



Guide utilisateur

Version V5R7

Documentation : Révision 0

SOMMAIRE

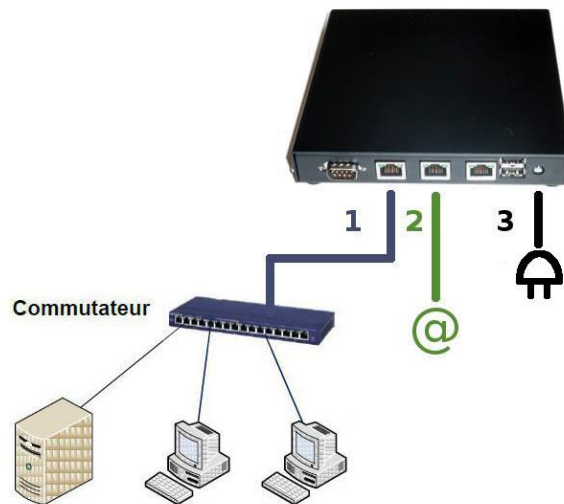
1.INSTALLATION DU BOITIER EN MODE PLUG&PLAY	6
2.ACCES ET CONNEXION A L'INTERFACE D'ADMINISTRATION	7
2.1.Accès à l'interface d'administration automatique	7
2.2.Accès à l'interface d'administration via l'IP	7
2.3.Accès à l'interface d'administration via l'IP permanente	7
2.4.Connexion à l'interface d'administration	8
3.ADMINISTRATION DU BOITIER	9
3.1.Le tableau de bord	10
3.1.1. Informations	10
3.1.2. Activité du jour	12
3.2.Profils de sécurité	14
3.2.1. Catégories	14
3.2.2. Postes autorisés	15
3.2.3. HTTPS (mode SNI et Proxy)	16
3.2.4. HTTPS en mode proxy	16
3.2.5. HTTPS en mode SNI	17
3.2.6. Mode SafeSearch	17
3.2.7. Catégorie « Sites dangereux »	18
3.2.8. Gestion de plusieurs profils de sécurité	18
3.2.9. Expressions	20
3.2.10. Exception de filtrage	21
3.2.10.1. Exception de filtrage par adresse Mac	21
3.2.10.2. Exception de filtrage par adresse IP	22
3.2.10.3. Exclure un site du filtrage	22
3.2.11. Filtrage des Smartphones	23
3.2.12. Liste des ports autorisés	25
3.2.13. Personnalisation des interfaces d'accueil	26
3.3.Listes N&B	27
3.3.1. Profils de sécurité	27
3.3.1.1. Liste blanche	27
3.3.1.2. Liste noire	28
3.4.Activité @	29
3.4.1. Format des traces	29
3.4.2. Actualiser les logs	30
3.4.3. Exportation des logs de traçabilité au format CSV	30
3.4.4. Analyse statistique (Top N)	30

3.4.5.	Exportation des résultats statistiques en fichier CSV	31
3.4.6.	Analyse statistique - Résultats	31
3.4.7.	Analyse multicritère – Recherche Avancée	32
3.4.8.	Exportations des résultats avancés au format CSV	32
3.4.9.	Analyse multicritère – Résultats	32
3.4.10.	Rapports d'activité	33
3.4.11.	Liste d'exclusion des résultats	33
3.5.	Plages horaires	35
3.6.	Authentification	36
3.6.1.	Activation	36
3.6.2.	Types d'authentification	36
3.6.3.	Options	37
3.6.4.	Hierarchie des authentifications	38
3.6.5.	Paramétrage de l'authentification par IP	38
3.6.6.	Paramétrage de l'authentification par Active Directory	38
3.6.7.	Paramétrage de l'authentification du portail utilisateur	39
3.6.8.	Paramétrage de l'authentification par page d'accueil	40
3.6.9.	Portails SMS	41
3.6.10.	Portail EMAIL	42
3.6.11.	Paramétrage de l'authentification temporaire	44
3.6.12.	Déclenchement du portail captif	45
3.6.13.	Gestion des groupes et des utilisateurs	46
3.6.13.1.	Gestion des groupes	46
3.6.13.2.	Gestion des utilisateurs	48
3.7.	Personnalisation de la page d'accueil du portail d'authentification.	50
3.8.	Administrateurs secondaires	51
3.9.	Système	52
3.9.1.	Nom du boîtier	52
3.9.2.	Configuration	52
3.9.3.	Mises à jour	52
3.9.4.	Gestion du boîtier	53
3.9.5.	Changement du mot de passe de l'administrateur	53
3.9.6.	Changement de l'email administrateur	53
3.9.7.	Sauvegarde / Restauration	54
3.9.7.1.	Sauvegarde automatique de la base de données système	54
3.9.7.2.	Sauvegarde / restauration manuelle de configuration système	55
3.9.7.3.	Sauvegarde / restauration manuelle de la base de données système	55
3.10.	Fonctions avancées	56
3.10.1.	Mode Bridge et Routeur	56
3.10.1.1.	Mode Bridge	56
3.10.1.2.	Mode Routeur	57
3.10.2.	Serveur DHCP	58
3.10.3.	Table de routage	59
3.10.4.	Réseau secondaire	59
3.10.5.	Options	61
3.10.5.1.	Télémaintenance	62
3.10.5.2.	Traçabilité et cryptage des historiques de navigation	62
3.10.5.3.	Comportement en cas de défaillance (Safe mode)	63

3.10.5.4.	Relais DNS	63
3.10.5.5.	Initialisation en configuration usine	64
3.10.5.6.	Fuseau Horaire	64
3.10.6.	Gestion de flotte de boitiers	65
3.10.6.1.	Description	65
3.10.6.2.	Boitier de référence MASTER	65
3.10.6.3.	Boitier dépendant appartenant à une flotte	67
3.10.6.4.	Boitier indépendant	68
3.10.7.	Internet X2 (Multiwan)	69
3.10.7.1.	Connectique	69
3.10.7.2.	Mode Bridge /Mode Routeur	69
3.10.7.3.	Paramètres	70
3.10.7.4.	Routage multiwan (route policy)	71
3.10.8.	Diagnostics	72
3.10.9.	Gestion des mises à jour logicielles	73
3.10.9.1.	Objectifs	73
3.10.9.2.	Administration des mises à jour logicielles	74
4.	REMISE EN CONFIGURATION USINE.	76
5.	REINITIALISATION DU MOT DE PASSE D'ADMINISTRATION	76
6.	SUPPORT TECHNIQUE	77
7.	ANNEXES	78
7.1.	Plateforme SMS lesms.com	78
7.2.	Plateforme OVH	79
7.3.	Connectique	83
7.4.	Installation du certificat SSL	84
7.4.1.	Installation du certificat via console MMC	84
7.4.2.	Installation du certificat	91
7.4.2.1.	Navigateur Mozilla Firefox	91
7.4.2.2.	Navigateur Internet Explorer / Chrome	92
7.5.	Connecteur AD/SSO	96
7.5.1.	Principe de fonctionnement	96
7.5.2.	Installation	97
7.5.2.1.	Installation des sources	97
7.5.2.2.	Installation du client SSH	97
7.5.2.3.	GPO Frogi-Login	99
7.5.2.4.	Création de la tâche planifiée	103
7.5.2.5.	Création de la relation AD / Profils	105
7.5.3.	Gestion DNS	105
7.5.3.1.	Le mode SafeSearch est activé dans tous les profils de sécurité	105
7.5.3.2.	Serveur AD exclu du filtrage ou mode SafeSearch différent selon les profils.	105
7.6.	Profil Profs / Elèves	108

7.6.1.	Objectif	108
7.6.2.	Création du profil « Profs »	108
7.6.3.	Création du groupe Ip « élèves »	109
7.6.4.	Création du groupe d'utilisateurs « Profs »	111
7.6.5.	Création de l'utilisateur « Prof »	112
7.6.6.	Activation des authentifications	112
7.6.7.	Connexion au profil « Profs »	113
7.6.8.	Déconnexion du profil « Profs »	113

1. Installation du boîtier en mode Plug&Play



1. Connectez votre accès réseau à l'un des ports du boîtier.
2. Connectez votre accès Internet à l'un des ports du boîtier.
3. Branchez l'adaptateur secteur.

Le boîtier démarre et reconnaît votre réseau. Il se met alors en relation avec le data center de Frogi Secure et procède à l'activation de votre produit.

Après quelques minutes (3 min) le boîtier est opérationnel et votre réseau est sécurisé.

Remarque :

Vous pouvez connecter votre accès réseau et l'accès Internet sur n'importe quel port du boîtier, **il est par contre impératif de réaliser ces connexions avant de mettre le boîtier sous tension.**

Contrainte d'utilisation :



Avertissement prolongé si aucun service DHCP n'est reconnu.

Par défaut, le boîtier fonctionne en mode bridge et s'appuie sur un service DHCP.

Vous devez disposer d'un service de distribution d'adresses IP (DHCP) soit au niveau du point d'accès Internet (box de l'opérateur), soit sur un des postes du réseau. Dans le cas contraire il est possible d'activer ce service en configurant votre boîtier en vous référant au paragraphe « fonctions avancées ».

2. Accès et connexion à l'interface d'administration

2.1. Accès à l'interface d'administration automatique

Depuis le réseau contrôlé par le boîtier, pour accéder à l'interface d'administration, connectez-vous depuis n'importe quel poste du réseau au site Internet suivant :

<http://admin.frogi-secure.com>

2.2. Accès à l'interface d'administration via l'IP

Il est possible d'accéder à la console d'administration directement par son adresse IP

Depuis le Lan de l'établissement

<https://@ip-privee/login.php>

Depuis l'extérieur en effectuant une redirection de port sur l'Ip du boîtier

<https://@ip-publique:30081/login.php>

2.3. Accès à l'interface d'administration via l'IP permanente

Quelle que soit sa configuration, le boîtier a toujours l'adresse d'administration 192.0.2.1

<https://192.0.2.1/login.php>

2.4. Connexion à l'interface d'administration

Une page de connexion sécurisée vous demande vos identifiants :



The login interface features the FROGI-SECURE logo at the top, with a cartoon frog character peeking over it. Below the logo is a box titled "ADMINISTRATION" containing two input fields labeled "UTILISATEUR:" and "MOT DE PASSE:". A green "CONNEXION" button is positioned below the fields. At the bottom of the page, a small copyright notice reads "Frogi-Secure - 2016 - © Tous droits réservés".

Le login administrateur est « **admin** », le mot de passe par défaut est indiqué sur l'étiquette sous votre boîtier. **Le mot de passe étant la dernière partie du numéro de série.**



(Exemple ici *vui7Iquu*)

3. Administration du boîtier



Tableau de bord : Tableau récapitulatif des services activés, des paramètres du boîtier et de l'activité Internet.

Profils de sécurité : Gestion des règles de sécurité et des exclusions de filtrage.

Listes N&B : Gestion des listes blanches et noires.

Activité @ : Configuration et analyse de l'activité Internet.

Plages horaires : Gestion des plages horaires.

Authentification : Gestion des utilisateurs et de l'authentification.

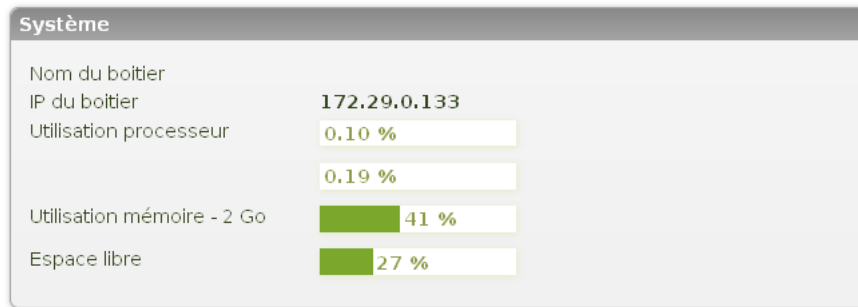
Antivirus : Gestion de l'antivirus.

Système : Sauvegarde, restauration et mise à jour du boîtier.

Fonctions avancées Permet de définir l'adresse IP du bridge, routeur, de paramétrer le multiwan et les services DHCP, de renseigner la table de routage, de paramétrer un réseau secondaire, changer les options de configuration.

3.1. Le tableau de bord

3.1.1. Informations



Nom du boîtier : Nom du boîtier tel que défini dans l'onglet «Système».

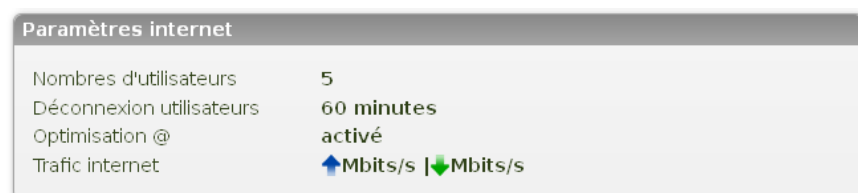
IP du boîtier : Adresse IP allouée au boîtier par le service DHCP du réseau ou défini dans les « fonctions avancées ».

IP publique : après avoir cliqué sur la loupe, l'IP publique Internet sera affichée.

Utilisation du processeur : ...

Utilisation mémoire : ...

Utilisation de l'espace disque : ...



Nombre d'utilisateurs : Nombre d'utilisateurs connectés à Internet dans les 20 dernières minutes.

Déconnexion utilisateurs : Si l'option d'authentification est activée, c'est la durée d'inactivité Internet qui déclenchera une déconnexion automatique de l'utilisateur.

Optimisation : Indique si la fonction QOS (optimisation du débit de la liaison Internet) est activée (voir onglet Système).

Trafic Internet : Débit montant et descendant de la liaison Internet.

Sécurité	
Authentification	désactivé
Traçabilité	activé
Nombres de sites référencés	4.288607 million(s)
Version de filtrage Web	Mardi 25 Octobre 2016 20:31:01
Antivirus	activé
Antivirus	26 Oct 2016 08:02:32

Authentification : Indique si la fonction d'authentification est activée.

Traçabilité : Indique si la fonction de traçabilité est activée.

Nombre de sites référencés : Nombre de sites référencés dans la base de filtrage.

Version de filtrage Web: Date de création de la base de filtrage.

Configuration	
Date de fin de garantie	Dimanche 20 Octobre 2019
Numéro de série	R20-APU2-415B0E
Système	V5R2
TBI	2
Patch	161019_0
Date de mise à jour système	Mercredi 19 Octobre 2016 18:44

Date de fin de garantie : La période de garantie démarre à la date de facturation.

Numéro de série : ...

Système : Version logicielle.

TBI : Révision du firmware.

Patch : Niveau de mise à jour.

Date de mise à jour système : Date de la dernière mise à jour logicielle.

3.1.2. Activité du jour

Informations sur l'activité Internet du jour selon différents critères.

Top 10 hits

URL	Hits	Utilisateurs
clients1.google.com	13	GEORGES-PC
ocsp.digicert.com	5	GEORGES-PC
xml.alexa.com	3	GEORGES-PC
toolbarqueries.google.com	3	GEORGES-PC
www.msftncsi.com	2	GEORGES-PC
www5.mail-cdiscount.com	2	GEORGES-PC
meetic.fr	1	GEORGES-PC
download.windowsupdate.com	1	GEORGES-PC
ocsp2.globalsign.com	1	GEORGES-PC
www.frogi-secure.com	1	GEORGES-PC

10 derniers sites visités

Heure de début	Heure de fin	IP	Utilisateurs	URL	Taille
10:39:13	10:40:41	172.29.0.114	GEORGES-PC	clients1.google.com	2.57 Ko
10:32:58	10:33:22	172.29.0.114	GEORGES-PC	www.fairesonchoix.net	12.95 Ko
10:32:58	10:32:58	172.29.0.114	GEORGES-PC	xml.alexa.com	0.91 Ko
10:32:58	10:32:58	172.29.0.114	GEORGES-PC	toolbarqueries.google.com	4.19 Ko
10:31:19	10:31:40	172.29.0.114	GEORGES-PC	clients1.google.com	1.71 Ko
10:29:27	10:29:27	172.29.0.114	GEORGES-PC	clients1.google.com	0.86 Ko
10:28:02	10:28:02	172.29.0.114	GEORGES-PC	crl.godaddy.com	13.9 Ko
10:19:01	10:19:40	172.29.0.114	GEORGES-PC	clients1.google.com	1.71 Ko
10:19:14	10:19:14	172.29.0.114	GEORGES-PC	www.frogi-secure.com	0.43 Ko
10:13:40	10:13:40	172.29.0.114	GEORGES-PC	clients1.google.com	0.86 Ko

Top 10 téléchargements

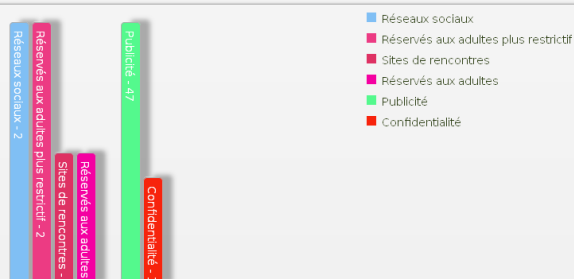
Heure de début	Heure de fin	IP	Utilisateurs	URL	Taille
11:57:35	11:57:39	172.29.0.114	GEORGES-PC	fpdownload2.macromedia.com	5.49 Mo
10:57:51	10:58:00	172.29.0.114	GEORGES-PC	fpdownload2.macromedia.com	5.15 Mo
09:45:51	09:45:56	172.29.0.114	GEORGES-PC	personal.avira-update.com	285.98 Ko
09:41:10	09:41:11	172.29.0.114	GEORGES-PC	www5.mail-cdiscount.com	98.65 Ko
11:45:55	11:45:59	172.29.0.114	GEORGES-PC	personal.avira-update.com	75.87 Ko
10:12:24	10:12:24	172.29.0.114	GEORGES-PC	ds.download.windowsupdate.com	32.4 Ko
13:45:52	13:45:52	172.29.0.114	GEORGES-PC	personal.avira-update.com	25.47 Ko
12:15:13	12:15:42	172.29.0.114	GEORGES-PC	172.29.0.133	24.55 Ko
14:46:56	14:46:56	172.29.0.114	GEORGES-PC	172.29.0.133	16 Ko
10:28:02	10:28:02	172.29.0.114	GEORGES-PC	crl.godaddy.com	13.9 Ko

Top 10 sites bloqués

URL	Hits	Catégories	Utilisateurs
meetic.fr	2	Sites de rencontres	GEORGES-PC
fdj.fr	1	Jeux d'argent (Gambling)	GEORGES-PC
teamviewer.com	1	Redirecteur	GEORGES-PC
sexe.fr	1	Réservés aux adultes	GEORGES-PC

Top des catégories bloquées

Catégories	Hits
Réseaux sociaux	2
Réservés aux adultes plus restrictif	2
Sites de rencontres	1
Réservés aux adultes	1
Nombres de publicités bloquées	47
Nombres d'atteinte potentiel à la confidentialité bloquées	19



3.2. Profils de sécurité

3.2.1. Catégories

CATÉGORIES		
Action	Catégories	Heures Ouvrées
	Seuls les postes autorisés (Mac Address) peuvent accéder à Internet	☐
	Tunnels VPN	☐
	Filtrage par ports TCP UDP (port autorisés)	☐
	Tous les sites Web Internet (HTTP/HTTPS)	☐
	HTTPS en mode SNI	☒
	HTTPS en mode proxy	☐
	Smartphones	☐
	Liste blanche	☒
	Liste noire	☒
	Sites labellisés Arjel	☐
	Sites labellisés Hadopi	☐
	Jeux d'argent (Gambling)	☒
	Sites Audio Video	☐
	Téléchargement de fichiers audio et video	☐
	Sites de téléchargement illégal (varez)	☒
	Réservés aux adultes	☒
	Filtre Safe Search pour les moteurs de recherche	☒
	Réservés aux adultes plus restrictif	☐
	Jeux-en-ligne	☐
	Sites de rencontres	☒
	Réseaux sociaux	☐
	Shopping	☐
	Sectes	☒
	Sites contenant des virus (hacking malware phishing)	☒
	Sites dangereux	☒
	Radios	☐
	Offres d'emplois (jobsearch)	☐
	Chat	☐
	Webmail	☐
	Loisirs Tourisme	☐
	Accès aux sites privés (RFC 1918)	☐
	Applications P2P	☐
	Sites accessibles par adresses IP	☐
	Interdit le trafic provenant d'Internet	☐

Les profils de sécurité s'appliquent en fonction de plages horaires qui sont définies dans l'onglet « Plages horaires ».

Certaines règles  correspondent à une autorisation d'accès, d'autres  à une interdiction.

Les règles s'appliquent de haut en bas, l'analyse s'arrête dès que le site appartient à une catégorie.

Si aucune règle n'est validée, la connexion sera autorisée.

Les bases de filtrage sont mises à jour automatiquement tous les jours.

Pour obtenir des informations sur les catégories, positionner le curseur sur le libellé de la catégorie, une info-bulle apparaîtra.

3.2.2. Postes autorisés

Seules les mac address connues du boitier seront autorisées à accéder à Internet, si leur profil de sécurité le permet.

Dans l'onglet « Profil de sécurité/Exceptions de sécurité » vous pouvez ajouter ou supprimer des address mac. Le mode apprentissage permet d'enregistrer automatiquement les mac address qui traversent le boitier, à la fin de la période d'apprentissage, la règle sera activée.

Liste des adresses mac autorisées

Ajouter une adresse MAC

Adresse MAC : : : : :

AJOUTER

Ajouter une liste d'adresses MAC

Liste adresse MAC Parcourir... Aucun fichier sélectionné.

AJOUTER

Découverte des postes présent sur le réseau

Exclure	IP	Adresse Mac	Nom Netbios
+	172.30.0.254	7c:26:64:65:cd:cb	SAGEMCOM
+	172.30.1.122	54:bf:64:10:bf:e3	PBS-PORTABLE

ACTUALISER

Mode apprentissage

Etat **Arrêt**

Durée d'apprentissage 1 jours

Date de fin d'apprentissage 0

DEMARRER

REPRENDRE

ARRETER

3.2.3. HTTPS (mode SNI et Proxy)

Le contrôle des connexions HTTPS se fait de deux façons :

1. Mode Proxy
2. Mode SNI

Remarque :

Le choix du mode de contrôle est un paramètre du profil, il est donc possible dans un même établissement d'avoir des profils qui utilisent le mode Proxy HTTPS et d'autres le mode SNI.

3.2.4. HTTPS en mode proxy

HTTPS en mode Proxy offre les mêmes fonctionnalités que le mode Proxy HTTP.

Si une connexion n'est pas autorisée, l'utilisateur en est informé.



L'utilisation du mode HTTPS Proxy nécessite l'installation d'un certificat sur chaque poste. Afin de faciliter le déploiement du certificat, celui-ci est disponible via l'emplacement Internet suivant :

<https://www.frogi-secure.com/certif/frogi-secure.der>

3.2.5. HTTPS en mode SNI

Le mode HTTPS SNI est totalement transparent, contrairement au mode HTTPS Proxy il ne nécessite pas l'installation d'un certificat sur les postes.

Par contre, du fait de l'absence de certificat pour valider la réponse à la connexion HTTPS, l'utilisateur n'est pas informé des raisons de l'échec de sa demande de connexion.



Désolé, nous ne pouvons pas atteindre cette page

Essayer

- Assurez-vous d'avoir la bonne adresse web : <https://www.pmu.fr>
- Rechercher "<https://www.pmu.fr>" sur Bing
- Actualiser la page

Details

3.2.6. Mode SafeSearch

Le mode SafeSearch permet d'indiquer aux moteurs de recherche de ne pas retourner des informations (listes de sites, images, vidéos) réservées aux adultes.

Les moteurs de recherche suivants sont supportés :

Mode HTTPS Proxy

Google.
Youtube
Bing.
Qwant
Yahoo

Mode HTTPS SNI

Google.
Youtube
Bing.
Qwant

3.2.7. Catégorie « Sites dangereux »

Contrairement aux autres catégories qui se mettent à jour toutes les 24 heures (entre 22 h et 5 h), la catégorie « Sites dangereux » est mise à jour toutes les heures.

Trois types de protections sont mis en œuvre :

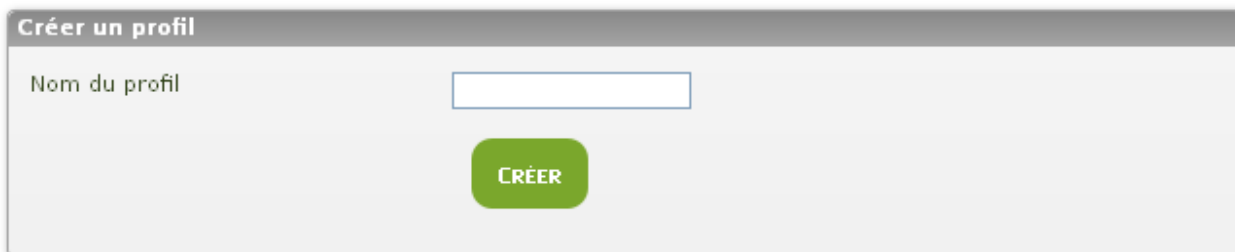
1. Filtrage d'Urls
2. Contrôle des adresses IP.
3. Base de signatures antivirales

Ces listes sont fournies par notre partenaire Malware Patrol (www.malwarepatrol.net) et permettent de mettre en œuvre des mécanismes automatiques de protection contre les menaces provenant de l'Internet.

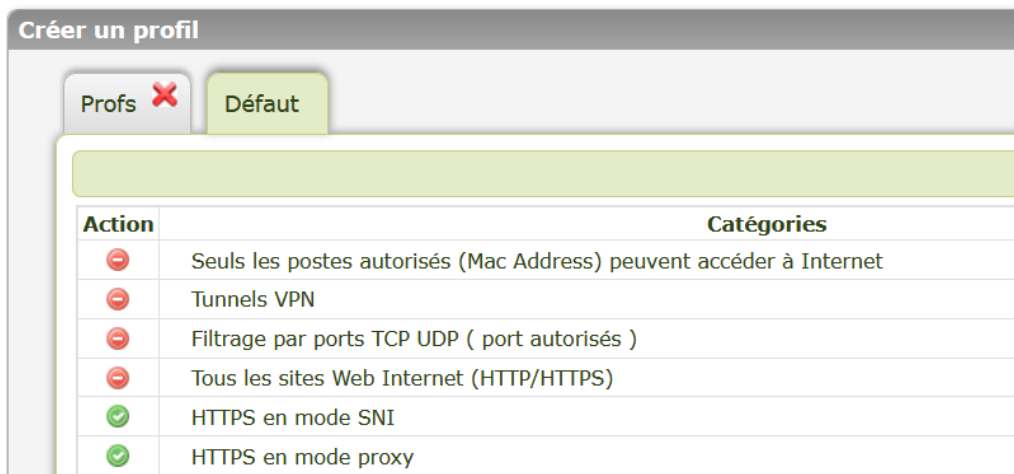
3.2.8. Gestion de plusieurs profils de sécurité

Il est possible de définir plusieurs profils de filtrage et d'affecter ces profils à des utilisateurs (si l'authentification est activée) ou à des postes (IP).

Création du profil



Chaque profil est paramétrable. Les modifications sont immédiates après application.



Action	Catégories
Seuls les postes autorisés (Mac Address) peuvent accéder à Internet	
Tunnels VPN	
Filtrage par ports TCP UDP (port autorisés)	
Tous les sites Web Internet (HTTP/HTTPS)	
HTTPS en mode SNI	
HTTPS en mode proxy	

Chaque profil est applicable à un ou plusieurs groupes d'utilisateurs. Pour cela, il suffit d'inclure ou d'exclure un groupe via l'interface présente au bas de l'onglet de paramétrage du profil.

GROUPE(S) ASSOCIÉ(S) AU PROFIL PROFIL2		
Groupe(s) existant(s)		Groupe(s) associé(s)
default SMS EMAIL PortailUser	INCLUDE >>> <<< EXCLUDE	

Remarque :

L'association Profil /Utilisateur ou Profil /@ip peut également se faire dans l'onglet « Authentification et Groupes ».

3.2.9. Expressions

Ce filtre ne s'active qu'en mode HTTPS Proxy.

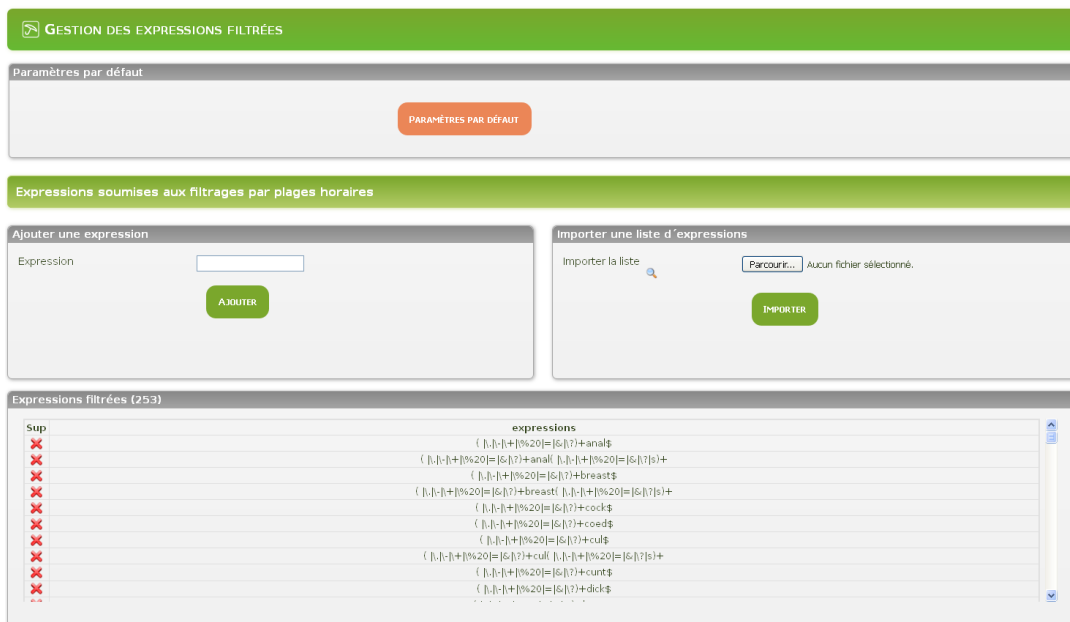
La catégorie de filtrage « réservée aux adultes plus restrictif » s'appuie sur des mots-clés ou expressions et s'applique à deux types de données.

1) **Les noms des sites Internet** (domaine et URL) incluant un des mots-clés de la liste seront automatiquement filtrés.

2) **La requête des moteurs de recherche**, si un des mots-clés apparaît dans la requête adressée au moteur de recherche la connexion, sera refusée.

La liste des expressions peut être créée à partir d'un fichier ou créée ou complétée manuellement.

Pour renforcer la pertinence des mots-clés vous pouvez utiliser des expressions régulières.



Sup	expressions
X	([i,j,-]+)%20=[Ss]?+anal\$
X	([i,j,-]+)%20=[Ss]?+anal[i,j,-]+)%20=[Ss]?+s)+
X	([i,j,-]+)%20=[Ss]?+breast\$
X	([i,j,-]+)%20=[Ss]?+breast[i,j,-]+)%20=[Ss]?+s)+
X	([i,j,-]+)%20=[Ss]?+cock\$
X	([i,j,-]+)%20=[Ss]?+cock\$
X	([i,j,-]+)%20=[Ss]?+cul\$
X	([i,j,-]+)%20=[Ss]?+cul[i,j,-]+)%20=[Ss]?+s)+
X	([i,j,-]+)%20=[Ss]?+cunt\$
X	([i,j,-]+)%20=[Ss]?+dick\$

Il est possible d'initialiser la liste par défaut en choisissant le bouton « paramètres par défaut » .

3.2.10. Exception de filtrage

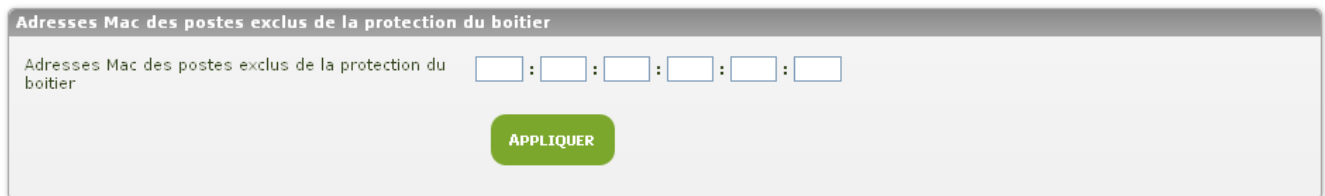
3.2.10.1.Exception de filtrage par adresse Mac

L'exclusion d'un poste par son adresse Mac peut se faire de 3 façons :

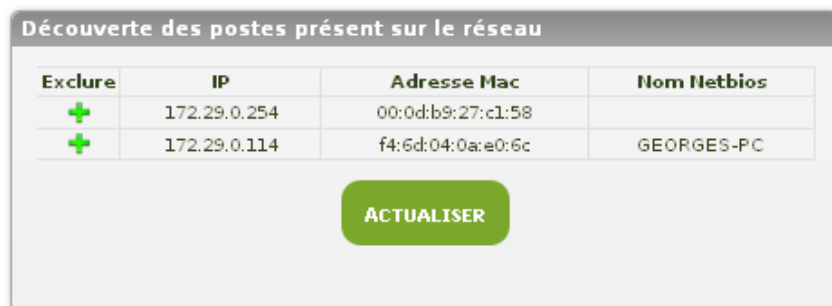
- 1) En se connectant sur l'interface d'administration à partir du poste que l'on désire exclure puis dans l'onglet « Profils de sécurité / Exception de sécurité » cliquer sur l'icône « Exclure ce poste des règles de filtrage ».



- 2) En renseignant directement l'adresse Mac du poste à exclure.



- 3) En lançant une découverte du réseau puis en sélectionnant le poste.



Exclure	IP	Adresse Mac	Nom Netbios
	172.29.0.254	00:0d:b9:27:c1:58	
	172.29.0.114	f4:6d:04:0a:e0:6c	GEORGES-PC

3.2.10.2.Exception de filtrage par adresse IP

Il existe deux manières de procéder soit en renseignant directement l'adresse IP du poste à exclure,

Adresses IP des postes exclus de la protection du boîtier

Adresses IP des postes exclus de la protection du boîtier

APPLIQUER

soit en utilisant l'outil de découverte du réseau qui liste les adresses IP des postes connectés à votre réseau :

Découverte des postes présent sur le réseau

Exclure	IP	Adresse Mac	Nom Netbios
	172.29.0.254	00:0d:b9:27:c1:58	
	172.29.0.114	f4:6d:04:0a:e0:6c	GEORGES-PC

ACTUALISER

Exceptions de filtrage par adresse IP

	Adresse IP
	172.29.0.117

3.2.10.3.Exclure un site du filtrage

Les exceptions de filtrage par adresse Mac ou par IP font référence à la source, l'exclusion d'un site fait référence à l'IP de destination

Il suffit de renseigner le nom du site ou son adresse IP et d'appliquer la règle.

Le site est immédiatement exclu et apparaît dans la liste des exceptions. Pour annuler l'exclusion de filtrage il suffit de supprimer l'adresse du site Internet de la liste en cliquant sur la croix .

Ajouter un site à la liste d'exception de filtrage

Adresse de site

AJOUTER

Liste des sites exclus du filtrage	
Sup	Sites exclus
	www.monerp.com

Remarque :

Si un nom de site est indiqué, la règle de firewall qui sera générée fera toujours référence à son adresse IP.

3.2.11. Filtrage des Smartphones

Le filtrage des smartphones s'active dans les profils de sécurité.

Action	Catégories	Heures Ouvrées	Heures NON Ouvrées	Heures Fermées
	Smartphones	☐	☐	☐
	Liste blanche	☒	☐	☐

Après activation, tous les smartphones sont bloqués par reconnaissance de leur « User Agent ». L'utilisateur est informé du blocage de sa demande de connexion.


FROGI-SECURE
 Contrôle et protection des accès Internet

INFORMATIONS

Veuillez renseigner le mot de passe de déblocage pour smartphones

Mot de passe de déblocage
 Nom
 Prénom

Frogi-Secure - 2016 - © Tous droits réservés

Vous pouvez débloquent un smartphone en indiquant le mot de passe de déblocage. Le smartphone débloquent est alors ajouté à la liste des smartphones autorisés.

Paramètres

Mot de passe de déblocage
 Confirmation

Liste des smartphones autorisés

	Smartphones	
✖	14:8f:c6:5a:dc:50	Franck Dupont

Il est possible de supprimer un smartphone de la liste des autorisations ou de supprimer tous les smartphones de la liste.

3.2.12. Liste des ports autorisés

Cette règle de filtrage s'active dans les profils de sécurité.

	Tunnels VPN	☐
	Filtrage par ports TCP UDP (port autorisés)	☒
	Tous les sites Web Internet (HTTP/HTTPS)	☐

Lorsque cette règle est activée, seuls les ports TCP 80 (HTTP) et TCP 443 (HTTPS) sont autorisés à ouvrir des sessions sur Internet.

Vous pouvez rajouter d'autres ports dans le sous-onglet « Exceptions de filtrage ».

Ajouter un port

Paramètres de port
Nature

TCP
Début
Fin

AJOUTER

Liste des ports autorisés

Sup	Protocole	Port début	Port fin
	tcp	5555	7777

3.2.13. Personnalisation des interfaces d'accueil

Lorsqu'une demande de connexion est refusée, une mire d'information est affichée (en mode HTTP et en mode HTTPS Proxy)

Vous pouvez personnaliser cette mire d'information.



Couleurs

Arrière plan 

Fond de l'encadré 

Bordure de l'encadré 

Police du texte d'annonce 

Police du texte dans l'encadré 

Logo Aucun fichier sélectionné.



Apparence mise à jour

 **FROGI-SECURE**
Contrôle et protection des accès Internet

ACCÈS NON AUTORISÉ

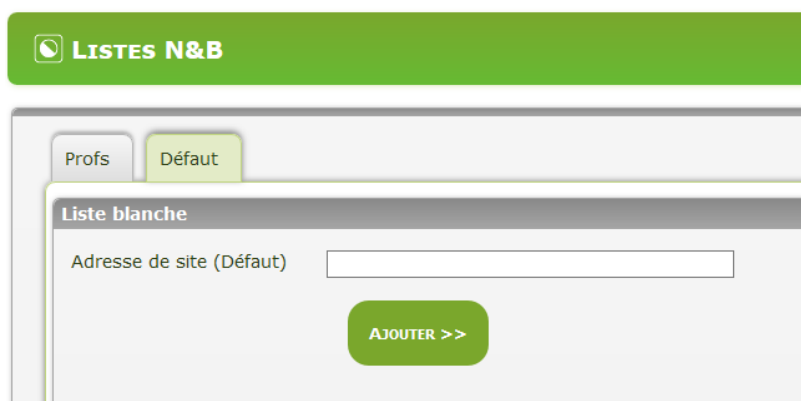
Postes	Adresse IP
URL	URL
Catégories	Catégories

Si vous pensez que c'est une erreur, contactez [l'administrateur](#)

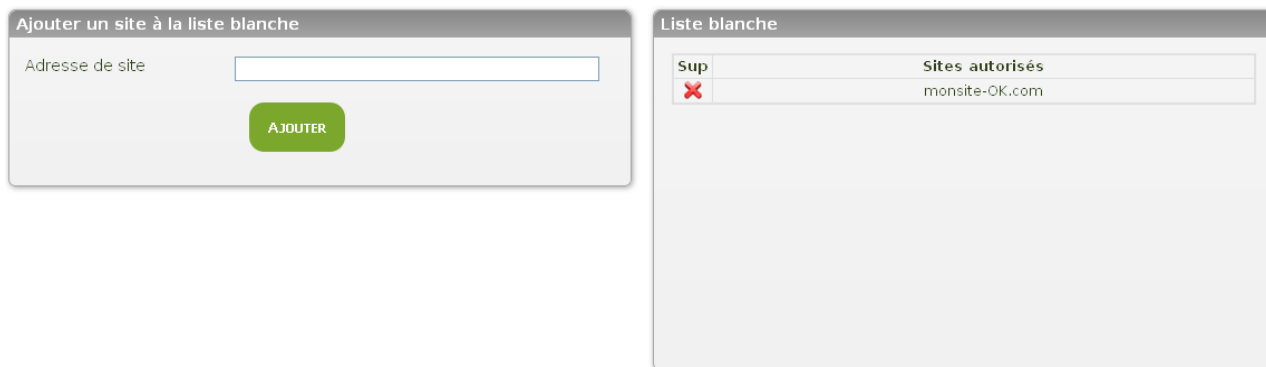
3.3. Listes N&B

3.3.1. Profils de sécurité

Chaque profil a ses propres listes blanche et noire.



1.1.1. Liste blanche



La liste blanche permet d'autoriser l'accès à des sites qui pourraient appartenir à l'une des catégories bloquées. La catégorie « Liste blanche » dans les règles de filtrage doit être sélectionnée pour que l'accès aux sites soit autorisé.

Il est également possible de mettre à jour la liste blanche à partir de l'onglet « Activité » ou depuis l'email d'information adressé à l'administrateur du site.

TOP 10 Sites bloqués					
Liste blanche	Exclure	Détails	Sites Web	Catégories	Hits
			meetit.fr	Sites de rencontres	1
			siteadult.com	Réservés aux adultes	1
			xxx.com	Réservés aux adultes	1

S'il y a plusieurs profils de sécurité, vous devez indiquer le profil auquel se rapporte la liste blanche.

1.1.2. Liste noire

Ajouter un site à la liste noire

Adresse de site

AJOUTER

Liste noire	
Sup	Sites bloqués
	monsie-NO-OK.com

La liste noire permet d'interdire l'accès à certains sites sans bloquer l'ensemble des sites de sa catégorie. La catégorie « Liste noire » dans les profils de sécurité doit être sélectionnée pour que l'accès aux sites soit interdit.

Il est également possible de mettre à jour la liste noire à partir de l'onglet « Activité ».

TOP 10 Sites accédés					
Liste noire	Exclure	Détails	Sites Web	Hits	
			frogi-secure.com	21	
			ssl.gstatic.com	17	
			shavar.services.mozilla.com	8	
			www.gstatic.com	6	
			ocsp.digicert.com	5	
			xml.alexa.com	5	
			dispatch.avira-update.com	4	
			personal.avira-update.com	4	
			admin.frogi-secure.com	3	
			aus5.mozilla.org	3	
			csi.gstatic.com	3	

3.4. Activité @

Le service de traçabilité Web est activé par défaut. Si vous souhaitez le désactiver ou crypter les traces, le paramétrage est disponible dans les options, onglets « fonctions avancées » puis « options ».

L'onglet « Activité » permet d'accéder à trois fonctionnalités :



Analyse : Fonctions d'analyse statistique et multicritère.

Rapport : Génération automatique de rapports statistiques.

Listes d'exclusion : Permet d'exclure certains sites des rapports statistiques.

3.4.1. Format des traces

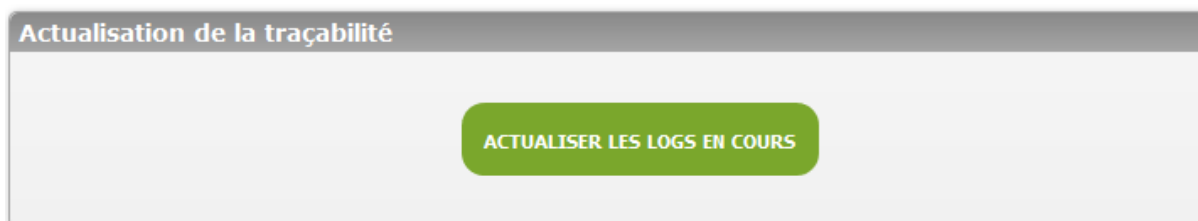
Les informations suivantes sont enregistrées dans la base de traçabilité :

- Date.
- Heure de début de la connexion.
- Heure de fin de la connexion.
- Durée de la connexion (champ calculé).
- Utilisateurs.
- Adresse du poste.
- Mac adresse du poste.
- Nom du site.
- Protocole.
- Port.
- Volume échangé (champ calculé).

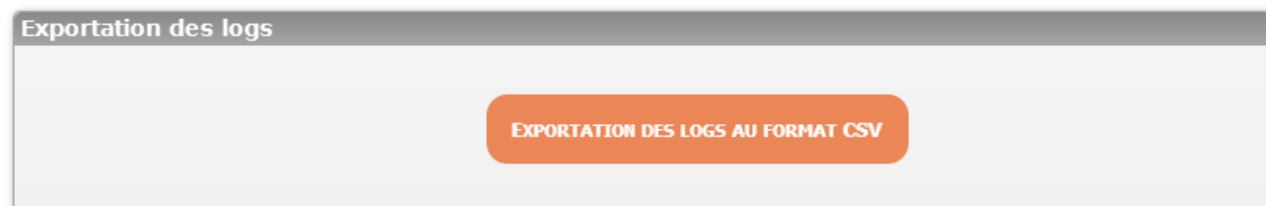
Dans un premier temps, les logs générés par Squid sont enregistrés dans un File System Memory. Toutes les 15 minutes, les logs de Squid sont analysés. Seul le nom du site est enregistré et non la totalité de l'Url, ceci afin de limiter le volume de la base de traçabilité et de répondre aux contraintes de non-profilage du R.G.P.D.

3.4.2. Actualiser les logs

Vous pouvez à tout moment demander à analyser les logs pour mettre à jour la base de traçabilité, sans attendre le déclenchement du processus automatique.



3.4.3. Exportation des logs de traçabilité au format CSV



La globalité de la traçabilité est exportable au format CSV.

3.4.4. Analyse statistique (Top N)



L'analyse statistique s'effectue à partir du bouton **Top N** et s'appuie sur quatre types de critères :

Trié par : L'analyse se fait sur le critère du nombre de visites, du volume échangé ou du temps passé.

Regroupé par : Les données sont regroupées par sites, web, utilisateurs ou postes.

Période d'analyse : Permet de définir la période d'analyse.

Top N : Nombre de lignes affichées.

Remarque :

L'« **utilisateur** » peut-être, soit le nom de connexion si l'authentification est activée, soit le nom du poste pour les PC sous Windows (il faut autoriser la recherche réseau dans le firewall Windows), soit l'adresse IP du poste.

Le « **poste** » (critère de regroupement) correspond à l'adresse Mac de la station.

3.4.5. Exportation des résultats statistiques en fichier CSV

La recherche, une fois effectuée, est téléchargeable au format CSV par le bouton « Télécharger le fichier CSV » apparaissant sous le bouton recherche.

3.4.6. Analyse statistique - Résultats

TOP 10 Sites accédés					
Liste noire	Exclure	Détails	Sites Web		Hits
			frogi-secure.com		21
			ssl.gstatic.com		18
			shavar.services.mozilla.com		8
			www.gstatic.com		6
			ocsp.digicert.com		5
			xml.alexa.com		5
			dispatch.avira-update.com		4
			personal.avira-update.com		4
			admin.frogi-secure.com		3
			aus5.mozilla.org		3
			csi.gstatic.com		3

Détails shavar.services.mozilla.com par Utilisateurs			
Utilisateurs			Hits
GEORGES-PC			8

TOP 10 Sites bloqués					
Liste blanche	Exclure	Détails	Sites Web	Catégories	Hits
			meetit.fr	Sites de rencontres	1
			dating.com	Réservés aux adultes	1
			xxx.com	Réservés aux adultes	1

Détails shavar.services.mozilla.com par Utilisateurs			
Utilisateurs	IP	Catégories	Hits



Ajoute directement le site dans la liste blanche ou la liste noire



Supprimer un site de l'analyse statistique (voir chapitre 3.4.6).



Permet une analyse en profondeur qui s'affichera sur la partie droite

3.4.7. Analyse multicritère – Recherche Avancée

Top WEB | **Avancée**

Période

Date début

Date fin

Heure de début -- h -- min

Heure de fin -- h -- min

Critère(s) de recherche

Nom du site

Adresse IP source

Adresse destination

Adresse MAC

Utilisateurs

Protocole

Port

RECHERCHER

TÉLÉCHARGER LE FICHIER CSV

L'analyse multicritère s'effectue à partir du bouton "Avancée" :

3.4.8. Exportations des résultats avancés au format CSV

La recherche une fois effectuée est téléchargeable au format CSV par le bouton « Télécharger le fichier CSV » apparaissant sous le bouton recherche.

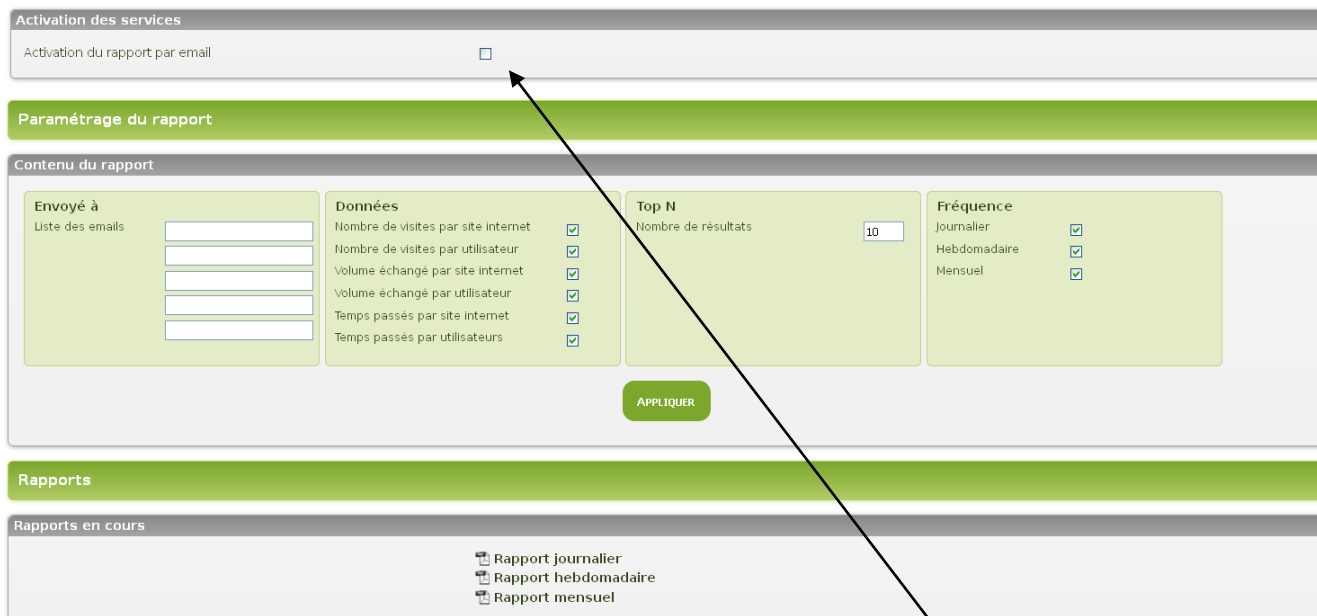
3.4.9. Analyse multicritère – Résultats

Les résultats se présentent sous un tableau détaillant toutes les informations répondant aux critères de recherche demandés.

Sites accédés											
Date	Début	Fin	Temps (h)	Utilisateurs	IP	Postes	URL	Protocole	Port	Taille	
03/11/2016	17:13	17:13	00:00:00	GEORGES-PC	172.29.0.114	f4:6d:04:0a:e0:6c	mail.google.com	tcp	80	0.01 Ko	
03/11/2016	17:08	17:08	00:00:00	GEORGES-PC	172.29.0.114	f4:6d:04:0a:e0:6c	mail.google.com	tcp	80	0.01 Ko	
03/11/2016	17:05	17:05	00:00:00	GEORGES-PC	172.29.0.114	f4:6d:04:0a:e0:6c	play.google.com	tcp	80	0.01 Ko	
03/11/2016	17:04	17:04	00:00:00	GEORGES-PC	172.29.0.114	f4:6d:04:0a:e0:6c	www.googleapis.com	tcp	80	0.01 Ko	
03/11/2016	17:03	17:03	00:00:00	GEORGES-PC	172.29.0.114	f4:6d:04:0a:e0:6c	clients6.google.com	tcp	80	0.01 Ko	
03/11/2016	17:03	17:03	00:00:00	GEORGES-PC	172.29.0.114	f4:6d:04:0a:e0:6c	clients1.google.com	tcp	80	0.86 Ko	
03/11/2016	17:03	17:03	00:00:00	GEORGES-PC	172.29.0.114	f4:6d:04:0a:e0:6c	mail.google.com	tcp	80	0.01 Ko	
03/11/2016	16:59	16:59	00:00:00	GEORGES-PC	172.29.0.114	f4:6d:04:0a:e0:6c	play.google.com	tcp	80	0.01 Ko	
03/11/2016	16:58	16:58	00:00:00	GEORGES-PC	172.29.0.114	f4:6d:04:0a:e0:6c	www.googleadservices.com	tcp	80	0.01 Ko	
03/11/2016	16:58	16:58	00:00:00	GEORGES-PC	172.29.0.114	f4:6d:04:0a:e0:6c	mail.google.com	tcp	80	0.01 Ko	
03/11/2016	16:56	16:56	00:00:00	GEORGES-PC	172.29.0.114	f4:6d:04:0a:e0:6c	play.google.com	tcp	80	0.01 Ko	
03/11/2016	16:56	16:56	00:00:00	GEORGES-PC	172.29.0.114	f4:6d:04:0a:e0:6c	clients1.google.com	tcp	80	1.71 Ko	
											714 résultat(s)

Sites bloqués						
Heure	IP	Postes	Utilisateurs	URL	Catégories	
03/11/2016 16:47:38	172.29.0.114	f4:6d:04:0a:e0:6c	GEORGES-PC	xxx.com	Réservés aux adultes	
03/11/2016 16:47:27	172.29.0.114	f4:6d:04:0a:e0:6c	GEORGES-PC	adult.com	Réservés aux adultes	
03/11/2016 16:47:14	172.29.0.114	f4:6d:04:0a:e0:6c	GEORGES-PC	meetic.fr	Sites de rencontres	
02/11/2016 17:11:55	172.29.0.114	f4:6d:04:0a:e0:6c	GEORGES-PC	dpm.zebestof.com	Sites contenant des virus (hacking malware phishing)	
02/11/2016 17:11:52	172.29.0.114	f4:6d:04:0a:e0:6c	GEORGES-PC	dpm.zebestof.com	Sites contenant des virus (hacking malware phishing)	
						5 résultat(s)

3.4.10. Rapports d'activité



Activation des services

Activation du rapport par email ☐

Paramétrage du rapport

Contenu du rapport

Envoyé à
Liste des emails

Données

- Nombre de visites par site internet ☒
- Nombre de visites par utilisateur ☒
- Volume échangé par site internet ☒
- Volume échangé par utilisateur ☒
- Temps passés par site internet ☒
- Temps passés par utilisateurs ☒

Top N
Nombre de résultats

Fréquence

- Journalier ☒
- Hebdomadaire ☒
- Mensuel ☒

APPLIQUER

Rapports

Rapports en cours

-  Rapport journalier
-  Rapport hebdomadaire
-  Rapport mensuel

Un menu permet d'indiquer les emails des utilisateurs qui recevront les rapports d'activité ou de télécharger directement ces rapports s'ils existent.

L'envoi d'email ne se fera que si la case « Activation du rapport par email » est validée.

Remarque :

Les boîtiers Frogi Secure utilisent leur propre serveur de messagerie (SMTP) situé dans notre Data Center, vous n'avez donc pas à indiquer les paramètres de votre serveur SMTP ou celui de votre F.A.I.

3.4.11. Liste d'exclusion des résultats

Cette fonction permet d'exclure des rapports d'activité des sites Internet afin de rendre plus pertinentes les informations statistiques.

Ajouter un site à la liste d'exclusion

Adresse de site

AJOUTER

Liste d'exclusion

Sup	Sites exclus des résultats de recherches statistiques
✖	google
✖	doubleclick.net
✖	microsoft

Important :

- 1) Les sites Internet sont exclus uniquement des résultats de l'analyse statistique. Ils sont toujours listés dans la recherche avancée ou multicritère.
- 2) Les règles de filtrage ne prennent pas en compte la liste d'exclusion. Cette liste est uniquement un confort de lisibilité dans les recherches simples statistiques.

3.5. Plages horaires

L'onglet de gestion des plages horaires est composé de trois parties :

1. Plages horaires en cours d'utilisation.
2. Modification.
3. Appliqué à.

Plages horaires en cours d'utilisation

Tranches horaires	0	1	1/2	2	1/2	3	1/2	4	1/2	5	1/2	6	1/2	7	1/2	8	1/2	9	10	11	1/2	12	1/2	13	1/2	14	1/2	15	1/2	16	1/2	17	1/2	18	1/2	19	20	1/2	21	1/2	22	1/2	23	1/2
Lundi																																												
Mardi																																												
Mercredi																																												
Jeudi																																												
Vendredi																																												
Samedi																																												
Dimanche																																												

Modification de la plage horaire

Modification

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
Heures ouvrées (0-30 min)	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Heures ouvrées (30-60 min)	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Heures NON ouvrées (0-30 min)	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Heures NON ouvrées (30-60 min)	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Heures fermées (0-30 min)	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Heures fermées (30-60 min)	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

Appliquer à

LUNDI

MARDI

MERCREDI

JEUDI

VENDREDI

SAMEDI

DIMANCHE

Pour modifier une plage horaire, procédez comme suit :

- 1) Dans la fenêtre « Modification », indiquez les 1/2 heures ouvrées, non-ouvrées et fermées.
- 2) Dans la fenêtre « Appliquer à », indiquez le jour de la semaine sur lequel la plage horaire sera appliquée.

Vous pouvez également à partir de la fenêtre « Plages horaires en cours d'utilisation » sélectionner une journée pour la faire apparaître dans la fenêtre « Modification » et ensuite l'appliquer à une autre journée.

3.6. Authentification

3.6.1. Activation

Activation des services	
Authentifications transparentes	
Authentification par ip	☐
Active Directory (AD)	☐
Authentifications de type utilisateur - mot de passe	
Base de comptes interne	☐
Ldap externe	☐
Authentification serveur CAS	☐
Portail SMS	☐
Portail Email	☐
Portail utilisateur	☐
Page d'accueil	☐
Aucune authentification	☒
Options	
Forcer le changement de mot de passe utilisateur à la première utilisation des comptes	☐
Autorise le multi login	☐
Authentification permanente	☐

3.6.2. Types d'authentification

Il existe plusieurs types d'authentification :

- Authentification par IP.
Associe à des @IP ou à des plages @IP un profil de sécurité
- Authentification Active Directory en mode S.S.O.
Associe à un utilisateur de l'A.D. un profil de sécurité Frogi Secure.
- Base de compte interne.
Contient les noms d'utilisateurs et les mots de passe d'authentification.
- Ldap externe
Il s'agit soit du schéma Ldap d'une Active Directory, soit d'un annuaire de type Open Ldap.
- Authentification C.A.S. (Central Authentication Service).
Associe à un utilisateur CAS/ENT un profil de sécurité.
- Portail SMS.

L'utilisateur indique son numéro de téléphone portable ainsi que son nom et prénom, il recevra en retour par SMS le mot de passe associé (le nom de l'utilisateur étant le numéro de téléphone).

- Portail utilisateur

L'utilisateur crée son propre compte.

- Portail Email

L'utilisateur indique son adresse email, il recevra en retour le mot de passe (l'adresse email étant le nom de l'utilisateur).

- Page d'accueil

A sa première connexion à Internet, l'utilisateur devra valider la page d'accueil pour pouvoir poursuivre sa navigation. Cette fonctionnalité permet de se conformer au R.G.P.D.

Les deux premières méthodes d'authentification (par IP et AD/SSO) sont dites transparentes car elles ne nécessitent pas de redirection vers un portail d'authentification.

3.6.3. Options

- Forcer le changement de mot de passe à la première connexion

Cette option permet d'assurer la confidentialité du mot de passe d'authentification. Une fois le mot de passe changé, l'utilisateur est le seul à en avoir connaissance. L'administrateur du boîtier a la possibilité de changer un mot de passe, mais il n'a pas la possibilité de le visualiser.

- Autorise le multi-login

Autorise plusieurs connexions avec le même compte utilisateur.

- Authentification permanente

Si cette option n'est pas activée, l'authentification sera temporaire. Les méthodes de déconnexion automatique sont décrites dans la suite de ce document.

3.6.4. Hiérarchie des authentifications

Les authentifications transparentes et par nom/mot de passe peuvent être utilisées simultanément.

Les règles suivantes s'appliquent :

- 1) Si l'IP du poste de l'utilisateur appartient à un groupe IP, le profil du groupe IP sera utilisé et il n'y aura pas d'authentification de type utilisateur.
- 2) Si l'authentification AD/SSO est utilisée, l'utilisateur qui ne s'est pas authentifié dans le domaine AD sera (si une des authentifications nom/mot de passe est activée) redirigé vers le portail d'authentification.
- 3) En mode Ldap externe, l'authentification avec la base interne sera effectuée en premier. Si l'authentification échoue, on utilisera ensuite la base Ldap.

3.6.5. Paramétrage de l'authentification par IP

Ce mode d'authentification est basé sur l'architecture IP du réseau. Il est possible de créer des groupes d'adresses IP et de leur affecter un profil de filtrage.

3.6.6. Paramétrage de l'authentification par Active Directory

Le connecteur AD permet de mettre en oeuvre une authentification de type S.S.O (Single Sign On).

Lorsqu' un utilisateur s'authentifie dans un domaine Active Directory, le connecteur transmettra au boîtier une commande d'authentification en indiquant le nom de l'utilisateur, son IP et le profil de sécurité associé.

Le téléchargement de la procédure d'installation est disponible dès que l'option d'authentification par AD est activée. Le fichier compressé téléchargé comprend la procédure d'installation illustrée sur le serveur AD ainsi que les fichiers sources nécessaires au fonctionnement.



Vous trouverez en annexe de ce document le descriptif complet pour l'installation et le paramétrage du connecteur AD/SSO.

3.6.7. Paramétrage de l'authentification du portail utilisateur



The screenshot shows the 'AUTHENTIFICATION' (Authentication) page of the FROGI-SECURE portal. At the top is the logo and the text 'Contrôle et protection des accès Internet'. Below this, the title 'AUTHENTIFICATION' is centered in red. There are two input fields: 'utilisateur:' and 'mot de passe:'. A green 'CONNEXION' button is positioned below the password field. At the bottom, there are two links: 'Ouvrir un compte' and 'Mot de passe oublié'.

A l'ouverture du portail d'authentification, cliquez sur « Ouvrir un compte »



The screenshot shows the 'OUVERTURE DE COMPTE' (Account Creation) page of the FROGI-SECURE portal. At the top is the logo and the text 'Contrôle et protection des accès Internet'. Below this, the title 'OUVERTURE DE COMPTE' is centered in red. There are six input fields: 'Email*', 'Nom*', 'Prénom*', 'Téléphone', 'Mot de passe*', and 'Confirmation *'. Below these fields are two sections: 'Conditions générales d'utilisation' and 'Charte Informatique'. At the bottom, there is a checkbox labeled 'J'ai lu et j'accepte les Conditions Générales d'utilisation énoncées ci-dessus' and a link 'Retour au portail d'authentification'.

Renseigner le formulaire.

3.6.8. Paramétrage de l'authentification par page d'accueil

La page d'accueil est soit intégrée au boîtier, soit externe.



La liste des utilisations ayant validés la page d'accueil est réinitialisée chaque nuit durant les processus de maintenance.



3.6.9. Portails SMS

Lorsqu'un portail est activé, la mire de signature permet d'accéder au portail.



Le portail SMS est un service de distribution de comptes via SMS. Particulièrement adapté pour les sites accueillant du public. Un utilisateur se connectant au réseau Internet est redirigé sur une demande de création de compte ou il renseigne son numéro de téléphone portable, nom et prénom. Après validation, il reçoit un SMS l'informant de son identifiant et mot de passe. Une période d'essai comportant 5 SMS permet d'essayer le service.



Il est possible de désactiver cette période d'essai et de configurer un compte SMS directement.

Paramètres du portail SMS

Nombres de SMS utilisés

0 / 5

Mettre fin à la période d'essai ?

✗

Plateforme SMS

ovh.com ▾

Compte (account)

En essai

Identifiant

En essai

Mot de passe

●●●●●●●●

Expéditeur (from)

●●●●●●●●

Les boîtiers Frogi Secure utilisent soit le service www.lesms.com, soit le service www.ovhtelecom.fr/sms/ pour l'envoi de sms.

Vous trouverez en annexe les procédures de création de compte pour ces deux plateformes.

3.6.10. Portail EMAIL

Le portail EMAIL est un service de distribution de comptes via email. Particulièrement adapté pour les sites accueillant du public. Un utilisateur se connectant au réseau Internet est redirigé sur une demande de création de compte ou il renseigne son email, nom et prénom. Après validation, il reçoit un email l'informant de son identifiant et mot de passe. Son identifiant sera l'adresse email précédemment renseignée et le mot de passe est généré automatiquement.

 **FROGI-SECURE**
Contrôle et protection des accès Internet

CODE D'ACCÈS

Veuillez remplir le formulaire de demande ci-dessous.
Vos code d'accès vous seront envoyés par email.

Email

Nom

Prénom

ENVOYER

[Retour au portail d'authentification](#)

Les utilisateurs ayant oublié leur mot de passe peuvent en demander un nouveau automatiquement en renseignant le mot de passe associé à leur compte utilisateur.

 **FROGI-SECURE**
Contrôle et protection des accès Internet

MOT DE PASSE OUBLIÉ

Saisissez l'adresse mail associée à votre compte utilisateur

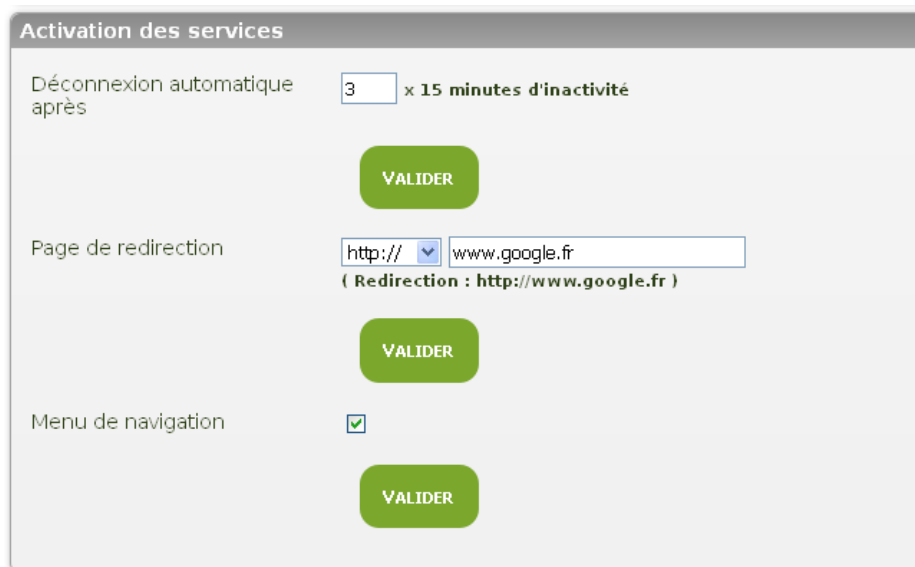
email

VALIDER

[Retour au portail d'authentification](#)

3.6.11. Paramétrage de l'authentification temporaire

Il existe trois paramétrages spécifiques :



The screenshot shows a configuration window titled "Activation des services". It contains three sections, each with a "VALIDER" button:

- Déconnexion automatique après**: A text input field containing "3" followed by "x 15 minutes d'inactivité".
- Page de redirection**: A dropdown menu showing "http://" and a text input field containing "www.google.fr". Below this, it says "(Redirection : http://www.google.fr)".
- Menu de navigation**: A checkbox that is checked.

Déconnexion automatique

Les utilisateurs seront automatiquement déconnectés après x fois 15 minutes d'inactivité Internet (ici dans l'exemple 45 min).

Page de redirection

Après connexion, les utilisateurs sont redirigés sur une page d'accueil qui est paramétrable dans l'interface d'administration dès que l'authentification temporaire ou permanente est activée.

Menu de navigation



La fermeture de cette page déclenchera une déconnexion automatique

-  mon compte
-  Accéder à Internet
-  Déconnexion

Si le service est activé, après connexion l'utilisateur dispose d'un menu de navigation.

L'utilisateur peut se connecter à Internet, envoyer un message à l'administrateur (si un email est paramétré en console d'administration) et a accès à ses paramètres de compte. Un dernier bouton lui permet de se déconnecter. La fermeture de ce menu déclenche une déconnexion automatique après quelques secondes.

Déconnexion manuelle

Les utilisateurs ont également la possibilité de se déconnecter à tout moment en se connectant à :

<http://logout.frogi-secure.com>



3.6.12. Déclenchement du portail captif

Mode HTTPS SNI (profil défaut)

Si la page d'accueil du navigateur est en HTTP, la page du portail captif s'affichera automatiquement.

Si la page d'accueil est en HTTPS (ou forcé en HTTPS par Chrome par exemple). Le portail captif ne pourra pas s'afficher car le mode SNI ne gère pas les redirections HTTPS.

Pour détecter un portail captif, les OS et les navigateurs lancent une requête HTTP vers un pseudo portail. Suivant les équipements, cela se fait à différents niveaux.

Firefox	A l'ouverture de la session, si aucune session Firefox n'est ouverte	detectportal.firefox.com
Windows	A l'ouverture de la connexion réseau	www.msftncsi.com www.msftconnecttest.com
Apple	A l'ouverture de la connexion réseau	captive.apple.com
Android	A l'ouverture de la connexion réseau	connectivitycheck.gstatic.com

Les équipements se connectant en Wifi lancent systématiquement la requête HTTP lorsqu'ils se connectent à la borne Wifi.

Si pour différentes raisons une requête HTTP n'est pas lancée, on peut indiquer

<http://google.frogi-secure.com> comme page d'accueil.

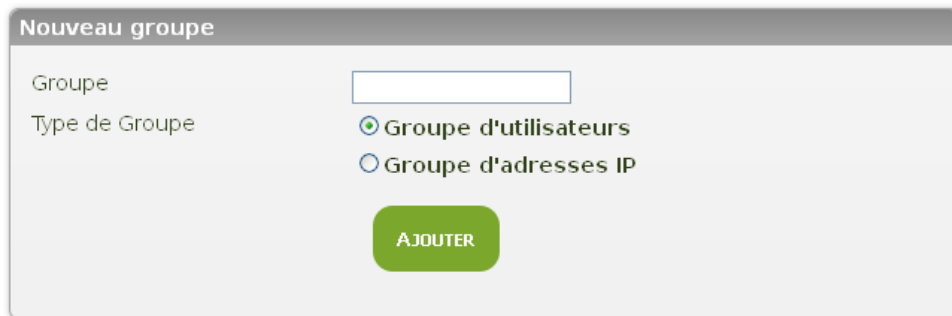
Mode Proxy HTTPS (profil défaut)

Si le certificat est installé sur le poste, toute requête HTTP ou HTTPS ouvrira le portail captif.

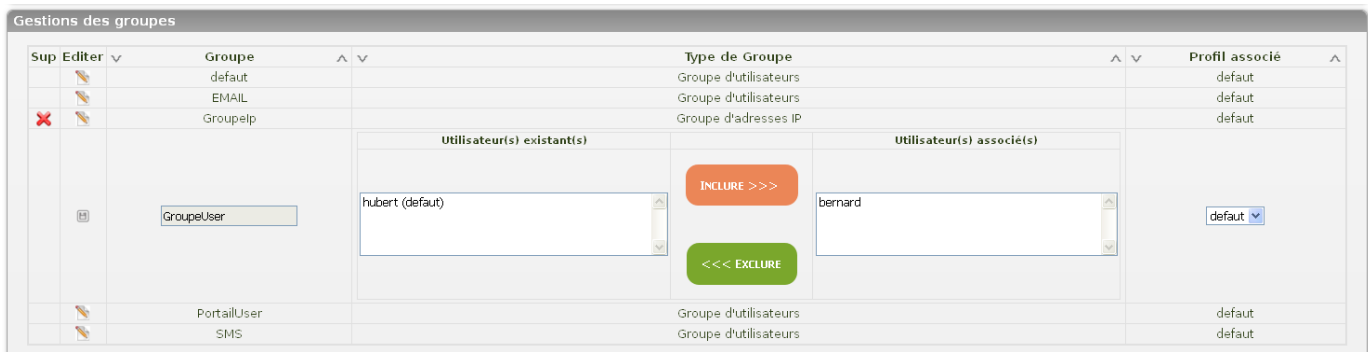
3.6.13. Gestion des groupes et des utilisateurs

3.6.13.1. Gestion des groupes

Il existe deux sortes de groupes :

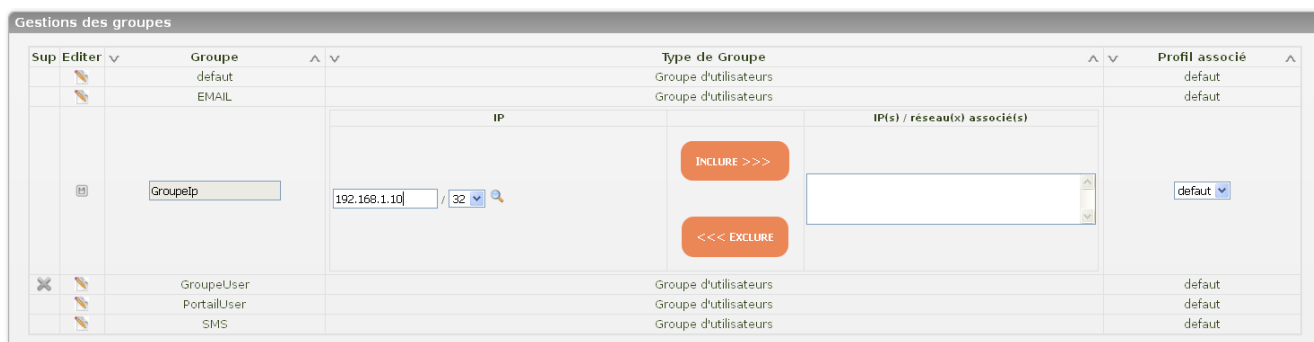


- Les groupes d'utilisateurs regroupent des utilisateurs utilisant le même profil de sécurité. Ils possèdent un login et un mot de passe pour accéder à Internet et sont transférables d'un groupe à l'autre via une interface de transfert.



- Les groupes IP sont des groupes réseaux regroupant un ensemble d'adresses IP (exemple 192.168.0.10, 192.168.0.12, 192.168.0.15) ou une plage d'adresse IP (exemple : 192.168.0.0). Les groupes IP ne sont pas captifs du portail d'authentification. Ils sont paramétrables dans la liste des groupes. Pour ajouter une adresse IP à un groupe il faut renseigner l'adresse IP et son masque réseaux au format CIDR (un tableau est disponible en survolant la loupe à côté du choix du masque réseau).

Remarque : Veillez à bien gérer les masques réseau afin d'éviter les recouvrements de profils.



Les groupes peuvent être liés à un profil de filtrage.

Gestions des groupes				
Sup	Editer	Groupe	Type de Groupe	Profil associé
		default	Groupe d'utilisateurs	default
		EMAIL	Groupe d'utilisateurs	default
		Groupelp	Groupe d'adresses IP	default
		GroupeUser	Groupe d'utilisateurs	default
		PortailUser	Groupe d'utilisateurs	default
		SMS	Groupe d'utilisateurs	default

Chaque groupe peut être supprimé en cliquant sur la croix .

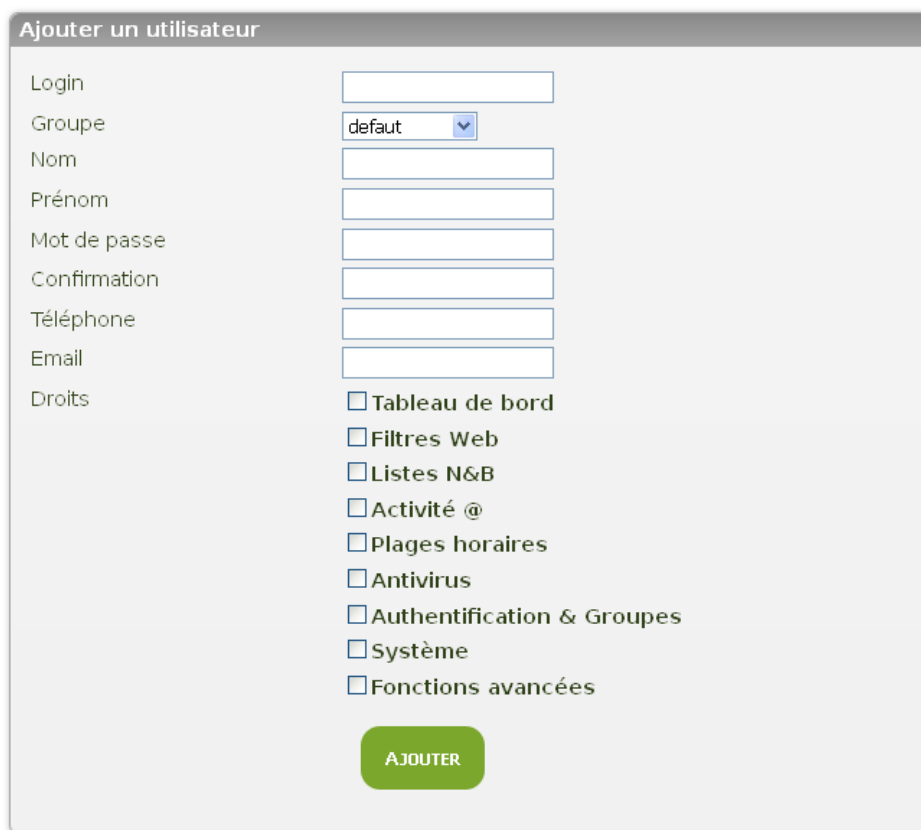
Seul un groupe ne comportant aucun utilisateur peut être supprimé. La croix grisée  signale les groupes comportant des utilisateurs qui ne peuvent pas être supprimés.

3.6.13.2. Gestion des utilisateurs

La création de groupes et de comptes utilisateurs n'est nécessaire que si vous activez la fonction d'authentification.

Pour ajouter un utilisateur, vous avez deux possibilités :

- **Création manuelle**



Ajouter un utilisateur

Login

Groupe

Nom

Prénom

Mot de passe

Confirmation

Téléphone

Email

Droits

- ☐ Tableau de bord
- ☐ Filtres Web
- ☐ Listes N&B
- ☐ Activité @
- ☐ Plages horaires
- ☐ Antivirus
- ☐ Authentification & Groupes
- ☐ Système
- ☐ Fonctions avancées

AJOUTER

Renseignez les coordonnées de l'utilisateur en le rattachant à un groupe puis cliquez sur "Valider". Le nom de l'utilisateur vient s'ajouter à la liste.

Il est possible de déclarer des droits d'administration sur des utilisateurs en limitant l'accès à des fonctionnalités spécifiques.

- **Création à partir d'une liste**

Vous avez la possibilité de charger une liste d'utilisateurs au format suivant «**login ;nom ;prénom ;groupe ;motdepasse ;téléphone ;email**» en comptant un utilisateur par ligne. Les caractères spéciaux ne sont pas autorisés. Le fichier peut être de format texte ou csv.

Importer une liste d'utilisateurs

Importer la liste

Parcourir...

Aucun fichier sélectionné.

AJOUTER

La liste des utilisateurs est visible dans un tableau récapitulant les différentes informations d'appartenance aux groupes et profil de filtrage. Il signale le statut du compte utilisateur et de son état.

Gestion des utilisateurs															
Sup	Editer	Online	Login	Mot de passe	Profil	Groupe	Droits	Nom	Prénom	Téléphone	Email	Date de création	Dernière utilisation	Quota sms	Etat
			bernard		default	GroupeUser	Non	dupont	Bernard		b.dupont@domaine.fr	2016-11-04 16:56:36	2016-11-04 16:56:36	0 / 3	
			hubert		default	default	Non	Smith	Hubert		h.smith@domaine.fr	2016-11-04 16:57:23	2016-11-04 16:57:23	0 / 3	

Pour supprimer un utilisateur cliquez sur. 

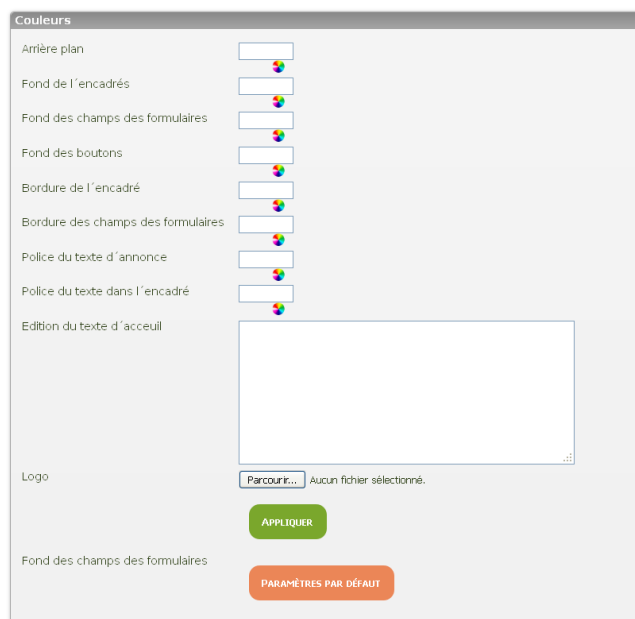
Les comptes utilisateurs comportent trois états :

-  Si l'option de forçage du changement de mot de passe à la première connexion est activée, le compte n'a pas été encore utilisé et est en attente de changement de mot de passe.
-  Le compte utilisateur est opérationnel
-  Le compte utilisateur est bloqué. L'utilisateur à la connexion sera informé du blocage et ne pourra pas accéder à Internet.

 Il est possible de renouveler un mot de passe utilisateur. Celui-ci lui sera envoyé par email et dans le cas du portail SMS activé également par SMS.

3.7. Personnalisation de la page d'accueil du portail d'authentification.

Vous pouvez personnaliser la page d'accueil du portail d'authentification en important un logo et une charte couleur. Le texte d'information est également éditable.




3.8. Administrateurs secondaires

L'administrateur « admin » a accès en lecture/écriture à tous les paramètres du boîtier.

Vous pouvez créer des administrateurs secondaires ayant une visibilité et des possibilités de modifications limités sur l'administration du boîtier.

La création d'un administrateur secondaire se fait dans l'onglet « Authentification ».

Gestion des utilisateurs

Ajouter un utilisateur

Login	profs
Groupe	default
Nom	Frogi
Prénom	Secure
Mot de passe	••••••••
Confirmation	••••••••
Téléphone	0290262124
Email	contact@frogi-secure.co
Droits	☒ Tableau de bord ☒ Profils de sécurité ☒ Listes N&B ☒ Activité @ ☒ Plages horaires ☐ Antivirus ☐ Authentification & Groupes ☐ Système ☐ Fonctions avancées

AJOUTER

Vous pouvez créer un administrateur secondaire sans activer l'authentification. L'accès à l'interface d'administration se fait comme pour l'administrateur « admin » du boîtier.

3.9. Système

3.9.1. Nom du boîtier



Le nom du boîtier est un commentaire qui permet de différencier les équipements autrement que par leur numéro de série.

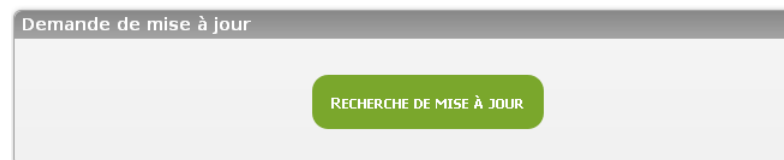
3.9.2. Configuration



Nom du boîtier	
Date de fin de garantie	Lundi 4 Novembre 2019
Numéro de série	R20-APU2-415B0E
Système	V5R2
TBI	2
Patch	161102_0
Date de mise à jour système	Mercredi 2 Novembre 2016 11:17

Ce panneau indique différentes caractéristiques du système.

3.9.3. Mises à jour



Le boîtier effectue quotidiennement la mise à jour de ses bases de données et vérifie si des mises à jour logicielles sont disponibles.

A la demande du support technique de Frogi Secure vous pouvez effectuer une mise à jour sans attendre le processus automatique.

3.9.4. Gestion du boîtier



Permet d'arrêter ou de redémarrer le boîtier. Si vous devez le déplacer, il est recommandé d'utiliser la procédure d'arrêt à partir de l'interface d'administration avant de déconnecter électriquement le matériel.

3.9.5. Changement du mot de passe de l'administrateur



Le mot de passe par défaut propre à chaque boîtier est indiqué sur l'étiquette après le numéro de série au dos des produits et dans la notice d'installation rapide fournie.

Il est possible via le bouton « par défaut » de réinitialiser le mot de passe administrateur à sa valeur par défaut.

Pour des raisons de sécurité, nous vous conseillons vivement de changer le mot de passe par défaut.

3.9.6. Changement de l'email administrateur



L'email de l'administrateur peut être utilisé par les utilisateurs lorsqu'ils demandent l'accès à un site qui n'est pas autorisé ou quand l'authentification est activée via le menu de navigation utilisateur.



En cliquant sur la zone « l'administrateur » un email formaté est envoyé à l'administrateur pour l'informer que l'accès au site n'est pas autorisé.

3.9.7. Sauvegarde / Restauration

3.9.7.1. Sauvegarde automatique de la base de données système

Activer le service

Sauvegarde automatique de la base de traçabilité ☒

VALIDER

Paramètres serveur FTP

Hostname	ftp.test.fr
Utilisateur	test
Mot de passe	csv
Chemin	/test_save_db/

Paramètres serveur FTP

Hostname	ftp.test.fr
Utilisateur	test
Mot de passe	
Chemin	/test_save_db/
Format de sauvegarde	csv

VALIDER

Vous pouvez sauvegarder la base de données de l'activité Internet sur un serveur FTP en renseignant les paramètres de connexion. La sauvegarde est journalière, le nom du fichier est constitué du numéro de série suivi de la date de sauvegarde (RX0_NumSerie_jj_mm_aaaa.zip).

Deux formats sont disponibles : csv et format Frogi-Secure. Chacun est compressé au format Zip.

Remarque :

Le format Frogi-Secure permet de recharger le fichier dans un boîtier et d'utiliser les outils d'analyse.

3.9.7.2.Sauvegarde / restauration manuelle de configuration système

Sauvegarder la configuration en cours	Restaurer la configuration
SAUVEGARDE DE LA CONFIGURATION	Fichier de configuration à restaurer Parcourir... Aucun fichier sélectionné. RESTAURATION DE LA CONFIGURATION

La sauvegarde de la configuration concerne l'ensemble des paramètres du boîtier à l'exception de la base de données de traçabilité.

Une sauvegarde automatique de la configuration est incluse dans le processus des mises à jour quotidien. Cette sauvegarde sera automatiquement restaurée lors de la première utilisation d'un produit de remplacement (fourni dans le cadre de la garantie en cas de dysfonctionnement d'un produit).

3.9.7.3.Sauvegarde / restauration manuelle de la base de données système

Sauvegarder la base de données	Restaurer la base de données
SAUVEGARDE DE LA BASE DE DONNÉES	Base de données à restaurer: Parcourir... Aucun fichier sélectionné. RESTAURATION DE LA BASE DE DONNÉES ?

Permet la sauvegarde et la restauration de la base de données.

3.10. Fonctions avancées

3.10.1. Mode Bridge et Routeur

Les boîtiers Frogi Secure peuvent fonctionner soit en mode transparent (Bridge) soit en mode Routeur.

Choix du mode de fonctionnement

Choix du mode de fonctionnement

☒ Transparent
 ☐ Routeur

En mode Transparent ou Bridge le réseau principal et le point d'accès Internet sont dans la même plage IP. Le boîtier s'alloue une @ip via un service DHCP présent sur le réseau ou utilise une @ip fixe.

En mode routeur le réseau principal et le point d'accès Internet sont sur des plages d'adresses IP différentes.

3.10.1.1. Mode Bridge

Paramètres du mode BRIDGE

@IP-DHCP (Interfaces banalisées) ☒

@IP-Fixe (WAN sur Int 1, LAN sur Int 2)

Masque

Passerelle

Paramètres du mode BRIDGE

@IP-DHCP (Interfaces banalisées) **activé**

@IP-Fixe (WAN sur Int 1, LAN sur Int 2) //

APPLIQUER

@IP-DHCP : C'est le mode par défaut, le boîtier est alors entièrement Plug&Play. A la mise sous tension le boîtier détecte les ports Lan et Wan, la disposition des branchements n'a aucune importance. Dans ce mode il est nécessaire de disposer d'un service DHCP sur le réseau.

@IP-fixe : Vous avez la possibilité d'indiquer une @ip fixe pour le boîtier. Dans ce cas le réseau WAN/Internet doit être connecté sur l'interface réseau Int 1 et le réseau LAN/utilisateur sur l'interface Int 2.



Procédure de configuration :

Branchez directement le boîtier sur un poste et mettez-le sous tension, après quelques minutes de démarrage le boîtier s'assigne une ip fixe (192.0.2.1). Connectez-vous via votre navigateur Internet au boîtier en renseignant l'adresse suivante <http://192.0.2.1/login.php>. Vous avez alors accès à l'interface d'administration. Rendez-vous dans les fonctions avancées à l'onglet Bridge / routeur et assignez une adresse IP et le masque de votre réseau, ainsi que la passerelle de sortie sur Internet.

Paramètres du mode BRIDGE	
@IP-DHCP (Interfaces banalisées)	☐
@IP-Fixe (WAN sur Int 1, LAN sur Int 2)	172.29.0.133
Masque	255.255.0.0
Passerelle	172.29.0.254

Paramètres du mode BRIDGE	
@IP-DHCP (Interfaces banalisées)	désactivé
@IP-Fixe (WAN sur Int 1, LAN sur Int 2)	172.29.0.133 / 255.255.0.0 / 172.29.0.254

Il est nécessaire de redémarrer le boîtier pour appliquer les changements.

3.10.1.2.Mode Routeur

Chaque interface réseau est paramétrable :

L'interface WAN sur le port int 1

L'interface LAN sur le port int 2



Procédure de configuration :

Après quelques minutes, le boîtier s'assigne une IP fixe (192.0.2.1). Connectez-vous à l'interface d'administration, puis allez dans l'onglet "Fonctions avancées / Bridge - Routeur".

Choisissez le mode routeur. Et renseignez les adresses IP et masques des réseaux à connecter.

L'interface Int1 (WAN) peut être sous DHCP :

Paramètres du mode ROUTEUR	
WAN en mode DHCP (sur Int 1)	☒
WAN en mode IP Fixe (sur Int 1)	☐
@IP-Fixe WAN (sur Int 1)	
Masque	
Passerelle	
@IP-Fixe LAN (sur Int 2)	192.168.1.1
Masque	255.255.255.0
NAT	☒

Paramètres du mode ROUTEUR	
@IP-Fixe WAN (sur Int 1)	dhcp /
@IP-Fixe LAN (sur Int 2)	192.168.1.1 / 255.255.255.0
Passerelle	
NAT	activé

Ou adressage fixe

Paramètres du mode ROUTEUR	
WAN en mode DHCP (sur Int 1)	☐
WAN en mode IP Fixe (sur Int 1)	☒
@IP-Fixe WAN (sur Int 1)	172.29.0.133
Masque	255.255.0.0
Passerelle	172.29.0.254
@IP-Fixe LAN (sur Int 2)	192.168.1.1
Masque	255.255.255.0
NAT	☒

Paramètres du mode ROUTEUR	
@IP-Fixe WAN (sur Int 1)	172.29.0.133 / 255.255.0.0
@IP-Fixe LAN (sur Int 2)	192.168.1.1 / 255.255.255.0
Passerelle	172.29.0.254
NAT	activé

Remarque :

- Le mode NAT peut être activé.
- Indiquez dans le champ « Passerelle » la route par défaut dans le cas d'un adressage fixe.

3.10.2. Serveur DHCP

Un serveur DHCP permet de distribuer dynamiquement des adresses IP sur un réseau. Le service DHCP peut être activé sur les interfaces Lan et Réseau secondaire.

Le service est disponible seulement si le boîtier est en mode transparent IP fixe ou en mode routeur

Activer le service DHCP	
Activer le service DHCP	☐

Paramètres du serveur DHCP LAN	
Nom du domaine (facultatif)	
Réseau	172.29.0.0
Masque	255.255.0.0
@IP début	172.29.0.100
@IP fin	172.29.0.200
Serveur Wins (facultatif)	
Passerelle	172.29.0.254
DNS	172.29.0.133

Paramètres du serveur DHCP LAN	
Nom du domaine (facultatif)	
Réseau	172.29.0.0
Masque	255.255.0.0
@IP début	172.29.0.100
@IP fin	172.29.0.200
Durée des baux	
Serveur Wins (facultatif)	
Passerelle	172.29.0.254
DNS	172.29.0.133

Dans le cas d'un boîtier équipé de trois ports réseaux, il est possible d'administrer également un serveur DHCP sur un réseau secondaire

Le service est disponible uniquement si le réseau secondaire est activé.

Activer le service DHCP
 Activer le service DHCP ☐

Paramètres du serveur DHCP Réseau secondaire

Nom du domaine (facultatif))	
Réseau	192.168.10.0
Masque	255.255.255.0
@IP début	192.168.10.100
@IP fin	192.168.10.200
Serveur Wins (facultatif)	
Passerelle	192.168.10.1
DNS	192.168.10.1

Paramètres du serveur DHCP Réseau secondaire

Nom du domaine (facultatif))	
Réseau	192.168.10.0
Masque	255.255.255.0
@IP début	192.168.10.100
@IP fin	192.168.10.200
Durée des baux	
Serveur Wins (facultatif)	
Passerelle	192.168.10.1
DNS	192.168.10.1

3.10.3. Table de routage

L'onglet « Table de routage » permet de définir les routes IP statiques.

Paramètres du routage

IP réseau	
Masque	
Passerelle	

APPLIQUER >>>

Paramètres du routage

Sup	IP réseau	Masque	Passerelle
✗	0.0.0.0	0.0.0.0	172.29.0.254

3.10.4. Réseau secondaire

Il est possible de paramétrer un réseau secondaire et d'en gérer les accès.

L'utilisation d'un réseau secondaire permet :

- 1) de partager un accès Internet entre deux réseaux ayant des droits différents,
- 2) d'interdire l'accès au réseau secondaire depuis le réseau principal,
- 3) d'autoriser ou non l'accès au réseau principal depuis le réseau secondaire.

Paramètres du réseau secondaire	
IP	192.168.10.1 (192.168.10.1)
Masque	255.255.255.0 (255.255.255.0)

Paramètres du réseau secondaire	
IP	192.168.10.1
Masque	255.255.255.0
Accès internet	filtré
Accès au réseau principal	Non
Authentification réseau secondaire	Oui

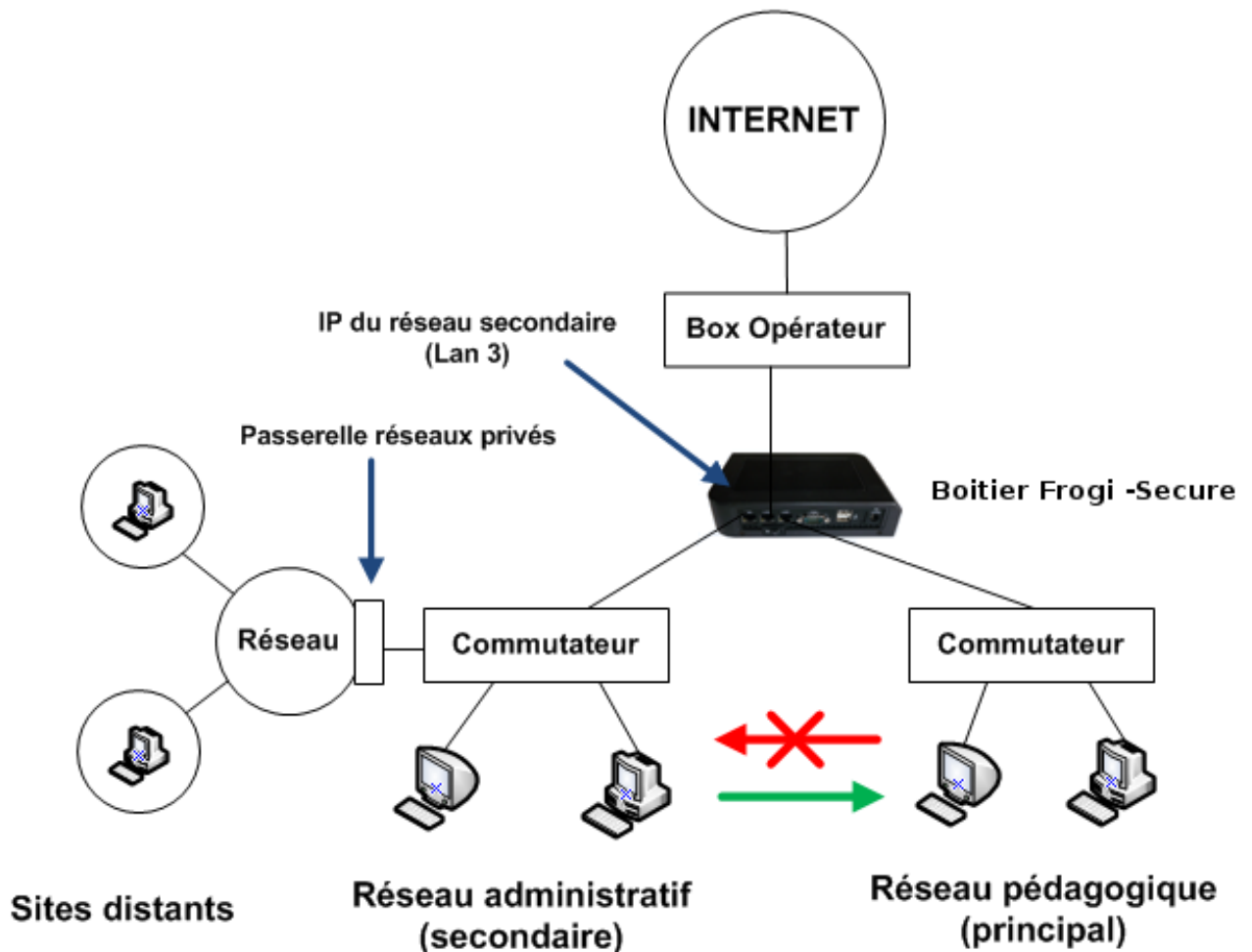
Accès internet	
Accès à Internet depuis le réseau secondaire :	
☐ Oui, sans être soumis aux règles de filtrage ☒ Oui, en étant soumis aux règles de filtrage ☐ Non	

Accès au réseau principal	
Les utilisateurs du réseau secondaire sont autorisés à accéder au réseau principal	
☐ Oui ☒ Non	

Authentification réseau secondaire	
Prise en compte des options d'authentification du réseau principal	
☒ Oui ☐ Non	
APPLIQUER	

Cette fonctionnalité a été développée pour répondre aux spécificités de certains établissements scolaires qui disposent d'un réseau pédagogique et d'un réseau administratif.

Vous avez également la possibilité d'indiquer une passerelle pour atteindre des sites distants en indiquant une route statique dans la table de routage (voir schéma).



Remarque :

- Le site secondaire doit impérativement être connecté sur le port LAN spécifique du boîtier (cf Annexe), les connexions au point d'accès Internet (box de l'opérateur) sur le port Lan 1 et au commutateur de l'établissement sur le port Lan 2.
- Les passerelles des réseaux privés peuvent se situer indifféremment sur le réseau administratif ou sur le réseau pédagogique ou sur les deux.

3.10.5. Options

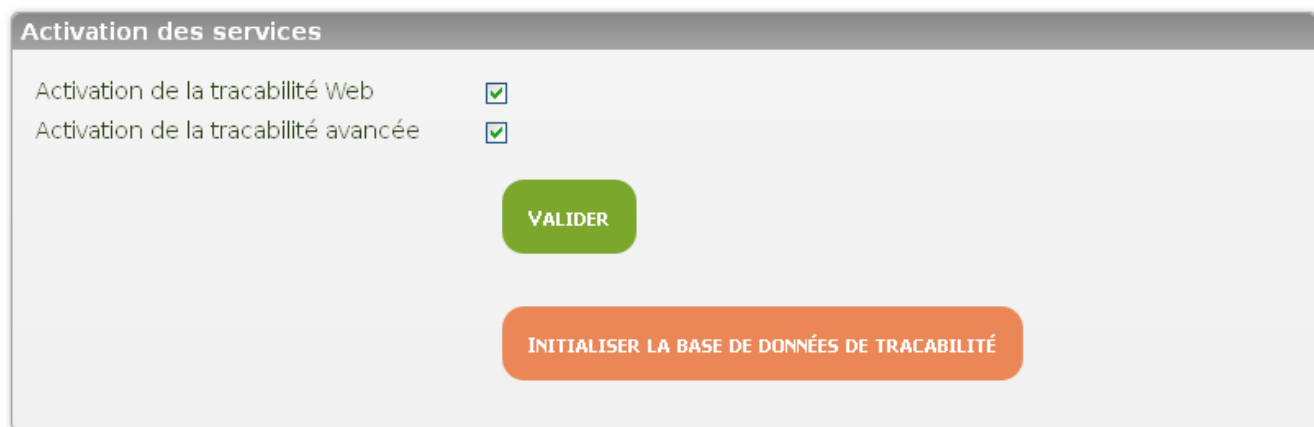
3.10.5.1. Télémaintenance



The image shows two side-by-side screenshots of the Frogi Secure web interface. The left screenshot, titled 'Activation du service', shows a checkbox for 'Autorisation de télémaintenance' which is checked, and a green 'VALIDER' button below it. The right screenshot, titled 'Lancement de la télémaintenance', shows a green button labeled 'LANCER LA TÉLÉMAINTENANCE'.

La télémaintenance est activée par défaut. Ce service permet au service technique de Frogi Secure de prendre la main sur le produit à distance et ainsi procéder à une intervention technique de mise à niveau ou d'assistance technique à l'utilisateur. Le bouton « lancer la télémaintenance » permet une télémaintenance immédiate sur demande en concordance avec le service technique de Frogi Secure.

3.10.5.2. Traçabilité et cryptage des historiques de navigation



The image shows a screenshot of the 'Activation des services' section of the Frogi Secure web interface. It contains two checkboxes: 'Activation de la traçabilité Web' and 'Activation de la traçabilité avancée', both of which are checked. Below these checkboxes are two buttons: a green 'VALIDER' button and an orange 'INITIALISER LA BASE DE DONNÉES DE TRACABILITÉ' button.

Le service de traçabilité Web est activé par défaut. Si vous souhaitez le désactiver, il suffit de décocher la case et de valider. La traçabilité est immédiatement interrompue.

Le service de traçabilité avancée concerne l'activité complète de l'activité réseau par protocole. Elle sauvegarde l'émetteur et le destinataire de chaque connexion réseau.

L'initialisation de la base de données de traçabilité efface entièrement les traces. Attention, après initialisation et confirmation il n'est plus possible d'annuler l'opération.

Info : Les postes restent soumis aux règles de filtrage même si la traçabilité est désactivée.

Activation du cryptage des données

Activation du cryptage des données ☐

VALIDER

Le cryptage des données de l'activité Internet permet de respecter la législation (décret n° 2006-358 du 24 mars 2006) tout en préservant la confidentialité des accès.

Lorsque la fonction de cryptage des données est activée (cryptage AES), vous ne pouvez plus accéder aux informations sur l'activité Internet. En cas de procédure judiciaire, Frogi Secure transmettra la clé de décryptage (qui est propre à chaque boîtier) aux autorités compétentes.

La seule façon d'annuler le cryptage des données est de remettre le boîtier en configuration usine mais dans ce cas la base de données sera réinitialisée.

3.10.5.3.Comportement en cas de défaillance (Safe mode)

Activation du service

En cas de dysfonctionnement des fonctions de filtrage du boîtier, autoriser les accès Internet ☒

VALIDER

En cas de dysfonctionnement des fonctions de filtrage du boîtier, il est possible de bloquer les accès Internet ou de les autoriser. Dans les deux cas un message sera envoyé à l'adresse email de l'administrateur (défini dans l'onglet « Authentification »).

3.10.5.4.Relais DNS

Les boîtiers Frogi Secure interceptent les requêtes DNS. Si cette option est désactivée, le certificat du boîtier ne sera plus reconnu et le mode SafeSearch en HTTPS/SNI ne fonctionnera pas. Il est possible d'indiquer un relais DNS spécifique qui est généralement celui de votre opérateur Internet.

Un domaine par défaut pour les serveurs Wins est paramétrable.

Activation du service

Oui

☒

Non

☐

IP relais DNS

☐

Domaine par défaut

VALIDER

3.10.5.5.Initialisation en configuration usine

Cette option réinitialise le boîtier en configuration usine.

Toutes les données sont initialisées y compris la base de traçabilité et les groupes et comptes utilisateurs.

Configuration usine

BOITIER EN CONFIGURATION USINE

Vous pouvez utiliser une procédure manuelle pour réinitialiser le boîtier en configuration usine (chapitre « Remise en configuration usine ».)

3.10.5.6.Fuseau Horaire

Le fuseau horaire est à configurer en fonction de votre zone géographique et de la ville la plus proche de votre position. Par défaut le fuseau horaire est celui de Paris.

Fuseau horaire

Continents

Europe - Paris

(actuel : Europe - Paris)

VALIDER

3.10.6. Gestion de flotte de boitiers

3.10.6.1. Description



Choix du mode

Mode

☐ Boitier de référence

☐ Boitier appartenant à une flotte

☒ Boitier indépendant

APPLIQUER

Chaque boitier a la possibilité de piloter un ensemble de boitiers. Le boitier de référence une fois configuré, pilote un ensemble de boitiers esclaves. Cette application facilite la gestion multi sites. La flotte ne comporte pas de limite en nombre et tout boitier peut être rattaché à une flotte sans aucune modification d'architecture.

Le boitier comporte trois possibilités de configuration :

- Boitier de référence : Le boitier est dit « MASTER », il est le boitier référent de la flotte. La configuration des autres boitiers seront alors synchronisés sur celui-ci.
- Boitier appartenant à une flotte : le boitier est raccroché à un ensemble de boitiers et se synchronise sur un boitier référent.
- Boitier indépendant : C'est le fonctionnement par défaut. Le boitier est indépendant.

3.10.6.2. Boitier de référence MASTER

Dans ce mode le boitier devient la référence de la flotte. L'administrateur peut alors configurer les paramètres à synchroniser sur les boitiers pilotés.

Vous devez indiquer deux types d'informations :

- les paramètres à synchroniser

Paramètres	Synchronisation
Profils de sécurité	☒
Liste(s) blanche(s)	☒
Liste(s) noire(s)	☒
Liste des sites exclus du profil de sécurité	☒
Liste des Mac Address exclues du profil de sécurité	☐
Liste des adresse IP exclues du profil de sécurité	☐
Liste des adresses Mac autorisées	☒
Paramètres d'apprentissage des Mac Address	☒
Mots de passe de déblocage des smartphones	☒
Liste des Mac Address des smartphones autorisés	☒
Plages horaires	☒
Paramètres d'authentification	☒
Paramètres Ldap	☒
Personnalisation de la page d'accueil	☒
Email administrateur	☒
Liste des sites exclus d'analyse	☒
Option relais DNS	☒
Option télémaintenance	☒
Optimisation de la bande passante	☒
Rapport email	☒
Sauvegarde automatique	☒
Activation de la tracabilité	☒
Groupes et comptes utilisateurs	☒
Antivirus	☒
Gestion des mises à jours logicielles	☒

APPLIQUER

- Les numéros de série des boitiers à synchroniser

Boitier à synchroniser

Numéro de série

Commentaire

AJOUTER

Boitiers de la flotte						
Sup	Boitiers de la flotte	Commentaire	Synchronisation	Date de demande	Dernière synchronisation	Etat
✗	R20-APU2-112233	Ecole Jaures	☐			
✗	R20-APU2-223344	Ecole St Marc	☐			

Les boitiers sélectionnés seront synchronisés en fonction des paramètres validés. Les demandes et accusés de réception sont visibles dans le tableau des boitiers de la flotte. Ces informations permettent d'avoir un suivi de l'état de la flotte.

Paramétrage du boitier appartenant à la flotte	
Boitier de référence	R20-APU2-123456
Mot de passe	••••••••
Synchronisation	☒
APPLIQUER	

Sur les boitiers à synchroniser vous devez également indiquer le numéro de série et le mot de passe de référence. Ces paramètres sont rappelés dans les paramètres de synchronisation.

3.10.6.3. Boitier dépendant appartenant à une flotte

Dans ce mode de fonctionnement, le boitier est intégré à une flotte de boitiers et se synchronise sur un boitier référent « Master ». Vous devez dans ce cas renseigner le numéro de série et le mot de passe du boitier référent « Master ».

Paramétrage du boîtier appartenant à la flotte

Boîtier de référence

R20-APU2-123456

Mot de passe

••••••••

Synchronisation

☒

APPLIQUER

Synchronisation

Lancer une synchronisation

3.10.6.4. Boîtier indépendant

C'est le mode de fonctionnement par défaut. Le boîtier est indépendant.

3.10.7. Internet X2 (Multiwan)

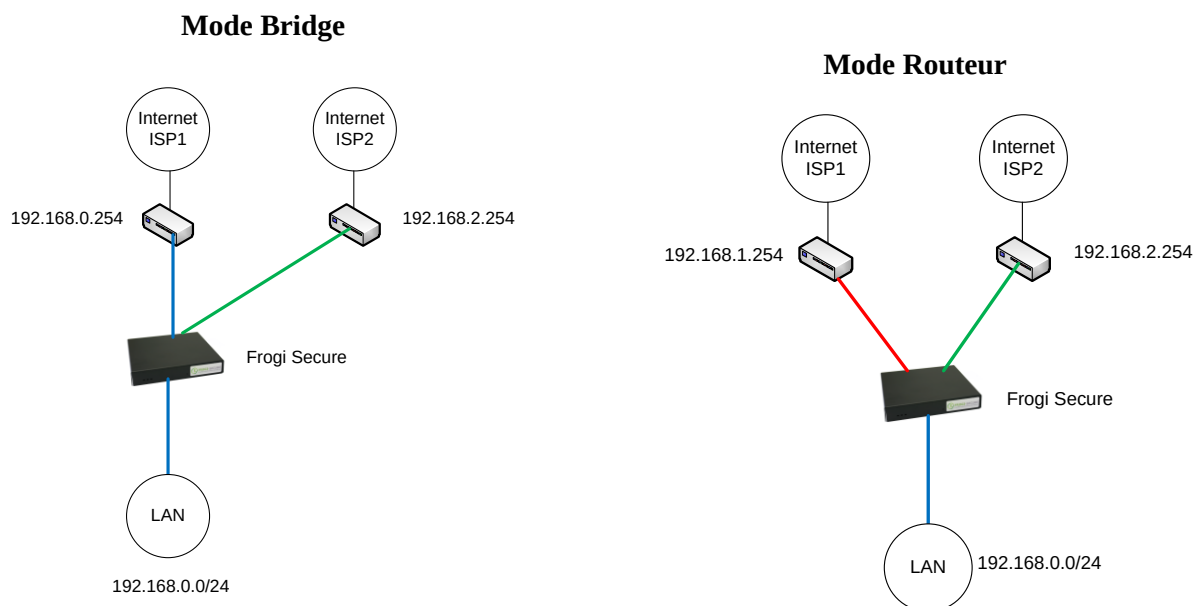
3.10.7.1. Connectique

Voir l'annexe « Connectique » à la fin de ce document.

3.10.7.2. Mode Bridge / Mode Routeur

Le Multi-Wan peut fonctionner soit en mode bridge ou en mode routeur.

Le mode est déterminé dans l'onglet Bridge/Routeur des fonctions avancées.



3.10.7.3.Paramètres

La première partie concerne l'adressage de l'interface Wan ISP2. Il peut être adressé directement ou laissé sous la gestion d'un service DHCP présent sur le réseau.

La deuxième partie concerne le mode de fonctionnement du service multi Wan. Il peut être en équilibrage ou en débordement.

L'option de secours permet un basculement automatique d'une interface WAN à l'autre en cas de défaillance d'un des accès Internet.

L'option de notification permet un envoi d'emails suivant les incidents survenant sur les accès Internet.

Paramètres

Activer le multiwan
☐

Paramètres Réseau

Interfaces	DHCP ☒ Fixe ☐	activé
Adresse IP		
Masque		
Passerelle		

Paramètres fonctionnels

Mode	Poids ISP1	Poids ISP2	ISP2/ISP1
Equilibrage ISP1 -> ISP2 ISP2 -> ISP1	1	1	.50

Secours ☒
Notifications ☒

VALIDER

PARAMÈTRES PAR DÉFAUT

Équilibrage de charge

Le mode d'équilibrage de charge permet de répartir la charge du flux réseau sur les deux accès Internet. Il est possible d'attribuer un poids à chaque interface et de spécifier le rapport de charge. Par défaut les interfaces ont les mêmes poids et le rapport ISP2/ISP1 est de 50%.

Débordement

Le mode débordement permet de répartir le flux réseau d'un accès principal sur un deuxième accès à partir d'une limite de charge de 70%. Ce qui permet d'utiliser efficacement des accès de bande passante différente.

Tests des lignes

Le test des lignes est un outil d'aide à la décision concernant le mode le plus adapté. Après avoir lancé la procédure, les informations caractérisant chaque accès sont mises en comparaison et un mode de fonctionnement adapté est proposé. Si le mode de fonctionnement proposé convient, il peut être chargé dans les paramètres de configuration par le bouton « accepter ». A noter qu'il est nécessaire de valider les paramètres chargés pour qu'ils soient effectifs.

Remarque : Les accès LAN sont temporairement bloqués durant les tests de lignes afin de ne pas interférer dans la détermination de la bande passante de chaque accès Internet.

Tests des lignes

	ISP1	ISP2
ISP	LANESTEL	France Telecom
Etat		
Débits montant MAX (Mbits/s)	1.38	0.83
Débit descendant MAX (Mbits/s)	84.22	17.57
Débits montant (Mbits/s)		
Débits descendant (Mbits/s)		

	Mode	Poids ISP1	Poids ISP2	ISP2/ISP1
<<< ACCEPTER	isp1 --> isp2	84	17	.17

LANCER LES TESTS

3.10.7.4. Routage multiwan (route policy)

Nouvelle règle de routage Multiwan

Source
Destination
Protocole
Port
Interface
Secours

all
Principale
Oui

APPLIQUER >>>

Règles Multiwan actives

Sup	Source	Destination	Protocole	Port	Interface	Secours
✗	192.168.0.0	all	all	all	Principale	Oui
✗	172.29.0.0	all	all	all	Secondaire	Oui

Une table de routage permet de diriger les flux réseau sur un accès ou un autre en fonction des paramètres réseaux spécifiques. La notion « all » caractérisant l'ensemble en fonction du paramètre choisi.

3.10.8. Diagnostics

Le diagnostic est un rapport détaillé d'une procédure de tests portant sur les différents points du système ainsi qu'une vue de l'environnement réseau.

La procédure de test peut être lancée directement. Le rapport de diagnostics est alors téléchargeable pour une exploitation externe.

Actions

Lancer un diagnostic
Télécharger le rapport détaillé

Rapport système

Serial	R20-APU2-415B0E
Mess-01	File System OK
Mess-02	Temporary File System OK
Mode	bridge IP fixe
IP	172.29.0.133
Masque	255.255.0.0
Mess-05	Internet OK
Mess-10	DNS OK
Mess-11	Squid OK
Mess-12	SquidGuard OK

IP	MAC	Nom
172.29.0.254	00:0d:b9:27:c1:58	Gateway
172.29.0.40	00:11:32:14:7d:e7	SERVEUR-F
172.29.0.193	00:17:c8:25:3d:aa	Imprimante
172.29.0.136	00:80:77:51:7b:b5	BRN008077517BB5



IP	MAC	Nom
172.29.0.42	64:70:02:52:6b:4e	Kyocera
172.29.1.100	f4:6d:04:0a:e0:6c	Daniel-PC
172.29.1.101	00:81:c5:0a:ab:c6	Marie-PC
172.29.1.102	00:45:dd:42:b1:2c	Judith-PC

Le rapport de diagnostics valide le bon fonctionnement hardware et software du boîtier.

- Vérification système
- Vérification des ressources disponibles
- Rappel du mode réseau choisi par l'administrateur : plug&play, bridge transparent ou routeur.
- Vérification de la connexion Internet
- Vérification des résolutions DNS

- Vérification des services actifs et de la base de filtrage
- Listing du positionnement des appareils actifs présent sur le réseau par rapport au boîtier

Remarque : Seuls les appareils positionnés côté LAN du boîtier sont sous la protection du boîtier Frogi Secure.

3.10.9. Gestion des mises à jour logicielles

3.10.9.1.Objectifs

La « Gestion des mises à jour logicielles » a pour objectif d'autoriser ou non les mises à jour logicielles des éditeurs (Apple, MS, etc.) lorsque celles-ci se font en HTTP ou HTTPS.

Pour chaque éditeur, les mises à jour peuvent être :

1. Toujours autorisées.
2. Jamais autorisées.
3. Autorisées dans une plage horaire.
4. Désactivées.

Il y a deux types d'éditeurs :

1. Les éditeurs référencés par Frogi Secure.
2. Les éditeurs créés par l'administrateur du boîtier.

Remarques :

- Les mises à jour logicielles autorisées le sont également lorsque l'authentification est activée et que l'utilisateur n'est pas ou plus connecté.
- Les mises à jour en HTTPS se font en mode SNI même si le mode Proxy HTTPS est activé. Certains éditeurs, Apple et MS par exemple, n'autorisent pas les mises à jour HTTPS par Proxy.

3.10.9.2.Administration des mises à jour logicielles

Présentation

La gestion des éditeurs se fait dans l'onglet « Fonctions avancées / Gestion des mises à jour logicielles ».

Liste des applications et services					
Sup	Liste des éditeurs	Bloqué	Autorisé sur plages horaires	Autorisation permanente	Désactivé
	Adobe	☐	☐	☒	☐
	Android	☐	☐	☒	☐
	Apple	☐	☐	☒	☐
	Avira	☐	☐	☒	☐
	CA	☐	☐	☒	☐
	Chromebook	☐	☐	☒	☐
	Defender	☐	☐	☒	☐
	Itslearning	☐	☐	☒	☐
	Kaspersky	☐	☐	☒	☐
	Mcafee	☐	☐	☒	☐
	Microsoft	☐	☐	☒	☐
	Mozilla	☐	☐	☒	☐
	Skype	☐	☐	☒	☐
	Symantec	☐	☐	☒	☐
	Trendmicro	☐	☐	☒	☐

Remarques

- Par défaut les mises à jour logicielles sont toujours autorisées.
- Seuls les éditeurs créés par l'administrateur peuvent être supprimés.
- Lorsque vous positionnez le curseur sur le nom d'un éditeur, la liste des serveurs est affichée.

Ajout d'un éditeur


Nouvel éditeur

Nom


Ajouter un domaine à une liste d'éditeur

Nouveau domaine --> mon-editeur ▼


Liste des domaines ajoutés

Sup	Domaines	Editeurs
☒	.maj_mon-editeur.bzh	mon-editeur

La gestion d'un nouvel éditeur se fait en 3 étapes :

1. Ajout de l'éditeur
2. L'ajout des serveurs de mises à jour associés à cet éditeur.
3. La stratégie de mise à jour.

Gestion des plages horaires

- Les plages horaires se définissent pour chaque jour et par heure.
- Une plage horaire autorisée est matérialisée par la couleur verte, une plage horaire non autorisée par la couleur rose.
- A l'installation du produit, toutes les plages horaires sont autorisées.
- Pour changer une plage horaire, il suffit de cliquer une fois pour la passer en rose et deux fois pour la passer en vert.

Exemple

 Plages horaires des mises à jour logicielles

 Plages horaires

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
Lundi	Green	Green	Green	Green	Green	Green	Green	Rose	Rose	Rose	Rose	Rose	Rose	Rose	Rose	Rose	Rose	Rose	Rose	Rose	Rose	Green	Green	Green
Mardi	Green	Green	Green	Green	Green	Green	Green	Rose	Rose	Rose	Rose	Rose	Rose	Rose	Rose	Rose	Rose	Rose	Rose	Rose	Rose	Green	Green	Green
Mercredi	Green	Green	Green	Green	Green	Green	Green	Rose	Rose	Rose	Rose	Rose	Rose	Rose	Rose	Rose	Rose	Rose	Rose	Rose	Rose	Green	Green	Green
Jeudi	Green	Green	Green	Green	Green	Green	Green	Rose	Rose	Rose	Rose	Rose	Rose	Rose	Rose	Rose	Rose	Rose	Rose	Rose	Rose	Green	Green	Green
Vendredi	Green	Green	Green	Green	Green	Green	Green	Rose	Rose	Rose	Rose	Rose	Rose	Rose	Rose	Rose	Rose	Rose	Rose	Rose	Rose	Green	Green	Green
Samedi	Green	Green	Green	Green	Green	Green	Green	Rose	Rose	Rose	Rose	Rose	Rose	Rose	Rose	Rose	Rose	Rose	Rose	Rose	Rose	Green	Green	Green
Dimanche	Green	Green	Green	Green	Green	Green	Green	Rose	Rose	Rose	Rose	Rose	Rose	Rose	Rose	Rose	Rose	Rose	Rose	Rose	Rose	Green	Green	Green

APPLIQUER

Remarque :

Les plages horaires utilisées pour les mises à jour logicielles sont différentes de celles utilisées par les profils de filtrage.

4. Remise en configuration usine.

1. Sur une clé USB, créer le répertoire : **frogi-secure-configuration-usine**.
2. Insérer la clé USB dans le boîtier.
3. Redémarrer le boîtier.



La remise en configuration usine supprimera le contenu de la base de données de l'activité Internet.

5. Réinitialisation du mot de passe d'administration

1. Sur une clé USB, créer le répertoire : **frogi-secure-restauration-mot-de-passe**.
2. Insérer la clé USB dans le boîtier.
3. Redémarrer le boîtier.

6. Support technique

02 90 26 21 22

tech@frogi-secure.com

7. Annexes

7.1. Plateforme SMS lesms.com

Après avoir ouvert votre compte client, vous obtenez vos paramètres de connexion au compte que vous renseignez dans l'interface du boîtier Frogi Secure.



The screenshot displays the LeSMS.com website interface. At the top, the logo "LeSMS.com" is shown with the tagline "Solutions professionnelles pour l'envoi de SMS par Internet". Below the logo is a navigation bar with links: ACCUEIL, PRÉSENTATION, NOS SOLUTIONS, and DÉVELOPPEURS / API. The main section is titled "SE CONNECTER" and features a login form with fields for "VOTRE EMAIL" and "MOT DE PASSE", and a "VALIDER" button. A red box highlights the login form. To the right, a "Paramètres service" panel is visible, showing the following details:

Paramètres service	
Nombres de SMS utilisés	0 / 5
Mettre fin à la période d'essai ?	✗
Identifiant	En essai
Mot de passe	••••••••

Below the login form, there are links for "Mot de passe oublié ?" and "Inscription et informations", and a contact number: "Pour toute question, remarque ou suggestion, n'hésitez pas à nous contacter au 01.76.240.240". On the right side, there is a "TESTER LE SERVICE" section with the text "Découvrez LeSMS.com gratuitement et sans engagement !", and a "MEMBRE" section for "La FRENCH TECH RENNES ST MALO".

7.2. Plateforme OVH

1. Ouvrir un espace client chez ovh.com
2. Se connecter à son manager OVH ou espace client



Identifiez-vous chez OVH

Je suis déjà client OVH

Identifiant ou adresse email

Mot de passe

Se connecter

Tout savoir sur l'identifiant client

Identifiant ou mot de passe oublié ?

Je n'ai pas encore de compte OVH

Prénom

Nom

Adresse email

Mot de passe

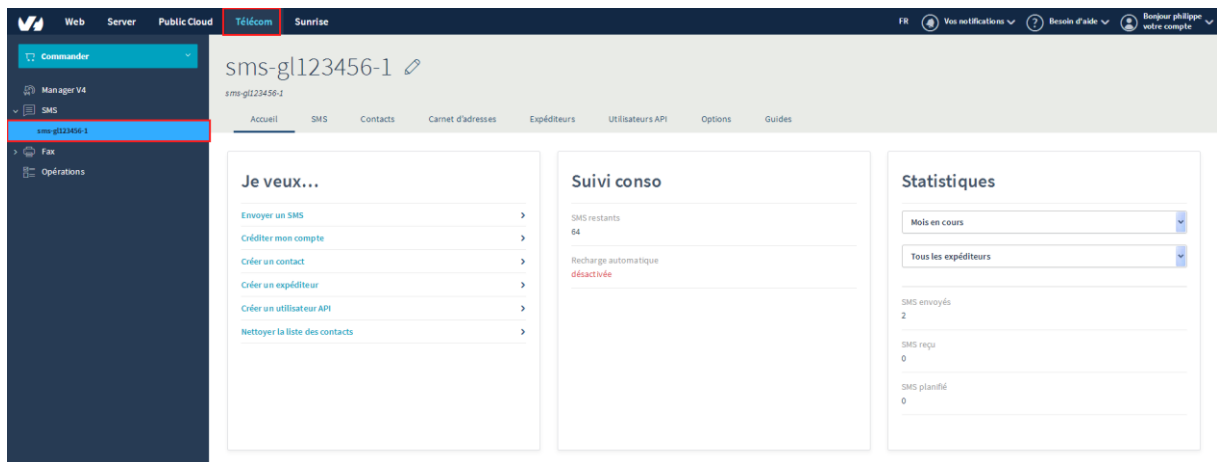
☐ Je confirme avoir plus de 18 ans et accepte les Conditions générales de service OVH

☐ J'accepte de recevoir des informations concernant les produits d'OVH

Créer un compte

Les données communiquées via ce formulaire sont collectées avec votre consentement et sont destinées à OVH S.A.S. en sa qualité de responsable du traitement. Elles pourront être transmises à ses sous-traitants agissant sur strictes instructions d'OVH S.A.S. ainsi qu'aux entités du Groupe OVH. Dans cette seconde hypothèse, et sous réserve que l'entité du Groupe OVH ait signé des règles d'entreprise contraignantes, les données pourront faire l'objet d'un transfert en dehors de l'Union Européenne. Les données de ce formulaire sont collectées à des fins de gestion de la relation client, de sollicitations commerciales et de respect de la réglementation applicable à OVH. Les données de votre compte client sont conservées jusqu'à la suppression de votre compte client, puis durant trente-six (36) mois. Certaines données traitées à des fins de gestion (exemple : facture) peuvent être conservées plus longtemps conformément à la réglementation applicable. Vous disposez de la faculté d'introduire une réclamation auprès de l'autorité de contrôle compétente ainsi qu'un droit d'accès, de

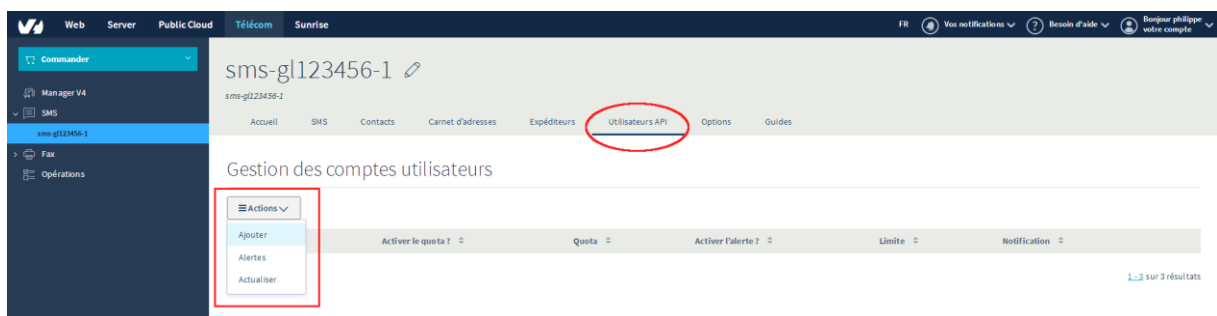
Choisir l'onglet Télécom puis son compte sms.



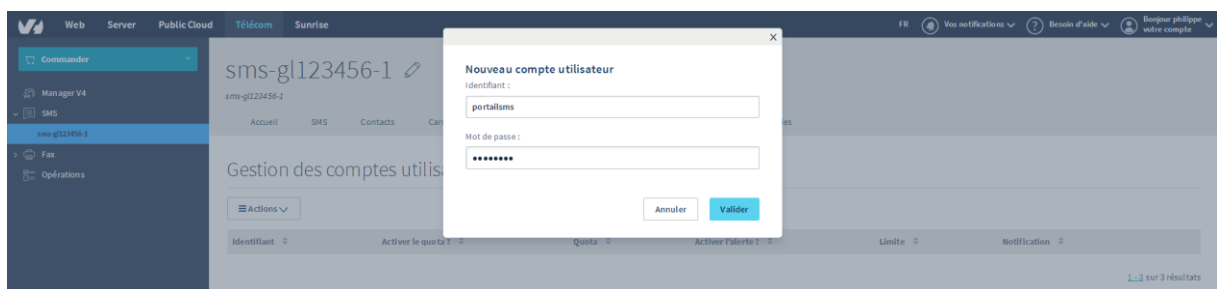
3. Ajouter un utilisateur API

Ouvrir l'onglet concernant les utilisateurs API.

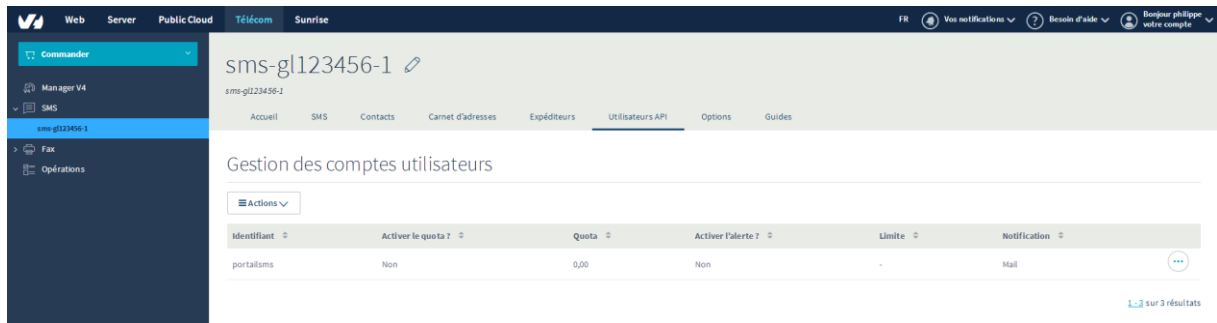
Ajouter un compte utilisateur par le menu déroulant Actions.



Renseigner les données du compte.



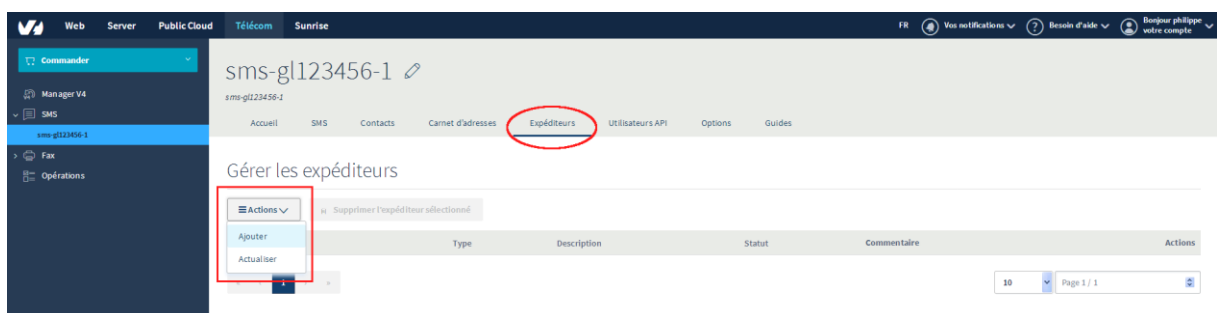
Le compte utilisateur est créé.



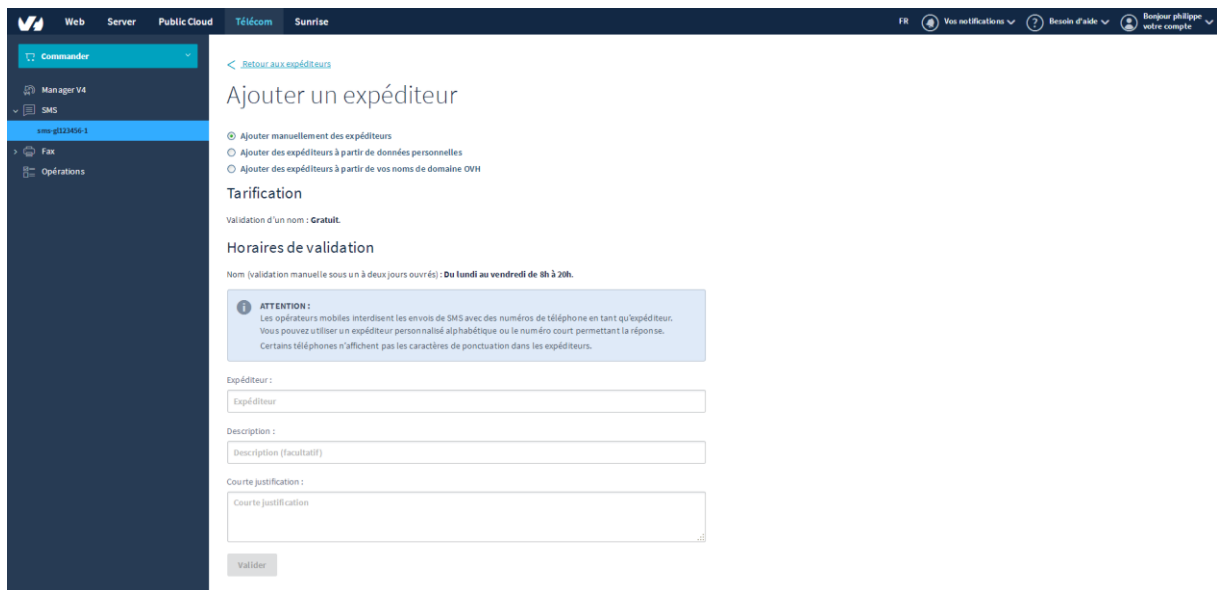
4. Ajouter un expéditeur

Aller dans l'onglet Expéditeurs

Ajouter un expéditeur via le menu déroulant Actions.

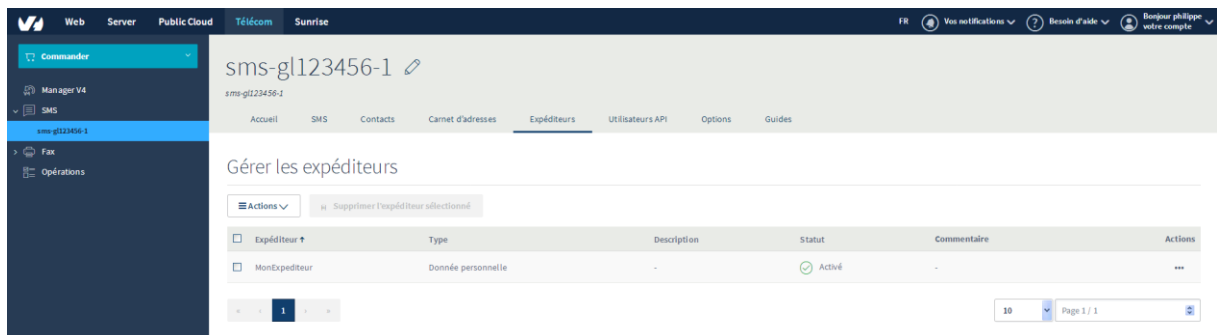


Renseigner les données concernant l'expéditeur.



The screenshot shows the 'Ajouter un expéditeur' (Add sender) form in the Frogi Secure interface. The form is located under the 'Télécom' (Telecom) tab. It includes a sidebar with navigation options like 'Commander', 'Manager V4', 'SMS', 'Fax', and 'Opérations'. The main content area has a title 'Ajouter un expéditeur' and a subtitle 'Retour aux expéditeurs'. Below the title, there are three radio buttons for adding a sender: 'Ajouter manuellement des expéditeurs' (selected), 'Ajouter des expéditeurs à partir de données personnelles', and 'Ajouter des expéditeurs à partir de vos noms de domaine OVH'. There is a 'Tarification' section with a note about validation. Below that, there is a 'Horaires de validation' section with a note about manual validation. The form includes input fields for 'Expéditeur', 'Description (facultatif)', and 'Courte justification'. A 'Valider' button is at the bottom right.

L'expéditeur est créé et une fois validé, il apparaît disponible.



The screenshot shows the 'Gérer les expéditeurs' (Manage senders) table in the Frogi Secure interface. The table has columns for 'Expéditeur', 'Type', 'Description', 'Statut', 'Commentaire', and 'Actions'. There is one row with the sender 'MonExpéditeur' of type 'Donnée personnelle', which is 'Activé' (Active). The table is part of a larger interface with a sidebar and a top navigation bar.

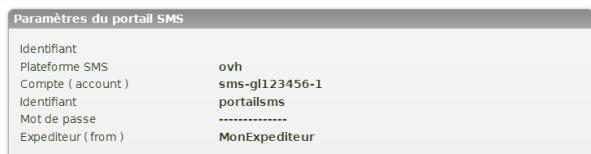
Expéditeur	Type	Description	Statut	Commentaire	Actions
MonExpéditeur	Donnée personnelle	-	Activé	-	...

5. Configuration du portail SMS dans la console d'administration.

Reporter la configuration dans les champs du paramétrage du portail SMS en choisissant « ovh.com » comme plateforme SMS et validé.



The screenshot shows the 'Paramètres du portail SMS' (SMS portal settings) form. It includes fields for 'Nombres de SMS utilisés' (1), 'Plateforme SMS' (ovh.com), 'Compte (account)' (sms-gl123456-1), 'Identifiant' (portalsms), 'Mot de passe' (masked), and 'Expéditeur (from)' (MonExpéditeur). A 'VALIDER' button is at the bottom.

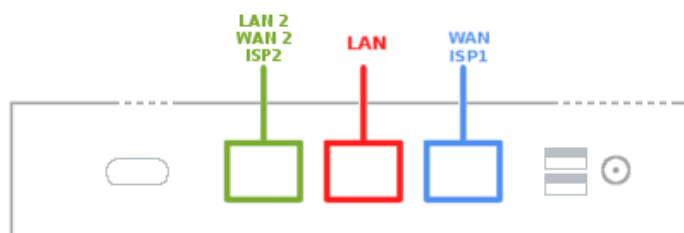


The screenshot shows the 'Paramètres du portail SMS' (SMS portal settings) form with the following configuration details:

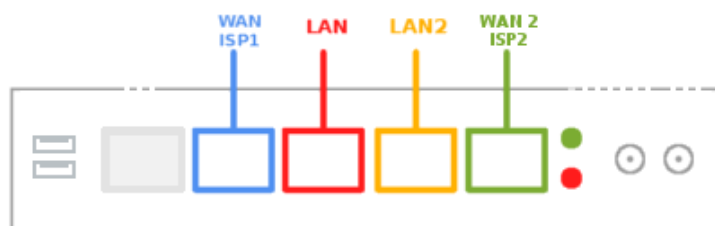
Identifiant	
Plateforme SMS	ovh
Compte (account)	sms-gl123456-1
Identifiant	portalsms
Mot de passe	
Expéditeur (from)	MonExpéditeur

7.3. Connectique

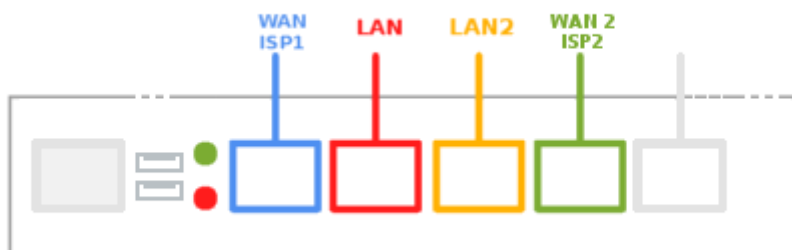
Frogi 20



Frogi 50



Frogi 100/250/1000



7.4. Installation du certificat SSL

Il est possible de l'installer directement par navigateur ou de l'installer au niveau session utilisateur via console MMC.

Le certificat de sécurité est sauvegardé dans le magasin de certificats sous « autorités de certifications racine de confiance » rattaché à la session utilisateur.

Remarque : Il faut noter que certains navigateurs, comme Mozilla Firefox, possèdent leur propre magasin.

7.4.1. Installation du certificat via console MMC

Télécharger le certificat sur :

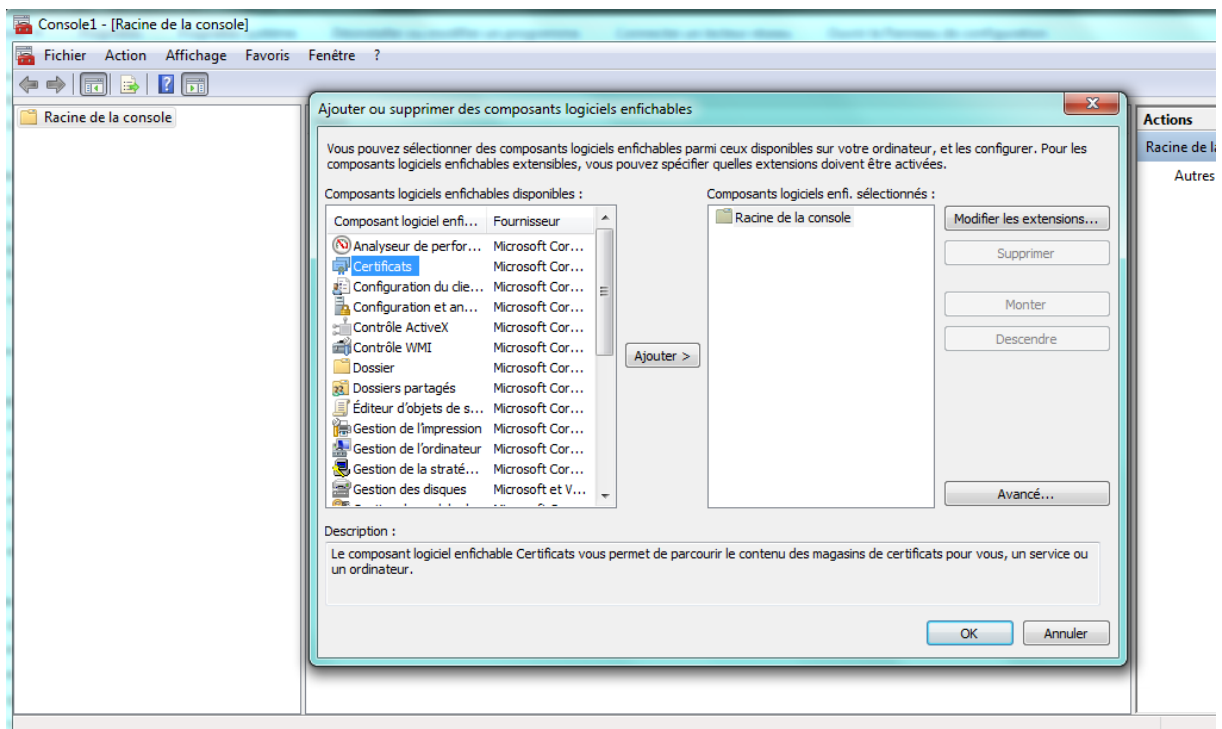
<https://www.frogi-secure.com/certif/frogi-secure.der>

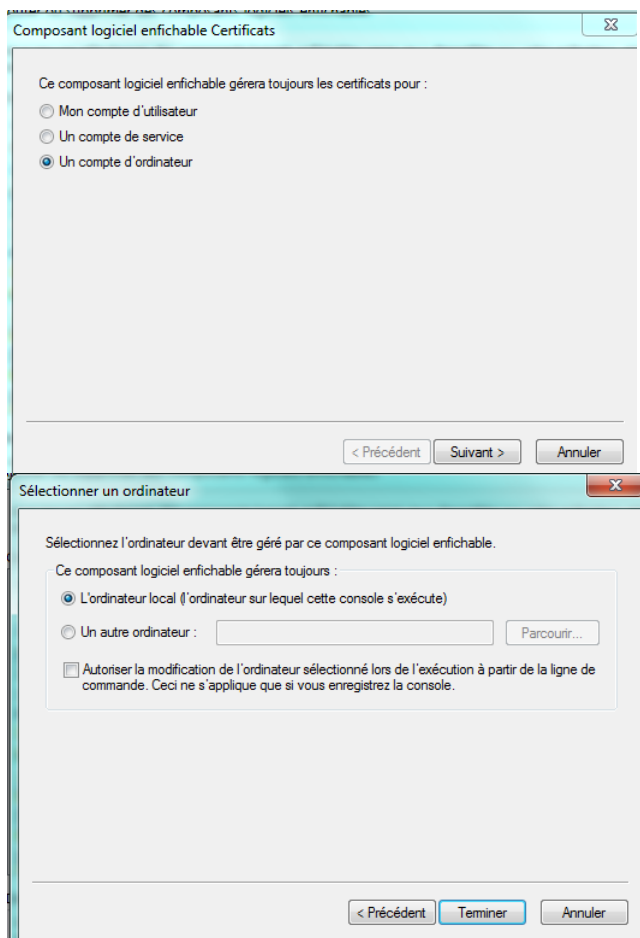
Lancer une console MMC (Menu Démarrer/ taper mmc).

Dans la console MMC :

Fichier → Supprimer/Ajouter un composant logiciel enfichable

Sélectionner Certificat et Ajouter.





Composant logiciel enfichable Certificats

Ce composant logiciel enfichable gérera toujours les certificats pour :

☐ Mon compte d'utilisateur

☐ Un compte de service

☒ Un compte d'ordinateur

< Précédent Suivant > Annuler

Sélectionner un ordinateur

Sélectionnez l'ordinateur devant être géré par ce composant logiciel enfichable.

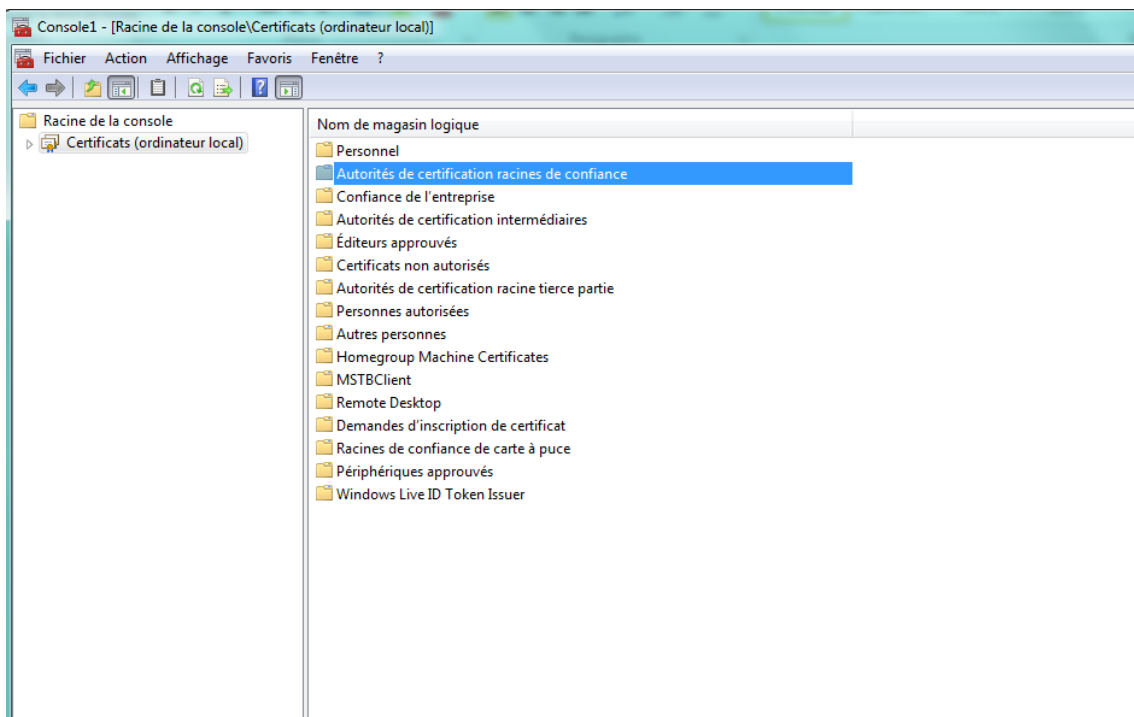
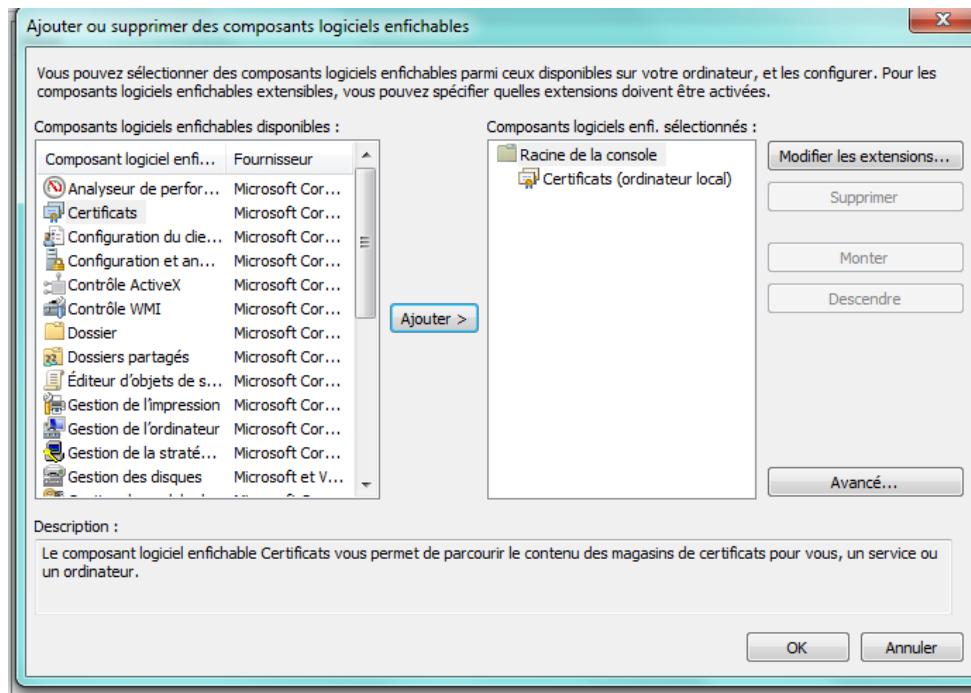
Ce composant logiciel enfichable gérera toujours :

☒ L'ordinateur local (l'ordinateur sur lequel cette console s'exécute)

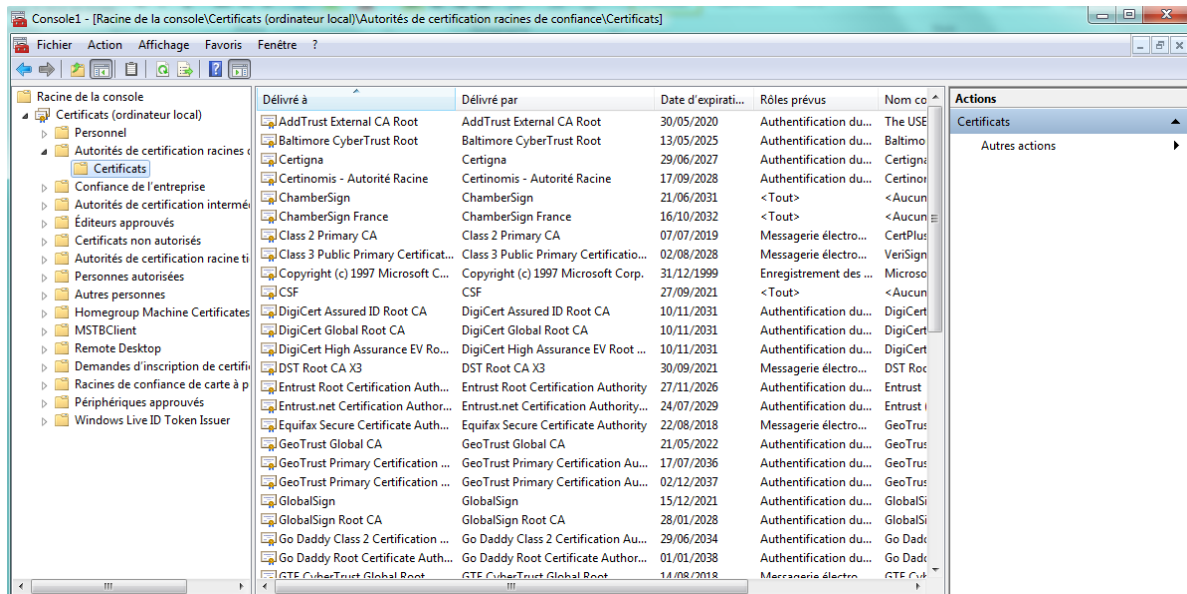
☐ Un autre ordinateur : Parcourir...

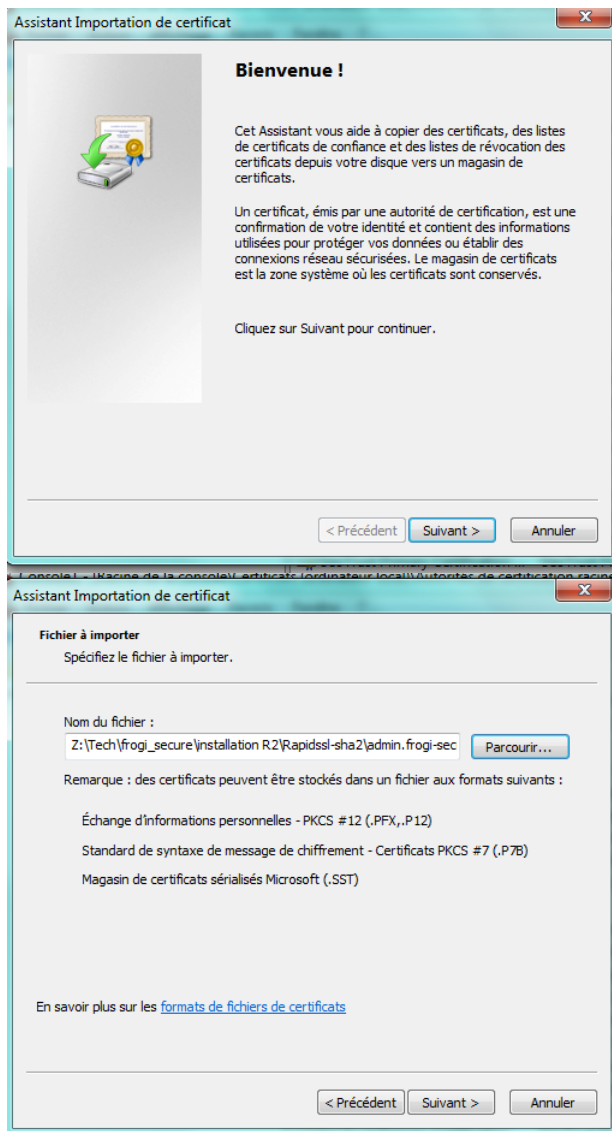
☐ Autoriser la modification de l'ordinateur sélectionné lors de l'exécution à partir de la ligne de commande. Ceci ne s'applique que si vous enregistrez la console.

< Précédent Terminer Annuler

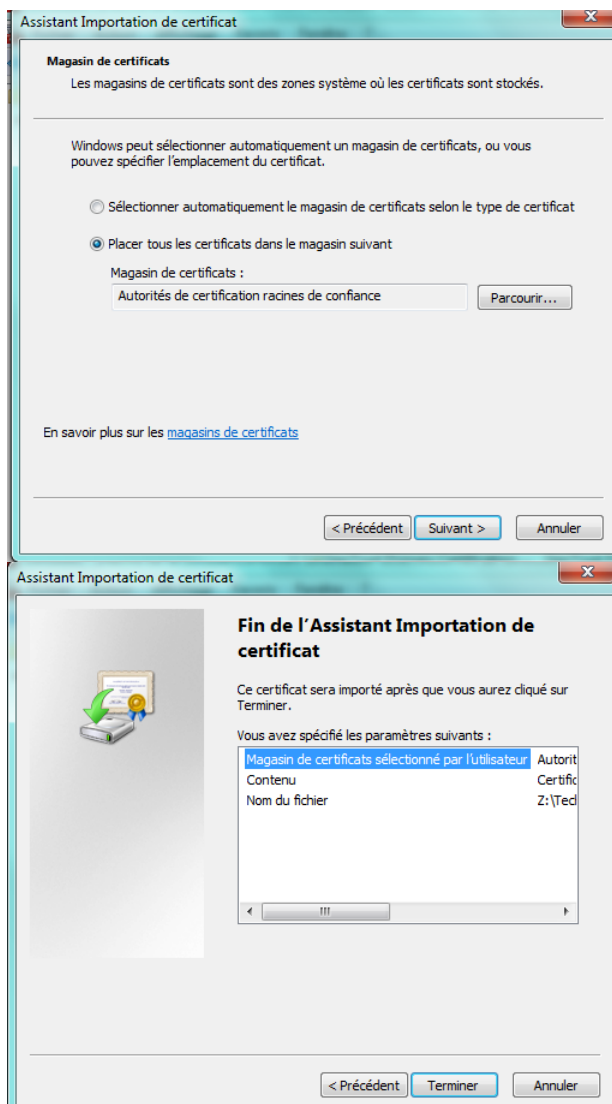


Certificats / clic droit /Toutes les tâches /Importer.





Vérifier que le certificat sera placé dans le magasin « **autorités de certification racines de confiance** ».



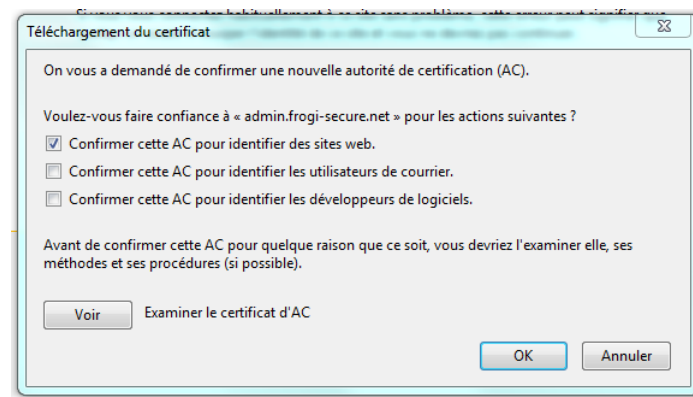
7.4.2. Installation du certificat

7.4.2.1. Navigateur Mozilla Firefox

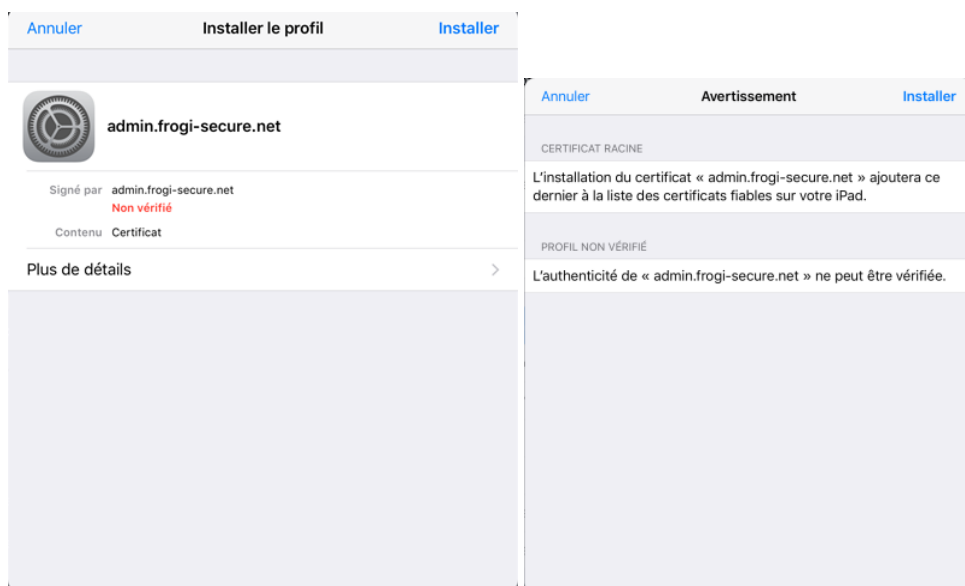
Aller à l'adresse suivante :

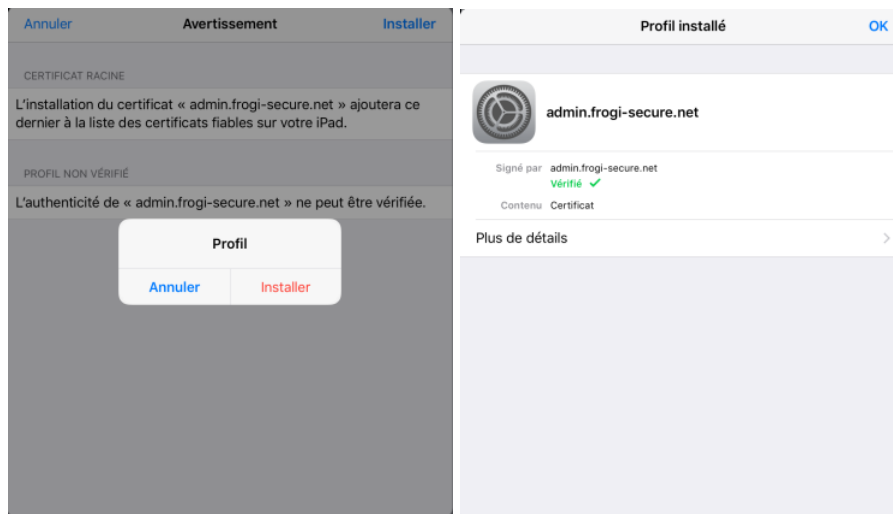
<http://www.frogi-secure.com/certif/frogi-secure.der>

Le navigateur propose automatiquement la procédure d'installation du certificat.



Le navigateur lance automatiquement la procédure d'installation de certificats.





7.4.2.2. Navigateur Internet Explorer / Chrome

Aller à l'adresse suivante :

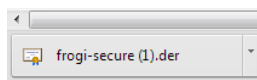
<http://www.frogi-secure.com/certif/frogi-secure.der>

Le navigateur lance une procédure de téléchargement du fichier.

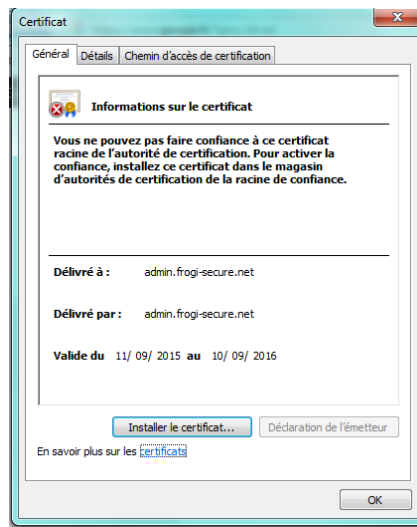
Internet Explorer



Chrome



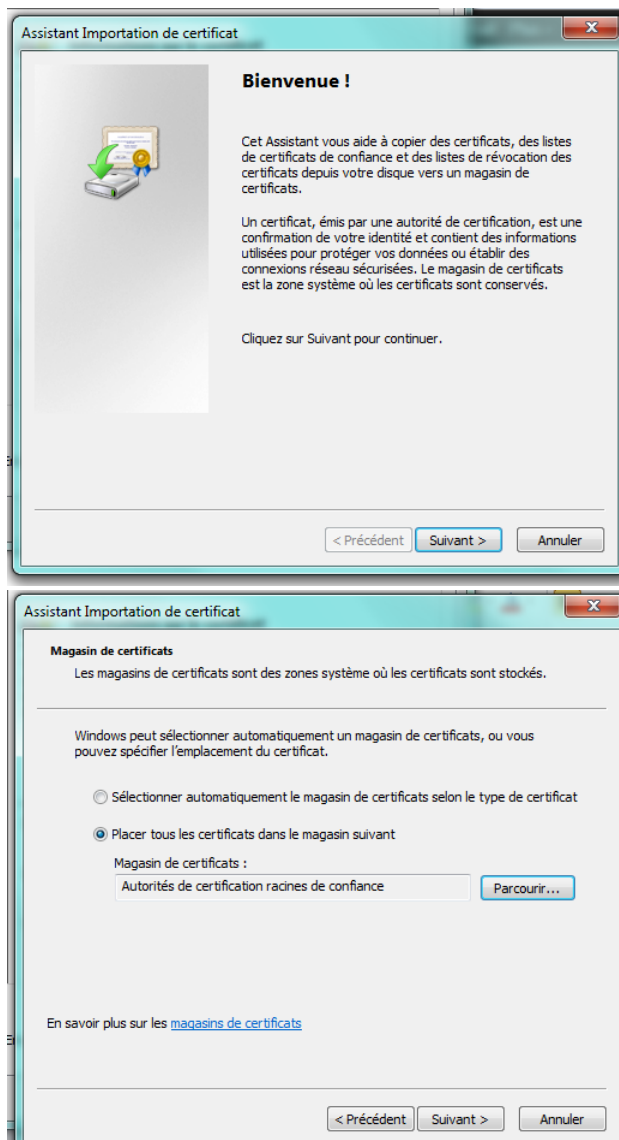
Cliquez sur « Ouvrir »,

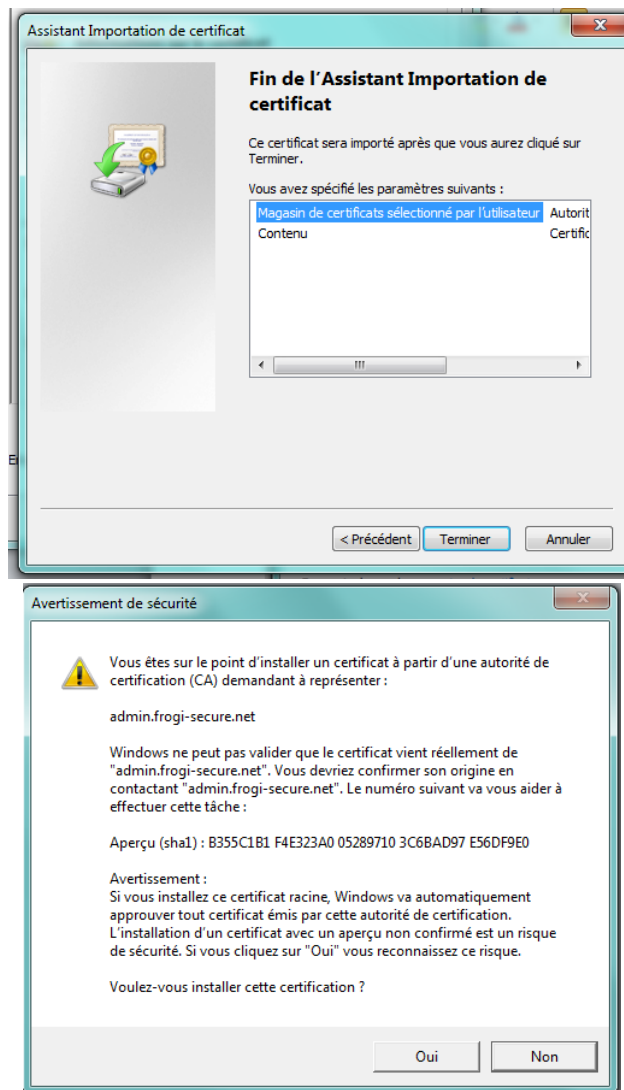


Cliquez sur « installer le certificat ».

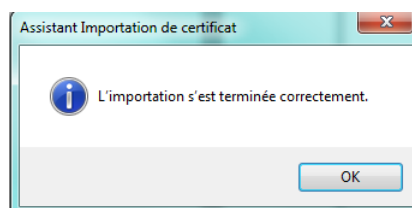
La procédure importation de certificats est lancée.

Veillez à placer le certificat dans le magasin « Autorités de certification racines de confiance ».



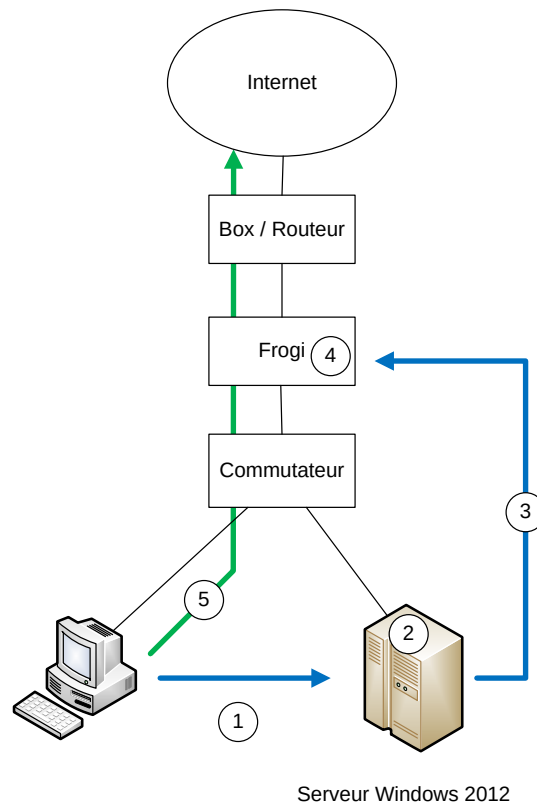


L'installation du certificat est terminée.



7.5. Connecteur AD/SSO

7.5.1. Principe de fonctionnement



- 1) L'utilisateur se connecte dans le domaine Windows AD.
- 2) L'ouverture de session déclenche l'exécution d'un script qui détermine :
 - Le nom de l'utilisateur.
 - L'IP du poste.
 - Le nom du profil à appliquer.
- 3) Le serveur se connecte au boîtier Frogi en mode SSH et transmet les paramètres de connexion.
- 4) Le boîtier Frogi installe le profil de l'utilisateur associé à l'IP du poste.
- 5) Les sessions vers Internet sont filtrées avec les paramètres du profil.

La mise en œuvre de ce processus nécessite d'installer :

- 1) Le client SSH sur le serveur Windows.
- 2) Une GPO pour créer un événement à chaque ouverture de session.
- 3) La création d'une tâche planifiée.
- 4) La création d'une OU et de groupes/profils.

7.5.2. Installation

7.5.2.1. Installation des sources

Décompresser le fichier Frogi-AD-SSO.zip dans le répertoire :

C:\Programmes\Frogi

Débloquer les programmes – Clic droit puis Propriétés

Nom	Type
 AD en mode SSO.pdf	Adobe Acrobat Document
 r2_check.exe	Application
 r2-eventlog.xml	Document XML
 r2-login.exe	Application
 SSH-SessionsPSv3.zip	Dossier compressé

Vérifier que les scripts ne sont pas bloqués (Clic droit – Propriétés – Débloquer).

7.5.2.2. Installation du client SSH

- 1) Recherche des conteneurs PowerShell

Ouvrir une session PowerShell et taper la commande :

\$env:PSModulePath –split ‘;’

```
PS C:\Users\Administrateur> $env:PSModulePath –split ';'
C:\Users\Administrateur\Documents\WindowsPowerShell\Modules
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\
PS C:\Users\Administrateur>
```

- 2) Création du répertoire du conteneur

Il faut utiliser le conteneur associé à l'administrateur et créer les répertoires.

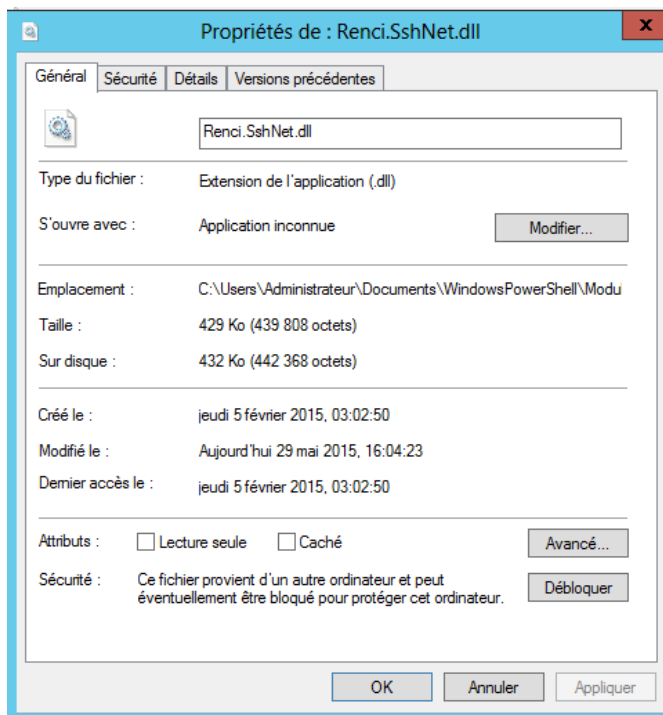
mkdir C:\Users\Administrateur\Documents\WindowsPowerShell

mkdir C:\Users\Administrateur\Documents\WindowsPowerShell\Modules

3) Décompresser SSH-SessionPSv3 dans

C:\Users\Administrateur\Documents\WindowsPowerShell\Modules.

4) Débloquer les programmes si nécessaire.



5) Installer le client SSH.

Dans une session PowerShell entrer les commandes suivantes :

Set-ExecutionPolicy Unrestricted
Import-Module -Verbose SSH-Sessions

```
COMMENTAIRES : Chargement du module à partir du chemin
« C:\Users\Administrateur\Documents\WindowsPowerShell\Modules\SSH-Sessions\SSH-Sessions.psdl ».
COMMENTAIRES : Importation de la fonction « ConvertFrom-SecureToPlain ».
COMMENTAIRES : Importation de la fonction « Enter-SshSession ».
COMMENTAIRES : Importation de la fonction « Get-SshSession ».
COMMENTAIRES : Importation de la fonction « Invoke-SshCommand ».
COMMENTAIRES : Importation de la fonction « New-SshSession ».
COMMENTAIRES : Importation de la fonction « Remove-SshSession ».
PS C:\>
```

6) Vérifier l'installation du client SSH

Exécuter **r2_check.exe**

Les messages suivants doivent apparaître :

```

Source          Destination    IPv4Address    IPv6Address    Bytes    Time(ms)
-----
FROGI-HYPERV    admin.frogi-... 172.29.100.98    32        0
FROGI-HYPERV    admin.frogi-... 172.29.100.98    32        0
FROGI-HYPERV    admin.frogi-... 172.29.100.98    32        0
FROGI-HYPERV    admin.frogi-... 172.29.100.98    32        0
Successfully connected to admin.frogi-secure.net
admin.frogi-secure.net: OK rewrite-url="http://172.29.100.98/v_login.php?clientaddr=10.0.0.1"
OK rewrite-url="http://172.29.100.98/v_login.php?clientaddr=10.0.0.1"
admin.frogi-secure.net should now be disconnected and disposed.

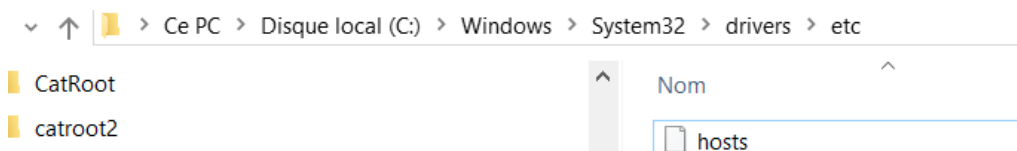
```

Remarque :

Pour communiquer avec le boîtier Frogi, les composants AD/SSO utilisent

admin.frogi-secure.net

Si les requêtes DNS du serveur AD ne traversent pas le boîtier Frogi, il faudra renseigner dans le fichier hosts du serveur AD l'IP du boîtier.

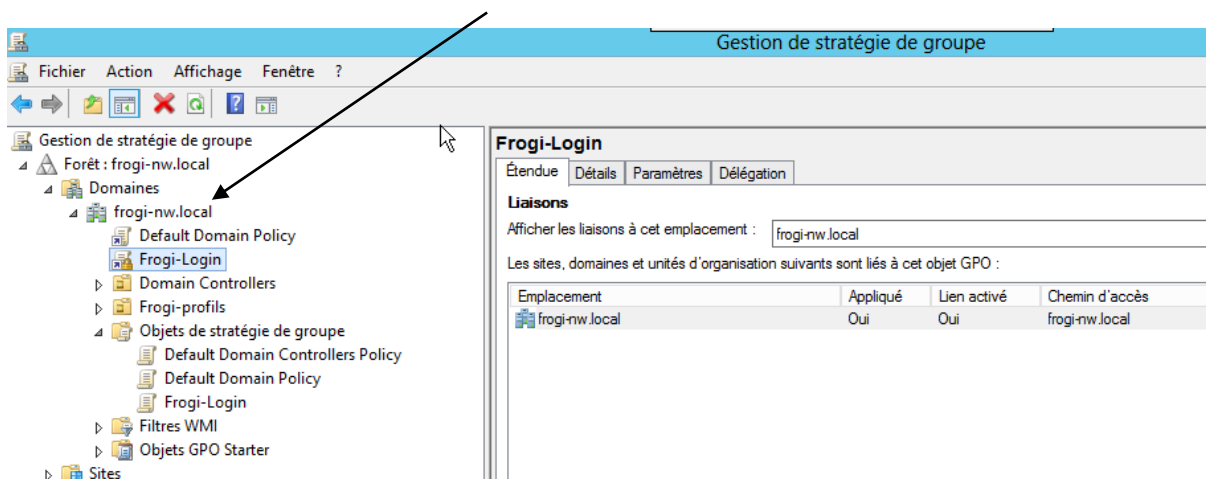


172.29.100.43 admin.frogi-secure.net

7.5.2.3.GPO Frogi-Login

1) Création de la GPO Frogi-Login

- Clic droit sur l'icône du serveur + Créer un objet du serveur « Frogi-Login »



2) Paramétrage de la GPO

(Clic droit → Modifier)

Gestion des stratégies de groupe

Default Domain Policy

Configuration ordinateur

Stratégies

Paramètres Windows

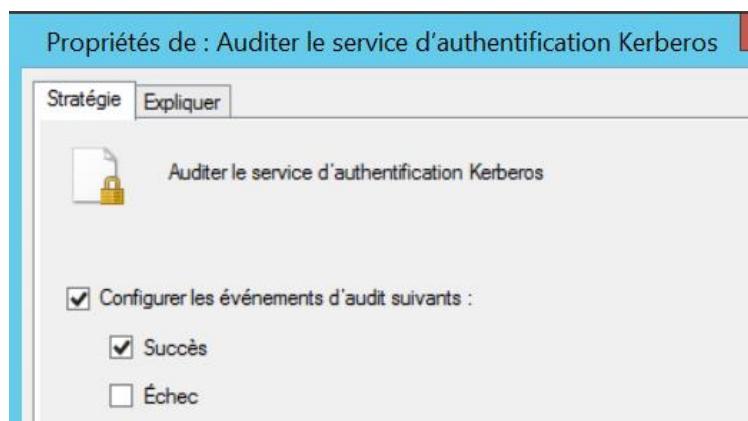
Paramètres de sécurité

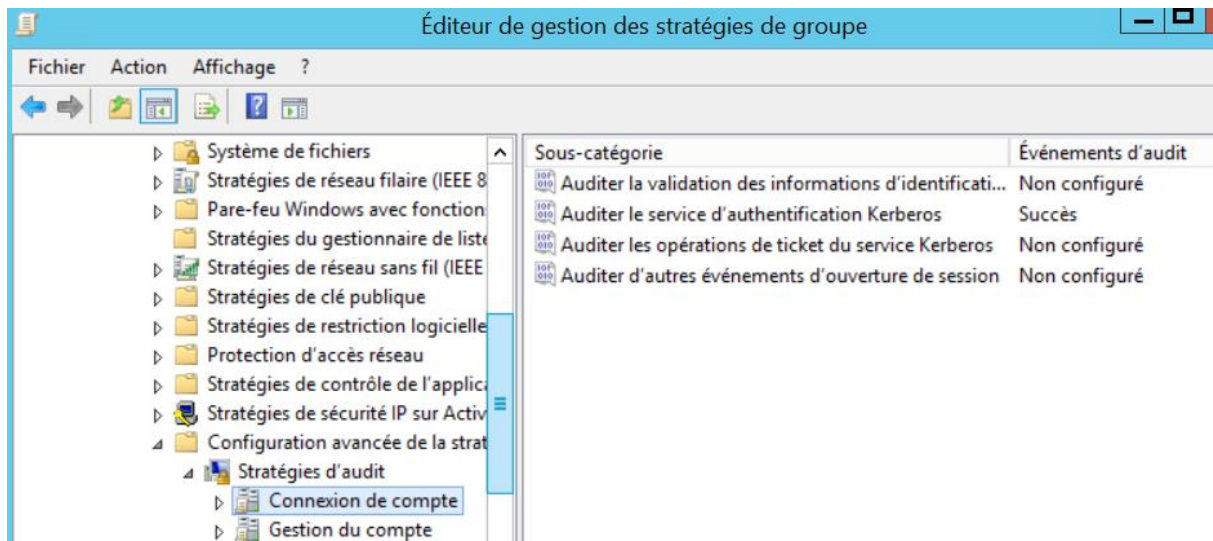
Configuration avancée

Stratégies d'Audit

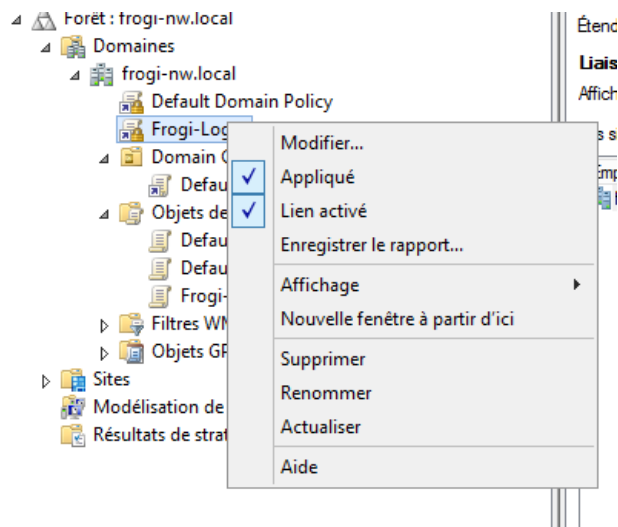
Connexion de compte

Sélectionner « **Auditer le service d'authentification Kerberos** ».

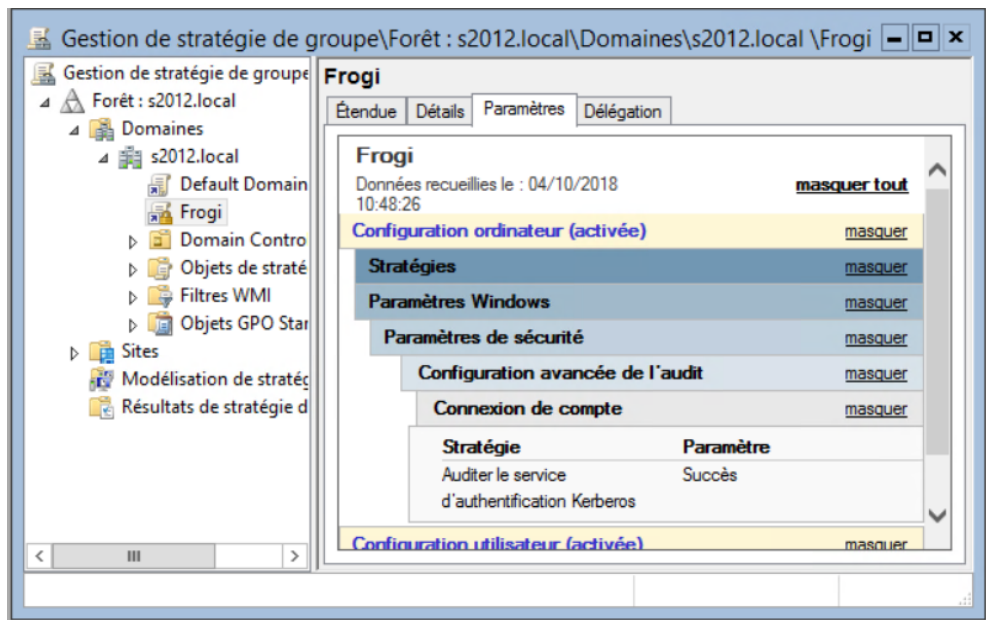




3) Appliquer la GPO

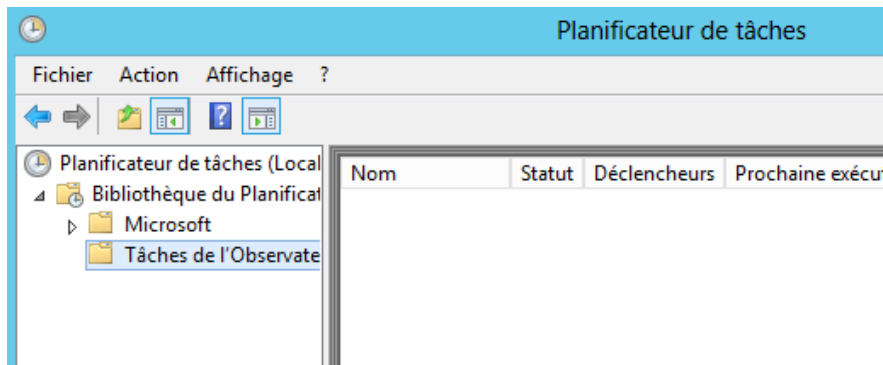


4) Vérification de l'application de la GPO

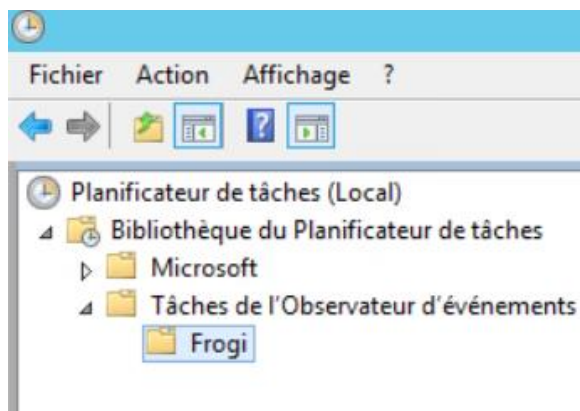


7.5.2.4. Création de la tâche planifiée

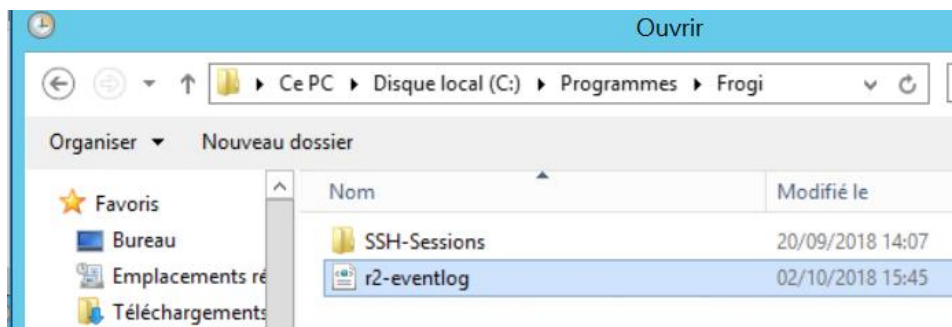
- 1) Ouvrir le Planificateur de tâches



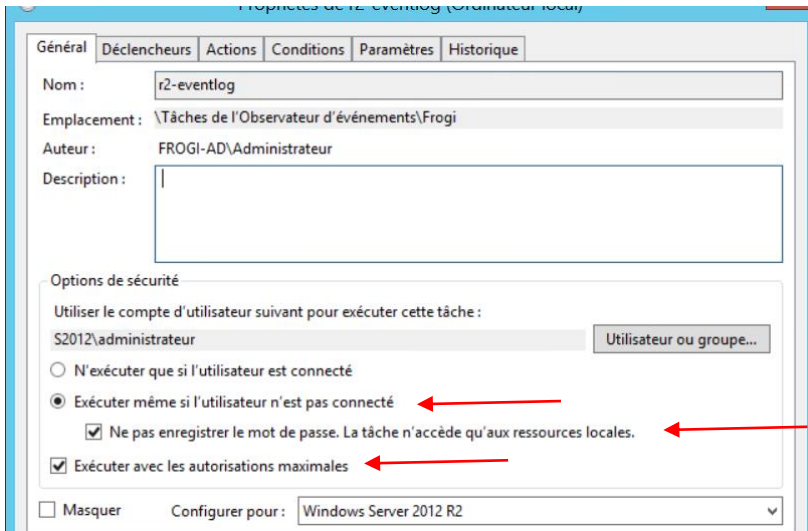
- 2) Faire un clic droit sur “Tâches de l’observateur d’événements » (si ce répertoire n’existe pas vous pouvez le créer, le nom n’a pas d’importance) et créer le dossier Frogi.



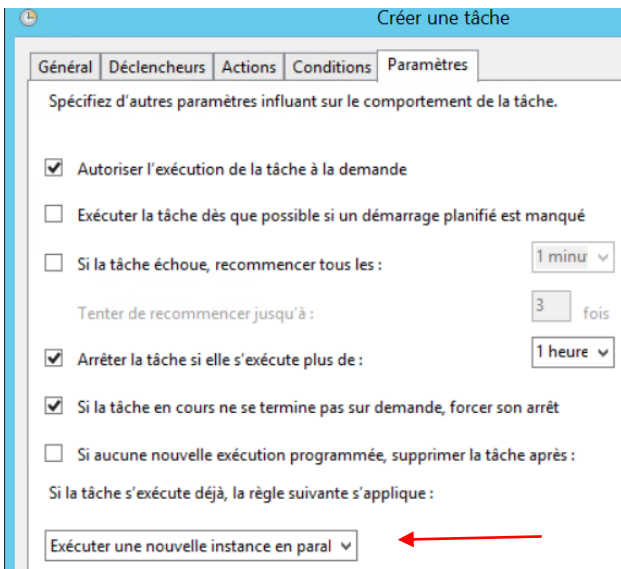
- 3) Importer le script **r2-eventlog.xml** (clic droit sur Frogi et sélectionner **Importer une tâche**)



- 4) Vérifier les paramètres de la tâche. Il est important que ces paramètres soient correctement enregistrés.



Le compte utilisateur devra être celui de l'administrateur du serveur.



7.5.2.5. Création de la relation AD / Profils

La relation AD / Profils Froggi-Secure se fait via les groupes ou les OU de l'AD.

Si un nom du groupe ou de l'OU auquel il appartient correspond à un nom de profil dans le boîtier Froggi, le profil sera associé à l'utilisateur, sinon le profil « **Défaut** » sera utilisé.

7.5.3. Gestion DNS

Les boîtiers Froggi Secure interceptent et traitent deux types de requêtes DNS :

1. **admin.froggi-secure.net** qui pointe sur l'IP du boîtier,
2. La résolution des noms des moteurs de recherche (www.google.fr/com/it/...) pour l'activation ou la désactivation du mode SafeSearch.

Dans un environnement A.D, les postes qui se connectent dans le domaine doivent avoir pour DNS le serveur A.D.

Deux cas de figure sont donc à considérer.

7.5.3.1. Le mode SafeSearch est activé dans tous les profils de sécurité

Dans la mesure où le serveur AD n'est pas exclu du filtrage, il n'y a aucun paramétrage spécifique à faire, le DNS des postes reste celui du serveur AD.

7.5.3.2. Serveur AD exclu du filtrage ou mode SafeSearch différent selon les **profils**.

Postes utilisateurs

La liste des DNS fait référence en premier au serveur Froggi puis au serveur AD. Ainsi, si le boîtier Froggi n'est plus opérationnel, les requêtes DNS seront transmises directement au serveur AD.

Boîtier Froggi Secure

Le DNS du boîtier traite les requêtes pour **admin.froggi-secure.net** pour la résolution des noms des moteurs de recherche afin d'activer ou de désactiver le mode **SafeSearch**.

Les autres requêtes seront transmises au serveur AD.

Pour activer le relais DNS vers le serveur AD allez à :

« Fonctions avancées/Options/Relais DNS »

Relais DNS

Informations

Les boîtiers Frogi Secure interceptent les requêtes DNS pour la résolution de admin.frogi-secure.net et l'activation ou la désactivation du mode SafeSearch..
Vous avez la possibilité d'indiquer un relais DNS qui est généralement celui de votre opérateur Internet.

Activation du service

Oui ☐

Non ☐

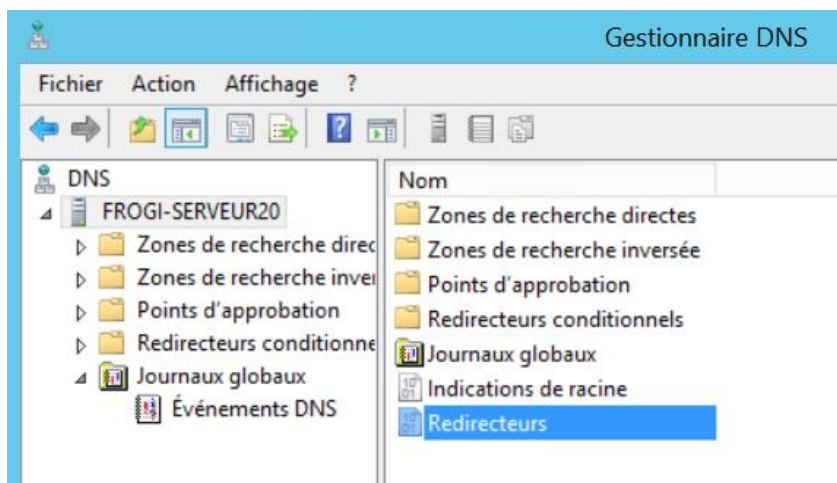
IP relais DNS ☒

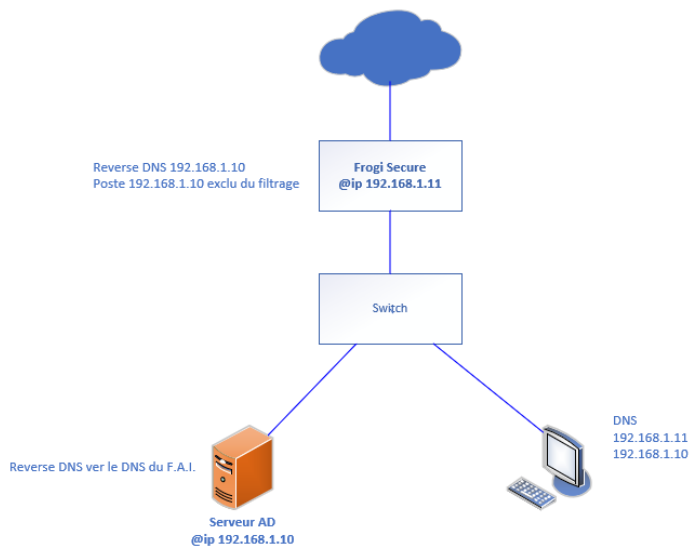
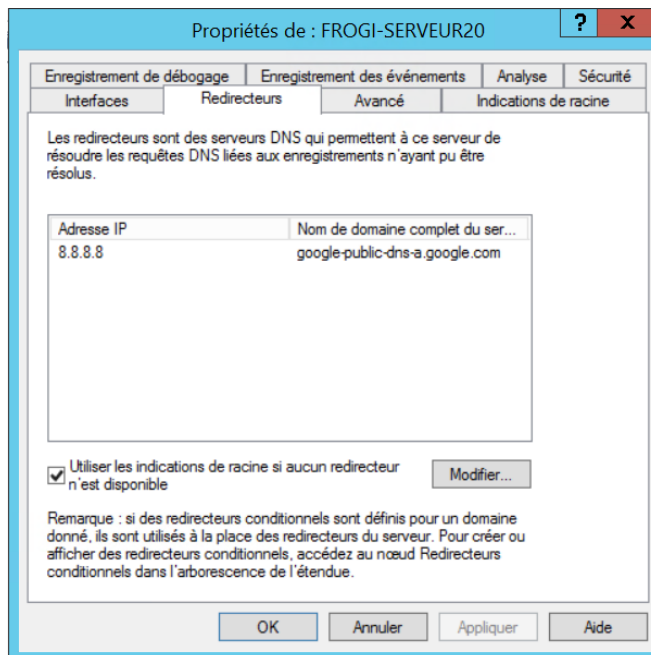
Domaine par défaut

VALIDER

Serveur AD

Activation de la redirection DNS du serveur AD vers le DNS du F.A.I. ou vers un DNS institutionnel.





Exclusion du serveur

Il est indispensable que le serveur AD soit exclu des règles de filtrage pour éviter que les requêtes DNS qu'il émet vers Internet soient interceptées par le boîtier Frogi Secure et lui soient retournées.

Pour exclure un poste du filtrage allez à l'onglet : « Profils de sécurité/Exceptions de filtrage »

7.6. Profil Profs / Elèves

7.6.1. Objectif

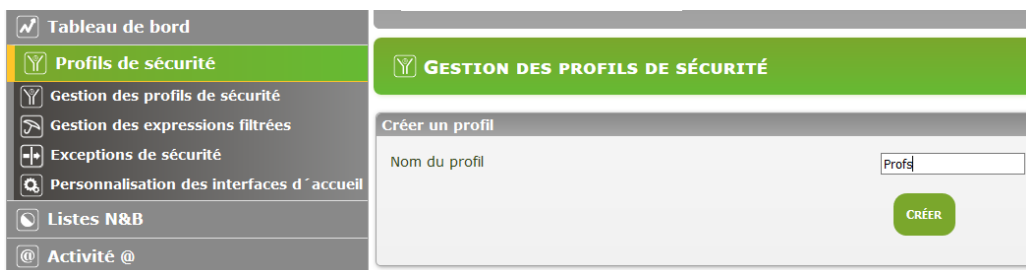
Dans un établissement scolaire, le profil de sécurité par défaut peut s'avérer trop restrictif notamment du fait de l'activation du mode « Safe Search ».

La solution décrite dans ce document met en place l'organisation suivante :

1. Le profil « défaut » est associé automatiquement à chaque demande de connexion à Internet.
2. Si l'enseignant ne peut pas accéder à une information (vidéo YouTube, site Internet), il aura la possibilité de passer une commande de « login » afin d'utiliser un profil moins restrictif lui permettant d'accéder à cette information.

7.6.2. Création du profil « Profs »

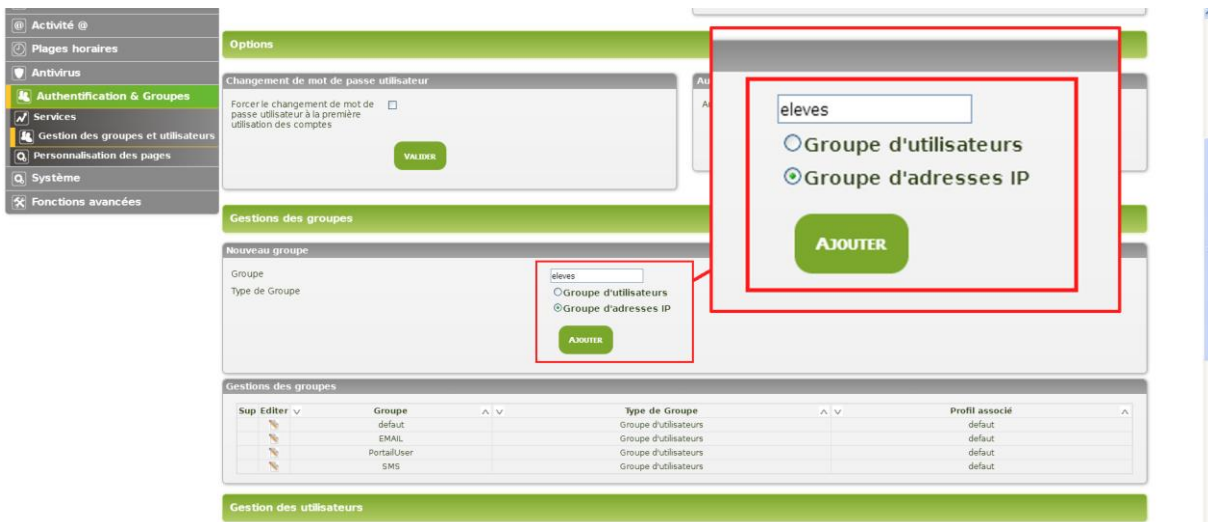
Dans l'onglet Profils de sécurité, créer le profil « Profs » :



CATÉGORIES		
Action	Catégories	Heures Ouvrées
	Smartphones	☐
	Liste blanche	☒
	Liste noire	☒
	Tous les sites Web Internet (HTTP/HTTPS)	☐
	HTTPS en mode SNI	☒
	HTTPS en mode proxy	☐
	Sites labellisés Arjel	☐
	Sites labellisés Hadopi	☐
	Jeux d'argent (Gambling)	☒
	Sites Audio Vidéo	☐
	Téléchargement de fichiers audio et video	☐
	Sites de téléchargement illégal (warez)	☒
	Réservés aux adultes	☐
	Filtre Safe Search pour les moteurs de recherche	☐
	Réservés aux adultes plus restrictif	☐
	Jeux-en-ligne	☐
	Sites de rencontres	☒
	Réseaux sociaux	☐
	Shopping	☐
	Sectes	☒
	Sites contenant des virus (hacking malware phishing)	☒
	Sites dangereux	☒
	Parfume	☐

7.6.3. Création du groupe Ip « élèves »

Dans l'onglet « Authentification et groupes » → sous onglet « Gestion des groupes et utilisateurs »,



The screenshot shows the 'Gestion des groupes et utilisateurs' section of the Frogi Secure interface. A sidebar on the left contains navigation links: 'Activité @', 'Plages horaires', 'Antivirus', 'Authentification & Groupes', 'Services', 'Gestion des groupes et utilisateurs' (highlighted), 'Personnalisation des pages', 'Système', and 'Fonctions avancées'. The main content area is divided into several sections. The 'Options' section includes a 'Changement de mot de passe utilisateur' form with a 'VALIDER' button. The 'Gestion des groupes' section contains a 'Nouveau groupe' form. In this form, the 'Groupe' field is set to 'eleves', and the 'Type de Groupe' is set to 'Groupe d'adresses IP'. An 'AJOUTER' button is visible. A red box highlights this 'AJOUTER' button. Below the 'Nouveau groupe' form is a table titled 'Gestions des groupes' with columns: 'Sup', 'Editer', 'Groupe', 'Type de Groupe', and 'Profil associé'. The table lists three groups: 'default', 'EMAIL', and 'PortalUser', all of type 'Groupe d'utilisateurs' and with 'default' profiles. At the bottom, there is a 'Gestion des utilisateurs' section.

Edition du groupe IP,

Authentification & Groupes
 Services
 Gestion des groupes et utilisateurs
 Personnalisation des pages
 Système
 Fonctions avancées

Forcer le changement de mot de passe utilisateur à la première utilisation des comptes ☐

VALIDER

Autoriser le multi-login ☐

VALIDER

Gestions des groupes

Nouveau groupe

Groupe

Type de Groupe

☒ Groupe d'utilisateurs
☐ Groupe d'adresses IP

AJOUTER

Gestions des groupes

Sup	Editer	Groupe	Type de Groupe	Profil associé
		default	Groupe d'utilisateurs	default
		eleves	Groupe d'adresses IP	default
		EMAIL	Groupe d'utilisateurs	default
		PortailUser	Groupe d'utilisateurs	default
		SMS	Groupe d'utilisateurs	default

Gestion des utilisateurs

Ajouter un utilisateur

Login

Groupe

Importer une liste d'utilisateurs

Importer la liste

Parcourir... Aucun fichier sélectionné.

Mappage de toutes les IP (0.0.0.0/0) associées au profil de sécurité « défaut »,

Gestions des groupes

Sup	Editer	Groupe	Type de Groupe	Profil associé
		default	Groupe d'utilisateurs	default
		eleves	IP 0.0.0.0 0 INCLUDE >>> <<< EXCLUDE IP(s) / réseau(x) associé(s)	default
		EMAIL	Groupe d'utilisateurs	default
		PortailUser	Groupe d'utilisateurs	default
		SMS	Groupe d'utilisateurs	default

Sauvegarde du paramétrage.

Gestions des groupes

Sup	Editer	Groupe	Type de Groupe	Profil associé
		default	Groupe d'utilisateurs	default
		eleves	IP 32 INCLUDE >>> <<< EXCLUDE IP(s) / réseau(x) associé(s)	default
		EMAIL	Groupe d'utilisateurs	default
		PortailUser	Groupe d'utilisateurs	default
		SMS	Groupe d'utilisateurs	default

7.6.4. Création du groupe d'utilisateurs « Profs »

Gestions des groupes

Nouveau groupe

Groupe: profs

Type de Groupe:

☒ Groupe d'utilisateurs

☐ Groupe d'adresses IP

AJOUTER

Gestions des groupes

Sup	Editer	Groupe	Type de Groupe
		default	Groupe d'utilisateurs
		eleves	Groupe d'adresses IP
		EMAIL	Groupe d'utilisateurs
		PortalUser	Groupe d'utilisateurs
		SMS	Groupe d'utilisateurs

Edition du groupe et liaison avec le profil associé « profs ».

Gestions des groupes

Sup	Editer	Groupe	Type de Groupe	Profil associé
		default	Groupe d'utilisateurs	default
		eleves	Groupe d'adresses IP	default
		EMAIL	Groupe d'utilisateurs	default
		PortalUser	Groupe d'utilisateurs	default

2

profs

1

profs

AJOUTER

<<< EXCLURE

INCLURE >>>

Utilisateur(s) existant(s)

Utilisateur(s) associé(s)

SMS

Groupe d'utilisateurs

default

7.6.5. Création de l'utilisateur « Prof »

Gestion des utilisateurs

Ajouter un utilisateur

Login

Groupe

profs

▼

Nom

Prénom

Mot de passe

Confirmation

Téléphone

Email

Droits

☐ Tableau de bord
 ☐ Filtres Web
 ☐ Listes N&B
 ☐ Activité @
 ☐ Plages horaires
 ☐ Antivirus
 ☐ Authentification & Groupes
 ☐ Système
 ☐ Fonctions avancées

Ajouter

Importer une liste d'utilisateurs

Importer la liste

Parcourir...

Aucun fichier sélectionné.

Ajouter

7.6.6. Activation des authentifications

Il faut activer les deux authentifications, celle par IP et la temporaire.
L'authentification par IP est prioritaire sur les autres authentifications.

- Tableau de bord
- Filtres Web
- Listes N&B
- Activité @
- Plages horaires
- Antivirus
- Authentification & Groupes**
- Services
- Gestion des groupes et utilisateurs
- Personnalisation des pages
- Système
- Fonctions avancées

Paramétrages des services

Activation des services

- Authentification par ip ☒
- Active Directory (AD) ☐
- Authentification serveur CAS ☐
- Authentification temporaire ☒
- Authentification permanente ☐
- Page d'accueil ☐
- Aucune authentification ☐

VALIDER

Activation des services

Déconnexion automatique après x 15 minutes d'inactivité

VALIDER

Page de redirection

(Redirection : http://www.google.fr)

VALIDER

Menu de navigation ☐

VALIDER

Portail SMS / Email

Activation du portail

- Portail SMS ☐
- Portail Email ☐
- Portail utilisateur ☐
- Aucun portail ☒

VALIDER

Paramètres service

Etat Aucun portail

Cas du multi login

Vous pouvez autoriser plusieurs authentifications simultanées pour un même utilisateur.

7.6.7. Connexion au profil « Profs »

<http://login.frogi-secure.com>.



The screenshot shows the login interface for Frogi-Secure. At the top, the logo consists of a green circle with a white keyhole icon, followed by the text 'FROGI-SECURE' in bold green and 'Contrôle et protection des accès Internet' in smaller black text. Below this, the word 'AUTHENTIFICATION' is centered in red. There are two input fields: 'utilisateur:' and 'mot de passe:', each followed by a white rectangular box with a green border. A green button with the text 'CONNEXION' is positioned below the password field. At the bottom, there is a link 'Demande de codes d'accès | Mot de passe oublié' in green. A small footer at the very bottom reads 'Frogi-Secure - 2018 - © Tous droits réservés'.

7.6.8. Déconnexion du profil « Profs »

La déconnexion peut être automatique, telle que définie dans l'onglet « Authentification et Groupes », ou manuelle en se connectant à l'Url : <http://logout.frogi-secure.com>.

