MOUTET OWEN

XEFI Pornic

Brevet de Technicien Supérieur

Services Informatiques aux organisations

E-5: SUPPORT ET MISE À DISPOSITION DES SERVICES INFORMATIQUES

MOUTET OWEN

BTS SIO – 2026

Sommaire :

Ma Présentation

Je m'appelle MOUTET Owen. J'ai tout d'abord suivi un Bac Pro MEI (Maintenance des Équipements Industriels), une formation que j'avais choisie par intérêt pour la technique, la mécanique et la maintenance. Cette voie m'a permis d'acquérir des compétences solides en mécanique, électricité et automatisme.

Avec le temps, j'ai cependant réalisé que ce domaine ne correspondait pas pleinement à mes aspirations. Passionné depuis longtemps par l'informatique et les nouvelles technologies, j'ai décidé de me réorienter vers un BTS SIO (Services Informatiques aux Organisations) afin de travailler dans un secteur qui me motive réellement : la gestion des systèmes, les réseaux et la cybersécurité.

Aujourd'hui, je poursuis mon BTS SIO en alternance au sein de l'entreprise XEFI Pornic, où j'occupe le poste de technicien informatique. Cette expérience professionnelle me permet de mettre en pratique mes connaissances, de participer à des projets concrets chez les clients et de développer mes compétences en administration réseau, en sécurité informatique et en support technique.

Mon objectif est de continuer à progresser dans ce domaine en constante évolution, afin de devenir un professionnel capable de concevoir, sécuriser et maintenir des infrastructures informatiques fiables, tout en accompagnant les entreprises dans leur transformation numérique.

Consultez mon portfolio à l'aide du lien suivant :

https://owen.moutet-temple.formation-esiac.fr

Présentation de XEFI

Xefi est une entreprise présente en France, en Belgique et en Suisse, Espagne dont le siège social se situe à Lyon. Forte de son implantation sur plusieurs territoires, Xefi s'impose comme un acteur majeur dans le domaine des services informatiques pour les entreprises.

Créée en 2021, Xefi Pornic est une agence locale qui s'inscrit dans cette dynamique en proposant des solutions adaptées aux besoins des professionnels. Son objectif est d'accompagner les entreprises dans le déploiement, la gestion et l'optimisation de leur système d'information, en garantissant performance et sécurité.

Les missions de Xefi vont bien au-delà de la simple fourniture de matériel. L'entreprise s'engage à assurer la sécurité et la sauvegarde des systèmes d'information de ses clients grâce à la mise en place de solutions fiables telles que des antivirus performants, des pare-feu (firewalls) et des systèmes de sauvegarde. Cette approche proactive permet de prévenir les cyberattaques et de garantir la continuité des activités. Xefi mise également sur la proximité avec ses clients, en offrant un accompagnement personnalisé et réactif.

Pour répondre à la diversité des besoins informatiques, Xefi propose une gamme complète de biens et services :

- **Vente de matériel informatique** : ordinateurs, serveurs, périphériques adaptés aux exigences professionnelles.
- **Maintenance et assistance technique** : interventions rapides pour assurer la disponibilité des systèmes.
- **Sécurité en ligne** : solutions de cybersécurité pour protéger les données sensibles.
- **Solutions logicielles** : logiciels métiers, outils collaboratifs et solutions cloud.
- **Hébergement de données** : infrastructures sécurisées pour garantir la confidentialité et la disponibilité des informations.

Grâce à cette offre globale, Xefi se positionne comme un partenaire de confiance pour les entreprises, en leur permettant de se concentrer sur leur cœur de métier tout en bénéficiant d'un système informatique performant et sécurisé.

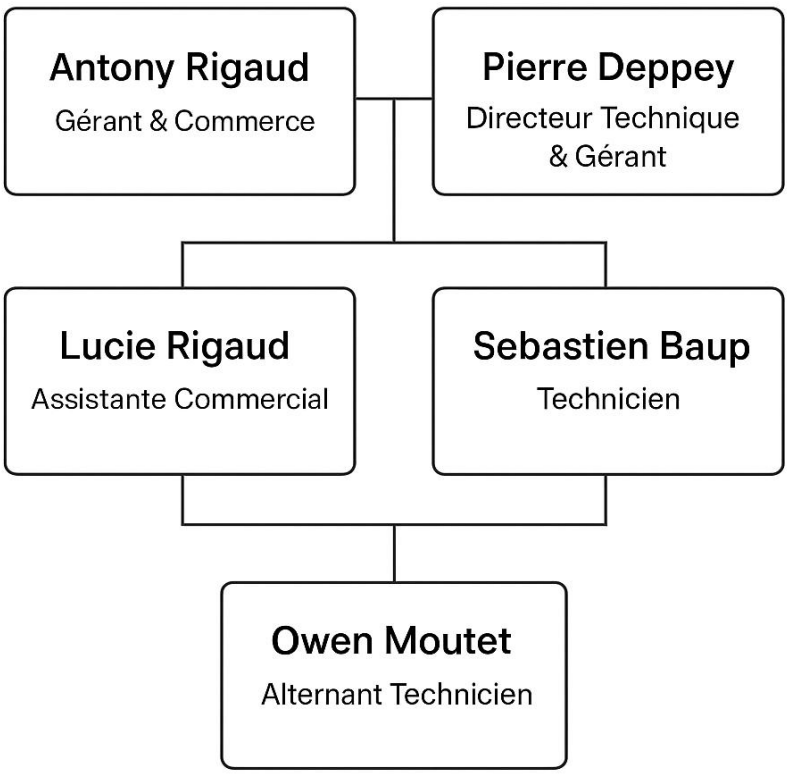
Remerciements :

Je tiens à exprimer ma sincère gratitude envers toute l'équipe de Xefi Pornic, et en particulier mon tuteur en entreprise, pour l'accompagnement et le soutien dont j'ai bénéficié tout au long de mon alternance.

Cette expérience m'a permis de développer mes compétences techniques en tant que technicien informatique en alternance, notamment dans l'installation et la maintenance de réseaux, la gestion des équipements réseau et la sécurisation de l'infrastructure informatique. Grâce à la confiance qui m'a été accordée, j'ai pu mettre en pratique les connaissances acquises en formation et découvrir le fonctionnement concret d'une entreprise spécialisée en solutions IT.

Je remercie également mes collègues pour leur disponibilité et leurs conseils, qui m'ont permis de progresser dans mes missions et de mieux comprendre les enjeux professionnels liés au métier de technicien réseau.

Organigrammes de l'entreprise :



Mes missions :

Rôle global du technicien informatique

Le technicien informatique chez XEFI a pour mission de :

- Assurer le bon fonctionnement du parc informatique des clients
- Participer à la mise en place de nouvelles infrastructures réseau et sécurité
- Effectuer la maintenance préventive et corrective des systèmes
- Assurer un support technique auprès des utilisateurs et clients professionnels
- Rédiger la documentation technique et assurer un reporting à son responsable d'agence

1. Installation et configuration de matériel informatique

- Préparation et configuration de postes de travail (Windows 10/11, Office 365, antivirus Sophos)
- Installation de serveurs Windows (AD, DNS, DHCP, partages réseaux)
- Raccordement des postes et périphériques (imprimantes, scanners, NAS)
- Configuration des switch et routeurs pour les nouveaux sites clients

2. Sécurisation et réseau Installation et configuration de pare-feu Sophos XGS

- Mise en place de VPN SSL pour les accès distants sécurisés
- Gestion des règles de filtrage et politiques de sécurité
- Vérification du bon fonctionnement du réseau local (LAN/WAN) et des connexions Internet
- Suivi via Sophos Central ou autres outils de supervision

3.Administration et services cloud

- Création et gestion de comptes Microsoft 365 / Exchange Online
- Sauvegarde des données sur XEFI Cloud ou Acronis Backup
- Gestion des licences et accès utilisateurs
- Synchronisation des postes avec les services cloud

4. Administration et services cloud

- Création et gestion de comptes Microsoft 365 / Exchange Online
- Gestion des licences et accès utilisateurs
- Synchronisation des postes avec les services cloud (one drive)

5. Documentation et communication

- Rédaction de fiches d'intervention et procédures techniques
- Tenue à jour des inventaires clients (matériel, IP, licences)
- Compte rendu hebdomadaire au technicien référent ou au chef d'agence
- Participation à des réunions techniques internes (suivi des incidents, nouveaux déploiements)

Compétences mobilisées (BTS SIO – SISR)

Domaine :	Compétences développées
Réseau et infrastructure :	Installation, configuration et maintenance d'équipements réseau (switch, routeur, pare-feu)
Sécurité :	Mise en place de politiques de sécurité, filtrage, sauvegarde, VPN
Système :	Installation de postes, serveurs Windows, gestion des partages et droits d'accès
Support :	Assistance technique de niveau 1 et 2, diagnostic et résolution d'incidents
Organisation :	Rédaction de documentation, gestion de planning et reporting d'activité

Outils et technologies utilisés

- Systèmes : Windows 10/11, Windows Server, Active Directory
- Sécurité : Sophos XGS, Sophos Central, Acronis Backup
- Réseau : Cisco / Netgear / TP-Link, VLAN, DHCP, DNS, NAT
- Support : GLPI, TeamViewer, AnyDesk
- Bureautique & Cloud : Microsoft 365, Exchange, OneDrive
- Supervision : Outils internes XEFI

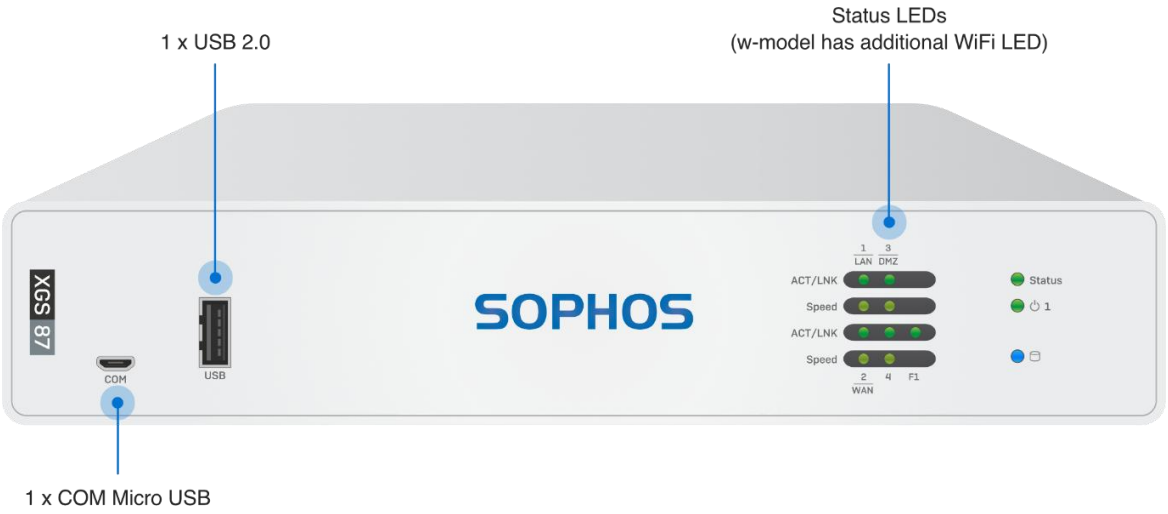
MES PROJETS :

Contexte du projet

En tant qu'alternant au sein de l'agence XEFI Pornic, je participe régulièrement à la préparation et à la mise en œuvre des solutions informatiques destinées à nos clients professionnels. Dans le cadre de cette situation, j'ai été chargé de préparer un pare-feu de nouvelle génération destiné à remplacer un ancien pare-feu Sophos chez l'un de nos clients. L'appareil actuellement en place est en fin de vie et ne répond plus aux exigences actuelles en matière de sécurité réseau, ce qui justifie son remplacement.

Mon rôle a consisté à initialiser et préconfigurer le nouveau pare-feu dans nos locaux avant son installation sur site par l'un de mes collègues. J'ai ainsi réalisé plusieurs tâches : mise à jour du firmware, configuration réseau de base, préparation des premières règles de filtrage, activation des licences, et vérification du bon fonctionnement global de l'équipement. L'objectif était de livrer un pare-feu prêt à être déployé, afin de garantir une installation rapide et sécurisée chez le client.

Cette mission m'a permis de développer mes compétences en sécurisation d'infrastructures, en préparation de matériels réseau, et en travail en équipe. Elle s'inscrit pleinement dans le cadre de mon parcours en BTS SIO, en me confrontant à une situation professionnelle réelle impliquant des enjeux de cybersécurité et de qualité de service pour le client.



Objectifs du projet :

- Sécuriser le réseau contre les attaques externes (intrusions, scans, malwares).
- Contrôler les flux réseau entrants et sortants selon une politique de filtrage adaptée.
- Mettre en place un VPN sécurisé pour permettre aux collaborateurs d'accéder aux ressources internes depuis l'extérieur.
- Garantir la continuité de service et la disponibilité de la connexion Internet.
- Fournir une interface centralisée de supervision et de logs via le portail Sophos Central.

Analyse et préparation :

Avant l'installation, une étude de l'environnement réseau du client a été réalisée :

- Recensement du matériel existant (routeur, switch, serveur, postes).
- Schéma du réseau et plan d'adressage IP.
- Identification des besoins en accès Internet et des flux à autoriser (HTTP, HTTPS, RDP, VPN, etc.).
- Vérification de la compatibilité avec les équipements réseau existants.

1. Initialisation et Configuration de Pare-feu Sophos :

En tant qu'alternant chez Xefi, l'une de mes principales missions consiste à initialiser et configurer des pare-feu Sophos pour les entreprises clientes. Cette tâche est essentielle pour renforcer la sécurité des systèmes d'information et protéger les infrastructures contre les cybermenaces.

L'initialisation d'un pare-feu Sophos ne se limite pas à une simple installation. Elle implique plusieurs étapes techniques :

- **Configuration des règles de filtrage** : je définis les politiques de sécurité pour contrôler le trafic entrant et sortant, en bloquant les connexions non autorisées et en autorisant uniquement les flux nécessaires.
- **Mise en place des fonctionnalités avancées** : activation de la détection et prévention des intrusions (IPS), filtrage web pour limiter l'accès à des sites non sécurisés, et contrôle des applications pour éviter l'utilisation de logiciels non conformes.
- **Paramétrage des VPN** : création de tunnels sécurisés pour permettre aux collaborateurs de se connecter à distance en toute sécurité.
- **Surveillance et mises à jour** : je veille à ce que les pare-feu soient toujours à jour afin de contrer les nouvelles menaces et garantir une protection optimale.

Ces configurations sont indispensables pour prévenir les cyberattaques, protéger les données sensibles et assurer la continuité des activités des entreprises. Dans un contexte où les menaces informatiques sont de plus en plus sophistiquées, la mise en place d'un pare-feu performant est un élément clé de la stratégie de cybersécurité.

Cette mission me permet de développer des compétences techniques en administration réseau, en sécurité informatique et en gestion des équipements de protection. Elle me donne également une vision concrète des enjeux liés à la cybersécurité et à la conformité réglementaire, des aspects essentiels pour toute entreprise aujourd'hui.

Procédure d'Initialisation d’un Firewall Sophos XGS (jusqu’au VPN SSL)

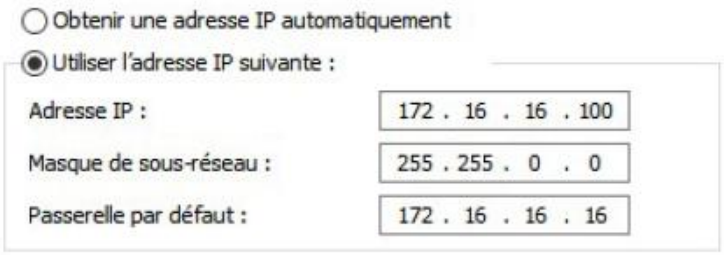
1. Prérequis

- Prévoir une licence Sophos (à demander via votre portail ou CRM).
- Préparer un PC avec accès au port LAN du firewall.
- Navigateur web compatible (En l'occurrence Edge).

2. Connexion au Firewall

- Connecter le PC au port LAN (Eth1).
- Configurer une IP statique dans le réseau **172.16.16.0/16** (ex: 172.16.16.100).
- Accéder à l’interface web via : https://172.16.16.16:4444.

Exemple :



Une fois le boitier démarré, accéder à l’interface web via :

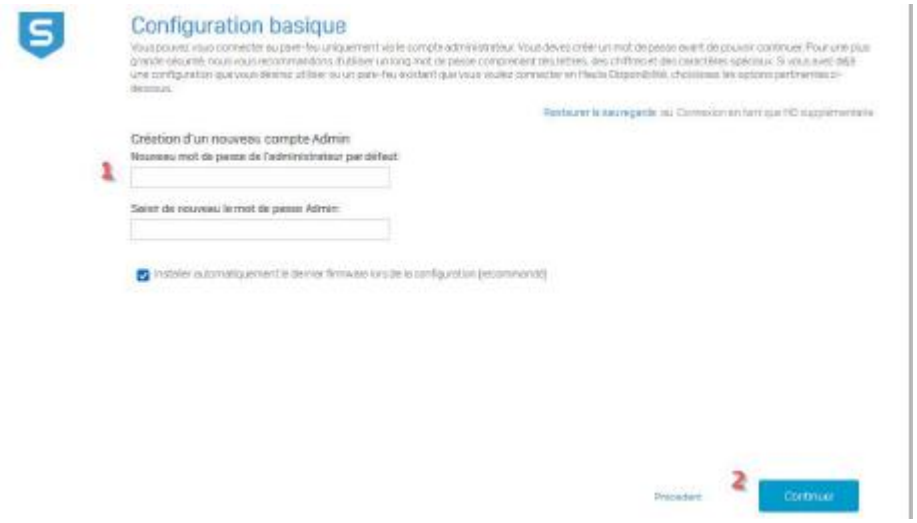
https://172.16.16.16:4444

3. Assistant de Configuration

- Choisir la langue.

- Lancer l'installation.

- Définir un mot de passe administrateur sécurisé.

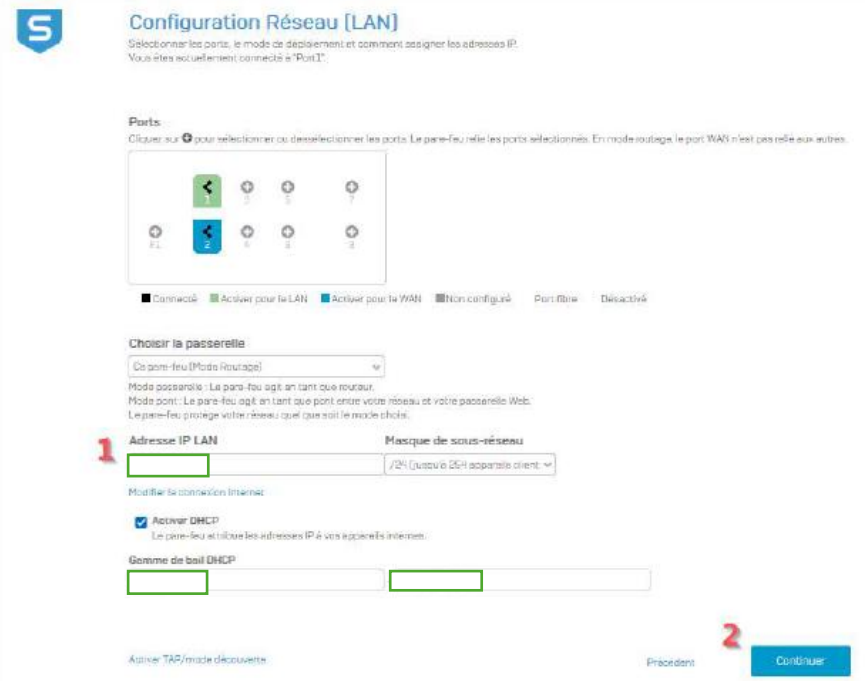


- Connecter le port WAN (Eth2) à Internet.

4. Paramètres de Base

- Nommer le firewall selon votre convention [FW-XEFI_PORNIC_(.....)].

- Définir la timezone (ex: Europe/Paris).
- Configurer le réseau LAN .



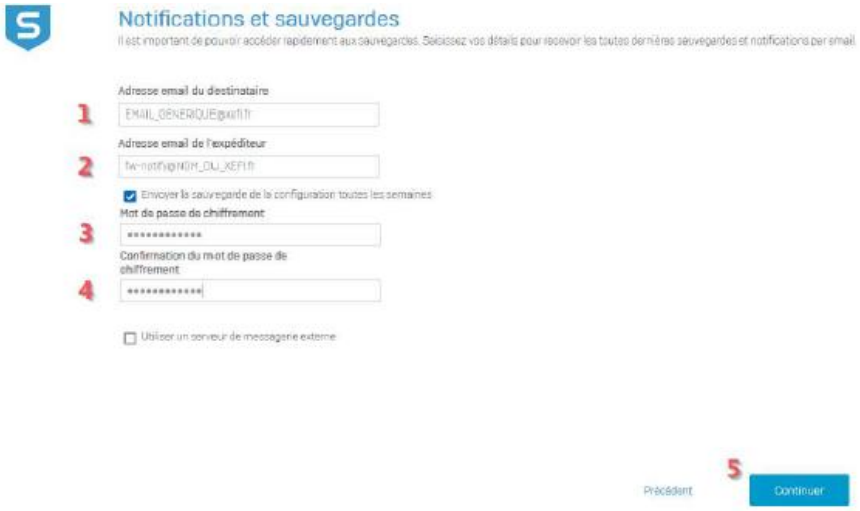
- Activer DHCP si nécessaire.

5. Protection & Sécurité

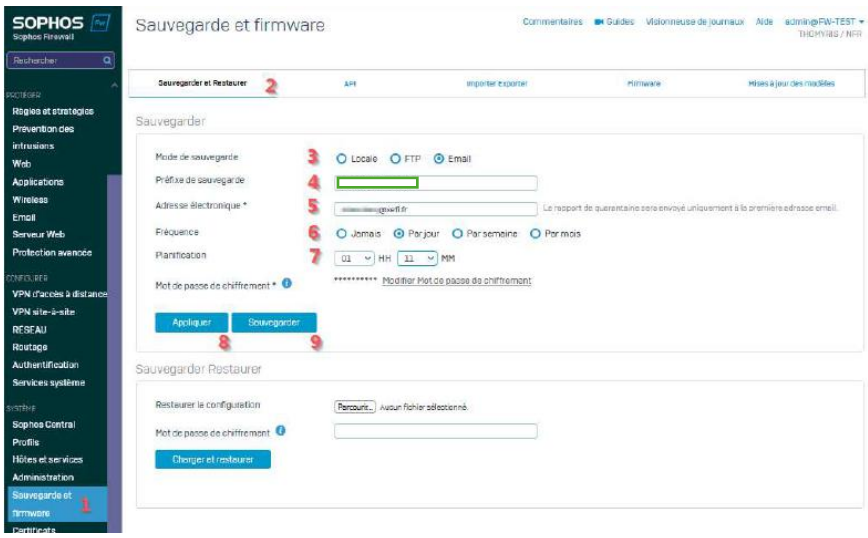
- Activer les protections réseau :
  - IPS (Intrusion Prevention)
  - Web Filtering
  - Zero-Day Protection (si licence Xstream)

6. Notifications & Sauvegardes

- Configurer une adresse email pour les notifications.



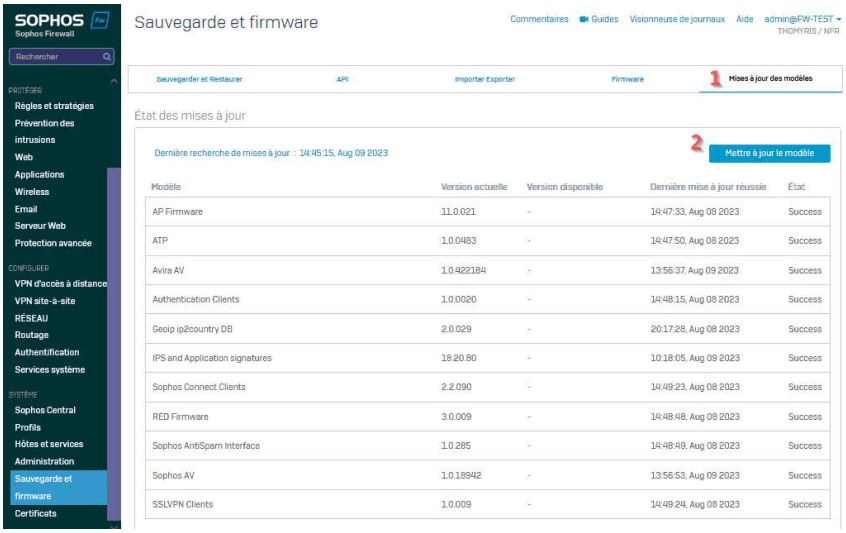
- Planifier des sauvegardes régulières.



- Créer une **clé de stockage sécurisée** (à conserver dans un gestionnaire de mots de passe).

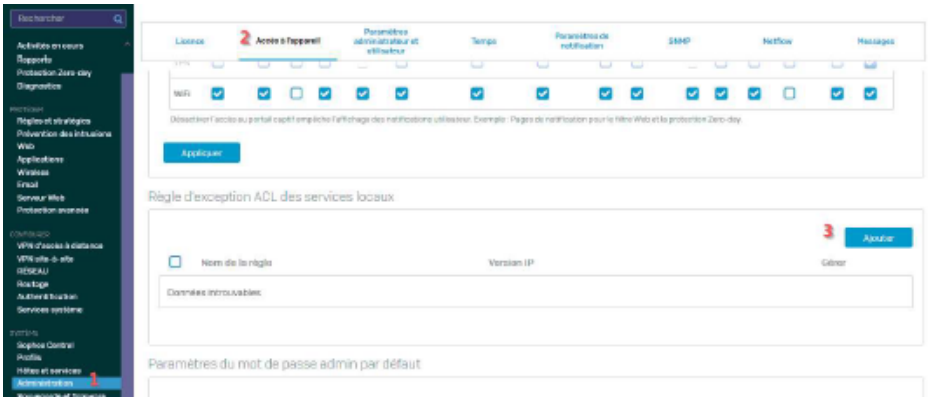
7. Mise à Jour

- 7.1:**Mettre à jour le firmware et les modèles via l'interface.**
  Aller dans l'onglet « Mises à jour des modèles »
  Cliquer sur « Mettre à jour le modèle »



8. Accès à Distance

- Configurer les ACL pour autoriser l'accès distant.



- Ajouter les noms de domaine ou IP publiques nécessaires.
  (En l'occurrence ici l'IP publique de l'agence de xefi Pornic).

9. SERVEUR NTP

Il faut absolument mettre en place un serveur NTP, pour cela aller dans la

Section « Administration » :

(1) Aller dans l'onglet « Temps »

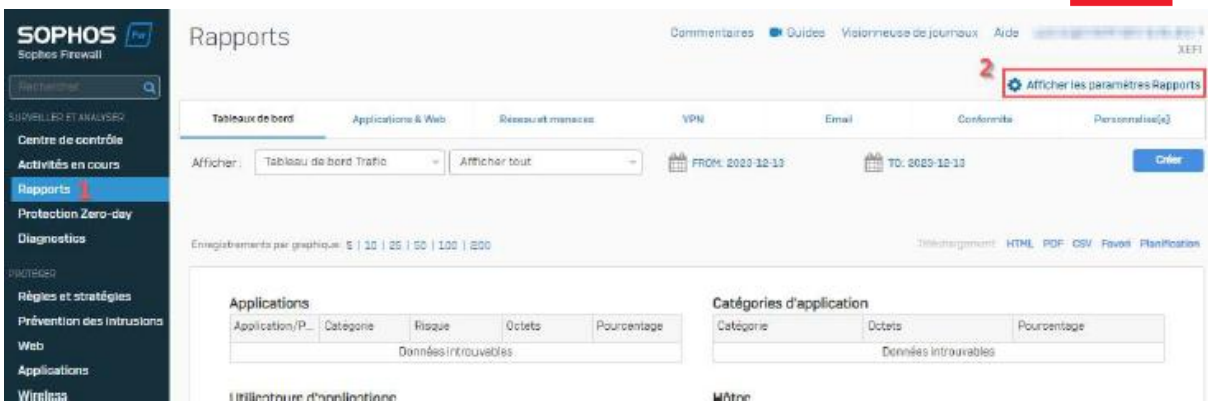
(2) Cocher « Utiliser un serveur NTP prédéfini » et appliquer et redémarrer le Sophos

10. LOGS

Afin de respecter la loi, les logs doivent être conservés 12 mois.

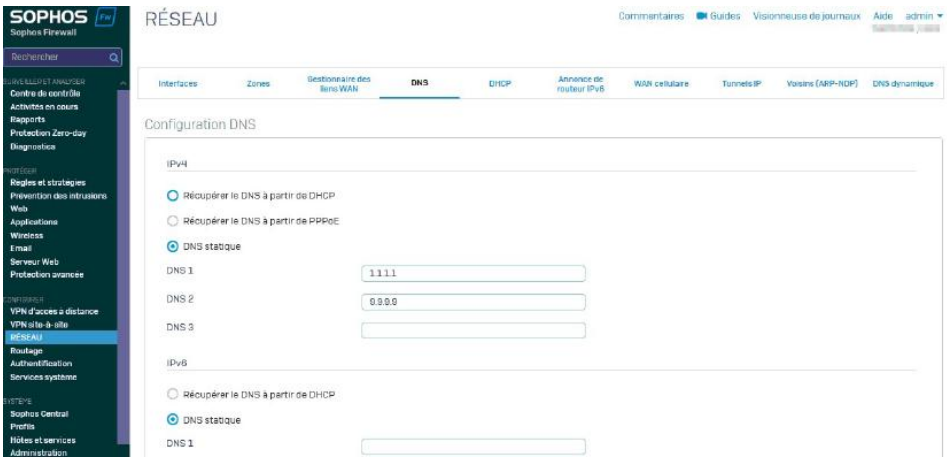
(1) Cliquer sur « Rapports »

(2) Cliquer sur « Afficher les paramètres Rapports »



11. Réseau & Services

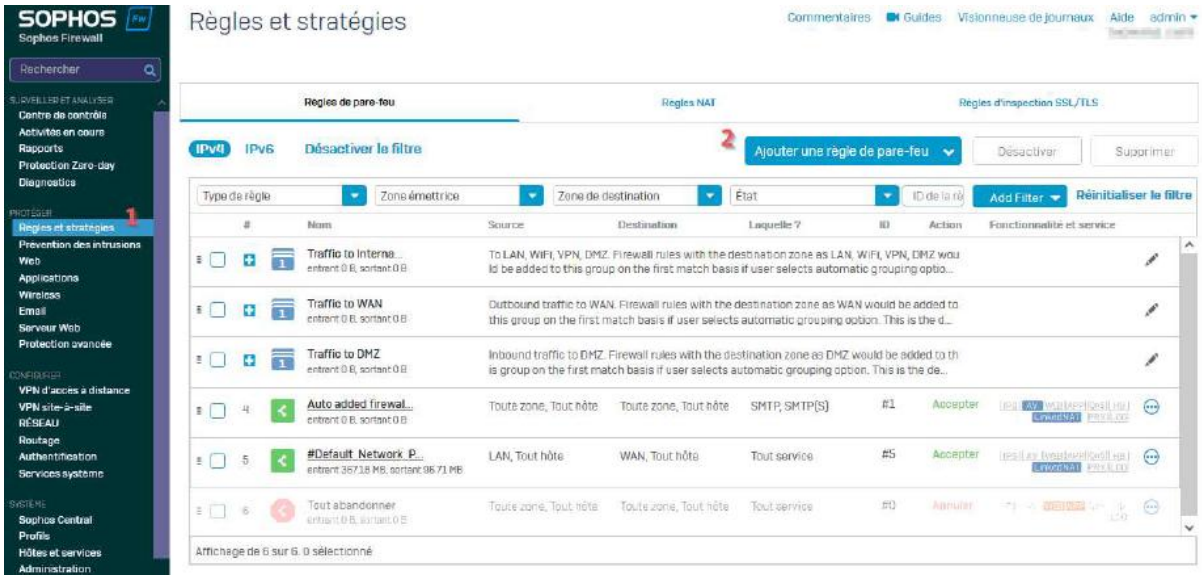
- Configurer le serveur NTP.
- Ajouter les DNS publics (ex: 1.1.1.1 et 9.9.9.9).



12. Règles de Pare-feu

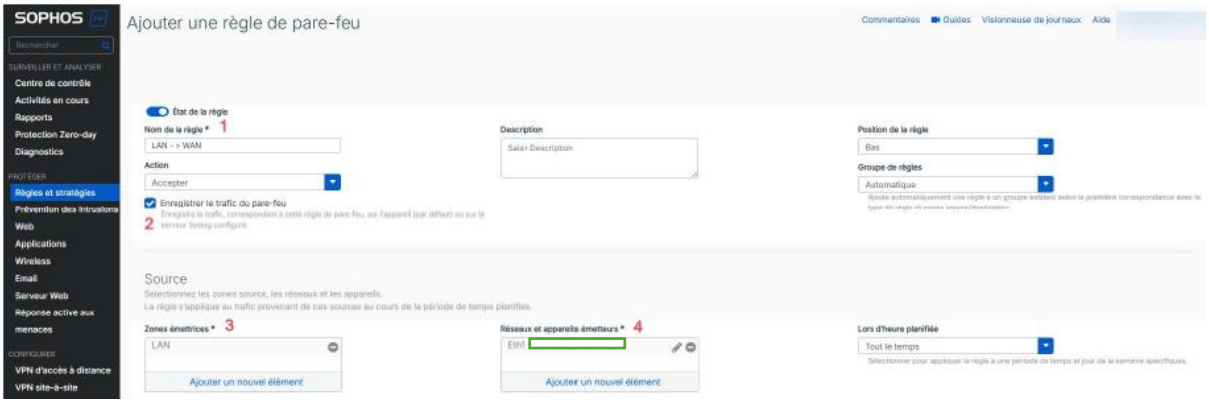
- Créer au minimum deux règles :

(1) Aller dans « Règles et stratégies »

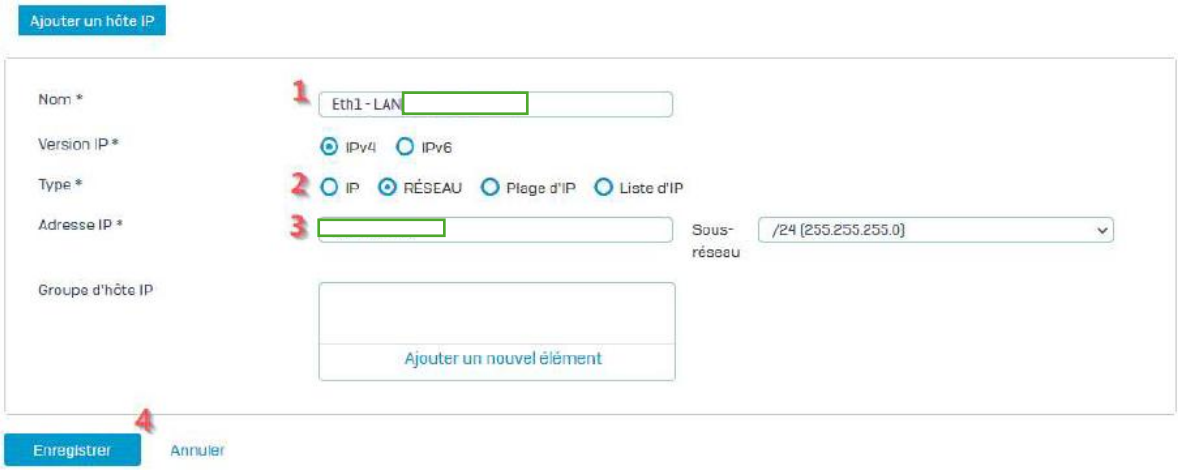


(2) Cliquer sur « Ajouter une règle de pare-feu »

- **LAN → WAN** : journalisation activée, services essentiels (DNS, HTTP, HTTPS, etc.).
- **LAN → WAN (Web Filtering)** : appliquer la stratégie Web, journalisation activée.



- (1) Nommer la règle de pare-feu
- (2) Activer la journalisation
- (3) Zone émettrice sélectionner LAN
- (4) « Réseaux et appareils émetteurs » cliquer sur « Ajouter un nouvel élément » > « Ajouter » > « RESEAU »



(1) Entrer le nom du réseau et son RESEAU
Exemple : Eth1-LAN (192.168.12.0/24)
Dans « Zone de destination » cliquer sur « Ajouter un nouvel élément » et choisir « WAN »

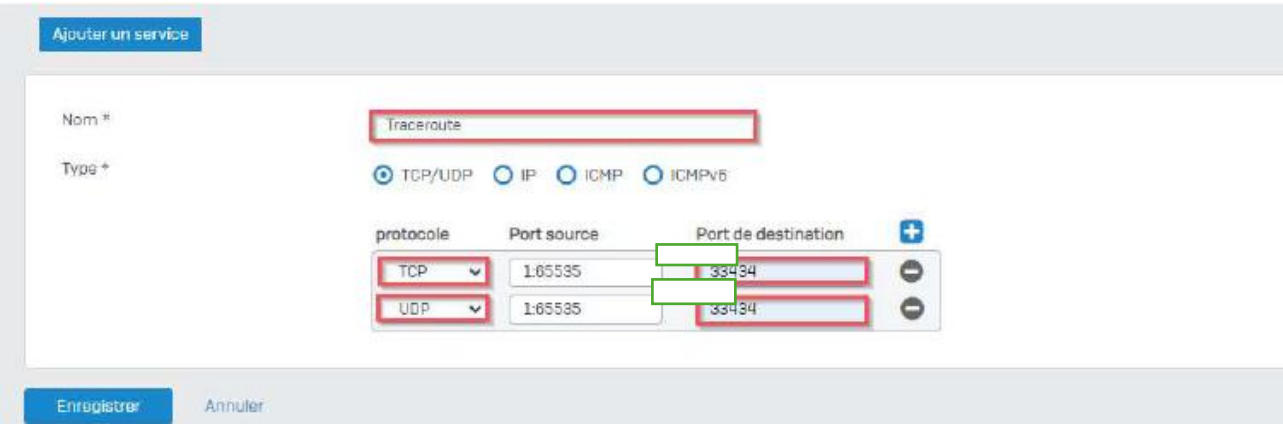
(2) Dans « Réseaux de destination cliquer sur « Ajouter un nouvel élément » et ajouter l'objet

« Internet IPv4 group »

(3) Cliquer sur « Ajouter un nouvel élément » et ajouter le service DNS

Cliquer sur « Ajouter un nouvel élément » puis sur « Ajouter » et enfin « Services »

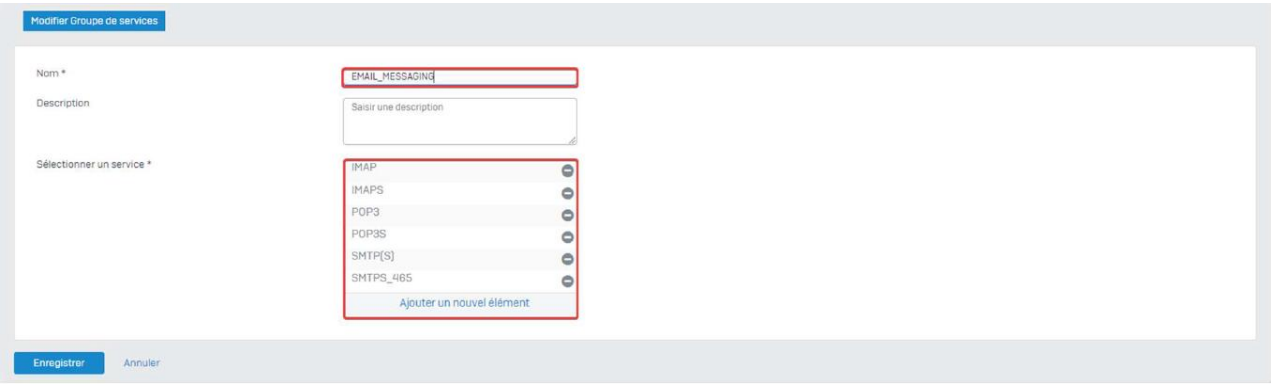
> Créer le service Traceroute



Cliquer sur « Ajouter un nouvel élément » puis sur « Ajouter » et enfin « Groupe de Services »

> Créer le groupe Email Messaging et ajouter les services IMAP / IMAPS / POP3 / POP3S / SMTPS_465

/ SMTP(S)

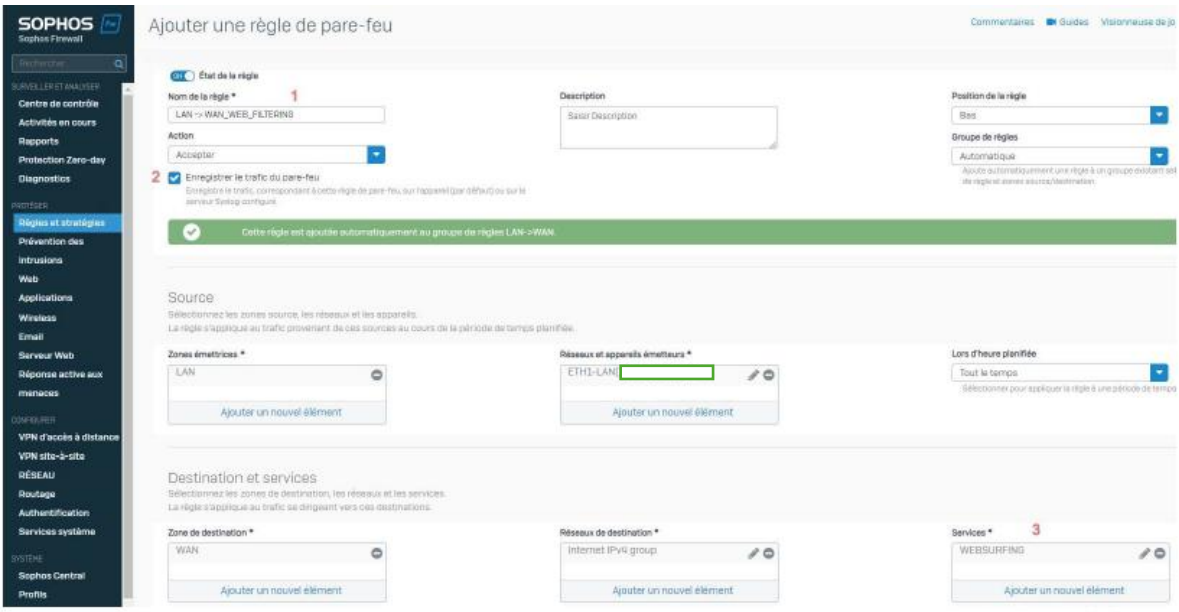


(1) Tout en bas de la page, au niveau de « Autres fonctionnalités de sécurité » dans « Détecte et

Empêche les exploits » sélectionner « LAN TO WAN »

LA DEUXIEME REGLE DE PARE-FEU SERT POUR LE FILTRAGE WEB

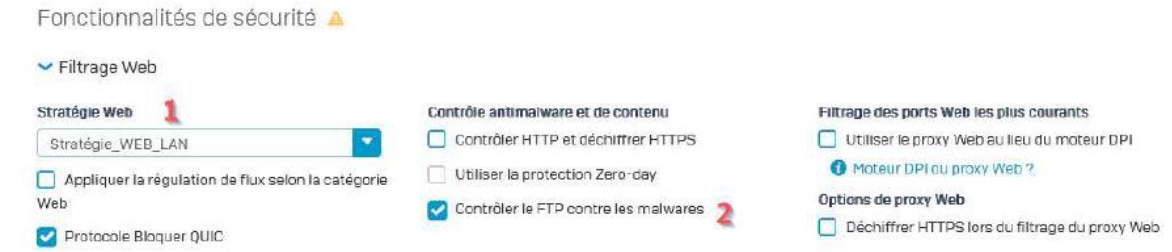
Créer la nouvelle règle :



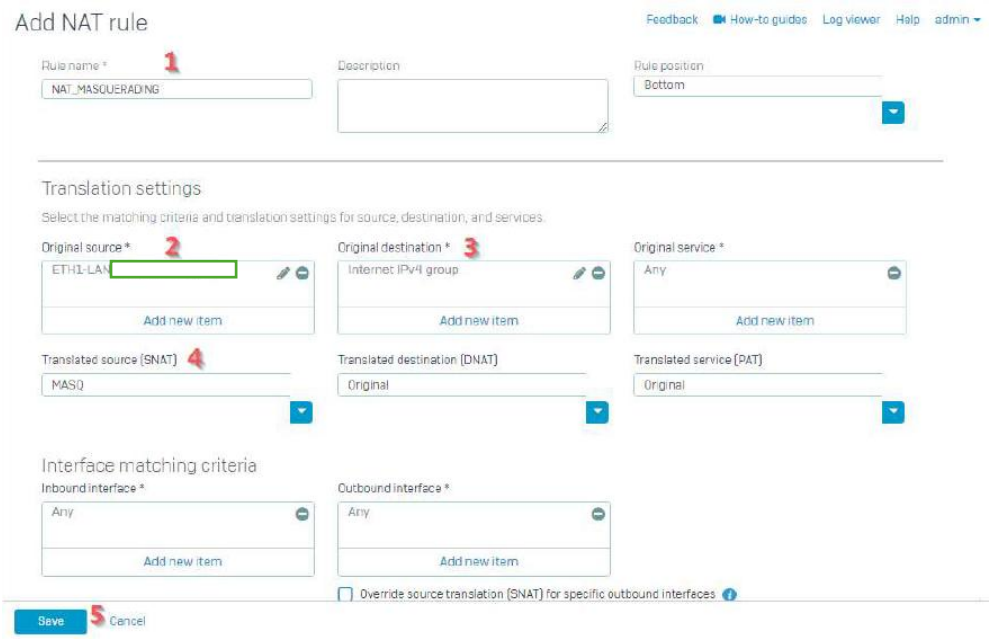
>3 Créer le groupe WebSurfing en ajoutant HTTP et HTTPS

(1) Choisir la « Stratégie Web » précédemment configurer

(2) Cocher « Contrôler le FTP contre les malwares »



Créer la règle NAT masquerading.



(1) Nommer la règle « NAT_MASQUERADING »

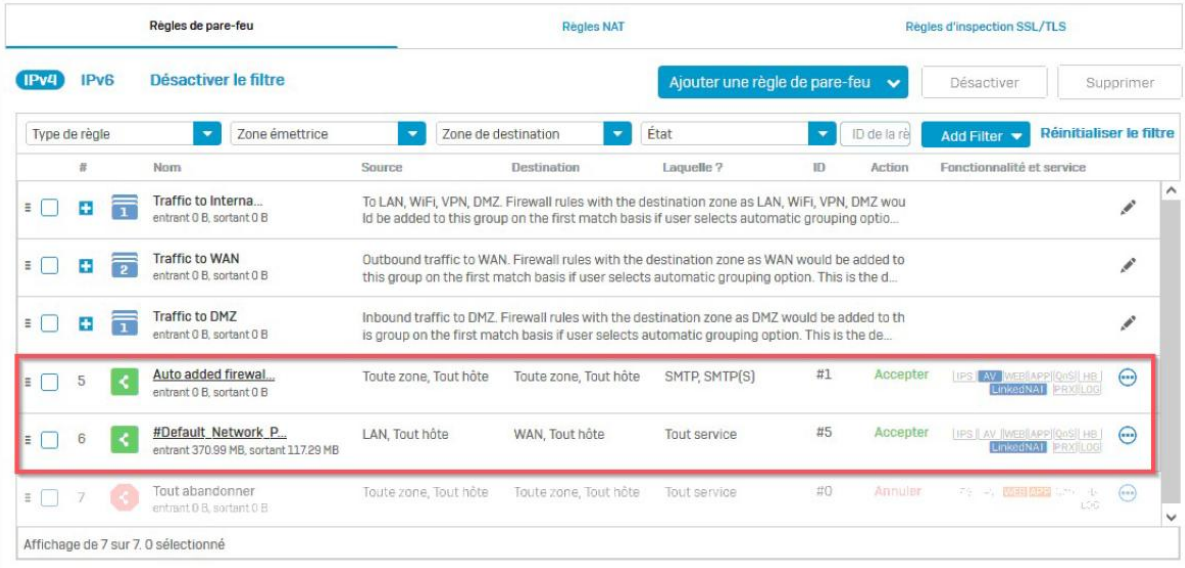
(2) Mettre le réseau LAN

(3) Mettre « Internet IPv4 group »

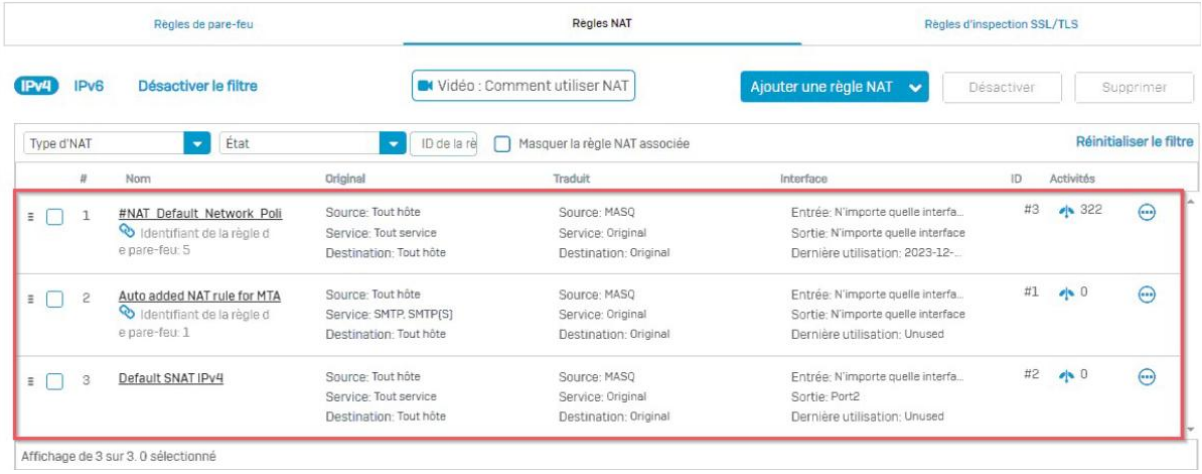
(4) Ajouter « MASQ »

(5) Enregistrer

Supprimer les règles #Default Network et Auto added firewall

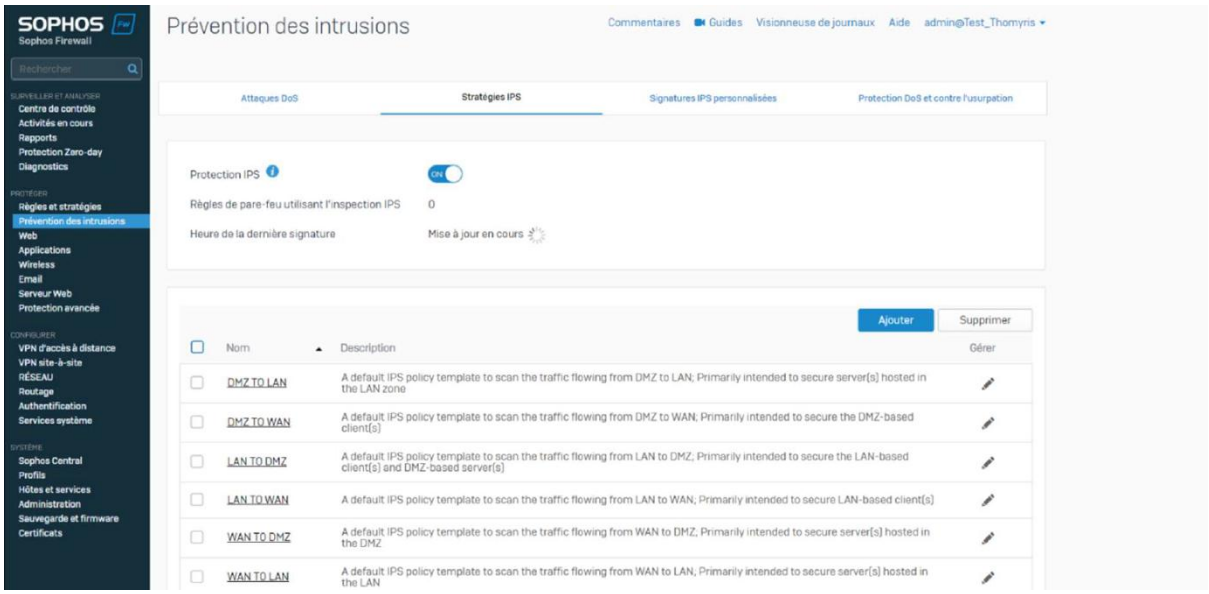


>Supprimer la règle NAT par défaut et les règles associées :



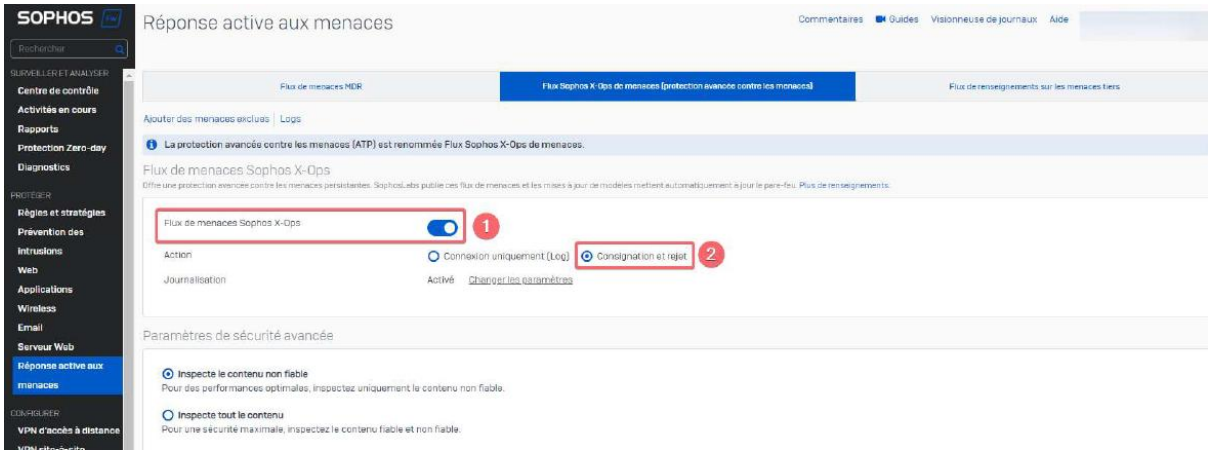
13. ACTIVER L'IPS

Activer la Prévention des intrusions > Stratégies IPS et cocher le bouton ON



14. ACTIVER PROTECTION AVANCEE CONTRE MENACES

Aller dans Réponse active aux menaces puis sur Flux Sophos X-Ops de menaces, mettre le bouton sur ON et sélectionner Consignation et rejet puis cliquer sur Appliquer.



14. VPN SSL Nomade

a. Création des utilisateurs

- Aller dans **Authentification** → Ajouter.
- Renseigner :
  - Nom d'utilisateur
  - Nom complet
  - Mot de passe sécurisé
  - Adresse email
  - Groupe d'appartenance

b. Activer la double authentification

- Aller dans **Authentification multifacteur**.
- Activer pour tous les utilisateurs.
- Cocher "Portail VPN" et "Accès à distance VPN SSL".

c. Configuration du VPN SSL

- Aller dans **VPN d'accès à distance** → SSL VPN → Ajouter.
- Définir :
  - Nom du VPN
  - Utilisateurs autorisés
  - Réseaux accessibles (ex: LAN)
- Aller dans **Paramètres généraux SSL VPN** :
  - Mettre le port à **443**
  - Définir un nom d'hôte ou IP publique si nécessaire

d. Règle de pare-feu pour le VPN

- Créer une règle **VPN → LAN** :
  - Source : zone VPN
  - Destination : LAN
  - Services : tous ou spécifiques
  - Journalisation activée

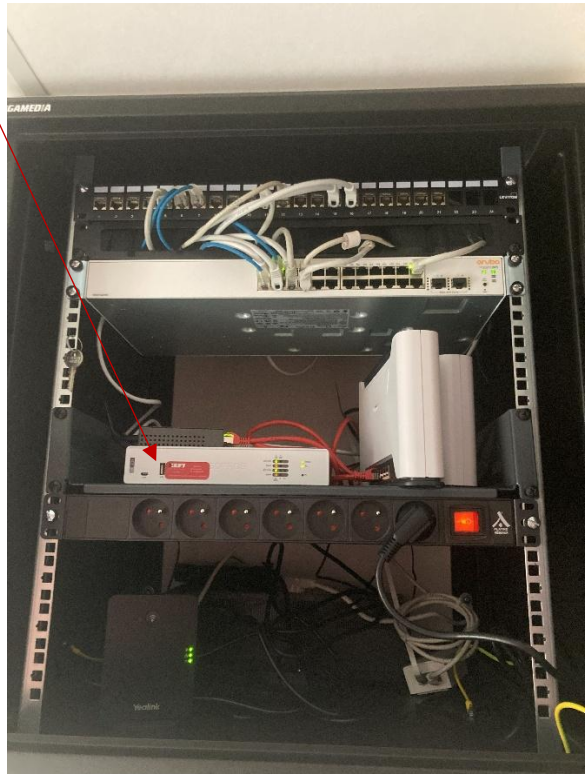
e. Connexion utilisateur

- Se connecter à l'IP publique du firewall via HTTPS.
- Télécharger le client Sophos Connect et le fichier de configuration.
- Se connecter avec identifiant + mot de passe + code MFA.

Aucune règle de l'ancien pare-feu n'a été retenue, car elles étaient soit obsolètes, soit inadaptées aux besoins actuels. Nous avons donc décidé de repartir sur une configuration propre en ne recréant que les règles réellement nécessaires.

Si certains accès sont bloqués, le client n'aura qu'à appeler pour créer une règle permettant de les débloquer.

Photo du nouveau pare-feu après son installation chez le client par mon collègue.



Développement personnel :

Cette expérience a été particulièrement enrichissante dans le cadre de mon BTS SIO. Elle m'a permis de développer plusieurs compétences essentielles :

- Compréhension et mise en œuvre de solutions de sécurité réseau, notamment à travers l'architecture d'un pare-feu NGFW.
- Méthodologie de préparation du matériel : mise à jour du firmware, tests fonctionnels, vérifications avant déploiement.
- Rigueur et autonomie, car j'ai dû suivre une procédure tout en prenant des initiatives lorsque cela était nécessaire.
- Travail en équipe, en collaborant avec mes collègues pour préparer l'équipement avant l'installation finale chez le client.
- Adaptation au contexte professionnel, en répondant à un besoin réel lié à la sécurité et à la continuité de service.

Conclusion :

Cette mission m'a permis de mettre en pratique mes connaissances en administration et sécurisation des infrastructures réseaux dans un contexte professionnel concret. La préparation du nouveau pare-feu a constitué une étape essentielle pour assurer une transition fluide et sûre depuis l'ancien équipement Sophos, tout en garantissant au client une solution moderne, fiable et conforme aux standards actuels de cybersécurité.

Grâce à ce projet, j'ai renforcé mes compétences techniques, notamment dans la configuration d'un pare-feu de nouvelle génération, la gestion des mises à jour, la création de règles de filtrage et l'activation de licences. J'ai également pu développer ma rigueur, mon autonomie et ma capacité à collaborer avec mes collègues afin de préparer un matériel opérationnel avant son installation finale.

Cette expérience s'inscrit pleinement dans la continuité de ma formation en BTS SIO, en me confrontant à des situations professionnelles authentiques et à des enjeux de sécurité réels. Elle contribue ainsi à enrichir mes compétences et à consolider ma capacité à intervenir efficacement dans la mise en œuvre de solutions techniques adaptées aux besoins des clients.

Second projet : Installation Switch Aruba Instant On, Borne Wi-Fi et Onduleur.

Contexte d'intervention :

Dans le cadre de ma mission, j'ai été chargé d'améliorer l'infrastructure réseau d'un client qui rencontrait plusieurs problèmes de stabilité, d'organisation et de couverture Wi-Fi. Lors de mon analyse, j'ai constaté que le client ne disposait pas de switch : tous les équipements étaient connectés directement sur la box Orange, ce qui limitait fortement la capacité du réseau, rendait les connexions instables et compliquait la gestion quotidienne.

Pour corriger ces dysfonctionnements et fournir une base réseau plus fiable, j'ai décidé d'installer un switch Aruba Instant On, une borne Wi-Fi Aruba Instant On, ainsi qu'un onduleur afin de sécuriser toute l'installation.
Le réseau reste volontairement simple, sans VLAN, car le client n'a pas de besoin de segmentation à ce jour, mais l'installation est pensée pour être évolutive.

Référence des équipements utilisé :

HPE Networking Instant On Switch série 1930 8 ports :

HPE Networking Instant On AP32

Onduleur Schneider Electric BVS1000I-GR 1000VA, 600W

Mise en place d'une infrastructure réseau propre et centralisée (Switch Aruba Instant On) :

La box Orange servait à la fois de routeur, de point d'accès Wi-Fi et de switch. Cette configuration posait plusieurs problèmes :

- Nombre limité de ports,
- Saturation du trafic,
- Impossibilité de gérer ou superviser les connexions,
- Câblage désorganisé,
- Difficultés de dépannage.

Pour remédier à cela, j'ai installé un switch Aruba Instant On dans la baie réseau. Grâce à ce switch, je peux désormais :

- Centraliser tout le câblage au même endroit,
- Stabiliser le réseau en utilisant un matériel professionnel,
- Connecter proprement tous les postes et périphériques,
- Administrer le switch à distance via l'interface Aruba Instant On,
- Surveiller les ports, le trafic et l'état du réseau en temps réel,
- Laisser la possibilité d'ajouter des VLAN plus tard si le client en exprime le besoin.

Cette étape était indispensable pour remplacer la fonction de commutation de la box Orange, trop limitée pour un usage professionnel.

Amélioration de la couverture Wi-Fi avec une borne Aruba Instant On :

Le Wi-Fi fourni par la box était insuffisant : faible portée, instabilité et débit irrégulier. Pour offrir au client un Wi-Fi professionnel, j'ai installé une **borne Aruba Instant On**.

Cette installation permet désormais :

- Une couverture Wi-Fi homogène dans l'ensemble des locaux,
- Un débit stable et adapté aux besoins professionnels,
- Une gestion simplifiée via la même plateforme cloud qu'avec le switch,

- Une meilleure sécurité du réseau sans fil,
- Une future possibilité de créer un réseau invité si nécessaire.

La borne fonctionne en complément du switch, ce qui assure une infrastructure cohérente et performante.

Synchronisation dans instant on du switch et de la borne :

Avant de procéder à l'installation physique des équipements, j'ai dû préparer la configuration depuis l'interface de gestion Aruba Instant On. Cette étape est essentielle pour garantir que le switch et la borne fonctionnent correctement une fois déployés sur site.

Dans un premier temps, j'ai synchronisé le switch dans l'interface afin qu'il soit automatiquement reconnu, supervisable et administrable à distance. J'ai ensuite réalisé la même opération pour la borne Wi-Fi, ce qui m'a permis de préparer l'ensemble de la configuration avant son installation réelle.

Synchronisation d'un Switch Instant On sur le portail Instant On :

Étape 1 : Créer un site sur le portail Instant On

Prérequis :

. Le switch est sous tension et connecté au réseau.

. Avoir un compte HPE Instant On.

Étapes :

Connectez-vous sur le portail Instant On.

Cliquez sur Créer un site ou Ajouter un site.

Saisissez les informations du site :

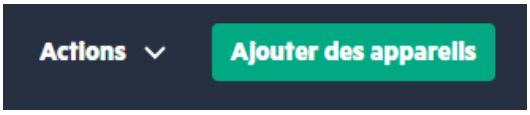
- Nom du site (ex : « Bureau Principal »)
- Adresse et localisation (optionnel mais recommandé pour gestion multi-sites)

Validez la création du site.

Étape 2 : Ajouter un switch Instant On au site

1. Branchez le switch au réseau et sous tension.

2. Si le switch est neuf, il devrait apparaître automatiquement dans le portail sous Appareils disponibles.
3. Dans le portail, allez dans Ajouter un appareil → Switch.



4. Sélectionnez le switch détecté et assignez-le au site que vous venez de créer.
5. Le portail provisionne automatiquement le switch.

Étape 3 : Ajouter une borne Wi-Fi Instant On au site

1. Branchez la borne Wi-Fi sur le réseau et sous tension.
2. Si la borne est neuve, elle devrait apparaître automatiquement dans le portail.
3. Dans le portail, allez dans Ajouter un appareil → Access Point.
4. Sélectionnez la borne détectée et assignez-la au même site.
5. Une fois la synchronisation faite, vous devriez avoir ceci dans les appareils:

Cela indique qu'ils sont bien synchronisés au réseau et aux sites.

Mise en place de réseaux pour les invités et les employés :

Une fois les équipements synchronisés, j'ai créé deux réseaux Wi-Fi distincts :

- Un premier réseau destiné aux employés, offrant un accès complet aux ressources internes de l'entreprise ;
- Un second réseau réservé aux invités, configuré avec des restrictions afin de limiter les accès uniquement à Internet et d'assurer la sécurité du réseau professionnel.

Cette préparation en amont permet d'arriver sur site avec une solution déjà opérationnelle, ce qui facilite le déploiement et réduit les risques d'erreurs lors de l'installation finale.

Créer un réseau Wi-Fi Employé et Invité sur Instant On :

Prérequis :

- Switch et borne Wi-Fi déjà synchronisés avec le site sur le portail Instant On.

Étape 1 : Créer le réseau Employé :

1. Connectez-vous sur le portail Instant On et sélectionnez le site correspondant.
2. Allez dans Réseaux Wi-Fi → Ajouter un réseau Wi-Fi.
3. Configurez le réseau Employé :
   Nom : par exemple « Entreprise-Employés »
   Sécurité : WPA2/WPA3

   VLAN (optionnel) : dans notre cas le réseau reste volontairement simple, sans VLAN, car le client n'a pas de besoin de segmentation à ce jour.

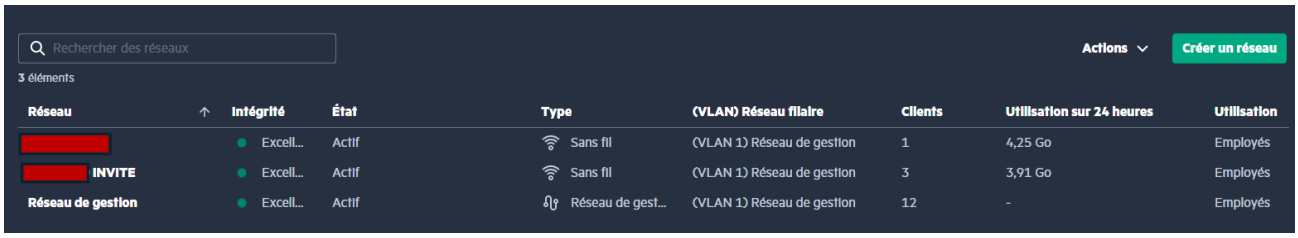
   4. Activez le réseau et appliquez les paramètres.

Étape 2 : Créer le réseau Invité :

1. Toujours dans Réseaux Wi-Fi, cliquez sur Ajouter un réseau Wi-Fi.
2. Configurez le réseau Invité :
   . Nom : par exemple Entreprise-Invités
   . Sécurité : WPA2/WPA3
   . Mot de passe : optionnel
3. Appliquez les paramètres.

Étape 3 : Vérifier et tester :

1. Assurez-vous que les deux réseaux apparaissent comme ci-dessous :



2. Connectez un appareil à chaque réseau pour vérifier la connexion et

   L'accès approprié :

Réseau Employé → accès complet aux ressources internes.

Réseau Invité → accès limité à Internet uniquement.

Intervention chez le client– Installation du réseau :

Étape 1 : Installation de l'onduleur :

1. Étape 1 : Installation de l'onduleur

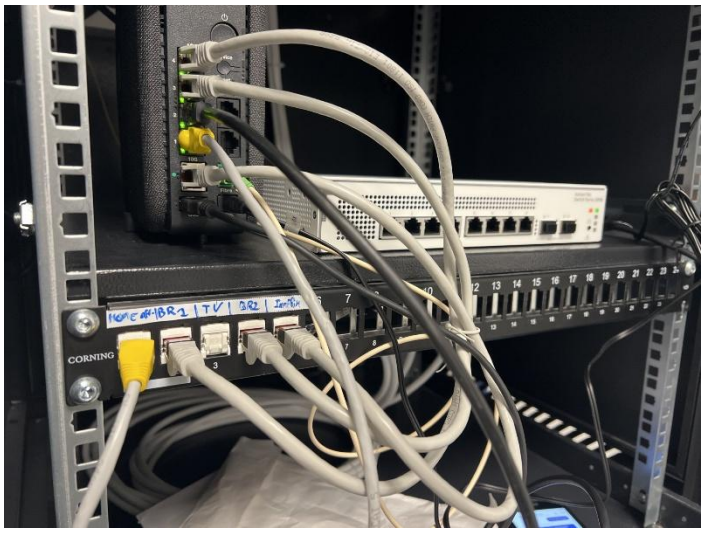
2. Installation de l'onduleur dans la baie pour sécuriser l'alimentation du Réseau.

3. Connexion de l'onduleur à une multiprise sur laquelle étaient déjà reliés Les appareils existants du client. Cela a permis de brancher tous les Équipements de la baie sur l'onduleur sans modifier la configuration Initiale.

4. Vérification du fonctionnement de l'onduleur et de l'alimentation des appareils Connectés.

Étape 2 : Installation du switch Aruba Instant On :

1. Repérage des câbles réseau provenant de la box Orange afin de préparer la Migration des connexions vers le switch (Photo en dessous).



2. Installation physique du switch dans la baie réseau.

3. Connexion des câbles repérés sur les ports correspondants du switch.

4. Se connecter sur le portail Instant On pour s'assurer que le switch fonctionne Correctement et que les appareils connectés conservent leur connectivité. Par exemple, j'ai réalisé un scan avec une imprimante connectée en filaire au Réseau, et cela a parfaitement fonctionné.

Étape 3 : Installation de la borne Wi-Fi :

1. Inspection de l'emplacement prévu pour la borne Wi-Fi.
2. Constat que l'architecture du plafond empêchait la fixation, car il n'y avait pas de rail pour monter la borne.
3. Installation réalisée par mon collègue le lendemain : perçage du plafond pour fixer solidement la borne.
4. Connexion de la borne au switch et configuration via le portail Instant On.
5. Vérification que la borne diffuse correctement le Wi-Fi et que les réseaux (Employé et Invité) sont accessibles et fonctionnels.

Résumé des bénéfices de l'intervention :

L'intervention a consisté à améliorer l'infrastructure réseau du client en installant un onduleur, un switch Aruba Instant On et une borne Wi-Fi. L'onduleur a été mis en place pour sécuriser l'alimentation de la baie réseau, en y connectant l'ensemble des équipements existants via une multiprise, afin de protéger le matériel contre les coupures de courant et les variations électriques. Le switch Aruba Instant On a remplacé la fonction de commutation limitée de la box Orange, offrant une gestion plus professionnelle des ports et des connexions filaires. Enfin, la borne Wi-Fi a été installée pour assurer un accès sans fil performant et stable, avec des réseaux distincts pour les employés et les invités, garantissant à la fois sécurité et efficacité.

Une semaine après l'intervention, le client n'a signalé aucun problème et tous les services réseau fonctionnent normalement. De notre côté, aucun dysfonctionnement ou anomalie n'a été relevé lors des vérifications post-installation. Ces éléments confirment que l'infrastructure mise en place répond pleinement aux besoins du client, assurant à la fois performance, sécurité et fiabilité pour un usage professionnel quotidien.

Principales sources / documentation

- HPE Networking Instant On – User Guide
  Ce guide utilisateur donne des instructions détaillées pour configurer et gérer les équipements Instant On (switches, points d'accès, etc.). HPE Aruba Networking+1
- Aruba Instant On Deployment Guide
  Document de déploiement destiné aux PME : il donne des recommandations de configuration, choix de matériel, bonnes pratiques réseau pour des installations professionnelles. Aruba Instant On
- Portail de documentation d'Aruba Instant On
  Site officiel listant tous les guides d'installation, hardware documentation, guides de démarrage, manuels pour switches, points d'accès, gateways, etc. Utile pour trouver la documentation selon le modèle utilisé.

CONCLUSION FINALE :

Au terme de cette année d'alternance au sein de XEFI Pornic, j'ai pu acquérir une expérience professionnelle riche et directement liée aux compétences attendues dans le cadre du BTS SIO option SISR. Les différentes missions qui m'ont été confiées m'ont permis de travailler sur des environnements variés, allant de la préparation de pare-feu Sophos XGS à l'installation complète d'infrastructures réseau incluant switchs, bornes Wi-Fi et onduleurs.

Ces projets m'ont permis d'approfondir mes compétences en sécurité informatique, en administration réseau et en déploiement d'infrastructures professionnelles. J'ai pu développer une méthodologie rigoureuse, apprendre à anticiper les problèmes potentiels et assurer une mise en service fiable et sécurisée pour les clients. Ils m'ont également offert l'opportunité de renforcer mon autonomie, ma capacité d'analyse et ma collaboration avec l'équipe technique.

Cette alternance m'a confirmé mon envie de poursuivre dans le domaine des réseaux et de la cybersécurité. Les connaissances et compétences acquises au sein de XEFI constituent désormais une base solide pour la suite de mon parcours professionnel. Je ressors de cette expérience mieux préparée à intervenir sur des environnements complexes, tout en restant attentif aux enjeux de sécurité, de performance et de qualité de service.