SIS EVOLUTION

GUIDE UTILISATEUR

SFR BUSINESS
Libérons l'énergie d'entreprendre

Révision			
Version	Date	Auteur	Commentaires
1.0	06/02/2017	NAKT	Création du document
1.2	05/05/2017	FLJO, DIMA	Modification de l'install policy
1.3	12/05/2017	JEMI	
1.4	19/05/2017	TOMA	Modifications et ajouts globaux
1.4	09/06/2017	NAKT	Création d'une règle de flux entrante
1.5	29/06/2017	TOMA	
1.6	17/01/2018	NAKT	Mise à jour > 4.3 Routage et VPN IPSec

NB : Vous pouvez télécharger la dernière version de ce document sur https://sisevolution.sfrbusiness.com/docclient/

CONFIDENTIALITE

SFR Business et les membres de son personnel s'engagent à respecter les contraintes de sécurité et de confidentialité de ces clients dans le cadre de SIS Evolution.

SFR Business et les intervenants s'engagent à considérer comme strictement confidentiel tant au sein de sa propre organisation que vis à vis de tiers, les informations, documents de toute nature et savoir-faire, qui lui seront transmis par le client dans le cadre du projet.

Cet engagement vaut quel que soit le support utilisé pour cette transmission ou simplement les informations que SFR Business aura pu obtenir ou eu connaissance au titre de la prestation. A cet effet, SFR Business ne communiquera ces informations qu'aux personnes affectées à l'exécution de la prestation.

SFR Business s'engage à ne pas utiliser les informations directement ou indirectement en tout ou partie, à quelque fin que ce soit en dehors de l'exécution de la prestation décrite dans le présent document.

SOMMAIRE DU DOCUMENT

1 INTRODUCTION

1.1 Objectifs du document

Ce document, à destination des clients SIS Evolution, a pour but de décrire le fonctionnement des principaux aspects de la solution, dans l'objectif de leur donner l'autonomie nécessaire à l'administration.

1.2 Architecture de base de SIS Evolution

La solution SIS Evolution est constituée de deux éléments fondamentaux :

- Un pare-feu « Fortigate » : il est hébergé dans vos locaux (offre Connect), ou bien dans un de nos Datacenter SFR (offre IPNET)

- Un portail de configuration SIS Evolution, qui vous permet d'administrer la politique de sécurité de l'ensemble des pare-feu auxquels vous avez souscrits.

Vous devez réaliser l'administration de votre pare-feu SIS Evolution exclusivement depuis le Portail SIS Evolution.

Le Portail SIS Evolution permet d'administrer, entres autres :

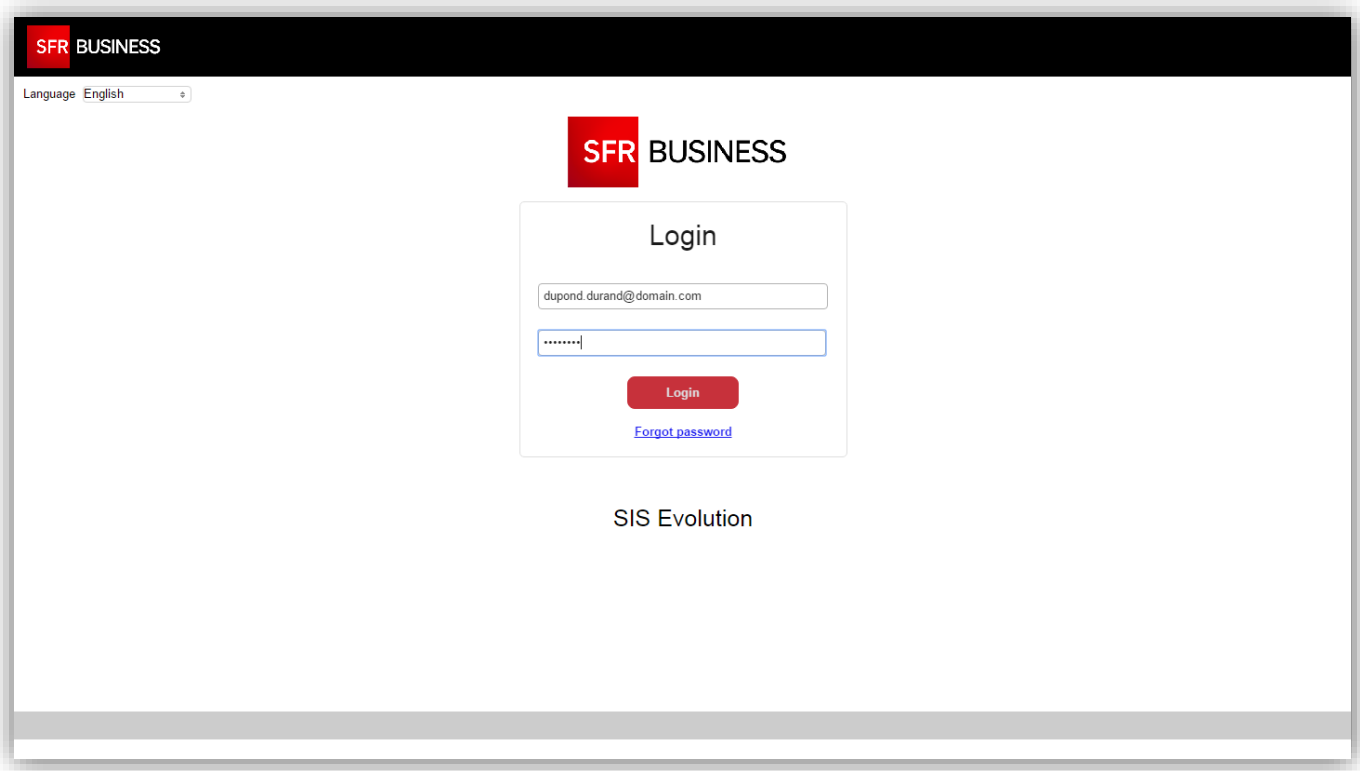
- La politique de filtrage du pare-feu
- La gestion des comptes utilisateurs
- La gestion des tunnels IPSEC site à site
- La gestion des VPN SSL

A la date de rédaction de ce document, les fonctionnalités d'administration IPSEC et SSL ne sont pas encore disponibles.

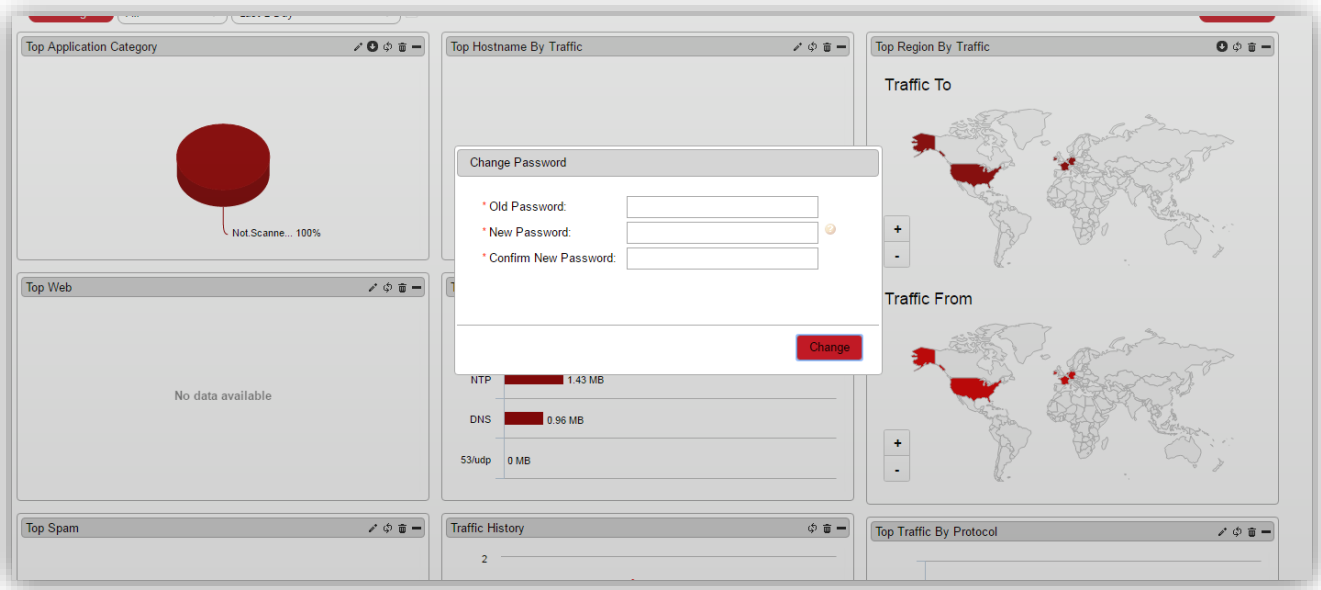
2 INTERFACE PORTAIL SIS EVOLUTION

2.1 Première connexion au portail SIS Evolution

Lors de la première connexion au Portail SIS Evolution, vous devez changer le mot de passe fourni par SFR Business, pour cela connectez-vous sur https://sisevolution.sfrbusiness.com avec le login/password fournis par SFR Business.

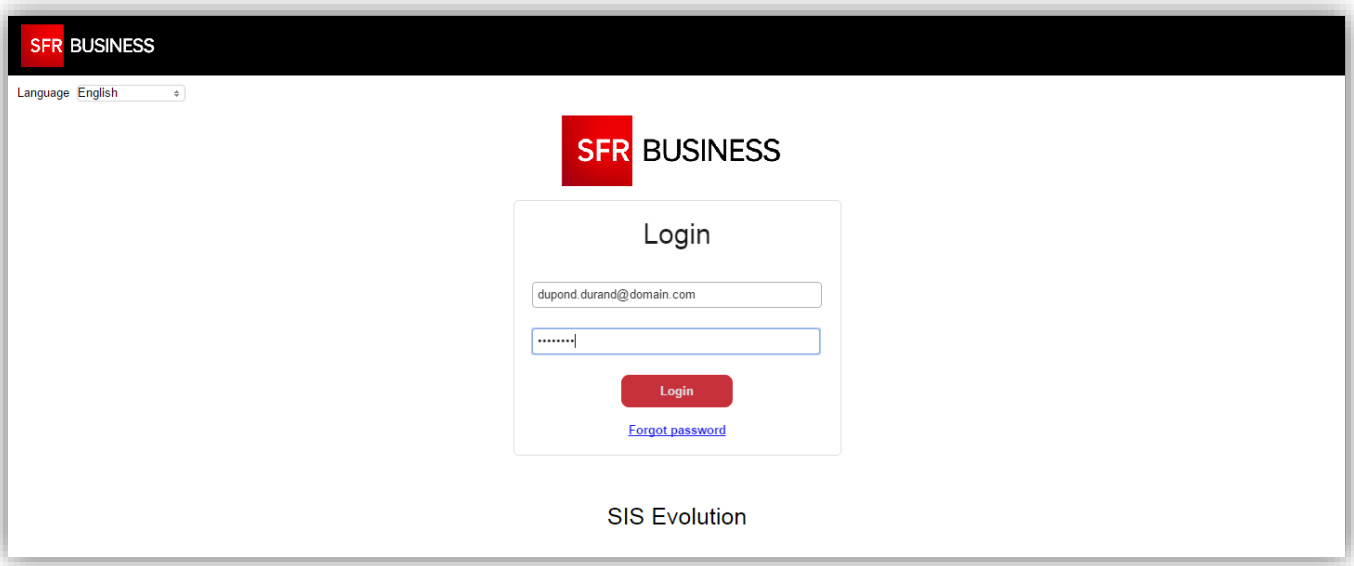


Ensuite laissez-vous guider et renseignez l'ancien mot de passe, puis le nouveau et validez :

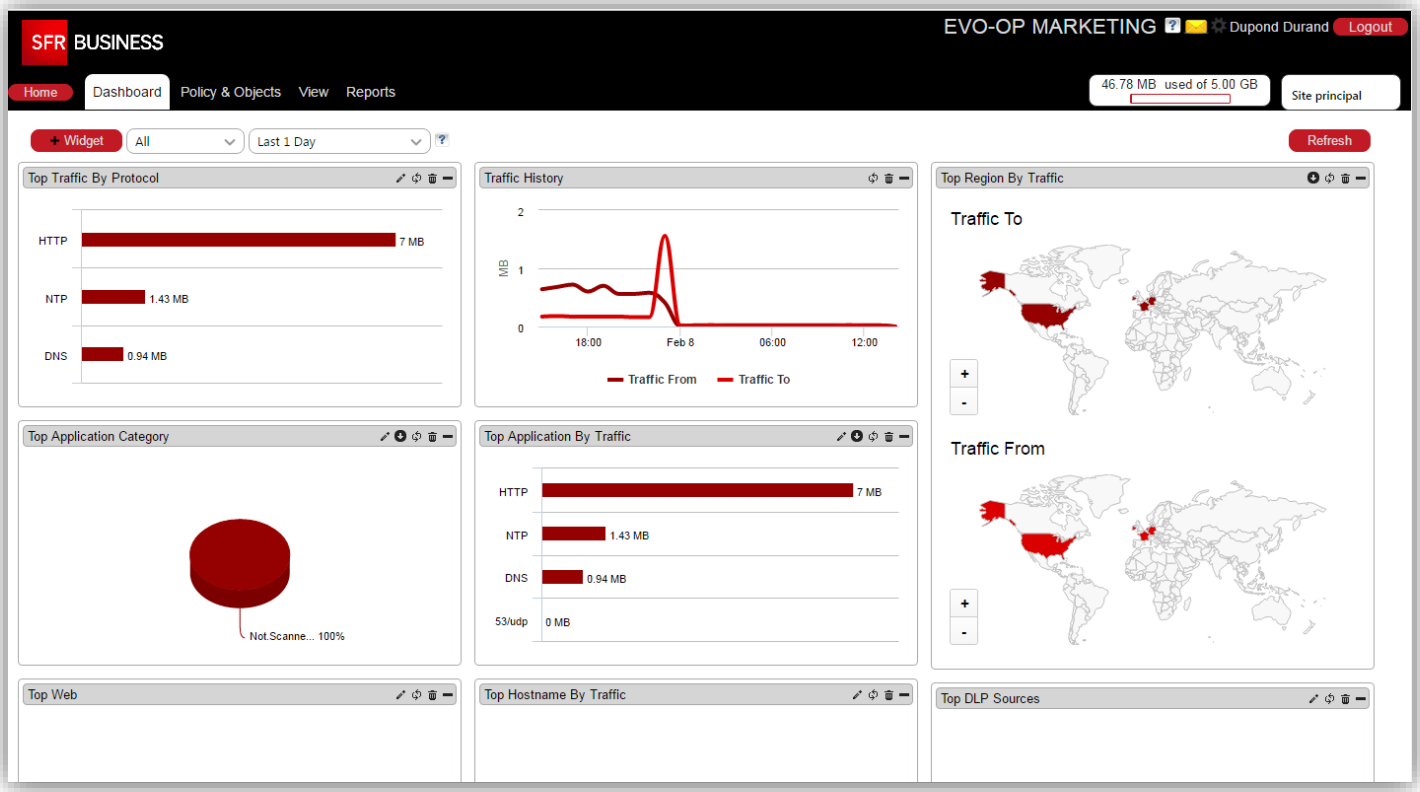


2.2 Connection au portail SIS Evolution

Pour accéder à l'interface Portail SIS Evolution, connectez-vous à : https://sisevolution.sfrbusiness.com

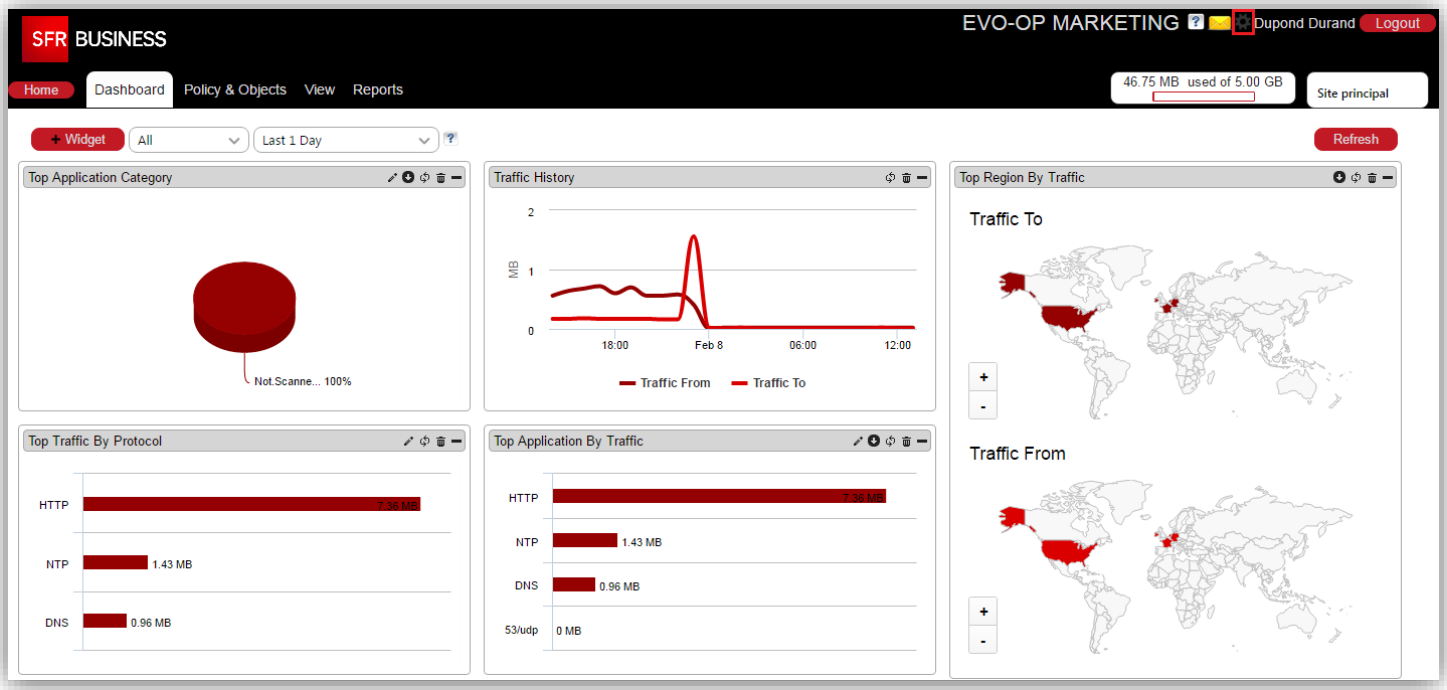


Une fois connecté vous arrivez dans le menu « **Dashboard** » ; vous permettant de visualiser de façon ergonomique vos journaux de connexion indexés :

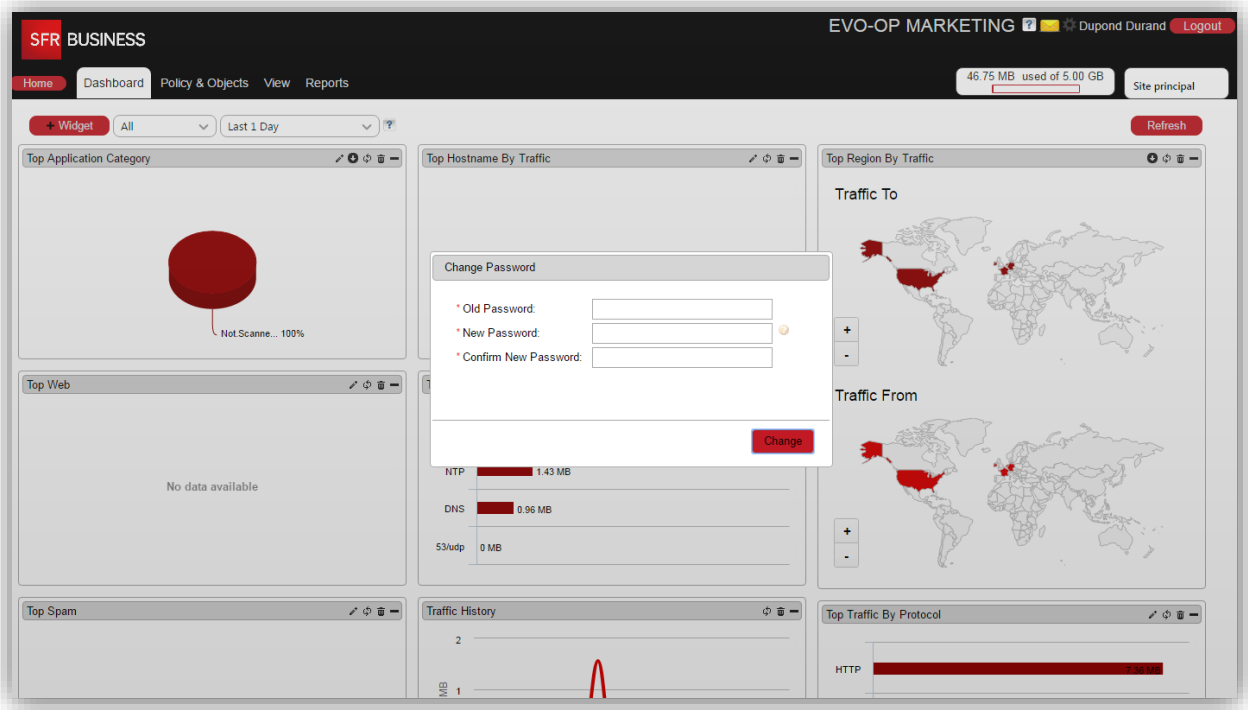


2.3 Changement du mot de passe du compte Portail SIS Evolution

Pour changer le mot de passe, il suffit de cliquer sur le bouton marqué en rouge sur la capture d'écran suivante (voir en haut à droite de l'interface) :



Ensuite laissez-vous guider : renseignez l'ancien mot de passe, puis le nouveau et validez.



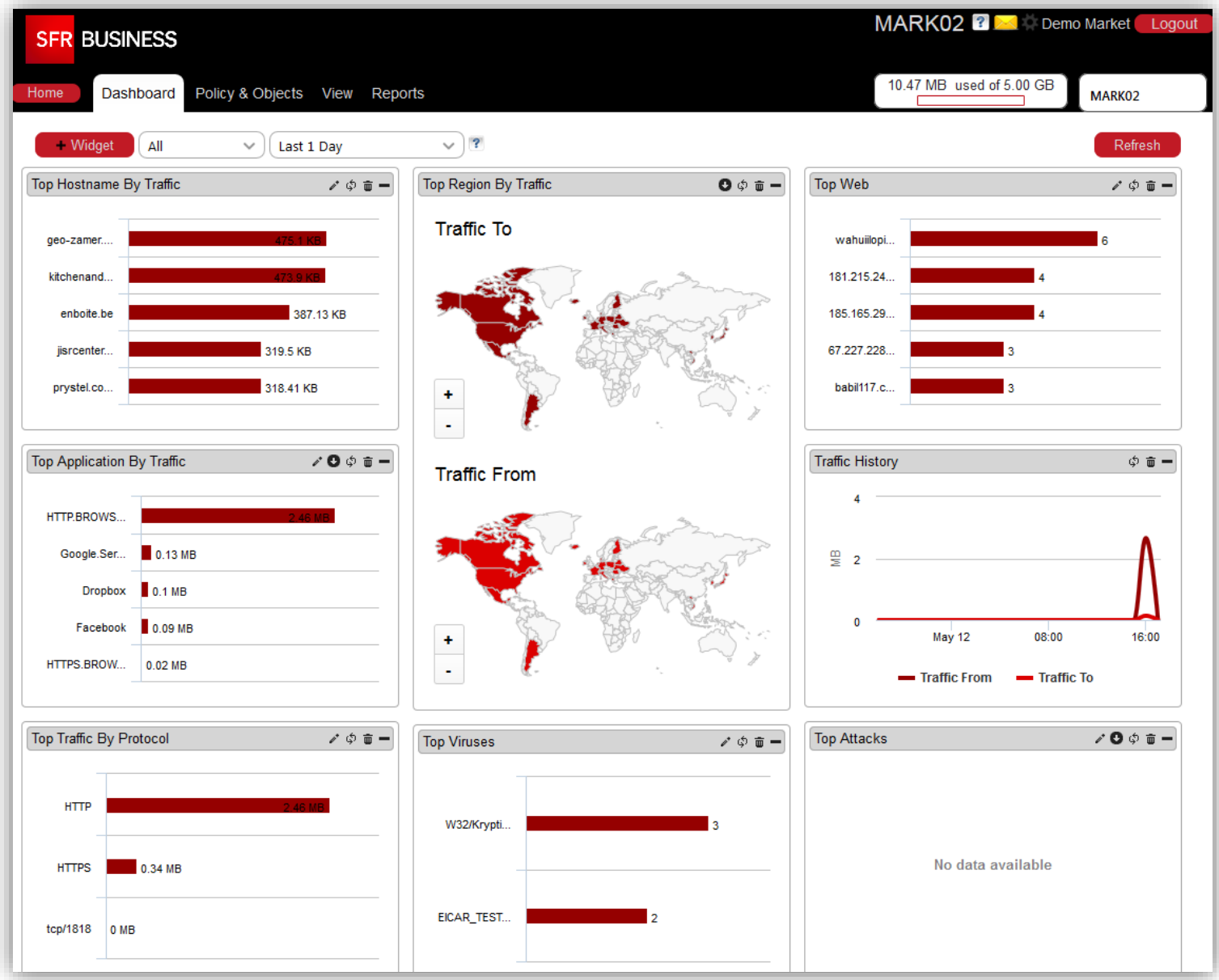
2.4 Contenu de l'interface

2.4.1 Le Dashboard

Le Dashboard vous permet de d'avoir une vue d'ensemble sur votre trafic à l'aide de widgets, comme :

- Top des sites visités
- Top des applications
- Top des protocoles
- Historique du trafic
- …

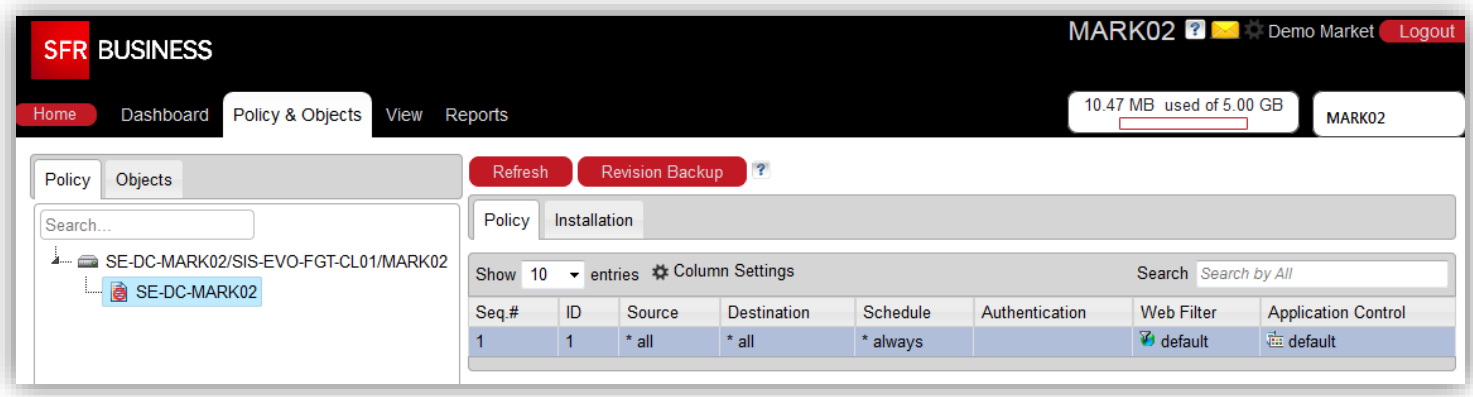
Il est possible de personnaliser cette interface :



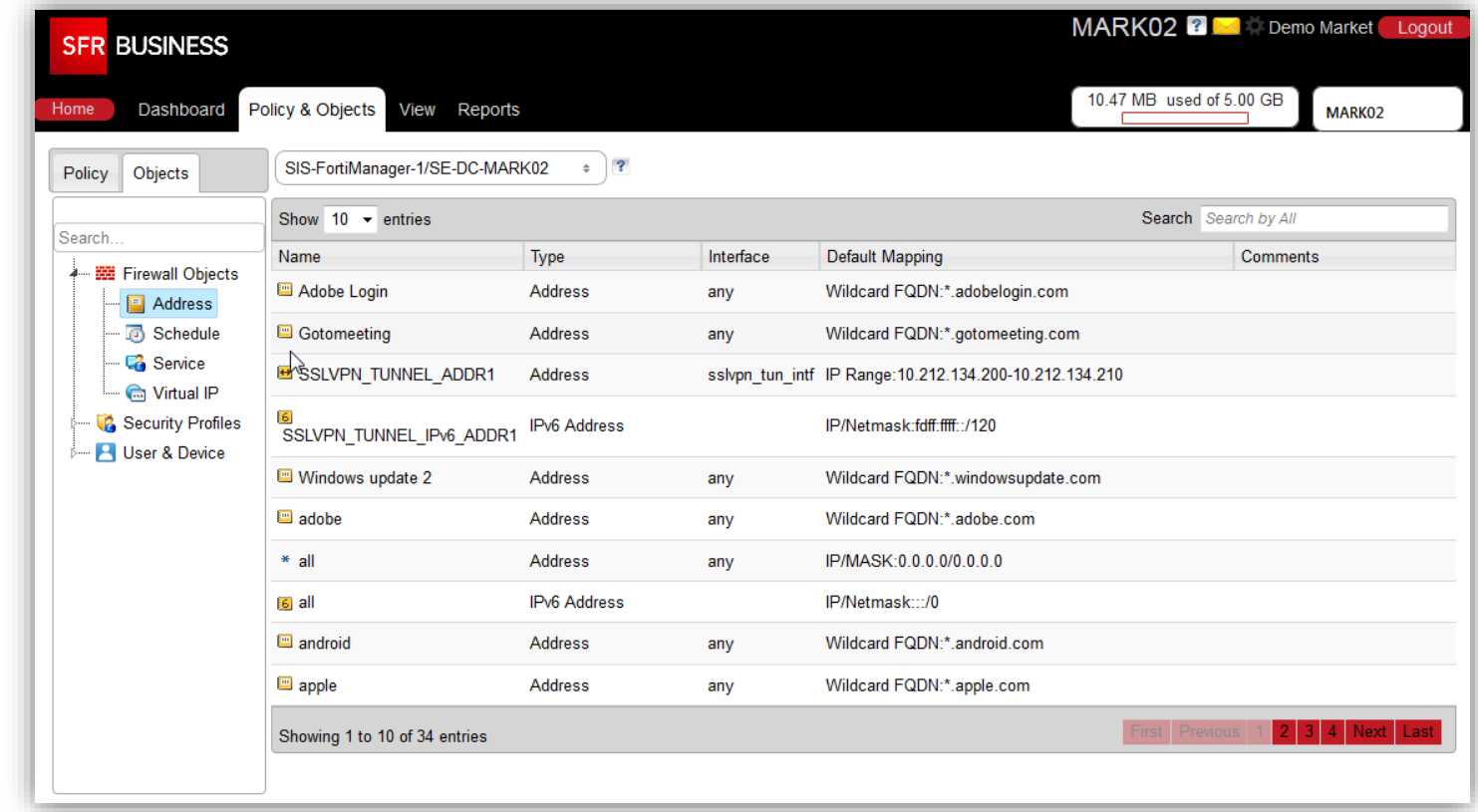
2.4.2 Policy & Objects

Cette vue est constituée de deux sous-onglets :

- Policy : permet de voir, configurer et appliquer la politique de sécurité :



- Objects : permet de créer les objets qui seront utilisés pour construire la politique de sécurité (sites web autorisés, serveurs, applications, comptes utilisateurs, …) :



2.4.3 View

Cet onglet permet d'accéder à l'ensemble des journaux de connexions.

2.4.4 Reports

Cet onglet permet de créer des rapports d'activité du pare-feu. Ils sont basés sur des éléments similaires au Dashboard, et sur une période de temps configurable. Les rapports basiques peuvent être extraits du Portail SIS Evolution, et des rapports plus complexes ou sur des périodes plus longues peuvent être extraits du FortiAnalyzer.

3 FONCTIONNEMENT DU FILTRAGE SUR VOTRE PARE-FEU SIS EVOLUTION

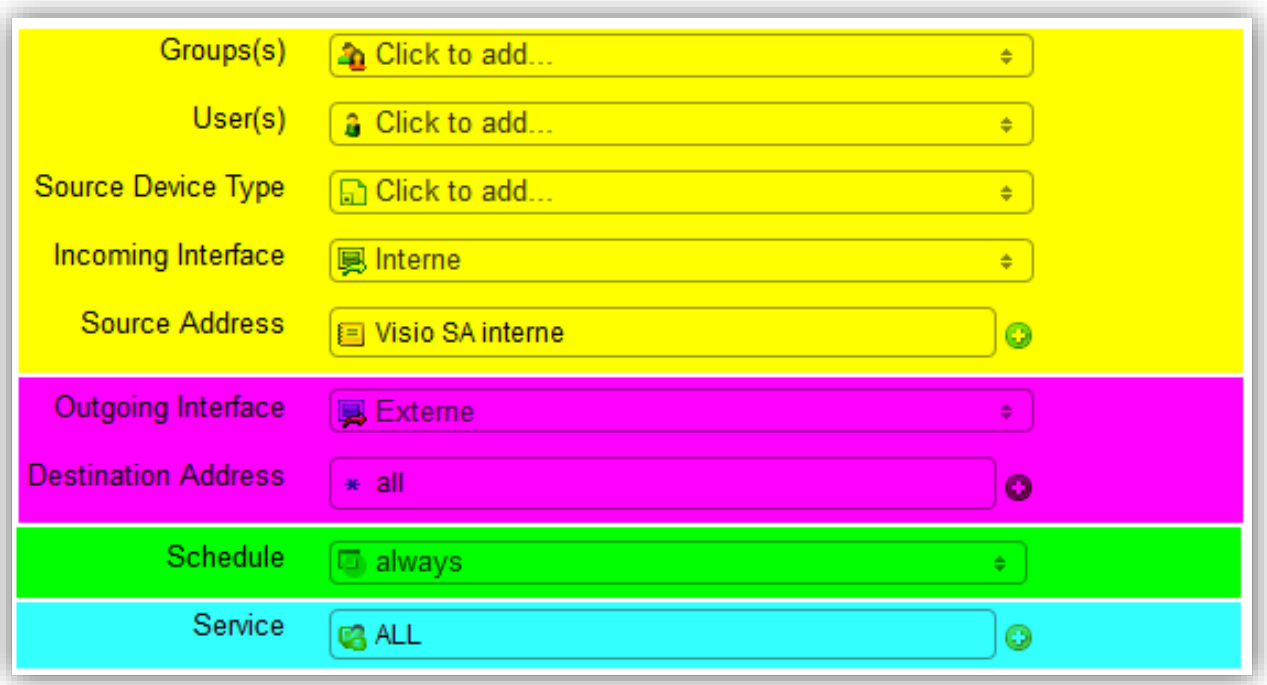
3.1 Fonctionnement

Votre pare-feu SIS Evolution applique une politique de sécurité que vous avez préalablement définie sur le Portail SIS Evolution.

La politique est constituée de plusieurs règles de sécurité permettant de définir comment le pare-feu doit réagir en fonction de tel ou tel flux.

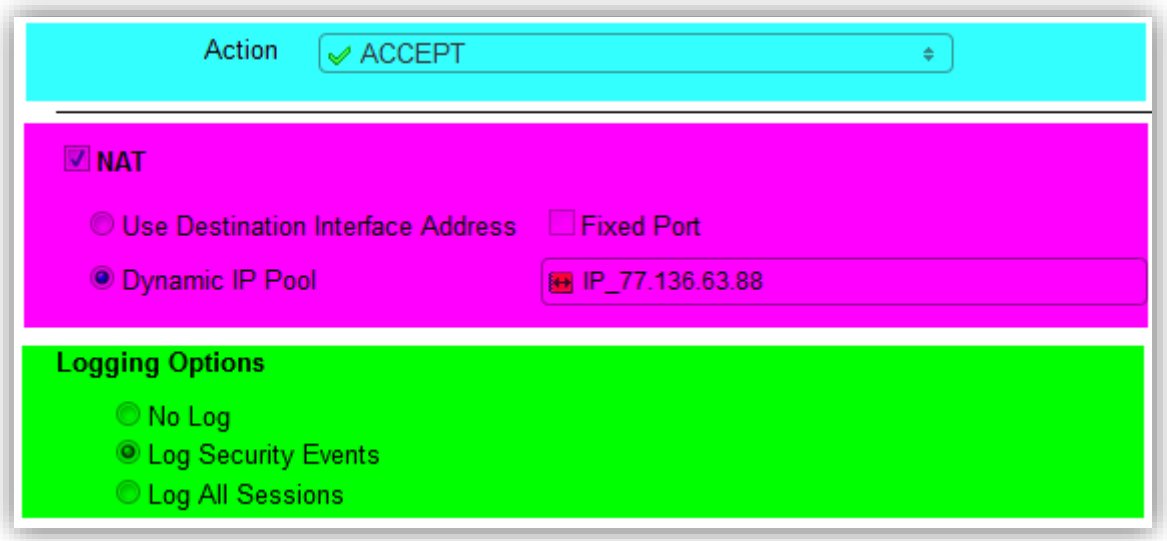
Un flux et une règle de filtrage est caractérisé selon 4 composantes fondamentales :

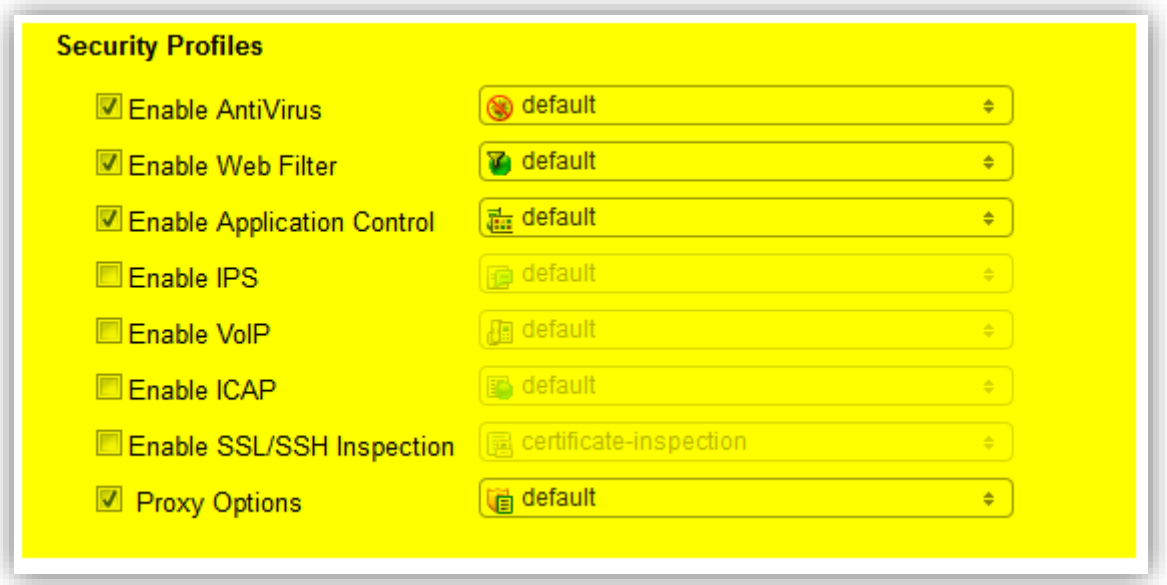
- D'où vient le flux (utilisateur, ordinateur source, IP source…)
- Où va le flux (serveur distant, IP destination)
- Quand (date et heure d'Europe/Paris)
- Quel service (http, https, ftp, …)



Ensuite, si un flux traversant le pare-feu répond à l'ensemble de ses critères ci-dessus, les actions résultantes sont appliquées :

- Flux autorisé ou bloqué
- Règle de Source NAT à appliquer (IP publique de sortie à utiliser)
- Politique de journalisation et traçabilité (logs)
- Profils de sécurité à appliquer
  - Politique de filtrage antivirus
  - Politique de filtrage web par catégories (Réseaux sociaux, pornographie, …)
  - Politique de filtrage des applications (Skype, Spotify, …)





Pour chaque flux reçu, le pare-feu va parcourir l'ensemble des règles et appliquer la première qui correspond aux critères de sélection. Il ne continuera pas à parcourir les règles ; par conséquent, les règles les plus « spécifiques » devront être placées en premier, et les plus « larges » en dernier, faute de quoi les règles « larges » seront susceptibles de superposer aux règles « spécifiques ».

Si le flux ne correspond à aucune règle, il est par défaut bloqué.

Il n'est pas nécessaire d'écrire les règles dans les deux sens. En effet votre pare-feu SIS Evolution est de type « Stateful », ce qui signifie qu'il est capable de tracer les flux « retour ». En d'autres termes, il faut écrire la règle dans le sens où le flux est initié uniquement.

3.2 Application de la politique

La configuration que vous créez sur le Portail SIS Evolution n'est pas appliquée instantanément sur votre pare-feu. En effet, il est nécessaire de « pousser » la configuration sur le boitier dès que vous avez terminé toutes vos modifications va l'onglet « **installation** ».

4 EXEMPLES DE CONFIGURATION PAS A PAS

4.1 Création d'une règle de flux sortante

4.1.1 Cas d'école

Cet exemple va vous présenter comment créer une règle autorisant le sous réseau interne (192.168.1.0/24) à accéder à Internet sur les ports HTTPS, HTTP, FTP, DNS et TCP/4242.

Nous y appliquerons un filtre antivirus par défaut, un filtre web avec une politique bloquant certaines catégories de sites, et un filtre applicatif bloquant le peer-to-peer et les botnets.

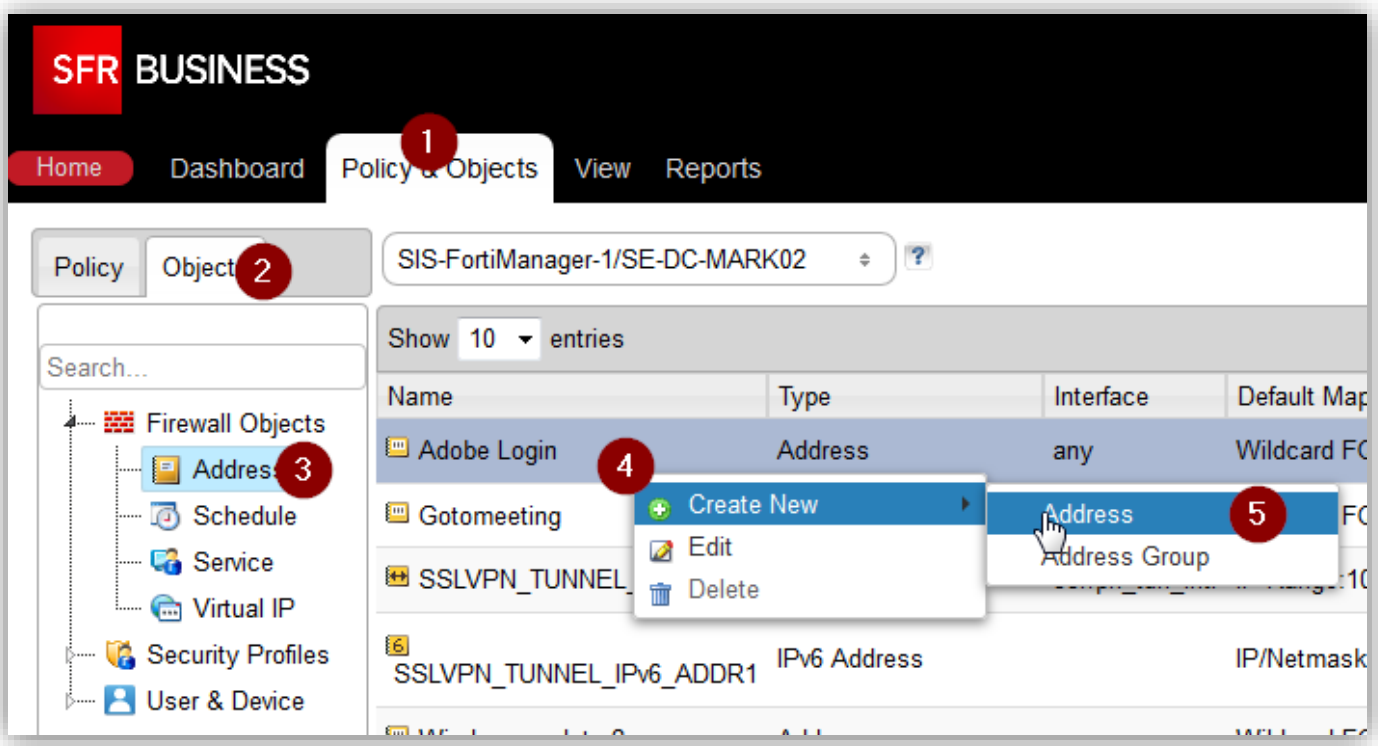
4.1.2 Création des objets « firewall »

On commence tout d'abord par créer les objets dont nous avons besoin. Les objets nécessaires sont :

- Un objet address « Réseau Interne » pointant sur 192.168.1.0/255.255.255.0
- Un objet service « TCP-4242 » pour le service réseau sur le port TCP/4242
- Un groupe d'objets services regroupant les ports HTTPS, HTTP, FTP, DNS et TCP/4242.

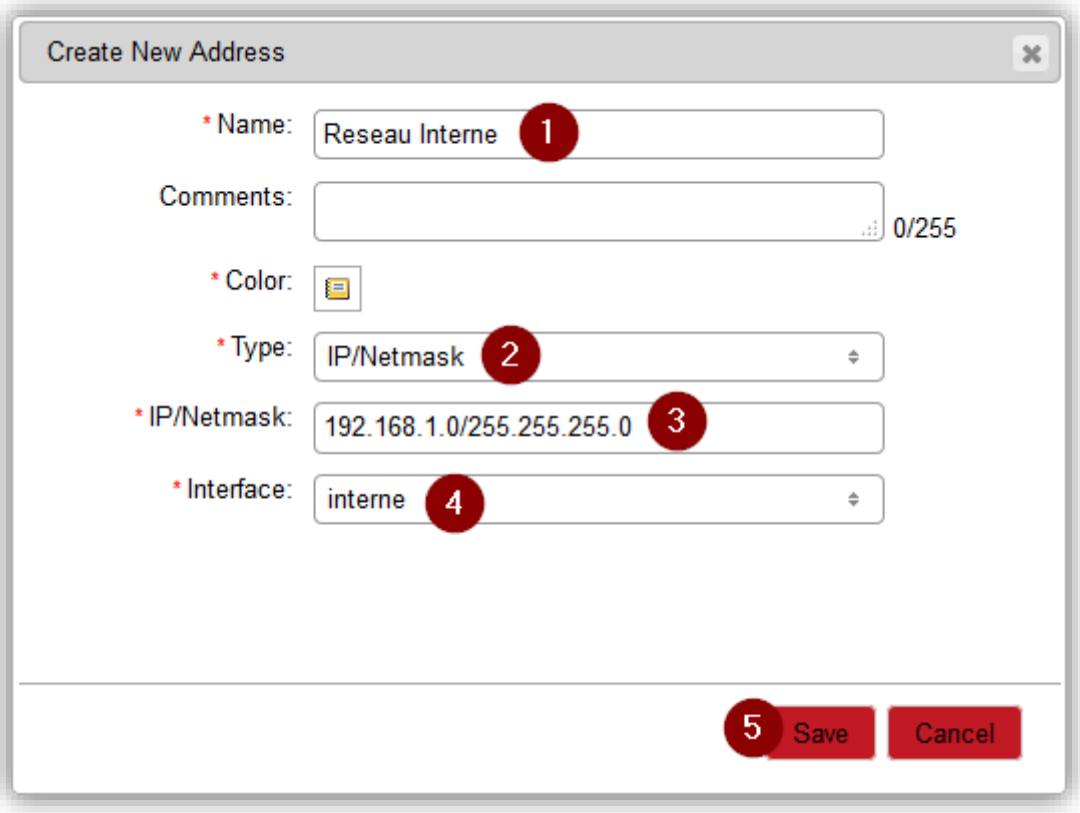
On commence par aller dans l'onglet « **Policy & Objects** » du Portail SIS Evolution, puis sur l'onglet « **Objects** » et enfin en cliquant sur « **Address** »

On effectue un clic droit sur la zone des objets et on fait « **Create new > Address** » :

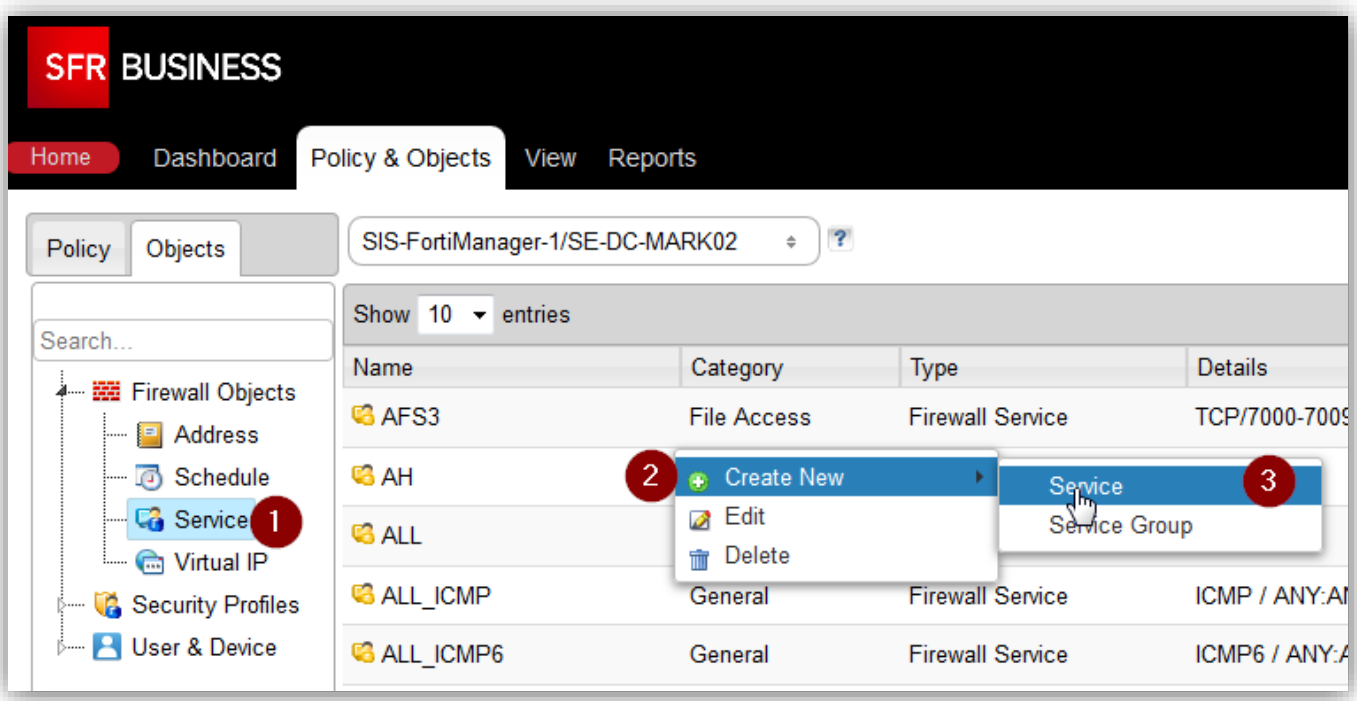


On saisit le nom de l'objet, le type de l'objet « **IP/Netmask** », on saisit le sous réseau interne, et l'interface attachée.

On valide par « **Save** » :

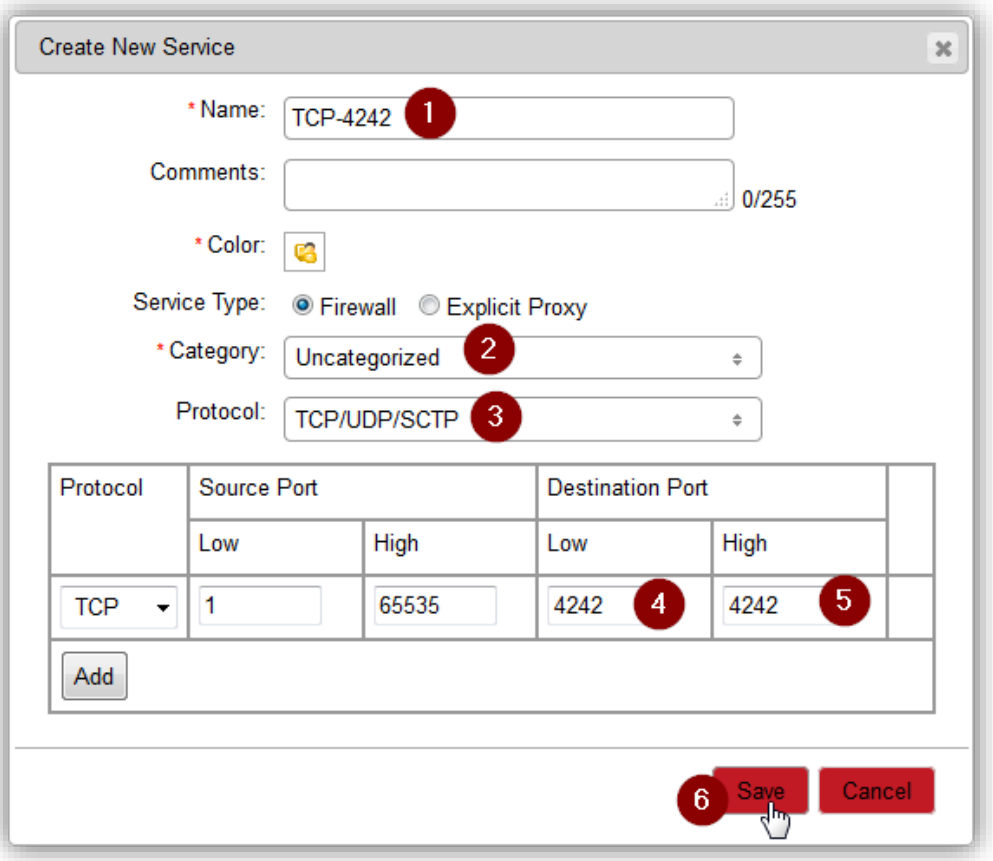


On se rend ensuite dans le menu « **Service** », et on fait un clic droit dans la zone des objets, puis « **Create New > Service** »

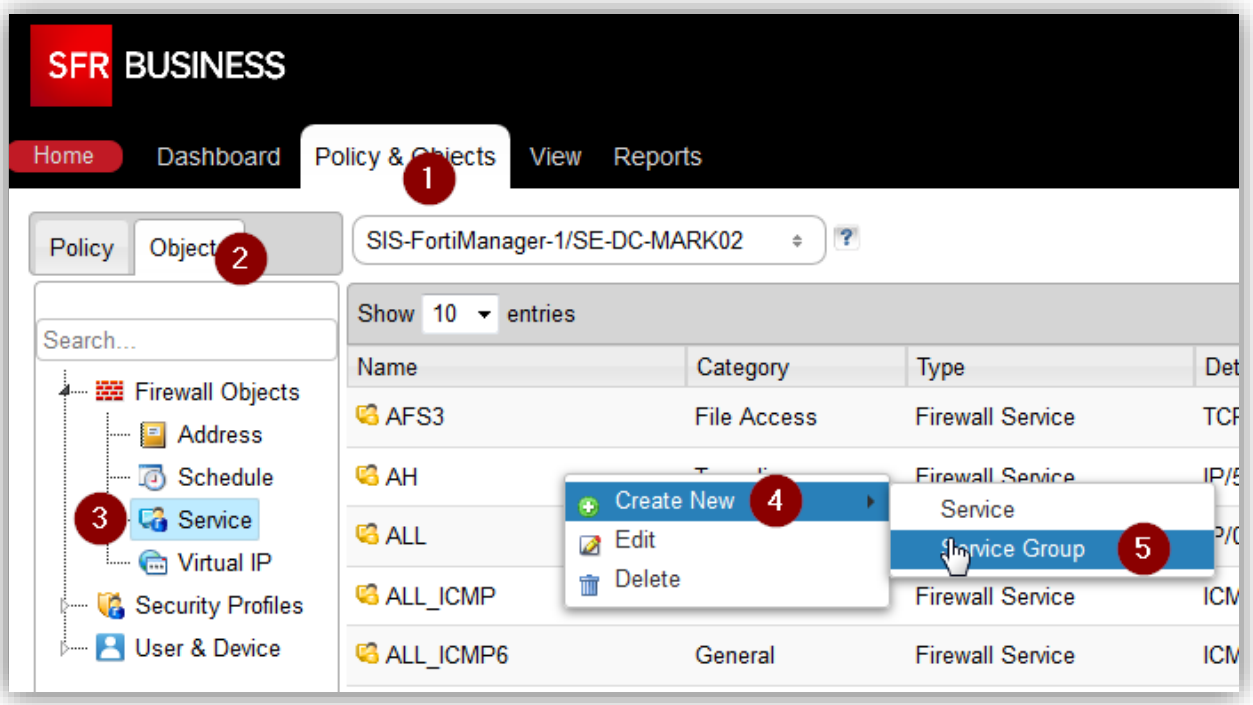


On renseigne ensuite le nom du service, on renseigne éventuellement sa catégorie, puis on renseigne le protocole, et la plage de ports de destination. Dans notre cas, ce sera une plage de 1 seul port.

On valide par « **Save** »

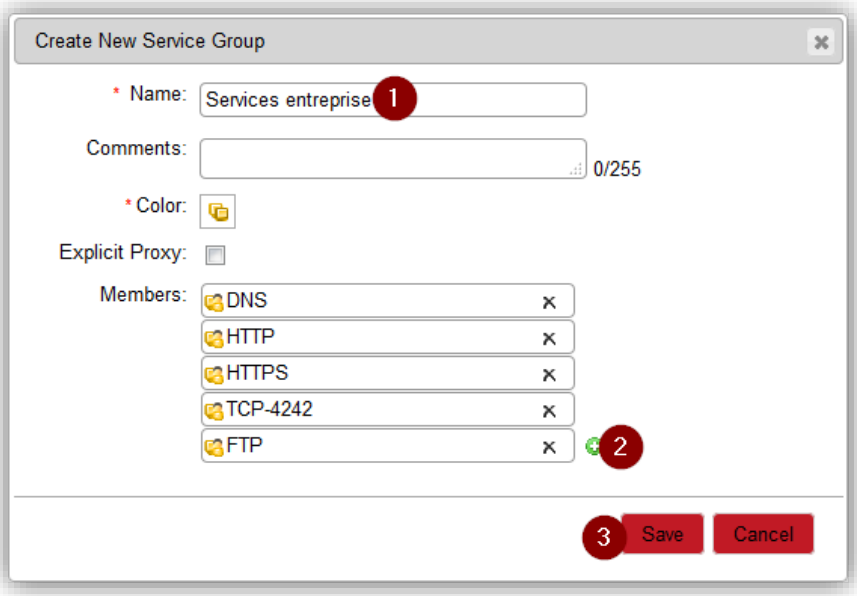


Il nous reste à créer le groupe de services en suivant la même logique :



Ensuite, nommer le groupe, puis cliquer sur le « + » vert, pour sélectionner les services. Il est possible d'en sélectionner plusieurs d'un coup.

Enfin, valider par « Save »

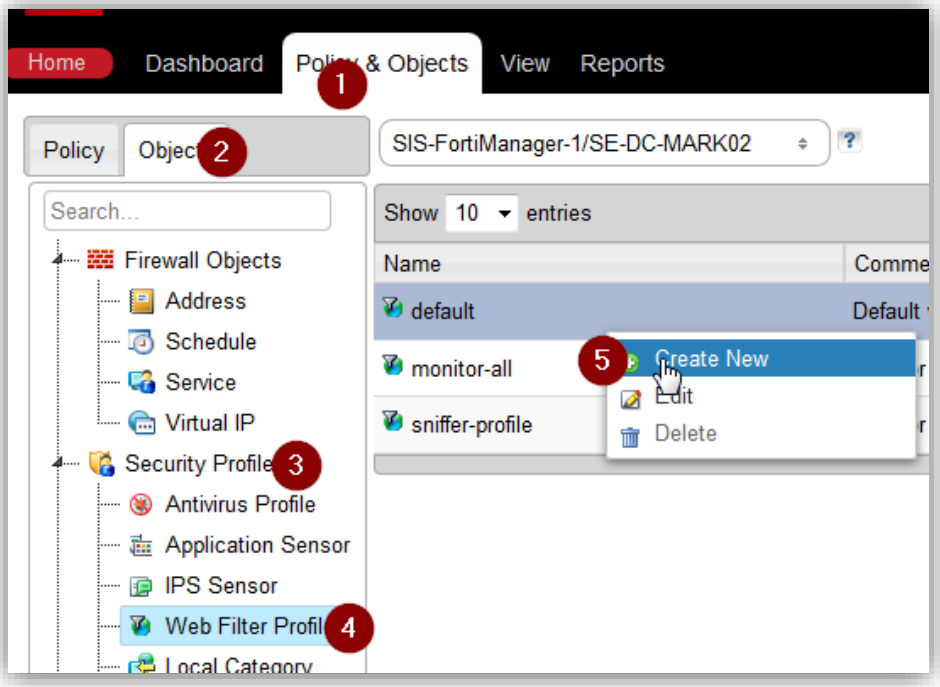


4.1.3 Création des objets « security profiles »

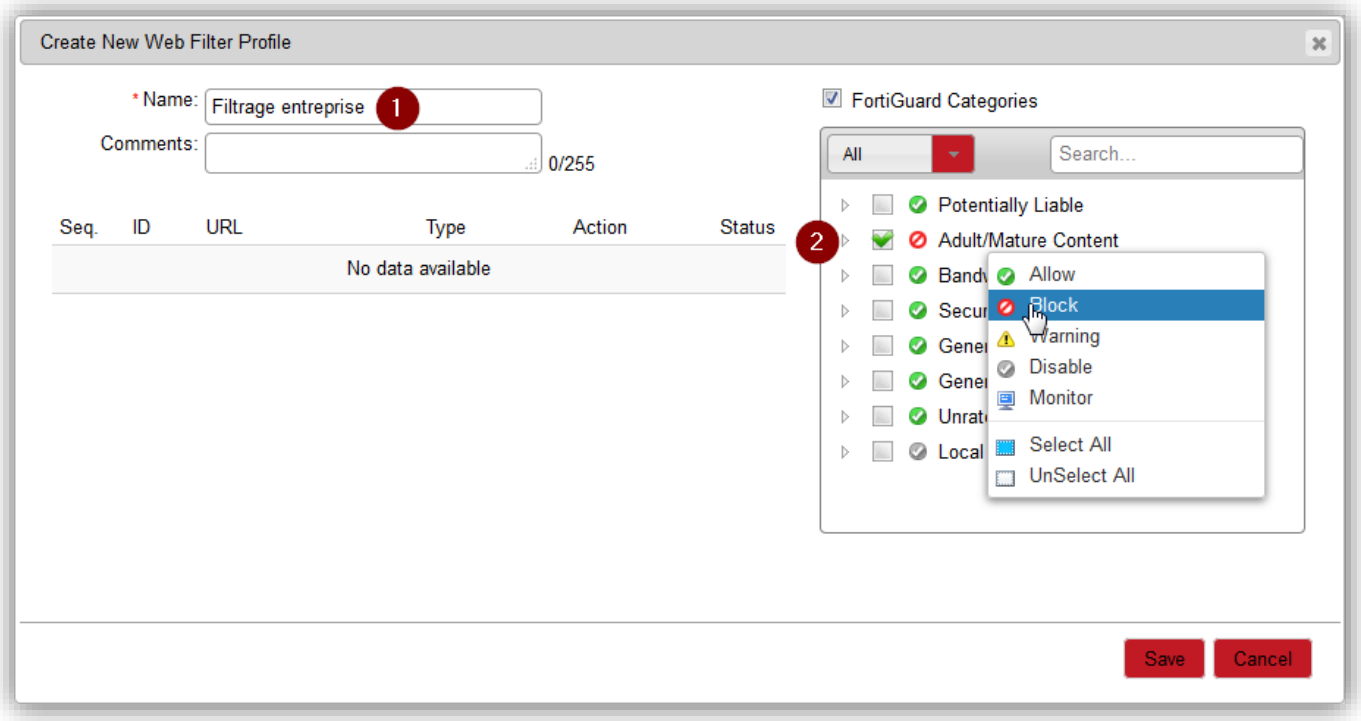
Dans notre exemple, nous utilisons la politique antivirus par défaut, mais nous allons créer :

- Un filtre web avec une politique bloquant certaines catégories de sites,
- un filtre applicatif bloquant le peer-to-peer et les botnets

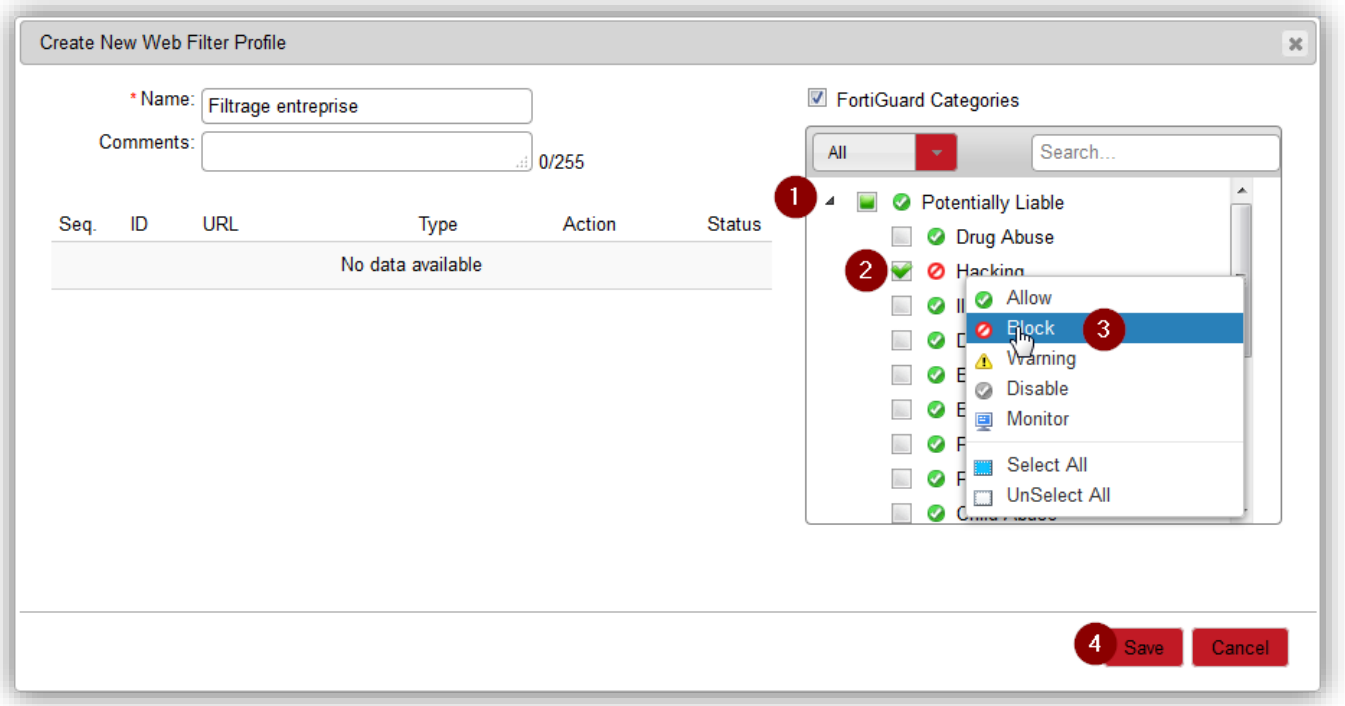
On commence par aller dans le menu « Security Profiles > Web Filter Profile » puis on fait un clic droit puis « **Create New** »



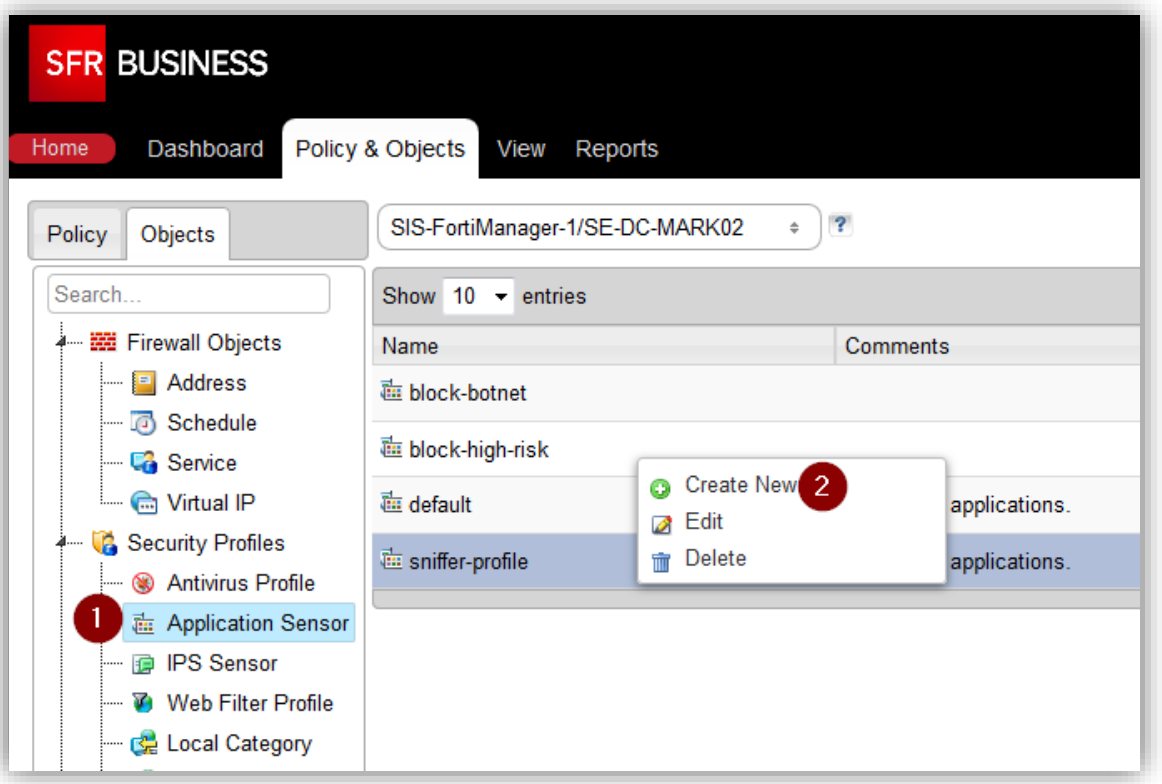
Nous allons bloquer tous les sites « adultes », et bloquer également les sites de « Hacking ». On commence par nommer notre politique. Ensuite, on coche la métacatégorie « **Adult / Mature Content** », puis on fait un clic droit puis « **Block** ».



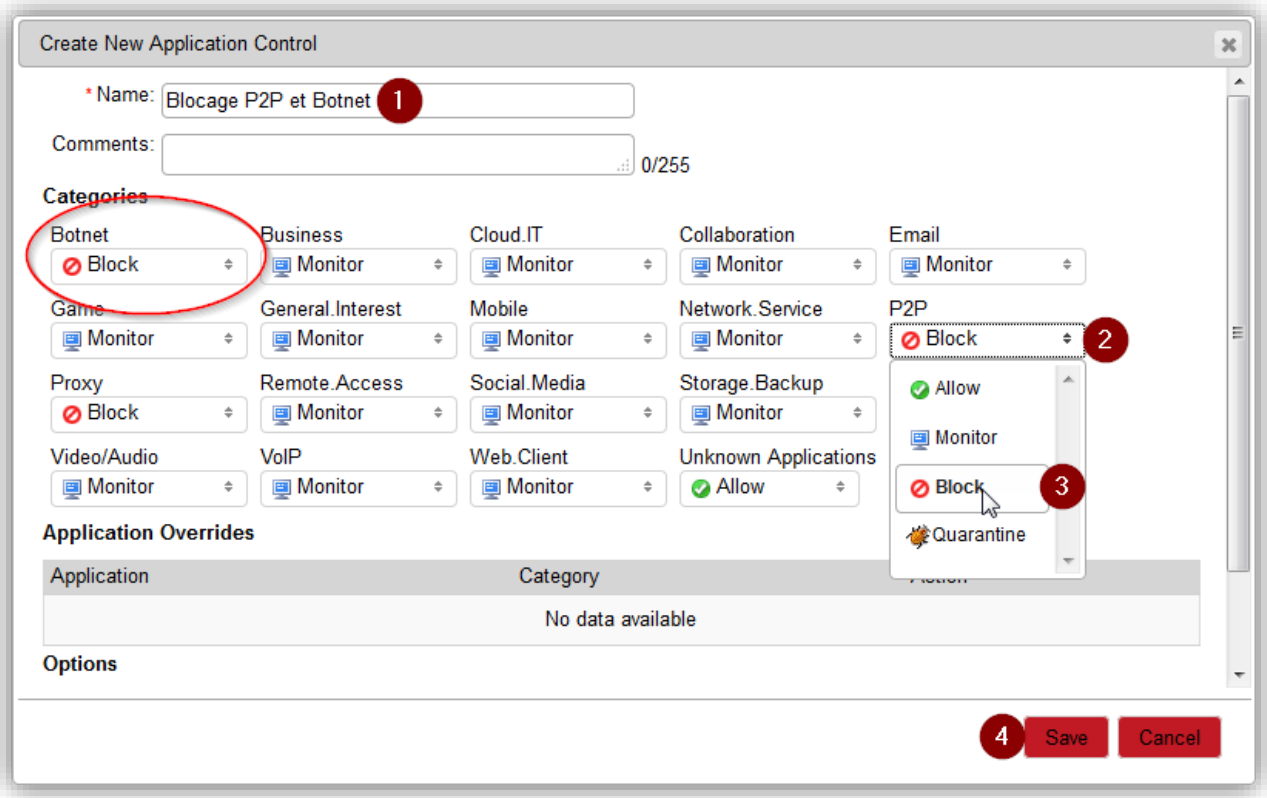
Pour bloquer les sites de « Hacking », il s'agit d'une sous-partie de la métacatégorie « **Potentially Liable** ». On déroule la catégorie pour laisser apparaitre les « sous catégories », dont « **Hacking** ». Cocher « **Hacking** », puis faire un clic droit puis « Block ». Valider notre profil par « **Save** »



Cliquer sur le menu « **Security Profile > Application Sensor** », puis faire un clic droit dans la liste, puis « **Create New** »



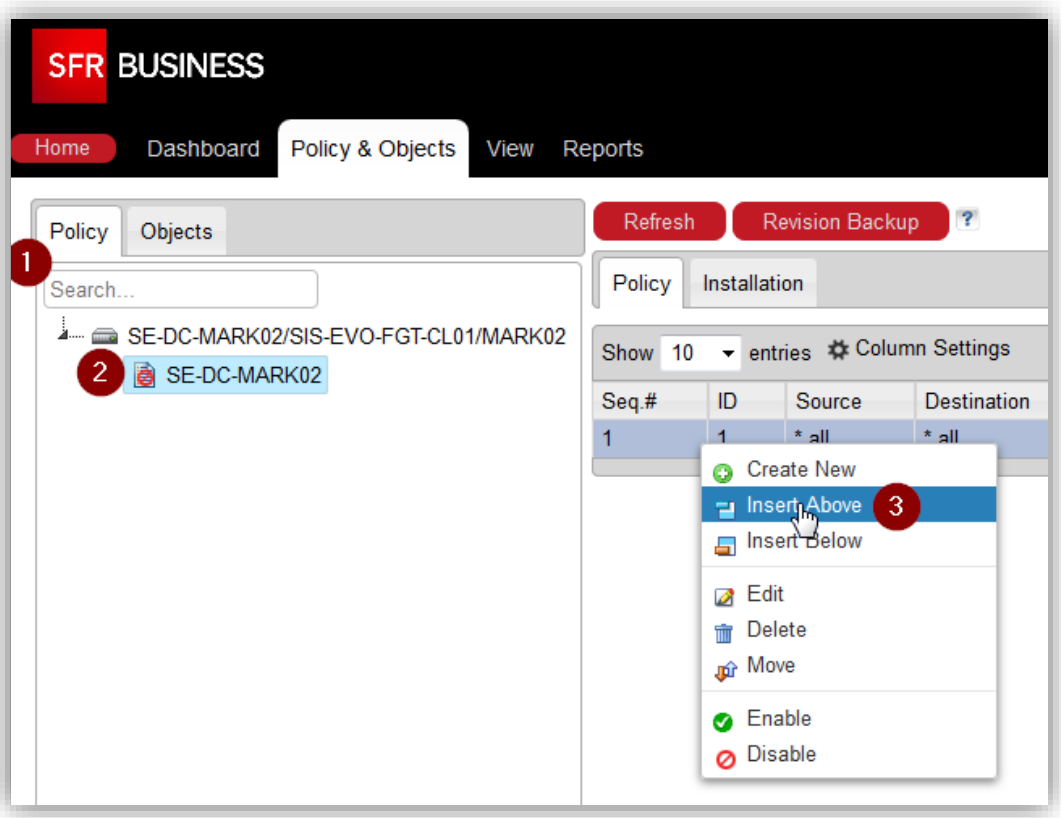
On commence par nommer notre objet. Les botnets sont déjà bloqués par défaut, mais ce n'est pas le cas du P2P. Cliquer sur la rubrique « P2P » et sélectionner « Block ». Valider par « Save »



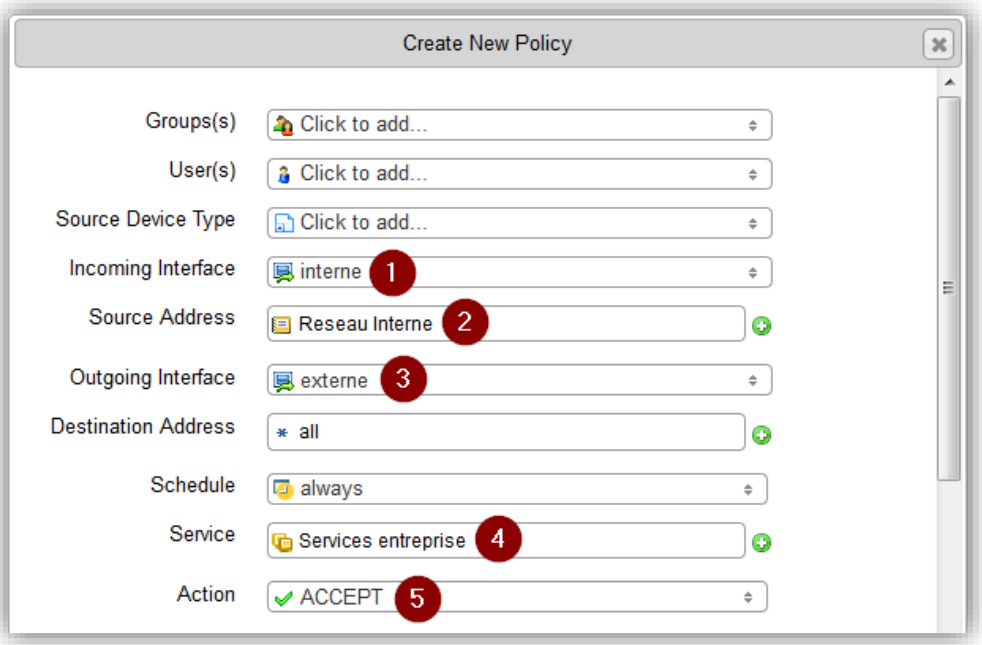
4.1.4 Création de la règle de pare-feu

La création de la règle de pare-feu se fait en retournant dans l'onglet « **Policy** », puis en cliquant sur la politique de sécurité.

Dans la liste des règles, faire un clic droit puis « **Insert Above** »

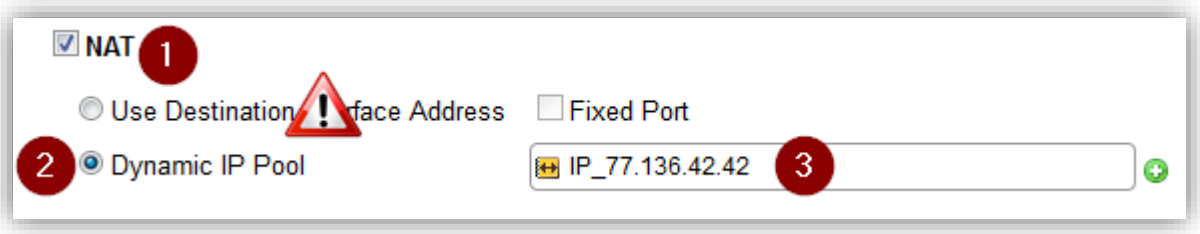


On sélectionne les conditions de notre règle, en utilisant les objets préalablement créés et on choisit une action « Accept » pour que le flux soit autorisé



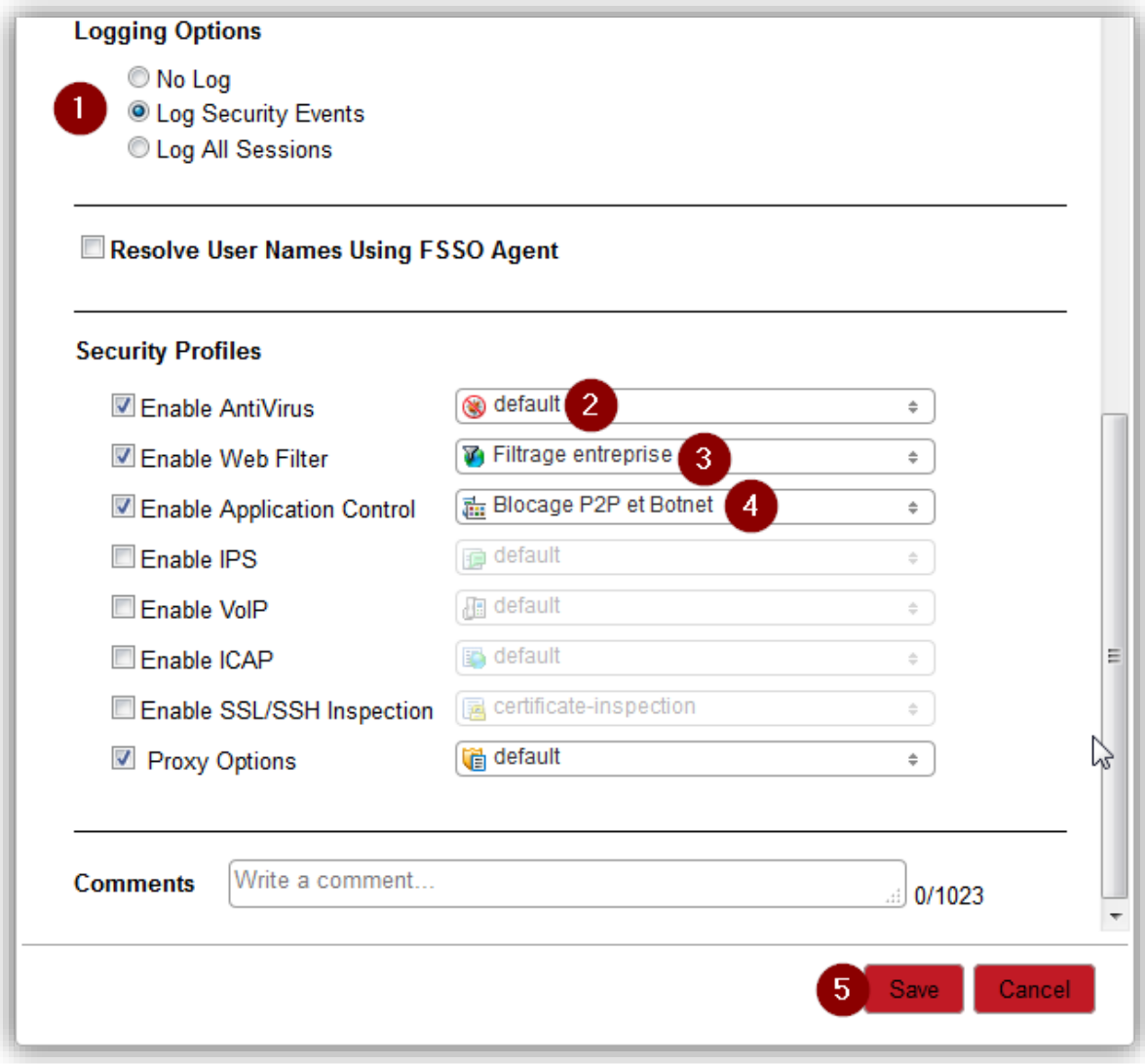
Comme il s'agit d'un flux sortant d'un réseau privé vers Internet, il est obligatoire de « NATter » le flux, c'est-à-dire de le transformer pour qu'il utilise une adresse IP publique, connue d'Internet.

Pour ce faire, on active la case « NAT », puis on sélectionne « Dynamic IP Pool », et on choisit l'IP que l'on souhaite utiliser (objet configuré d'avance par l'équipe intégration SIS Evolution)



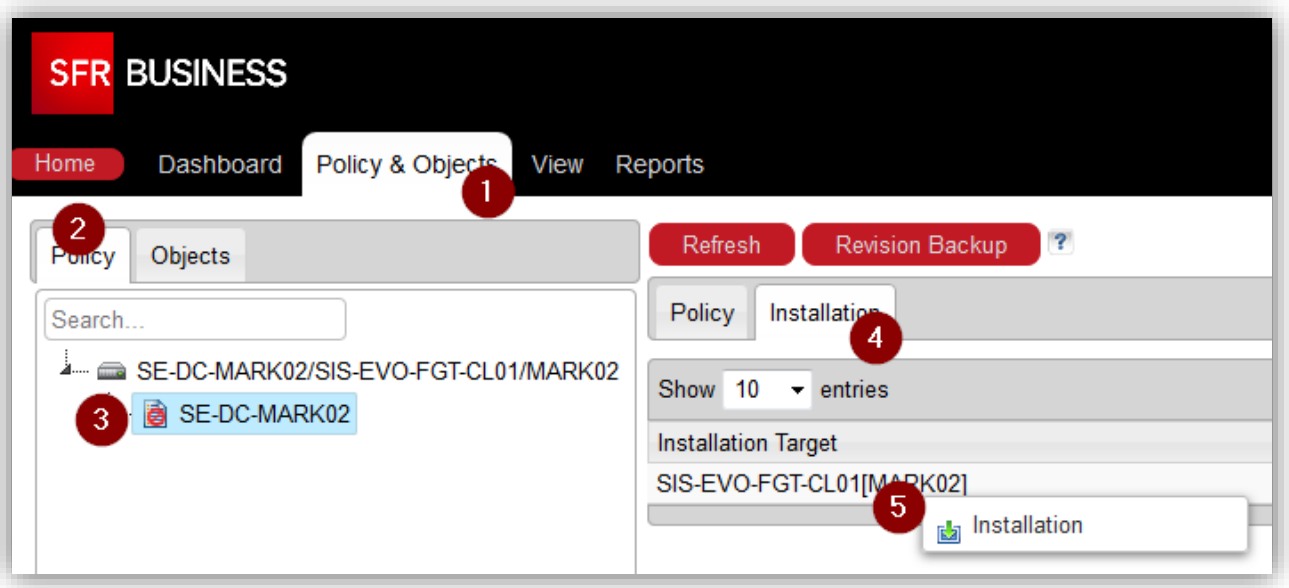
Note aux clients utilisant un pare-feu hébergé en Datacenter SFR (IPNET), il est indispensable d'utiliser un IP Pool. La fonctionnalité « Use Destination Interface Address » n'est pas utilisable.

Activer un niveau de log à « **Security Events** », puis activer les profils de sécurité idoine. Valider par « **Save** » :

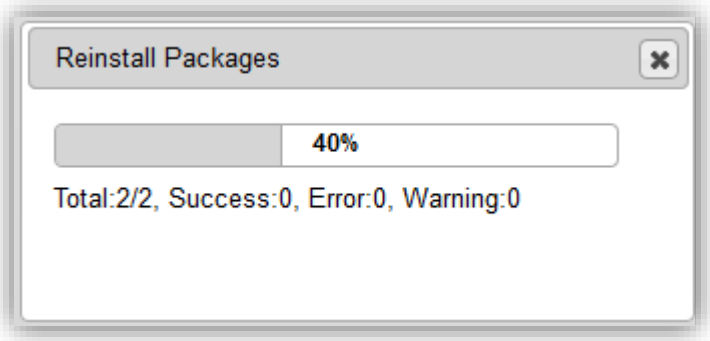


4.1.5 Installation de la politique sur votre pare-feu

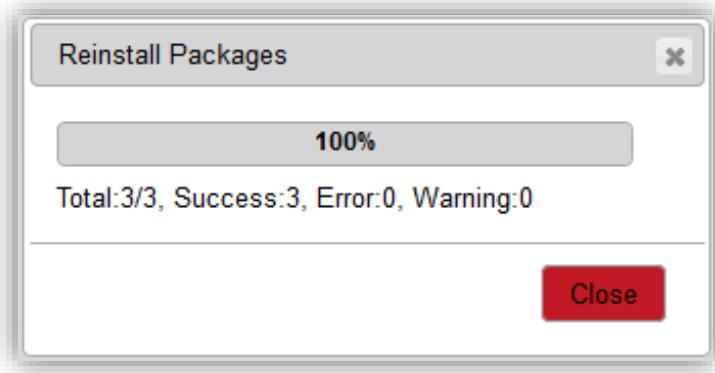
Il reste à installer la nouvelle politique sur votre pare feu. Pour ce faire, cliquer sur l'onglet « **Installation** », puis faire un clic droit sur votre pare-feu, et faire « **Installation** »



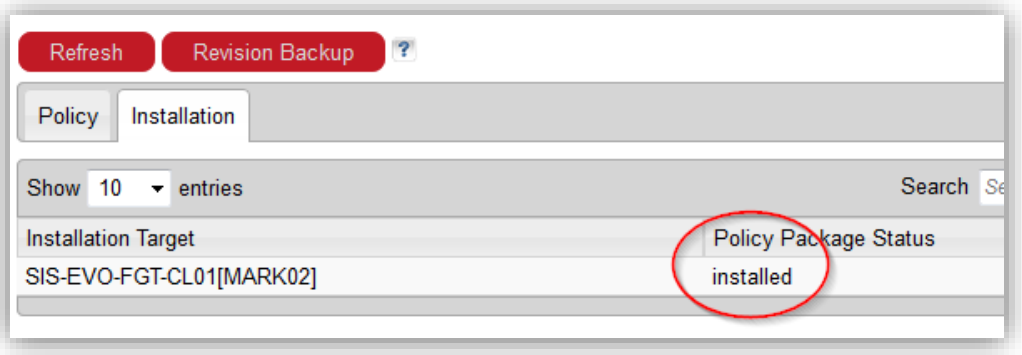
L'installation se déroule



Cliquer sur « **Close** » à la fin de l'installation



Un statut « **Installed** » vous permet de savoir si la politique en place est à jour



4.2 Création d'une règle de flux entrante

4.2.1 Cas d'école

Cet exemple va vous présenter comment créer une règle autorisant les accès externes vers des ressources internes.

Nous y appliquerons un filtre IPS par défaut.

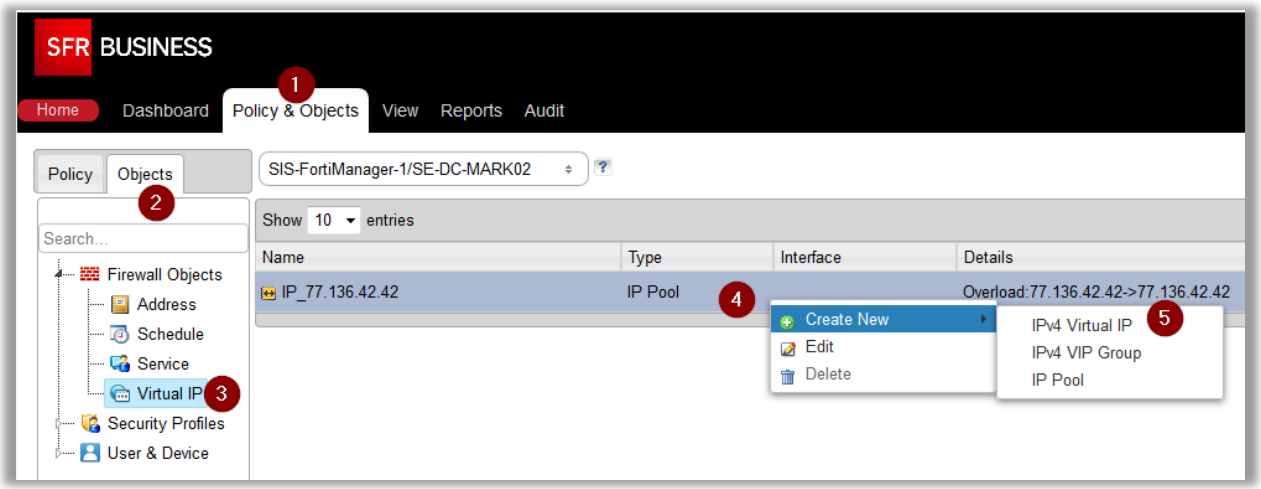
4.2.2 Création des objets « firewall »

On commence tout d'abord par créer les objets dont nous avons besoin. Les objets nécessaires sont :

- Un objet address « ServeurWeb » pointant sur 192.168.1.250
- Un objet Virtual IP « VIP-SRV-WEB » pour renseigner l'adresse IP publique, l'adresse IP privée et le port 80.
- Un objet Virtual IP « VIP-SRV-SSH » pour renseigner l'adresse IP publique, l'adresse IP privée et le port 22.
- Un objet Virtual IP « VIP-SRV-FTP » pour renseigner l'adresse IP publique, l'adresse IP privée et le port 21.
- Un groupe Virtual IP regroupant les objets « VIP-SRV-WEB », « VIP-SRV-SSH » et « VIP-SRV-FTP »

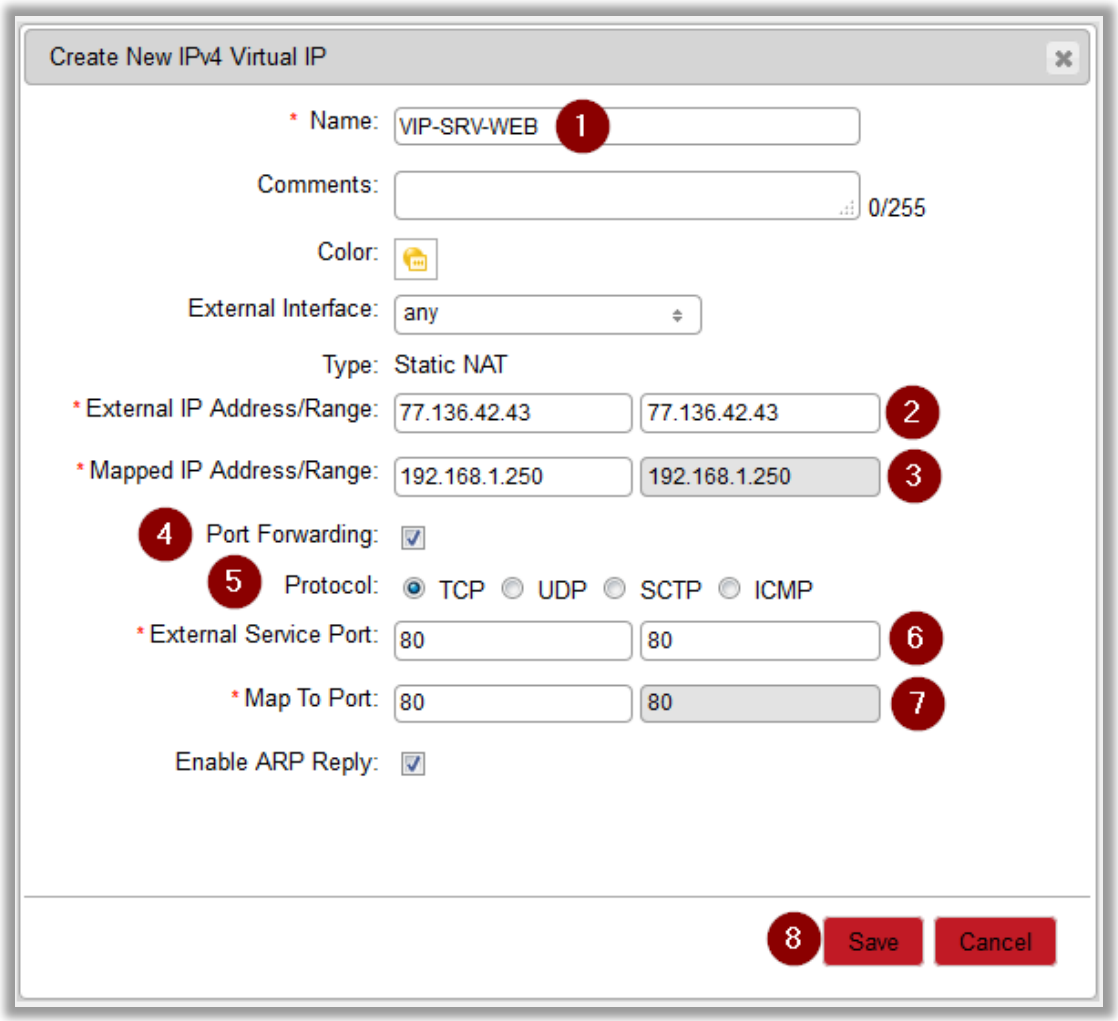
On commence par aller dans l'onglet « **Policy & Objects** » du Portail SIS Evolution, puis sur l'onglet « **Objects** » et enfin en cliquant sur « **Virtual IP** »

On effectue un clic droit sur la zone des objets et on fait « **Create new > IPv4 Virtual IP** » :



On saisit le nom de l'objet, l'adresse IP externe, l'adresse IP interne, on coche « Port Forwarding », « Protocole TCP » et on saisit le numéro de port externe et le numéro de port interne.

On valide par « **Save** » :

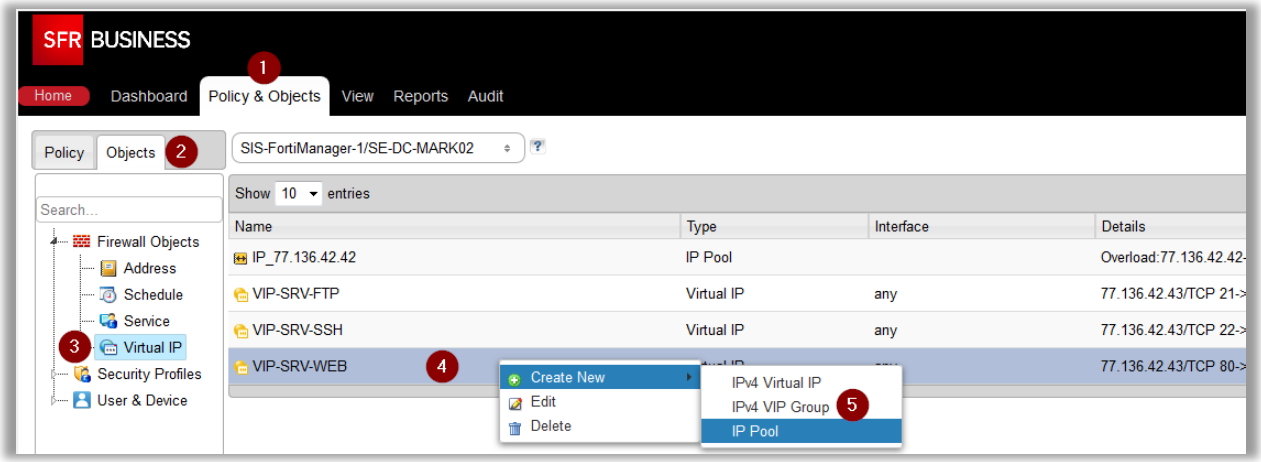


Les objets « VIP-SRV-SSH » et « VIP-SRV-FTP » seront créés de la même manière que l'objet « ServeurWeb »

On doit créer le groupe de VIP pour regrouper les VIP crées précédemment.

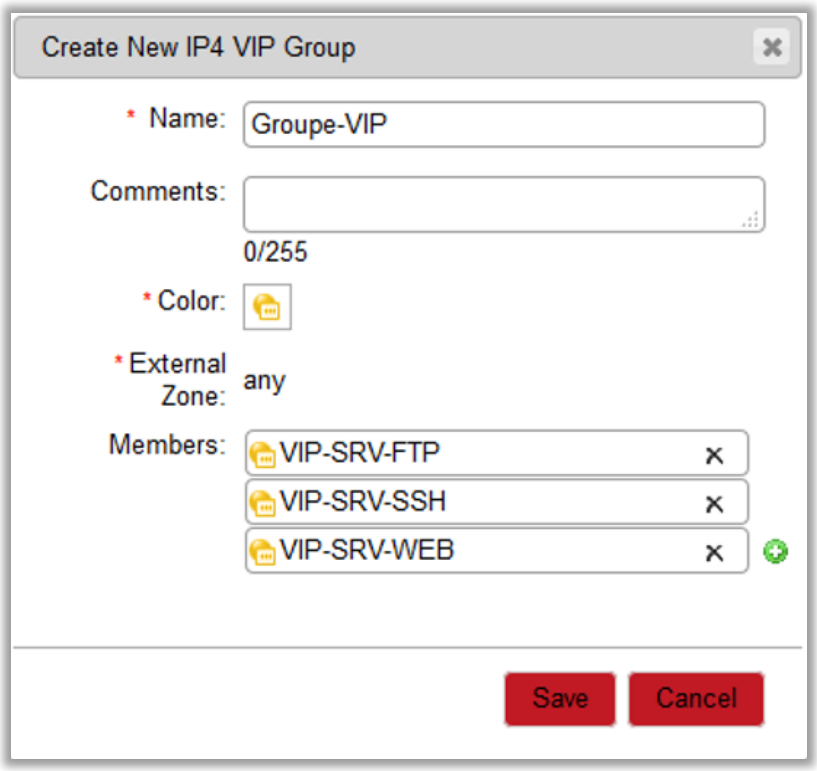
Pour cela, il faut aller dans l'onglet « **Policy & Objects** » du Portail SIS Evolution, puis sur l'onglet « **Objects** » et enfin en cliquant sur « **Virtual IP** »

On effectue un clic droit sur la zone des objets et on fait « **Create new > IPv4 VIP GROUP** » :



On saisit le nom de l'objet, et on rajoute les objets en utilisant le « + » vert.

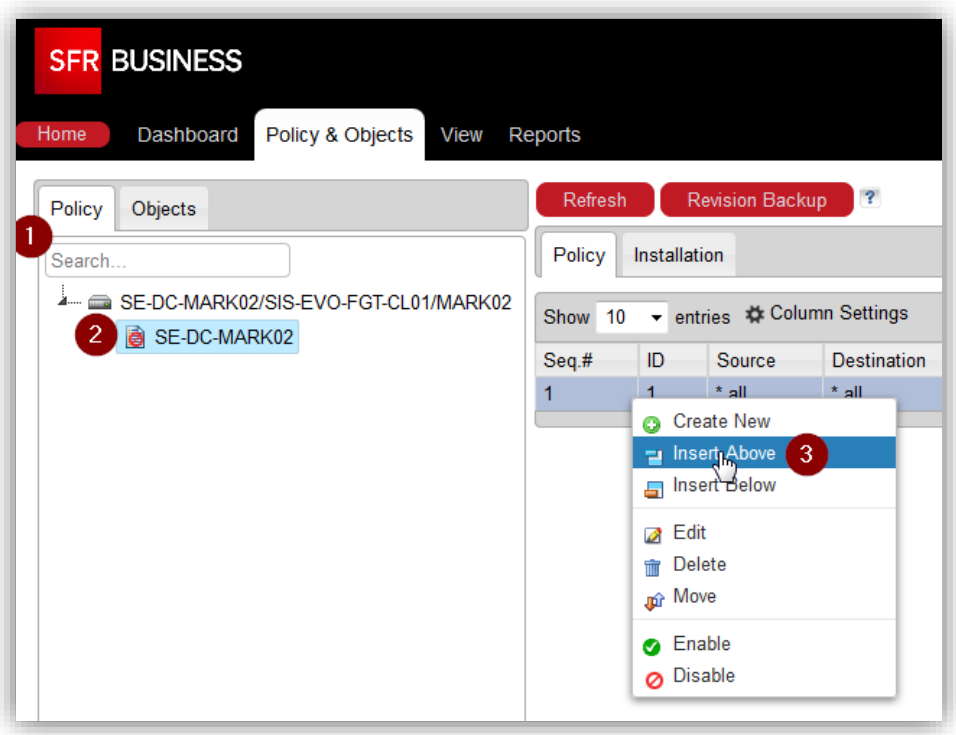
On valide par « **Save** » :



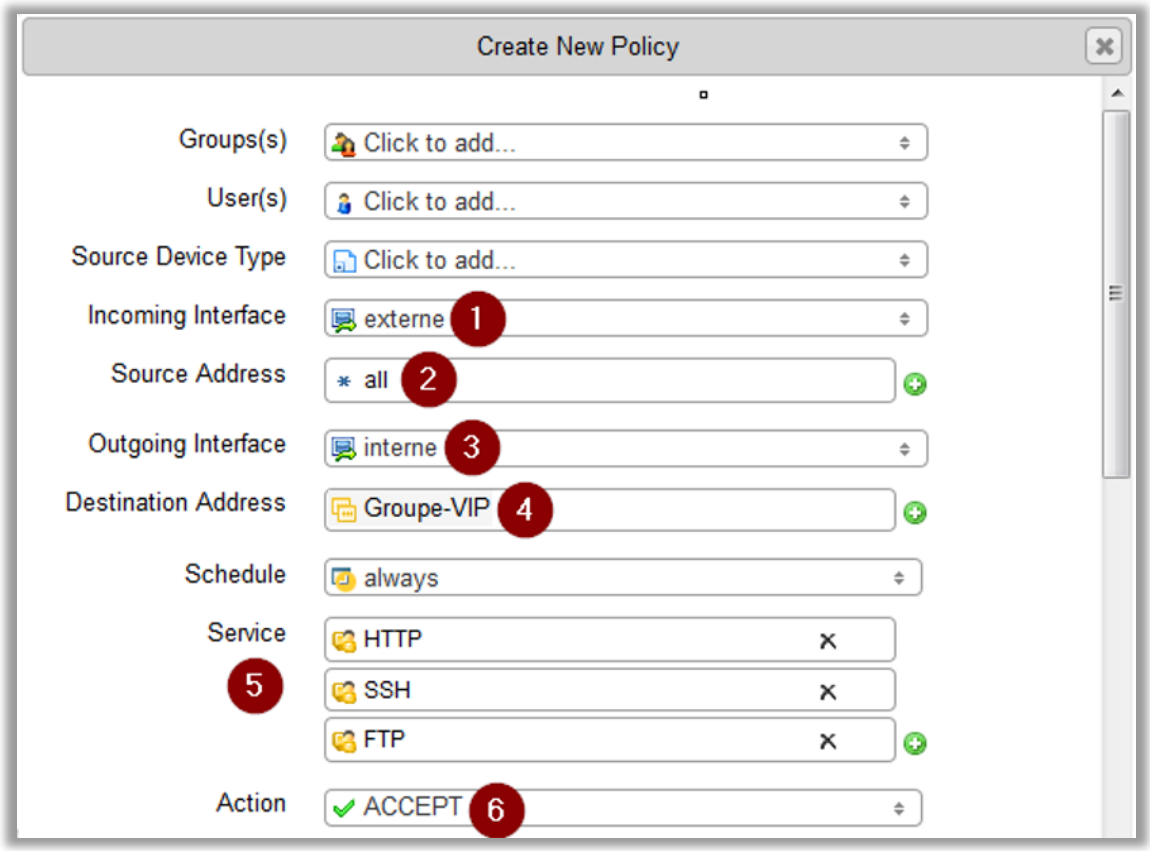
4.2.3 Création de la règle de pare-feu

La création de la règle de pare-feu se fait en retournant dans l'onglet « **Policy** », puis en cliquant sur la politique de sécurité.

Dans la liste des règles, faire un clic droit puis « **Insert Above** »



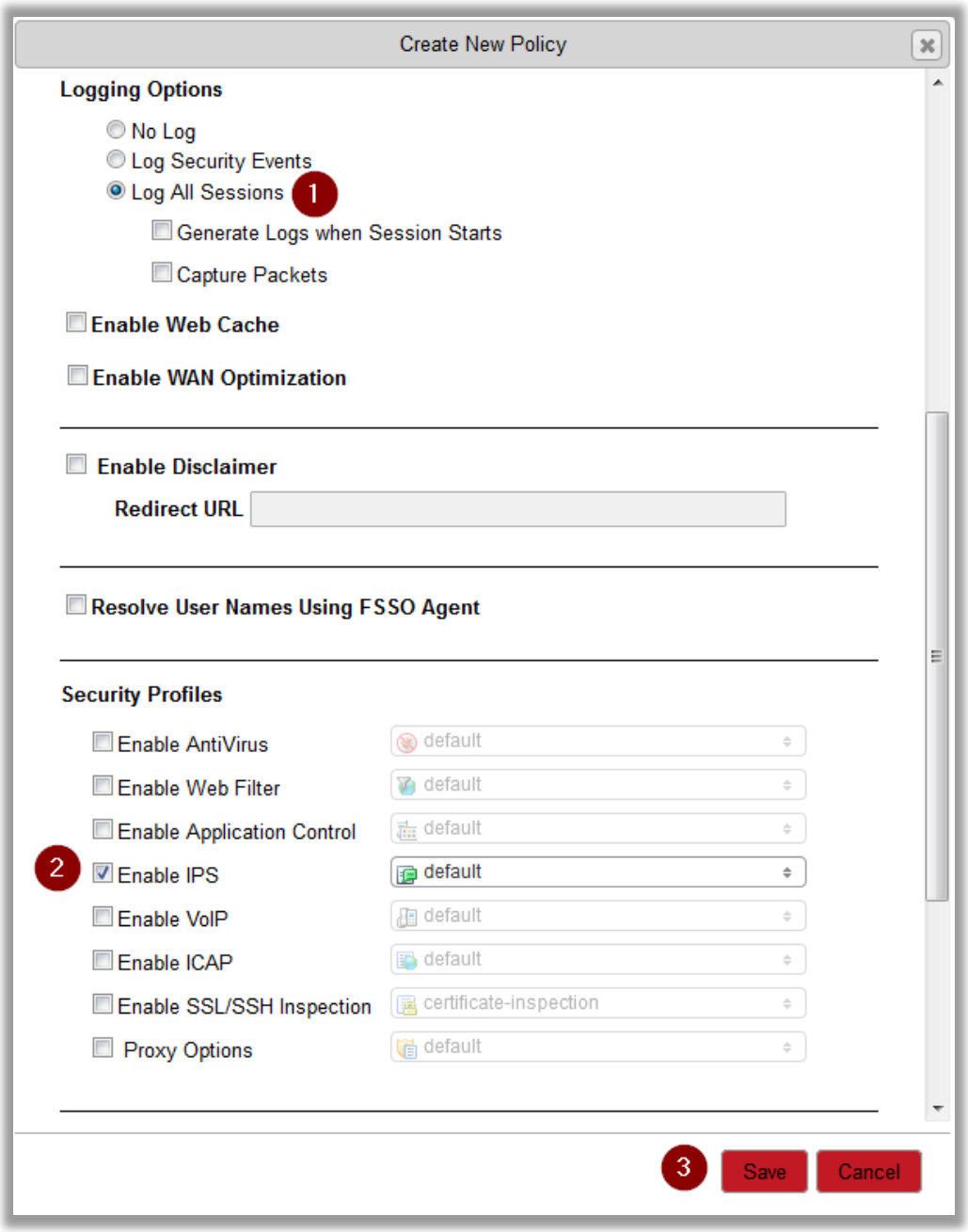
On sélectionne les conditions de notre règle, en utilisant les objets préalablement créés et on choisit une action « Accept » pour que le flux soit autorisé.



Comme il s'agit d'un flux entrant vers un serveur interne, il est obligatoire de « NATter » le flux entrant, c'est-à-dire de transformer l'adresse IP publique en adresse IP privée. Pour cela il faut sélectionner:

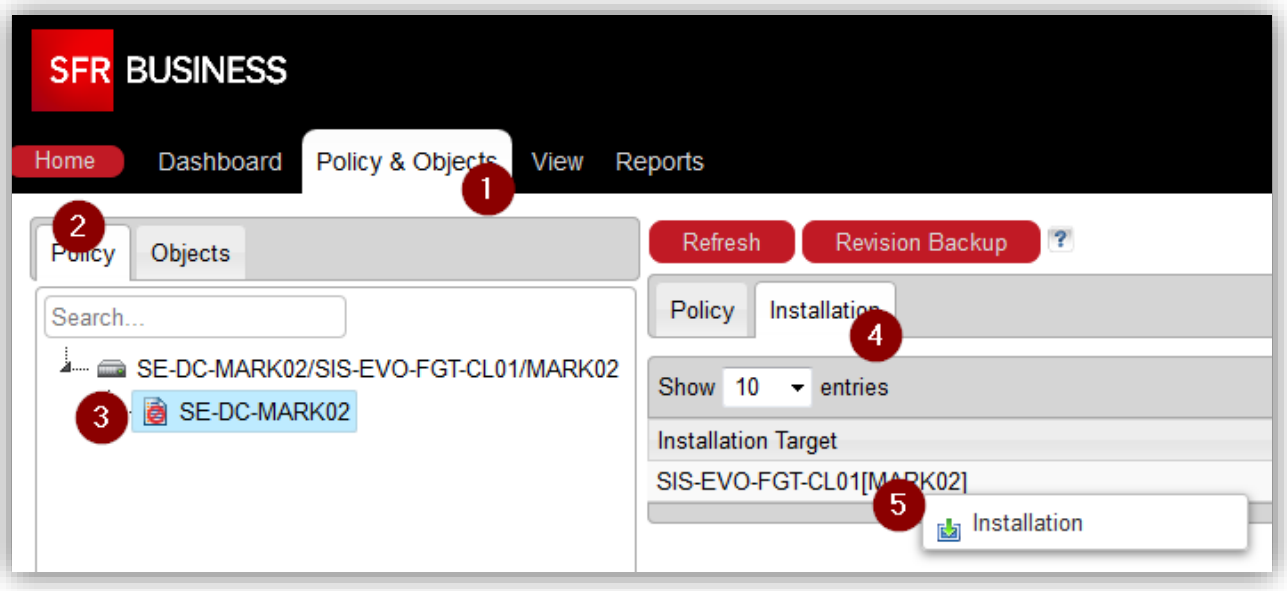
- l'interface « externe » dans « Incoming Interface »
- l'interface « interne » dans « Outgoing Interface »
- le groupe « Groupe-VIP » dans « Destination Address »
- les services : http, SSH et FTP dans la partie « Service »
- « Accept » dans « Action »

Activer un niveau de log à « **Security Events** », puis activer les profile « default » de l'IPS et valider par « **Save** » :

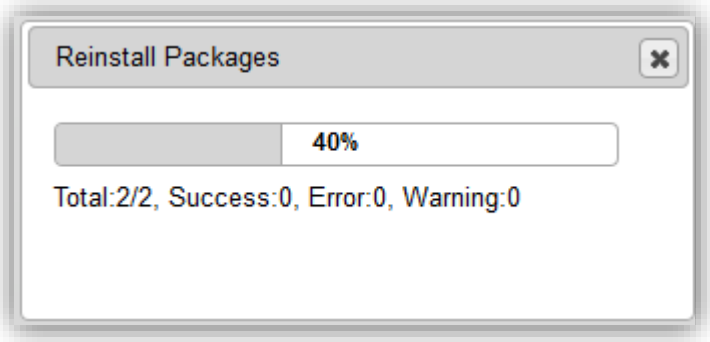


4.2.4 Installation de la politique sur votre pare-feu

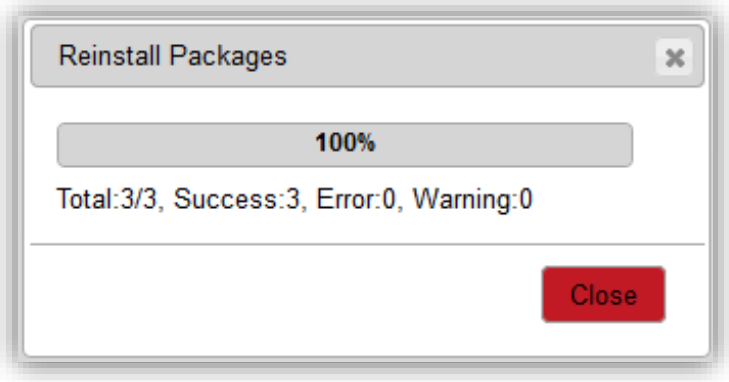
Il reste à installer la nouvelle politique sur votre pare feu. Pour ce faire, cliquer sur l'onglet « **Installation** », puis faire un clic droit sur votre pare-feu, et faire « **Installation** »



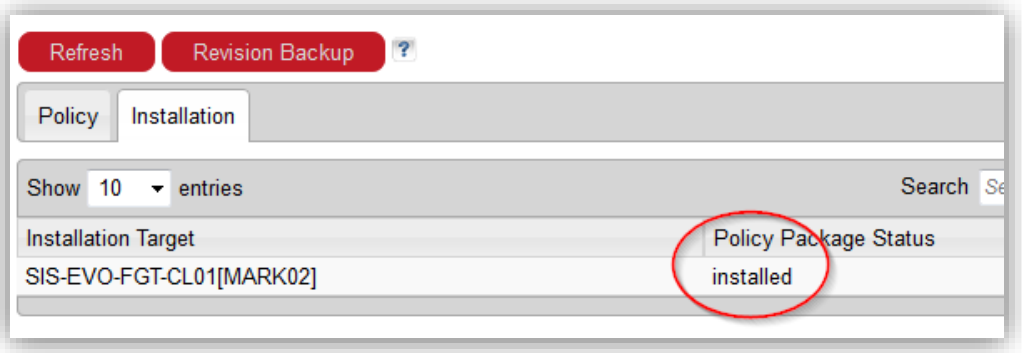
L'installation se déroule



Cliquer sur « **Close** » à la fin de l'installation



Un statut « **Installed** » vous permet de savoir si la politique en place est à jour

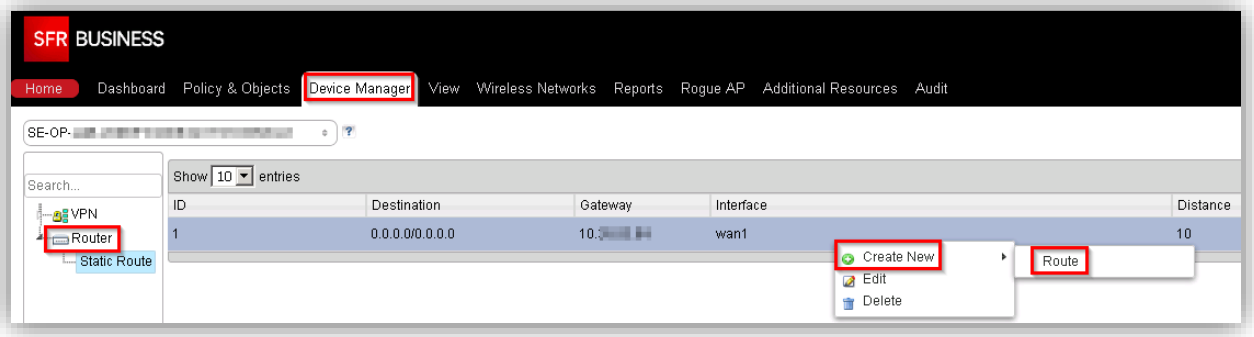


4.3 Routage et VPN IPSec

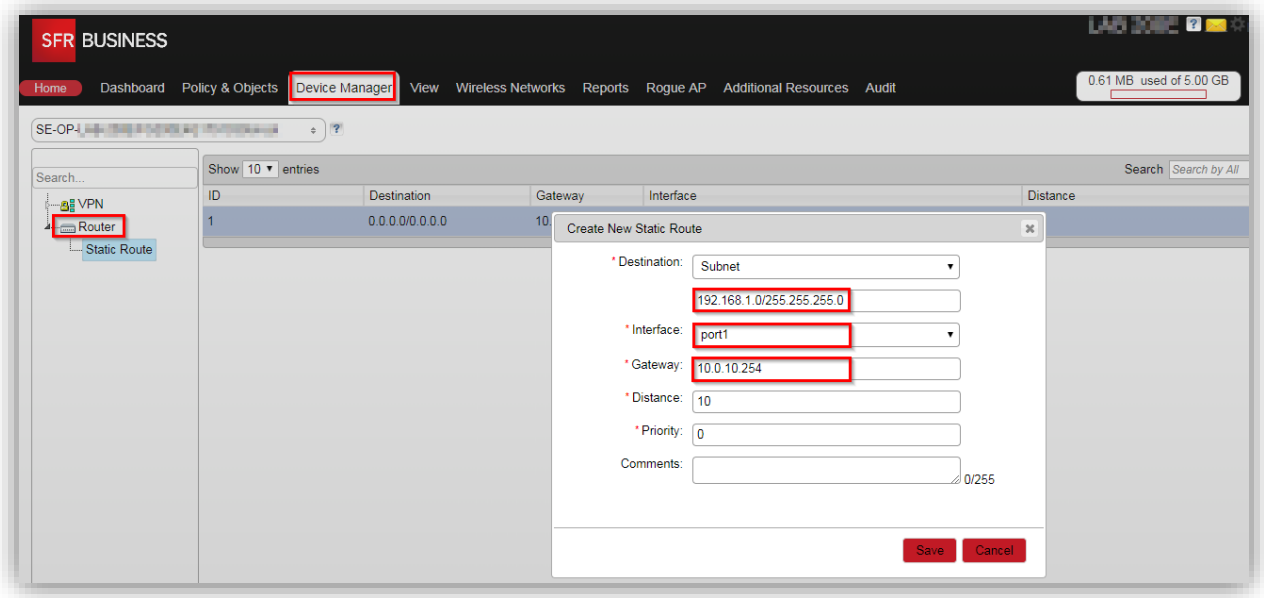
4.3.1 4.3.1 - Routage

La configuration des routes statiques se fait au niveau de l'onglet « **Device Manager** » en cliquant sur le menu « **Router » « Static route »**

Dans la liste des routes, faire un clic droit puis « **Create new** » > « **Route** »



On saisit le réseau de destination, l'interface de sortie et la Gateway.



On valide par « **Save** » et on installe la politique de sécurité comme indiqué dans le paragraphe 4.2.4

IMPORTANT :

Veuillez ne pas supprimer la route par défaut.

4.3.2 VPN IPSec

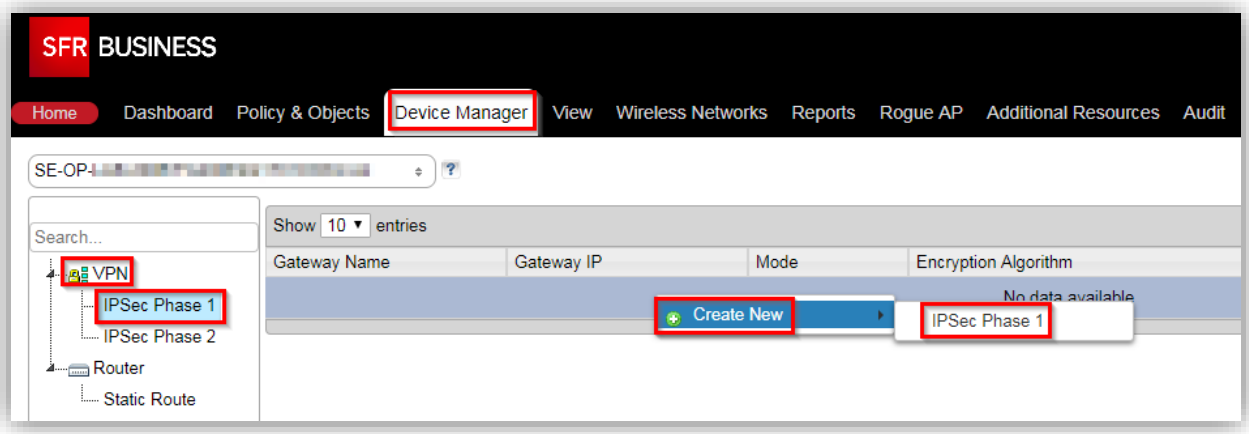
Afin de monter un tunnel VPN IPSec, nous devons paramétrer :

- la Phase 1
- la Phase 2
- les routes statiques
- et les règles de sécurité.

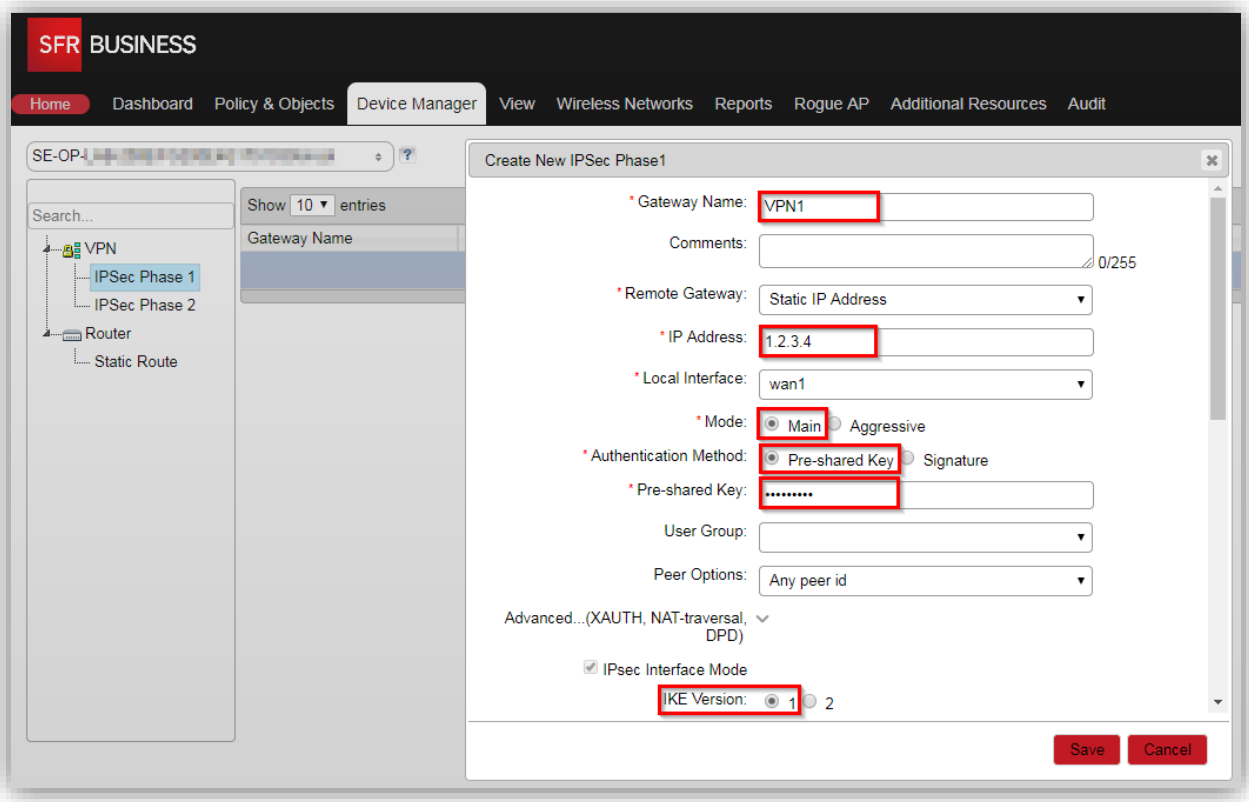
La configuration du VPN IPSec se fait dans l'onglet « **Device Manager** » en cliquant sur le menu « **VPN** »

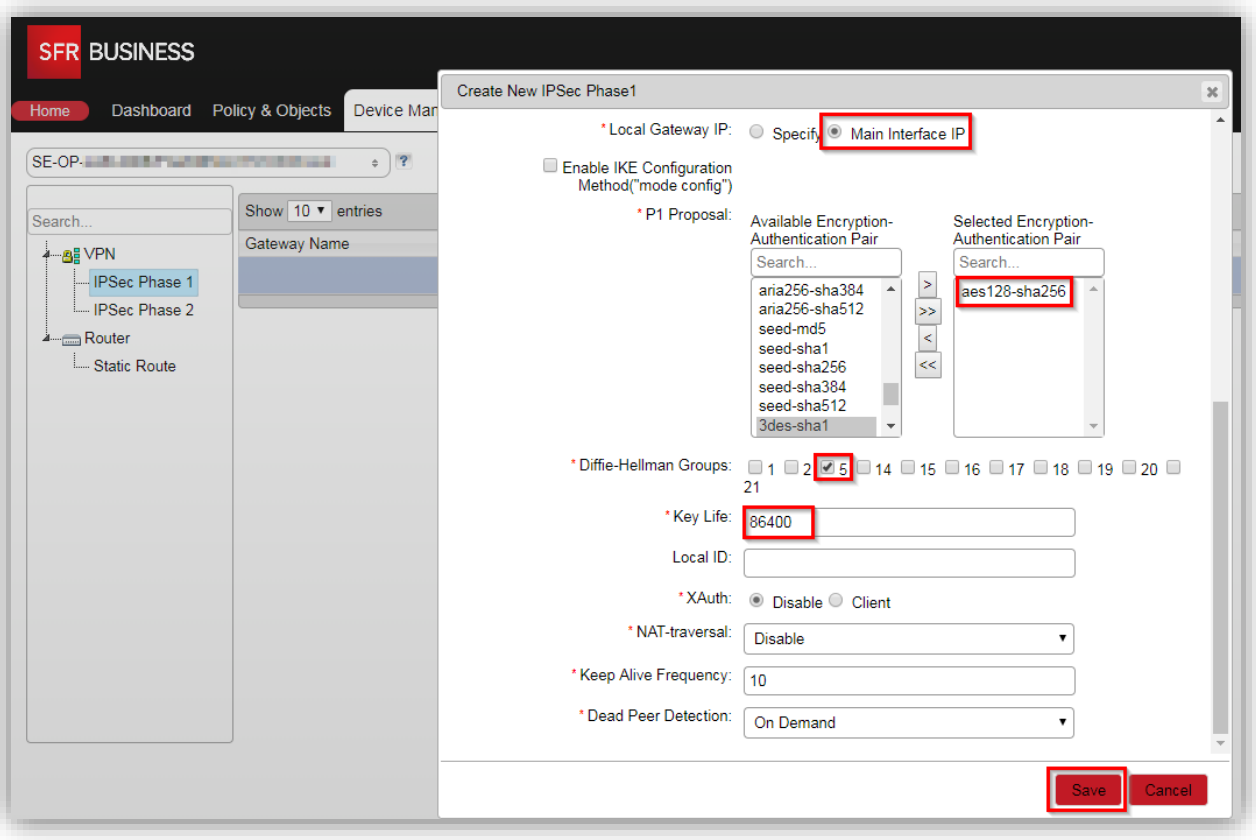
On commence tout d'abord par créer la Phase 1, pour cela allez dans « **Device Manager** » > « **VPN** » > « **IPSec Phase 1** »

Dans la liste des Phases 1, faire un clic droit puis « **Create new** » > « **IPSec Phase 1** »



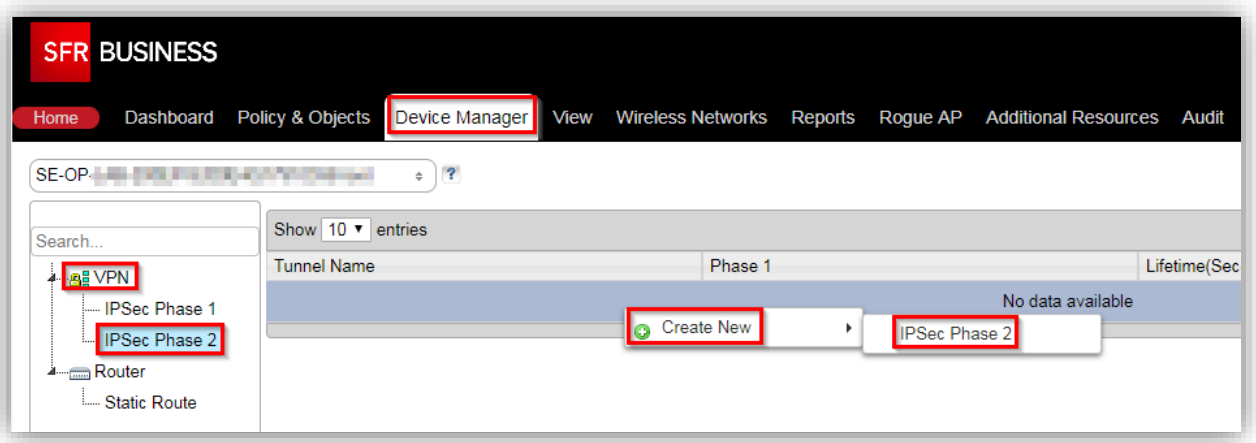
On saisit les différents champs, comme indiqué sur ces deux screenshots :



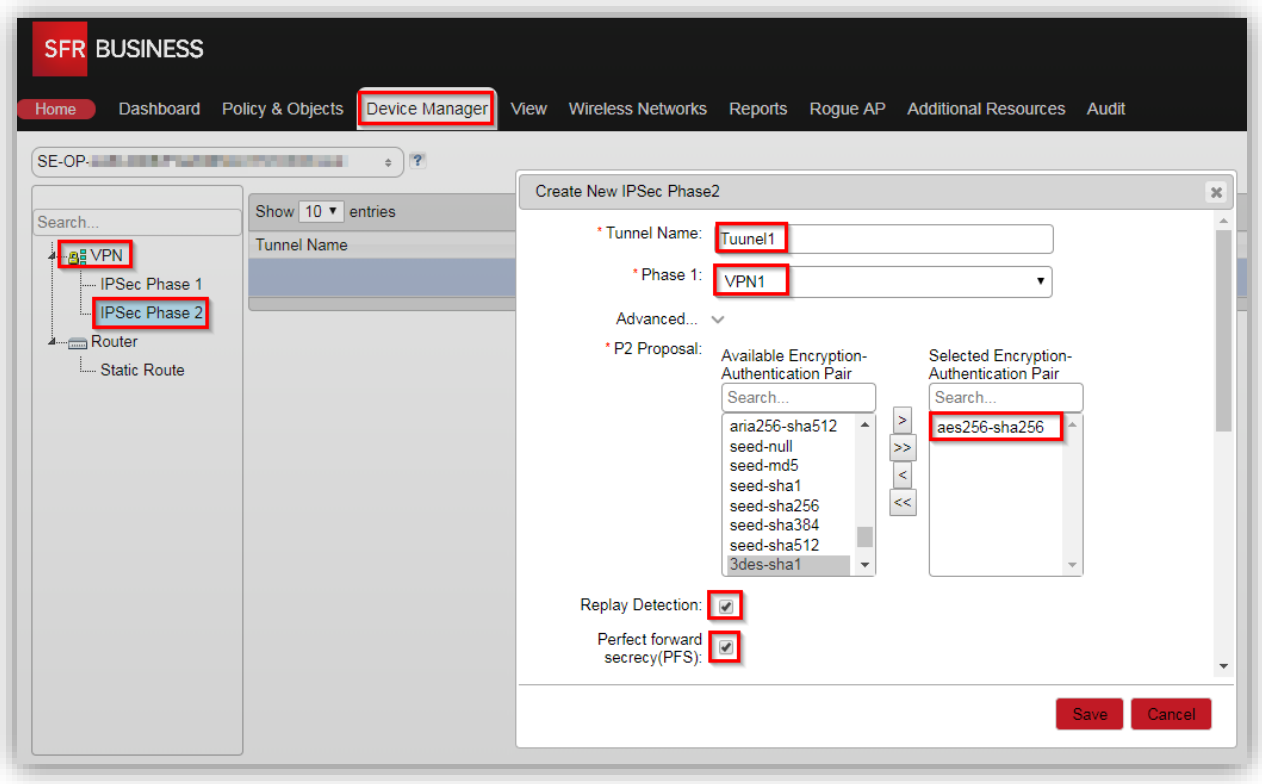


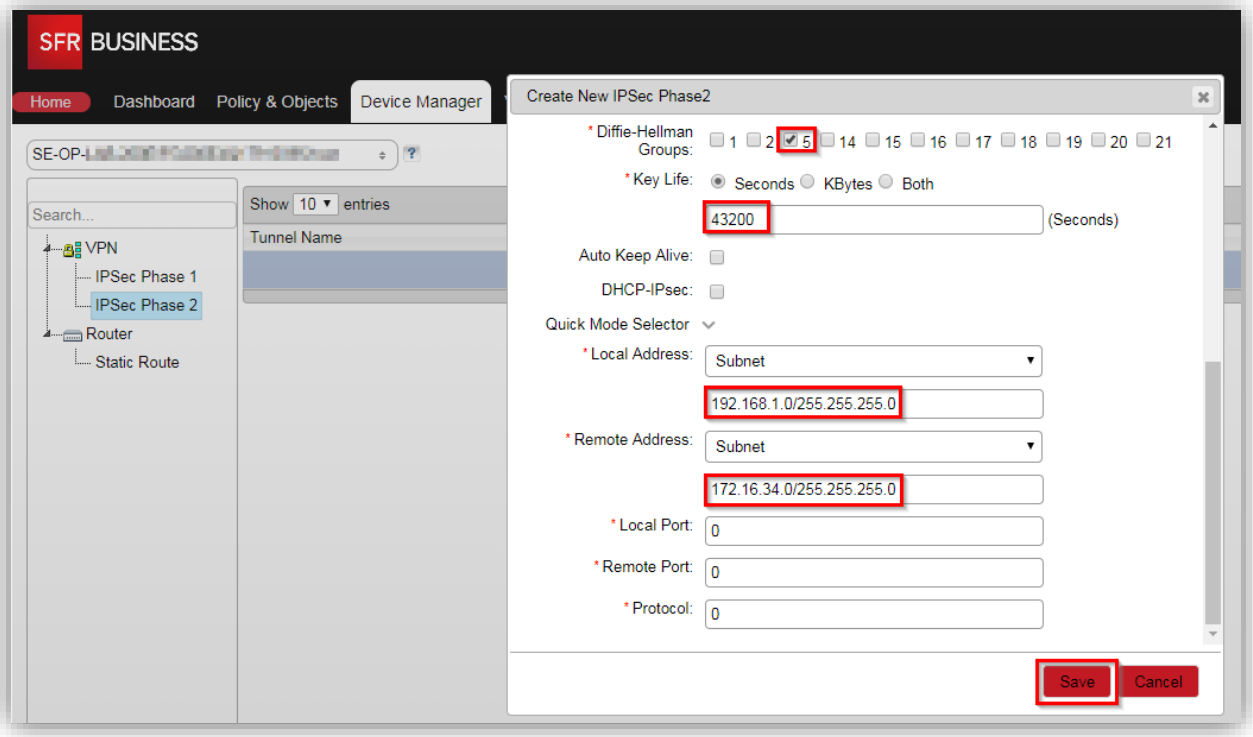
Ensuite, on créé la Phase 2, pour cela allez dans « **Device Manager** » > « **VPN** » > « **IPSec Phase 2** »

Dans la liste des Phases 2, faire un clic droit puis « **Create new** » > « **IPSec Phase 2** »

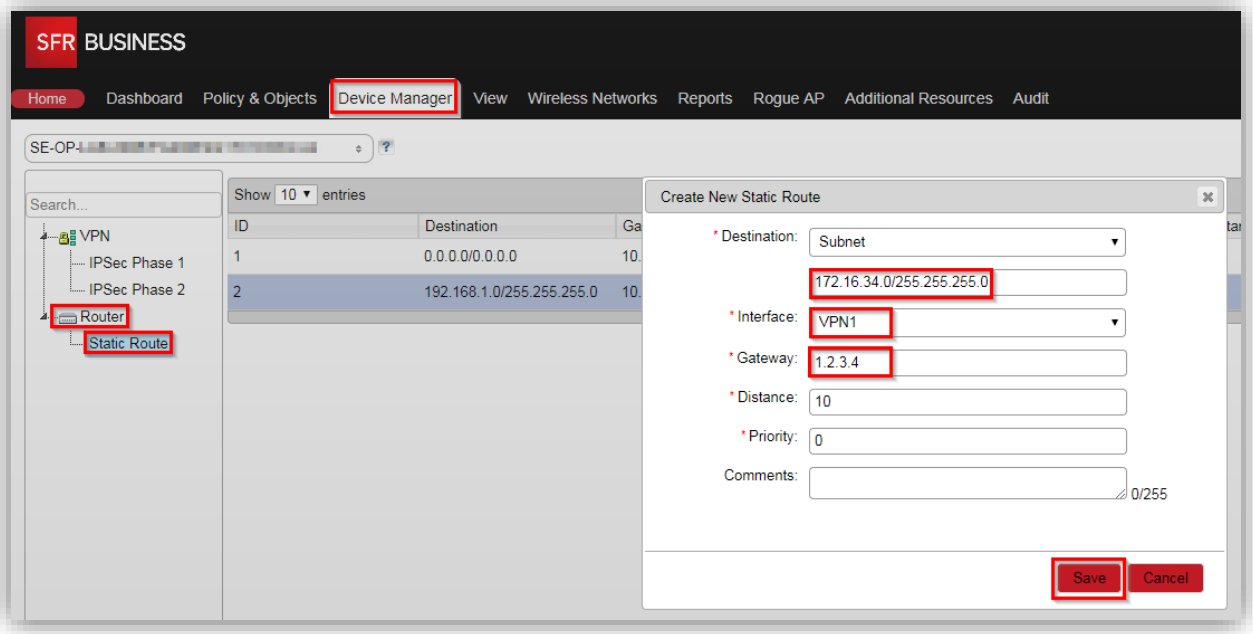


On saisit les différents champs, comme indiqué sur ces deux screenshots :





Après, on créé une nouvelle route statique (voir 4.3.1) pour router les flux du réseau local sur le tunnel VPN



Et enfin, on créé une règle de sécurité qui autorise le réseau local à accéder au réseau distant a travers le tunnel VPN IPSec, voir 4.2.3 et 4.2.4.