

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 :

- 1. Présentation personnelle**
- 2. Présentation de l'entreprise XEFI Pornic**
- 3. Remerciements**
- 4. Organigrammes de l'entreprise**
- 5. Mes missions en alternance**
  - 5.1 Rôle global du technicien informatique**
  - 5.2 Installation et configuration de matériel informatique**
  - 5.3 Sécurisation et réseau**
  - 5.4 Administration et services cloud**
  - 5.5 Documentation et communication**
- 6. Compétences mobilisées (BTS SIO – SISR)**
- 7. Outils et technologies utilisés**
- 8. Projet 1 : Initialisation et Configuration d'un pare-feu Sophos XGS**
  - 8.1 Contexte du projet**
  - 8.2 Objectifs**
  - 8.3 Analyse et préparation**
  - 8.4 Procédure d'initialisation (étapes détaillées)**
  - 8.5 Mise en place du VPN SSL**
  - 8.6 Développement personnel**
  - 8.7 Conclusion du projet**
- 9. Projet 2 : Installation Switch Aruba Instant On, borne Wi-Fi et onduleur**
  - 9.1 Contexte d'intervention**
  - 9.2 Équipements installé**
  - 9.3 Synchronisation dans Instant On**
  - 9.4 Création des réseaux Employés / Invités**
  - 9.5 Intervention chez le client**
  - 9.6 Résultats et bénéfices**
- 10. Sources / documentation**
- 11. Conclusion générale**

## 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 XIFI 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.

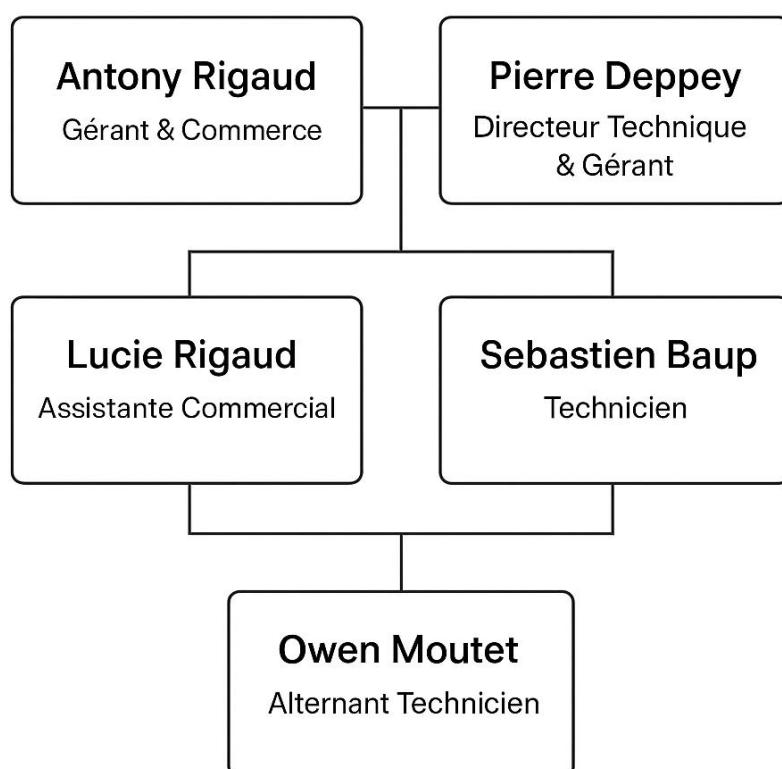


**Remerciements :**

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 XIFI 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 XIFI

## 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 :

Obtenir une adresse IP automatiquement  
 Utiliser l'adresse IP suivante :

Adresse IP :	172 . 16 . 16 . 100
Masque de sous-réseau :	255 . 255 . 0 . 0
Passerelle par défaut :	172 . 16 . 16 . 16

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.

This screenshot shows the first step of the 'Configuration basique' (Basic Configuration) wizard. It asks for the creation of a new administrator account. The fields required are 'Nouveau mot de passe de l'administrateur par défaut:' (step 1) and 'Saisir de nouveau le mot de passe Admin:' (step 2). There is also a checkbox for 'Instaler automatiquement le dernier firmware lors de la configuration (recommandé)'. At the bottom right, there are 'Précédent' and 'Continuer' buttons.

- Connecter le port WAN (Eth2) à Internet.

## 4. Paramètres de Base

- Nommer le firewall selon votre convention [FW-XEFI\_PORNIC\_(.....)].

**Name and time zone**

Enter a firewall name. We recommend that you use a fully qualified domain name (FQDN) that points to this device.

1 Firewall name: FW-AG\_XEFI-NOM\_CLIENT

Time zone: Europe/Paris

Current time: Tuesday, August 8, 2023, 11:38 AM

2

3 Previous Continue

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

**Configuration Réseau [LAN]**

Selectionnez les ports, le mode de déclassement et comment assigner les adresses IP.  
Vous êtes actuellement connecté à "Port1".

Ports: Cliquez sur pour sélectionner ou désélectionner les ports. Le pare-feu régit les ports sélectionnés. En mode routage, le port WAN n'est pas relié aux autres.

1	2	3	4
5	6	7	8
9	10	11	12

■ Connecté ■ Activer pour la LAN ■ Activer pour la WAN ■ Non configuré Port Réseautisé Désactivé

Choisir la passerelle:

1 Adresse IP LAN:  2 Masque de sous-réseau: /24 (jusqu'à 254 appareils client)

Modifier la connexion Internet:

Activer DHCP Le pare-feu attribue les adresses IP à vos appareils internet.

Génére de bail DHCP:

3

Précédent Continuer

- Activer DHCP si nécessaire.

## 5. Protection & Sécurité

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

**S** Protection des réseaux

Vous pouvez configurer les permissions des utilisateurs sur les réseaux câblés et sans fil afin de les protéger lorsqu'ils accèdent à Internet.

1  **Protection des utilisateurs contre les menaces réseau**  
Protège les utilisateurs contre les tentatives d'intrusion. La protection IPS est désactivée par défaut. Pour l'activer, aller dans Prévention des intrusions > Stratégies IPS après avoir terminé la configuration.

2  **Protection des utilisateurs contre les sites Web suspects et malveillants**  
Protège les utilisateurs contre les liens malveillants et les sites dangereux. Il ne contrôle pas le trafic SSL. Cliquez ici pour savoir comment contrôler le trafic HTTPS.

3  **Contrôle antimalware des fichiers téléchargés depuis Internet**  
Même les sites risqués peuvent contenir des fichiers malveillants. Contrôle les fichiers avec la moteur de détection Sophos afin d'interroger les malwares connus et leurs variantes.

4  **Dirige les fichiers suspects vers la protection Zero-day**  
Protège les utilisateurs contre les malwares insinués grâce à des techniques de détection avancée qui implique l'exécution d'applications, la visualisation de documents dans un environnement sain (sandbox) dans le Cloud avant même que les utilisateurs n'aient téléchargé les fichiers sur leurs ordinateurs.

5 Continuer

## 6. Notifications & Sauvegardes

- Configurer une adresse email pour les notifications.

**S** Notifications et sauvegardes

Il est important de pouvoir accéder rapidement aux sauvegardes. Déclarez vos détails pour recevoir les toutes dernières sauvegardes et notifications par email.

1  **Adresse email du destinataire**  
EMAIL\_GENEPIQUE@GMAIL.FR

2  **Adresse email de l'expéditeur**  
TUTO@GMAIL.COM.XEFI.FR

3  **Envoyer la sauvegarde de la configuration toutes les semaines**

4  **Mot de passe de chiffrement**  
\*\*\*\*\*

5  **Confirmation du mot de passe de chiffrement**  
\*\*\*\*\*

Utiliser un serveur de messagerie externe

5 Continuer

- 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 »

Modèle	Version actuelle	Version disponible	Dernière mise à jour réussie	État
AP Firmware	11.0.021	-	14:47:33, Aug 08 2023	Success
ATP	1.0.0463	-	14:47:50, Aug 08 2023	Success
Avira AV	1.0.422184	-	13:56:37, Aug 09 2023	Success
Authentication Clients	1.0.0020	-	14:48:15, Aug 09 2023	Success
Geolip ip2country DB	2.0.029	-	20:17:28, Aug 08 2023	Success
IPS and Application signatures	18.20.80	-	10:18:05, Aug 09 2023	Success
Sophos Connect Clients	2.2.090	-	14:49:23, Aug 08 2023	Success
RED Firmware	3.0.009	-	14:48:48, Aug 08 2023	Success
Sophos AntiSpam Interface	1.0.285	-	14:48:49, Aug 08 2023	Success
Sophos AV	1.0.18842	-	13:56:53, Aug 09 2023	Success
SSLVPN Clients	1.0.008	-	14:49:24, Aug 08 2023	Success

## 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 » :

- Aller dans l'onglet « Temps »
- 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.

- Cliquer sur « Rapports »
- Cliquer sur « Afficher les paramètres Rapports »

The screenshot shows the Sophos Firewall's "Rapports" (Reports) section. The left sidebar includes options like "Centre de contrôle", "Activités en cours", "Rapports" (selected), "Protection Zero-day", "Diagnostics", "Règles et stratégies", "Prévention des intrusions", "Web", "Applications", and "Wireless". The main area displays "Tableaux de bord" and "Applications & Web" tabs. A search bar and date range filters ("FROM: 2020-12-13" to "TO: 2020-12-13") are present. Below the filters, there are two tables: "Applications" and "Catégories d'application", both showing "Données introuvable(s)".

## 11. Réseau & Services

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

The screenshot shows the Sophos Firewall's "Réseau" (Network) configuration section. The left sidebar includes "Centre de contrôle", "Activités en cours", "Rapports", "Protection Zero-day", "Diagnostics", "Règles et stratégies", "Prévention des intrusions", "Web", "Applications", "Wireless", "Email", "Serveur Web", and "Protection avancée". The "Réseau" tab is selected. The main area shows the "DNS" tab of the "Configuration DNS" (DNS Configuration) screen. It includes sections for IPv4 and IPv6, each with radio button options for "Récupérer le DNS à partir de DHCP", "Récupérer le DNS à partir de PPPoE", or "DNS statique", along with input fields for static DNS servers.

## 12. Règles de Pare-feu

- Créer au minimum deux règles :
- (1) Aller dans « Règles et stratégies »

Règles et stratégies

Commentaires | Guidés | Visionneuse de journaux | Aide | admin ▾

**Règles de pare-feu**

Type de règle Zone émettrice Zone de destination État ID de la règle Ajouter une règle de pare-feu ▾ Désactiver Supprimer Add Filter Réinitialiser le filtre

#	Nom	Source	Destination	Laquelle ?	ID	Action	Fonctionnalité et service
1	Traffic to Internal...	entrent 0 B, sortent 0 B	To LAN, WiFi, VPN, DMZ	Firewall rules with the destination zone as LAN, WiFi, VPN, DMZ would be added to this group on the first match basis if user selects automatic grouping option.	#1	Accepter	[REDACTED]
1	Traffic to WAN	entrent 0 B, sortant 0 B	Outbound traffic to WAN	Firewall rules with the destination zone as WAN would be added to this group on the first match basis if user selects automatic grouping option. This is the de...	#1	Accepter	[REDACTED]
1	Traffic to DMZ	entrent 0 B, sortant 0 B	Inbound traffic to DMZ	Firewall rules with the destination zone as DMZ would be added to this group on the first match basis if user selects automatic grouping option. This is the de...	#1	Accepter	[REDACTED]
4	Auto added firewall...	Toute zone, Tout hôte	Toute zone, Tout hôte	SMTP, SMTP[S]	#1	Accepter	[REDACTED]
5	#Default Network P...	LAN, Tout hôte	WAN, Tout hôte	Tout service	#5	Accepter	[REDACTED]
6	Tout abandonner	Toute zone, Tout hôte	Toute zone, Tout hôte	Tout service	#6	Annuler	[REDACTED]

Affichage de 6 sur 6. 0 sélectionné

## (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.

Ajouter une règle de pare-feu

Commentaires | Guidés | Visionneuse de journaux | Aide

Etat de la règle

État de la règle \* 1 LAN -> WAN

Description

Saisir Description

Position de la règle

Bas

Groupe de règles

Automatique

Route automatiquement une règle à un groupe existant selon la première correspondance avec le type de règle ou une correspondance.

Enregistrer le trafic du pare-feu

Traffic de toute correspondance à cette règle de pare-feu, sur l'appareil (par défaut) ou sur le serveur Syslog configuré.

Source

Sélectionnez les zones source, les réseaux et les appareils.

La règle s'applique au trafic provenant de ces sources au cours de la période de temps planifiée.

Zones émettrices \* 3 LAN

Réseaux et appareils émetteurs \* 4 Ethernet

Lors d'une heure planifiée

Tout le temps

Sélectionner pour appliquer la règle à une période de temps et jour de la semaine spécifiques.

- (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 »

Ajouter un hôte IP

Nom *	1 Eth1 - LAN
Version IP *	<input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6
Type *	<input checked="" type="radio"/> IP <input type="radio"/> RÉSEAU <input type="radio"/> Plage d'IP <input type="radio"/> Liste d'IP
Adresse IP *	2 3 <input type="text"/> Sous-réseau /24 [255.255.255.0]
Groupe d'hôte IP	<input type="text"/> Ajouter un nouvel élément

Enregistrer Annuler 4

(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 »

Destination et services

Sélectionner les zones, les réseaux et les appareils de destination.  
Cette règle s'applique au trafic vers ces destinations.

Zone de destination * 1	Réseaux de destination * 2	Services * 3
WAN	Internet IPv4 group	DNS Email Messaging Traceroute
<a href="#">Ajouter un nouvel élément</a>	<a href="#">Ajouter un nouvel élément</a>	<a href="#">Ajouter un nouvel élément</a>

Les services sont des types de trafic basés sur une combinaison de protocoles et de ports.

(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

Ajouter un service

Nom \*

Type \*

protocole	Port source	Port de destination	
TCP	1:65535	33434	-
UDP	1:65535	33434	-

Enregistrer Annuler

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)

Modifier Groupe de services

Nom \*

Description

Sélectionner un service \*

IMAP
IMAPS
POP3
POP3S
SMTP[S]
SMTPS_465

Ajouter un nouvel élément

Enregistrer Annuler

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

Empêche les exploits » sélectionner « LAN TO WAN »

## Autres fonctionnalités de sécurité

### Identifier et contrôler les applications [App Control]

**Aucune**

Appliquer une Stratégie de régulation de flux d'application

### Déetecte et empêche les exploits (IPS) **1**

**LAN TO WAN**

Contrôle le contenu des emails

### Réguler le flux

**Aucune**

### Marquage DSCP

**Sélectionner le marquage DSCP**

## LA DEUXIÈME RÈGLE DE PARE-FEU SERT POUR LE FILTRAGE WEB

### Créer la nouvelle règle :

The screenshot shows the Sophos Firewall interface under the 'Règles et stratégies' tab. A green banner at the top indicates that the rule is applied automatically to the LAN-to-WAN group. The configuration fields include:

- Etat de la règle:** LAN > WAN\_WEB\_FILTERING (highlighted with a red box)
- Action:** Accepter
- Description:** Sans Description
- Position de la règle:** Bas
- Groupe de règles:** Automatique
- Enregistrer le trafic du pare-feu:** Checked (highlighted with a red box)
- Source:** LAN
- Réseaux et appareils émetteurs:** ETH0-LAN
- Lors d'une heure planifiée:** Tout le temps
- Destination et services:** WAN
- Réseaux de destination:** Internet IPv4 group
- Services:** WEBSURFING (highlighted with a red box)

### >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 »

## Fonctionnalités de sécurité **▲**

### Filtrage Web

#### Stratégie Web **1**

- Stratégie\_WEB\_LAN
- Appliquer la régulation de flux selon la catégorie Web
- Protocole Bloquer QUIC

#### Contrôle antimalware et de contenu

- Contrôler HTTP et déchiffrer HTTPS
- Utiliser la protection Zero-day
- Contrôler le FTP contre les malwares **2**

#### Filtrage des ports Web les plus courants

- Utiliser le proxy Web au lieu du moteur DPI
- Moteur DPI ou proxy Web ?

#### Options de proxy Web

- Déchiffrer HTTPS lors du filtrage du proxy Web

## Créer la règle NAT masquerading.

Add NAT rule

Feedback How-to guides Log viewer Help admin ▾

Rule name * <b>1</b>	Description	Rule position
NAT_MASQUERADING		Bottom

---

Translation settings

Select the matching criteria and translation settings for source, destination, and services.

Original source * <b>2</b> ETH1-LAN	Original destination * <b>3</b> Internet IPv4 group	Original service * Any
Add new item	Add new item	Add new item
Translated source [SNAT] <b>4</b> MASQ	Translated destination [DNAT] Original	Translated service [PAT] Original
▼		

---

Interface matching criteria

Inbound interface \* Any

Outbound interface \* Any

Override source translation (SNAT) for specific outbound interfaces **5**

Save Cancel

(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

Règles de pare-feu		Règles NAT		Règles d'inspection SSL/TLS	
IPv4	IPv6	Désactiver le filtre	Ajouter une règle de pare-feu		Désactiver Supprimer
Type de règle	Zone émettrice	Zone de destination	État	ID de la règle	Add Filter Réinitialiser le filtre
#	Nom	Source	Destination	Laquelle ?	ID Action Fonctionnalité et service
<input type="checkbox"/>	<b>1</b> Traffic to Internal... entrant 0 B, sortant 0 B	To LAN, WiFi, VPN, DMZ.	Firewall rules with the destination zone as LAN, WiFi, VPN, DMZ would be added to this group on the first match basis if user selects automatic grouping option.		<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
<input type="checkbox"/>	<b>2</b> Traffic to WAN entrant 0 B, sortant 0 B	Outbound traffic to WAN.	Firewall rules with the destination zone as WAN would be added to this group on the first match basis if user selects automatic grouping option. This is the def...		<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
<input type="checkbox"/>	<b>1</b> Traffic to DMZ entrant 0 B, sortant 0 B	Inbound traffic to DMZ.	Firewall rules with the destination zone as DMZ would be added to this group on the first match basis if user selects automatic grouping option. This is the def...		<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
<input type="checkbox"/>	<b>5</b> Auto added firewall... entrant 0 B, sortant 0 B	Toute zone, Tout hôte	Toute zone, Tout hôte	SMTP, SMTP(S)	#1 Accepter <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
<input type="checkbox"/>	<b>6</b> #Default_Network_P... entrant 370.99 MB, sortant 117.29 MB	LAN, Tout hôte	WAN, Tout hôte	Tout service	#5 Accepter <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
<input type="checkbox"/>	<b>7</b> Tout abandonner entrant 0 B, sortant 0 B	Toute zone, Tout hôte	Toute zone, Tout hôte	Tout service	#0 Annuler <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
Affichage de 7 sur 7, 0 sélectionné					

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

The screenshot shows a list of NAT rules in a firewall configuration interface. The rules are:

- #1: #NAT\_Default\_Network\_Poli (Selected)
- #2: Auto added NAT rule for MTA
- #3: Default SNAT IPv4

Each rule has columns for Type d'NAT, Nom, Original, Traduit, Interface, ID, and Activité. The first rule (#1) is selected, indicated by a red box around its row.

## 13. ACTIVER L'IPS

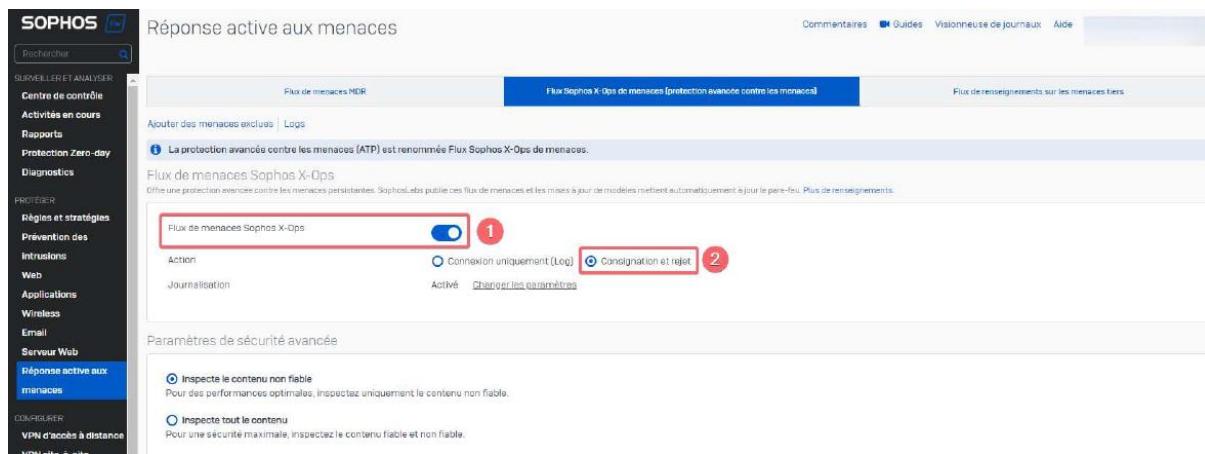
Activer la Prévention des intrusions > Stratégies IPS et cocher le bouton ON

The screenshot shows the Sophos Firewall interface under the 'Prévention des intrusions' section. The 'Stratégies IPS' tab is selected. The 'Protection IPS' toggle switch is turned on. Below it, there are fields for 'Règles de pare-feu utilisant l'inspection IPS' (0) and 'Heure de la dernière signature'. A table lists various IPS policy templates:

Nom	Description	Gérer
DMZ TO LAN	A default IPS policy template to scan the traffic flowing from DMZ to LAN. Primarily intended to secure server(s) hosted in the LAN zone.	
DMZ TO WAN	A default IPS policy template to scan the traffic flowing from DMZ to WAN. Primarily intended to secure the DMZ-based client(s).	
LAN TO DMZ	A default IPS policy template to scan the traffic flowing from LAN to DMZ. Primarily intended to secure the LAN-based client(s) and DMZ-based server(s).	
LAN TO WAN	A default IPS policy template to scan the traffic flowing from LAN to WAN. Primarily intended to secure LAN-based client(s).	
WAN TO DMZ	A default IPS policy template to scan the traffic flowing from WAN to DMZ. Primarily intended to secure server(s) hosted in the DMZ.	
WAN TO LAN	A default IPS policy template to scan the traffic flowing from WAN to LAN. Primarily intended to secure server(s) hosted in the LAN.	

## 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 rejeter 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

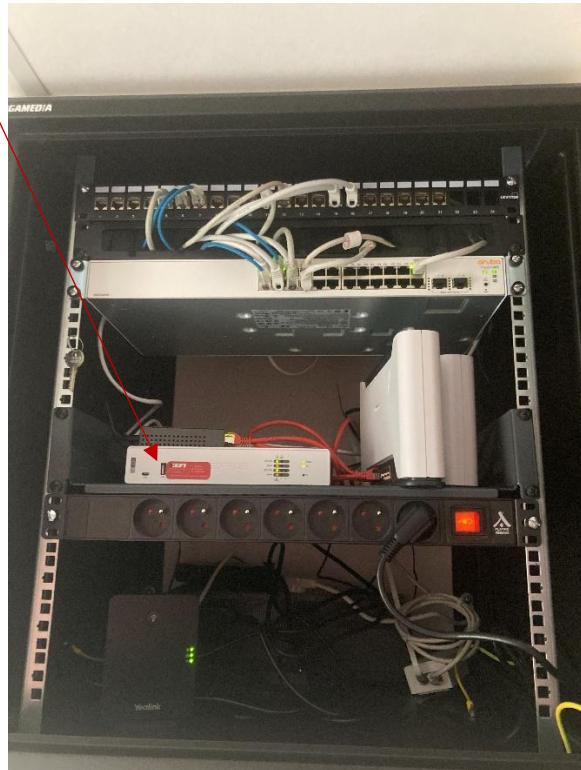
### e. Connexion utilisateur

- 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:

CNTCKPPA18	<span>Excellent</span>	<span>En ligne</span>	4 jours 12 heures	<span>Point d'accès</span>	AP22	a8:ba:25:c8:9a:ce	192.168.1.14	0	...
VN55KYGOH5	<span>Excellent</span>	<span>En ligne</span>	8 jours 10 heures	<span>Commutateur</span>	1830 48G PoE 4SFP 370W	14:ab:ec:60:cd:00	192.168.1.13	12	

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 :

Réseau								Actions	Créer un réseau
	↑	Intégrité	État	Type	(VLAN) Réseau filaire	Clients	Utilisation sur 24 heures	Utilisation	
		● Excell...	Actif	WiFi Sans fil	(VLAN 1) Réseau de gestion	1	4,25 Go	Employés	
INVITE		● Excell...	Actif	WiFi Sans fil	(VLAN 1) Réseau de gestion	3	3,91 Go	Employés	
Réseau de gestion		● Excell...	Actif	WiFi Réseau de gest...	(VLAN 1) Réseau de gestion	12	-	Employés	

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.

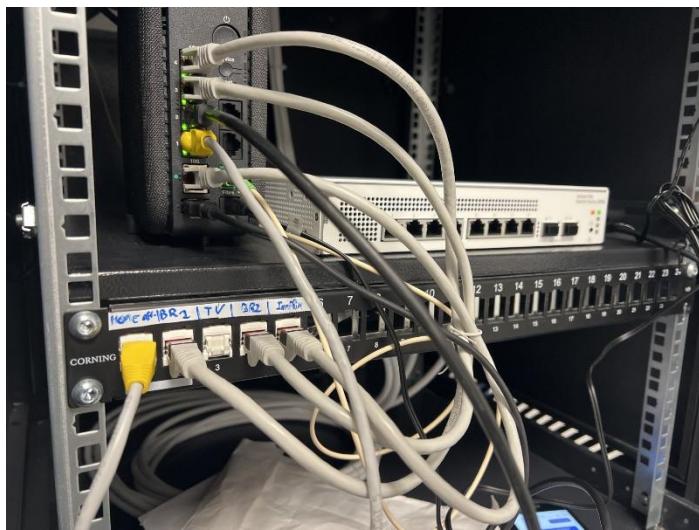
## **Intervention chez le client– Installation du réseau :**

### **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 XIFI 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 XIFI 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.