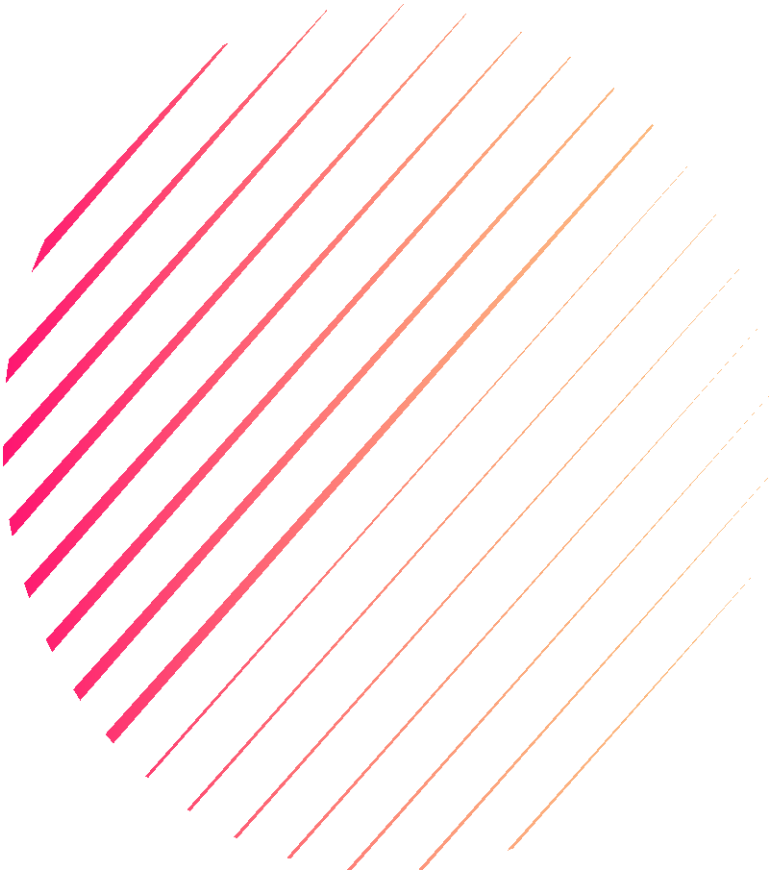
Atelier Pro 3



31/01/2026
Projet : migration Firewall

Ethan BAMBARA--DASYLVA
BTS SIO 2024 – 2026

Table des matières

Contexte du Projet

Description du laboratoire GSB

Le secteur d'activité :
L'industrie pharmaceutique est un secteur très lucratif dans lequel le mouvement de fusion acquisition est très fort. Les regroupements de laboratoires ces dernières années ont donné naissance à des entités gigantesques au sein desquelles le travail est longtemps resté organisé selon les anciennes structures.
Des déboires divers récents autour de médicaments ou molécules ayant entraîné des complications médicales ont fait s'élever des voix contre une partie de l'activité des laboratoires : la visite médicale, réputée être le lieu d' arrangements entre l'industrie et les praticiens, et tout du moins un terrain d'influence opaque.

L'entreprise :
Le laboratoire Galaxy Swiss Bourdin (GSB) est issu de la fusion entre le géant américain Galaxy (spécialisé dans le secteur des maladies virales dont le SIDA et les hépatites) et le conglomérat européen Swiss Bourdin (travaillant sur des médicaments plus conventionnels), lui même déjà union de trois petits laboratoires .
En 2009, les deux géants pharmaceutiques ont uni leurs forces pour créer un leader de ce secteur industriel. L'entité Galaxy Swiss Bourdin Europe a établi son siège administratif à Paris.
Le siège social de la multinationale est situé à Philadelphie, Pennsylvanie, aux Etats-Unis.
La France a été choisie comme témoin pour l'amélioration du suivi de l'activité de visite.

Description du système informatique

Le système informatique :
Sur le site parisien, toutes les fonctions administratives (gestion des ressources humaines, comptabilité, direction, commerciale, etc.) sont présentes. On trouve en outre un service labo-recherche, le service juridique et le service communication.

La salle serveur occupe le 6ème étage du bâtiment et les accès y sont restreints (étage accessible par ascenseur à l'aide d'une clé sécurisée, portes d'accès par escalier munies d'un lecteur de badge, sas d'entrée avec gardien présent 24h/24).

Les serveurs assurent les fonctions de base du réseau (DHCP, DNS, Annuaire et gestion centralisée des environnements) et les fonctions de communication (Intranet, Messagerie, Agenda partagé, etc.).
On trouve aussi de nombreuses applications métier (base d'information pharmaceutique, serveurs dédiés à la recherche, base de données des produits du laboratoire, base de données des licences d'exploitation pharmaceutique, etc.) et les fonctions plus génériques de toute entreprise (Progiciel de Gestion Intégré avec ses modules RH, GRC, etc.).
Un nombre croissant de serveurs est virtualisé.

Constitué autour de VLAN, le réseau segmente les services de manière à fluidifier le trafic.

Les données de l'entreprises sont considérées comme stratégiques et ne peuvent tolérer ni fuite, ni destruction. L'ensemble des informations est répliqué quotidiennement aux Etats-Unis par un lien dédié. Toutes les fonctions de redondances (RAID, alimentation, lien réseau redondant, Spanning-tree, clustering, etc.) sont mises en œuvre pour assurer une tolérance aux pannes maximale.

L'équipement :
L'informatique est fortement répandue sur le site. Chaque employé est équipé d'un poste fixe relié au système central. On dénombre ainsi plus de 350 équipements terminaux et un nombre de serveurs physiques conséquent (45 en 2012) sur lesquels tournent plus de 100 serveurs virtuels.

On trouve aussi des stations de travail plus puissantes dans la partie labo-recherche, et une multitude d'ordinateurs portables (personnels de direction, service informatique, services commerciaux, etc).

Les visiteurs médicaux reçoivent une indemnité bisannuelle pour s'équiper en informatique (politique Swiss-Bourdin) ou une dotation en équipement (politique Galaxy). Il n'y a pas à l'heure actuelle d'uniformisation des machines ni du mode de fonctionnement

Chaque employé de l'entreprise a une adresse de messagerie de la forme **nomUtilisateur@steph.com**. Les anciennes adresses de chaque laboratoire ont été définitivement fermées au 1er janvier 2011.

Organisation du réseau

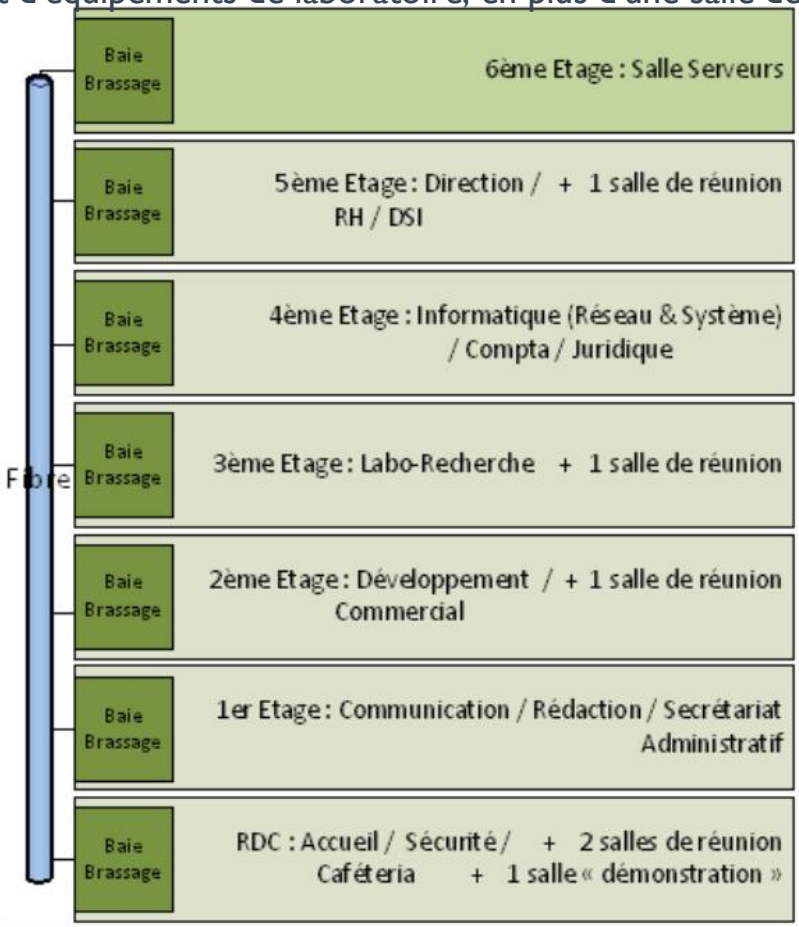
Répartition des services :
Chaque étage dispose d'une baie de brassage qui le relie par une fibre à la baie centrale de la salle serveurs.

Toutes les salles de réunion sont équipées d'un point d'accès Wifi positionné par défaut dans le VLAN "Visiteurs" qui autorise uniquement un accès Internet.
Les portables connectés en wifi à ce point d'accès reçoivent ainsi une adresse IP et n'ont, par conséquent accès qu'aux services DHCP et DNS.

Le point d'accès peut être configuré à la demande pour être raccordé à un VLAN présent au niveau de l'étage.

Chaque salle de réunion dispose d'un vidéoprojecteur, d'enceintes et d'un tableau numérique interactif.

La salle "Démonstration" est destinée à l'accueil des organismes de santé (AFSSAPS notamment) et des partenaires scientifiques. Elle dispose de paillasses et d'équipements de laboratoire, en plus d'une salle de réunion.



Projet

Segmentation du réseau :

L'organisation des VLAN et de l'adressage IP est la suivante :

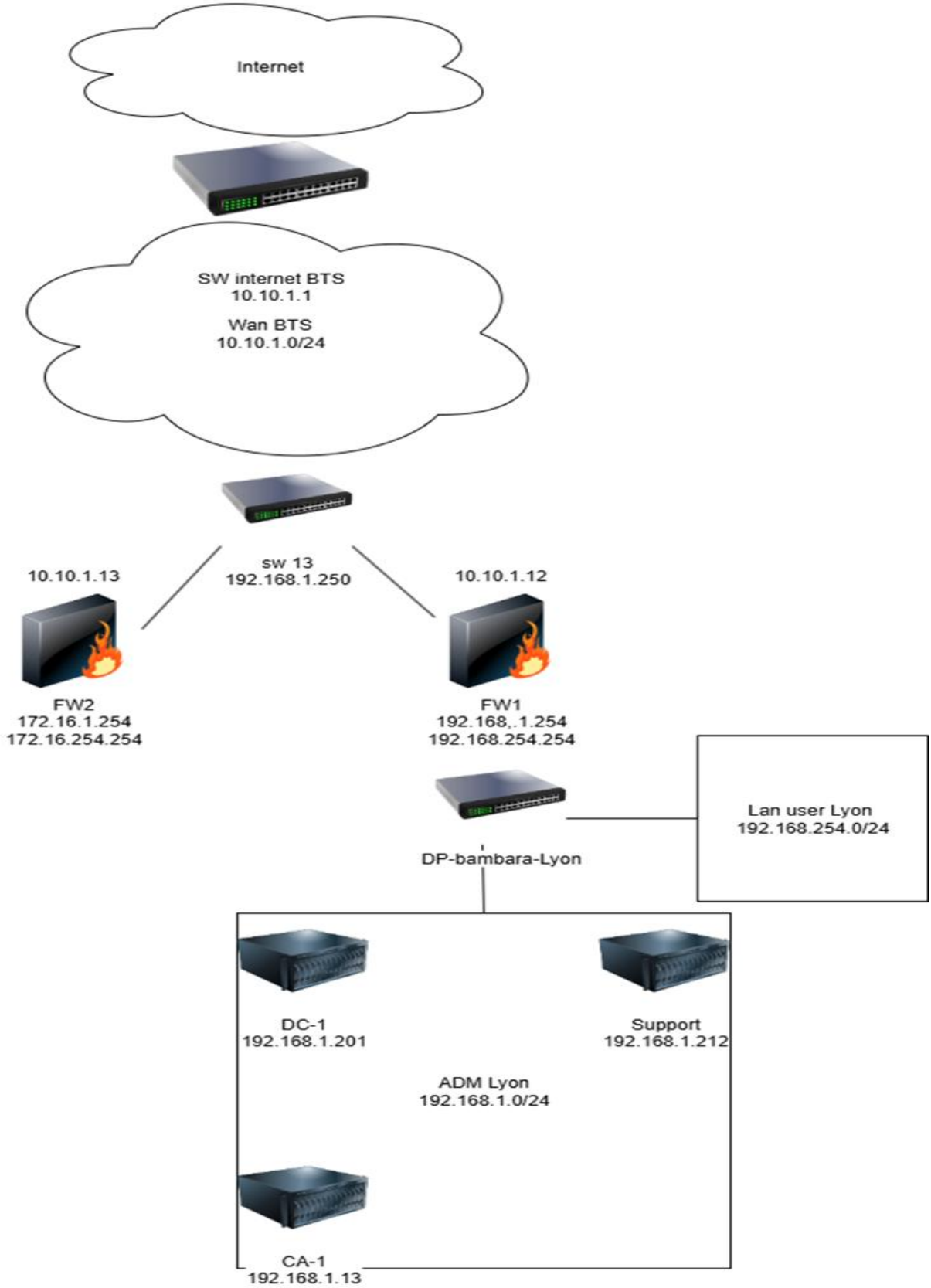
N° VLAN	Service(s)	Adressage IP
20	ADM-LYON	192.168.1.0/24
21	LAN-LYON	192.168.254.0/24
22	ADM-SLM	172.16.1.0/24
23	LAN-SLM	172.16.254.0/24
555	WAN	10.10.1.0/24

Salle serveur et connexion internet

L'organisation des serveurs et des équipements réseaux est la suivante :

- Le serveur principal est virtualisé sous le système Vmware Vcenter 7.0
- Un Commutateur Multicouche Cisco permet l'interconnection du serveur principal et la liaison vers le firewall de proximité (Internet).
- L'environnement Virtuel et réseau des Projets d'Atelier de Professionnalisation sont référencées ci-dessous :

Schéma réseau



Rapport

Reset du Firewall et configuration de base

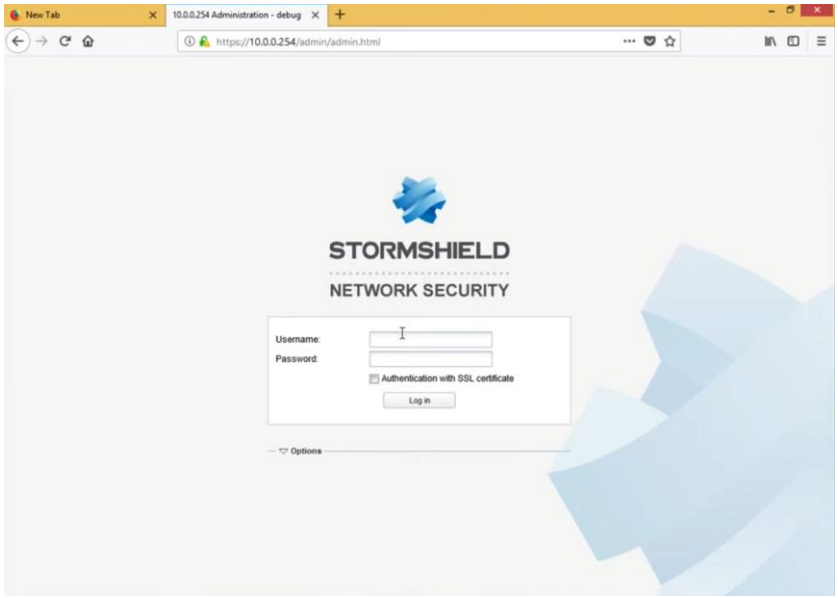
Avant de configurer le firewall, nous allons le réinitialiser en *factory default*.
Pour le réinitialiser, localisez le trou du bouton *reset*.

Ensuite, utilisez un outil assez fin pour entrer dans le trou, puis maintenez le bouton jusqu'à ce que les LED du firewall clignotent, cela indiquera que la procédure a commencé. Le reset peut prendre jusqu'à 10 minutes.

Après avoir reset le firewall, ce dernier aura comme IP **10.0.0.254/8**.

Pour vous connecter au firewall, saisissez l'IP dans un navigateur.
Les identifiants et le mot de passe par défaut sont les suivants :

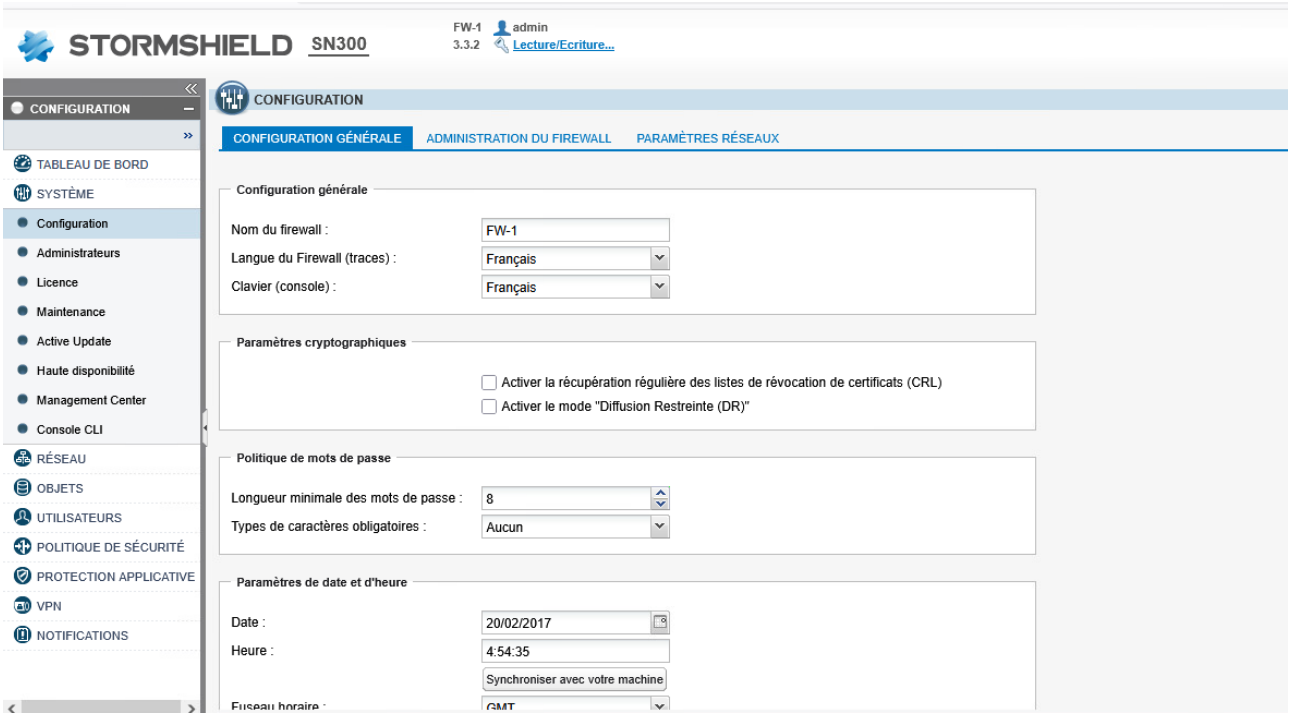
Username : admin
Password : admin



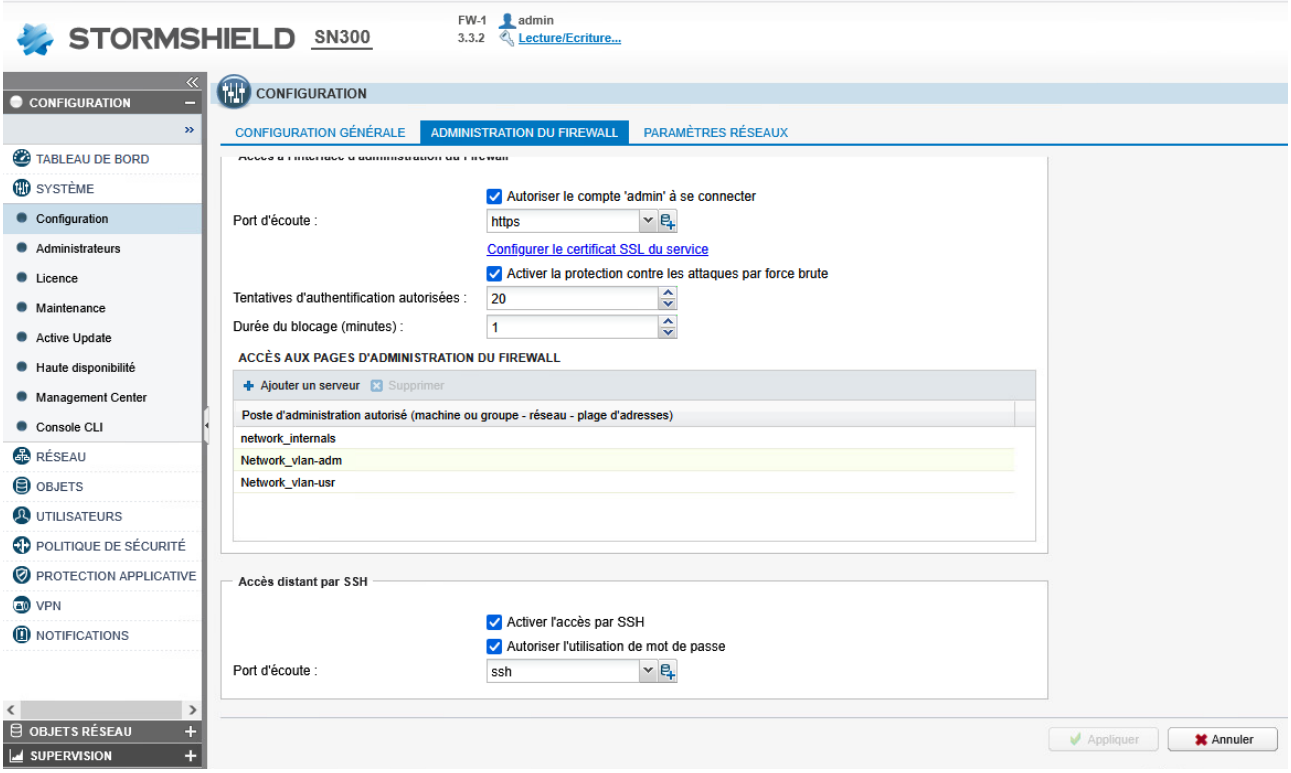
Configuration du Firewall

Une fois sur le firewall, nous allons changer son nom et définir sa langue.
Allez dans l'onglet Configuration.

Ici, changez le nom du firewall et la langue selon vos préférences.

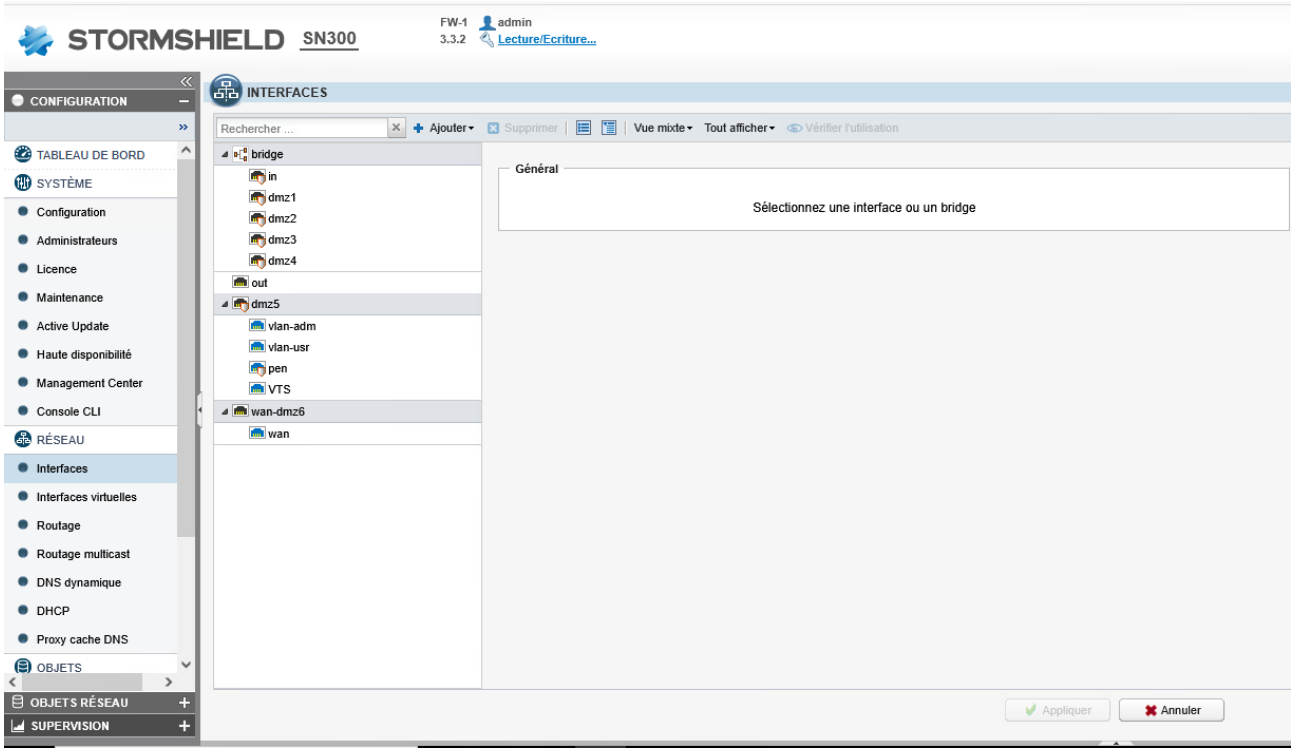


Ensuite, nous allons activer l'accès SSH sur le firewall.
Allez dans l'onglet Administration du firewall, puis cochez la case Activer l'accès par SSH.

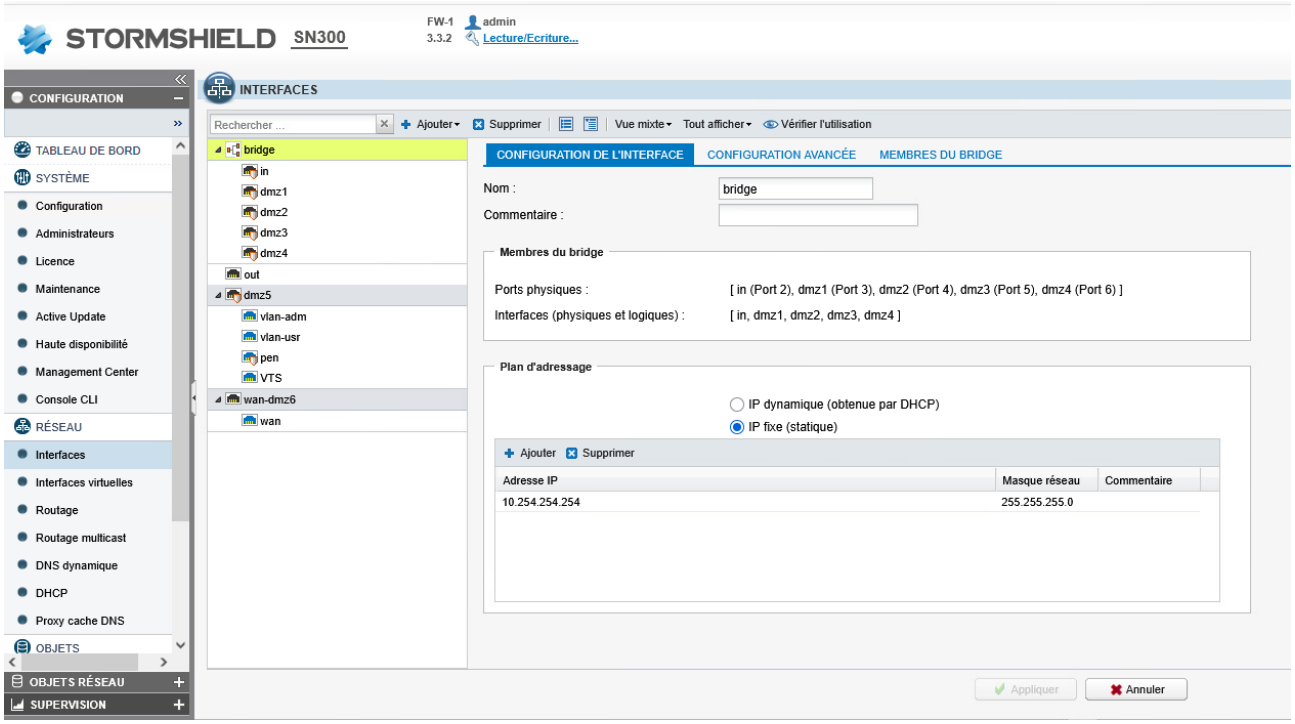


Ensuite, nous allons changer l'IP pour accéder au firewall.

Pour ce faire, dans la catégorie Réseau, allez dans l'onglet Interfaces.



Ensuite, par défaut, toutes vos interfaces seront dans un bridge ; nous allons changer l'IP de celui-ci. Cliquez sur le bridge puis changez son IP.
Attention, vous n'aurez plus accès au firewall, il faudra changer votre IP afin d'être dans le même réseau que le firewall.



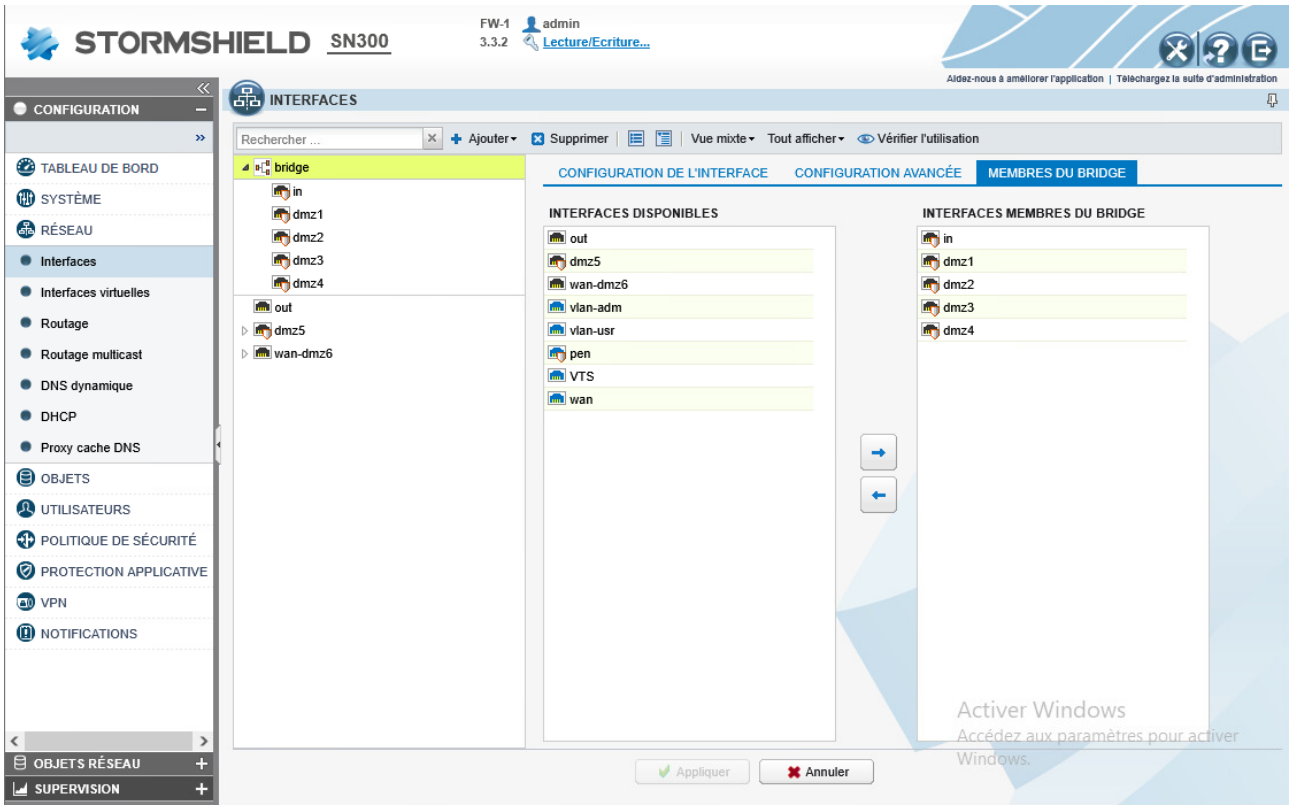
Configuration des interfaces

Tant que nous sommes dans la catégorie Interfaces, nous allons configurer celles-ci.

Pour commencer, nous allons sortir des interfaces du bridge par défaut afin de pouvoir les configurer. Dans mon cas, j'en utiliserai deux : une pour le réseau LAN et une pour le WAN.

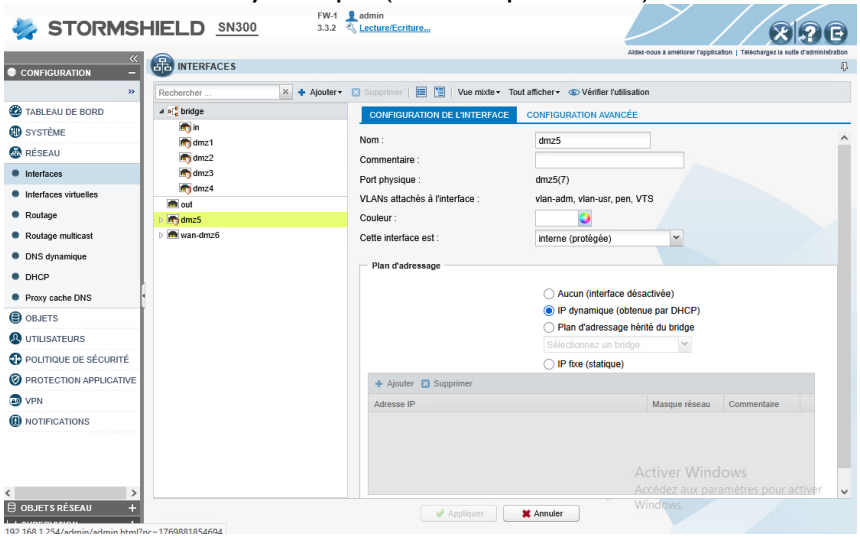
Il est conseillé d'utiliser l'interface OUT pour le WAN et l'interface IN pour le LAN.

Pour sortir une interface du bridge, allez dans la section Membres du bridge, puis retirez les interfaces souhaitées..

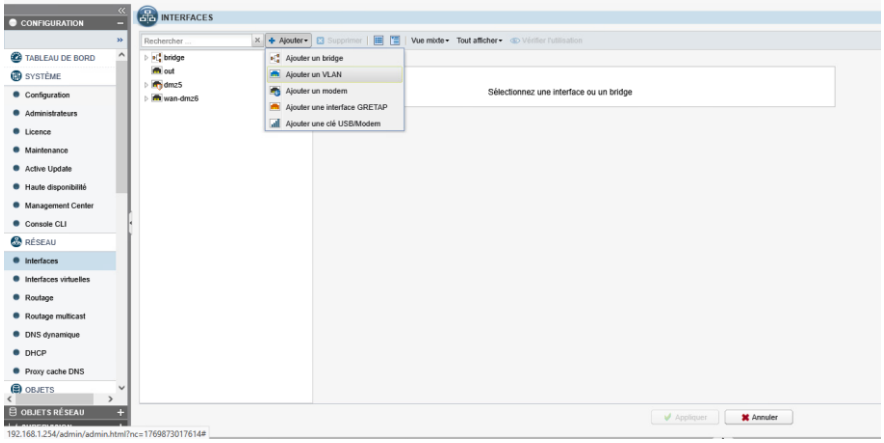


Ensuite, nous allons configurer les interfaces. Dans mon cas, je vais créer des VLANs et utiliser les interfaces sorties du bridge pour héberger les VLANs.

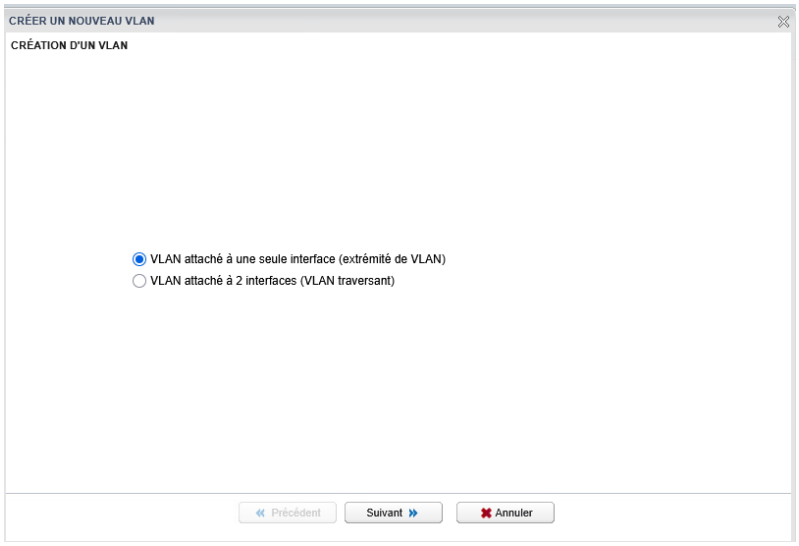
Ensuite, allez sur les interfaces que vous allez utiliser pour les VLANs, puis dans Plan d'adressage, cochez la case IP Dynamique (obtenue par DHCP). Ainsi, l'interface n'obtiendra pas d'IP.



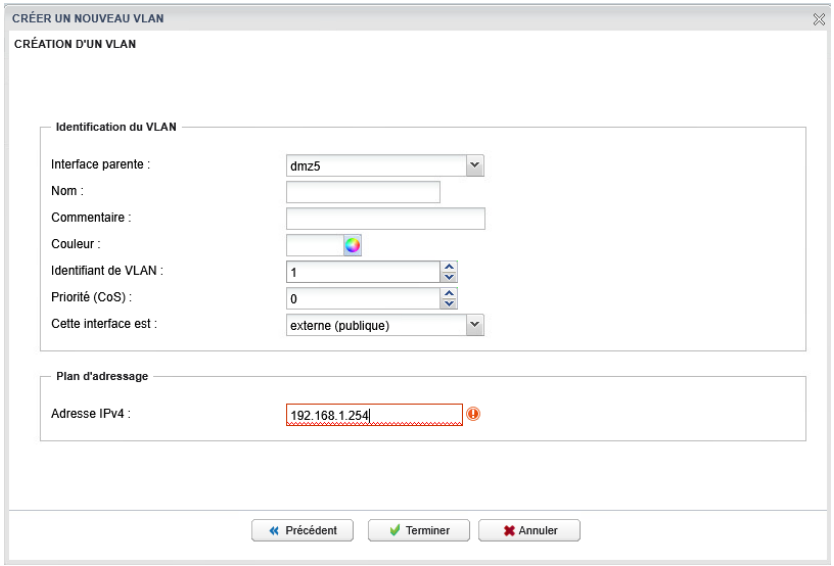
Pour créer un VLAN, cliquez sur le bouton **Ajouter**, puis sélectionnez **Ajouter un VLAN**.



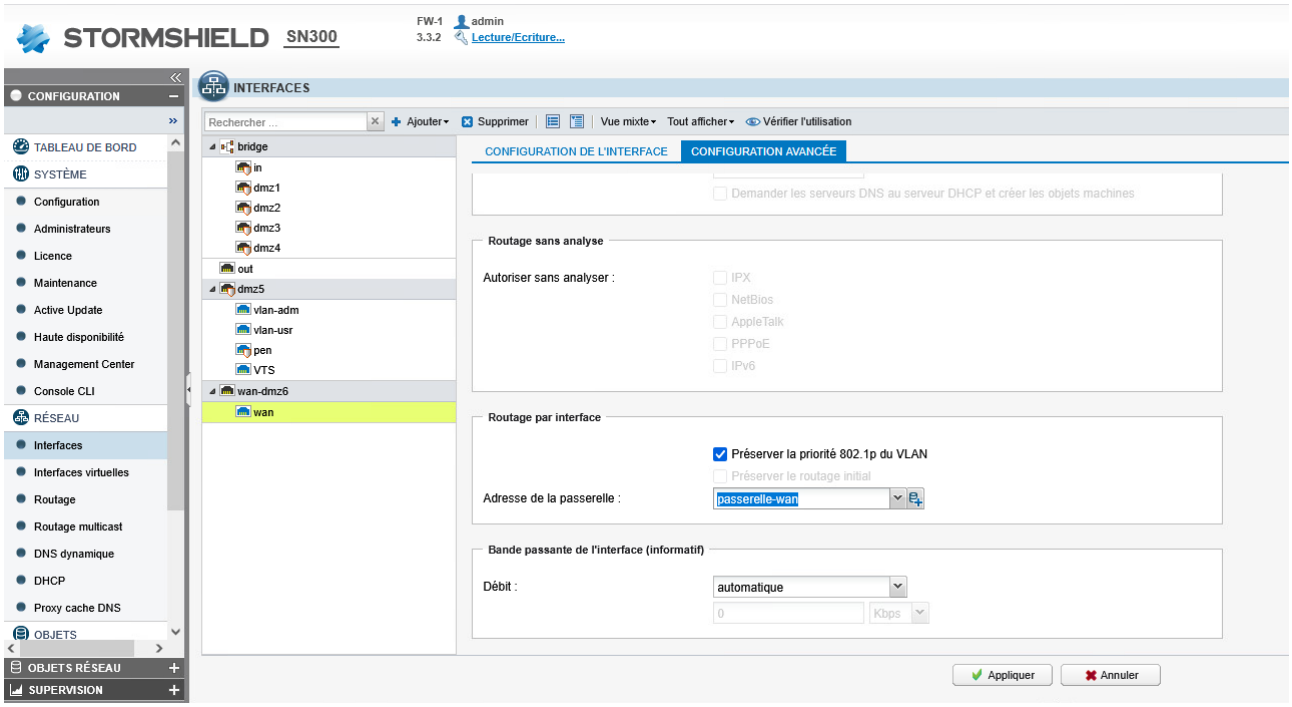
Si votre VLAN sera présent sur une seule interface, cochez l'option **VLAN attaché à une seule interface**.



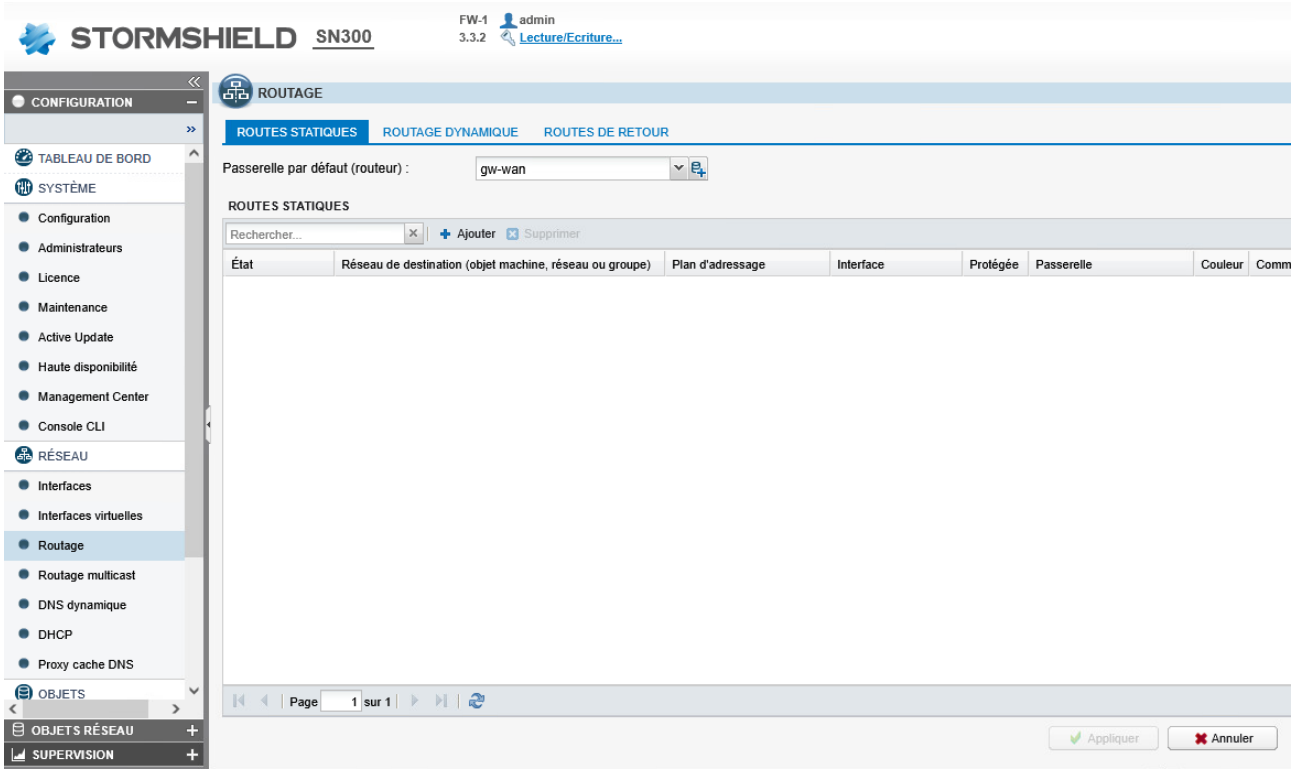
Ensuite, ici, vous devrez choisir l'interface parente du VLAN, nommer votre VLAN, choisir l'ID du VLAN, indiquer si cette interface est externe ou interne, puis définir l'IP que le routeur aura sur le VLAN.



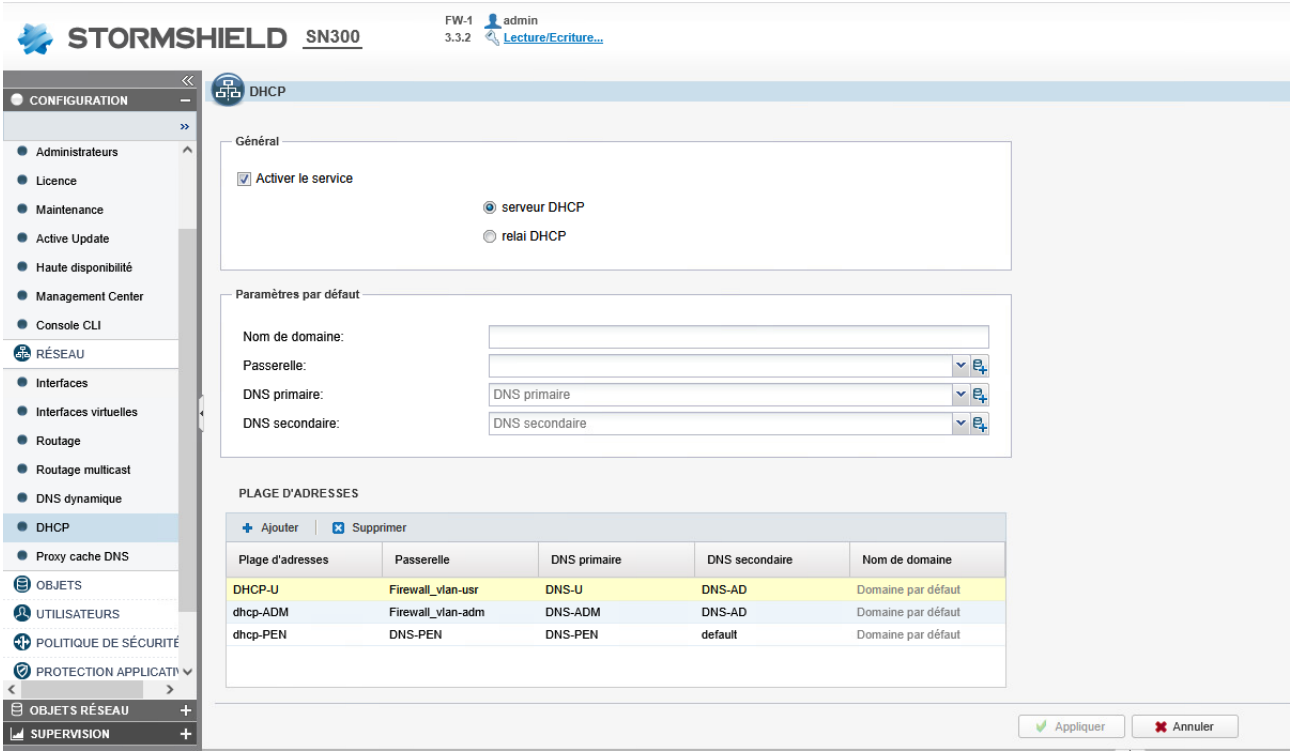
Répétez l'opération pour tous les VLANs que vous souhaitez attribuer.
Une fois vos VLANs créés, attribuez-leur les passerelles par défaut dans l'onglet **Configuration avancée**.
Pour les interfaces LAN, mettez l'IP du routeur du réseau en passerelle.



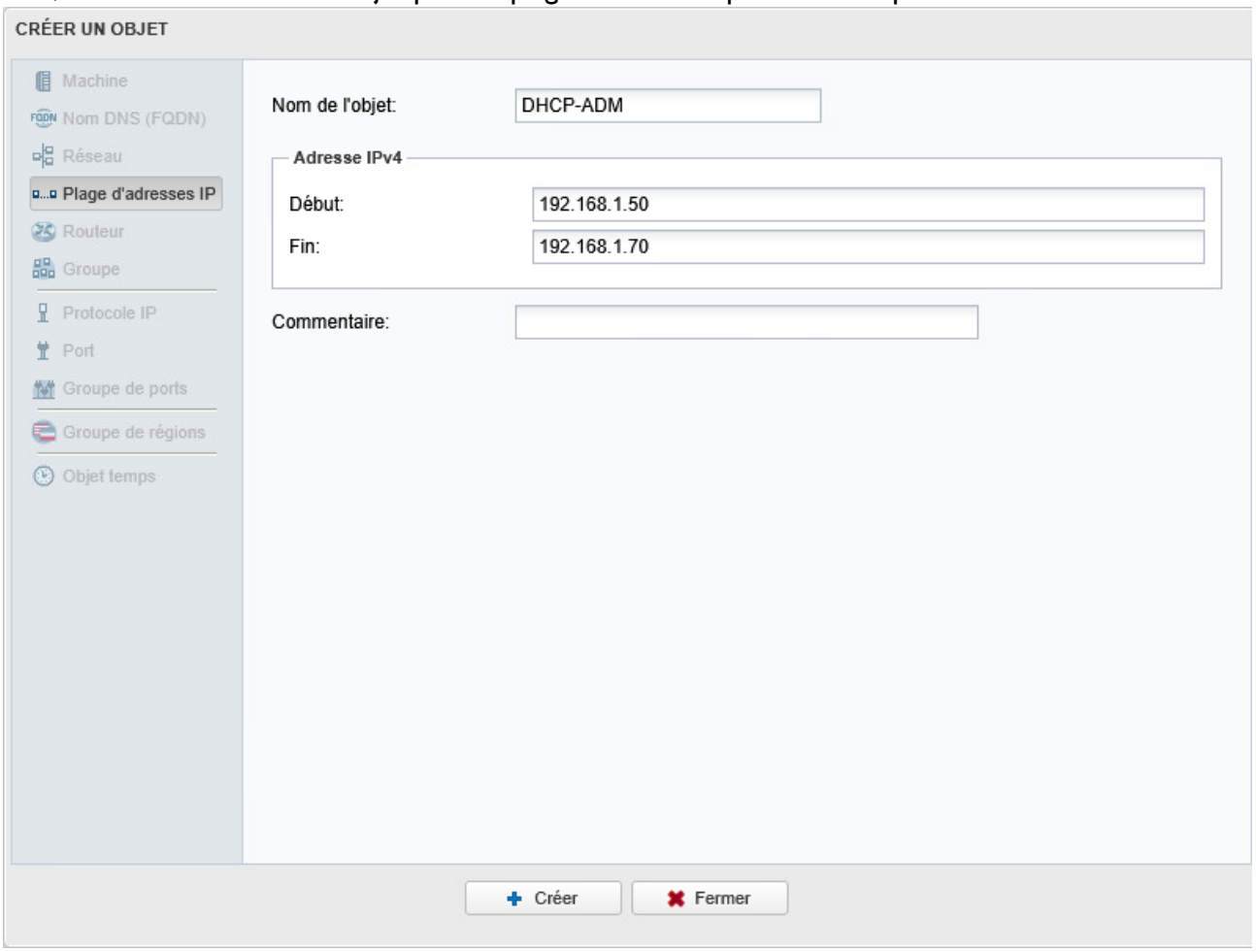
Ensuite, nous allons configurer la passerelle par défaut. Pour ce faire, allez dans l'onglet **Routage**, puis dans le champ **Passerelles par défaut**, mettez-y l'objet correspondant à l'IP WAN du routeur.



Ensuite, nous allons configurer notre routeur en tant que serveur DHCP.
Allez dans la section **DHCP**, et assurez-vous que la case **Serveur DHCP** soit cochée.
Pour ajouter une plage d'adresses DHCP, cliquez sur le bouton **Ajouter**.



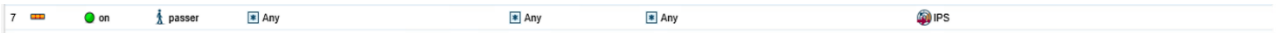
Puis, vous devrez créer un objet pour la plage d'adresses que le DHCP pourra attribuer.



Une fois la plage d'adresses créée, il faut lui attribuer un DNS et une passerelle. Vous devrez les créer si cela n'est pas déjà fait.

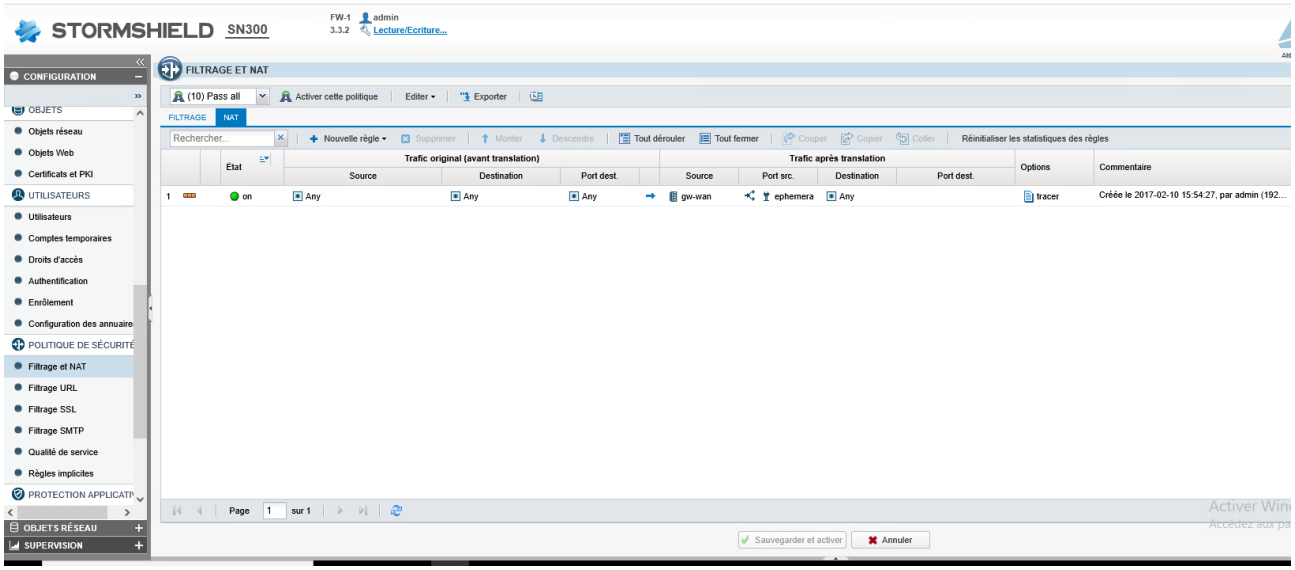
Pour finir, il ne nous reste plus qu'à configurer les règles de NAT et de filtrage réseau pour accéder à Internet et aux autres réseaux distants.
Allez dans la section **Filtrage** et **NAT**.

Ensuite, dans les règles de filtrage, je vais créer une règle qui laisse passer tout le trafic. À terme, il faudra retirer cette règle, car elle est peu sécurisée ; elle laisse passer n'importe quel trafic en provenance de n'importe quel réseau.



Ensuite, nous allons créer une règle de NAT qui va traduire l'IP des réseaux privés par l'IP publiquedu firewall.

La règle ressemblera à cela : la source, au niveau du trafic après translation, sera l'IP publique du firewall.



Après avoir configuré ces règles, normalement, notre réseau local devrait avoir accès à Internet.

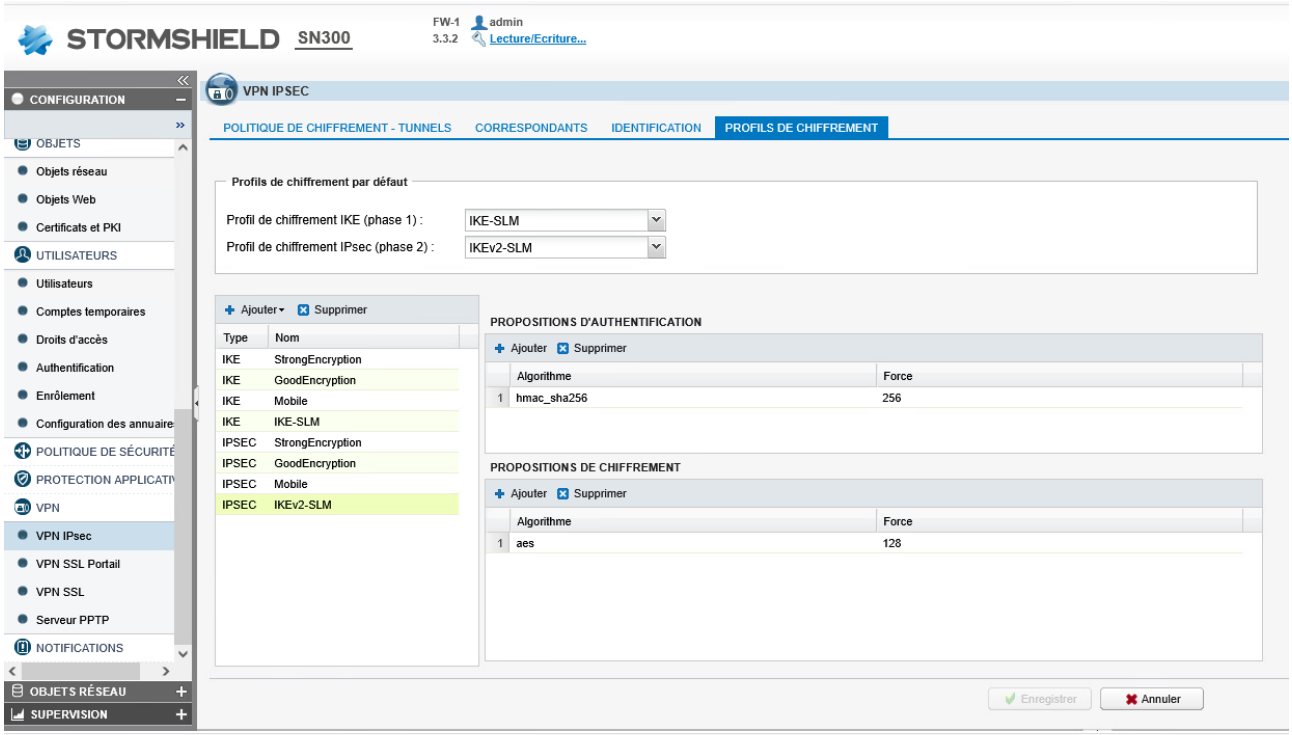
Création du VPN IPSEC

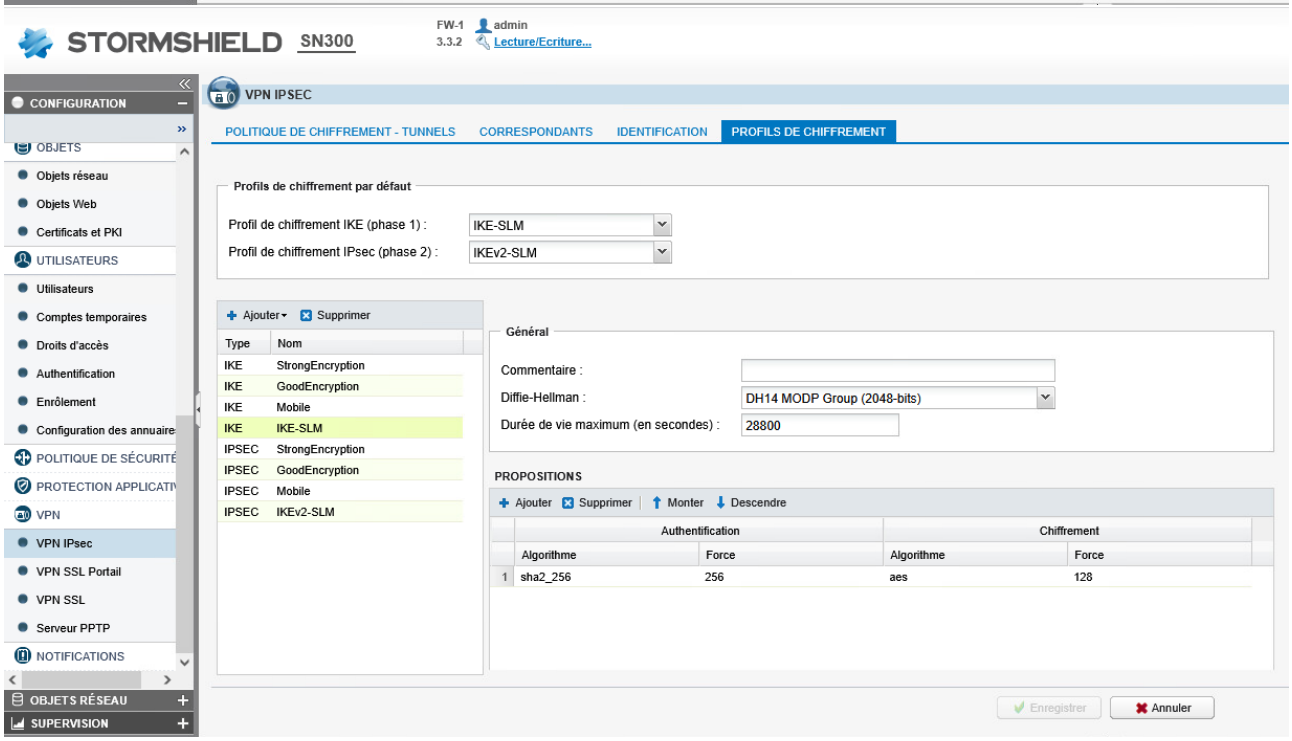
Maintenant, nous allons créer le VPN IPSec pour relier mes deux sites : Lyon et SLM.

Pour ce faire, allez dans l'onglet **VPN**, puis dans la catégorie **IPSec**.

Ensuite, allez dans la section **Profils de chiffrement**.

Ici, nous allons créer deux profils : un pour la phase 1 et le second pour la phase 2.
Configurez les deux profils selon les algorithmes de chiffrement souhaités.
.





Ensuite, allez dans l'onglet correspondant.

Créez un nouveau correspondant et renseignez les champs comme suit :

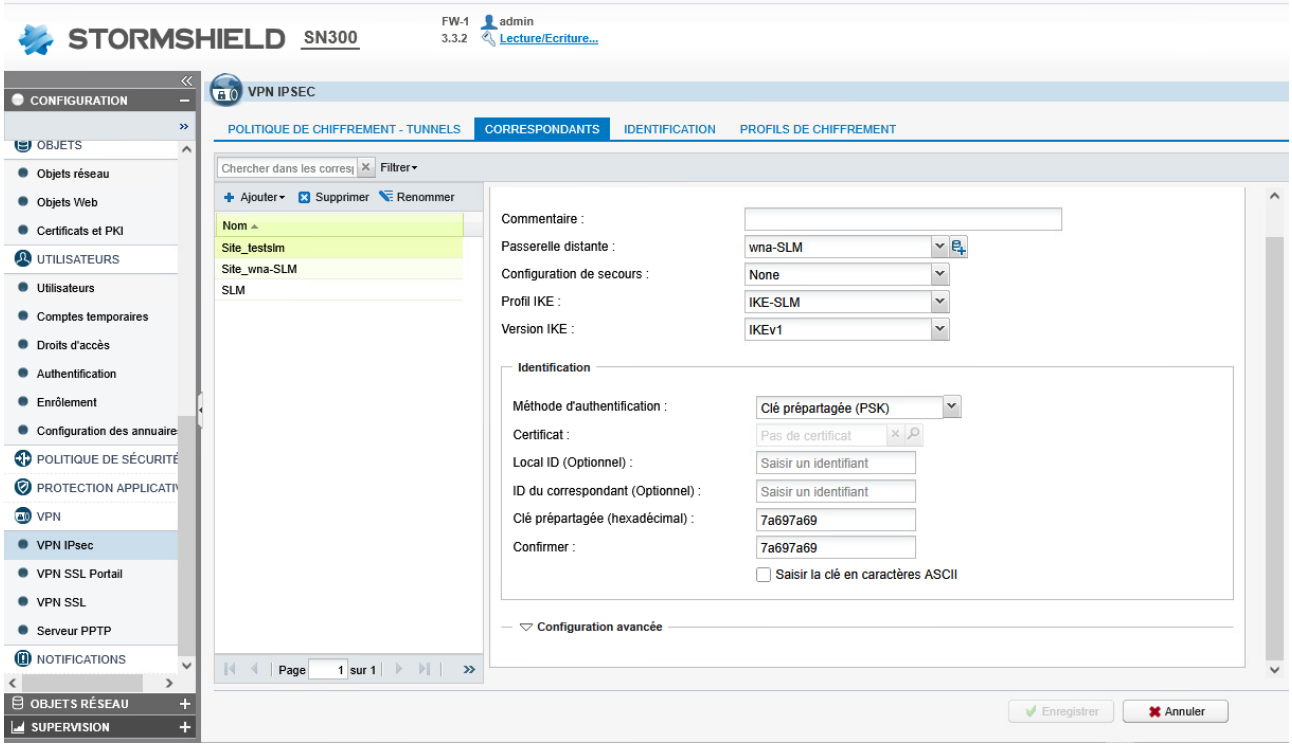
Passerelle distante : IP publique du réseau distant

Profil IKE : renseignez le profil de chiffrement de la phase 1 créé précédemment

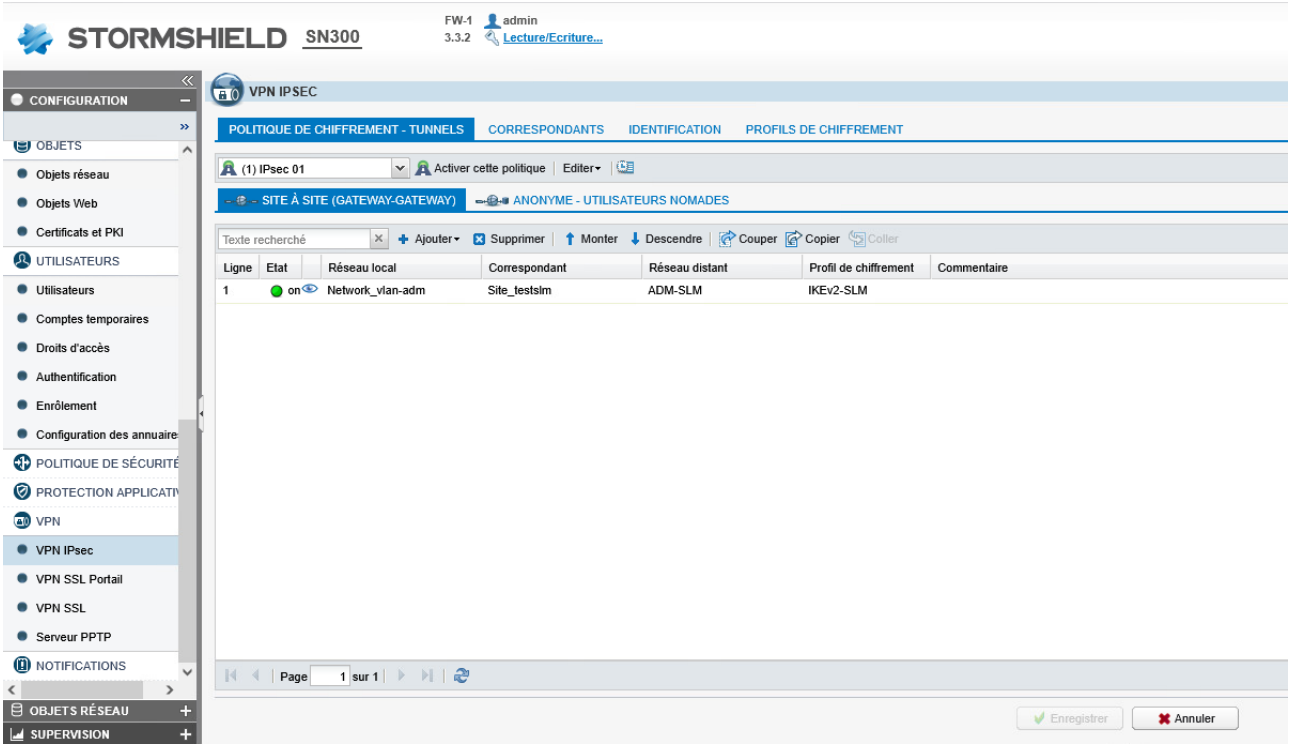
Version IKE : sélectionnez la version IKE souhaitée

Méthode d'authentification : choisissez votre méthode d'authentification

Clé prépartagée : renseignez la clé d'authentification

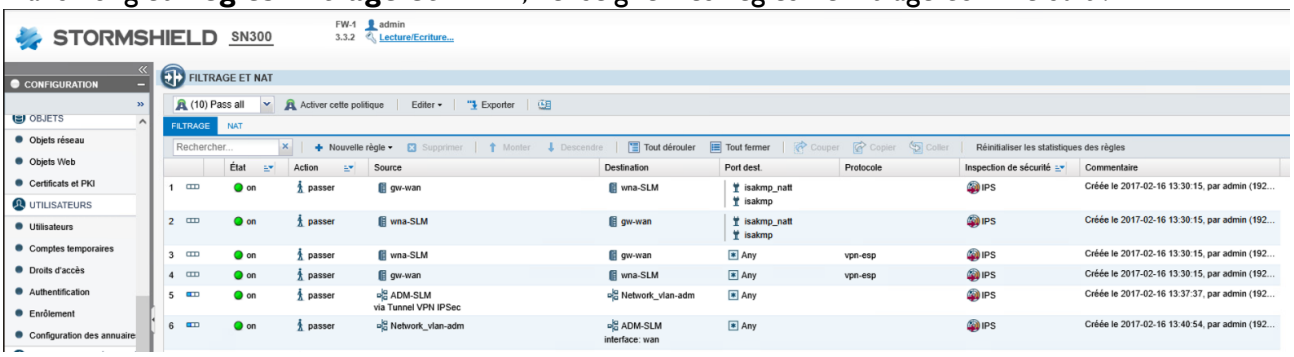


Ensuite, dans Politique de chiffrement – Tunnel, créez un nouveau tunnel IPSec. Comme source, sélectionnez le réseau local désiré et, comme destination, renseignez le réseau local distant souhaité. Puis, sélectionnez le correspondant que vous avez créé.



Une fois le tunnel IPSec configuré, nous allons ajouter les règles de filtrage pour permettre la communication avec le site distant.

Dans l'onglet **Règles Filtrage et NAT**, renseignez les règles de filtrage comme suit :



Dans l'image, **network_vlan-adm** représente mon réseau local, **ADM-SLM** représente le réseau local distant, **wan-slm** représente l'IP publique distante, et **gw-lan** est l'IP publique de mon site local.

Une fois ces règles configurées, nos deux sites pourront communiquer entre eux.