



Procédure SOPHOS

Configuration Sophos XGS

Sommaire

1 CONFIGURATION DE DÉMARRAGE	1
1.1 Configuration du mot de passe	1
1.2 Configuration du port WAN	2
1.3 Nom et fuseau horaire	3
1.4 Enregistrement du pare-feu	4
1.5 Configuration du réseau LAN	6
1.6 Configuration du WIFI	7
1.7 Protection des réseaux	8
1.8 Notifications et sauvegarde	8
2 CONFIGURATION BASIQUE	8
2.1 Clef principale de stockage sécurisé	9
2.2 Serveur de temps NTP	10
2.3 Mise à jour	10
2.3.1 Firmware	10
2.3.2 Modèle	10
3 CONFIGURATION RÉSEAU	11
3.1 Configuration port WAN - CAPAIX	11
3.2 Configuration port LAN	12
3.3 Configuration DNS	13
3.4 Configuration DHCP	15
4 CONFIGURATION DES STRATÉGIES WEB	16
4.1 Création des catégories d'activités	16
4.1.1 Catégorie de Niveau 1	16
4.2 Création d'une stratégie Web	17
4.2.1 Stratégie de Niveau 1	17
4.3 Personnaliser les messages de blocage	18
4.3.1 Utiliser un message de blocage personnalisé	19
4.3.2 Utiliser un message d'avertissement personnalisé	20
5 CONFIGURATION DES STRATÉGIES APPLICATION	21
5.1 Création d'un filtre d'applications	21
5.1.1 Blocage des applications de risque 4 et 5	22
5.1.2 Autorisation des applications de risque 1, 2 et 3	22
5.1.3 Autorisations spéciales	23
6 CONFIGURATION DES RÈGLES DE PARE-FEU	24
6.1 Création d'une règle temporaire ANY to ANY	24
6.2 Configuration du groupe : Traffic to WAN	25
6.2.1 Créer le groupe Traffic to WAN	25
6.2.2 Configuration réseau	26
6.2.3 Filtrage Web	27
6.2.4 Filtrage Applicatif	27
6.2.5 IPS	27

Configuration Sophos XG

6.3 Configuration du groupe : Traffic to LAN	28
6.3.1 Créer le groupe Traffic to LAN	28
6.3.2 Configuration réseau	29
6.3.3 Filtrage Web	30
6.3.4 Filtrage Applicatif	30
6.3.5 IPS	30
6.4 Configuration de la règle de blocage	31
7 VPN – SOPHOS CONNECT (IPsec)	32
7.1 Création du groupe des utilisateurs VPN	32
7.2 Création des utilisateurs VPN	34
7.2.1 Création de l'utilisateur	34
7.2.2 Enregistrer le mot de passe sur LOCKSELF	34
7.3 Configuration du service VPN	34
7.4 Création des règles de pare-feu VPN	35
7.4.1 VPN to WAN	35
7.4.2 VPN to LAN	36
8 VPN – SOPHOS CONNECT (SSL)	38

CONTEXTE :

Il nous a été demandé d'améliorer l'infrastructure réseau déjà existant, en y ajoutant un paramétrage complet de firewall, des switches manageables et des bornes wifi. J'ai pu mettre en place les firewalls avec des paramétrages sur mesure (Vlan, règles, RED), le tout dans le but de proposer au client un réseau complet et sécurisé.

1 CONFIGURATION DE DÉMARRAGE

1.1 Configuration du mot de passe

- Se brancher sur le port 1 du pare-feu
- Configurer sa carte réseau en 172.16.16.x (hors .16)
- Se rendre à l'adresse suivante : <https://172.16.16.16:4444>
- Après avoir mis la langue en Français et cliquez sur Commencer vous tombez sur cette page

Configuration basique

Vous pouvez vous connecter au pare-feu uniquement via le compte administrateur. Vous devez créer un mot de passe avant de pouvoir continuer. Pour une plus grande sécurité, nous vous recommandons d'utiliser un long mot de passe comprenant des lettres, des chiffres et des caractères spéciaux. Si vous avez déjà une configuration que vous désirez utiliser ou un pare-feu existant que vous voulez connecter en Haute Disponibilité, choisissez les options pertinentes ci-dessous.

[Restaurer la sauvegarde](#)

Création d'un nouveau compte Admin

Nouveau mot de passe Admin :

Saisir de nouveau le mot de passe Admin:

☒ Installer automatiquement le dernier firmware lors de la configuration (recommandé)

L'utilisation de ce logiciel est soumise au [Contrat de Licence de l'Utilisateur Final Sophos \(CLUF\)](#). Vous devez accepter le CLUF pour pouvoir continuer. Veuillez le lire attentivement. Vous acceptez également que Sophos traite les données personnelles conformément à l'[Avis de confidentialité](#).

☒ J'accepte le Contrat de Licence de l'Utilisateur Final de Sophos et l'Avis de confidentialité.

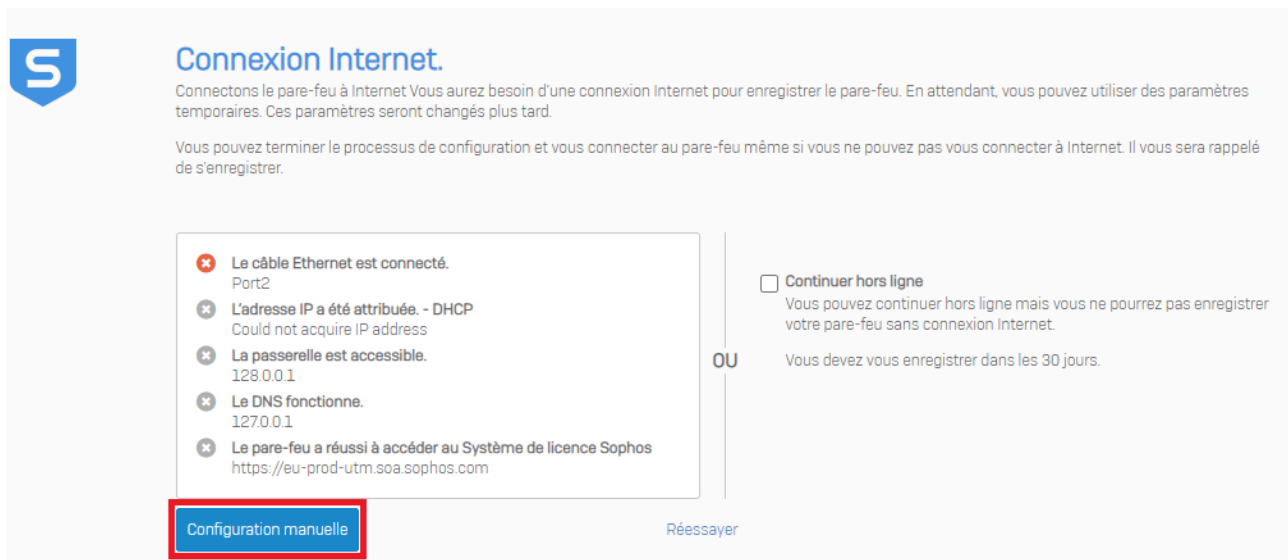
[Précédent](#) [Continuer](#)

- **Remplir le MDP en suivant la procédure LOCKSELF !!**
- Cochez "Installer automatiquement le dernier firmware lors de la configuration (recommandé)"
- Cochez "J'accepte le Contrat de Licence de l'Utilisateur Final de Sophos et l'Avis de confidentialité."
- Puis Continuer

1.2 Configuration du port WAN

Pour les mises à jour de firmware et enregistrement nous allons utiliser un port WAN temporaire.

- Branchez le port 4 de Sophos sur un switch avec un accès Internet (Ou port WAN choisis)
- Passez par la configuration manuelle pour renseigner le port WAN



- Renseignez les informations suivantes :
 - o Port à configurer : Port 4 (Ou port WAN choisis)
 - o Type d'interface : Adresse IP dynamique
 - o Nom de la passerelle : WAN_temp
 - o Serveur DNS 1 : 1.1.1.1
 - o Serveur DNS 2 : 1.0.0.1

Configuration Sophos XG

Configuration manuelle

Si votre fournisseur d'accès a des paramètres de configuration Internet spécifiques, saisissez-les ici.

Choisir un port à configurer Port4	Type d'interface Adresse IP dynamique
Adresse IP	Sous-réseau /30 (255.255.255.252)
Nom de la passerelle WAN_temp	Adresse IP de la passerelle 128.0.0.1
Serveur DNS 1 185.162.210.129	Serveur DNS 2 185.162.210.130
<input type="checkbox"/> Configurer les paramètres de Mandataire direct	
Nom de domaine/Adresse IPv4	Port
Nom d'utilisateur	Mot de passe
<div>Réinitialiser Annuler Appliquer</div>	

- Appuyez ensuite sur Continuer

1.3 Nom et fuseau horaire

- Remplir *Nom du pare-feu* par « SUIVRE LA NOMENCLATURE CHOISIE »
- Renseignez le bon fuseau horaire : Europe/Paris
- Puis appuyez sur Continuer

Configuration Sophos XG

Nom et fuseau horaire

Saisissez le nom du pare-feu Nous vous recommandons d'utiliser un nom de domaine pleinement qualifié (FQDN) qui pointe vers cet appareil.

Nom du pare-feu

Fuseau horaire

Vous pouvez choisir le fuseau horaire sur la carte ou depuis la liste déroulante ci-dessous.

Il est important de choisir le bon fuseau horaire. Celui-ci affecte les événements programmés, les journaux et les rapports.



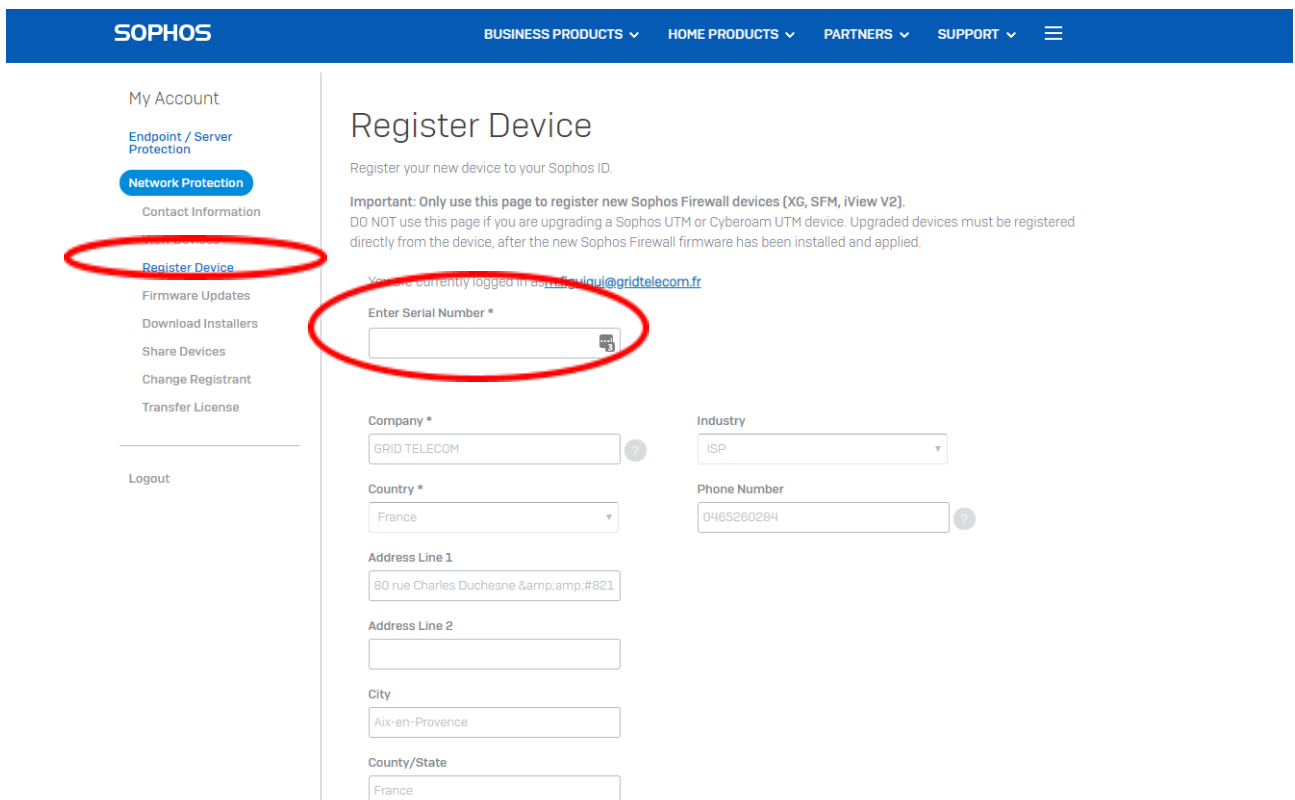
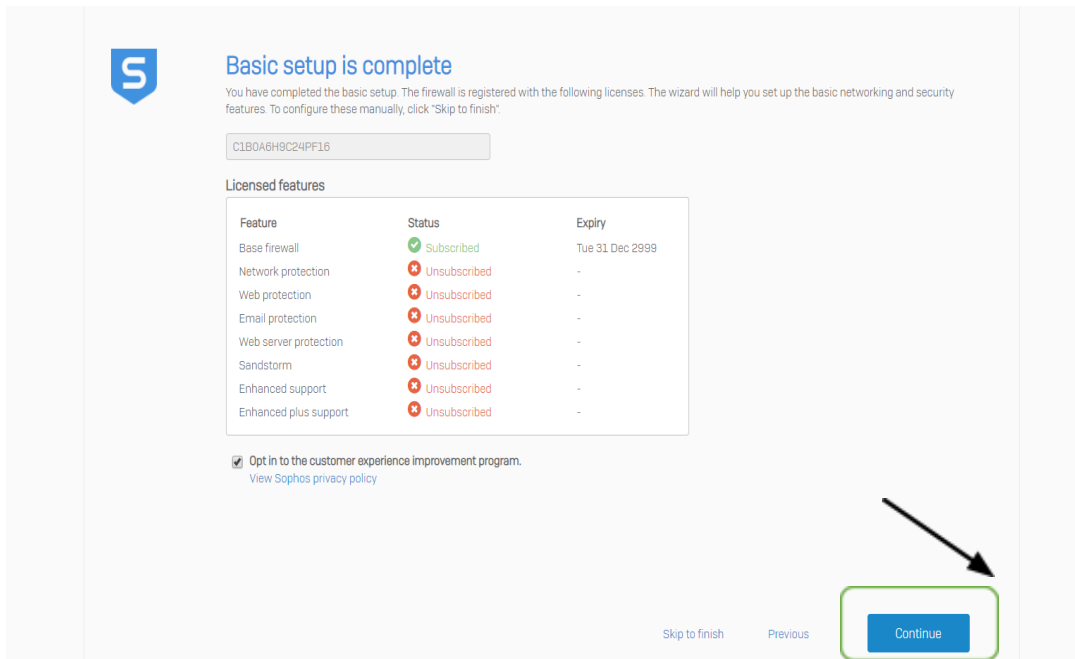
Europe/Paris

Heure : Friday, October 29, 2021, 02 29 PM

Précédent

Continuer

1.4 Enregistrement du pare-feu



My Account

Endpoint / Server
Protection

Network Protection

Contact Information

View Devices

Register Device

Firmware Updates

Download Installers

Share Devices

Change Registrant

Transfer License

Logout

Confirm your registration

Using the details you have supplied, we have identified your device matches the following details. Please review them, and if the details are not correct, please contact customercare@sophos.com with your serial number.

Device Details

Serial Number	C1A0A5PDKWRHG14
Product Type	UTM
Model	XG125W

Confirm Registration

Cancel

Configuration Sophos XG

1.5 Configuration du réseau LAN

- Bien veillez à la configuration des zones :
 - o Le port fibre et le port 4 (Ou port WAN choisis) doivent être *activer pour le WAN*
 - o Tous les autres ports doivent être *activer pour le LAN*
- Sélectionnez le pare-feu en mode Routage
- Saisir l'adresse IP qui servira de passerelle au client (à voir avec le client)
- Désactivez le DHCP
- Appuyez sur Continuer

Configuration Réseau (LAN)

Configurons un réseau protégé. Sélectionnez les ports auxquels vous connecterez les appareils à protéger. Les ports sélectionnés seront liés ensemble et le trafic sera permis. Vous êtes actuellement connecté à "Port1"



■ Connecté ■ Activer pour le LAN ■ Activer pour le WAN ■ Non configuré ▨ Port fibre

Choisir la passerelle

Ce pare-feu (Mode Routage)

Voulez-vous que ce pare-feu agisse en tant que passerelle pour le réseau protégé (utilisé couramment) ? Vous pouvez également utiliser votre passerelle Internet existante et créer un pont avec le réseau protégé. Le pare-feu fournit le même niveau de sécurité dans les deux cas. De plus, il peut agir comme routeur entre le réseau protégé et les autres réseaux locaux s'il est configuré en tant que passerelle.

Adresse LAN et Taille du réseau client interne

192.168.10.1 /24 (jusqu'à 254 appareils client: ▾)

[Modifier la connexion Internet](#)

☐ Activer DHCP

Le pare-feu attribue les adresses IP à vos appareils internes.

[Activer TAP/mode découverte](#)

[Précédent](#)

[Continuer](#)

1.6 Configuration du WIFI

- Renseignez le SSID du réseau WIFI
- Choisir un MDP
- Cochez *Connecter les clients directement au LAN*
- Appuyez sur Continuer

Installation de Sophos Wireless On-Box

Votre système a une radio sans fil intégrée. Prenons un moment pour décider de sa configuration.

Le « réseau sans fil protégé » permet à vos utilisateurs d'accéder en toute sécurité à Internet et à des ressources locales sélectionnées. Le « réseau sans fil invité » permet à vos visiteurs d'accéder à Internet tout en protégeant les ressources locales présentes sur votre réseau.

☒ Configurer le réseau sans fil protégé

Nom du réseau sans fil

GRID TELECOM

Phrase de chiffrement [Afficher la clé pré-partagée \(PSK\)](#)

.....

☒ Connecter les clients directement au LAN

Ceci créera un pont entre votre réseau sans fil protégé et votre LAN. Vos clients sans fil auront directement accès à votre LAN.

☐ Ajouter un réseau sans fil invité

Nom du réseau sans fil

SophosGuest

☐ Nécessite une phrase secrète [Phrase de chiffrementAfficher la clé pré-partagée \(PSK\)](#)

.....

Si vous n'utilisez pas une phrase secrète, tout le monde pourra accéder à votre Wi-Fi.

[Précédent](#)

[Continuer](#)

1.7 Protection des réseaux

- Cochez toutes les cases et appuyez sur Continuer

Protection des réseaux

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

- ☒ **Protection des utilisateurs contre les menaces réseau**
Protège les utilisateurs contre des tentatives d'intrusion sur le réseau, protège contre les menaces avancées qui peuvent se trouver sur votre réseau et bloque le trafic réseau provenant des applications à haut risque.
- ☒ **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.](#)
- ☒ **Contrôle antimalware des fichiers téléchargés depuis Internet**
Même les sites réputés peuvent contenir des fichiers malveillants. Contrôlez les fichiers avec le moteur de détection Sophos afin d'intercepter les malwares connus et leurs variantes.
- ☒ **Envoi des fichiers suspects à Sophos Sandstorm**
Protège les utilisateurs contre les malwares inconnus 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 ne puissent télécharger les fichiers sur leurs ordinateurs.

[Précédent](#) [Continuer](#)

1.8 Notifications et sauvegarde

- Dans les deux e-mails renseignez : support@alvecom.fr
- Cochez *Envoi hebdomadaire de la sauvegarde de configuration*
- Remplir le mot de passe de chiffrement avec l'entrée LOCKSELF associé à ce Sophos

Backup

Backup mode: ☐ Local ☐ FTP ☒ Email

Backup prefix: [BACKUP_SOPHOS_ALVECOM]

Email address *: support@alvecom.fr Quarantine digest will be sent to the first email address only.

Frequency: ☐ Never ☐ Daily ☒ Weekly ☐ Monthly

Schedule: Sunday Day 00 HH 00 MM

Encryption password * Change Encryption password

[Apply](#) [Backup now](#)

2 CONFIGURATION BASIQUE

- Configurer sa carte réseau dans le réseau configuré précédemment
- Si configuration de base, se rendre à l'adresse : <https://192.168.10.1:4444>
- Se connecter avec les identifiants stockés dans LOCKSELF


2.1 Clef principale de stockage sécurisé

Lors du premier démarrage un popup va nous demander de créer une clé

- Cliquez sur Créer une clé
- Renseignez la clé avec l'entrée LOCKSELF associé à ce Sophos
- Cochez *J'ai sauvegardé la clé dans un appli...* Puis cliquez sur Créer une clé

Créer la clé principale de stockage sécurisé

Avant de créer la clé de stockage sécurisé, assurez-vous de pouvoir la sauvegarder dans une appli de gestion des mots de mots de passe ou un autre emplacement sécurisé.

 Il est impossible de la récupérer en cas de perte.

Saisir la clé principale de stockage sécurisé

Robustesse du mot de passe : **Excellente**

Ressaisir la clé pour confirmer

Exigences de complexité :

- ✓ 12 caractères minimum
- ✓ Au moins une lettre majuscule
- ✓ Au moins une lettre minuscule
- ✓ Au moins un chiffre (0-9)
- ✓ Au moins un caractère spécial



J'ai sauvegardé la clé dans une appli de gestion des mots de mots de passe ou un autre emplacement sécurisé

Précédent

Créer une clé

2.2 Serveur de temps NTP

- Dans la catégorie *Administration*, se rendre dans l'onglet *Temps*
- Sélectionnez *Utiliser le serveur NTP personnalisé* et renseigner les serveurs suivants :
 - o 0.fr.pool.ntp.org
 - o 1.fr.pool.ntp.org
 - o 2.fr.pool.ntp.org
 - o 3.fr.pool.ntp.org
- Puis cliquez sur Appliquer










Heure locale 2021-10-29 15:31:46 Europe/Paris

Fuseau horaire Europe/Paris

☐ Utiliser un serveur NTP prédéfini

☒ Utiliser le serveur NTP personnalisé

[Saisissez l'adresse IP/le domaine du serveur NTP]

0.fr.pool.ntp.org		
1.fr.pool.ntp.org		
2.fr.pool.ntp.org		
3.fr.pool.ntp.org		
Rechercher / Ajouter		

Lancer la synchronisation (Sync Now)

☐ Ne pas utiliser le serveur NTP

Date 10/29/2021

Temps 15 HH 31 MM 46 SS

Appliquer

2.3 Mise à jour

2.3.1 Firmware

- Dans la catégorie *Sauvegarde & Firmware*, se rendre dans *Firmware*
- Rechercher et faire si disponible toutes les mise à jour de firmware disponible

2.3.2 Modèle

- Se rendre l'onglet *Mises à jour des modèles*
- Cliquez sur *Mettre à jour le modèle* pour mettre à jour tous les modèles

Configuration Sophos XG

État des mises à jour

Dernière recherche de mises à jour : 14:55:46, Oct 29 2021

Mettre à jour le modèle

Modèle	Version actuelle	Version disponible	Dernière mise à jour réussie	État
AP Firmware	11.0.016	-	15:22:33, Oct 08 2021	Success
ATP	1.0.0384	-	11:42:29, Oct 29 2021	Success

3 CONFIGURATION RÉSEAU

3.1 Configuration port WAN - CAPAIX

- Dans la catégorie *RÉSEAU* se rendre dans l'onglet *Interfaces*
- Sur le port 4 cliquez sur *Edit Interface*

The screenshot shows the 'Interfaces' tab in the Sophos XG web interface. The table below lists the available interfaces:

Interface	État/Vitesse de l'interface	Adresse IP	Misc
Port4 WAN Physique	Débranché Autonégocié	S/O DHCP	Matériel: Port4
br0 N/A Paire de ponts	Connecté S/O	192.168.10.1/255.255.255.0 Statique	Matériel: b Membres: 3 MTU hérité

A context menu is open for the 'Port4' interface, showing the 'Edit Interface' option. The menu also displays the MAC address (7C:5A:1C:6D:5E:07), the maximum segment size (1460), and the MTU (1500).

- Remplir les informations suivantes :
 - o Nom : WAN-OPERATEUR
 - o Zone de réseau : WAN
 - o Attribution de l'IP : DHCP
 - o Nom de la passerelle : WAN-OPERATEUR
- Puis enregistrez

Configuration Sophos XG

General settings

Name *	<input type="text" value="WAN_ORANGE"/>	
Hardware	Port10	
Network zone	<input type="text" value="WAN"/>	

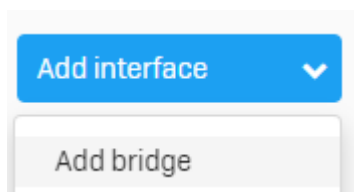
☒ IPv4 configuration

IP assignment	<input type="radio"/> Static <input type="radio"/> PPPoE (DSL) <input checked="" type="radio"/> DHCP	
IPv4/netmask	<input type="text" value="192.168.30.100"/>	<input type="text" value="/24 (255.255.255.0)"/>
Gateway detail		
Gateway name *	<input type="text" value="WAN_ORANGE"/>	
Gateway IP	<input type="text" value="192.168.30.1"/>	

☐ IPv6 configuration

3.2 Configuration port LAN

- Dans la catégorie *RÉSEAU* se rendre dans l'onglet *Interfaces*
- Ajouter un BRIDGE



- Remplir les informations suivantes :
 - Nom : LAN
 - Cochez *Activer l'acheminement sur cette paire de ponts*
 - Interfaces membre :
 - Port 1 – LAN
 - Port 2 – LAN
 - Port 3 – LAN
 - (Etc.)
 - Attribution de l'IP : Statique
 - IPv4/Masque réseau : 192.168.x.x/24 (à définir avec le client)
- Puis enregistrez

Configuration Sophos XG

General settings

Name *

Hardware *

Description

☒ Enable routing on this bridge pair

Member interfaces

Interface	Zone
Port6	LAN
Port7	LAN
Port1	LAN
Port2	LAN
Port3	LAN
Port4	LAN
Port5	LAN
Port8	LAN

☒ IPv4 configuration

IP assignment ☒ Static ☐ DHCP

IPv4/netmask *

Gateway detail

3.3 Configuration DNS

- Dans la catégorie *Réseau* se rendre dans l'onglet *DNS*
- Dans la partie IPv4, sélectionnez *Récupérer le DNS à partir de DHCP*
- Puis Appliquer

Configuration Sophos XG

Configuration DNS

IPv4

☒ Récupérer le DNS à partir de DHCP

☐ Récupérer le DNS à partir de PPPoE

☐ DNS statique

DNS 1

DNS 2

DNS 3

IPv6

☐ Récupérer le DNS à partir de DHCP

☒ DNS statique

DNS 1

DNS 2

DNS 3

Configuration de la requête DNS

☒ Choisir le serveur pour le type d'enregistrement de requêtes entrantes

☐ Choisir le serveur DNS IPv6 plutôt qu'IPv4

☐ Choisir le serveur DNS IPv4 plutôt qu'IPv6

☐ Choisir IPv6 si l'adresse d'origine de la requête est IPv6. Autrement, choisir IPv4

Appliquer

Tester la recherche par nom

3.4 Configuration DHCP

- Dans la catégorie *RÉSEAU*, se rendre dans l'onglet *DHCP*
- Dans la partie *Serveur*, en haut à droite cliquez sur *Ajouter*
- Renseignez les informations suivantes :
 - Nom : LAN
 - Interface : LAN
 - Décochez *Accepter les requêtes client via relais*
 - Bail de l'adresse IP dynamique :
 - Adresse IP de début : 192.168.x.x (à définir avec le client)
 - Adresse IP de fin : 192.168.x.x (à définir avec le client)
 - Masque de sous-réseau : /24
 - Passerelle : Cochez *Utiliser l'IP de l'interface en tant que passerelle*
 - Durée du bail par défaut : 1440
 - Durée max du bail : 2880
 - Détection d'un conflit : Activer
 - Cochez utiliser les paramètres DNS de l'appareil
- Puis cliquez sur Enregistrer

Configuration Sophos XG

Nom *	LAN								
Interface	LAN - 192.168.2.254								
	<input type="checkbox"/> Accepter les requêtes client via relais								
Bail de l'adresse IP dynamique	<table><tr><td>Adresse IP de début</td><td>Adresse IP de fin</td><td>+</td></tr><tr><td>192.168.2.10</td><td>192.168.2.210</td><td>-</td></tr></table> <p>* Appuyez sur l'onglet pour ajouter une nouvelle rangée</p>	Adresse IP de début	Adresse IP de fin	+	192.168.2.10	192.168.2.210	-		
Adresse IP de début	Adresse IP de fin	+							
192.168.2.10	192.168.2.210	-							
Mappage d'adresse IP ou MAC statique	<table><tr><td>Nom d'hôte</td><td>Adresse MAC</td><td>Adresse IP</td><td>+</td></tr><tr><td></td><td></td><td></td><td>-</td></tr></table> <p>* Appuyez sur l'onglet pour ajouter une nouvelle rangée</p>	Nom d'hôte	Adresse MAC	Adresse IP	+				-
Nom d'hôte	Adresse MAC	Adresse IP	+						
			-						
Masque de sous-réseau *	/24 [255.255.255.0]								
Nom de domaine									
Passerelle *	<input checked="" type="checkbox"/> Utiliser l'IP de l'interface en tant que passerelle 192.168.2.254								
Durée du bail par défaut *	1440 1 à 43200 minutes (30 jours)								
Durée max. du bail *	2880 1 à 43200 minutes (30 jours)								
Détection d'un conflit	<input checked="" type="checkbox"/> Activer								

Serveur DNS

<input checked="" type="checkbox"/> Utiliser les paramètres DNS de l'appareil	
DNS principal	185.162.210.129
DNS secondaire	185.162.210.130

Enregistrer Annuler

4 configuratiON des strategies web

4.1 Création des catégories d'activités

4.1.1 Catégorie de Niveau 1

- Dans la catégorie *Web*, se rendre dans l'onglet *Activités de l'utilisateur*
- En haut à droite cliquez sur Ajouter
- Remplir avec les informations suivantes :
 - o Nom : ALVECOM_LVL_1
 - o Catégorie :
 - Criminal Activity
 - Gambling

Configuration Sophos XG

- Hacking
 - Marijuana
 - Nudity
 - Peer-to-peer & torrents
 - Pro-suicide & Self-Harm
 - Sexually Explicit
 - Spyware & Malware
 - Weapons
- Puis appuyez sur Enregistrer

Edit user activity

Name *

Category

- cat Criminal Activity
- cat Gambling
- cat Hacking
- cat Marijuana
- cat Nudity
- cat Peer-to-peer & torrents
- cat Pro-Suicide & Self-Harm
- Add new item

Save Cancel

4.2 Création d'une stratégie Web

4.2.1 Stratégie de Niveau 1

Configuration Sophos XG

- Dans la catégorie *Web*, se rendre dans l'onglet *Stratégies*
- En haut à droite cliquez sur Ajouter une stratégie
- Remplir avec les informations suivantes :
 - o Nom : ALVECOM_LVL_1
 - o Cliquez sur Ajouter une règle
 - o Utilisateurs : N'importe qui
 - o Activités : ALVECOM_LVL_1
 - o Actions :
 - Bloquer HTTP
 - Bloquer HTTPS
 - o État : ON
- Puis cliquez sur Enregistrer

Edit web policy

Name*

Description

Add rule

Users	Activities	Action	Constraints	Manage	Status
<input type="checkbox"/> Anybody	<input type="checkbox"/> ALVECOM_LVL_1	<input type="checkbox"/> Block HTTP and HTTPS	<input type="checkbox"/>	<input type="checkbox"/> + <input type="checkbox"/> - <input type="checkbox"/>	<input checked="" type="checkbox"/> ON
Default action <input checked="" type="checkbox"/>					

Search engine enforcement

☐ Enforce SafeSearch
Enforce additional image filters

☐ Enforce YouTube restrictions
Restriction level

Prevent potentially inappropriate images, videos, and text from appearing in Google, Yahoo, and Bing search results. You can reduce the risk of exposure to explicit content by enabling additional filters that display only images with a Creative Commons license.
⚠ This option can be enforced by the web proxy only.

Prevent access to potentially inappropriate content by restricting which videos are returned in YouTube search results.
⚠ This option can be enforced by the web proxy only.

Policy Quota Status

Allowed time quota Hours Minutes

Set the maximum allowed time for a single user to browse web content that falls into categories restricted by a quota policy action.

4.3 Personnaliser les messages de blocage

Nous pouvons créer des messages pour les actions bloquer ou avertir avec un peu de code

Configuration Sophos XG

- Cochez Utiliser des images personnalisées
- Ajoutez pour l'image du haut : Le NOUVEAU logo alvecom
- Ajoutez pour l'image du bas : Le NOUVEAU logo alvecom

The firewall displays notifications to users when "Web policy" is set to block or warn a website. Use this page to customize the appearance of those notifications.

Logo images on notification page

☐ Use custom images

Custom top image
Choisir un fichier | Aucun fichier choisi
Maximum size 125x70 pixels (.jpg or .jpeg)

Custom bottom image
Choisir un fichier | Aucun fichier choisi
Maximum size 70x60 pixels (.jpg or .jpeg)

Message for block action

☐ Use custom block message
[Preview block message](#)

Custom block message
The administrator of this network has restricted access to sites categorized as {category}.
If you think this is incorrect, you may [suggest a different category.](#)

Message for warn action

☐ Use custom warn message
[Preview warn message](#)

Custom warn message
The administrator of this network has restricted access to sites categorized as {category}.
Clicking proceed will allow temporary access to this site, but you should only do this if necessary.

Message for block action

☒ Use custom block message
[Preview block message](#)

Block message
<!DOCTYPE html>
<html>

☐ Use custom override message
[Preview override message](#)

Override message
You can still browse these websites if you have a valid override code, which you can enter here.

☐ Use custom quota message
[Preview quota message](#)

Quota message
You have a limited daily time quota for accessing this content. If you do not wish to use your time quota, you can return to the previous page.

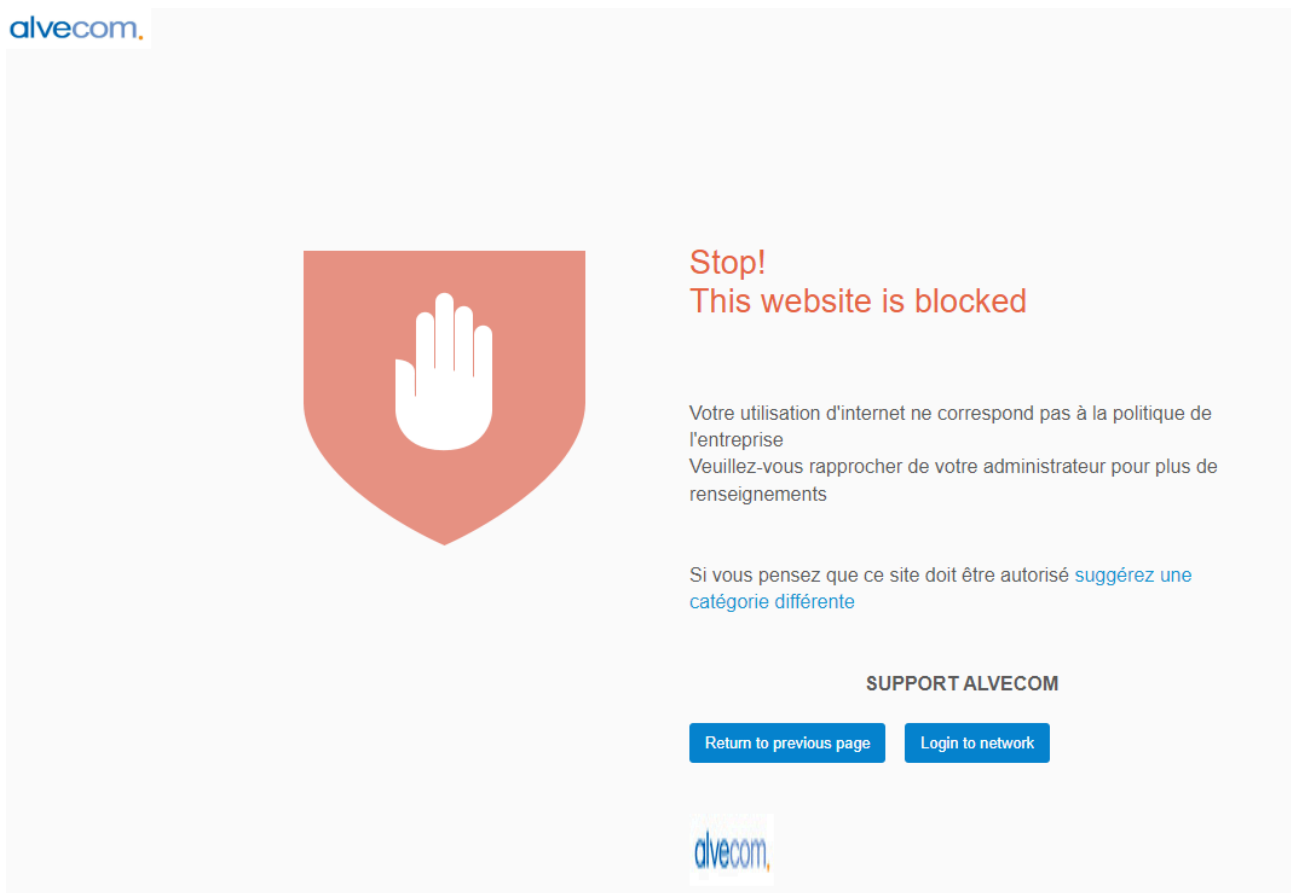
Message for warn action

☒ Use custom warn message
[Preview warn message](#)

Warn message
<!DOCTYPE html>
<html>

4.3.1 Utiliser un message de blocage personnalisé

```
<!DOCTYPE html>
<html>
<br>
<br>
Votre utilisation d'internet ne correspond pas à la politique de l'entreprise
<br>
Veuillez-vous rapprocher de votre administrateur pour plus de renseignements
<br>
<br>
<br>
<span>Si vous pensez que ce site doit être autorisé </span><a href="#"
onclick="callReevaluationFunction()">suggérez une catégorie différente </a>
<br><br>
<br>
<b><CENTER>SUPPORT ALVECOM </CENTER><b>
</html>
```



4.3.2 Utiliser un message d'avertissement personnalisé

```
<!DOCTYPE html>
```


Configuration Sophos XG

<html>

L'administrateur de ce réseau a restreint l'accès aux sites classés dans la catégorie {catégorie}.

En cliquant sur Continuer, vous pourrez accéder temporairement à ce site, mais vous ne devriez le faire que si nécessaire.

<CENTER>SUPPORT ALVECOM </CENTER>

</html>

alvecom.



Warning!

L'administrateur de ce réseau a restreint l'accès aux sites classés dans la catégorie {catégorie}.

En cliquant sur Continuer, vous pourrez accéder temporairement à ce site, mais vous ne devriez le faire que si nécessaire.

SUPPORT ALVECOM

Return to previous page

Proceed

Login to network

alvecom.

5 CONFIGURATION DES stratégies APPLICATION

5.1 Création d'un filtre d'applications

- Dans la catégorie *Applications*, se rendre dans l'onglet *Filtre d'applications*
- En haut à droite cliquez sur Ajouter

Configuration Sophos XG

- Remplir avec les informations suivantes :

- o Nom : Alvecom APP
- o Modèle : Allow All

Name *	<input type="text" value="ALVECOM APP LVL1"/>
Description	<input type="text"/>
Template	<input type="text" value="Allow All"/>

- Ensuite modifiez la règle nouvellement créée en appuyant sur le petit crayon

5.1.1 Blocage des applications de risque 4 et 5

- Appuyez sur Ajouter :
 - o Dans Risque : cochez High et Very High
 - o Actions : Refuser

Catégorie

Risque

Caractéristiques

Technologie

Classification

Filtre intelligent

Effacer le filtre

Risque: High x Very High x

☒ Tout sélectionner ☐ Sélectionner une application individuelle

<input type="checkbox"/>	Nom	Description	Catégorie	Risque	Technologie	Caractéristiques	Classification
<input checked="" type="checkbox"/>	100BA0 P2P	100BA0 P2P	P2P	4 - High	P2P	Excessive Band...	
<input checked="" type="checkbox"/>	56.com Streaming	56.com Streaming	Streaming Media	4 - High	Browser Based	Excessive Band...	
<input checked="" type="checkbox"/>	AIM Android	AIM Android	Mobile Applications	4 - High	Client Server	Loss of producti...	
<input checked="" type="checkbox"/>	AOL Radio Website	AOL Radio Website	General Internet	4 - High	Browser Based	Excessive Band...	
<input checked="" type="checkbox"/>	AOL WebMail	AOL WebMail	Web Mail	4 - High	Browser Based	Transfer files, Tu...	
<input checked="" type="checkbox"/>	ASUS WebStorage	ASUS WebStorage	Storage and Backup	4 - High	Client Server	Prone to misuse,...	

Liste d'applications correspondantes (1 - 50 sur 451)

Action * ☐ Autoriser ☒ Refuser

Planification *

Enregistrer

Annuler

5.1.2 Autorisation des applications de risque 1, 2 et 3

- Cliquez de nouveau sur Ajouter
 - o Dans Risque : cochez Very Low, Low et Medium
 - o Actions : Autoriser

Configuration Sophos XG

- Puis cliquez sur Enregistrer

Catégorie Risque Caractéristiques Technologie Classification Filtre intelligent Effacer le filtre

Risque: Very Low Low Medium

☒ Tout sélectionner ☐ Sélectionner une application individuelle

<input type="checkbox"/>	Nom	Description	Catégorie	Risque	Technologie	Caractéristiques	Classification
<input checked="" type="checkbox"/>	1 & 1 Webmail	1 & 1 Webmail	Web Mail	2 - Low	Browser Based	<input type="checkbox"/> Cloud Applicatio...	New
<input checked="" type="checkbox"/>	10000ft Plans	10000ft Plans	General Business	1 - Very Low	Browser Based	<input type="checkbox"/> Cloud Applicatio...	New
<input checked="" type="checkbox"/>	101 Network	101 Network	Streaming Media	1 - Very Low	Browser Based	Loss of producti...	
<input checked="" type="checkbox"/>	123RF	123RF	E-commerce	1 - Very Low	Browser Based	Loss of producti...	
<input checked="" type="checkbox"/>	126 Mail	126 Mail	Web Mail	2 - Low	Browser Based	Transfer files, Wi...	
<input checked="" type="checkbox"/>	163 Alumni	163 Alumni	Social Networking	2 - Low	Browser Based	Loss of producti...	

Liste d'applications correspondantes (1 - 50 sur 3081)

Action * ☒ Autoriser ☐ Refuser

Planification * All the Time

Enregistrer Annuler

- Enfin cliquez sur Enregistrer pour valider le filtre d'applications

5.1.3 Autorisations spéciales

Pour pallier certain faux-positifs il faut manuellement autoriser certaines applications

- Cliquez de nouveau sur Ajouter
 - o Dans Filtre intelligent : tapez whatsapp
 - o Actions : Autoriser
- Puis cliquez sur Enregistrer

Configuration Sophos XG

Catégorie Risque Caractéristiques Technologie Classification Filtre intelligent Effacer le filtre

Catégorie: All x Filtre intelligent: whatsapp x

☒ Tout sélectionner ☐ Sélectionner une application individuelle

<input type="checkbox"/>	Nom	Description	Catégorie	Risque	Technologie	Caractéristiques	Classification
<input checked="" type="checkbox"/>	WhatsApp	WhatsApp	Mobile Applications	4 - High	Client Server	Widely Used	
<input checked="" type="checkbox"/>	WhatsApp Call	WhatsApp Call	VoIP	1 - Very Low	Client Server	Loss of producti...	
<input checked="" type="checkbox"/>	WhatsApp File Transfer	WhatsApp File Transfer	Mobile Applications	3 - Medium	Client Server	Loss of producti...	
<input checked="" type="checkbox"/>	WhatsApp Video Call	WhatsApp Video Call	VoIP	1 - Very Low	Client Server	Loss of producti...	
<input checked="" type="checkbox"/>	WhatsApp Web	WhatsApp Web	Instant Messenger	3 - Medium	Browser Based	Loss of producti...	

Liste d'applications correspondantes (1 - 5 sur 5)

Action * ☒ Autoriser ☐ Refuser

Planification * All the Time

Enregistrer Annuler

- Enfin cliquez sur Enregistrer pour valider le filtre d'applications

☐ WhatsApp, WhatsApp Web, WhatsApp File Transfer, WhatsApp Call, WhatsApp Video Call Filtre intelligent = whatsapp All the Time Autoriser

Bronto, Tapin Radio, Accelo, Contract Wars, Attix5 Backup, DouBan FM, iCloud Numbers, Zippyshare, Mixwit Website, Zoho WebMessenger, iMeet Central, Elixio Website, Zoom Meetings, IMGames, Tortoise SVN, Get Attribute All, Pogo Website, Pearls Peril, Datawrapper, REPCmd, WMX Video Streaming, Shopify Manage Orders, LinkedIn Videos, FarmVille 2, E Entertainment, MIUI OTA Update, Zshare Download, Google Plus Comment, HSRP, OwnerIQ Website, Aniscartujo Web Proxy, NIC Name, ShareBlast, IGN, Google Website, WebDAV, Papa Pear Saga, ZirMed, FXP, List Services, Qik Streaming, Battlefield Heroes, Redbooth, Workday, Windows Remote Desktop, iSwifter Games Browser, iTrix, Slotomania Slot Machines, YupTV Streaming, OCBinder, Mobile Legends, Italki Website, Dailywire, TapCash, EpicCare, Top Gear, Egnyte Upload, Naked Streaming, WhatsApp Call, Lokalistens Photo Upload, SendRRData-FWD Open Response, KanbanFlow, Advogato Website, Monday, Friendica Website, Web.De WebMail, Hubspot, Shelfari Website, Google Location, XNS-Mail, Filmow Website, EMBL-NDT, Gapyear Website, Unacademy, FarmVille-Facebook Games, Work, SOCKS Proxy, Yahoo Cricket Website, Urban Ladder, Wikipedia Website, Backblaze User Restore, Phuks, TaxiforSure, Wynk Music, Twitter Upload, Nykaa, Last FM Streaming, Xinhuanet, Worldcric, Mobileip-mn, Party Poker Website, TLVMedia, Seismic, Panda Antivirus Update, Global News, Alpermix, Quopn Wallet, Magnatune Website, Base, Itunes Update, Marvel Avengers Alliance Tactics, Google Drive Base, Yesware, Plex, Juice Cubes, Mxit Android, CuteBears FacebookApp, Ebaumsworld Video Streaming, Garena Web Messenger, DCEPDC, Nomadesk Download, Moneycontrol Markets on Mobile, ViewOn, Blogger Create Blog, CoralCDN Proxy, Shockwave, PAWServ, File host File Transfer, Mega, MTV Website, FileZilla, SlideShare Download, Appliance Authentication Service, Bloomberg Businessweek, Travelocity, RMT, SNPP, Weibo Website, Silverpop, Chartio, Hayu, Vidazoo, AIM Express Messenger, Wikispaces, Airtel TV, Imgur, GTalk Update, Zshare Upload, Blogger Comment, L.M.P. Google Plus Add To Circle, Get Attribute Single, Ravelyr

Enregistrer Annuler

6 CONFIGURATION DES RÈGLES DE PARE-FEU

6.1 Création d'une règle temporaire ANY to ANY

- Dans la catégorie *Règles et stratégies*, se rendre dans l'onglet *Règles de pare-feu*
- Cliquez sur *Ajouter une règle de pare-feu* puis *Nouvelle règle de pare-feu*

Configuration Sophos XG

- Renseignez les informations suivantes :
 - o Nom de la règle : ANY to ANY
 - o Action : Accepter
 - o Position de la règle : Haut
 - o Groupe de règle : Aucune
 - o Source :
 - Zones émettrices : Tous
 - o Destination et services :
 - Zone de destination : Tous
- Puis cliquez sur Enregistrer

☒ État de la règle

Nom de la règle *
ANY to ANY

Action
Accepter

☐ Enregistrer le trafic du pare-feu
Enregistre le trafic, correspondant à cette règle de pare-feu, sur l'appareil (par défaut) ou sur le serveur Syslog configuré.

Description
Saisir Description

Position de la règle
Haut

Groupe de règles
Aucune

Source
Sélectionner les zones, les réseaux et les appareils sources.
Cette règle s'applique au trafic provenant de ces sources lors des période de temps planifiées.

Zones émettrices *
Tous
Ajouter un nouvel élément

Réseaux et appareils émetteurs *
Tous
Ajouter un nouvel élément

Lors d'heure planifiée
Tout le temps
Sélectionner pour appliquer la règle à une période de temps et jour de la semaine spécifiques.

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 *
Tous
Ajouter un nouvel élément

Réseaux de destination *
Tous
Ajouter un nouvel élément

Services *
Tous
Ajouter un nouvel élément
Les services sont des types de trafic basés sur une combinaison de protocoles et de ports.

Enregistrer Annuler

- Maintenant, supprimer toutes les autres règles, ainsi que tous les autres groupes présents. De sorte qu'il ne nous reste que notre règle temporaire : ANY to ANY

Configuration Sophos XG

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
<div>≡</div> <div><div></div></div> 1 <div><div></div></div>	<div>ANY to ANY</div> <div>entrant 0 B, sortant 0 B</div>	Toute zone, Tout hôte	Toute zone, Tout hôte	Tout service	#6	Accepter	<div>[IPS] [AV] [WEB] [APP] [QoS] [HB]</div> <div>[LinkedNAT] [PRX] [LOG]</div> <div></div>
<div>≡</div> <div><div></div></div> 2 <div><div></div></div>	<div>Tout abandonner</div> <div>entrant 0 B, sortant 0 B</div>	Toute zone, Tout hôte	Toute zone, Tout hôte	Tout service	#0	Annuler	<div>[IPS] [AV] [WEB] [APP] [QoS] [HB]</div> <div>[LOG]</div> <div></div>

Affichage de 2 sur 2. 0 sélectionné

6.2 Configuration du groupe : Traffic to WAN

6.2.1 Créer le groupe Traffic to WAN

- Cliquez sur *Ajouter une règle de pare-feu* puis Nouvelle règle de pare-feu
- Dans groupe de règles, appuyez sur Créer

Position de la règle

Bas

Groupe de règles

Créer

Aucune

Automatique

- o Nom du groupe : Traffic to WAN
- o Type de règle : Règle de réseau
- o Zone émettrice : Tous
- o Zone de destination : WAN

Configuration Sophos XG

Ajouter un nouveau groupe ×

Nom du groupe *

Description du groupe

Critère de correspondance du groupe ⓘ

Type de règle

Zone émettrice

[Ajouter un nouvel élément](#)

Zone de destination

[Ajouter un nouvel élément](#)

[Annuler](#) [Ajouter](#)

6.2.2 Configuration réseau

- Renseignez les informations suivantes :
 - Nom de la règle : LAN to WAN
 - Action : Accepter
 - Enregistrer le trafic du pare-feu
 - Position de la règle : Bas
 - Groupe de règles : Traffic to WAN
 - Source :
 - Zones émettrices : LAN
 - Réseaux et appareils émetteurs : Tous
 - Lors d'heure planifiée : Tout le temps
 - Destination et services :
 - Zone de destination : WAN
 - Réseaux de destination : Tous
 - Services : Tous

Configuration Sophos XG

Nom de la règle * LAN to WAN	Description Saisir Description	Position de la règle Bas
Action Accepter		Groupe de règles Traffic to WAN
<input checked="" type="checkbox"/> Enregistrer le trafic du pare-feu Enregistre le trafic, correspondant à cette règle de pare-feu, sur l'appareil (par défaut) ou sur le serveur Syslog configuré.		

Source
Sélectionner les zones, les réseaux et les appareils sources.
Cette règle s'applique au trafic provenant de ces sources lors des période de temps planifiées.

Zones émettrices * LAN Ajouter un nouvel élément	Réseaux et appareils émetteurs * Tous Ajouter un nouvel élément	Lors d'heure planifiée Tout le temps Sélectionner pour appliquer la règle à une période de temps et jour de la semaine spécifiques.
---	--	--

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 * WAN Ajouter un nouvel élément	Réseaux de destination * Tous Ajouter un nouvel élément	Services * Tous Ajouter un nouvel élément <small>Les services sont des types de trafic basés sur une combinaison de protocoles et de ports.</small>
--	--	---

6.2.3 Filtrage Web

- Cliquez sur Filtrage WEB :
 - o Stratégie Web : AIVECOM_LVI_1
 - o Tout cocher sauf l'utilisation du web proxy

6.2.4 Filtrage Applicatif

- Dans le menu Identifie et contrôle les applications (App Control) : ALVECOM APP LVL1

6.2.5 IPS

- Dans le menu Détecte et empêche les exploits (IPS) : lantowan_general

Configuration Sophos XG

Security features

Web filtering

Web policy

ALVECOM_LVL_1

☒ Apply web category-based traffic shaping

☒ Block QUIC protocol

Malware and content scanning

☒ Scan HTTP and decrypted HTTPS

☒ Use zero-day protection

☒ Scan FTP for malware

Filtering common web ports

☐ Use web proxy instead of DPI engine

[DPI engine or web proxy?](#)

Web proxy options

☒ Decrypt HTTPS during web proxy filtering

Configure Synchronized Security Heartbeat

Other security features

Identify and control applications (App control)

ALVECOM_APP

☐ Apply application-based traffic shaping policy

Shape traffic

VoIP Guarantee

DSCP marking

Select DSCP marking

Detect and prevent exploits (IPS)

lantowan_general

Scan email content

- Enfin, cliquez sur Enregistrer

6.3 Configuration du groupe : Traffic to LAN

6.3.1 Créer le groupe Traffic to LAN

- Cliquez sur *Ajouter une règle de pare-feu* puis Nouvelle règle de pare-feu
- Dans groupe de règles, appuyez sur Créer

Configuration Sophos XG

Position de la règle

Bas

Groupe de règles

Créer

Aucune

Automatique

- Nom du groupe : Traffic to LAN
- Type de règle : Règle de réseau
- Zone émettrice : Tous
- Zone de destination : LAN

Ajouter un nouveau groupe

×

Nom du groupe *

Traffic to LAN

Description du groupe

Saisir Description du groupe

Critère de correspondance du groupe ⓘ

Type de règle

Règle de réseau

Zone émettrice

Tous

Ajouter un nouvel élément

Zone de destination

LAN

Ajouter un nouvel élément

Annuler

Ajouter

6.3.2 Configuration réseau

- Renseignez les informations suivantes :
 - Nom de la règle : LAN to LAN
 - Action : Accepter

Configuration Sophos XG

- Enregistrer le trafic du pare-feu
- Position de la règle : Bas
- Groupe de règles : Traffic to LAN
- Source :
 - Zones émettrices : LAN
 - Réseaux et appareils émetteurs : Tous
 - Lors d'heure planifiée : Tout le temps
- Destination et services :
 - Zone de destination : LAN
 - Réseaux de destination : Tous
 - Services : Tous

Nom de la règle * LAN to LAN	Description Saisir Description	Position de la règle Bas
Action Accepter		Groupe de règles Traffic to LAN
<input checked="" type="checkbox"/> Enregistrer le trafic du pare-feu Enregistre le trafic, correspondant à cette règle de pare-feu, sur l'appareil (par défaut) ou sur le serveur Syslog configuré.		

Source

Sélectionner les zones, les réseaux et les appareils sources.
Cette règle s'applique au trafic provenant de ces sources lors des période de temps planifiées.

Zones émettrices * LAN Ajouter un nouvel élément	Réseaux et appareils émetteurs * Tous Ajouter un nouvel élément	Lors d'heure planifiée Tout le temps Sélectionner pour appliquer la règle à une période de temps et jour de la semaine spécifiques.
---	--	--

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 * LAN Ajouter un nouvel élément	Réseaux de destination * Tous Ajouter un nouvel élément	Services * Tous Ajouter un nouvel élément <small>Les services sont des types de trafic basés sur une combinaison de protocoles et de ports.</small>
--	--	---

Configuration Sophos XG

6.3.3 Filtrage Web

- Cliquez sur Filtrage WEB :
 - o Stratégie Web : AIVECOM_LVI_1
 - o Tout cocher sauf l'utilisation du web proxy

6.3.4 Filtrage Applicatif

- Dans le menu Identifie et contrôle les applications (App Control) : ALVECOM_LVL_1

6.3.5 IPS

- Dans le menu Détecte et empêche les exploits (IPS) : lantowan_general
- Enfin, cliquez sur Enregistrer

6.4 Configuration de la règle de blocage

- Cliquez sur *Ajouter une règle de pare-feu* puis Nouvelle règle de pare-feu
- Renseignez les informations suivantes :
 - o Nom de la règle : Interdiction Globale
 - o Action : Annuler
 - o Enregistrer le trafic du pare-feu
 - o Position de la règle : Bas
 - o Groupe de règle : Aucune
 - o Source :
 - Zones émettrices : Tous
 - o Destination et services :
 - Zone de destination : Tous
- Puis cliquez sur Enregistrer

Configuration Sophos XG

Nom de la règle * Interdiction Globale	Description Saisir Description	Position de la règle Bas
Action Annuler		Groupe de règles Aucune
<input checked="" type="checkbox"/> Enregistrer le trafic du pare-feu Enregistre le trafic, correspondant à cette règle de pare-feu, sur l'appareil (par défaut) ou sur le serveur Syslog configuré.		

Source
Sélectionner les zones, les réseaux et les appareils sources.
Cette règle s'applique au trafic provenant de ces sources lors des période de temps planifiées.

Zones émettrices * Tous Ajouter un nouvel élément	Réseaux et appareils émetteurs * Tous Ajouter un nouvel élément	Lors d'heure planifiée Tout le temps Sélectionner pour appliquer la règle à une période de temps et jour de la semaine spécifiques.
--	--	--

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 * Tous Ajouter un nouvel élément	Réseaux de destination * Tous Ajouter un nouvel élément	Services * Tous Ajouter un nouvel élément <small>Les services sont des types de trafic basés sur une combinaison de protocoles et de ports.</small>
---	--	---

Enregistrer Annuler

- **Supprimer maintenant la règle temporaire ANY to ANY !!!!**

7 VPN – SOPHOS CONNECT (IPsec)







7.1 Création du groupe des utilisateurs VPN

- Dans la catégorie *Authentification*, se rendre dans l'onglet *Groupes*
- Cliquez sur le bouton Ajouter et remplir les informations suivantes :
 - o Nom du groupe : Groupe VPN
 - o Type de groupe : Normal
 - o Quota de navigation : Unlimited Internet Access
 - o Temps d'accès : Allowed all the time
- Puis cliquez sur Enregistrer

Configuration Sophos XG

Nom du groupe *	<input type="text" value="Groupe VPN"/>
Description	<input type="text" value="Description"/>
Type de groupe *	<input type="text" value="Normal"/>

Stratégies

Quota de navigation *	<input type="text" value="Unlimited Internet Access"/>	
Temps d'accès *	<input type="text" value="Allowed all the time"/>	
Trafic réseau	<input type="text" value="None"/>	
Régulation de flux	<input type="text" value="None"/>	
Accès à distance *	<input type="text" value="Aucune stratégie appliquée"/>	
Sans client *	<input type="text" value="Aucune stratégie appliquée"/>	
Rapport de quarantaine *	<input checked="" type="radio"/> Activer <input type="radio"/> Désactiver	
Liaison MAC	<input checked="" type="radio"/> Activer <input type="radio"/> Désactiver	
L2TP *	<input checked="" type="radio"/> Activer <input type="radio"/> Désactiver	
PPTP *	<input checked="" type="radio"/> Activer <input type="radio"/> Désactiver	
Accès à distance IPsec *	<input type="radio"/> Activer <input checked="" type="radio"/> Désactiver	
Restriction de connexion*	<input checked="" type="radio"/> Tous les nœuds <input type="radio"/> Nœuds sélectionnés <input type="radio"/> Plage de nœud	

7.2 Création des utilisateurs VPN

7.2.1 Création de l'utilisateur

- Dans la catégorie *Authentification*, se rendre dans l'onglet *Utilisateurs*
- Cliquez sur Ajouter et renseigner les informations pour chaque utilisateur pouvant se connecter en VPN
- L'ajouter au groupe : Groupe VPN

Stratégies

Groupe *

Groupe VPN

7.2.2 Enregistrer le mot de passe sur LOCKSELF

7.3 Configuration du service VPN

- Dans la catégorie *VPN*, se rendre dans l'onglet *IPsec (accès à distance)*
- Renseigner les informations suivantes :
 - o Accès à distance IPsec : Activer
 - o Interface : *sélectionner votre port WAN*
 - o Générer une clé pré-partagée à l'aide de LOCKSELF (30 caractères)
 - o Utilisateurs et groupes autorisés : Groupe VPN
 - o Nom : NOM_DU_CLIENT
 - o Attribuer l'IP à partir de : *définir une plage IP avec le client*
 - o Serveur DNS 1 : 1.1.1.1
 - o Serveur DNS 2 : 1.0.0.1

Configuration Sophos XG

Accès à distance IPsec	<input checked="" type="checkbox"/> Activer
Interface *	Port4.811 - NA
Type d'authentification *	Clé prépartagée
Clé prépartagée *
Identifiant local	Sélectionner l'identifiant local
Identifiant distant	Sélectionner l'identifiant distant
Utilisateurs et groupes autorisés *	Groupe VPN Ajouter un nouvel élément

Informations sur le client

Nom *	NOM DU CLIENT
Attribuer l'IP à partir de *	172.16.1.10 - 172.16.1.210
<input type="checkbox"/> Autoriser l'allocation d'une adresse IP avec bail à partir du serveur RADIUS pour l'accès à distance IPsec, L2TP et PPTP	

- Dans les paramètres avancés, cochez : Permettre aux utilisateurs de sauvegarder un nom d'utilisateur et un mot de passe

☒ Permettre aux utilisateurs de sauvegarder un nom d'utilisateur et un mot de passe

- Puis appuyez sur Appliquer, puis Exporter la connexion pour récupérer le .tgz
- Pour se connectez au VPN depuis un client, voir la doc associée

7.4 Création des règles de pare-feu VPN

7.4.1 VPN to WAN

- Dans la catégorie *Règles et stratégies*, se rendre dans l'onglet *Règles de pare-feu*
- Dans le groupe Traffic to WAN, cliquez sur la règle LAN to WAN, puis Cloner la règle au-dessous

Configuration Sophos XG

#	Nom	Source	Destination	Laquelle ?	ID	Action	Functionalité et service
	Traffic to WAN	entrant 0 B, sortant 0 B					
1	LAN to WAN	LAN, Tout hôte	WAN, Tout hôte	Tout service	#1	Accepter	IPS, AV, WEB, App, QoS, HE, L2, NAT, PRX, LOG
3	Interdiction Globale	Toute zone, Tout hôte	Toute zone, Tout hôte	Tout service	#3	Annuler	
4	Tout abandonner	Toute zone, Tout hôte	Toute zone, Tout hôte	Tout service	#0	Annuler	

Affichage de 4 sur 4. 0 sélectionné

LAN to WAN

- Modifier
- Réinitialiser le compte du tra...
- Cloner la règle au-dessus
- Cloner la règle au-dessous
- Ajouter une règle avant
- Ajouter une règle après
- Détacher

- Changez le nom par VPN to WAN
- Changez la zone émettrice par VPN
- Cliquez sur Cloner

Nom de la règle *

VPN to WAN

Action

Accepter

☒ Enregistrer le trafic du pare-feu

Enregistre le trafic, correspondant à cette règle de pare-feu, sur l'appareil (par défaut) ou sur le serveur Syslog configuré.

Description

Saisir Description

Groupe de règles

Traffic to WAN

Source

Sélectionner les zones, les réseaux et les appareils sources. Cette règle s'applique au trafic provenant de ces sources lors des période de temps planifiées.

Zones émettrices *

VPN

Ajouter un nouvel élément

Réseaux et appareils émetteurs *

Tous

Ajouter un nouvel élément

Lors d'heure planifiée

Tout le temps

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

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 *

WAN

Ajouter un nouvel élément

Réseaux de destination *

Tous

Ajouter un nouvel élément

Services *

Tous

Ajouter un nouvel élément

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

Cloner Annuler

7.4.2 VPN to LAN

- Dans la catégorie *Règles et stratégies*, se rendre dans l'onglet *Règles de pare-feu*
- Dans le groupe Traffic to LAN, cliquez sur la règle LAN to LAN, puis Cloner la règle au-dessous

Configuration Sophos XG

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
2	Traffic to WAN	entrant 0 B, sortant 0 B					
1	Traffic to LAN	entrant 0 B, sortant 0 B					
3	LAN to LAN	LAN, Tout hôte	LAN, Tout hôte	Tout service	#2	Accepter	IPS AV WEB APP QoS HB PRX LOG
4	Interdiction Globa...	Toute zone, Tout hôte	Toute zone, Tout hôte	Tout service	#3	Annuler	
5	Tout abandonner	Toute zone, Tout hôte	Toute zone, Tout hôte	Tout service	#0	Annuler	

Affichage de 5 sur 5. 0 sélectionné

LAN to LAN ON
Modifier
Réinitialiser le compte du tra...
Cloner la règle au-dessus
Cloner la règle au-dessous
Ajouter une règle avant

- Changez le nom par VPN to LAN
- Changez la zone émettrice par VPN
- Cliquez sur Cloner

Nom de la règle *
VPN to LAN

Description
Saisir Description

Groupe de règles
Traffic to LAN

Action
Accepter

☒ Enregistrer le trafic du pare-feu
Enregistre le trafic, correspondant à cette règle de pare-feu, sur l'appareil (par défaut) ou sur le serveur Syslog configuré.

Source
Sélectionner les zones, les réseaux et les appareils sources.
Cette règle s'applique au trafic provenant de ces sources lors des période de temps planifiées.

Zones émettrices *
VPN
Ajouter un nouvel élément

Réseaux et appareils émetteurs *
Tous
Ajouter un nouvel élément

Lors d'heure planifiée
Tout le temps
Sélectionner pour appliquer la règle à une période de temps et jour de la semaine spécifiques.

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 *
LAN
Ajouter un nouvel élément

Réseaux de destination *
Tous
Ajouter un nouvel élément

Services *
Tous
Ajouter un nouvel élément
Les services sont des types de trafic basés sur une combinaison de protocoles et de ports.

Cloner Annuler

8 VPN – SOPHOS CONNECT (SSL)

Configuration Sophos

Project Vlans définition

- Licence
- Sauvegardes
- Définition des Zones pour chacun des VLANs
- Création des VLANs
- Création des différents DHCP
- Baux statiques
- Création du RED vers Alvecom
- Règles firewall
- Filtrage Web
- Filtrage applicatif :
- Routage statique
- Portail Captif
 - Certificats et clé serveur Web Sophos
- ACL d'accès locales
 - Utilisateur Guest portail captif
- Enfin le fichier de configuration en Backup

Project Vlans définition

Le réseau est 10.XX.YY.00 /23

où XX correspond au département géographique

où YY pour le site déployé est compris entre :

0 (A) et 1 (B) pour le Site 1

2 (A) et 3 (B) pour le site 2

4 (A) et 5 (B) pour le site 3

6 (A) et 7 (B) pour le site 4

et ainsi de suite

Le pool 10.XX.A.254 /24 est réservé au wifi étudiants (VLAN20)

Le Pool 10.XX.B.30 /27 est utilisé pour le vlan de Management (VLAN1) que l'on retrouve sur le Sophos. Le Pool 10.XX.B.126 /26 est dédié à la VOIP (VLAN30)

Le Pool 10.XX.B.254 /25 est dédié au département administratif de l'établissement (VLAN10) Vlan Management 10.94.1.30/27

Configuration Sophos XG

Licence

Configuration Sophos - ***** 1

Device registration details

Model

XG126 (XG126E14MYFP36)

Company name

Alvecom

Contact person

Bastien

Registered email address

bastien@alvecom.fr

Module subscription

Add a subscription to your serial number or add time to your existing subscription.

Activate subscription

Module subscription details

Synchronize

Activate evaluations

Licensed subscriptions: Xstream Protection bundle. Extreme value and protection for your network. Includes essential network, web, and zero-day protection, and Sophos Central VPN orchestration [site-to-site and remote access] with advanced Central Firewall Reporting.

Xstream Protection bundle	Status	Expiration date
Base Firewall Stateful Firewall, VPN, Wireless	Subscribed	Dec 31, 2099
Network Protection IPS, ATP, SO-RED Device Management	Subscribed	Sep 14, 2024
Web Protection Web Security and Control, Application Control, Web Malware Protection	Subscribed	Sep 14, 2024
Zero-Day Protection Machine Learning, Sandboxing File Analysis, Threat Intelligence	Subscribed	Sep 14, 2024
Central Orchestration SD-WAN VPN Orchestration, CFR Advanced	Subscribed	Sep 14, 2024
Enhanced Support Enhanced Support	Subscribed	Sep 14, 2024

Sauvegardes

Backup

Backup mode

☐ Local

☐ FTP

☒ Email

Backup prefix

[SOPHOS_XG126_ALTERNANCE_VDM]

Email address *

support@alvecom.fr

Quarantine digest will be sent to the first email address only.

Frequency

☐ Never

☐ Daily

☒ Weekly

☐ Monthly

Schedule

Sunday

Day

00

HH

00

MM

Encryption password *











***** [Change Encryption password](#)

Apply

Backup now

De plus, Sophos central sauvegarde dans le cloud aussi






Définition des Zones pour chacun des VLANs

<input type="checkbox"/>	Etudiants	Etudiants	LAN	Ping/Ping6, DNS, Captive Portal, Client Authentication	 
<input type="checkbox"/>	VDP	VDP	LAN	Ping/Ping6, DNS	 
<input type="checkbox"/>	Administratif	Administratif	LAN	Ping/Ping6, DNS, User Portal, Captive Portal, Client Authentication	 
<input type="checkbox"/>	Management	Port1, Port8	LAN	Ping/Ping6, HTTPS, SSH, DNS, SNMP, Captive Portal	 
<input type="checkbox"/>	RED	To_Alvecom	LAN	Ping/Ping6, HTTPS, SSH, DNS, SNMP	 

Création des VLANs



Configuration Sophos XG

 Port1 Management Physique	Connecté 1000 Mbps - Full Duplex Auto-négocié	10.94.1.30/255.255.255.224 Statique	Matériel: Port1	
 Administratif Administratif VLAN	S.O. S.O.	10.94.1.254/255.255.255.128 Statique	Matériel: Port1.10 ID du VLAN: 30	
 Etudiants Etudiants VLAN	S.O. S.O.	10.94.0.254/255.255.255.0 Statique	Matériel: Port1.20 ID du VLAN: 20	
 VOIP VOIP VLAN	S.O. S.O.	10.94.1.126/255.255.255.192 Statique	Matériel: Port1.30 ID du VLAN: 30	

Création des différents DHCP

InterfacesZonesWAN link managerDNSDHCPIPv6 router advertisementCellular WANIP tunnelsNeighbors (ARP-NDP)Dynamic DNS

Server

Add

Delete


	Name	Interface	Lease detail		IP version	Status	Manage
			Dynamic	Static			
<input type="checkbox"/>	Default DHCP Server	Port1 - 10.94.1.30	10.94.1.1 - 10.94.1.2	View detail	IPv4	<div><div></div></div>	<div><div></div><div></div></div>
<input type="checkbox"/>	VOIP	VOIP - 10.94.1.126	10.94.1.100 - 10.94.1.110	-	IPv4	<div><div></div></div>	<div><div></div><div></div></div>
<input type="checkbox"/>	Admin	Administratif - 10.94.1.254	10.94.1.153 - 10.94.1.250	View detail	IPv4	<div><div></div></div>	<div><div></div><div></div></div>
<input type="checkbox"/>	Etudiant	Etudiants - 10.94.0.254	10.94.0.10 - 10.94.0.250	-	IPv4	<div><div></div></div>	<div><div></div><div></div></div>

Baux statiques

Hostname	MAC address	IP address
SWITCH	48:22:54:10:4E:4A	10.94.1.10
AP1	1C:61:B4:3D:10:CA	10.94.1.20
AP2	1C:61:B4:7A:0A:E0	10.94.1.21
AP3	1C:61:B4:7A:0C:DE	10.94.1.22
RNP-BUREAU-ADMIN	58:38:79:77:67:EF	10.94.1.151
RNP-BUREAU-FORMATEUR	58:38:79:70:06:24	10.94.1.152

Création du RED vers Alvecom

Configuration Sophos - ***** 3

All	VLAN	RED	Add interface	
Interface	Status/Interface speed	IP address	Mac	
 To Alvecom RED RED	Enabled Auto-negotiated	10.10.130.2/255.255.255.252 Static	Remote IP: 81.250.169.142	

Règles firewall

Configuration Sophos XG

1			LANs to WAN in 646 GB, out 1.25 GB							
1	2		AP to Onoda/NTP/D... in 18.61 MB, out 37.72 MB	Management, AP	WAN, DNS, onoda cont roller, N...	Any service	#0	Accept	[PS] [AS] [THREAT] [POST] [H...	[Unblock] [P...
1	3		Management to WAN in 0 B, out 0 B	Management, Any host	WAN, Any host	Any service	#5	Accept	[PS] [AS] [THREAT] [POST] [H...	[Unblock] [P...
1	4		Administratif to W... in 6.29 GB, out 879.04 MB	Administratif, Any host	WAN, Any host	Any service	#1	Accept	[PS] [AS] [THREAT] [POST] [H...	[Unblock] [P...
1	5		Etudiants to WAN in 79.97 KB, out 17.67 KB	Etudiants, Any host, Gue	WAN, Any host	Any service	#2	Accept	[PS] [AS] [THREAT] [POST] [H...	[Unblock] [P...
1	6		VDP to 3CX/DNS/N... in 360.42 MB, out 381.21 MB	VDP, Any host	WAN, DNS, 3cx, 3CX, N	Any service	#3	Accept	[PS] [AS] [THREAT] [POST] [H...	[Unblock] [P...
1	7		Avescom to All in 33.06 MB, out 11.61 MB	RED, Any host	Any zone, Any host	Any service	#8	Accept	[PS] [AS] [THREAT] [POST] [H...	[Unblock] [P...
1			LAN to LAN in 0 B, out 836.05 B							
1	8		Management to LAN in 0 B, out 836 B	Management, Any host	VDP, Administratif, Etad	Any service	#7	Accept	[PS] [AS] [THREAT] [POST] [H...	[Unblock] [P...
1	9		DENY in 3157 KB, out 773.35 KB	Any zone, Any host	Any zone, Any host	Any service	#4	Drop	[PS] [AS] [THREAT] [POST] [H...	[Unblock] [P...

Showing 10 of 10. Selected 0

Filtrage Web

administratif : filtrage par défaut pour du pro

étudiant : filtrage par défaut pour le pro + blocage online chat et social networking

Filtrage applicatif :

administratif : bloque niveau 4 et 5

étudiant : on bloque niveau 4 et 5 + tiktok, snapchat, instagram, reddit, twitter, discord

Route statique

Configuration Sophos - ***** 4

IPv4 unicast route						
	IP/netmask	Gateway	Interface	Administrative distance	Metric	Manage
	192.168.0.0 / 255.255.255.0	10.10.130.1	To_Avescom	1	0	[Edit] [Delete]
	10.10.1.0 / 255.255.255.0	10.10.130.1	To_Avescom	1	0	[Edit] [Delete]

Portail Captif

Configuration Sophos XG

Captive portal behavior

☐ Show user portal link

☒ Show web page after sign-in

Open web page

☒ In new browser window

☐ In captive portal window

Web page

☒ Originally requested by user

☐ Custom

Sign out user

☐ When captive portal page is closed or redirected

☒ When user is inactive

☐ Never

Traffic flow required to consider the user active

bytes in minutes

☐ Use insecure HTTP instead of HTTPS

Captive portal appearance

Layout

☒ Default layout

☐ Custom HTML

Logo

☐ Default

☒ Custom

Logo image

Choisir un fichier

Aucun fichier choisi

Logo link

Sign-in page header HTML

User prompt *

Connectez-vous à ce réseau

Username field label *

Nom d'utilisateur

Password field label *

Mot de passe

Sign-in button label *

Connexion

Sign-out button label *

Déconnexion

Sign-in page footer HTML

<p> En vous connectant vous acceptez la charte informatique</p>

footer html du Portail captif

Configuration Sophos - ***** 5

<p> En vous connectant vous acceptez la charte informatique</p>
Télécharger la charte informatiqu </p> Powered
by ALVECOM </p>

Certificats et clé serveur Web Sophos

https://drive.google.com/file/d/1HFxdh3LBUQ1LgM7J5S_29Ru66Gx98iN2/view?usp=sharing

ACL d'accès locales

Configuration Sophos XG

Local service ACL

Zone	Admin services		Authentication services				Network services			Other services						
	HTTPS	SSH	AD SSO	Captive portal *	Radius SSO	Client Authentication	Chromebook SSO	Ping/Ping6	DNS	Wireless Protection	SSL VPN	Web proxy	User Portal	Dynamic Routing	SMTP Relay	SNMP
LAN	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
WAN	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
DH2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
VPN	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
WiFi	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Etudiants	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
VVIP	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Administratif	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Management	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
RED	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>

* Wireless off services for wireless portal allow user authentication from wireless. If wireless block other user wireless authentication services.

Utilisateur Guest portail captif

Charte Informatique

Charte Informatique pour l'utilisation du WiFi de I***** *****

1. Introduction

La présente charte informatique a pour objectif de réglementer l'utilisation du réseau WiFi de

I***** *****. Le WiFi est un outil précieux qui offre un accès à Internet sans fil

à des fins éducatives et professionnelles. Il est essentiel que tous les utilisateurs respectent

cette charte afin de garantir un environnement en ligne sécurisé et efficace pour tous.

1. Accès au réseau WiFi

2.1. Utilisation autorisée Le réseau WiFi de I***** ***** est réservé à un usage

éducatif et professionnel. Les étudiants, le personnel enseignant et le personnel administratif

Configuration Sophos XG

peuvent utiliser le WiFi pour accéder à des ressources en ligne, effectuer des recherches,

communiquer et réaliser des activités liées à leurs études ou à leurs responsabilités

professionnelles.

2.2. Identifiants de connexion Chaque utilisateur doit utiliser ses propres identifiants de

connexion fournis par l'***** pour accéder au réseau WiFi. Les identifiants ne doivent pas être

partagés avec d'autres personnes.

2.3. Restriction d'accès L'accès au réseau WiFi peut être restreint ou bloqué pour des raisons

de sécurité ou de maintenance. L'***** se réserve le droit de prendre de telles mesures si

nécessaire.

1. Utilisation responsable

3.1. Respect des droits d'auteur Les utilisateurs doivent respecter les lois sur les droits d'auteur

et ne pas télécharger, partager ou accéder à du contenu protégé sans autorisation appropriée.

3.2. Respect de la vie privée Les utilisateurs doivent respecter la vie privée des autres et ne

pas accéder, modifier ou partager des informations personnelles sans autorisation appropriée.

3.3. Utilisation appropriée des ressources Les utilisateurs doivent utiliser le réseau WiFi de

manière responsable et appropriée. Toute activité illégale, frauduleuse, diffamatoire, obscène



Configuration Sophos XG

ou nuisible est strictement interdite.

3.4. Sécurité informatique Les utilisateurs doivent prendre des mesures de sécurité

appropriées pour protéger leurs appareils et les informations sensibles. Cela comprend

l'utilisation de mots de passe forts, la mise à jour régulière des logiciels de sécurité et la

vigilance face aux tentatives de phishing ou de logiciels malveillants.

1. Responsabilités

4.1. Responsabilité individuelle Chaque utilisateur est responsable de ses actions sur le réseau

WiFi. Tout comportement inapproprié ou en violation de cette charte peut entraîner des

sanctions disciplinaires.

4.2. Signalement des incidents Les utilisateurs doivent signaler tout incident ou comportement

suspect au responsable informatique de l'***** afin de maintenir un environnement en ligne

sûr et sécurisé.

4.3. Respect des règles supplémentaires En plus de cette charte, les utilisateurs doivent

respecter toutes les règles et politiques supplémentaires établies par l'***** concernant

l'utilisation des technologies de l'information et de la communication.



Configuration Sophos XG

1. Sanctions

En cas de violation de cette charte, des sanctions disciplinaires peuvent être appliquées,

conformément aux règles et procédures de l'*****. Les sanctions peuvent inclure la suspension

ou la résiliation de l'accès au réseau WiFi, ainsi que d'autres mesures disciplinaires

appropriées.

1. Révision de la charte

Cette charte informatique est sujette à révision périodique. Toute modification sera

communiquée aux utilisateurs, et il sera demandé à chaque utilisateur de confirmer son

acceptation de la charte mise à jour.

En vous connectant au réseau wifi, vous acceptez ces conditions.

Enfin le fichier de configuration en Backup

Il est envoyé par mail tous les dimanches soir à 23h.