

MANUEL DE CONFIGURATION DU SOPHOS

I-/ CONFIGURATION DE BASE.....	3
I.1-/ Configuration en mode passerelle	3
II-/ CONFIGURATION DU VPN CLIENT TO SITE	5
II.1-/ Définition des groupes vpn ssl et client.....	5
II.1.1-/ Définition des groupes vpn ssl	5
II.1.2-/ Définition des clients vpn ssl.....	6
II.2-/Définition des sous-réseaux et la plage de réseau des clients vpn	7
II.2.1-/ Définition des sous-réseaux	7
II.2.2-/ Définition du réseau des clients vpn	8
II.3-/Définition de la politique des clients vpn ssl distant.....	8
II.4-/ Vérification des services d'authentification pour le VPN SSL	10
II.5-/ Vérification des zones autorisées pour le VPN SSL	10
II.6-/ Configuration des paramètres VPN SSL avancés.....	11
II.7-/ Créer une règle de pare-feu	12
II.8-/ Configuration du client VPN SSL	14
II.8.1-/ Téléchargement du logiciel client SSL VPN	14
II.8.2-/ Installation du logiciel client SSL VPN sous Windows	15
II.9-/ Configuration de dyn Dns.....	16
III-/ Configuration des RED.....	17
III.1-/ Création de la zone	17
III.2-/ Configuration de base.....	18
III.3-/ Paramètres des liaisons montantes	21
III.4-/ Les paramètres du sous-réseau du RED	22
III.5-/ Le règle pour le fonctionnement des RED.....	22
.....	25
III.6-/ La connexion RED et livebox	25
IV- / Redirection de port	27
IV.1- / Le choix du paramètre.....	28
IV.2-/ La configuration de la redirection.....	28
V- / Migration Cyberoam en sophos	30
V.1-/ L es Appliance prise en charge	30
V.2-/ Les points à prendre en compte avant la migration	30

V.3-/ Les nouveauté apporté dans sophos	31
V.4-/ Les étapes de la migration.....	31
V.5-/ Le connecter a sophos	35
V.6 -/ Navigation dans sophos	36
V.7-/ Migration de la licence.....	36
V.8- / Transformation des règles aux stratégie de sécurités	37
V.9-/ Changement dans les caractéristiques	39
V.9.1-/ Caractéristiques sous licence.....	39
V.9.2-/ Pare-feu d'application Web (WAF).....	39
V.9.4-/ VPN SSL.....	40
V.9.5-/ Filtrage Web et d'application	41
V.9.6-/ Identité.....	41
V.9.7-/ Haute disponibilité (HA)	41
V.9.8-/ Certificats.....	41
V.9.9-/ DHCP / PPPoE	42
V.9.10-/ SNMP	42
V.10-/ Arrêter les fonctions de CR	42
VI-/ La configuration du waf et les règles qui l'accompagnes.....	43
VI.1-/ Configuration du waf	43
VI.2-/ Règle du waf	43
VII-/ Configuration du routeur Dray tek en pont	45
VIII-/ L'utilisation d'un seul certificat pour le déploiement de plusieurs sites.....	47
VIII.1-/ Configuration du waf	47
VIII.2-/ Règle du waf	48
VIII. 3-/ Règle pour un autre site	50
VIII.4-/ Déploiement de site dans IIS.....	51
VIII.4-/ Routage statique d'une adresse IP (CAS RCMEC).....	52

I-/ CONFIGURATION DE BASE

I.1-/ Configuration en mode passerelle

La Gateway ou passerelle est un dispositif destiné à connecter des réseaux de télécommunication ayant des architectures différentes ou des protocoles différents, ou offrant des services différents. Une passerelle peut par exemple connecter un réseau local d'entreprise avec un autre réseau local ou un réseau public de données. Dans les entreprises, la passerelle est l'appareil qui achemine le trafic à partir d'un poste de travail au réseau extérieur. Dans les maisons, la passerelle est le FAI qui relie l'utilisateur à Internet. Le sophos lorsqu'il est déployé en mode passerelle achemine le trafic en sein du réseau.

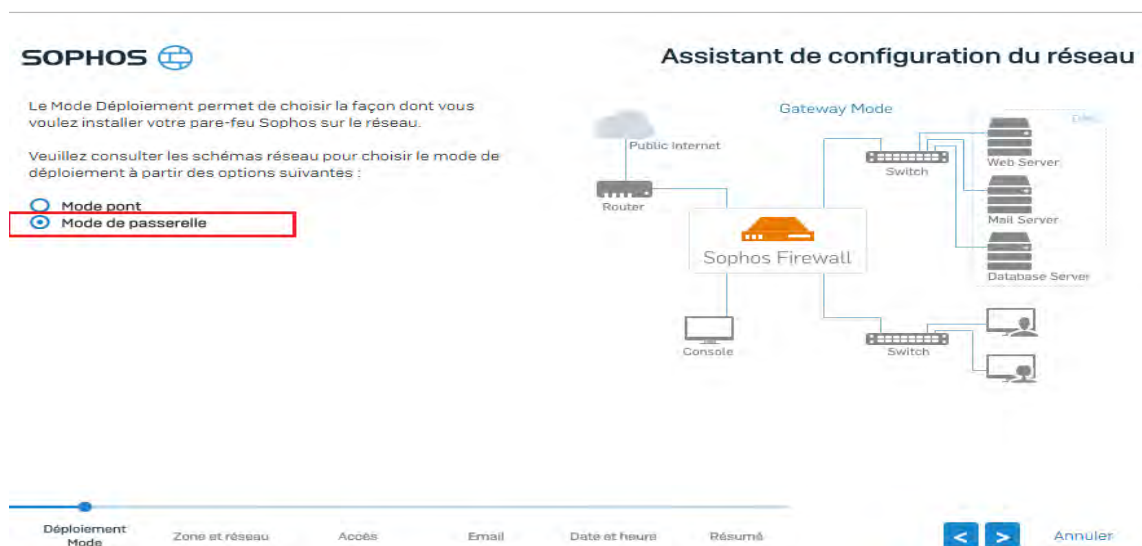
Le mode Gateway fournit une solution idéale pour les réseaux qui ont déjà un pare-feu existant et prévoit de remplacer leur pare-feu existant et qui souhaitent ajouter la sécurité par le biais approfondie des paquets de contrôle de sophos, Prévention intrusion, Gateway Antiviruset Gateway Anti spam. Si vous ne disposez pas de sophos modules de sécurité abonnements, vous pouvez vous inscrire pour un essai gratuit.

Sophos Appliance doit être déployé en mode passerelle lorsque :

- Vous souhaitez remplacer votre pare-feu ou un routeur agissant existant en tant que passerelle
- Vous voulez que votre passerelle agit comme un concentrateur VPN
- Vous voulez éviter la redondance dans votre réseau en utilisant le multibras et HA (haute disponibilité) caractéristiques de sophos
- Vous souhaitez configurer zone DMZ séparée pour protéger les serveurs de zone LAN et WAN.

Pour configurer le mode Gateway on procède comme suit :

- 1- Cliquez sur assistant et cet écran s'affiche et cochez le mode passerelle



- 2- Cliquez sur le bouton suivant ensuite sur suivant en renseignez successivement comme suit

Configuration du port

Port1	<input type="radio"/> Obtenir une IP par DHCP
Port2	<input type="radio"/> Obtenir une IP par PPPoE
Port3	<input checked="" type="radio"/> Utiliser une IP statique
Port4	
Adresse IP	<input type="text" value="192.168.10.110"/>
Masque de sous-réseau	<input type="text" value="255.255.255.0"/>
Zone	<input type="text" value="LAN"/>

Zone et Réseau vous permet de configurer les interfaces sur votre appareil, y compris vos paramètres DNS.

Vous pouvez sélectionner la méthode d'attribution des adresses IP sur DHCP, PPPoE ou IP statique. Avant cela, veuillez-vous munir des informations nécessaires concernant votre schéma réseau.

Déploiement
Mode

Zone et réseau

Accès

Email

Date et heure

Résumé



Annuler

Port 1 : c'est le port Lan. C'est ici que s'effectue la configuration de notre réseau local

3- On sélectionne la zone Lan et on clique sur suivant et renseigner comme ci-dessous

Configuration du port

Port1	<input type="radio"/> Obtenir une IP par DHCP
Port2	<input type="radio"/> Obtenir une IP par PPPoE
Port3	<input checked="" type="radio"/> Utiliser une IP statique
Port4	
Adresse IP	<input type="text" value="192.168.1.4"/>
Masque de sous-réseau	<input type="text" value="255.255.255.0"/>
Zone	<input type="text" value="WAN"/>
Détails de la passerelle	
Nom de la passerelle	<input type="text" value="GLORY"/>
Adresse IP	<input type="text" value="192.168.1.10"/>

Zone et Réseau vous permet de configurer les interfaces sur votre appareil, y compris vos paramètres DNS.

Vous pouvez sélectionner la méthode d'attribution des adresses IP sur DHCP, PPPoE ou IP statique. Avant cela, veuillez-vous munir des informations nécessaires concernant votre schéma réseau.

Déploiement
Mode

Zone et réseau

Accès

Email

Date et heure

Résumé



Annuler

Port : c'est le port Wan c.-à-d. le port d'arrivée Internet

192.168.1.4 : c'est l'adresse IP délivré par le routeur ADSL au routeur sophos

192.168.1.10 : C'est l'adresse IP du routeur ADSL qui représente la patte du sophos

4- Renommer le nom de la passerelle et puis cliquez sur suivant pour configurer le Dns

Configuration DNS

Configuration IPv4

- ☐ Récupérer le DNS à partir de DHCP
☐ Récupérer le DNS à partir de PPPoE
☒ DNS statique

DNS 1
DNS 2
DNS 3

Configuration du nom d'hôte

Nom d'hôte
Description

En fonction de la méthode d'attribution des adresses IP sélectionnée sur la page précédente, la configuration DNS sera automatiquement sélectionnée. Si vous avez choisi DHCP ou PPPoE comme méthode d'attribution des adresses IP, l'adresse DNS sera reçue de la même manière. Vous pouvez quand même indiquer le DNS statique, et en cas de serveurs DNS multiples, ils seront interrogés dans l'ordre de saisie.

Déploiement
Mode

Zone et réseau

Accès

Email

Date et heure

Résumé



Annuler

NB : le DNS ici doit être configuré avec les paramètres par défaut de Google

5- Cliquez sur suivant successivement puis sur terminer

Aperçu de la configuration

Port1

IPAddress: 192.168.10.110
NetMask : 255.255.255.0
Zone : LAN

Port2

IPAddress: 192.168.1.4
NetMask : 255.255.255.0
Zone : WAN

Port3

Sophos Adaptive Learning

Comprendre comment les clients utilisent Sophos Firewall nous aide à créer de meilleurs produits. Le produit envoie périodiquement à Sophos des informations qui sont utilisées pour améliorer la stabilité du produit, raffiner les priorités des fonctionnalités et améliorer l'efficacité de la protection. Retrouvez plus de renseignements sur les données que nous collectons dans l'aide en ligne.

☒ Envoyer les données application et menace

Déploiement
Mode

Zone et réseau

Accès

Email

Date et heure

Résumé

Annuler



Terminer

II-/ CONFIGURATION DU VPN CLIENT TO SITE

II.1-/ Définition des groupes vpn ssl et client

II.1.1-/ Définition des groupes vpn ssl

Le groupe vpn ssl est le regroupement de tous les clients vpn distant. Pour un **besoin d'administration** des clients vpn il est important de regrouper tous les clients dans un groupe et sous une appellation.

Pour créer un client vpn on procède comme suit :

- 1- Cliquez sur le menu authentification puis groupe
- 2- Cliquez sur ajouter et renseigner comme suit

Authentification Visionneuse de journaux Aide admin HOME TECHNOLOGY

[Serveurs](#)
[Services](#)
[Groupes](#)
[Utilisateurs](#)
[Mot de passe à usage unique](#)
[Portail captif](#)
[Utilisateurs invités](#)
[Utilisateurs sans client](#)
[STAS](#)
[...](#)

Nom du groupe * REMOTE SSL VPN GROUP

Description

Type de groupe * Normal

Stratégies

Quota de navigation * Unlimited Internet Access

Temps d'accès * Allowed all the time

Trafic réseau None

Régulation de flux None

Accès à distance * SSL POLICY

[Enregistrer](#)
[Ajouter des membres](#)
[Afficher les membres du groupe](#)
[Annuler](#)

3- Cliquez sur enregistrer

II.1.2-/ Définition des clients vpn ssl

Le client vpn ssl c'est l'entité distant qui devrait s'il le souhaite se connecter depuis l'ordinateur a tous moment quel que soit le lieu où il se trouve. Pour cela on procède comme suit :

- 1- Cliquez sur authentification puis sur utilisateur
- 2- Cliquez sur Ajouter et renseigner comme suite

Authentification Visionneuse de journaux Aide admin HOME TECHNOLOGY

[Serveurs](#)
[Services](#)
[Groupes](#)
[Utilisateurs](#)
[Mot de passe à usage unique](#)
[Portail captif](#)
[Utilisateurs invités](#)
[Utilisateurs sans client](#)
[STAS](#)
[...](#)

Modifier l'utilisateur

Nom d'utilisateur * dg

Nom *

Description

Mot de passe * ***** [Modifier Mot de passe](#)

Type d'utilisateur * ☒ Utilisateur ☐ Administrateur

Profil * Profil

Email * Séparez les différentes adresses électroniques par une virgule

Temps d'utilisation d'Internet 00:17 (HH:MM)

Stratégies

[Enregistrer](#)
[Réinitialiser la comptabilisation des utilisateurs](#)
[Voir l'utilisation](#)
[Annuler](#)

Authentication Visionneuse de journaux Aide admin HOME TECHNOLOGY

[Serveurs](#)
[Services](#)
[Groupes](#)
[Utilisateurs](#)
[Mot de passe à usage unique](#)
[Portail captif](#)
[Utilisateurs invités](#)
[Utilisateurs sans client](#)
[STAS](#)
[...](#)

Stratégies

Groupe * REMOTE SSL VPN GROUP

Quota de navigation * Unlimited Internet Access ⓘ

Temps d'accès * Allowed all the time ⓘ

Trafic réseau None ⓘ

Régulation de flux None ⓘ

Stratégie SSL VPN

Accès à distance * SSL POLICY ⓘ

Sans client * Aucune stratégie appliquée ⓘ

L2TP * ☒ Activer ☐ Désactiver Adresse IP ⓘ

[Enregistrer](#)
[Réinitialiser la comptabilisation des utilisateurs](#)
[Voir l'utilisation](#)
[Annuler](#)

3- Cliquez sur Enregistrer

II.2-/Définition des sous-réseaux et la plage de réseau des clients vpn

II.2.1-/ Définition des sous-réseaux

Les sous-réseaux sont des segments du réseau que l'on définit pour une utilisation éventuelle

Pour créer un sous réseau on procède comme suit :

- 1- Cliquez sur hôte et service puis sur IP hôte
- 2- Cliquez sur Ajouter et renseigner comme suit

Modifier l'hôte IP Visionneuse de journaux Aide admin HOME TECHNOLOGY

[Hôte IP](#)
[Groupe d'hôte IP](#)
[Hôte MAC](#)
[Hôte FQDN](#)
[Groupe d'hôte FQDN](#)
[Groupe de pays](#)
[Services](#)
[Groupe de services](#)

Nom * LOCAL

Famille d'IP * IPv4

Type * Réseau

Adresse IP * 192.168.10.0 Sous-réseau /24 [255.255.255.0]

Groupe d'hôte IP

[Ajouter un nouvel élément](#)

3- Puis cliquez sur enregistrer

II.2.2-/ Définition du réseau des clients vpn

C'est le réseau des clients vpn distant ce qui signifie que si un utilisateur ne se trouve pas dans ce réseau il lui sera impossible de se connecter au vpn.

- 1- Cliquez sur Hôte et services puis sur hôte IP
- 2- Cliquez sur Ajouter et renseigner comme suit

The screenshot shows a web interface titled "Modifier l'hôte IP". In the top right corner, there are links for "Visionneuse de journaux", "Aide", and "admin", along with the text "HOME TECHNOLOGY". Below the title is a horizontal tab bar with the following tabs: "Hôte IP", "Groupe d'hôte IP", "Hôte MAC", "Hôte FQDN", "Groupe d'hôte FQDN", "Groupe de pays", "Services", and "Groupe de services". The "Hôte IP" tab is currently selected. The main content area contains the following fields:

- Nom ***: A text input field containing the word "REMOTE".
- Famille d'IP ***: A dropdown menu currently set to "IPv4".
- Type ***: A dropdown menu currently set to "Plage d'IP".
- Adresse IP ***: Two text input fields separated by a hyphen. The first field contains "10.10.1.2" and the second field contains "10.10.1.254".
- Groupe d'hôte IP**: A large, empty rectangular box.
- Below the "Groupe d'hôte IP" box is a button labeled "Ajouter un nouvel élément".

- 3- Cliquez sur Enregistrer pour terminer

II.3-/Définition de la politique des clients vpn ssl distant

La politique c'est un ensemble de règle définie strictement établissant le comportement du vpn. Elle définit la manière donc les utilisateurs se connectent à distance. Pour créer la politique on procède comme suit :

- 1- Cliquez sur vpn puis sur ssl vpn (accès distance)
- 2- Cliquez sur Ajouter et renseigner comme suit

VPN

[Visionneuse de journaux](#) [Aide](#) [admin](#) [HOME TECHNOLOGY](#)

[Afficher les paramètres VPN](#)

[Connexions IPsec](#) [SSL VPN \(accès à distance\)](#) [SSL VPN \(Site à Site\)](#) [Client VPN CISC0&.c](#) [L2TP \(Accès à distance\)](#) [Accès sans client](#) [Favoris](#) [Groupes de favoris](#) [PPTP \(Accès à distance\)](#) [Profils IPsec](#)

Paramètres généraux

Nom *

SSL POLICY

Description

Saisir une description

Identité

Membres de la stratégie

Open Group

REMOTE SSL VPN GROUP

dg

josue

Appliquer

Annuler

VPN

[Visionneuse de journaux](#) [Aide](#) [admin](#) [HOME TECHNOLOGY](#)

[Afficher les paramètres VPN](#)

[Connexions IPsec](#) [SSL VPN \(accès à distance\)](#) [SSL VPN \(Site à Site\)](#) [Client VPN CISC0&.c](#) [L2TP \(Accès à distance\)](#) [Accès sans client](#) [Favoris](#) [Groupes de favoris](#) [PPTP \(Accès à distance\)](#) [Profils IPsec](#)

ACCES tunnel

Utiliser comme passerelle par défaut

ON

Ressources réseau autorisées (IPv4)

LOCAL

Ajouter un nouvel élément

Ressources réseau autorisées (IPv6)

Ajouter un nouvel élément

Délai d'inactivité

Appliquer

Annuler

VPN

[Visionneuse de journaux](#) [Aide](#) [admin](#) [HOME TECHNOLOGY](#)

[Afficher les paramètres VPN](#)

[Connexions IPsec](#) [SSL VPN \(accès à distance\)](#) [SSL VPN \(Site à Site\)](#) [Client VPN CISC0&.c](#) [L2TP \(Accès à distance\)](#) [Accès sans client](#) [Favoris](#) [Groupes de favoris](#) [PPTP \(Accès à distance\)](#) [Profils IPsec](#)

Ajouter un nouvel élément

Ressources réseau autorisées (IPv6)

Ajouter un nouvel élément

Délai d'inactivité

Déconnecter les clients inactifs

ON

Remplacer le délai d'inactivité global (Valeur par défaut 15 Minutes)

Minutes [15-60]

Appliquer

Annuler

3- Cliquez sur enregistrer

II.4-/ Vérification des services d'authentification pour le VPN SSL

Il s'agit de la vérification des services qui doivent être configurée pour que le vpn fonctionne correctement. Pour se faire on procède comme suit :

- 1- Cliquez sur authentification puis sur services
- 2- Cocher comme ci-dessous (Vérifiez que le serveur d'authentification local est sélectionné dans la section Méthodes d'authentification SSL VPN)

Authentification Visionneuse de journaux Aide admin HOME TECHNOLOGY

Serveurs Services Groupes Utilisateurs Mot de passe à usage unique Portail captif Utilisateurs invités Utilisateurs sans client STAS ...

Méthodes d'authentification SSL VPN

☐ Identiques au VPN
☐ Identiques au pare-feu
☒ Définir des méthodes d'authentification pour le SSL VPN

Liste des serveurs d'authentification...
saisir un texte pour la recherche...
☒ Local

Serveur d'authentification sélectionné...
Local

faire glisser pour modifier la priorité

Appliquer

Remarque: Assurez-vous également que le serveur d'authentification local est sélectionné dans la section Méthodes d'authentification par pare-feu. Cela est nécessaire pour les utilisateurs distants pour se connecter au portail pour télécharger le logiciel client SSL VPN plus loin dans cet article.

Authentification Visionneuse de journaux Aide admin HOME TECHNOLOGY

Serveurs Services Groupes Utilisateurs Mot de passe à usage unique Portail captif Utilisateurs invités Utilisateurs sans client STAS ...

Méthodes d'authentification du pare-feu

Liste des serveurs d'authentification...
saisir un texte pour la recherche...
☒ Local

Serveur d'authentification sélectionné...
Local

faire glisser pour modifier la priorité

Groupe par défaut Open Group

Appliquer

Méthodes d'authentification VPN (IPsec/L2TP/PPTP)

- 3- Cliquez sur Appliquer pour enregistrer

II.5-/ Vérification des zones autorisées pour le VPN SSL

Cette vérification permet d'autoriser le vpn seulement à la zone autorisée afin de travailler en toute sécurité. Cette vérification se fait de la manière suivante :

- 1- Cliquez sur Administration puis sur accès à l'appareil
- 2- Et cochez comme ci-dessous

Administration Visionneuse de journaux Aide admin HOME TECHNOLOGY

Licence **Accès à l'appareil** Paramètres d'administration Gestion centrale Temps Paramètres de notification SNMP Netflow Messages

ACL des services locaux

Zone	Services admin			Services d'authentification				Services de réseau			Autres services					
	HTTPS	Telnet	SSH	NTLM	Portail captif	Radius SSO	Client Authentication	Ping/Ping6	DNS	Wireless Protection	SSL VPN	Proxy Web	User Portal	Dynamic Routing	SMTP Relay	SNMP
LAN	<input checked="" type="checkbox"/>	<input 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 type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
WAN	<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"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
DMZ	<input checked="" type="checkbox"/>	<input 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"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input 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 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 type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Appliquer

- 3- Cliquez sur Application

II.6-/ Configuration des paramètres VPN SSL avancés

C'est ici qu'on paramètre les options nécessaires au bon fonctionnement du vpn. On a la possibilité de vérifier la plage de location IPv4 configurée précédemment et définissez le reste des options si nécessaire. Pour faire le paramétrage on procède comme suit :

- 1- Cliquez sur vpn et sur le bouton en rouge

VPN Visionneuse de journaux Aide admin HOME TECHNOLOGY

Connexions IPsec **Afficher les paramètres VPN** SSL VPN (accès à distance) SSL VPN (Site à Site) Client VPN CISC0&,c L2TP (Accès à distance) Accès sans client Favoris Groupes de favoris PPTP (Accès à distance) Profils IPsec

Connexions IPsec

Afficher d'autres propriétés Ajouter Supprimer Assistant

<input type="checkbox"/>	Nom	Nom du groupe	Stratégie	Type de connexion	État	Connexion	Gestion
<input type="checkbox"/>					Actif		

Données introuvables

Groupe de basculement

Ajouter Supprimer

<input type="checkbox"/>	Nom	État	Connexion	Gestion
<input type="checkbox"/>				

Données introuvables

- 2- Puis renseigner comme suit

VPN

[Visionneuse de journaux](#)
[Aide](#)
[admin](#)
HOME TECHNOLOGY

Paramètres

Fermer les paramètres VPN

VPN SSL
L2TP

Paramètres SSL VPN

Protocole *

☒ TCP
☐ UDP
(Sélectionner l'UDP pour des performances accrues)

Certificat serveur SSL *

ApplianceCertificate

Remplacer le nom d'hôte

Plage d'attribution des IPv4 *

10.10.1.2 - 10.10.1.254
(Doit provenir des plages d'IP privées. La première IP de la plage sera utilisée par le serveur.)

Masque de sous-réseau *

/24 (255.255.255.0)

Bail IPv6 (IPv6/Préfixe) *

2001:db8::1:0 / 64

Mode bail *

IPv4 uniquement

DNS IPv4

Principal
Secondaire

WINS IPv4

Principal
Secondaire

Nom de domaine

Appliquer

VPN

[Visionneuse de journaux](#)
[Aide](#)
[admin](#)
HOME TECHNOLOGY

Paramètres

Fermer les paramètres VPN

VPN SSL
L2TP

Algorithme de chiffrement

AES-128-CBC

Algorithme d'authentification

SHA2 256

Taille de la clé

2048 bit

Durée de vie de la clé

28800

Secondes

Paramètres de compression

☒ Compresser le trafic SSL VPN

Paramètres de débogage

☐ Activer le mode de débogage

Appliquer

3- Cliquez sur Appliquer

II.7-/ Créer une règle de pare-feu

Pour créer une règle on procède comme suit :

- 1- Cliquez sur pare-feu puis sur Ajouter une règle
- 2- Renseigner comme ci-dessous

Modifier Règle d'utilisateur / de réseau

[Visionneuse de journaux](#) [Aide](#) [admin](#) [HOME TECHNOLOGY](#)

Nom de la règle * <input type="text" value="RÈGLE D'ACCÈS DISTANT"/>	Description <input type="text" value="Saisir Description"/>
Action <input type="button" value="Accepter"/> <input type="button" value="Annuler"/> <input type="button" value="Refuser"/>	

Source

Zones émettrices * <input type="text" value="VPN"/> <input type="button" value="Ajouter un nouvel élément"/>	Réseaux et appareils émetteurs * <input type="text" value="REMOTE"/> <input type="button" value="Ajouter un nouvel élément"/>	Lors d'heure planifiée <input type="text" value="Tout le temps"/>
---	--	---

Modifier Règle d'utilisateur / de réseau

[Visionneuse de journaux](#) [Aide](#) [admin](#) [HOME TECHNOLOGY](#)

Destination & services

Zone de destination * <input type="text" value="LAN"/> <input type="button" value="Ajouter un nouvel élément"/>	Réseaux de destination * <input type="text" value="LOCAL"/> <input type="button" value="Ajouter un nouvel élément"/>	Services * <input type="text" value="Tous"/> <input type="button" value="Ajouter un nouvel élément"/>
--	---	--

Identité

<input checked="" type="checkbox"/> Faire correspondre les utilisateurs connus <input type="checkbox"/> Afficher le portail captif aux utilisateurs inconnus	Utilisateur ou groupes * <input type="text" value="REMOTE SSL VPN GROUP"/> <input type="button" value="Ajouter un nouvel élément"/> <input type="checkbox"/> Exclure l'activité de cet utilisateur de la comptabilisation des données
---	---

Modifier Règle d'utilisateur / de réseau

[Visionneuse de journaux](#) [Aide](#) [admin](#) [HOME TECHNOLOGY](#)

Avancés

Applications utilisateur Prévention des intrusions ⚠ <input type="text" value="Aucune"/> Stratégie de régulation de flux <input type="text" value="Stratégie de l'utilisateur appliquée"/> Stratégie Web ⚠ <input type="text" value="Aucune"/> <input type="checkbox"/> Appliquer une Stratégie de régulation de flux de catégorie Web Contrôle des applications ⚠ <input type="text" value="Aucune"/> <input type="checkbox"/> Appliquer une Stratégie de régulation de flux d'application	Protection synchronisée ⚠ Source HD minimale autorisée : <input type="radio"/> GREEN <input type="radio"/> YELLOW <input checked="" type="radio"/> No Restriction <input type="checkbox"/> Bloquer les clients sans Heartbeat Destination HD minimale autorisée : <input type="radio"/> GREEN <input type="radio"/> YELLOW <input checked="" type="radio"/> No Restriction <input type="checkbox"/> Bloquer la requête de destination sans Heartbeat	NAT & routage <input type="checkbox"/> Réécrire l'adresse source (déguiement) Passerelle principale <input type="text" value="Aucune"/> Passerelle de secours <input type="text" value="Aucune"/> Marquage DSCP <input type="text" value="Sélectionner le marquage DSCP"/>
--	---	---

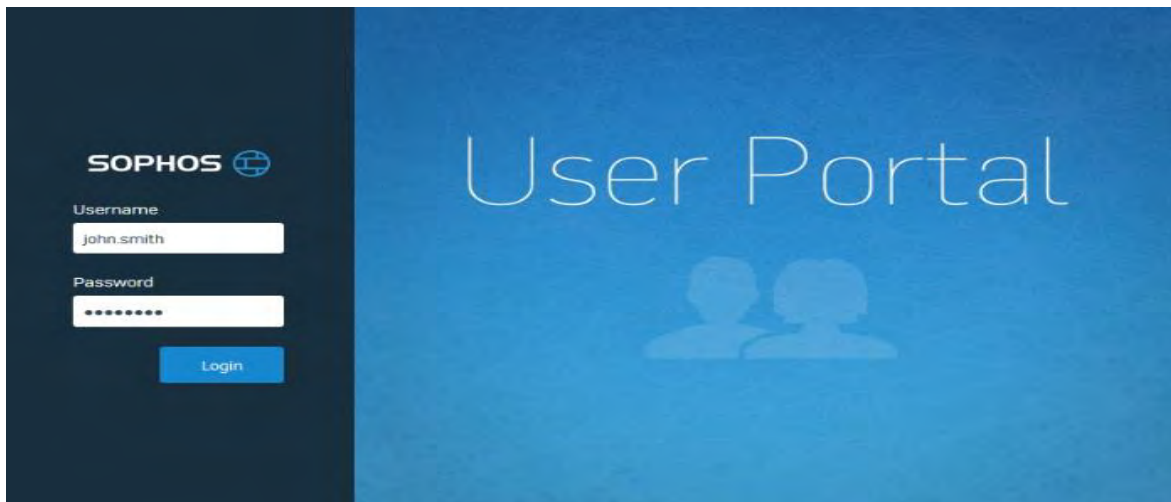
Enregistrement du trafic

3- Cliquez sur Appliquer

II.8-/ Configuration du client VPN SSL

II.8.1-/ Téléchargement du logiciel client SSL VPN

Par le biais du navigateur, connectez-vous au portail utilisateur à l'aide de l'adresse IP publique du pare-feu Sophos et du port https du portail utilisateur. Dans cet exemple, le portail utilisateur est accessible à l'adresse <https://172.20.120.15:443>



Remarque: Vous pouvez trouver le port https du portail utilisateur configuré dans le pare-feu Sophos en accédant à la section Administration> Paramètres administrateur sous la section Paramètres du port administrateur.

Administration Visionneuse de journaux Aide admin HOME TECHNOLOGY

Licence Accès à l'appareil Paramètres d'administration Gestion centrale Temps Paramètres de notification SNMP Netflow Messages

Description

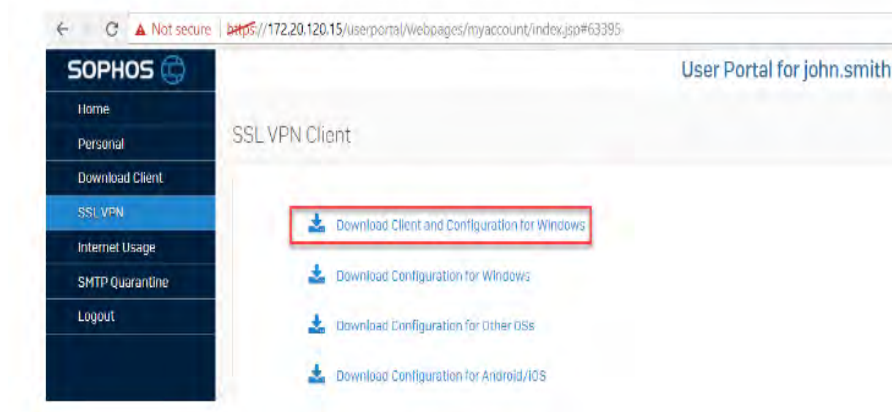
Paramètres du port admin

Port HTTPS de la console d'administration *

Port HTTPS du portail utilisateur *

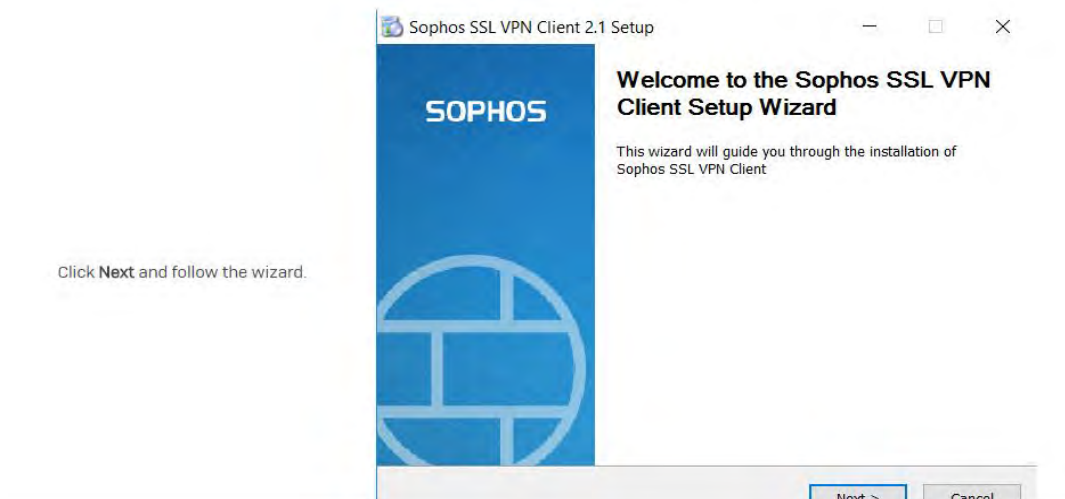
Certificat * (le certificat sélectionné sera utilisé pour Mon Compte, le Portail Captif, le Portail d'enregistrement et le Portail de réponses)

Une fois connecté au portail, téléchargez le client VPN SSL pour le point de terminaison requis en conséquence. Dans cet article, nous allons télécharger et installer le client et la configuration.

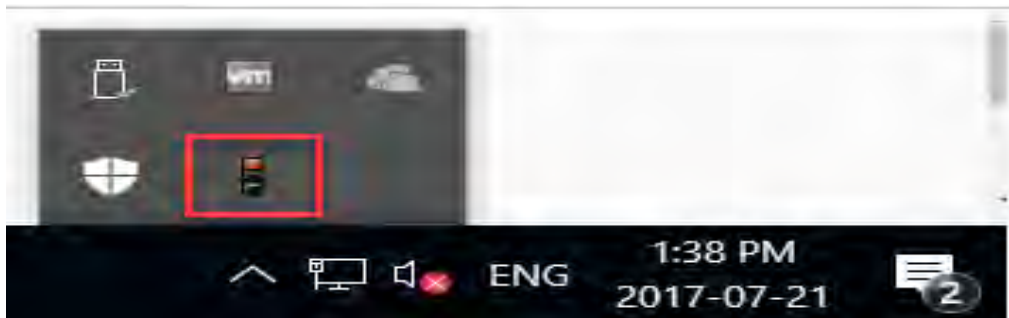


II.8.2-/ Installation du logiciel client SSL VPN sous Windows

Exécutez le client SSL VPN téléchargé.

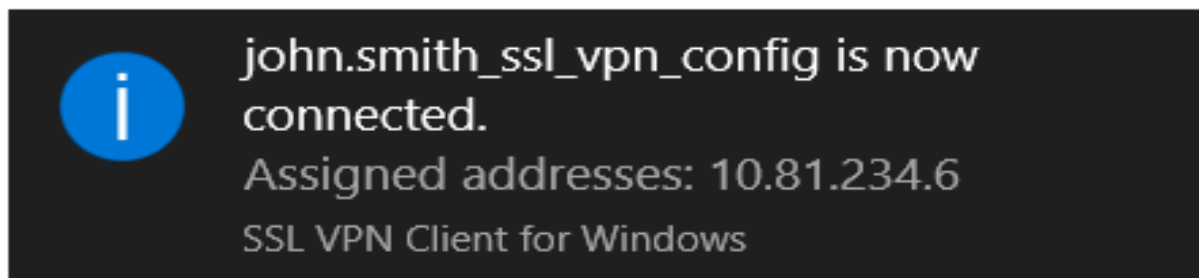


Une fois installé, démarrez l'authentification VPN en cliquant sur le symbole du feu dans la barre des tâches.



Connectez-vous en utilisant les mêmes informations d'identification pour le portail utilisateur.

Le feu de circulation passe du rouge (débranché) au rouge et à l'ambre (négociation / connexion). Dès que le feu passe au vert, un message contextuel apparaît confirmant que la connexion VPN SSL est établie



II.9-/ Configuration de dyn Dns

Dyn est un service informatique et l'entreprise informatique américaine éponyme. Il permet aux utilisateurs d'une adresse IP dynamique de pouvoir quand même l'associer à un nom de domaine. Le serveur DNS (Domain Name System) reçoit la nouvelle adresse IP via un petit programme et met à jour le nom de domaine ou de sous-domaine attaché à l'adresse IP.

Sophos donne la possibilité de configurer Dyn dns lorsque l'adresse du port B c.-à-d. le port Wan n'est pas une adresse IP fixe. Pour configurer le dyndns on procède comme suit :

- 1- Cliquez sur réseau puis sur Dns dynamique
- 2- Renseigner comme ci-dessous

Réseau

Visionneuse de journaux
Aide
admin
HOME TECHNOLOGY

Interfaces
Zones
Gestionnaire des liens WAN
DNS
DHCP
Annonce de routeur IPv6
WAN cellulaire
Tunnels IP
Voisins (ARP-NDP)
DNS dynamique

Détails de l'hôte

Nom d'hôte *
celpaid.myfirewall.co
(Exemple :xyz.dyndns.com)

Interface *
Port2 - 192.168.1.4

Adresse IPv4 *

Utiliser le port IP
IP publique traduite

Intervalle de vérification et de modification de l'IP *
4
4 à 60 minutes

Informations sur le fournisseur de services

Fournisseur de services *
Sophos

Enregistrer
Annuler

Hôte : **c'est votre nom de domaine** qui sera rattaché à l'IP dynamique

Interface : **c'est le port Wan (ici ce n'est pas une adresse IP publique)**

Fournisseur de service : **sophos (il s'agit ici du dyndns de sophos)**

3- Cliquer sur enregistrer

III-/ Configuration des RED

III.1-/ Création de la zone

Il est plus facile de créer une zone où on regroupera tous les RED. Cela **facilitera l'administration et la maintenance** des RED et la procédure pour la création des RED est la suivante :

1- Cliquez sur réseau> zone>Ajouter et renseigner comme ci-dessous

Réseau Visionneuse de journaux Aide admin HOME TECHNOLOGY

Interfaces Zones Gestionnaire des liens WAN DNS DHCP Annonce de routeur IPv6 WAN cellulaire Tunnels IP Voisins (ARP-NDP) DNS dynamique

Ajouter une zone

Nom * LAN_FILIALE

Description Saisir une description

Type * ☒ LAN ☐ DMZ

Membres Aucune

Accès à l'appareil Services admin

☒ HTTPS ☐ TELNET ☐ SSH

Services d'authentification

☐ Authentification client ☐ Portail captif ☐ NTLM ☐ Radius SSO

Services de réseau

Enregistrer Annuler

2- Cliquez sur enregistrer

3- Cliquez sur administration >Accès à l'appareil et cocher les éléments comme indiqué

Administration Visionneuse de journaux Aide admin HOME TECHNOLOGY

Licence Accès à l'appareil Paramètres d'administration Gestion centrale Temps Paramètres de notification SNMP Netflow Messages

ACL des services locaux

Zone	Services admin			Services d'authentification				Services de réseau		Autres services						
	HTTPS	Telnet	SSH	NTLM	Portail captif	Radius SSO	Client Authentication	Ping/Ping6	DNS	Wireless Protection	SSL VPN	Proxy Web	User Portal	Dynamic Routing	SMTP Relay	SNMP
LAN	<input checked="" type="checkbox"/>	<input 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 type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
WAN	<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"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
DMZ	<input checked="" type="checkbox"/>	<input 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"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input 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 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 type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
LAN_FILIALE	<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"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Appliquer

III.2-/ Configuration de base

Il s'agira pour nous de donner étape par étape dans les moindres détails la configuration des RED.
Cette configuration a été détachée en sept étapes.

Etape 1 : Relever l'ID du RED

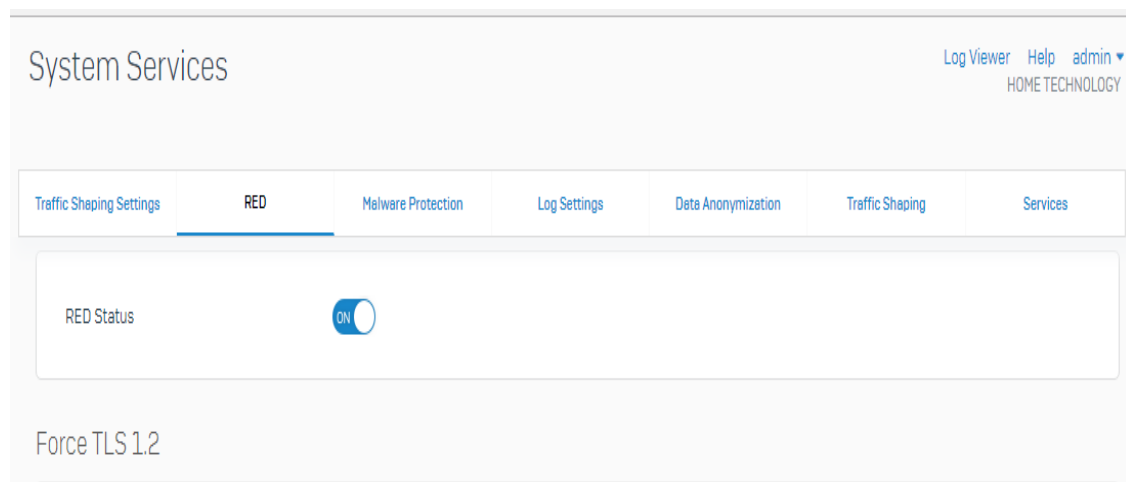
Il s'agit de relever l'ID du RED à l'arrière de l'équipement



Etape 2 : Connectez-vous au SOPHOS XG

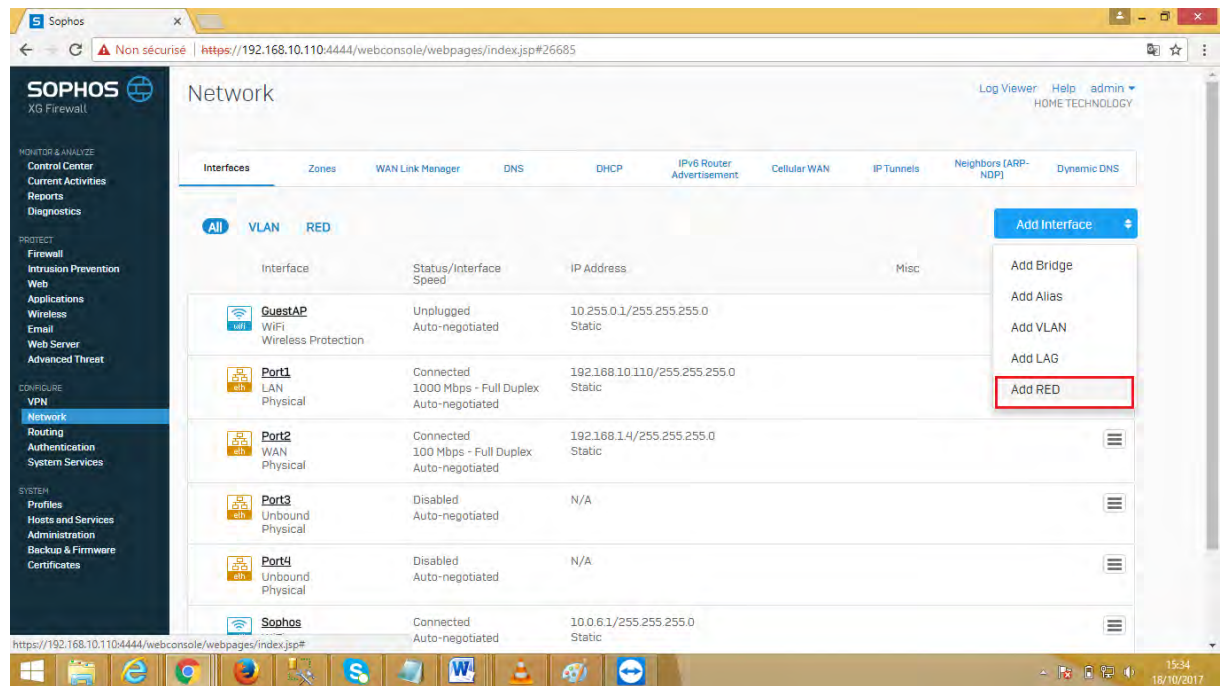
Etape 3 : assurez-vous que vous êtes sur la dernière version [SFOS 16.05.1] si vous prévoyez de configurer un "RED 15w" ou un "serveur rouge RED Firewall \ Client Interface

Etape 4 : Activer la configuration RED sur votre pare-feu XG en allant dans (Configurer \ System Services \ RED)



Etape 4 : **Création du l'interface RED**

Il s'agira tout simplement d'ajouter une interface pour le RED et cela se fait en cliquant sur réseau>Interface>Ajouter une Interface>Ajouter RED



Etape 5 : Renseigner tous les paramètres du RED

The 'RED Settings' form includes the following fields and options:

- A)** Branch Name *: Warsaw Office
- B)** Type: RED 15w
- C)** RED ID *: [Redacted]
- D)** Tunnel ID *: Automatic
- E)** Unlock Code *: [Empty]
- F)** Firewall IP/Hostname *: 95.75.117.45
- G)** 2nd Firewall IP/Hostname: [Empty]
- H)** Use 2nd IP/Hostname for: ☒ Failover ☐ Load Balancing
- I)** Description: [Empty]
- J)** Device deployment: ☒ Automatically via Provisioning Service ☐ Manually via USB Stick

A : Nom de l'Office à distance, le RED sera déployé

B : Le type d'appareil RED que vous déploierez

C : L'ID RED que vous avez trouvé à l'arrière de l'appareil RED

D : L'identification du tunnel reconnu par le pare-feu

E : Cela peut être prédéfini ou laissé vider pour être généré automatiquement

F : C'est l'adresse IP ou le nom d'hôte de votre pare-feu XG

G : Ceci est utile si vous avez deux connexions WAN différentes utilisées par votre pare-feu XG

H : Cela vous permet de sélectionner ce que vous souhaitez que la 2ème connexion WAN fasse.

I : Cela vous permet de mettre une brève description de cette interface RED

J : "Automatique" permet à l'appareil RED d'extraire la configuration de votre XG Firewall automatiquement sur Internet

Add RED Interface

Log ViewerHelpadminHOME TECHNOLOGY

InterfacesZonesWAN Link ManagerDNSDHCPIPv6 Router AdvertisementCellular WANIP TunnelsNeighbors (ARP-NDP)Dynamic DNS

Branch Name *

TEST

Type

RED 15

RED ID *

A3501DF3148AF4D

Tunnel ID *

1

Unlock Code *

0ak3ll30

Firewall IP/Hostname *

celpaid.myfirewall.co

2nd Firewall IP/Hostname

Use 2nd IP/Hostname for

☒ Failover☐ Load Balancing

Description

Device deployment

☒ Automatically via Provisioning Service☐ Manually via USB Stick

Save

Cancel

III.3-/ Paramètres des liaisons montantes

Ici, vous déterminez si la connexion WAN sur l'appareil RED obtiendra une adresse IP DHCP ou une adresse IP attribuée statiquement

Uplink Settings

Uplink Connection

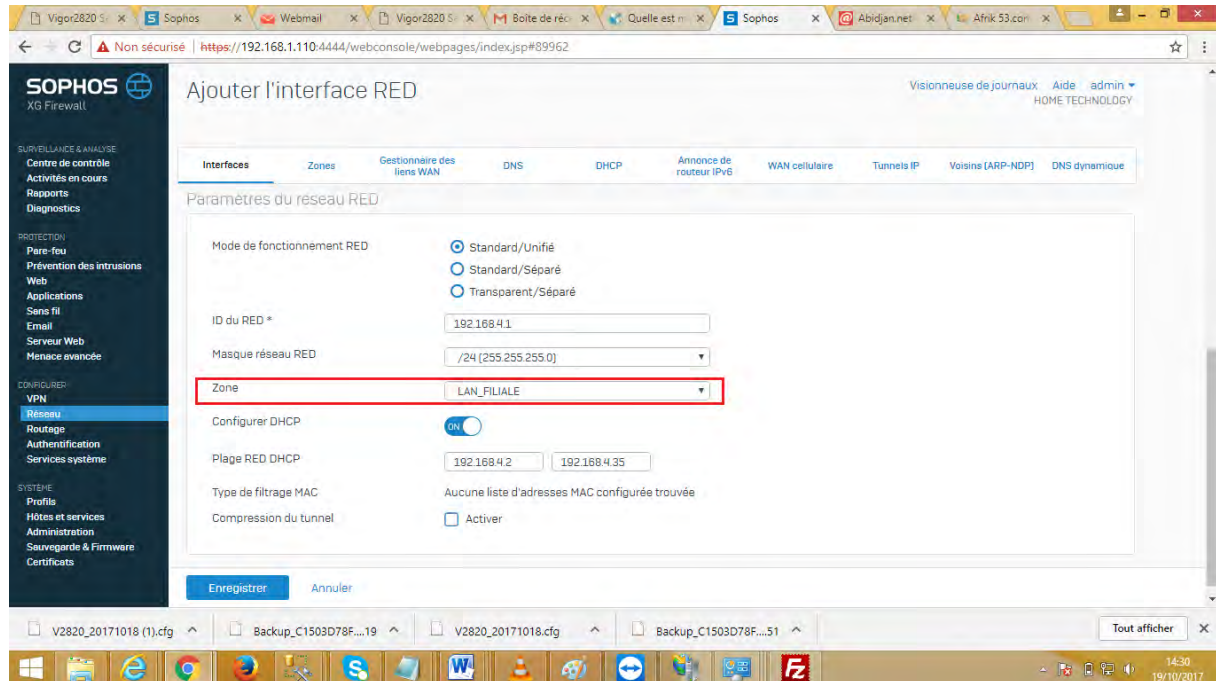
☒ DHCP☐ Static

3G/UMTS Failover

☒ Enable

III.4-/ Les paramètres du sous-réseau du RED


Ici que vous configurez le réseau LAN pour le bureau distant. Assurez-vous que le sous-réseau que vous définissez est différent du sous-réseau du bureau principal. (Ex., Si le réseau du bureau principal est 10.1.1.0/24, créez le réseau RED comme 10.1.2.0/24)



NB : Une fois que vous avez terminé la configuration de l'interface RED, vous n'avez plus rien à faire .Vous pourrez voir votre nouvel appareil RED sous (Control Center / RED) dans votre pare-feu XG.

III.5-/ Le règle pour le fonctionnement des RED

Après la configuration des RED il faut établir les règles pour son bon fonctionnement auquel cas la connexion risque de ne s'établir avec le site principal. Les trois règles ci-dessous sont importantes

	REGLE D'ACCES FILIALES [ID : 3] entrant 0 B, sortant 0 B 	LAN_FILIALE Tout hôte	LAN LOCAL	Tout service	Accepter Journal	
	LAN-LANFILIAL [ID : 6] entrant 0 B, sortant 0 B 	LAN Tout hôte	LAN_FILIALE Tout hôte	Tout service	Accepter Journal	
	TEST_INTERNET [ID : 4] entrant 0 B, sortant 0 B 	LAN_FILIALE Tout hôte	WAN Tout hôte	Tout service	Accepter Journal	

Pour créer ses réglés on procède comme suit :

- 1- Cliquez sur pare-feu puis sur Ajouter une règle de pare-feu

IPv4 IPv6 Activer le filtre

Ajouter une règle de pare-feu

Règle	Source	Destination	Laquelle ?
 BUREAU_DISTANT [ID : 7] entrant 284.66 KB, sortant 76.23 KB 	WAN 192.168.5.4	LAN 192.168.1.100	#BUREAU_DISTANT [ID : 7] 3389(TCP)
 #Default_Network_Policy [ID : 1] entrant 6.71 MB, sortant 1.61 MB 	LAN Tout hôte	WAN Tout hôte	Tout service


Règle d'utilisateur / de réseau
 Contrôlez le trafic de vos utilisateurs et réseaux.


Règle d'application métier
 Protégez et contrôlez l'accès à vos serveurs et services.

2- Et on renseigne l'écran ci-dessous

Source

Zones émettrices *

LAN_FILIALE

Ajouter un nouvel élément

Réseaux et appareils émetteurs *

Tous

Ajouter un nouvel élément

Lors d'heure planifiée

Tout le temps

Destination & services

Zone de destination *

LAN

Ajouter un nouvel élément

Réseaux de destination *

LOCAL

Ajouter un nouvel élément

Services *

Tous

Ajouter un nouvel élément

Identité

☐ Faire correspondre les utilisateurs connus

Enregistrer

Annuler

Source

Zones émettrices *

LAN_FILIALE

Ajouter un nouvel élément

Réseaux et appareils émetteurs *

Tous

Ajouter un nouvel élément

Lors d'heure planifiée

Tout le temps

Destination & services

Zone de destination *

LAN

Ajouter un nouvel élément

Réseaux de destination *

LOCAL

Ajouter un nouvel élément

Services *

Tous

Ajouter un nouvel élément

Identité

☐ Faire correspondre les utilisateurs connus

Enregistrer

Annuler

Source

Zones émettrices *
 LAN
 Ajouter un nouvel élément

Réseaux et appareils émetteurs *
 Tous
 Ajouter un nouvel élément

Lors d'heure planifiée
 Tout le temps

Destination & services

Zone de destination *
 LAN_FILIALE
 Ajouter un nouvel élément

Réseaux de destination *
 Tous
 Ajouter un nouvel élément

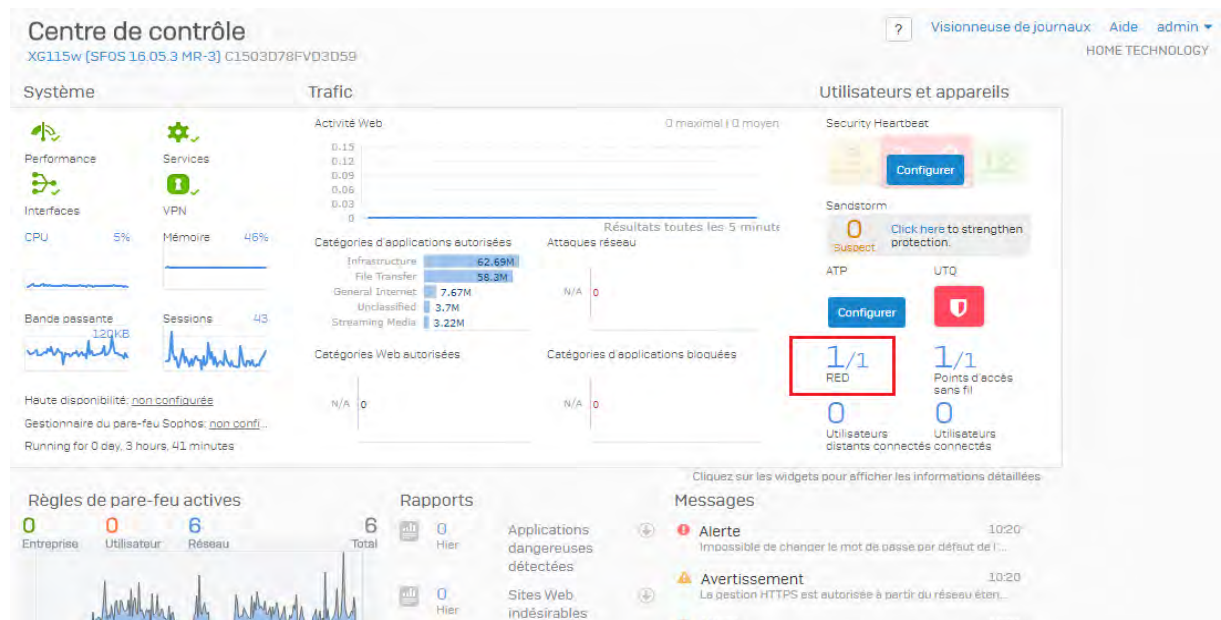
Services *
 Tous
 Ajouter un nouvel élément

Identité

☐ Faire correspondre les utilisateurs connus

Enregistrer Annuler

3- Cliquez sur Enregistrer



En cliquant sur l'élément en rouge vous avez tous les détails sur la connexion du RED

Centre de contrôle
XG115w (SFOS 16.05.3 MR-3) C1503D78FVD3D59

VISIONNEUSE DE JOURNAUX AIDE ADMIN

SYSTÈME UC ET MÉMOIRE RÉSEAU HEARTBEAT ATP RED ALERTE CONNEXIONS ET INTERFACES

RED 1/1
Configurer le RED

Afficher tout

NOM / TYPE, MODE	CONNECTÉ À PARTIR DE	VU POUR LA DERNIÈRE FOIS
reds1(TEST) RED 1.5, Standard/Unité	192.168.75.2	online

Règles de pare-feu actives

Rapports

Messages

Alerte

Avertissement

III.6-/ La connexion RED et livebox

Très souvent, lorsque le RED est connecté à un LiveBox chez le client vous pouvez constater un problème de connexion avec le sophos. Dans la console du sophos vous pouvez voir les informations indiquant que le RED est connecté mais en réalité sur le terrain le voyant tunnel a du mal à se stabiliser. Ce problème de connexion est provoqué par la configuration de base du livebox. Pour régler ce problème il faut refaire la configuration de la livebox. Cette configuration consiste à ouvrir deux ports dans le pare-feu du livebox afin d'autoriser la connexion entre RED et le sophos. Pour ouvrir les ports on procède comme suit :

- 1- Connectez-vous à l'interface de livebox
- 2- Cliquez sur l'onglet **configuration avancée**. Puis, dans le menu de gauche, sélectionnez **configuration pare-feu**.

orange Livebox Français

mon réseau mon WiFi mon téléphone assistance **configuration avancée**

configuration
réseau
configuration pare-feu
accès à distance
utilisateur
connexion à Internet
administration

[configuration avancée](#) > configuration pare-feu

pare-feu

Configuration du pare-feu (firewall).

vous pouvez configurer le niveau de protection de la Livebox. le niveau par défaut (moyen) est satisfaisant et recommandé.

choisir le niveau de sécurité

faible

- 3- Dans le menu qui s'affiche cliquez sur personnalisé

pare-feu

Configuration du pare-feu (firewall).

vous pouvez configurer le niveau de protection de la Livebox, le niveau par défaut (moyen) est satisfaisant et recommandé.

choisir le niveau de sécurité



faible

Le pare-feu ne filtre rien. Attention, ce niveau est réservé aux utilisateurs avancés pour lesquels la sécurité n'est pas une priorité. Veuillez noter aussi que même dans ce mode une connexion initiée depuis Internet sera rejetée si une règle NAT/PAT correspondante n'a pas été créée.



moyen

Le pare-feu filtre toutes les connexions entrantes, le trafic sortant est autorisé à l'exception des services netbios. Il est recommandé d'utiliser ce mode.



élevé

Le pare-feu vous permet d'utiliser les applications standards sur Internet (web, mail, news...) et rejette les connexions entrantes non désirées. Ce choix est recommandé pour disposer d'un niveau de sécurité maximal. Attention incompatible avec Unix et d'autres services.



personnaliser

Ce profil vous permet de personnaliser votre pare-feu, vous pouvez ainsi définir des règles de filtrage spécifiques. (réservé aux utilisateurs experts).

personnaliser

annuler

enregistrer

- 4- Créer une nouvelle règle en sélectionnant nouveau dans le champ application/service pour créer une règle personnalisée

règles personnalisées

adresse IP statique

application / service	protocole	adresse IP source	masque adresse IP	port source	adresse IP destination	masque adresse IP	port destination	action	
WINS	TCP							accept	enregistrer
WINS									
nouveau...									
HTTP	TCP								

Description :

- Saisissez, dans le champ **application / service**, le nom de la règle que vous êtes en train de créer (**red**).
- Saisissez **3400** pour le **port de destination**
- Cliquez sur le bouton **enregistrer** pour enregistrer votre règle personnalisée.

règles personnalisées

adresse IP statique

application / service	protocole	adresse IP source	masque adresse IP	port source	adresse IP destination	masque adresse IP	port destination	action	
red	TCP						3400	accept	enregistrer

- Vous créez aussi une règle pour le port **3410** avec le **protocole UDP** et le port **[443-8443]** **protocole TCP** avec pour nom **HTTPS**

En résumé vous avez trois nouvelles règles à créer : les règles d'ouvertures des ports 3400, 3410 et la plage [443-8443]

- Après la création des différentes règles il faudra redémarrer le livebox pour prendre en compte la nouvelle configuration

NNTPS	TCP	563	accepter	supprimer
DNS	les deux	53	accepter	supprimer
IMAP	TCP	143	accepter	supprimer
IRC	TCP	6665-6667	rejeter	supprimer
IMAPS	TCP	993	accepter	supprimer
ISAKMP	UDP	500	accepter	supprimer
STUN	UDP	3478	accepter	supprimer
IPSEC-NAT-T	UDP	4500	accepter	supprimer
ICMP	les deux		accepter	supprimer
red	TCP	3400	accepter	supprimer
sos	UDP	3410	accepter	supprimer
HTTPS	TCP	443-8443	accepter	supprimer

IV- / Redirection de port

Ce chapitre explique les étapes pour configurer SOPHOS pour fournir l'accès des ressources internes à l'aide de l'hôte virtuel.

La mise en œuvre de l'hôte virtuel est basée sur la destination NAT concept des versions plus anciennes de SOPHOS.

L'hôte virtuel permet de bénéficier des services **d'une machine hôte d'un réseau privé a partir de l'adresse IP publique. En d'autres termes, c'est un mappage d'adresse IP** publique à une adresse IP interne. Cet hôte virtuel est utilisé comme adresse de destination pour accéder au serveur interne ou DMZ.

Un hôte virtuel peut être une seule adresse IP ou une plage d'adresses IP ou de l'interface SOPHOS lui-même. SOPHOS répond automatiquement à la demande ARP reçue sur la zone WAN pour l'adresse IP externe de l'hôte virtuel.

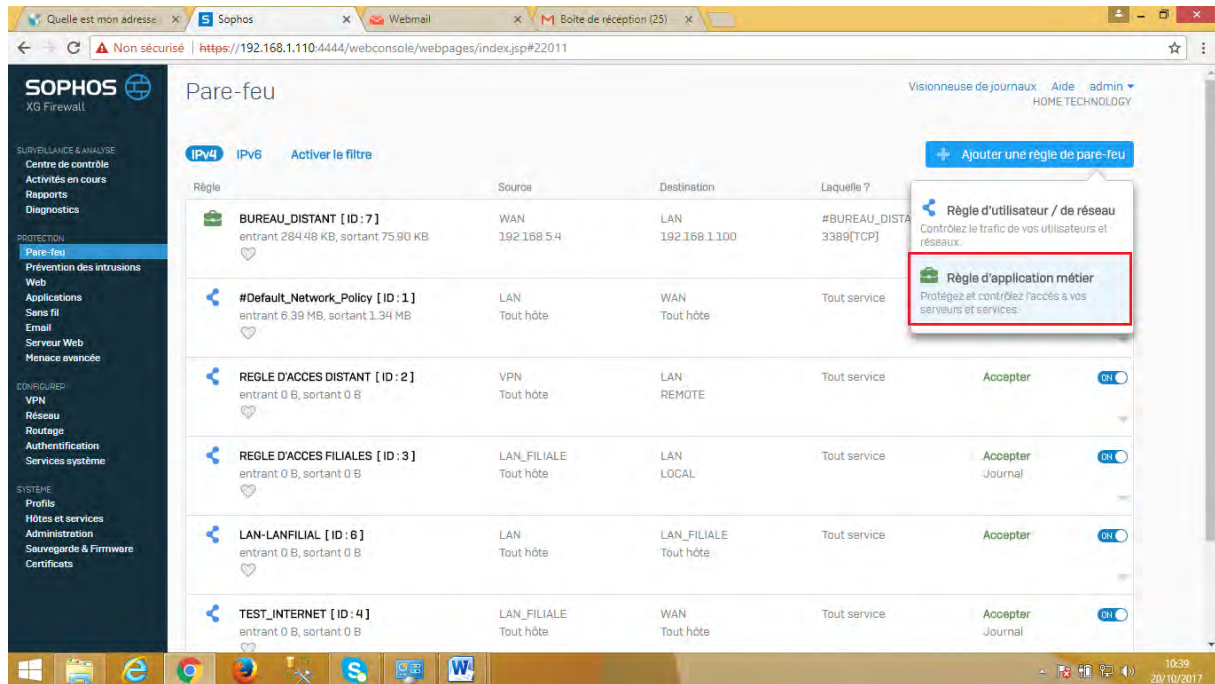
Le SOPHOS fait donc la redirection pour les hôtes virtuels. On peut aussi configurer une liste Port de l'hôte virtuel. Dans ce cas les ports dans la liste sont séparés par des virgules. En outre, une plage de ports peut désormais être mappée sur un seul port. Cela crée une application à une ou plusieurs mappages entre le port externe et le port mappé.

Remarque :

- Pour un seul hôte virtuel, un maximum de 16 ports peut être configuré dans une liste de Port.
- Tous les ports d'une liste doivent utiliser un seul protocole (TCP ou UDP) et non les deux à la fois

IV.1- / Le choix du paramètre

- 1- Les règles de redirection sont configurées depuis le pare-feu en faisant le choix de la deuxième option comme indiqué ci-dessous



- 2- Et on choisit l'option en rouge



IV.2- / La configuration de la redirection

Etape 1 : La source

Il s'agit ici d'indiquer la zone qui initie l'action tout en précisant les réseaux client autorisé et les réseaux clients a bloquer

Nom de la règle *	Description
BUREAU_DISTANT	Description

Source

Zones émettrices *	Réseaux client autorisés *	Bloqués les réseaux client
WAN	Tous	
Ajouter un nouvel élément	Ajouter un nouvel élément	Ajouter un nouvel élément

Etape 2 : Destination

Il s'agit ici d'indiquer la zone de destination, la zone vers laquelle l'action est orientée. Ensuite il faut préciser le type de redirection et les ports concernés.

Destination & Service

Hôte/Réseau de destination *	Type de redirection	Ports de service redirigés *
#Port2-192.168.5.4	Port	3389 Pour
Protocole		
<input checked="" type="radio"/> TCP <input type="radio"/> UDP		

Etape 3 : Redirection

Il s'agit ici d'indiquer le serveur vers lequel la redirection se fera tout en précisant la zone dans laquelle ce serveur est situé

Redirection

Serveur(s) protégé(s) *	Type de port mappé	Port mappé *
SERVEUR_SQL.1	Port	3389 Pour
Zone protégée *	<input type="checkbox"/> Changer le ou les Ports de destination	
LAN		

Etape 4 : Avancés

Cette partie **comme son nom l'indique permet** les configurations avance selon le besoin et la politique de sécurité mise en place

Avancés

<p>Stratégies pour les applications métiers</p> <p>Prévention des intrusions </p> <p>Aucune</p> <p>Régulation de flux</p> <p>Aucune</p>	<p>Protection synchronisée </p> <p>Source HD minimale autorisée :</p> <p><input checked="" type="radio"/> GREEN <input type="radio"/> YELLOW <input checked="" type="radio"/> No Restriction</p> <p><input type="checkbox"/> Bloquer les clients sans Heartbeat</p> <p>Destination HD minimale autorisée :</p> <p><input checked="" type="radio"/> GREEN <input type="radio"/> YELLOW <input checked="" type="radio"/> No Restriction</p> <p><input type="checkbox"/> Bloquer la requête de destination sans Heartbeat</p>	<p>Routage</p> <p><input type="checkbox"/> Réécrire l'adresse source (dégüisement)</p> <p><input type="checkbox"/> Créer une règle réflexive</p>
---	--	--

Enregistrement du trafic

☐ Enregistrer le trafic du pare-feu

Enregistrer Annuler

V- / Migration Cyberoam en sophos

V.1-/ Les Appliance prise en charge

Les Appliance Cyberoam (CR) suivantes peuvent être mises à niveau vers le microprogramme Sophos Firewall (SF):

- Appareils virtuels: tous les appareils virtuels
- Série iNG: CR25iNG et ci-dessus.
 - Appareils qui NE PEUVENT PAS être mis à niveau: CR10iNG, CR10wiNG, CR15iNG / 4P, CR15wiNG, CR25wiNG / 6P et CR35wiNG
- Série Cyberoam i: CR200i et CR300i.
 - Appareils qui NE PEUVENT PAS être mis à niveau: CR15i, CR15wi, CR25wi et CR35wi.
- Série Cyberoam ia: CR500ia et ci-dessus.
 - Appareils qui NE PEUVENT PAS être mis à niveau: CR25ia à CR100ia.

Cyberoam doit avoir la version du micrologiciel 10.6.2 MR2 et suivantes pour mettre à jour le micrologiciel SF.

- Pour les Appliance exécutant 10.6.2 MR1 et les versions ultérieures, la mise à niveau vers le microprogramme SF est un processus en deux étapes dans lequel elles sont mises à niveau vers la version 10.6.2 MR2, puis vers le microprogramme SF.
- Pour les Appliance exécutant 10.6.3, la mise à niveau vers le microprogramme SF est un processus en deux étapes dans lequel elles sont d'abord mises à niveau vers la version 10.6.3 MR1, puis vers le microprogramme SF.

Remarque:

- Pour mettre à niveau, l'**Appliance** CR doit être enregistrée sur le portail client Cyberoam.
- La mise à niveau n'est pas disponible sur le Virtual Trial Appliance (CRiV-TR).
- Seules certaines révisions matérielles de 15iNG peuvent migrer vers SFOS.

V.2-/ Les points à prendre en compte avant la migration

1. Si votre Appliance CR est migrée vers le microprogramme SF-OS sur une licence d'essai Full Guard, le redémarrage en continu vers Cyberoam OS est possible en redémarrant l'Appliance avec le microprogramme CR. Toutefois, la restauration ne sera pas possible après la migration de vos licences CR existantes vers des licences SF-OS.
 2. Les Appliance mises à niveau vers le firmware SF ne peuvent plus être gérées par CCC. Vous aurez besoin de Sophos Firewall Manager (SFM) pour gérer les Appliance mises à niveau.
 3. Les Appliance mises à niveau vers le firmware SF ne peuvent plus être intégrées à Cyberoam iView. Vous aurez besoin de Sophos iView (version 2) pour signaler les Appliance migrées.
 4. Une fois que votre Appliance a été mise à niveau vers le micrologiciel SF, la Garantie sera valable jusqu'à 5 ans à compter de la date d'enregistrement initiale de l'Appliance, à condition que vous ayez une licence d'assistance active.
 5. Une fois migré, votre Appliance ne sera PAS applicable pour les systèmes Cyberoam Trade-Up. Toutefois, vous pouvez opter pour les programmes Sophos Firewall Hardware Refresh lors de son lancement.
- Reportez-vous également à la rubrique Problèmes connus - Cyberoam to Sophos Firewall Migration.

V.3-/ Les nouveautés apporté dans sophos

Sophos est la version améliorée de Cyberoam **avec l'ajout de ces détails ci-dessous** dans sa configuration

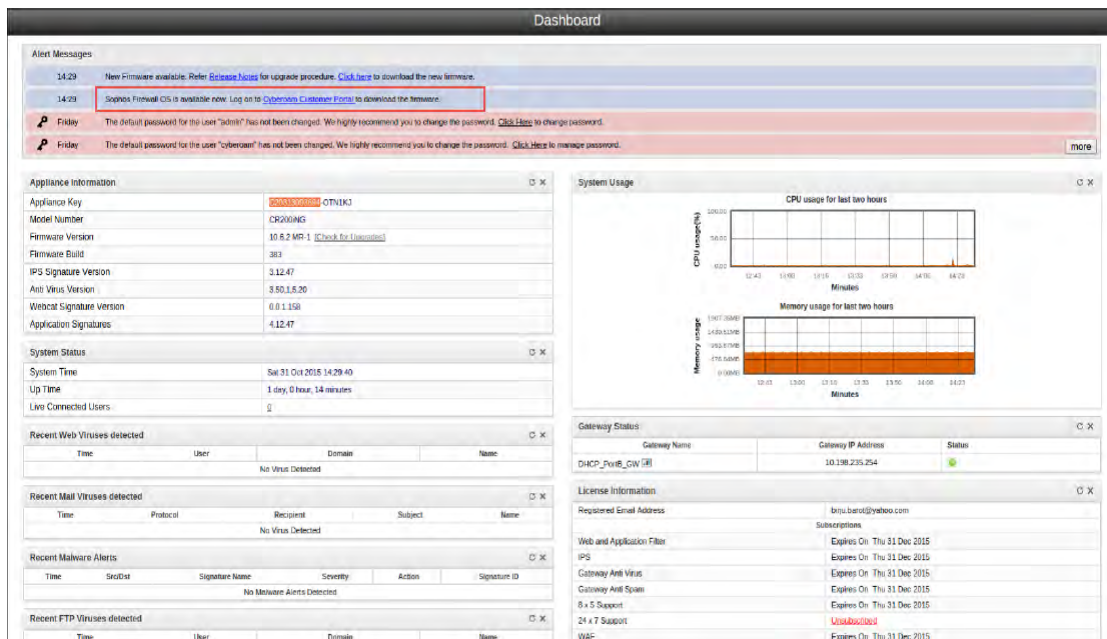
1. Configuration de stratégie simplifiée avec 2 types de règles - Règle d'application métier, Règle utilisateur / réseau.
2. Nouveau centre de contrôle pour un aperçu et un contrôle instantané.
3. ATP pour protéger votre réseau contre les menaces avancées.
4. Security Heartbeat connecte le pare-feu et les points de terminaison pour une sécurité plus intelligente.
5. RED étend la sécurité du bureau principal aux bureaux distants sans aucune configuration.
6. Une protection renforcée des e-mails avec cryptage SPX et DLP intégré.

V.4-/ Les étapes de la migration

La migration de l'**Appliance** Cyberoam vers Sophos Firewall se fait en suivant les étapes ci-dessous.

Étape 1

Une fois le micrologiciel SF disponible, une alerte s'affiche sur votre tableau de bord. Cliquer sur le lien.



Étape 2

En cliquant sur le lien, vous serez redirigé vers le portail client de Cyberoam. Connectez-vous au portail.

CUSTOMER LOGIN

Email

 (case-sensitive)

Password

 (case-sensitive)

[Forgot your Email ID / Password?](#) [Sign In](#) [Register your Appliance](#)

SOPHOS Cyberoam

Cyberoam continuously enhances and updates its features to offer latest security to its customers against evolving threats. Customers are therefore advised to use the latest firmware to stay updated.

Étape 3

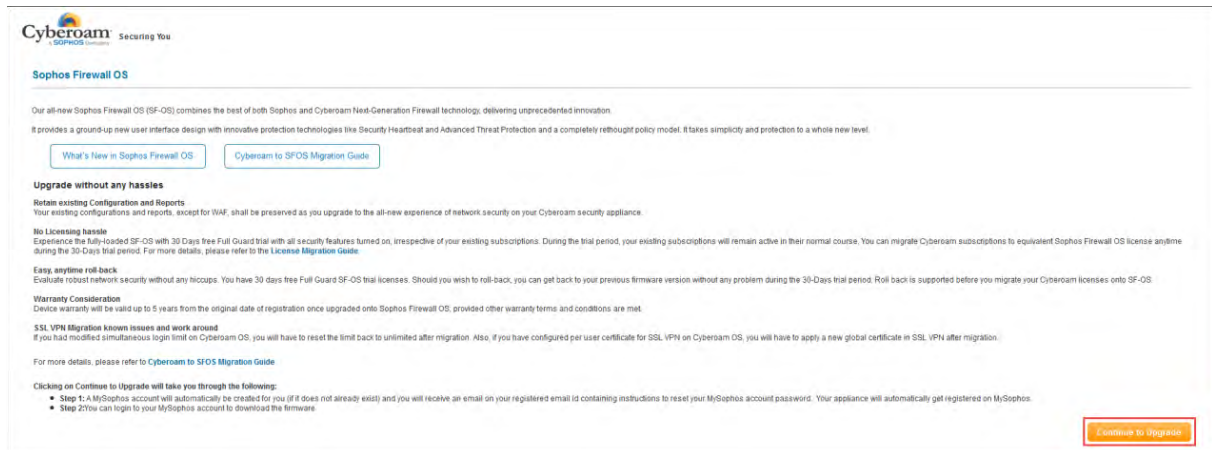
Cliquez sur Mettre à niveau par rapport au matériel ou à l'**Appliance** virtuelle que vous souhaitez mettre à niveau.

Remarque :

Les Appliance mises à niveau vers le microprogramme Sophos Firewall ne peuvent plus être gérées par CCC. Vous aurez besoin de Sophos Firewall Manager (SFM) pour gérer les Appliance mises à niveau.

Étape 5


Lisez les instructions complètes et cliquez sur Continuer pour mettre à niveau.



Étape 6

En cliquant sur Continuer pour mettre à jour :

1. Un compte Sophos ID et My Sophos sera automatiquement créé pour vous (s'il n'existe pas déjà) et vous recevrez un e-mail sur votre adresse e-mail enregistrée contenant des instructions pour réinitialiser votre mot de passe de compte Sophos. Votre appareil sera automatiquement enregistré sur My Sophos.
2. Vous pouvez vous connecter à votre compte My Sophos pour télécharger le firmware.



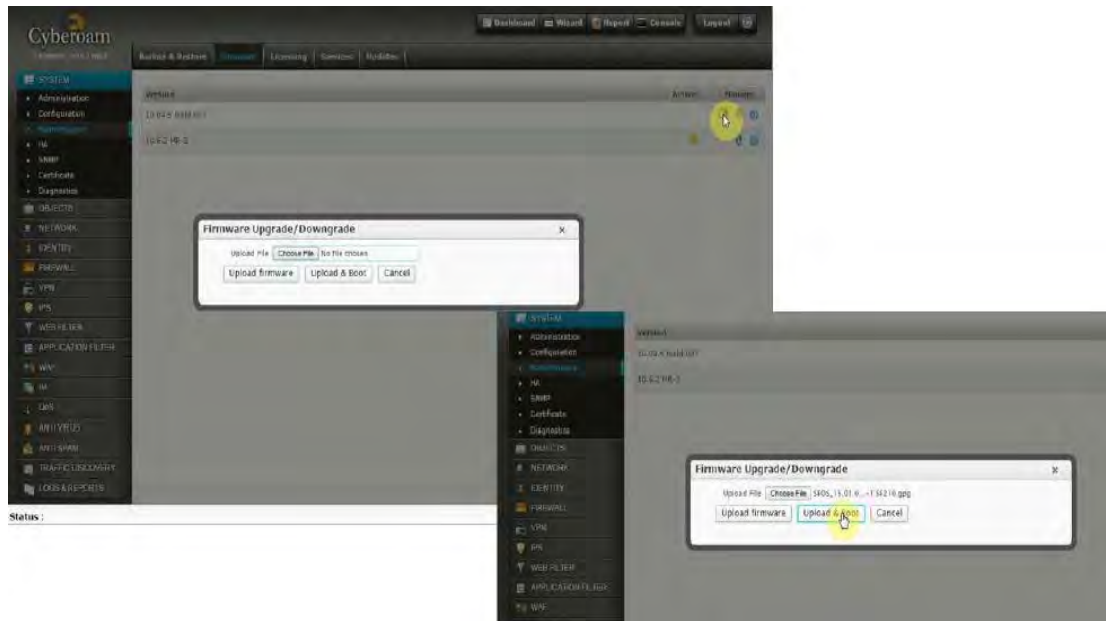
Étape 7

Une fois le firmware téléchargé, suivez les instructions ci-dessous :

- Connectez-vous à Cyberoam Web Admin Console et allez dans Système> Maintenance> Firmware.
- Cliquez sur l'icône Télécharger et téléchargez le fichier .gpg téléchargé, c'est-à-dire le micrologiciel

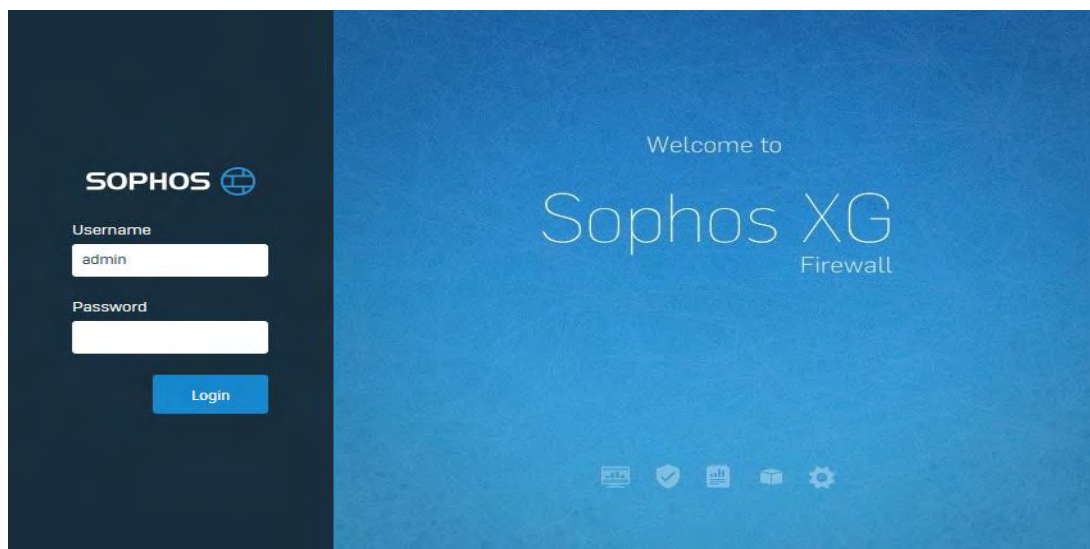
téléchargé.

- Cliquez sur Télécharger et démarrer.



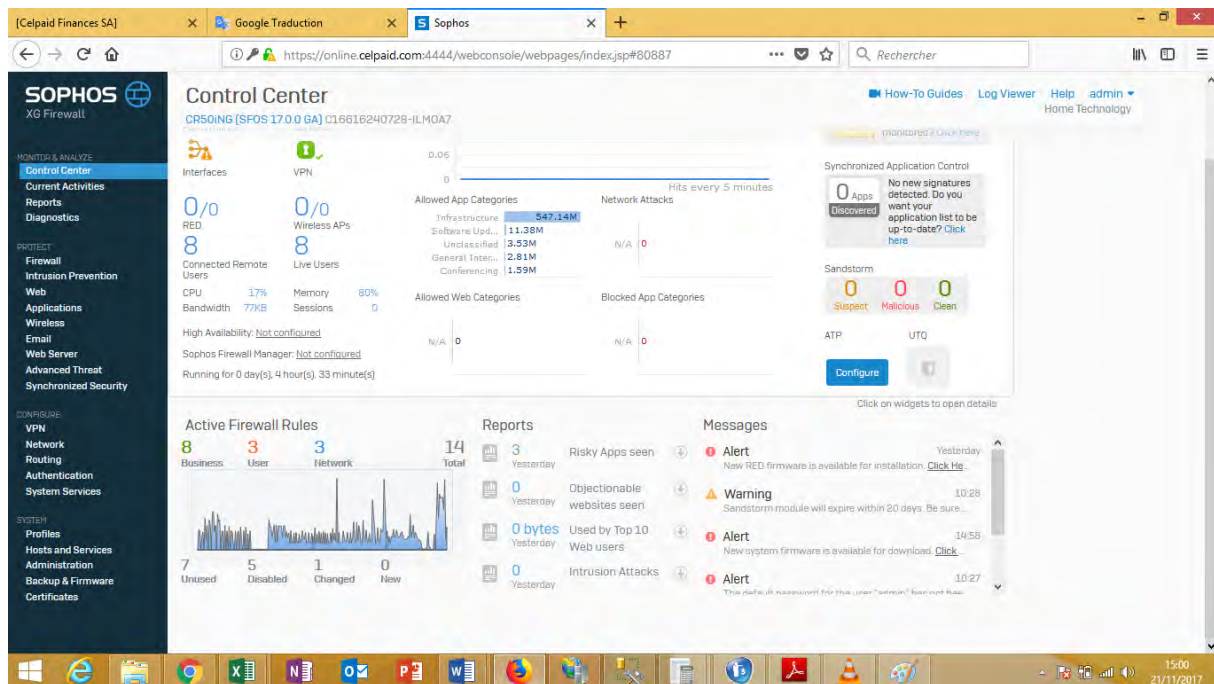
Étape 8

Une fois l'appareil démarré, connectez-vous en utilisant vos informations d'identification d'administrateur.



V.5/- Le connecter a sophos

Après la mise à niveau, le numéro de modèle et la clé de série de votre Appliance matérielle CR resteront les mêmes. Les appareils virtuels seront renommés en leurs modèles SF correspondants.



V.6 -/ Navigation dans sophos

La barre de navigation de la console d'administration comprend des menus, des sous-menus et des onglets. Le menu contient les modules suivants :

Centre de contrôle de la sécurité réseau : il sert de tableau de bord pour fournir des informations générales sur l'état du système, les informations sur le trafic, les informations relatives à l'utilisateur et aux périphériques connectés, l'utilisation et le statut des stratégies de sécurité actives.

Rapports : Les rapports fournissent aux organisations une visibilité sur leurs réseaux tout en répondant aux exigences de conformité réglementaire. Cela permet aux organisations non seulement d'afficher des informations sur des centaines d'utilisateurs, d'applications et de protocoles ; cela les aide également à corréler les informations, en leur donnant une vision globale de l'activité du réseau.

Stratégies : les stratégies sont des ensembles de règles de sécurité permettant de contrôler les utilisateurs, les applications ou les objets réseau d'une organisation. À l'aide de stratégies, vous pouvez créer des règles générales ou particulières de transit du trafic en fonction des besoins. Les stratégies fournissent une gestion centralisée pour l'ensemble des stratégies de sécurité des périphériques.

Protection : le menu Protection regroupe tous les onglets associés dans les sous-menus Sans fil, Web, Application, Serveur Web et Protection de la messagerie.

System : Le menu System contient des sous-menus qui permettent l'administration globale du périphérique SF, comme le réseau, le VPN, les diagnostics, l'activité en cours, etc.

Objets : les objets sont les blocs de construction logiques de diverses règles et règles. Ce menu facilite la création de différents hôtes, des règles telles que la gestion du trafic et le temps d'accès, les utilisateurs, les groupes, les ressources telles que les points d'accès et les serveurs Web.

V.7-/ Migration de la licence

Vous pouvez migrer les licences de Cyberoam OS vers Sophos Firewall OS (SFOS) depuis :

- Portail Clients

- Système> Maintenance> Licence

Pour plus de détails sur la migration des licences, reportez-vous au Guide de migration de licences.

V.8- / Transformation des règles aux stratégies de sécurité

Les règles de pare-feu de Cyberoam seront connues sous le nom de politiques de sécurité dans SF. En effet, ces règles ne vont plus uniquement exécuter des fonctions de pare-feu, mais intégrer toutes les stratégies requises pour les implémenter sur différents types de trafic. En d'autres termes, chaque **politique de sécurité mettra en œuvre une politique d'organisation / institution définie**.

Vos règles de pare-feu seront migrées vers SF conformément aux instructions suivantes :

1. Les règles liées au WAF ne seront PAS migrées.

2. Pour les règles liées à la zone LOCAL :

a- Si l'action dans la règle source est marquée "Rejeter" ou "Abandonner", l'action dans la règle migrée sera "Abandonner".

b- Le paramètre Log Firewall Traffic sera désactivé pour toutes les règles migrées.

c- L'identité sera désactivée pour toutes les règles migrées.

d- L'hôte de destination sera toujours "Tous" dans la règle migrée. Les règles avec un hôte de destination spécifique ne seront pas migrées.

e- Toutes les règles spécifiques au service seront migrées telles quelles. Toutefois, si le service spécifié dans la règle Cyberoam n'est pas présent dans SF, la règle ne sera pas migrée.

3- Pour les règles non basées sur l'identité :

a. Les règles dont l'identité est désactivée seront migrées vers SF en tant que stratégies de réseau.

b. Les règles pour lesquelles l'analyse par courrier électronique est activée seront migrées vers SF en tant que stratégies d'application métier. Les règles avec l'analyse SMTP et / ou SMTPS activée seront migrées en tant que stratégie avec le modèle Email Server, tandis que les règles avec POP, POPS et / ou IMAP seront migrées en tant que stratégie avec le modèle Email Client.

c. Pour les règles avec analyse du courrier électronique et l'analyse HTTP / HTTPS / FTP activée, deux (2) stratégies de sécurité seront créées : Un (1) modèle de stratégie d'application commerciale avec un client email ou un serveur de courrier électronique (le cas échéant) et une (1) Filtre Web correspondant, filtre d'application et configuration d'analyse HTTP / HTTPS / FTP (le cas échéant).

d. Les règles dont l'hôte de destination est "Any" seront migrées vers SF en tant que stratégies d'application métier avec un modèle non HTTP. Les règles avec l'analyse SMTP et / ou SMTPS activée seront migrées en tant que stratégie avec le modèle Email Server, tandis que les règles avec POP, POPS et / ou IMAP seront migrées en tant que stratégie avec le modèle Email Client. Le filtre Web, le filtre d'application, la gestion de liens multiples (MLM) et la configuration d'analyse HTTP / HTTPS / FTP (le cas échéant) correspondants seront reportés dans une stratégie réseau distincte.

4. Pour les règles basées sur l'hôte virtuel :

a. Les règles avec Action comme 'Drop' ou 'Reject' seront migrées en tant que règles utilisateur / réseau respectives contenant des informations externes de la règle source.

- b. Les règles avec Action comme 'Accept' seront migrées vers SF en tant que stratégies d'application métier avec un modèle non HTTP. Le filtre Web correspondant, le filtre d'application, la gestion MLM (Multi-Link Management) et la configuration d'analyse HTTP / HTTPS / FTP / IMAP / POP (le cas échéant) ne seront PAS transférés.
- c. Les règles de bouclage seront migrées vers SF en tant que stratégies d'application métier avec un modèle non HTTP. Le filtre Web correspondant, le filtre d'application, la gestion MLM (Multi-Link Management) et la configuration d'analyse HTTP / HTTPS / FTP / IMAP / POP (le cas échéant) ne seront PAS transférés.
- d. Les règles réflexives seront migrées telles quelles dans les règles utilisateur / réseau. Les règles avec l'analyse SMTP et / ou SMTPS activée seront migrées en tant que stratégie avec le modèle Email Server, tandis que les règles avec POP, POPS et / ou IMAP seront migrées en tant que stratégie avec le modèle Email Client.

5. Pour les règles basées sur **l'identité** :

- a. Les règles dans lesquelles les stratégies de filtre Web et de filtre d'application sont définies sont migrées telles quelles dans les stratégies utilisateur. Si la zone de destination de la règle est une zone autre que WAN, les valeurs Web et Filtre d'application ne sont pas reportées sur la règle migrée.
- b. Les règles dans lesquelles des utilisateurs spécifiques sont spécifiés sont migrées en tant que stratégies utilisateur. Les stratégies de filtre d'application et de Web spécifiques à l'utilisateur sont reportées en tant que configuration correspondante dans la règle. Toutefois, si la règle CR elle-même a des paramètres Web et filtre d'application définis, la règle est migrée en l'état.
- c. Les stratégies de filtre d'application et de Web spécifiques au groupe sont reportées en tant que configuration correspondante dans la règle. Toutefois, si la règle CR elle-même a des paramètres Web et filtre d'application définis, la règle est migrée en l'état.
- d. Les règles dans lesquelles des groupes spécifiques ou "Any" sont spécifiés sont migrées en tant que stratégies utilisateur.
- e. Si les stratégies spécifiques à l'utilisateur sont différentes de celles du groupe, une stratégie utilisateur distincte est créée pour les stratégies spécifiques à l'utilisateur, conformément à la méthode décrite au point 5 b.
- F. Si l'analyse du courrier électronique est activée dans la règle CR, une règle d'application métier correspondante avec le modèle Email Client est également créée avec cette règle

Différence de comportement

Une fois la migration effectuée, différence de comportement entre les règles de pare-feu Cyberoam et les stratégies de sécurité SF :

- L'administrateur ne sera pas en mesure de configurer l'analyse des courriers électroniques, le WAF et l'hôte virtuel sur les règles réseau / utilisateur.
- Les stratégies de filtre Web et d'application ne sont plus associées à des utilisateurs ou groupes individuels. Ils devront être appliqués en utilisant les politiques de sécurité.
- L'analyse AV / AS, la politique de filtre Web / d'application et MLM ne sont pas disponibles dans les stratégies d'application métier non HTTP (hôte virtuel).
- Les stratégies de filtre Web / Application ne sont pas disponibles dans les modèles Email Client et

Email Server.

- La gestion multi-lien n'est pas disponible sur le modèle de serveur de messagerie.
- L'hôte de destination "Tout" ne couvrira pas tous les hôtes virtuels.

V.9-/ Changement dans les caractéristiques

V.9.1-/ Caractéristiques sous licence

Pour les fonctionnalités liées au Web, au courrier électronique et à la protection réseau, si la licence correspondante n'est pas abonnée, SF vous permettra de configurer la fonctionnalité, mais ne procédera pas à l'analyse et à la journalisation correspondantes. Par exemple, si votre module Protection réseau n'est pas abonné, SF vous permettra de créer des signatures IPS personnalisées, des stratégies, etc., mais ne scannerera pas et ne consignera pas le trafic.

De même, si une licence expire, SF arrêtera l'analyse et la consignment du trafic lié à ce module sans perturber le trafic réseau.

Toutefois, pour des raisons de sécurité, ce comportement n'est pas vrai pour Web Server Protection Module. Vous avez besoin d'une licence valide du module pour SF pour autoriser le trafic de votre (vos) serveur (s) Web

V.9.2-/ Pare-feu d'application Web (WAF)

La configuration WAF de l'appliance Cyberoam ne sera pas migrée vers le microprogramme SF. Vous devrez reconfigurer les stratégies liées à WAF dans le microprogramme SF.

V.9.3-/ Client d'authentification générale

Les utilisateurs ne pourront PAS se connecter à SFOS à l'aide du GAC (Cyberoam General Authentication Client). Ils devront télécharger et installer de nouvelles instances appelées agents d'authentification client à partir du portail utilisateur

V.9.4-/ VPN SSL

Les changements de comportement sont :

- **Les utilisateurs de VPN SSL ne pourront PAS se connecter à SFOS en utilisant Cyberoam SSL VPN Client.** Ils devront installer de nouvelles instances de Client VPN SSL pour SF qui peuvent être obtenues à partir du Portail Utilisateur.
- **Le portail VPN SSL (accessible en accédant à https : // <Adresse IP du réseau WAN Cyberoam>: 8443)** fera partie du portail utilisateur SF. Après la migration, vous pouvez accéder au portail utilisateur en accédant à https : // <Adresse IP du réseau local Cyberoam>: 8443.
- **Si vous avez configuré votre accès au portail VPN SSL via un port personnalisé, après la migration, le portail utilisateur SF doit être accessible via ce port personnalisé.** Par exemple, si vous avez configuré le port SSL VPN Portal sur 8080, vous devrez accéder au portail utilisateur SF après la migration en accédant à https : // <adresse IP SF>: 8080.
- **Les marque-pages SSL VPN de type IBM Server Terminal** seront convertis en type TELNET Bookmark après la migration.
- **Si vous avez personnalisé les utilisateurs VPN SSL de connexion simultanée, après la migration, réinitialisez la limite sur illimité** pour empêcher l'affichage de l'erreur "Limite de connexion maximale" pour les utilisateurs.
- **Si vous avez configuré un certificat d'utilisateur pour VPN SSL, après la migration, vous devrez supprimer les certificats d'utilisateur de votre appliance.** Ensuite, le ou les utilisateurs doivent télécharger et importer un nouveau groupe de clients VPN SSL pour SF à partir du portail utilisateur.

Les commandes SSL VPN suivantes sont interrompues:

```
Console> set ssl vpn proxy-sslv3
```

```
Console> set ssl vpn web-access
```

```
Console> show ssl vpn log
```

Cyberoam to Sophos Firewall Guide de migration

Novembre 2015 Page 13 sur 15

```
Console> show ssl vpn proxy-sslv3
```

```
Console> show ssl vpn web-access
```


V.9.5-/ Filtrage Web et d'application

La base de données de catégorisation Web dans SF contiendra un ensemble de catégories différent de celui de Cyberoam.

Si Web Protection License n'est pas abonné, vous serez autorisé à configurer les paramètres Web et d'application, mais le trafic ne sera pas analysé ni enregistré.

De plus, par rapport à Cyberoam, SF ne supporte pas :

- Proxy amont sélectif (commande CLI : console> set service-param HTTPS ssl_upstream_tunnel)
- Domaines hébergés par Google (commande CLI: console> set service-param HTTPS hébergé sur google)
- ICAP (commande CLI : console> set icap édit)
- Paramètres proxy Proxy (commande CLI : définir http_proxy dos)

V.9.6-/ Identité

Pour l'intégration avec un serveur Active Directory (AD), le type d'intégration 'Loose Intégrations' a été interrompu. Par défaut, SF Device s'intègre à un serveur AD avec une intégration étroite. Si vous avez configuré votre serveur AD avec Loose Integration, lors de la migration, il sera converti en Tight

V.9.7-/ Haute disponibilité (HA)

La spécification d'une phrase secrète sera obligatoire pour la configuration HA dans SF. Les configurations de haute disponibilité de Cyberoam seront migrées vers SF avec une phrase de passe aléatoire unique. Vous pouvez vérifier et mettre à jour la configuration HA à partir de System> System Services> HA dans le micrologiciel SF

V.9.8-/ Certificats

Les certificats Cyberoam seront transférés dans le micrologiciel SF avec les modifications suivantes:

- L'AC par défaut sera inchangée.
- L'AC Cyberoam auto-signée sera renommée Security Appliance Self Signed CA, le contenu restera le même.
- Cyberoam_SSL_CA sera renommé Security Appliance_SSL_CA et sera régénéré avec les valeurs par défaut
- Le certificat d'appareil restera le même et restera signé par Security Appliance Self Signed CA.
- Le comportement de SSLVPN par certificat d'utilisateur restera le même que dans Cyberoam.

V.9.9-/ DHCP / PPPoE

Dans le firmware SF, DHCP et PPPoE peuvent être configurés sur les interfaces de toutes les zones sauf VPN. Dans Cyberoam, il n'était disponible que dans la zone WAN

V.9.10-/ SNMP

Vous n'avez plus besoin de créer une règle de pare-feu (Stratégie de sécurité dans SF) pour autoriser le trafic SNMP lors de la configuration de SNMP. La règle de pare-feu connexe créée dans Cyberoam NE sera PAS migrée en l'état

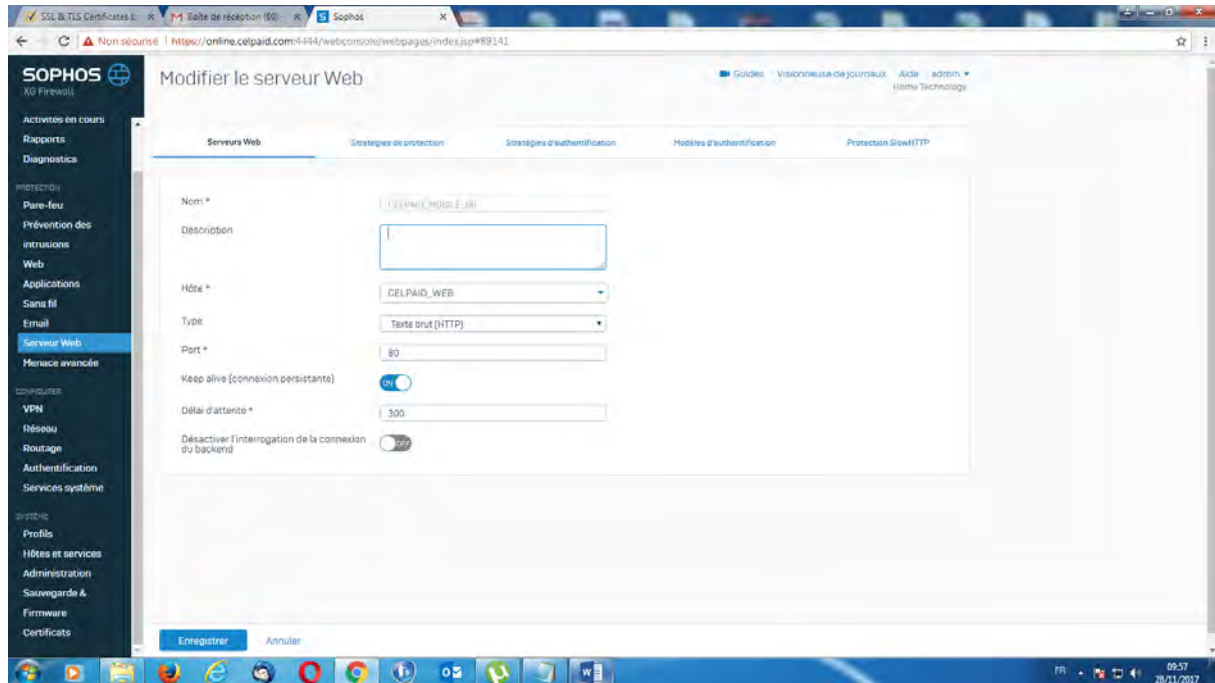
V.10-/ Arrêter les fonctions de CR

1. Prise en charge des domaines hébergés par Google
2. ICAP
3. Paramètres DOS du proxy
4. Support de la base de données d'URL externe
5. Prise en charge de la numérisation AV sans WAF
6. Possibilité de créer toutes les règles basées sur le service pour la règle ACL (locale)
7. Possibilité de créer un HTTP basé sur VH avec WAF et sans WAF
8. Support de la numérisation FTP pour VH
9. Émulation Javascript pour les URL / cookies
10. Auto-apprentissage pour ajouter des exceptions
11. Support de messagerie instantanée (IM)
12. Support VPN basé sur la route (disponible en 10.6.3)
13. Support de groupe imbriqué dans NTLM (disponible en 10.6.3)
14. Remplacement des restrictions de stratégie de filtre Web organisationnel (disponible en 10.6.3)
1. Prise en charge des domaines hébergés par Google
2. ICAP
3. Paramètres DOS du proxy
4. Support de la base de données d'URL externe
5. Prise en charge de la numérisation AV sans WAF
6. Possibilité de créer toutes les règles basées sur le service pour la règle ACL (locale)
7. Possibilité de créer un HTTP basé sur VH avec WAF et sans WAF
8. Support de la numérisation FTP pour VH
9. Émulation Javascript pour les URL / cookies
10. Auto-apprentissage pour ajouter des exceptions
11. Support de messagerie instantanée (IM)
12. Support VPN basé sur la route (disponible en 10.6.3)
13. Support de groupe imbriqué dans NTLM (disponible en 10.6.3)
14. Remplacement des restrictions de stratégie de filtre Web organisationnel (disponible en 10.6.3)

VI-/ La configuration du waf et les règles qui l'accompagnent

VI.1-/ Configuration du waf

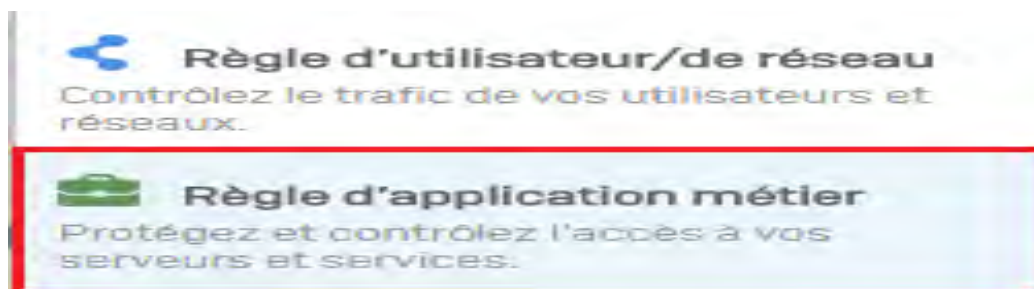
Contrairement au Cyberoam, la configuration d'un waf dans le Sophos se fait simplement en renseignant cet écran dans le menu serveur web



Hôte : représente ici le serveur sur lequel le site web est hébergé

VI.2-/ Règle du waf

La configuration du waf doit obligatoirement se terminer par une règle sans laquelle le site web n'apparaîtra pas dans un navigateur. La configuration de cette règle se fait avec la deuxième option



SOPHOS

XG Firewall

SURVEILLANCE & ANALYSE

Centre de contrôle

Activités en cours

Rapports

Diagnostics

PROTECTION

Pare-feu

Prévention des intrusions

Web

Applications

Sans fil

Email

Serveur Web

Menace avancée

CONFIGURER

VPN

Réseau

Routeur

Authentification

Services système

SYSTÈME

Profil

Hôtes et services

Administration

Sauvegarde & Firmware

Certificats

Guides

Visionneuse de journaux

Aide

admin

Home Technology

Modifier Règle d'application métier

Nom de la règle *

WAN TO WEB

Description

Description

1

2

3

4

Serveur hébergé

Adresse hébergée *

#PortB

☒ HTTPS

☒ Redirection HTTP

Port d'écoute *

443

Certificat HTTPS *

CELPaid_online

Domaines *

online.celpaid.com

Rechercher / Ajouter

SOPHOS

XG Firewall

SURVEILLANCE & ANALYSE

Centre de contrôle

Activités en cours

Rapports

Diagnostics

PROTECTION

Pare-feu

Prévention des intrusions

Web

Applications

Sans fil

Email

Serveur Web

Menace avancée

CONFIGURER

VPN

Réseau

Routeur

Authentification

Services système

SYSTÈME

Profil

Hôtes et services

Administration

Sauvegarde & Firmware

Certificats

Guides

Visionneuse de journaux

Aide

admin

Home Technology

Modifier Règle d'application métier

Serveur(s) protégé(s)

☐ Routage selon le chemin

4

5

Serveur Web *

Liste des serveurs Web

saisir un texte pour la recherche

Créer

☐ CELPAID_MOBILE_8080

☐ CELPAID_MOBILE_88

☒ CELPAID_MOBILE_80

Serveur(s) Web sélectionné(s)

CELPaid_MOBILE_80

faire glisser pour modifier la priorité

Autorisation d'accès

Autorisés les réseaux client

Any IPv4

Ajouter un nouvel élément

Bloqués les réseaux client

Ajouter un nouvel élément

Authentification

Aucune

SOPHOS

XG Firewall

SURVEILLANCE & ANALYSE

Centre de contrôle

Activités en cours

Rapports

Diagnostics

PROTECTION

Pare-feu

Prévention des intrusions

Web

Applications

Sans fil

Email

Serveur Web

Menace avancée

CONFIGURER

VPN

Réseau

Routeur

Authentification

Services système

SYSTÈME

Profil

Hôtes et services

Administration

Sauvegarde & Firmware

Certificats

Guides

Visionneuse de journaux

Aide

admin

Home Technology

Modifier Règle d'application métier

Exceptions

Chemins

Sources

Vérification

Catégories

État

Modifier/Supprimer

Données introuvables

Ajouter une nouvelle exception

6

Avancés

Stratégies

Protection

WEB

Prévention des intrusions

WAN TO DMZ

Régulation de flux

Aucune

Options supplémentaires

☐ Désactiver la prise en charge de la compression

☐ Réécrire le HTML

☐ Ignorer l'en-tête de l'hôte

Enregistrer

Annuler

Description :

Zone 1

PORT B : c'est le port wan le port d'entrée du pare-feu

HTTPS : c'est le protocole par lequel on accède au site web de façon sécurisé : doit être coché

REDIRECTION HTTP : permet de rediriger l'internaute qui utilise http vers https : doit être coché

Zone 2

C'est ici qu'il faut configurer le port d'écoute du protocole https : 443

Zone 3

C'est ici qu'il faut ajouter le certificat de sécurité

Zone 4

C'est ici qu'il faut ajouter le nom de domaine lié au site web

Zone 5

Cette zone permet d'ajouter le serveur sur lequel le site web est hébergé ; Il s'agit du serveur configuré dans le waf

Zone 6

Protection : La stratégie de protection appliqué ici est la stratégie web

Prevention des intrusions : Ici il s'agit de prévenir les intrusions qui viennent du wan vers la DMZ

VII-/ Configuration du routeur Dray tek en pont

La configuration du routeur Dray **tek en mode pont s'impose** à notre configuration pour un besoin bien spécifique. Le routeur Cyberoam étant un routeur DSL il faut obligatoirement un routeur en amont de type ADSL pour le connecter à Internet. La configuration du routeur Dray tek en pont a pour avantage **de récupérer directement l'adresse** IP publique et le mettre dans le Cyberoam. Cette configuration nous **permet d'accéder au Cyberoam depuis n'importe quel endroit et cela simplifie l'administration**. Pour configurer le Dray tek en pont on procède comme suit :

- 1- On se connecte à l'interface graphique du Dray tek 192.168.1.1
- 2- Clique sur Wan puis sur accès Internet et sur pppoE/pppoA

WAN >> Accès Internet

WAN 1

PPPoE / PPPoA	MPoA (RFC1483/2684)
<input type="radio"/> Activer <input checked="" type="radio"/> Désactiver	Configuration de l'accès au FAI Nom d'utilisateur: <input type="text" value="aviso/orangecelpaid1"/> Mot de passe: <input type="password" value="....."/> Authentification PPP: <input type="text" value="PAP ou CHAP"/> Délai d'inactivité: <input type="text" value="-1"/> seconde(s)
Configuration de modem DSL Canal Multi-PVC: <input type="text" value="Channel 1"/> VPI: <input type="text" value="8"/> VCI: <input type="text" value="35"/> Type Encapsulation: <input type="text" value="LLC/SNAP"/> Protocole: <input type="text" value="PPPoE"/> Modulation: <input type="text" value="Multimode"/>	Adresse IP fournie par FAI <input type="text" value="Alias de l'IP du WAN"/> IP fixe: <input type="radio"/> Oui <input checked="" type="radio"/> Non (IP dynamique) Adresse IP fixe: <input type="text"/> <input checked="" type="radio"/> Adresse MAC par défaut <input type="radio"/> Spécifier une adresse MAC Adresse MAC: <input type="text" value="00"/> <input type="text" value="50"/> <input type="text" value="7F"/> <input type="text" value="EA"/> <input type="text" value="4C"/> <input type="text" value="B9"/> Index(1-15) dans Horaire Configuration: => <input type="text"/> , <input type="text"/> , <input type="text"/> , <input type="text"/>
PPPoE Pass-through <input type="checkbox"/> Pour LAN filaire <input type="checkbox"/> Pour LAN sans fil	
WAN Connection Detection Mode: <input type="text" value="Toujours actif"/> Ping IP: <input type="text"/> TTL: <input type="text"/>	

OK

Annuler

3- Cliquez sur désactiver

4- Cliquez sur PVCs multiples puis décocher le canal 1 comme indiquez ci-dessous

WAN >> Multi-PVC

Multi-PVC

Général	QoS ATM	Mode pont (port-based)				
Canal	Activer	VPI	VCI	Type de QoS	Protocole	Encapsulation
1.	<input type="checkbox"/>	8	35	UBR	PPPoE	LLC/SNAP
2.	<input checked="" type="checkbox"/>	8	35	UBR	MPoA	1483 Bridged IP LLC
3.	WAN	1	43	UBR	PPPoA	VC MUX
4.	WAN	1	44	UBR	PPPoA	VC MUX
5.	WAN	1	45	UBR	PPPoA	VC MUX
6.	<input type="checkbox"/>	1	46	UBR	PPPoA	VC MUX
7.	<input type="checkbox"/>	1	47	UBR	PPPoA	VC MUX
8.	<input type="checkbox"/>	1	48	UBR	PPPoA	VC MUX

Remarque: VPI/VCI doit être unique pour chaque canal.

OK

Effacer

Annuler

- 5- Revenir sur Accès Internet puis cliquer sur MPoA (RFC1483/2684) et renseigner comme ci-dessous

WAN >> Internet Access

WAN 1

PPPoE / PPPoA **MPoA (RFC1483/2684)**

☐ Activer ☒ Désactiver

Paramètres du modem DSL

Canal multi-PVC Channel 2

Encapsulation 1483 Bridged IP LLC

VPI 8

VCI 36

Modulation Multimode

WAN Connection Detection

Mode Toujours actif

Ping IP

TTL:

Protocole RIP

☐ Activer RIP

Mode Pont

☒ Activer le mode pont

Paramètres de réseau IP WAN

Alias de l'IP du WAN

☐ Obtenir une adresse IP automatiquement

Nom du routeur *

Nom de domaine *

* : Nécessaire pour certains FAIs

☒ Specify an IP address

Adresse IP

Masque de sous-réseau

Adresse IP de passerelle

☐ Adresse MAC par défaut

☐ Spécifier une adresse MAC

MAC Address: 00 . 50 . 7F : EA . 4C . B9

Adresse IP du serveur DNS

Adresse IP primaire

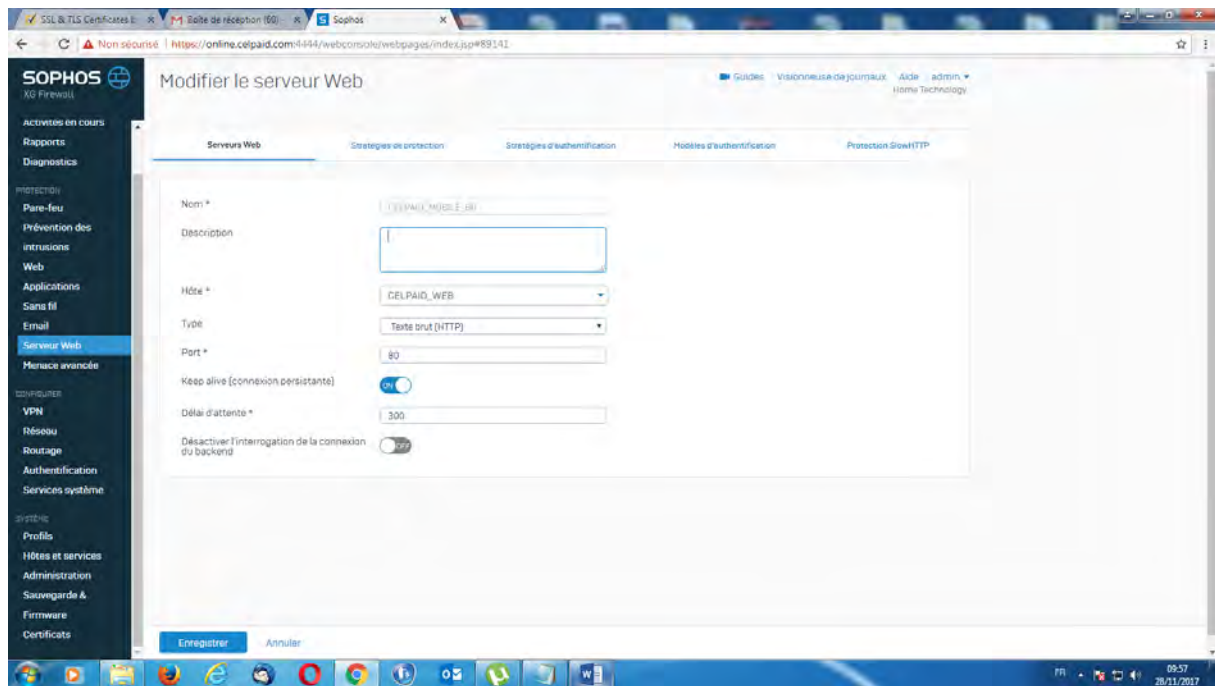
Adresse IP secondaire

- 6- Cliquez sur Ok et le routeur est configuré en pont

VIII-/ L'utilisation d'un seul certificat pour le déploiement de plusieurs sites

VIII.1-/ Configuration du waf

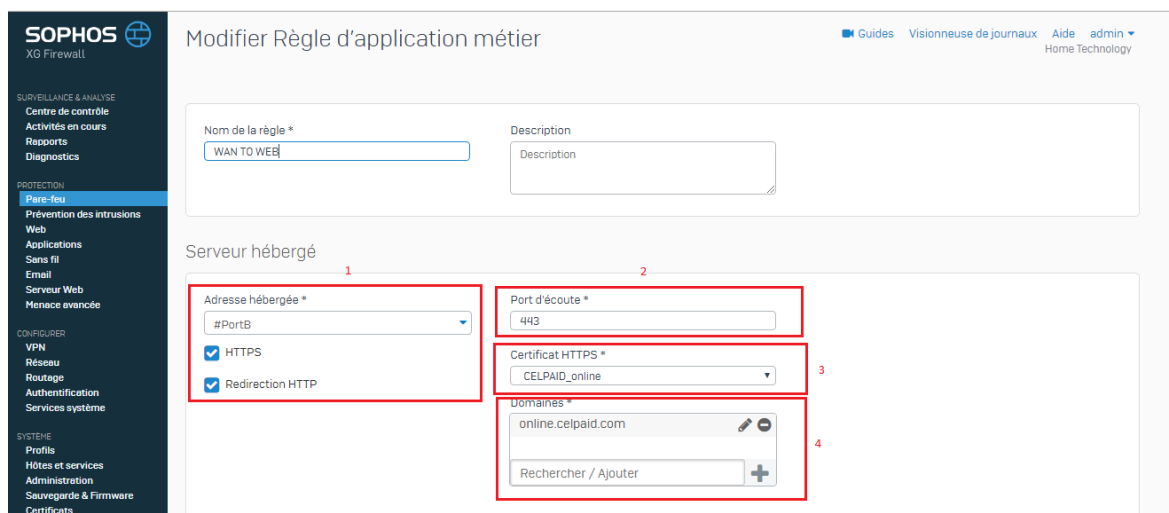
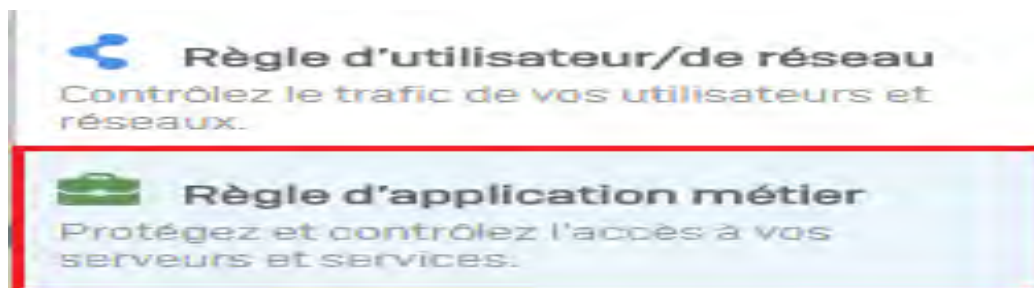
Contrairement au Cyberoam, la configuration d'un waf dans le Sophos se fait simplement en renseignant cet écran dans le menu serveur web



Hôte : représente ici le serveur sur lequel le site web est hébergé

VIII.2-/ Règle du waf

La configuration du waf doit obligatoirement se terminer par un règle sans laquelle le site web n'apparaîtra pas dans un navigateur. La configuration de cette règle se fait avec la deuxième option



SOPHOS XG Firewall

Modifieur Règle d'application métier

Guides Visionneuse de journaux Aide admin Home Technology

SURVEILLANCE & ANALYSE
Centre de contrôle
Activités en cours
Rapports
Diagnostics

PROTECTION
Pare-feu
Prévention des intrusions
Web
Applications
Sans fil
Email
Serveur Web
Menace avancée

CONFIGURER
VPN
Réseau
Routage
Authentification
Services système

SYSTÈME
Profil
Hôtes et services
Administration
Sauvegarde & Firmware
Certificats

5

Serveur(s) protégé(s)

☐ Routage selon le chemin

Serveur Web *

Liste des serveurs Web

saisir un texte pour la recherche Créer

☐ CELPAID_MOBILE_8080
☐ CELPAID_MOBILE_88
☒ CELPAID_MOBILE_80

Serveur(s) Web sélectionné(s)
CELPAID_MOBILE_80

faire glisser pour modifier la priorité

Autorisation d'accès

Autorisés les réseaux client
Any IPv4

Bloqués les réseaux client

Authentification
Aucune

Ajouter un nouvel élément

SOPHOS XG Firewall

Modifieur Règle d'application métier

Guides Visionneuse de journaux Aide admin Home Technology

SURVEILLANCE & ANALYSE
Centre de contrôle
Activités en cours
Rapports
Diagnostics

PROTECTION
Pare-feu
Prévention des intrusions
Web
Applications
Sans fil
Email
Serveur Web
Menace avancée

CONFIGURER
VPN
Réseau
Routage
Authentification
Services système

SYSTÈME
Profil
Hôtes et services
Administration
Sauvegarde & Firmware
Certificats

Exceptions

Chemins	Sources	Vérification	Catégories	État	Modifier/Supprimer
Données introuvables					

Ajouter une nouvelle exception

Avancés

Stratégies

6

Protection
WEB

Prévention des intrusions
WAN TO DMZ

Régulation de flux
Aucune

Options supplémentaires

☐ Désactiver la prise en charge de la compression
☐ Réécrire le HTML
☐ Ignorer l'en-tête de l'hôte

Enregistrer Annuler

Description :

Zone 1

PORT B : c'est le port wan le port d'entrée du pare-feu

HTTPS : c'est le protocole par lequel on accède au site web de façon sécurisé : doit être coché

REDIRECTION HTTP : permet de rediriger l'internaute qui utilise http vers https : doit être coché

Zone 2

C'est ici qu'il faut configurer le port d'écoute du protocole https : 443

Zone 3

C'est ici qu'il faut ajouter le certificat de sécurité

Zone 4

C'est ici qu'il faut ajouter le nom de domaine lié au site web

Zone 5

Cette zone permet d'ajouter le serveur sur lequel le site web est hébergé ; Il s'agit du serveur configuré dans le waf

Zone 6

Protection : La stratégie de protection appliquée ici est la stratégie web

Prévention des intrusions : Ici il s'agit de prévenir les intrusions qui viennent du wan vers la DMZ

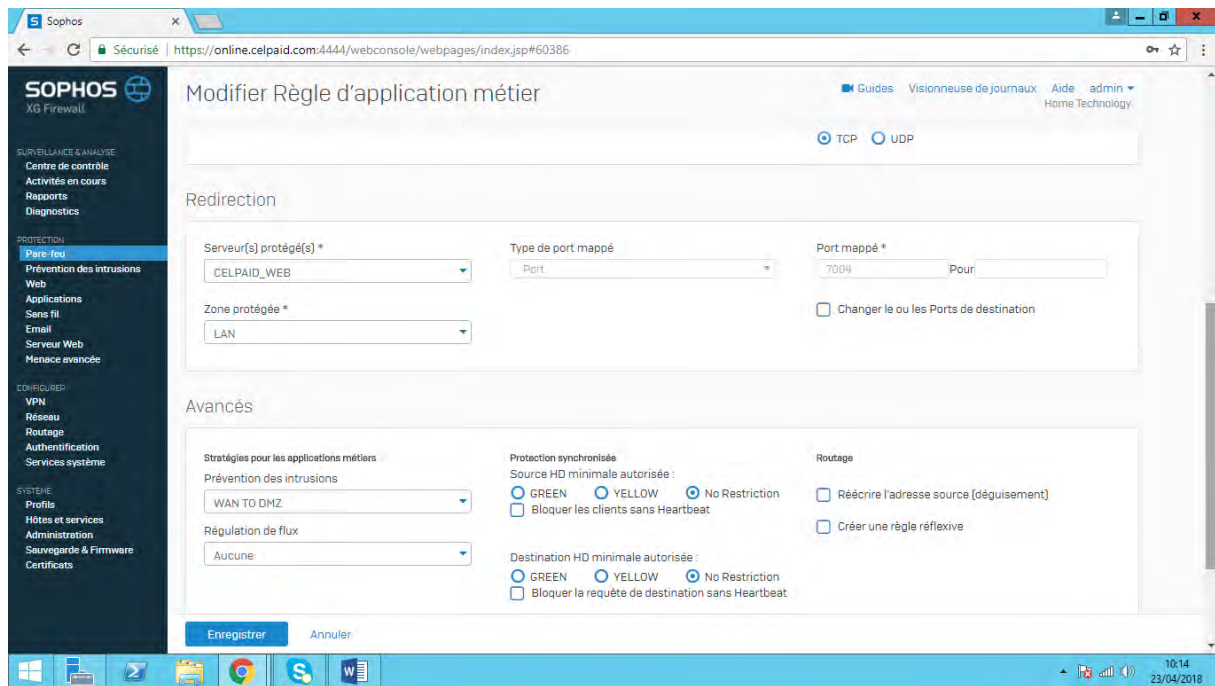
VIII. 3-/ Règle pour un autre site

Le certificat de sécurité a été déjà pour le sous-domaine. Tous les sites tu même sous domaine bénéficie de la sécurité du même certificat. Ainsi nous n'avons plus besoin de configurer le WAF pour ce site une simple règle de redirection suffit.

The screenshot shows the Sophos XG Firewall web interface. The browser address bar displays <https://online.celpaid.com:4444/webconsole/webpages/index.jsp#60386>. The page title is 'Modifier Règle d'application métier'. The left sidebar contains navigation menus for 'SURVEILLANCE & ANALYSE', 'PROTECTION', 'CONFIGURATION', and 'SYSTÈME'. The main content area is divided into three sections:

- Rule Details:** Includes 'Nom de la règle *' (PAIEMENT_MARCHAND) and 'Description'.
- Source:** Includes 'Zones émettrices *' (WAN), 'Autorisés les réseaux client *' (Tous), and 'Bloqués les réseaux client'.
- Destination & Service:** Includes 'Hôte/Réseau de destination *' (#PortB-41.207.10.216), 'Type de redirection' (Port), and 'Ports de service redirigés *' (7004 Pour).

At the bottom of the form are buttons for 'Enregistrer' (Save) and 'Annuler' (Cancel). The Windows taskbar at the bottom shows the date and time as 10:14 on 23/04/2018.

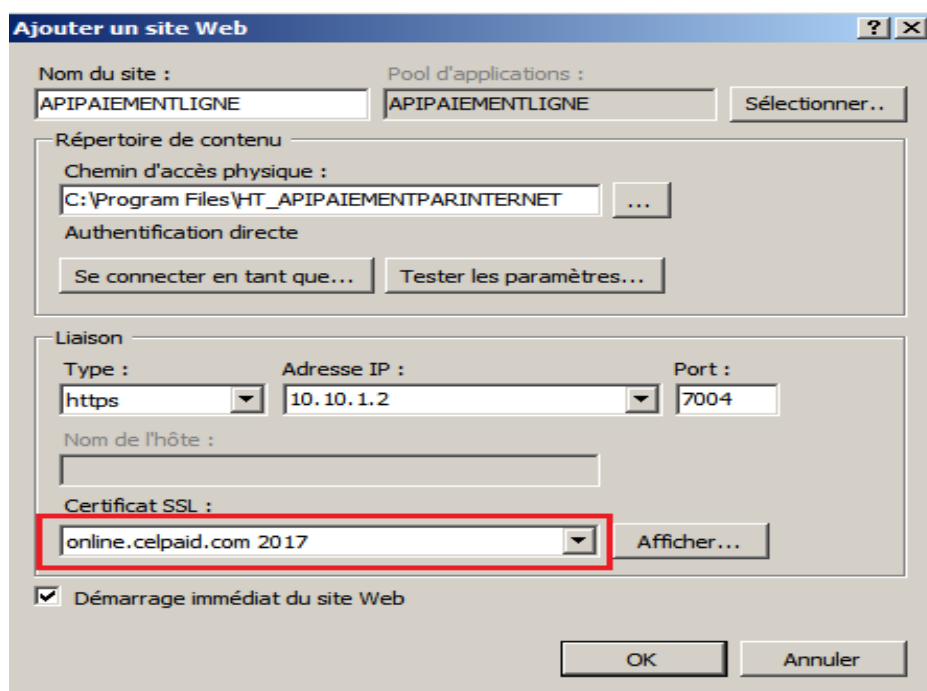


VIII.4- / Déploiement de site dans IIS

Le déploiement du site se fait sur le serveur d'application en https contrairement aux autres sites qui sont déployé en http.

Pour la configuration du site on procède comme suit :

- 1- On lance IIS
- 2- On fait un Clic droit sur site puis on clique sur ajout de site
- 3- On renseigne comme ci-indiqué



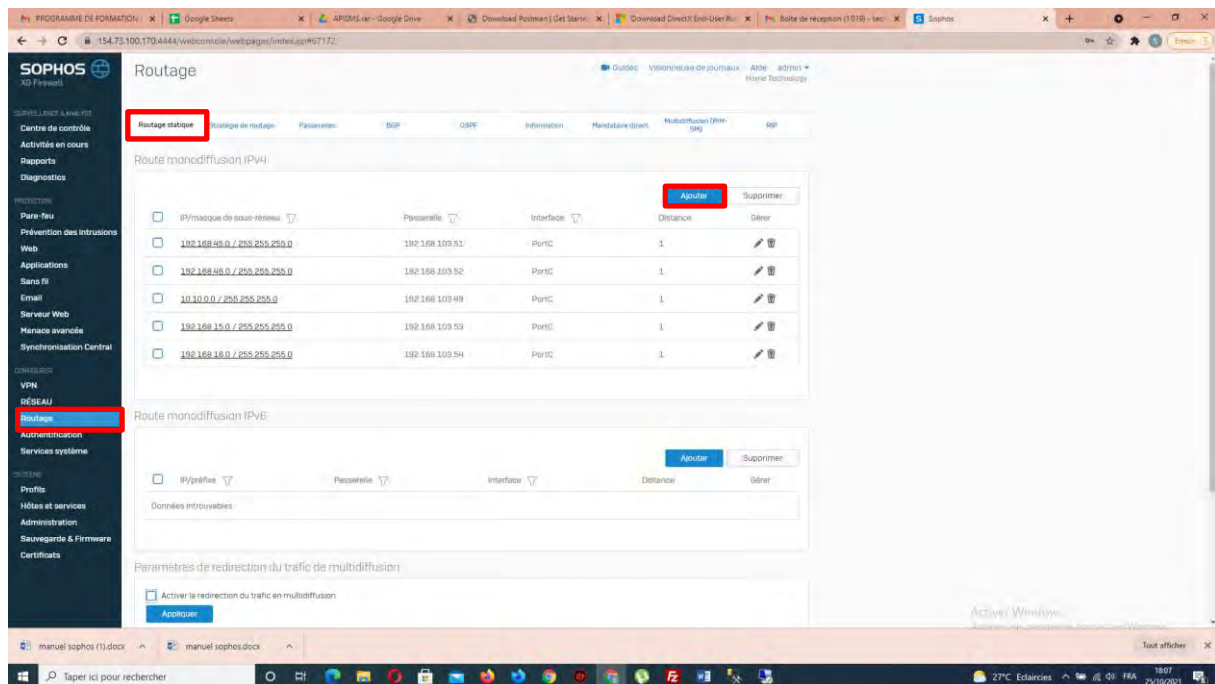
- 4- Prend soit de sélectionner le certificat

VIII.4-/ Routage statique d'une adresse IP (CAS RCMEC)

Le routage statique d'adresse IP intervient lorsqu'on souhaite accéder à un autre équipement via une route définie au préalable.

Pour la configuration on procède comme suit :

1. On se connecte à la console Sophos
2. On clique sur le menu Routage
3. Dans le menu Routage Static, on clique sur le bouton Ajouter



4. Renseigner les informations comme suit :

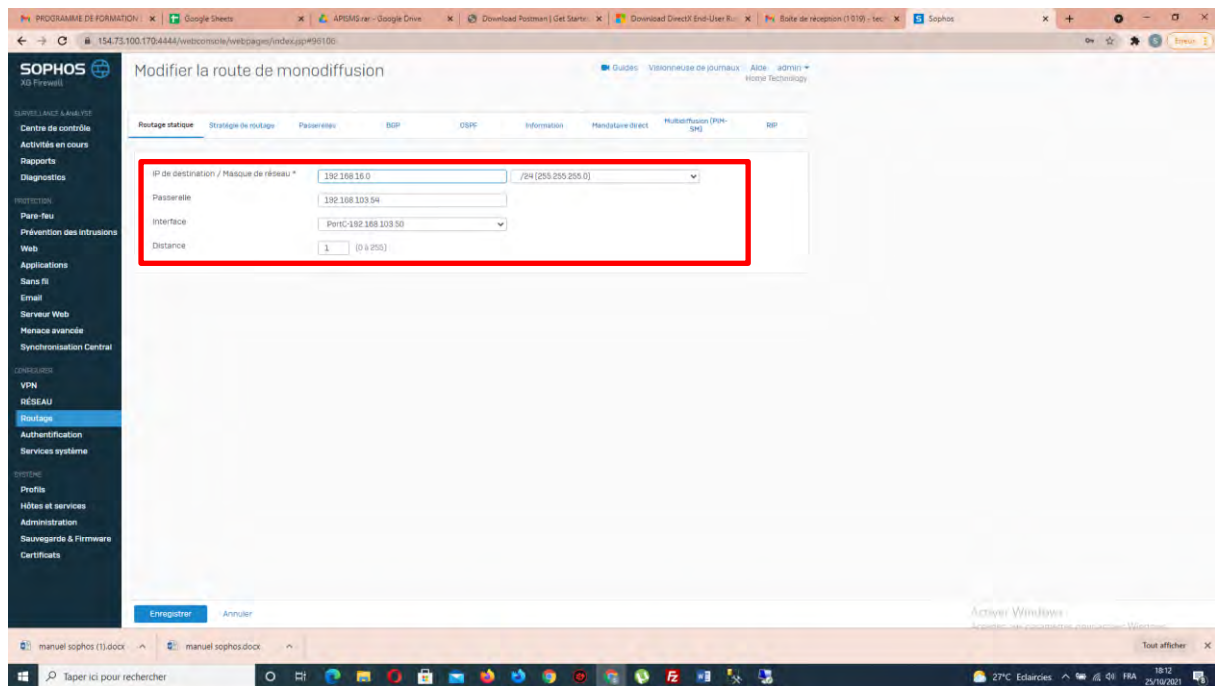
IP de destination / Masque de réseau = LAN ; Ex : 192.168.16.0

Passerelle = GW (Gateway) ; Ex : 192.168.103.54

Interface = Port C

Distance = 1

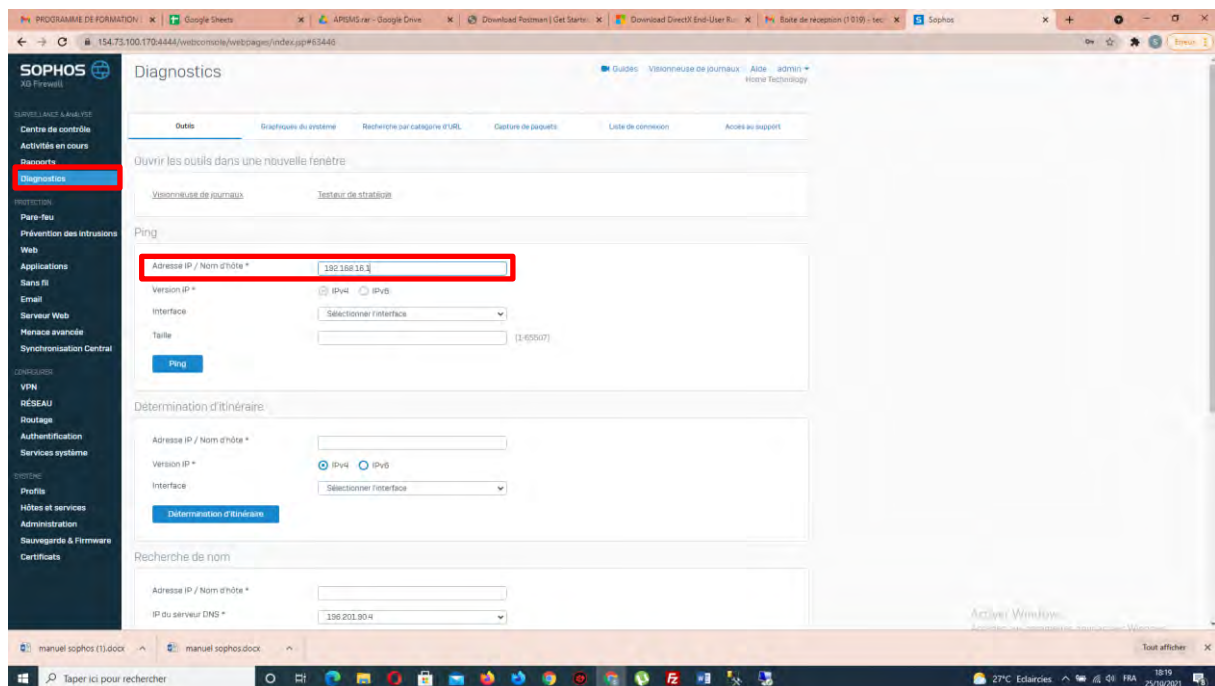
La passerelle et la gateway seront transmis par ECOBAND. **L'interface et la distance restent identiques à ceux présentés en haut.**



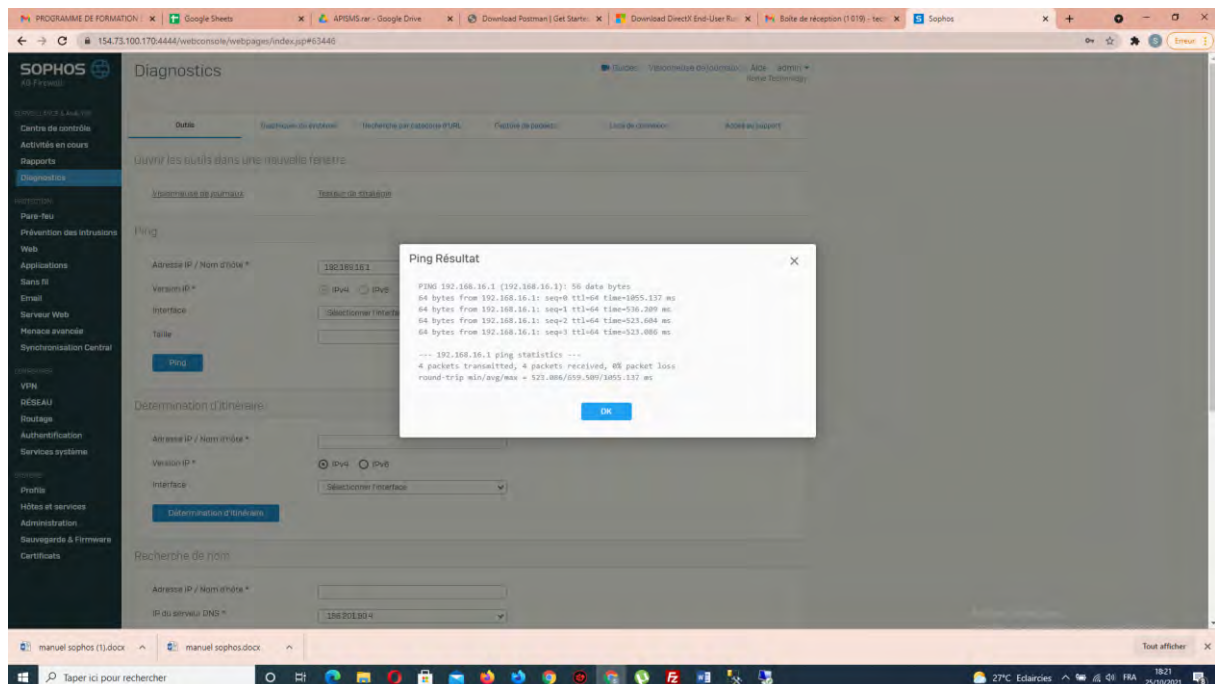
5. Faire le ping de la passerelle et du LAN. On clique sur le menu Diagnostics

Test du LAN (*On met l'adresse IP du routeur du LAN*)

- **Adresse IP / Nom d'hôte : 192.168.16.1**
- **Clique sur Ping pour lancer le ping**

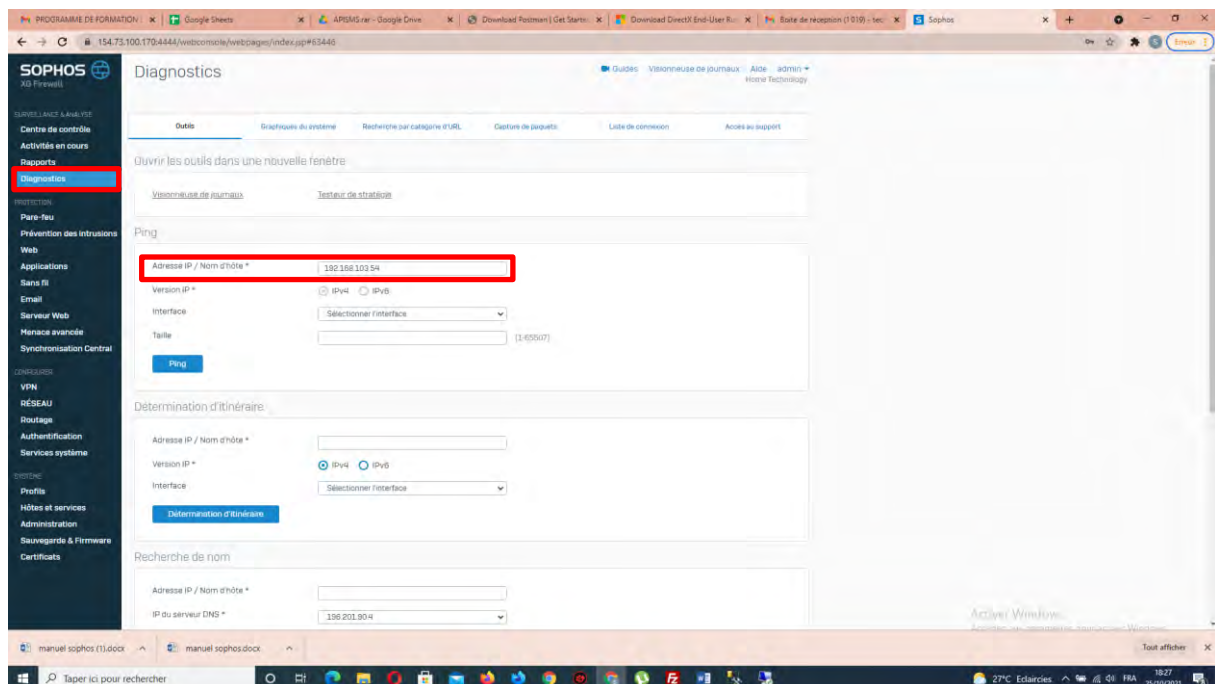


Vous devez avoir ce message si tout est OK. Sinon contactez Ecoband.



Test de la passerelle ou Gateway (GW)

- **Adresse IP / Nom d'hôte : 192.168.103.54**
- **Clique sur Ping pour lancer le ping**



Vous devez avoir ce message si tout est OK. Sinon contactez Ecoband.

