

Installation du logiciel KeePassXC :

https://keepassxc.org/

S'il y a un problème ou en savoir plus, voici une vidéo très bien détaillée .

https://www.youtube.com/watch?v=tT5AmNXjl_g

Mécanisme de cryptographie :

https://cyber.gouv.fr/publications/mecanismes-cryptographiques

Document de l'ANSSI qui certifie KeepassXC :

https://cyber.gouv.fr/produits-certifies/keepass-version-210-portable

Document PDF utilisé

rv320_qsg_fr_78-20998-02B0

rv32x_ag_frhttps://www.clubic.com/actualite-525162-des-pare-feu-cisco-touches-par-une-faille-zero-day-ciblent-des-

sites-gouvernementaux-a-travers-le-monde.html