

**Institut Universitaire de Technologie,  
Aix-Marseille Université**

**Document Annexes  
Bachelor Universitaire de Technologie  
Réseaux et Télécommunications**

**Support utilisateur, préparation de PC et  
installation conseil utilisateur**

**Hugo CARBONNIER**

**Xefi Informatique**

**Tuteur entreprise: Grégory FLAMENT**

**Tuteur Académique: Sébastien SANCHEZ**

**2024**

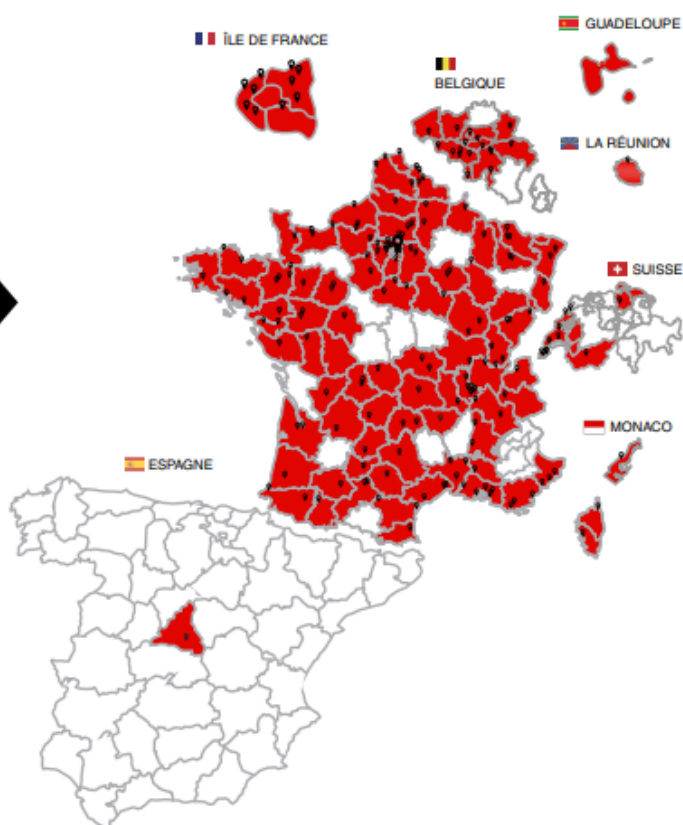


## Table des matières

<b>Annexe 01: Chiffres clés de XEFI</b>	<b>1</b>
<b>Annexes relatives au Firewall Sophos</b>	<b>2</b>
<b>Annexe 02: Interface de gestion des stratégies web</b>	<b>2</b>
<b>Annexe 03 (1/2): Interface pour la création de règle</b>	<b>3</b>
<b>Annexe 03 (2/2): Interface pour la création de règle</b>	<b>3</b>
<b>Annexe 04: Création de la liste noire test</b>	<b>4</b>
<b>Annexe 05: Ajout de la consigne dans la stratégie web</b>	<b>4</b>
<b>Annexe 06: Message d'erreur lorsque le site est bloqué</b>	<b>5</b>
<b>Configuration VPN partie firewall</b>	<b>5</b>
<b>Annexe 07: Création du profil IPsec</b>	<b>5</b>
<b>Annexe 08: Paramètres généraux</b>	<b>6</b>
<b>Annexe 09: Paramètres de la phase 1</b>	<b>6</b>
<b>Annexe 10: Paramètres de la phase 2</b>	<b>7</b>
<b>Annexe 11: Paramètres de chiffrements</b>	<b>7</b>
<b>Annexe 12: Paramètres des passerelles de part et d'autres du tunnel</b>	<b>8</b>
<b>Annexes Relatives à l'installation de l'onduleur</b>	<b>9</b>
<b>Annexe 13: Onduleur SMT3000RMI2UC - APC Smart-UPS</b>	<b>9</b>
<b>Annexe 14: Installation finale de face</b>	<b>10</b>
<b>Annexe 15: Installation finale de derrière</b>	<b>11</b>
<b>Annexe 16: Baie contenant les switchs et le Firewall sophos</b>	<b>12</b>



# CHIFFRES-CLÉS



**+190**

AGENCES DE PROXIMITÉ

**+2 000**

COLLABORATEURS

**+27**

ANS D'EXPÉRIENCE

Annexe 01: Chiffres clés XEFI

# Annexes relatives au Firewall Sophos

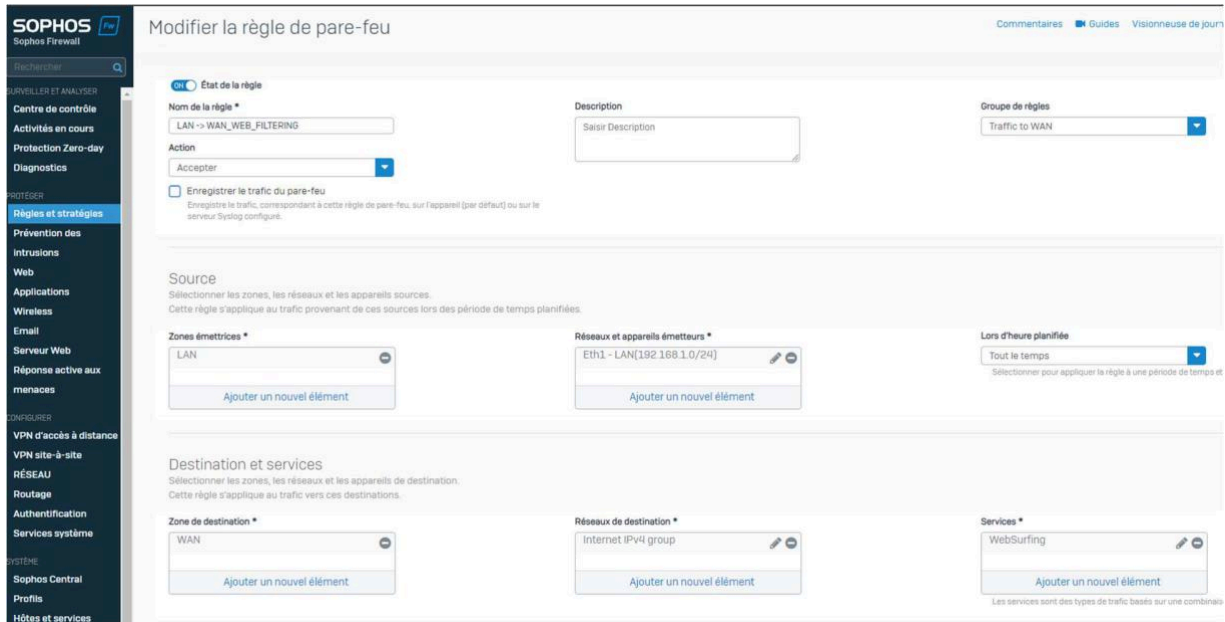
The screenshot displays the Sophos Firewall management interface, specifically the 'Stratégies' (Policies) section for web filtering. The left sidebar contains navigation menus for various system functions. The main content area shows a list of policies and their associated activities.

Stratégies	Etat de la stratégie de quota	Activités de l'utilisateur	Catégories	Groupes d'URL
+ No Games Ads or Explicit Content		Deny access to games, advertisements, and sexually explicit sites		
+ No Online Chat		Deny access to online chat sites		
+ No Web Mail		Deny access to web mail sites		
+ No Web Mail or Chat		Deny access to web mail and online chat sites		
+ No web uploads		Restrict users from uploading content to any site		
- Stratégie_WEB_LAN		Stratégie de Web Filtering pour le réseau LAN TO WAN		

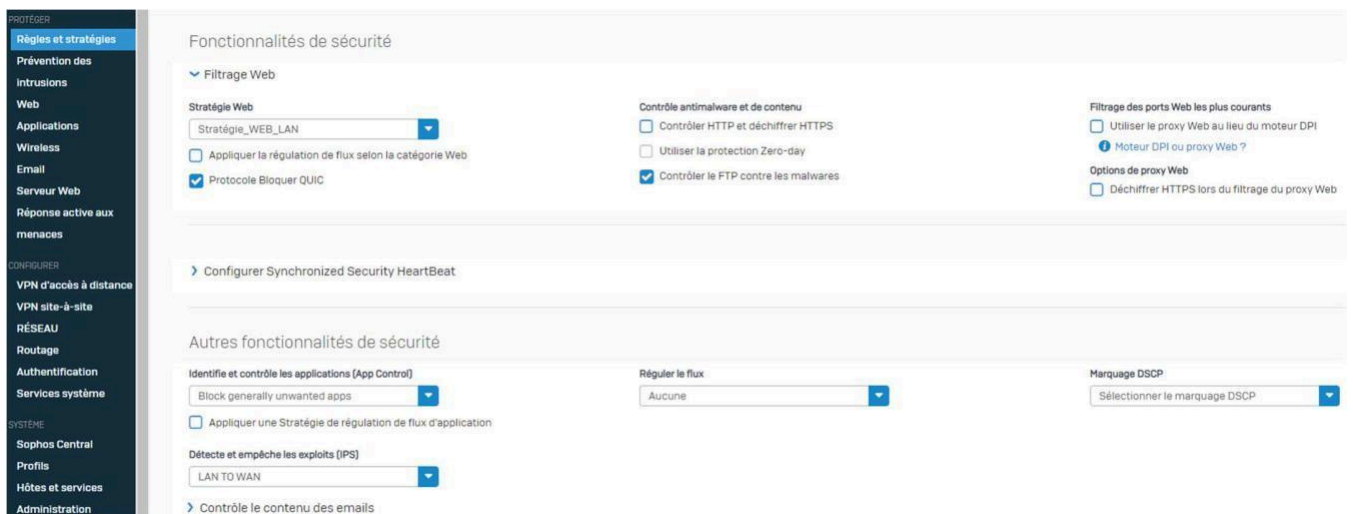
  

Utilisateurs	Activités	Action
N'importe qui	LISTE_BLANCHE	✓
N'importe qui	Bandwidth-heavy Browsing	⚠
	Criminal Activities	⚠
	Drugs and Controlled Subs...	⚠
	Extreme or Violent Web Co...	⚠
	IT Web Content and Servic...	⚠
	<i>1 more ...</i>	
	Action par défaut	✓

Annexe 02: Interface de gestion des stratégies web



## Annexe 03 (1/2): Interface pour la création de règle



## Annexe 03 (2/2): Interface pour la création de règle

**J'ai fait un test: Inscrire un site dans une liste noire pour voir ce qui est affiché lorsqu'un utilisateur essaie d'accéder à ce site**

Stratégies État de la stratégie de quota Activités de l'utilisateur Catégories **Groupes d'URL** Exceptions Paramètres généraux Types de fichier Quotas de navigation

Norm du groupe d'URL \* liste\_noire\_test

Description test

Noms de domaine à faire correspondre ent.univ-amu.fr

Le Groupe d'URL fera correspondre toutes les requêtes pour ces domaines et leurs sous-domaines.

Rechercher / Ajouter

## Annexe 04: Création de la liste noire test

Stratégies État de la stratégie de quota Activités de l'utilisateur Catégories Groupes d'URL Exceptions Paramètres généraux Types de fichier Quotas de navigation

No Online Chat Deny access to online chat sites

No Web Mail Deny access to web mail sites

No Web Mail or Chat Deny access to web mail and online chat sites

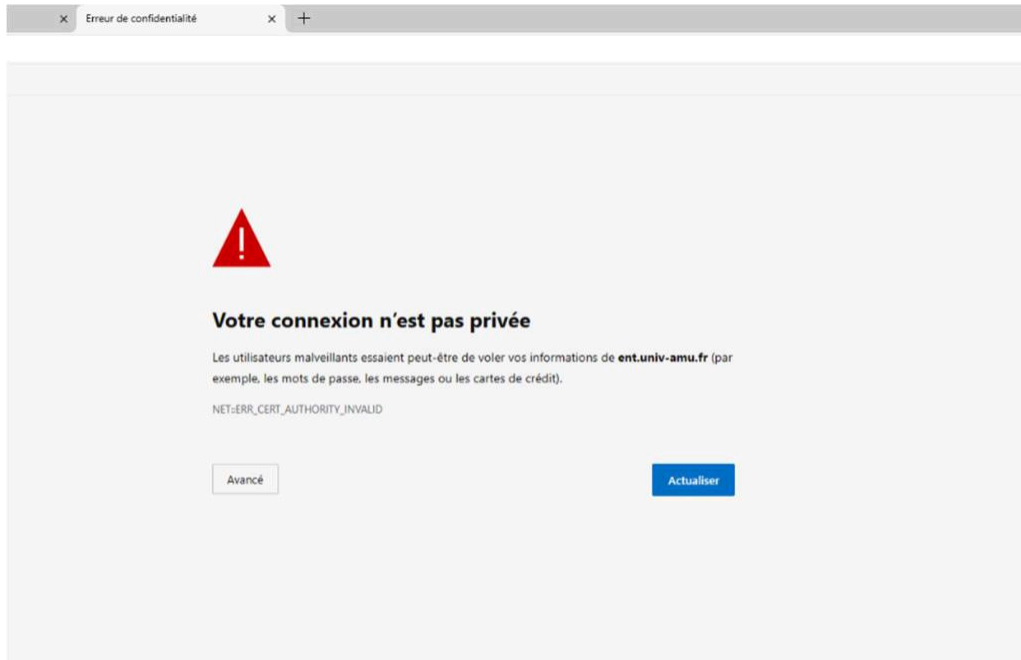
No web uploads Restrict users from uploading content to any site

Stratégie\_WEB\_LAN Stratégie de web filtering pour le réseau LAN TO WAN 1

Utilisateurs	Activités	Action	Contraintes	Gérer	Etat
N'importe qui	LISTE_BLANCHE	✔		+ Ⓞ 🗑	☑
N'importe qui	liste_noire_test	🛡		+ Ⓞ 🗑	☑
N'importe qui	Criminal Activities Drugs and Controlled Subs... Extreme or Violent Web Co... Not Suitable for the Office Nudity and Adult Content ⋮ more ...	🛡		+ Ⓞ 🗑	☑
	Action par défaut	✔			

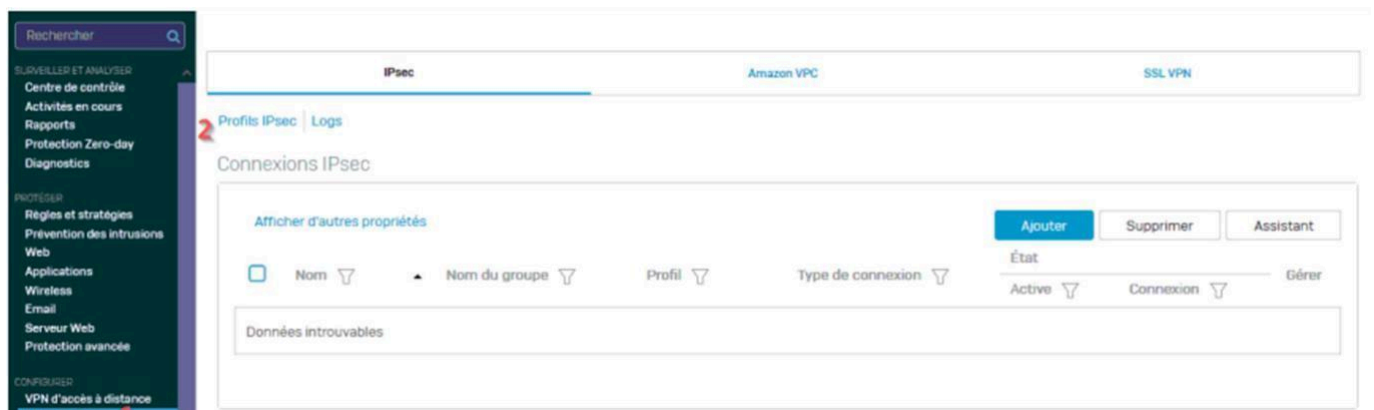
Modifier les paramètres supplémentaires

## Annexe 05: Ajout de la consigne dans la stratégie web



**Annexe 06: Message d'erreur lorsque le site est bloqué**

## Configuration VPN partie firewall



**Annexe 07: Création du profil IPsec**

Dans l'onglet VPN Site à site, il faut créer un profil IPsec.

C'est dans ce profil que l'on détermine le le mode d'échange de clé (IkeV1 ou ikeV2). C'est aussi à ce moment que l'on détermine les paramètres de la phase 1 et les paramètres de la phase 2.

Profils

Commentaires Guides Visionneuse de journaux Aide admin@FW-XEFL\_AIX-MUGUET XEFL

Planification Temps d'accès Quota de navigation Quota de trafic réseau Profils de déchiffrement Profils IPsec Accès à l'appareil

Paramètres généraux

Nom: new Profil

Description: Description

Échange de clé:  IKEV1  IKEV2

Mode d'authentification:  Mode principal  Mode agressif

Tentatives de négociation des clés: 0

Saisir de nouveau la connexion

Ignorer les données au format compressé

SHA2 avec une troncature 96 bits

Phase 1

## Annexe 08: Paramètres généraux

Phase 1

Durée de vie de la clé: 86400 Secondes

Délai avant nouvelle négociation des clés: 360 Secondes

Indiquer un délai aléatoire avant nouvelle négociation des clés: 50 %

Groupe DH (groupe des clés): 14 [DH2048]

Chiffrement: AES256

Authentification: SHA2 256

Vous pouvez ajouter jusqu'à 3 combinaisons d'algorithmes différentes

## Annexe 09: Paramètres de la phase 1

- (1) Etablissement de la durée de vie de la clé entre les deux extrémités du tunnel avant la négociation d'une nouvelle
- (2) Taille de la clé partagé Diffie-Hellman ici 2048 bits
- (3) Choix de la méthode chiffrement ici AES256
- (4) Choix de la méthode d'authentification ici SHA256

Phase 2

Groupe PFS (groupe DH) 14 (DH2048)	Durée de vie de la clé 3600 Secondes
Chiffrement AES256	Authentification SHA2 256

+ Vous pouvez ajouter jusqu'à 3 combinaisons d'algorithmes différentes

Détection d'homologue injoignable

Détection d'homologue injoignable

Enregistrer Annuler

## Annexe 10: Paramètres de la phase 2

Faire la même chose pour la phase 2

Chiffrement

Profil <b>1</b> Profil_IPsec	Type d'authentification <b>2</b> Clé prépartagée
	Clé prépartagée .....
	Répéter le clé pré-partagée <b>3</b> .....

## Annexe 11: Paramètres de chiffrements

- (1) Choix du bon profil**
- (2) Choix du type d'authentification**
- (3) Coller la clé choisie sur l'interface XEFI**

## Paramètres de la passerelle

Passerelle locale	Passerelle à distance
Interface d'écoute <b>1</b> Port2 - [192.168.1.1] [v]	Adresse de la passerelle <b>2</b> [192.168.1.1] [v]
Type d'identifiant local Adresse IP [v] <b>3</b>	Type d'identifiant distant Adresse IP [v]
Identifiant local <b>4</b> [192.168.1.1] [v]	Identifiant distant <b>5</b> [192.168.1.1] [v]
Sous-réseau local <b>6</b> Eth1 - LAN([192.168.1.0/24]) [v]	Sous-réseau distant <b>7</b> LAN_DISTANT [v]
<input type="checkbox"/> Network Address Translation (NAT) Vous devez d'abord créer des sous-réseaux dans	
<a href="#">IPsec NAT setting versus NAT rules</a>	
<b>Enregistrer</b> <b>8</b> Annuler	

## Annexe 12: Paramètres des passerelles de part et d'autres du tunnel

- (1)** L'interface d'écoute est l'interface LAN
- (2)** IP cote XEFI
- (3)** Le type d'authentification local et distant est le même
- (4)** IP public du Firewall
- (5)** IP cote XEFI
- (6)** LAN du Firewall
- (7)** LAN de l'autre bout du tunnel (objet qu'il faut créer)
- (8)** Ne pas oublier d'enregistrer

## Annexes Relatives à l'installation de l'onduleur

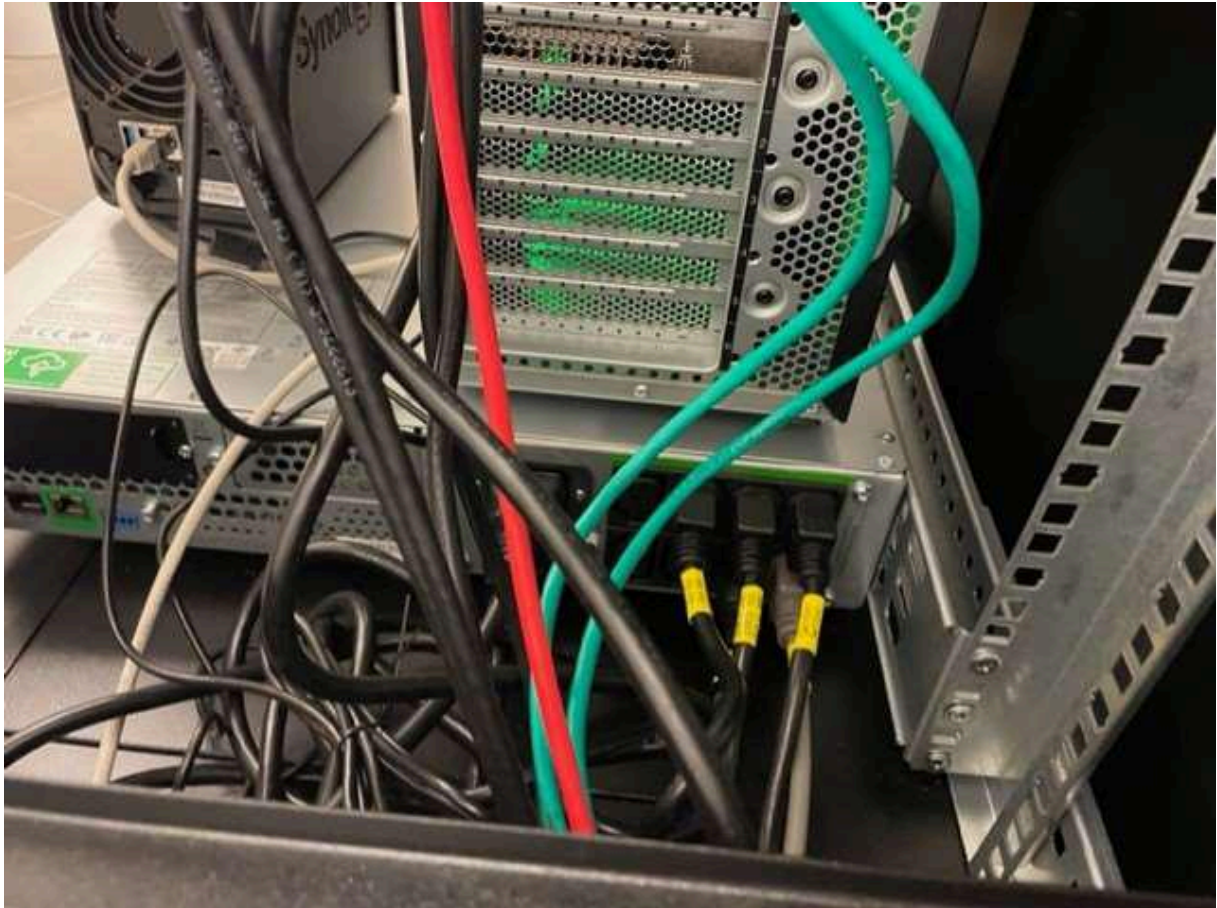


### Annexe 13: Onduleur SMT3000RMI2UC - APC Smart-UPS



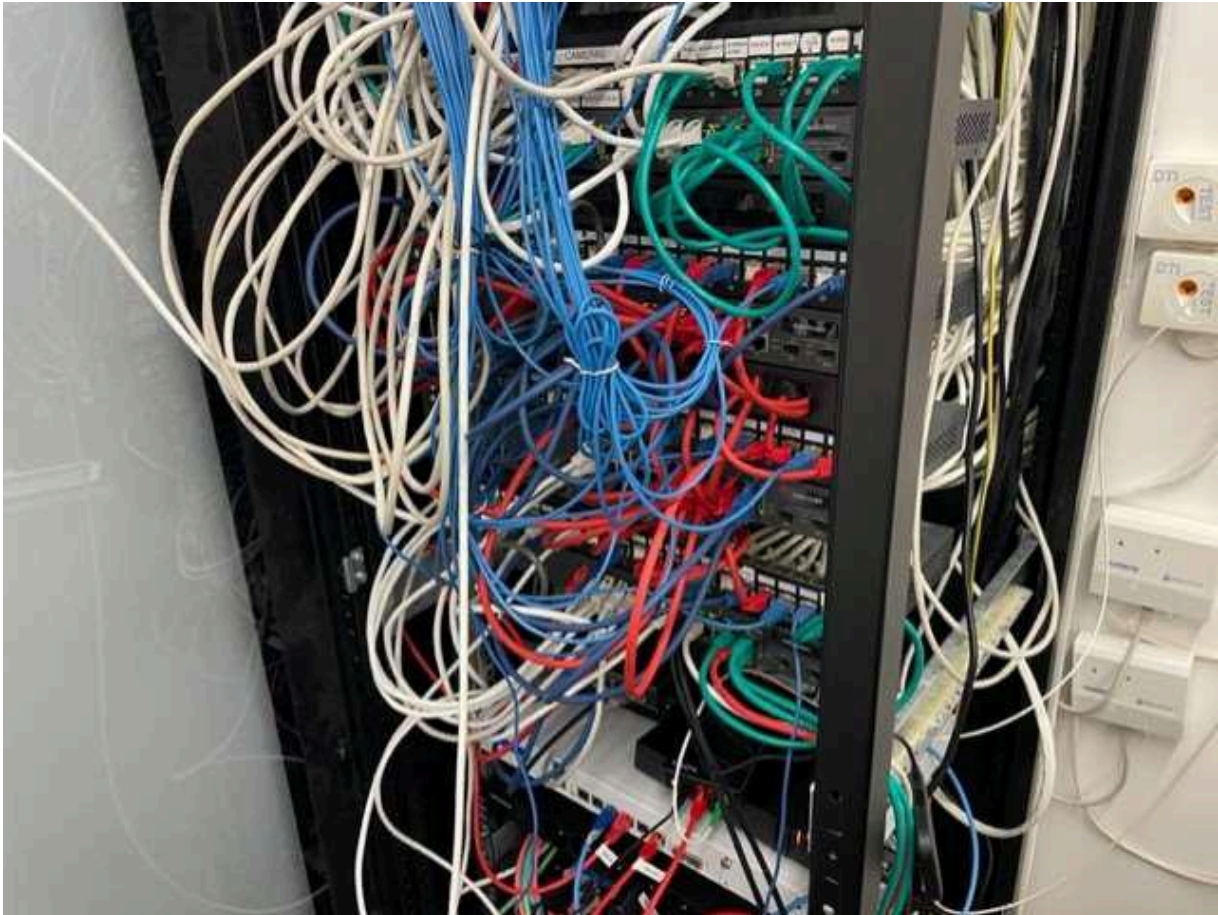
## **Annexe 14: Installation finale de face**

**L'onduleur est en bas et le serveur est positionné sur l'onduleur à gauche**



## **Annexe 15: Installation finale de derrière**

**Nous pouvons remarquer l'ajout d'étiquettes pour identifier l'origine des câbles**



**Annexe 16: Baie contenant les switches et le Firewall sophos**