Nom du document	Version	Date de MAJ	Auteure	Contenu
Stormshield Bases - Fiches1a8-v1-2.docx	1.2	**01/03/2022**	V Martinez	Cours issu du support CSNA v4 Routage, NAT, Filtrage Lab 1 à 6 VPN SSL et VPN IPSec

Support de formation réalisé dans le cadre du partenariat Stormshield Académie avec le réseau national Certa
Relecture de Quentin Démoulière et de l'équipe formation Stormshield

Remarques

Les fiches pratiques des travaux en laboratoire peuvent se traiter de manière indépendante une fois que la configuration de base de la plateforme est réalisée (Fiche N°1).
Ce support se base sur la version 4.2 du firmware du pare-feu SNS et du support de formation officiel Stormshield.
Ce support concerne l'utilisation de boitiers physiques ou de VM hébergées dans une ferme de serveurs. Pour l'utilisation de VM en autonomie, reportez-vous à la version « VirtualBox » ou au Kit CSNA de Stormshield.

Table des matières

I Présentation du document

Objectif du document

Ce support comporte des fiches pratiques de travaux en laboratoire permettant d'exploiter les pare-feu Stormshield SNS virtuels ou physiques dans le cadre du bloc 3 sur la cybersécurité.
Il est basé sur les documents et les laboratoires de la formation officielle Stormshield pour les formations CSNA et CSNE et a été réalisé dans le cadre du partenariat Stormshield Académie avec le réseau national Certa.

Utilisation du document

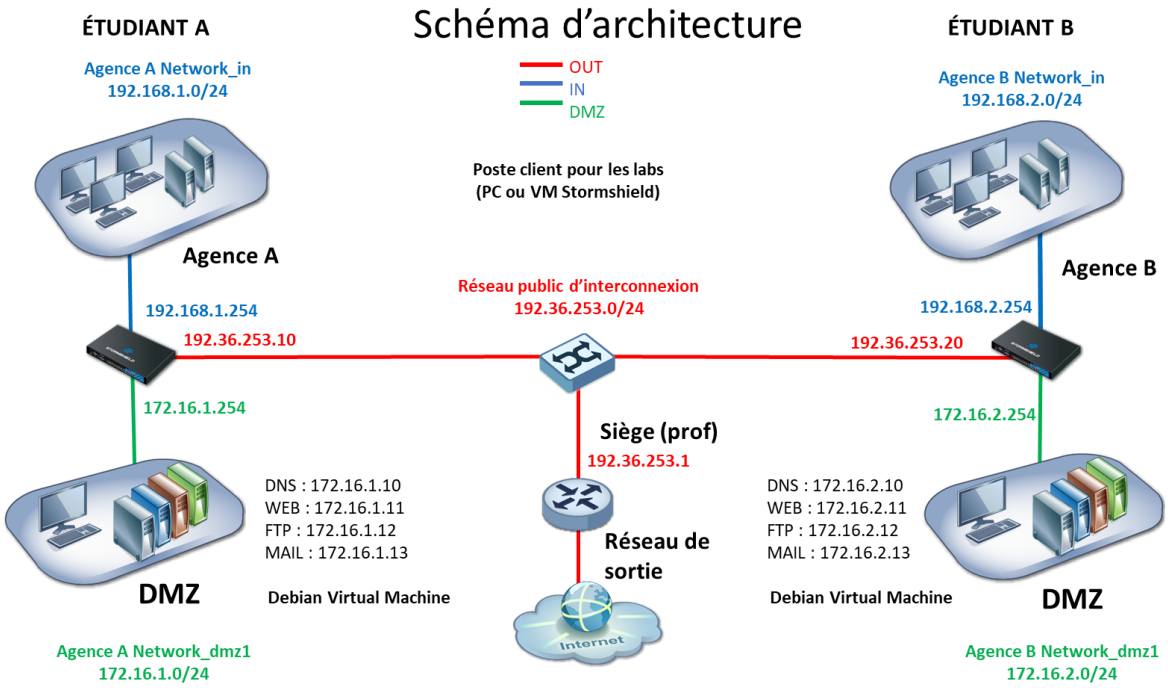
Chaque fiche pratique est un exemple destiné à aborder certaines compétences du bloc 3. Les professeurs peuvent reprendre, en l'état, ces fiches pratiques ou les modifier pour les intégrer dans leurs travaux en laboratoire. Le support vise l'option SISR et comporte plusieurs fiches en fonction du thème abordé.

II Présentation de l'architecture du laboratoire

Stormshield, dans le cadre du partenariat avec le réseau Certa fournit gratuitement les machines virtuelles de sa plateforme de formation (le pare-feu Stormshield SNS, un serveur Debian en DMZ, un client graphique linux optionnel) exploitables sous VirtualBox, ou après conversion sur un hyperviseur pour l'ensemble des étudiants (n agences et le siège). Nous nous placerons dans ce second cas où chaque étudiant gère une agence reliée via un réseau public d'interconnexion factice aux autres agences et au pare-feu de l'enseignant (siège). Si l'établissement possède des boitiers physiques, l'infrastructure sera identique. Si vous utilisez les kits en autonomie, reportez-vous à l'annexe **Annexe – Paramétrage du lab virtuel sous Virtual Box** ou à la documentation d'installation des laboratoires fournie dans le kit de formation CSNA Stormshield pour la configuration des réseaux virtuels.
Dans la suite du texte, le terme **pare-feu SNS** concerne l'appliance virtuelle (EVA1) ou le boîtier physique Stormshield. L'architecture proposée (issue du kit de formation CSNA Stormshield) est constituée de plusieurs agences (A, B, C…) correspondant à chaque étudiant et d'un siège géré par l'enseignant. Chaque agence possède une plateforme composée d'un pare-feu SNS Stormshield (physique ou virtuel), d'une machine cliente (physique ou virtuelle) et d'un serveur virtuel Debian préconfiguré avec des services accessibles en DMZ (DNS, WEB, FTP et MAIL) et présentant volontairement des vulnérabilités.
Chaque agence comporte un réseau interne privé **IN,** une **DMZ** et un réseau d'interconnexion **OUT** (simulant le WAN) relié au siège de l'entreprise où le pare-feu SNS Siège est configuré pour permettre l'accès à Internet des agences via le réseau du BTS SIO.

Fiche pratique n°1 : Configuration de base avec NAT/PAT accès Internet

Le schéma ci-dessous représente l'architecture de la plateforme avec 2 agences et un réseau d'interconnexion avec le « siège ».



Chaque agence est composée :

- d'un réseau externe **OUT** « 192.36.253.x0/24 » auquel les firewalls de toutes les agences sont reliés via leur interface **OUT** (WAN) ;
- d'un réseau interne **IN** Agence x « 192.168.x.0/24 » relié à l'interface **IN** du pare-feu SNS avec un poste d'administration et de test utilisateur : machine virtuelle cliente graphique (client Linux fourni ou autre VM) ;
- d'un réseau **DMZ1** « 172.16.x.0/24 » avec des services (DNS, WEB, FTP, MAIL) intégrés dans la machine virtuelle Debian serveur fournie dans le kit Stormshield CSNA ;
- et en option d'un réseau **DMZ2** d'administration en DHCP relié au LAN BTS SIO interne accessible depuis une machine physique du BTS SIO sans modification de configuration (cette configuration sera indispensable dans le cas de l'utilisation de machines virtuelles SNS, et peut être intéressante également avec des boîtiers physiques type SN310).

Plan d'adressage du pare-feu SNS

em0	@Interface **OUT** 192.36.253.x0 /24	**OUT** : Réseau d'interconnexion « 192.36.253.x0 /24 »
em1	@Interface **IN** 192.168.x.254 /24	**IN** : Réseau interne Agence X « 192.168.x.0/24 »
em2	@Interface **DMZ1** 172.16.x.254 /24	**DMZ1** : Réseau DMZ « 172.16.x.0/24 »
em3	@Interface **DMZ2** DHCP	**DMZ2 (optionnelle)** : Réseau d'administration BTS SIO

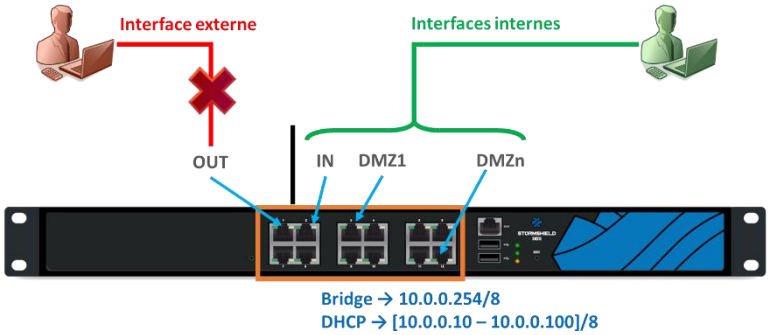
NB : L'architecture ci-dessus peut être étendue à plus que deux agences en respectant le plan d'adressage ci-dessus. Il suffira de modifier le « **x** » suivant la lettre de l'agence **A⇒1**, B⇒2, C⇒3, D⇒4…

La machine cliente graphique doit disposer d'un navigateur web et d'un accès administrateur pour modifier les paramètres réseaux ; vous pouvez utiliser n'importe quelle VM sous Linux ou Windows.

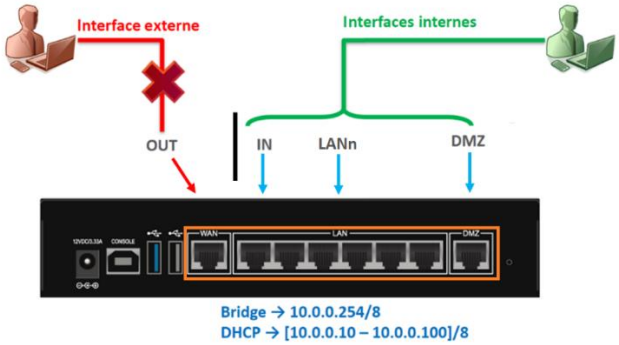
NB : Les boitiers SN210 disposent quant à eux de 3 interfaces distinctes : une interface **OUT***, d'une interface* **IN***, d'interfaces LANx qui correspondent à des ports de type commutateur et d'une interface* **DMZ***. La configuration présentée ci-dessus devra donc être adaptée en fonction des équipements utilisés.*

Phase 1 Prise en main – configuration initiale

Avertissement : les manipulations décrites ici peuvent être complétées par celles décrites dans le chapitre Prise en main du firewall (p40) du support de cours CSNA Stormshield.
La configuration d'usine par défaut du *pare-feu SNS* (boîtier ou appliance VM laboratoire) est la suivante.
La première interface **(1)** du pare-feu SNS physique est nommée « **OUT** », la seconde « **IN** » et le reste des interfaces « **DMZx** ». L'interface « OUT » est une interface **externe**, utilisée pour connecter le pare-feu SNS à internet et le reste des interfaces sont **internes** et servent principalement à connecter le pare-feu SNS à des réseaux locaux.



La distinction interne/externe pour les interfaces permet de se protéger contre les attaques d'usurpation d'adresse IP.
Le schéma présenté ci-dessous correspond, quant à lui, à un boîtier SN210. Comme vous pouvez le constater, l'organisation des interfaces est différente de celle des machines virtuelles ou des modèles SN310 et supérieur.



En configuration usine, sur un **boitier physique** de type SN210 ou SN310 ou sur les **VM individuelles VirtualBox** de labo, **toutes les interfaces sont incluses dans un bridge** dont l'adresse est 10.0.0.254/8. Sur les **boitiers physiques**, un serveur DHCP est actif sur toutes les interfaces du bridge et il distribue des adresses IP comprises entre 10.0.0.10 et 10.0.0.100. L'accès à l'interface web de configuration du pare-feu SNS se fait avec l'url : **`https://10.0.0.254/admin`.**
Un bridge (ou pont) est un mode de configuration qui regroupe toutes les interfaces physiques du pare-feu en une entité logique. Ceci permet d'avoir plusieurs réseaux physiques partageant le même réseau logique. Grâce à ce mode, le firewall Stormshield peut s'intégrer de manière transparente à un réseau existant sans devoir en modifier la configuration.

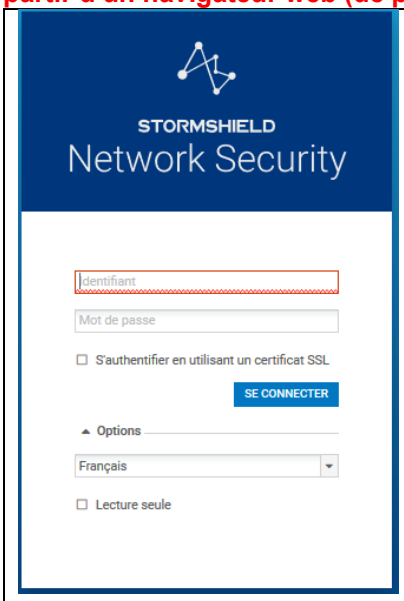
Par défaut, seul le compte système **admin** (mot de passe par défaut **admin**), disposant de tous les privilèges sur le boîtier, existe et peut s'y connecter.
Remarque : Sur une VM installée sur une ferme de serveurs, il est recommandé d'utiliser le mode de remise à zéro de la configuration pour lancer un dialogue de pré-configuration qui va vous demander de changer le mot de passe par défaut (8 caractères et Maj/min demandés), de configurer vos interfaces, le clavier de la console… La manipulation est décrite en annexe de ce document.

1.1 - Connexion au pare-feu SNS

Pour accéder à l'interface d'administration du pare-feu SNS, il est indispensable de connecter votre machine cliente (physique ou virtuelle) sur une interface interne (**IN** ou **DMZ1 ou 2**) sous peine de devoir redémarrer le firewall qui aura détecté une tentative d'usurpation d'adresse IP sur le bridge et bloquera tout le trafic généré par la machine connectée sur l'interface **OUT**.
Pour faciliter la mise en place de la configuration initiale du pare-feu SNS de votre agence, nous l'administrerons depuis une interface en DMZ (**DMZ2** si elle existe) qui sera momentanément reliée à une machine physique, soit en direct sur le boitier soit sur une ferme de serveurs via le réseau local du BTS SIO.

➢ Vérifiez que votre machine cliente a bien obtenu une adresse IP dans la plage **10**.0.0.0**/24**, ou sur le réseau du BTS SIO, le cas échéant la configurer manuellement : attribuez-lui une adresse IP fixe en **10.0.0.x0/24** avec pour passerelle **10.0.0.254**.
NB : avec le client Linux graphique Stormshield, utiliser le script **network_config.sh** (double-cliquer puis **Run in Terminal**) et choisir **Y** pour oui puis **sns**, et donner le mot de passe *toor* par défaut, l'adresse IP de la VM est alors configurée en 10.0.0.2/24.

L'accès à l'interface graphique d'administration du pare-feu SNS se fait par https://10.0.0.254/admin à partir d'un navigateur web (de préférence Firefox, Chrome ou Edge)



L'écran ci-contre apparaît pour vous connecter une fois le pare-feu SNS démarré.

Pour modifier les options de langue de l'interface web d'administration, dépliez **Options** puis choisissez la langue.

La fenêtre est actualisée, vous pouvez vous connecter à nouveau.

Saisir l'identifiant **admin,** le mot de passe **admin** ou celui que vous avez dû configurer si vous avez effectué la réinitialisation de la machine virtuelle (par ex **Sio2022*** ou autre).

Remarque : pour s'authentifier, l'utilisateur peut également sélectionner un certificat SSL dans le magasin de son navigateur (à configurer au préalable dans les préférences du pare-feu SNS). Nous étudierons cette possibilité dans la partie avancée sur la mise en place d'une PKI avec Stormshield

NB : Pour des raisons évidentes de sécurité, il conviendra de modifier ce mot de passe lorsque le pare-feu SNS sera utilisé en contexte réel d'entreprise.

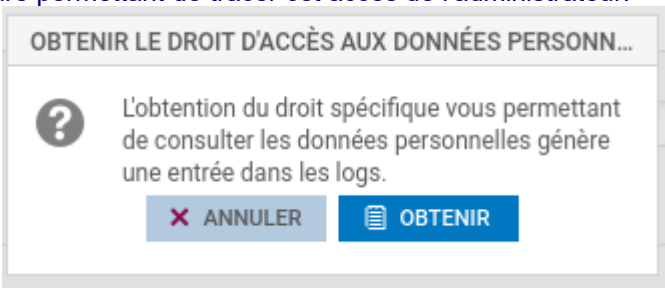
1.2 - Interface d'administration du pare-feu SNS

La page d'accueil de votre pare-feu SNS s'ouvre sur un **Tableau de bord** qui permet de visualiser un certain nombre d'informations sur votre équipement et est personnalisable.

L'interface d'administration est découpée en quatre parties :

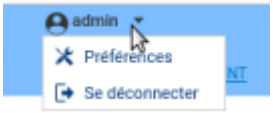
1. **L'en-tête (partie encadrée en vert)** contient les informations suivantes :
   - le **nom** du pare-feu SNS : le nom par défaut est le numéro de série,
   - la **version du système** (firmware),

- l'**utilisateur connecté** sur l'interface et ses droits d'accès à la configuration : lecture seule ou écriture ÉCRITURE. Vous pouvez acquérir ou **libérer le droit d'écriture** en cliquant sur l'icône. Notez qu'à un instant donné, un seul utilisateur peut disposer du droit d'écriture sur le pare-feu SNS.
- les droits d'accès aux logs : restreint ACCÈS RESTREINT ou complet, vous pouvez obtenir le droit d'accès aux données personnelles en cliquant sur l'icône **Accès restreint** puis **Obtenir** dans la fenêtre de confirmation.
  NB : le fait de demander l'accès aux données personnelles des logs, inscrit dans les logs une ligne supplémentaire permettant de tracer cet accès de l'administrateur.



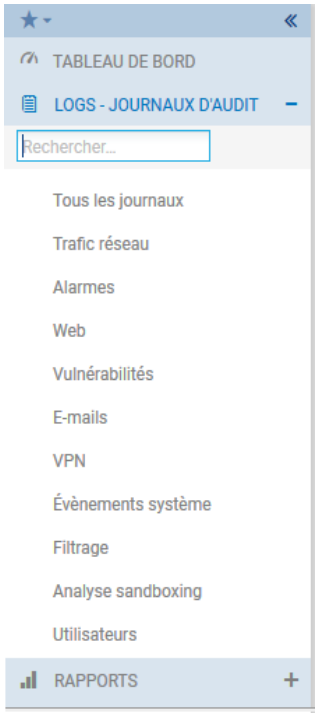
- un lien **?** vers **l'aide en ligne** du menu courant ainsi que des informations complémentaires sur les paramètres et les options du menu.

💻 **Cliquez sur la flèche à droite du nom d'utilisateur** (admin) permet d'accéder aux préférences générales d'administration et à la déconnexion de l'administrateur.



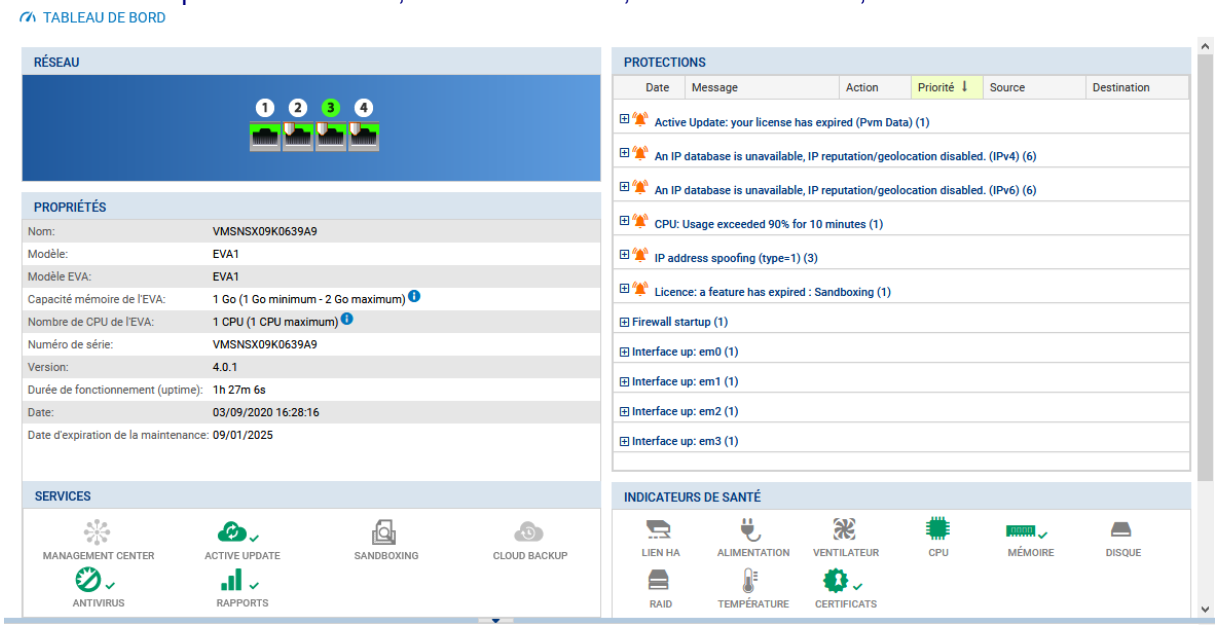
- Le menu « **Préférences** » permet de configurer plusieurs paramètres en relation avec l'interface d'administration. Les plus importants sont :
  - Le **temps d'inactivité** avant de déconnecter l'utilisateur de l'interface d'administration (30 minutes par défaut) ;
  - Les options d'affichage dans les menus (toujours afficher les configurations avancées, nombre de règles de filtrage par page, etc.) ;
  - Liens externes vers les sites Stormshield
- **Se déconnecter** : déconnecte l'utilisateur courant.

2. **Les menus (partie encadrée en rouge)** regroupent les menus de configuration, de supervision (Monitoring) ainsi que des raccourcis organisés sous forme de listes rétractables.



Les menus sont séparés en 2 catégories qui s'affichent ensuite sur la zone de menu de gauche constituée d'un ensemble de panneaux qui permettent d'accéder aux différents menus de votre pare-feu SNS.
L'onglet **Monitoring** pour tout ce qui touche à la supervision, les log et l'état du pare-feu SNS.
L'onglet **configuration** pour les objets et le paramétrage des diverses fonctionnalités.

3. **Le contenu du menu (partie encadrée en bleu)** affiche le contenu du menu sélectionné.
4. **Les traces de l'interface d'administration (partie encadrée en marron)** affichent une liste (paramétrable) des logs de l'interface web. On peut y faire apparaitre par exemple les commandes NSRPC exécutées par l'interface web, les erreurs levées, les avertissements, ….



Le **`Tableau de bord`**, regroupe l'ensemble des informations et indicateurs du pare-feu SNS :

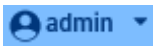
- ❖ État du module Active Update ;
- ❖ Alarmes ;
- ❖ Licence (date d'expiration de chaque module),
- ❖ Propriétés (N° de série, politiques actives, date et heure…) ;
- ❖ Interfaces (listing des interfaces réseau configurées) ;
- ❖ État des différents services.

Un clic sur un élément du tableau de bord renvoie directement vers la page de supervision ou de configuration liée à cet élément.

1.3 - Configuration générale

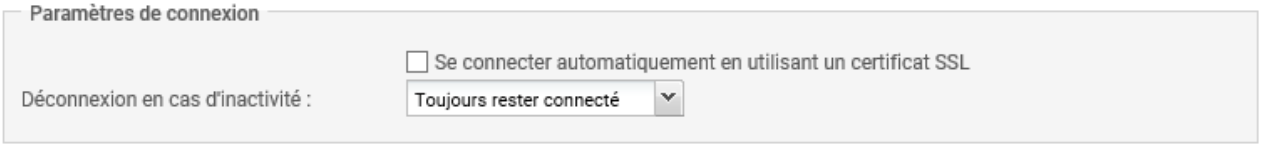
Nous verrons ci-après un certain nombre d'éléments de configuration générale utiles pour la bonne mise en œuvre de votre pare-feu SNS. Nous étudierons notamment les éléments du menu **`Configuration / Système`** qui correspond à la configuration générale : licence, mise à jour, mot de passe...

Afin de ne jamais être déconnecté en cas d'inactivité sur l'interface d'administration pendant ces exercices pratiques, il conviendra de modifier vos préférences, en usage réel vous utiliserez un délai de 5 minutes pour éviter de laisser votre session ouverte sur le pare-feu SNS.

- Cliquez sur la flèche à droite de l'icône représentant l'utilisateur connecté 

en haut à droite.
- Cliquez sur l'icône **Préférences** 

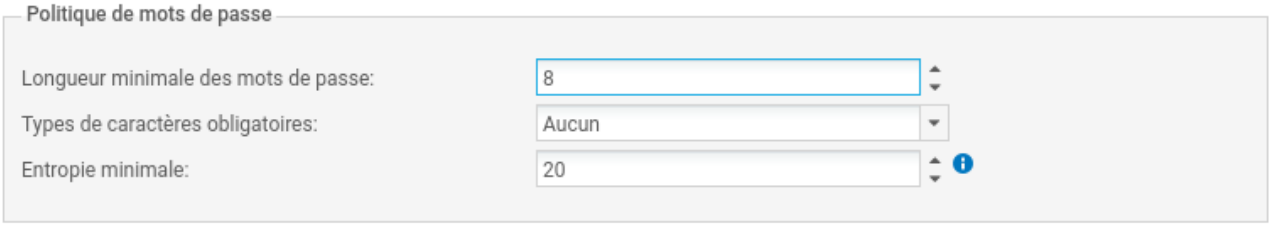
- Dans la zone **Paramètres de connexion**, sélectionnez dans la liste "Déconnexion en cas d'inactivité :" la valeur **Toujours rester connecté**.



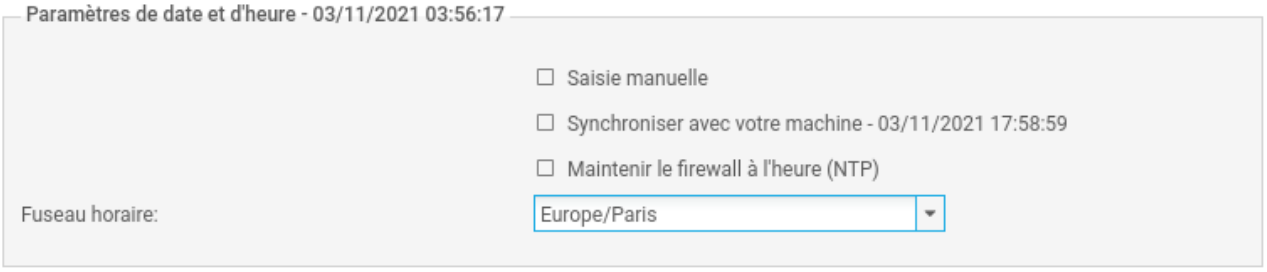
- Sélectionnez dans le menu à gauche **Configuration / Système** puis **Configuration**. Le volet **Configuration générale** est affiché.
- Commencez par donner un **nom** à votre boîtier : FWX_AgenceX et **changer la langue** de la console.

Nous laisserons les logs en anglais : *Langue du Firewall(traces)* afin de pouvoir rechercher plus facilement des références à d'éventuels problèmes dans les ressources documentaires Stormshield et sur les forums avec les bons mots-clés.

➢ La zone **Politique de mots de passe** permet de définir la longueur du mot de passe (8 par défaut) et la zone **Types de caractères obligatoires** permet de gérer la complexité du mot de passe (Aucun, Alphanumériques, Alphabétiques et spéciaux), la zone **Entropie minimale** correspond à la robustesse du mot de passe. En utilisation en entreprise, il est recommandé de changer le mot de passe de l'administrateur et d'augmenter à 12 le nombre de caractères. Nous laisserons les valeurs par défaut.

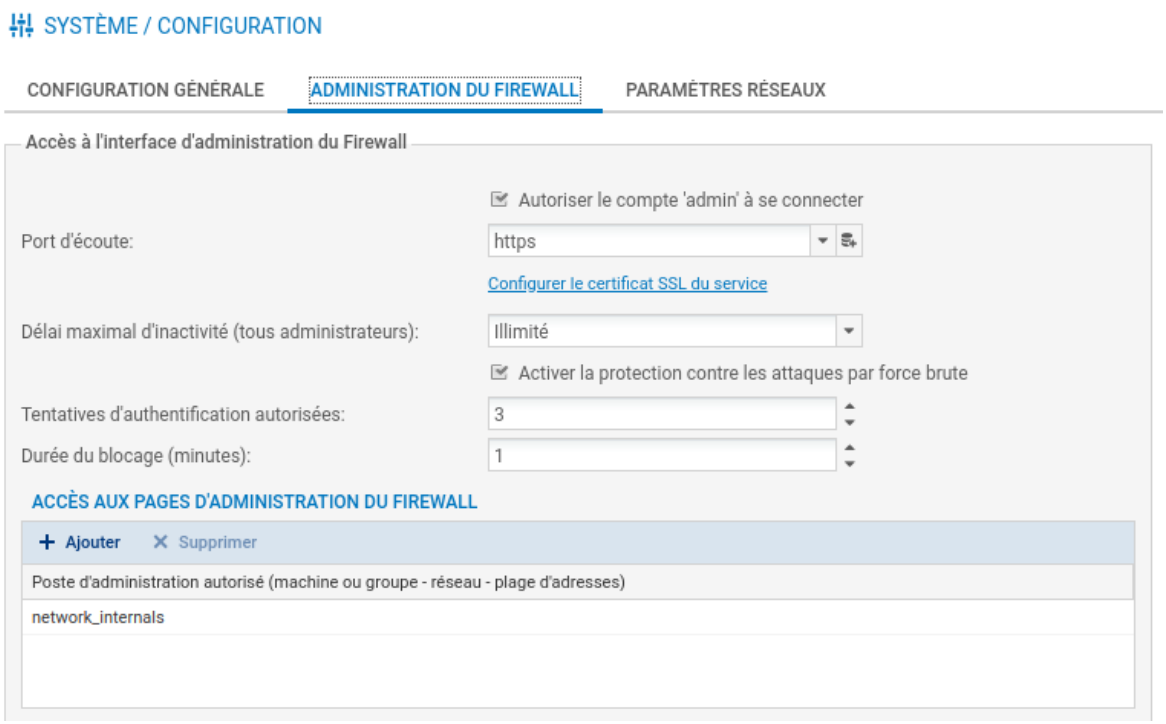


- La zone **Paramètres de date et d'heure** permet de modifier le fuseau horaire dans la zone **Fuseau horaire**, sélectionnez **Europe/Paris**.



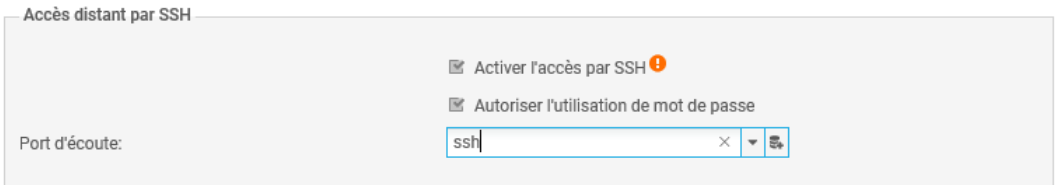
NB : La modification du fuseau horaire implique un redémarrage immédiat, pour ne pas avoir de décalage dans les journaux ou avec une PKI.

- Cliquez le bouton **Appliquer** pour sauvegarder la configuration et **Sauvegarder**.
- Dans le volet **Système / Configuration**, ouvrez l'onglet **Administration du firewall** pour visualiser les options de configuration de l'administration du pare-feu.



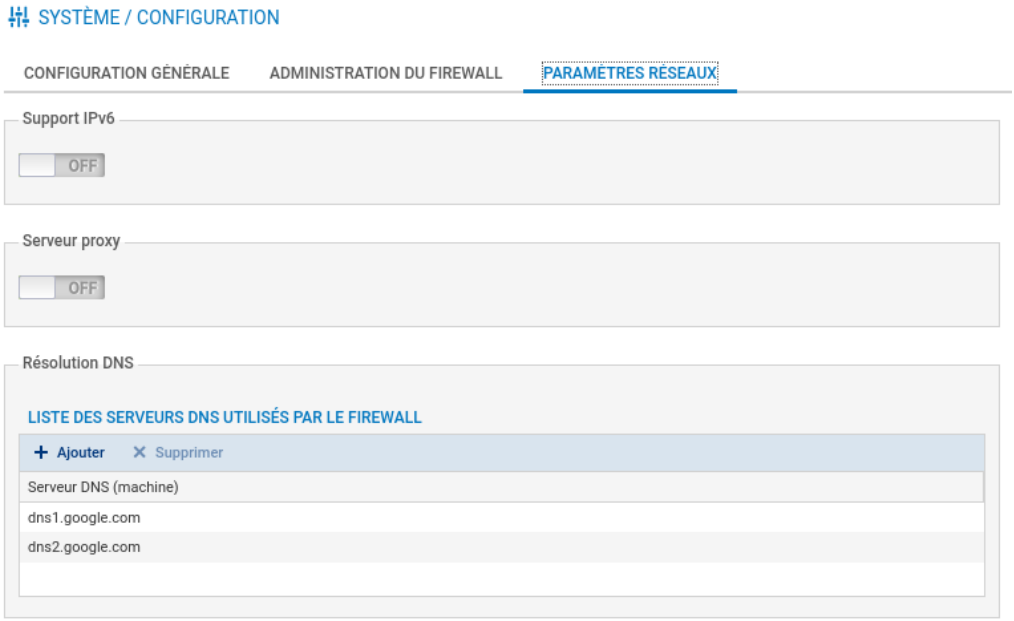
Plusieurs options sont configurables :

- Il est possible de ne plus autoriser le compte « admin » à accéder à l'interface d'administration. Cela implique qu'un nouvel administrateur ait été créé avec des droits suffisants. Dans le cas contraire, vous perdrez définitivement l'accès à l'interface d'administration du firewall.
- Le port utilisé pour accéder à l'interface d'administration du firewall peut être un autre port que le standard HTTPS (443/TCP), défini par défaut. L'URL d'accès devient alors : *https://@IP_firewall:port/admin.*
- Par défaut, l'interface d'administration du firewall utilise un certificat issu de l'autorité de certification du firewall. Le lien « Configurer le certificat SSL pour l'accès à l'interface d'administration » renvoie vers le menu qui permet de modifier ce certificat.
- Le délai maximal d'inactivité peut être défini pour tous les administrateurs. Un administrateur peut configurer un temps de déconnexion en cas d'inactivité dans ses préférences (menu accessible en cliquant sur son nom utilisateur), si ce temps de déconnexion est inférieur ou égal au délai maximal paramétré.
- La protection contre les attaques force brute pour l'accès à l'interface d'administration peut être activée/désactivée et le nombre de tentatives ainsi que le temps d'attente (en minutes) sont paramétrables. Par défaut, après 3 tentatives d'authentification infructueuses, l'accès depuis cette adresse IP sera bloqué pendant 1 minute.
- L'accès à l'interface d'administration peut être limité à une machine ou un réseau spécifique. Dans ce cas, la machine ou le réseau doit apparaître dans la liste « Poste d'administration autorisé ». Par défaut, seuls les réseaux internes et représentés par l'objet « Network_internals » sont autorisés à y accéder.
- Un avertissement pour l'accès à l'interface d'administration peut être affiché. Le fichier d'avertissement peut contenir du texte, ou être au format HTML (mais ne doit pas comporter de Javascript).
- Il est possible d'activer l'accès par SSH (connexion sécurisée) et de modifier le port d'écoute du service qui est par défaut SSH (22/TCP). L'activation du mot de passe est nécessaire pour un accès simplifié. Dans ce cas, l'utilisateur est invité à saisir un login et un mot de passe lors de la connexion. Dans le cas contraire, vous êtes obligés de gérer les accès par une paire de clés de chiffrement (non détaillé ici).
- Sur un boîtier physique, vous pouvez activer l'accès SSH : cochez **Activer l'accès par SSH** et **Autoriser l'utilisation de mot de passe**, puis choisir **ssh** dans Port d'écoute.



NB : l'activation de l'accès SSH n'est pas recommandé par Stormshield.

- Cliquez le bouton **Appliquer** pour sauvegarder la configuration et **Sauvegarder**.
- Dans le volet **Système / Configuration**, ouvrez l'onglet **Paramètres réseaux** pour visualiser les options de configuration réseau du pare-feu.

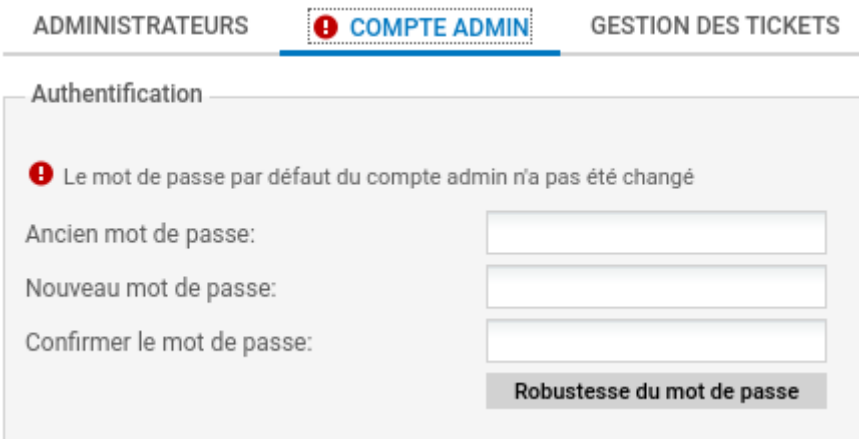


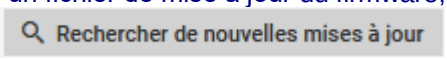
Les firewalls Stormshield Network supportent le protocole IPv6 et plusieurs fonctionnalités (interface, routage, filtrage, VPN et administration) sont compatibles IPv6. Cependant, ce support est optionnel et son activation s'effectue via le bouton **Activer le support du protocole IPv6 sur ce Firewall**.
NOTE : Cette action étant irréversible, la sauvegarde de la configuration du firewall vous sera proposée automatiquement lorsque vous cliquerez sur ce bouton. Le retour à un support IPv4 exclusif (sans IPv6) n'est possible qu'après une remise à la configuration usine (reset) du firewall.
Dans le cas où le firewall transite par un proxy pour accéder à Internet, les paramètres se renseignent depuis ce menu.
Un ou plusieurs serveurs DNS peuvent être ajoutés. Le firewall contacte ces serveurs pour toute résolution qu'il émet ou doit relayer. Ces résolutions de noms sont nécessaires pour des fonctionnalités telles que Active Update qui interroge les serveurs de mise à jour pour télécharger les bases de données (signatures contextuelles, antivirus, Vulnerability Manager, …). Ces serveurs DNS sont également utilisés dans la cas où le service cache DNS est activé en mode transparent (voir 2.3 configuration du Proxy cache DNS).

- *Au besoin,* ajoutez le DNS de votre domaine Active Directory et cliquez le bouton **Appliquer** pour sauvegarder la configuration et **Sauvegarder**.
- Cliquez l'icône  apparue dans l'entête vous invitant à redémarrer le firewall, cliquez l'icône et sélectionnez **Redémarrer maintenant**.
- Après le redémarrage (au bout d'environ 3 minutes), revenez au menu **Configuration / Système** puis **Configuration** et dans la zone **Paramètres de date et d'heure** cliquez **Synchroniser avec votre machine** ou **Maintenir le firewall à l'heure (NTP)** pour que les mises à jour d'heure d'été/heure d'hiver soient également effectives.

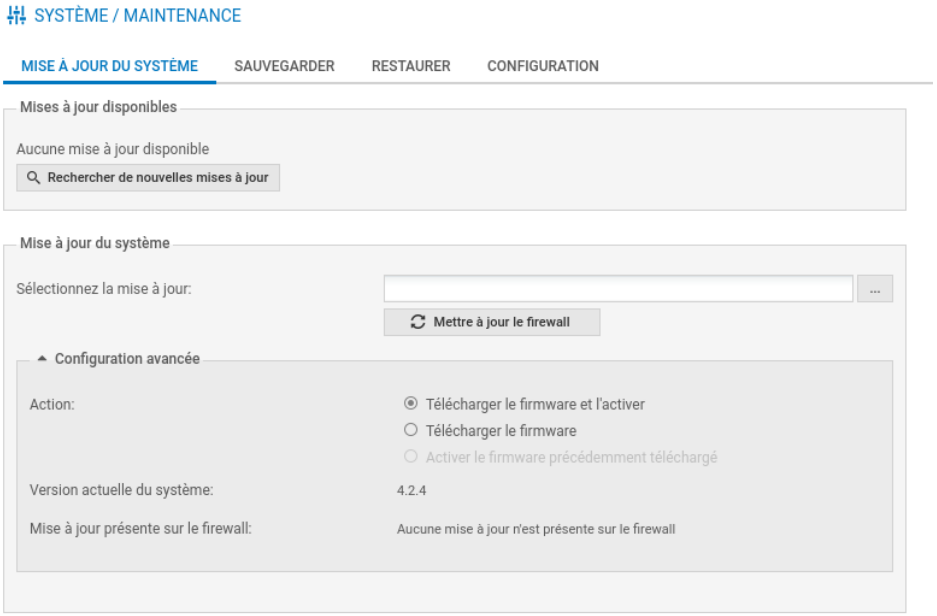
Voici quelques commandes rapides pour réaliser le paramétrage initial du pare-feu SNS.

- La **modification du mot de passe admin** (recommandée) se fait dans le menu **Configuration / Système / Administrateurs /** onglet **Compte ADMIN.** Le mot de passe doit par défaut, comporter au moins **8 caractères** et doit respecter la politique de mot de passe définie dans le menu **Configuration**. La robustesse du mot de passe choisit s'affiche alors. Elle indique son niveau de sécurité : Très faible, faible, moyen, bon, excellent. Il est fortement conseillé d'utiliser les majuscules et les caractères spéciaux pour augmenter le niveau de sécurité.
  Pour simplifier les activités, nous garderons par défaut le compte **admin/admin**.



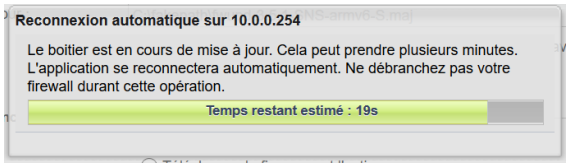
- Le menu **`Configuration / Système / Maintenance /`** onglet **`Mise à jour du système`** permet de mettre à jour le système le cas échéant. Afin d'appliquer un fichier de mise à jour du firmware, vous devrez le télécharger sur le firewall (soit directement via le lien 

une fois que la configuration du réseau et de la passerelle par défaut est réalisée et que le firewall a accès à Internet, soit en allant le télécharger sur le site https://mystormshield.eu). Nous allons décrire la mise à jour vers la dernière version disponible que vous aurez au préalable téléchargée et copiée sur une clé USB ou sur votre machine cliente. Il est recommandé d'installer au minimum la version 4.2.8 du firmware.
- Cliquez **`Configuration / Système / Maintenance`** / onglet **Mise à jour du système**.



- Cliquez le bouton **…** et sélectionnez le fichier de mise à jour présent sur le poste client ou une clé USB.
- Dépliez la zone **`Configuration avancée.`**
- Dans la « configuration avancée », vous pouvez choisir de **Télécharger le firmware et l'activer** ce qui appliquera la mise à jour ou bien de la télécharger uniquement, son activation pourra se faire ultérieurement avec l'option **Activer le firmware précédemment téléchargé**.
- Dans la zone **`Configuration avancée`** choisir **Télécharger le firmware et l'activer.**
- Cliquez le bouton 

L'opération prendra plusieurs minutes surtout ne débranchez pas le pare-feu pendant la mise à jour. Le pare-feu sera ensuite redémarré.



- Le menu **`Configuration / Système / Maintenance /`** `onglet` **`Configuration`** permet **uniquement sur les boitiers physiques** de déterminer la partition active et ainsi de garder deux versions

du système disponibles avec une partition de sauvegarde qui permet de revenir en arrière sur le boitier (firmware n-1, config n-1).
NB : Pour revenir à une configuration ou version n-2 ou supérieure il faut utiliser USB Recovery accessible seulement sur mystormshield.eu avec un compte client.

- La **sauvegarde de la configuration** se fait dans le menu **`Configuration / Système / Maintenance / onglet Sauvegarder`**. Au besoin modifiez le nom du fichier et cliquez sur le bouton pour le télécharger. La sauvegarde automatique du fichier de configuration peut être mise en place et effectuée sur le Cloud Stormshield.
  NB : le fichier de configuration est un fichier texte chiffré.
- La **restauration d'une configuration** s'effectue dans le menu **`Configuration / Système / Maintenance /`** onglet **`Restaurer`**. Sélectionnez le fichier à restaurer en cliquant sur le bouton **...**

➢ Le menu **`Configuration / Système / Active update`** permet de contrôler la mise à jour automatique des modules de Bases d'URLs embarquées, IPS : Signatures de protection contextuelles, Géolocalisation / Réputation IP publiques, signatures antispam, antivirus et autres listes noires préconfigurées par Stormshield. Il est conseillé d'activer uniquement celles qui vous sont utiles.

- Le menu **`Configuration / Système / Licence`** affiche les détails de la licence et permet le cas échéant de l'installer (à récupérer par l'administrateur sur le site *mystormshield.eu* avec les informations figurant sous le boitier).
  NB : À noter que si vous n'activez pas la licence au bout d'un certain temps les fonctionnalités se réduisent et surtout vous ne pourrez pas stocker les logs sur les boitiers physiques.

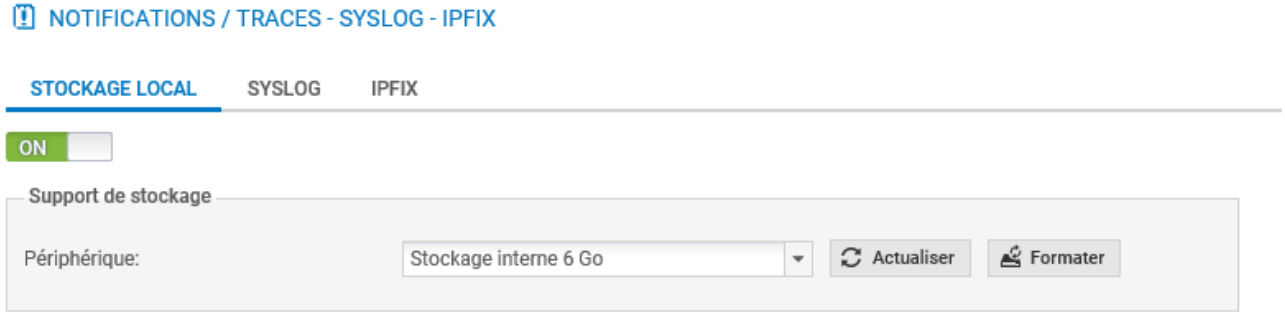
1.4 – Traces, Journaux et supervision

Le stockage des journaux (logs) des pare-feu Stormshield peut être configuré soit en local, soit vers un serveur Syslog, soit avec le protocole IPFIX. Les journaux, rapports d'activités et graphiques d'historiques sont disponibles sur les firewalls ne disposant pas de stockage local des journaux. Cependant, ils sont limités à 5 rapports et graphiques au total avec un historique maximal de 7 jours.

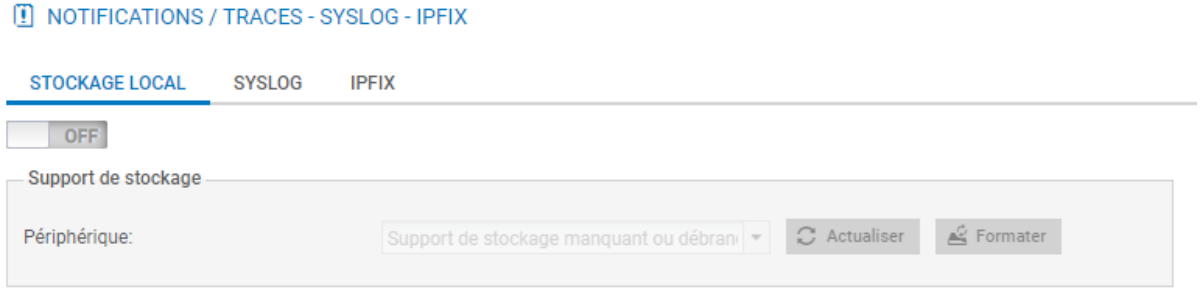
a) Configuration du Stockage des journaux (logs)

Le stockage en local n'est activé par défaut que sur les machines virtuelles, il faut donc le cas échéant le configurer c'est ce stockage local des journaux que nous utiliserons dans ce support.

- Sélectionnez dans le menu à gauche **`Configuration / Notifications / Traces – Syslog - IPFIX`** puis dans l'onglet **`/ Traces – Syslog - IPFIX`** choisir **`Stockage local`**.
  - Sur une machine virtuelle, celui-ci est activé par défaut et occupe un **espace disque de 6Go** :

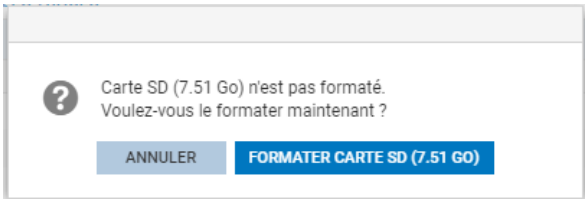


  - **Sur un boitier physique**, le stockage local des logs n'est pas activé par défaut. Vous devez insérer une carte SD dans l'emplacement en façade du pare-feu SNS, lorsque le pare-feu est éteint, elle sera automatiquement détectée lors du démarrage (*sauf si vous n'avez pas installé la licence*) et le système vous proposera de la formater avant utilisation.

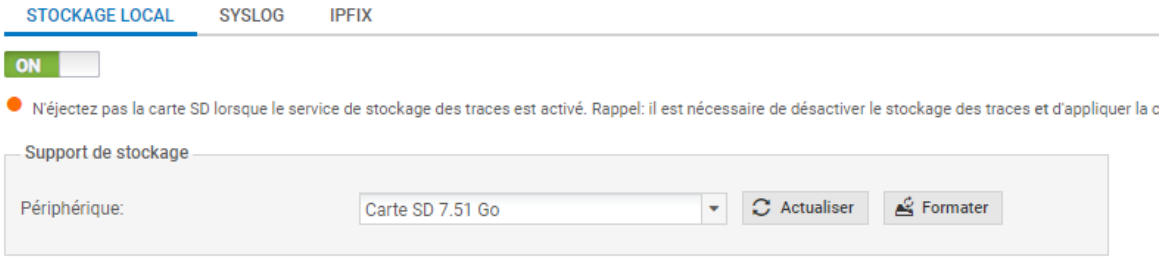


La zone **Support de stockage** permet de sélectionner le support de stockage local :disque dur interne ou carte mémoire SD.

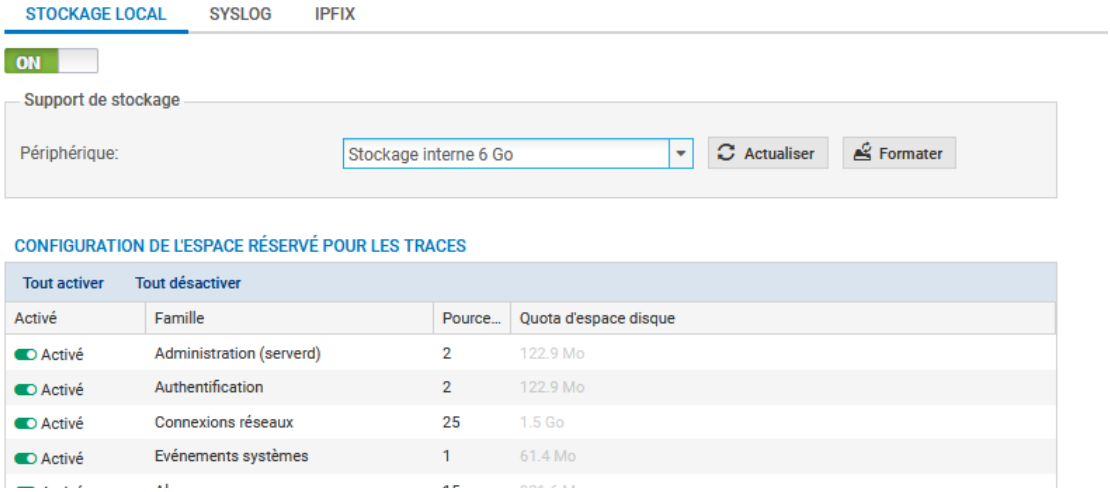
- Au besoin, cochez le bouton **ON** et dans la zone **Support de stockage** sélectionnez dans la liste **`Périphérique`** la carte SD comme support de stockage.



- Le système vous propose de la formater avant utilisation, cliquez **`Formater Carte SD`**. Cette opération prend quelques secondes.
  NB : Afin de stocker les journaux du pare-feu SNS sur un support externe (carte SD) vous devez d'abord enregistrer la licence, le message d'erreur qui apparaît alors n'est pas explicite, le système fait comme s'il ne pouvait détecter la carte SD.



Une fois le support formaté, la liste des journaux préconfigurés est activée avec pour chaque journal un espace dédié. Vous pouvez désactiver certains journaux si vous le souhaitez.



- Le cas échéant, cliquez **Appliquer** puis **Sauvegarder** pour activer le stockage local des journaux.

- Le cas échéant, cliquez **Conserver les rapports d'activité désactivés.**

CONFIGURATION DE L'ESPACE RÉSERVÉ POUR LES TRACES

Tout activer | Tout désactiver

Activé	Famille	Pource...	Quota d'espace disque
Activé	Administration (serverd)	2	–
Activé	Authentification	2	–
Activé	Connexions réseaux	25	–
Activé	Evénements systèmes	1	–
Activé	Alarmes	15	–
Activé	Proxy HTTP	10	–
Activé	Connexions applicatives (plugin)	15	–
Activé	Proxy SMTP	4	–
Activé	Politique de filtrage	8	–

La zone **Configuration de l'espace réservé pour les traces** permet d'activer ou non l'écriture des traces pour une famille donnée en double-cliquant dans la colonne **État** correspondante. Elle permet également de configurer le pourcentage de l'espace disque réservé pour la famille de trace dans la partie **Pourcentage**. Il est important de noter que le total des pourcentages ne doit pas dépasser 100%. La taille réelle de l'espace disque réservé à une famille de traces est indiquée dans la partie **Quota d'espace disque.**

Les entrées de journal anciennes sont écrasées par les nouvelles entrées (rotation) ; il s'agit du comportement par défaut. Pour une journalisation sans rotation, il faut un stockage externe (serveur SYSLOG par exemple).

L'activation des rapports s'effectue depuis le menu **`Configuration / Notifications / Configuration des rapports`**

Cliquez **`Configuration / Notifications / Configuration des rapports`** et activez l'option **Rapports statiques**, ensuite sélectionnez les rapports souhaités dans le panneau **Liste des rapports**.

NOTIFICATIONS / CONFIGURATION DES RAPPORTS

Général

Rapports statiques: ON

Courbes historiques: ON

Avertissement : L'activation de rapports peut impacter les performances de votre Firewall.

LISTE DES RAPPORTS | LISTE DES GRAPHIQUES HISTORIQUES

Rechercher... dans les catégories Toutes | Définir l'état on | Réinitialiser la base de données

Etat	Catégorie	Description	Avertissement	Données person...
Inactif	Sécurité	Taux de détection par moteur d'analyse (Sandboxing, Antivirus, AntiSpam).		
Inactif	Spam	Taux de spam dans les e-mails reçus	L'antispam est désactivé	
Inactif	Réseau	Top des machines par volume échangé		
Actif	Réseau	Top des protocoles par volume échangé		
Inactif	Réseau	Top des utilisateurs par volume échangé	L'authentification est désactivée	
Inactif	Réseau	Top des applications clientes par volume échangé		
Inactif	Réseau	Top des applications serveur par volume échangé		
Inactif	Réseau industriel	Top des serveurs EtherNet/IP par volume échangé		

Rapports actifs : 5 sur 30 — Taille de la base de données : 136 Ko

Par défaut le rapport sur le **Top des protocoles** par volume est activé si vous activez les rapports.

L'onglet **Liste des graphiques historiques** permet de visualiser et modifier les graphiques activés par défaut.

LISTE DES RAPPORTS | LISTE DES GRAPHIQUES HISTORIQUES

Etat	Description
Actif	Historique de l'utilisation de bande passante
Actif	Historique de la consommation CPU
Actif	Stats on packets
Actif	Historique des vulnérabilités

b) Les Journaux

Les fichiers journaux sont organisés en plusieurs catégories dont les plus importantes sont listées ci-dessous.

- **Administration:** Regroupe les évènements liés à l'administration du pare-feu SNS. Ainsi, toutes les modifications de configuration effectuées sur le firewall sont journalisées.
- **Authentification:** Regroupe les évènements liés à l'authentification des utilisateurs sur le pare-feu SNS.
- **Connexions réseaux:** Regroupe les évènements liés aux connexions TCP/UDP traversant ou à destination du pare-feu SNS non traitées par un plugin applicatif.
- **Évènements systèmes:** Regroupe les évènements liés directement au système: arrêt/démarrage du pare-feu SNS, erreurs système, allumage/extinction d'une interface, haute disponibilité, mises à jour Active Update, etc.
- **Alarmes:** Regroupe les évènements liés aux fonctions de prévention d'intrusions (IPS) et les évènements tracés avec le niveau alarme mineure ou majeure de la politique de filtrage.
- **Proxy HTTP:** Regroupe les évènements liés aux connexions traversant le proxy HTTP.
- **Connexions applicatives (plugin)**: regroupe les évènements liés aux connexions traitées par un plugin applicatif (HTTP, FTP, SIP, etc).
- **Politique de filtrage:** regroupe les évènements liés aux règles de filtrages et/ou de NAT, lorsque la journalisation des règles est en mode verbeux.

Dans le contexte **Monitoring**, le menu **LOGS - JOURNAUX D'AUDIT** permet de visualiser les journaux et traces sauvegardés en local sur le pare-feu SNS, regroupés par famille de journaux : trafic réseau, alarmes, web, etc.

Exemple : la famille **Trafic réseau** concatène les journaux Connexions réseaux, filtrage, Proxy FTP, connexions applicatives, Proxy POP3, Proxy SMTP, Proxy SSL, Proxy HTTP, VPN SSL.

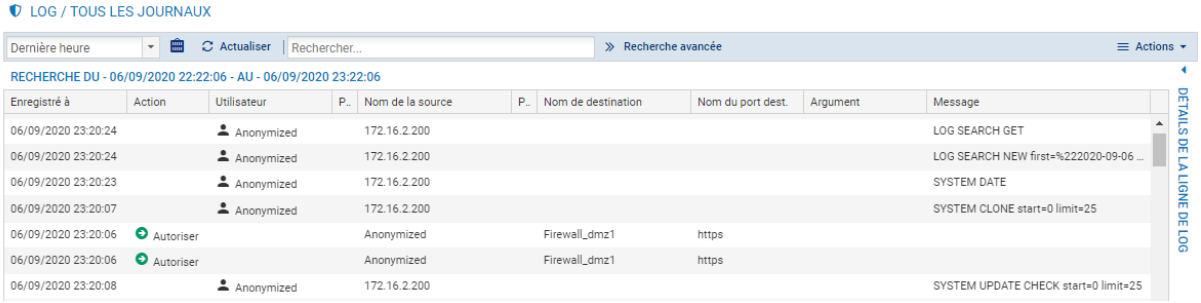
Les traces sont affichées par ordre antichronologique (la trace la plus récente est en tête de liste).

Pour appliquer la nouvelle réglementation européenne sur les données personnelles, le RGPD (Règlement Général sur la Protection des Données), l'accès aux logs des firewalls SNS est restreint par défaut pour tous les administrateurs.

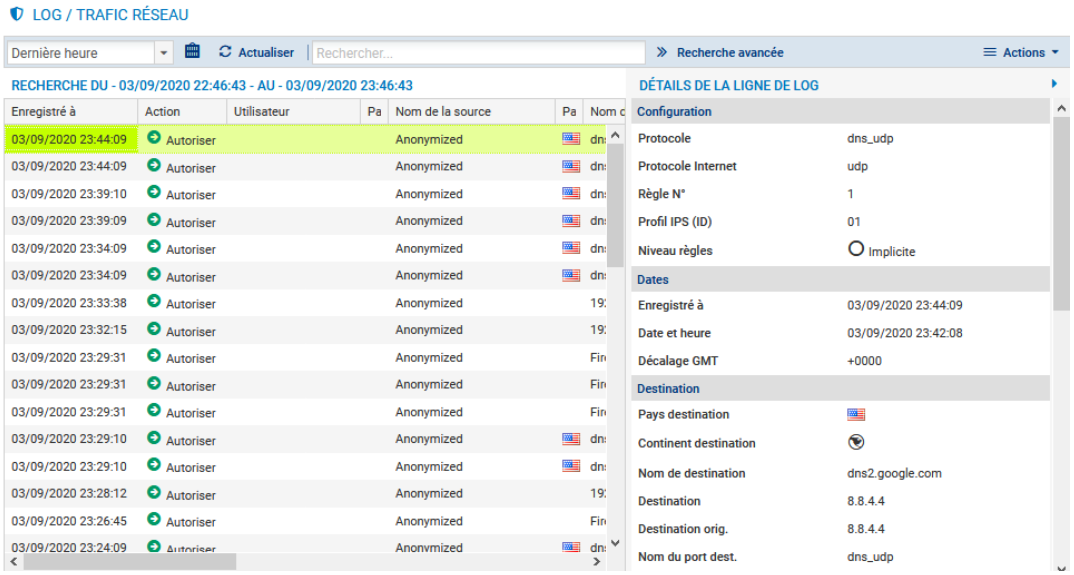
Le super administrateur « admin », ainsi que les administrateurs disposant du droit « Accès aux données personnelles » peuvent accéder aux logs complets en cliquant simplement sur **Obtenir le droit d'accès aux données personnelles (logs)**. Cette manipulation ajoute une entrée dans les journaux qui permet de la tracer.

c) Consultation des Journaux

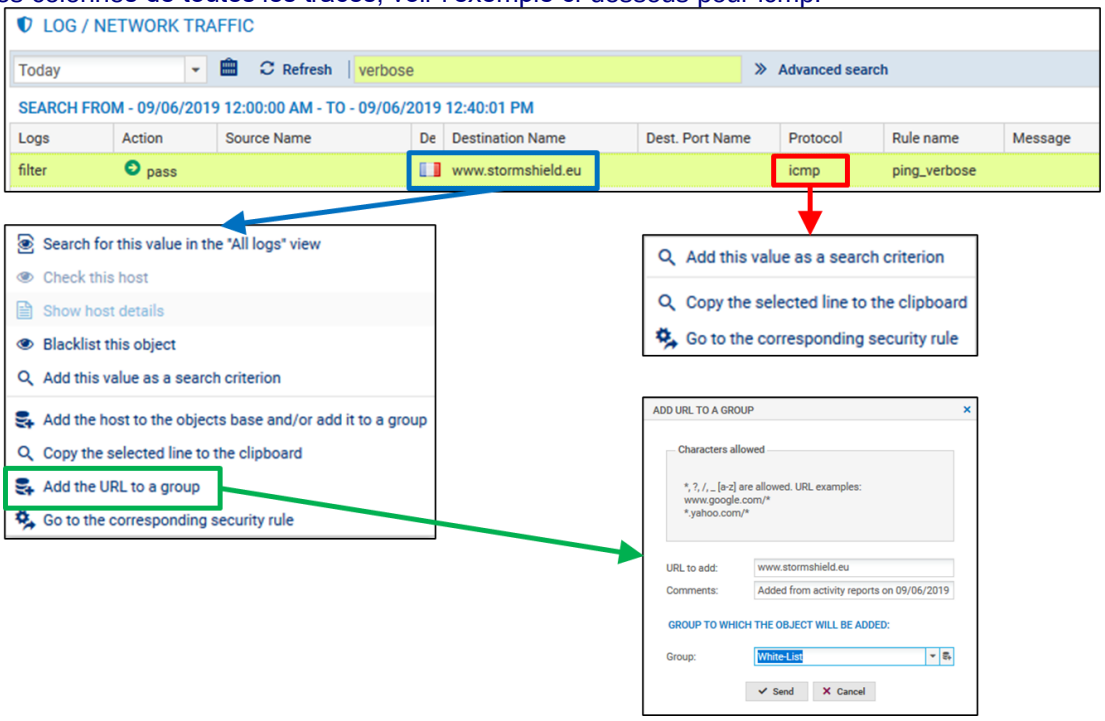
Cliquez **Monitoring** puis **LOGS - JOURNAUX D'AUDIT** puis **Trafic réseau**.



Pour voir l'ensemble des données relatives à une trace, mettez la ligne désirée en surbrillance et cliquez sur la flèche en haut à droite **Détails de la ligne de log**.



L'affichage des journaux peut être restreint à une plage temporelle prédéfinie (dernière heure, aujourd'hui, hier, semaine dernière ou mois dernier) ou personnalisée.
En cliquant sur un type de trace, une fenêtre s'affiche pour offrir des raccourcis vers plusieurs fonctionnalités qui diffèrent suivant le type de trace affichée : afficher de l'aide, ajouter la machine à la base objet, filtrer les traces en se basant sur la valeur, voir la ligne complète de la trace, etc.
Pour **filtrer les traces**, une barre de recherche simple permet de rechercher une chaine de caractères dans toutes les colonnes de toutes les traces, voir l'exemple ci-dessous pour icmp.



Phase 2 Mise en place du plan d'adressage réseau

2.1 - Configuration des interfaces réseau

Dans une configuration usine, la **première interface** du pare-feu SNS est nommée « OUT » (qui correspond à l'interface WAN sur un boitier physique), la **seconde** « IN » et le reste des interfaces « **DMZx** ». L'interface « OUT » est une **interface externe**, utilisée pour connecter le pare-feu SNS à internet (WAN) et le reste des interfaces sont internes et servent principalement à connecter le pare-feu SNS à des réseaux locaux. La distinction interface interne/externe permet de se protéger contre les attaques d'usurpation d'adresse IP.
Pour accéder à l'interface d'administration du pare-feu SNS, il faut connecter votre machine sur une interface interne sous peine d'être détecté comme tentative d'intrusion qui nécessite le redémarrage du firewall.

NB : Dans ce cas, on aura un message « forbidden » sur le navigateur, on peut déconnecter le câble (faisable aussi en virtuel en désactivant la carte), changer son IP et se reconnecter à une autre interface interne sans redémarrage.

Nous allons configurer votre pare-feu SNS selon les paramètres de l'architecture globale présentée dans la phase 1 (interfaces IN, OUT et DMZ1) en utilisant le pare-feu SNS en mode « routeur ».

@Interface **OUT** 192.36.253.x0 /24 qui correspond au premier port (WAN)
@Interface **IN** 192.168.x.254 /24 qui correspond au deuxième port (port LAN N°1)
@Interface **DMZ1** 172.16.x.254 /24 qui correspond au port DMZ
@Interface **DMZ2** DHCP qui correspond au port DMZ2 relié à votre LAN interne (BTSSIO).

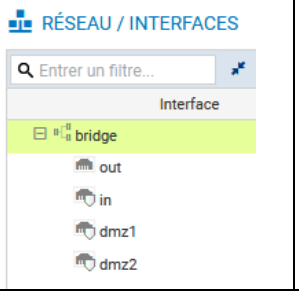
La **passerelle par défaut** de votre pare-feu SNS sera le pare-feu SNS **Siège** (ou enseignant) @ **192.36.253.1**.

Pour faciliter la configuration, nous proposons d'effectuer la configuration depuis un poste client connecté à l'interface DMZ2 ou DMZ1 suivant votre pare-feu SNS, que l'on conservera en DHCP sur le réseau interne BTSSIO.

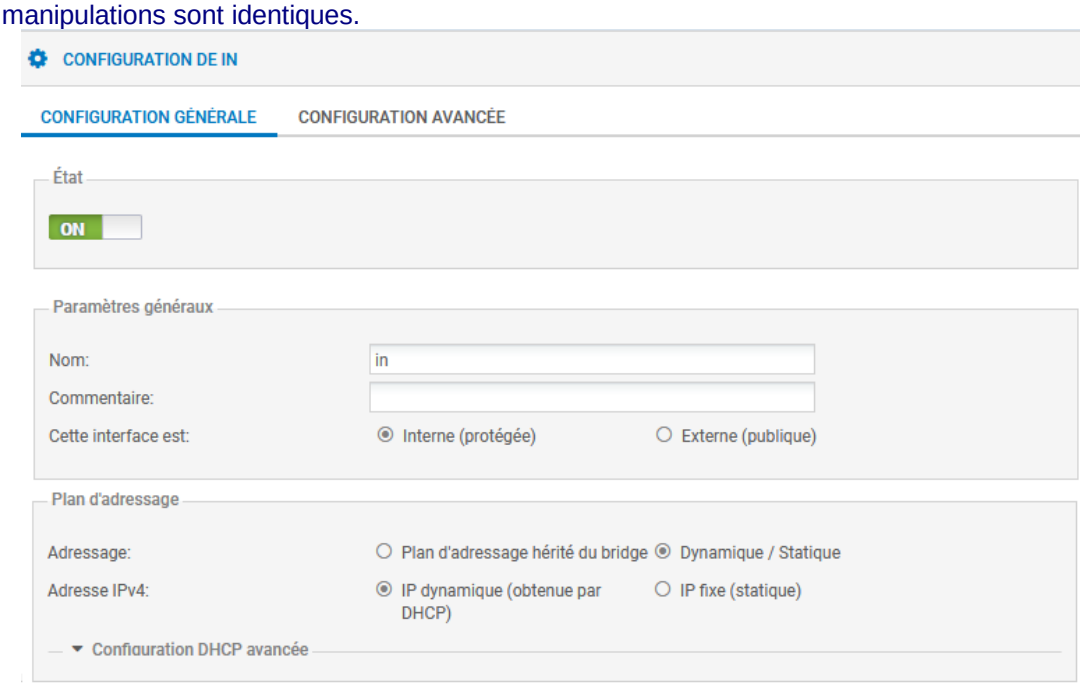
La **configuration des interfaces** s'effectue dans le menu **`Configuration / Réseau / Interfaces`**, en faisant « sortir » les interfaces Ethernet de l'interface bridge créée par défaut.

NB : Si vous avez effectué la réinitialisation de la VM, alors vous avez déjà configuré des adresses pour vos interfaces réseau.

- Sélectionner **`Configuration / Réseau / Interfaces`**.

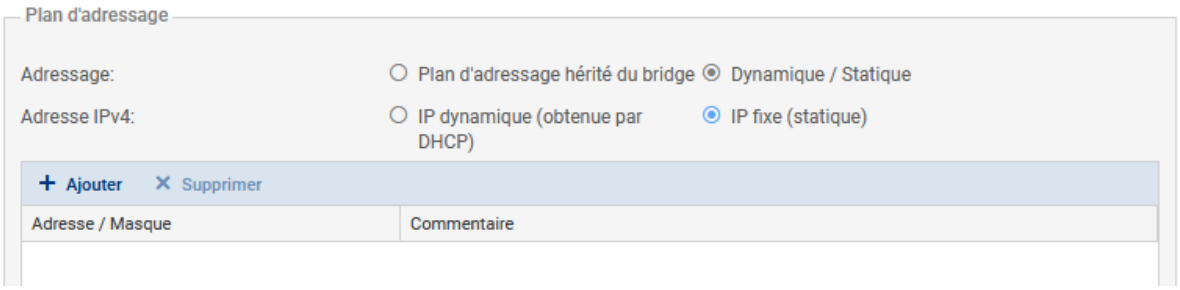
Configuration par défaut avec bridge	Configuration en mode routeur
	

- Choisir une première interface (par exemple **IN**), pour la sortir du bridge ou la configurer avec une IP fixe, les manipulations sont identiques.

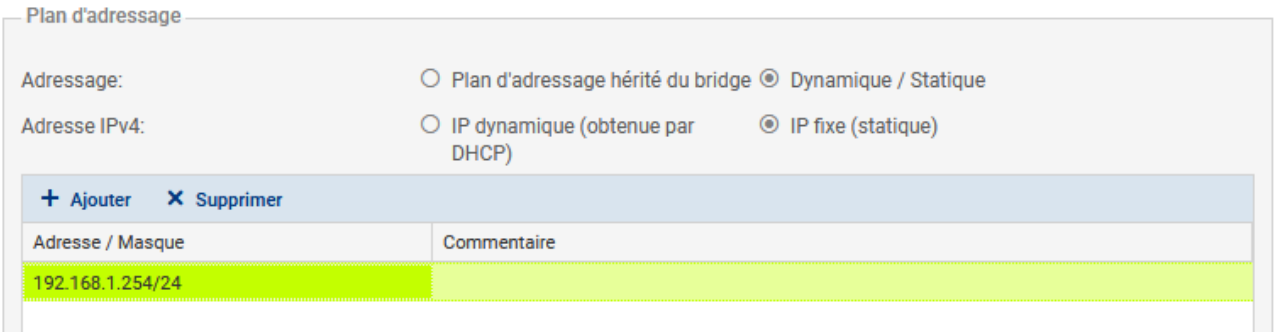


Si l'interface était membre d'un bridge, la configuration est légèrement différente pour la zone **Plan d'adressage** :

- Le cas échéant, cliquez dans la zone **Plan d'adressage** sur **`Dynamique/Statique`**.
- Cliquez **`Ip fixe (statique)`**, un tableau apparaît :



- Cliquez **`+Ajouter`** et dans la zone **`Adresse / Masque`** saisissez **l'adresse IP de l'interface IN** 192.168.x.254 puis le masque en CIDR, ***/24*** ou en notation décimale pointée : 255.255.255.0.

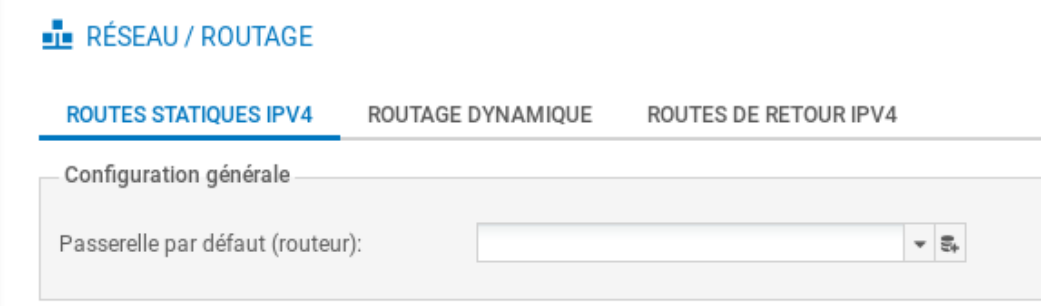


- Cliquez le bouton **`Appliquer`** puis **`Sauvegarder`** et à nouveau **`Sauvegarder`**.
  Un message de reconnexion peut s'afficher, le cas échéant reconnectez-vous.
- Procédez de manière identique pour les autres interfaces (**DMZ1, DMZ2** et **OUT**) à configurer.

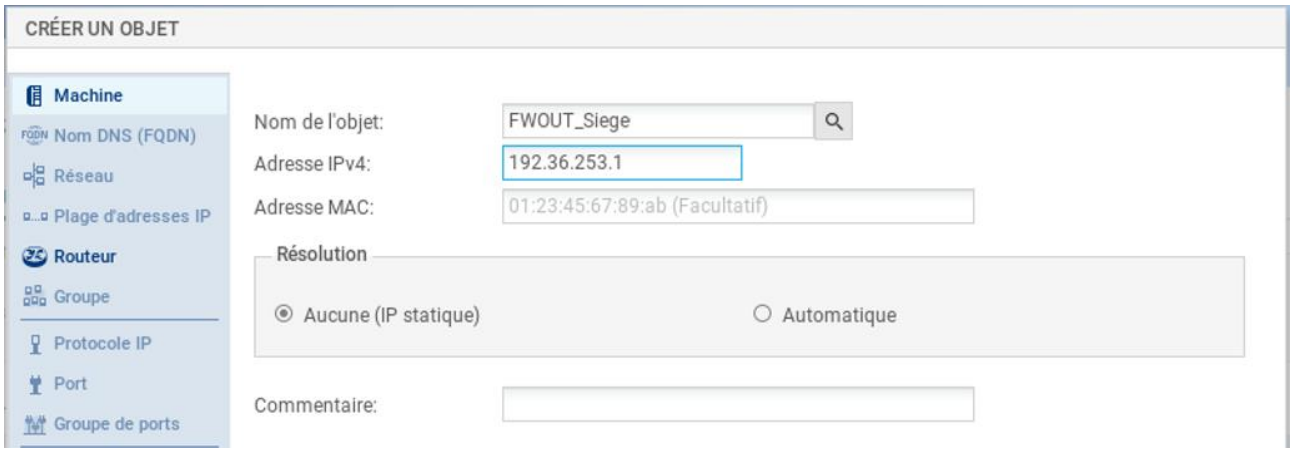
2.2 - Route par défaut

La configuration de la passerelle par défaut de votre pare-feu SNS doit pointer sur l'adresse IP du pare-feu SNS **Siège** (ou enseignant) : **192.36.253.1** qui devra permettre la sortie vers Internet de vos réseaux.

- Cliquez **`Configuration / Réseau / Routage /`** onglet **`Routes statiques IPv4`**.



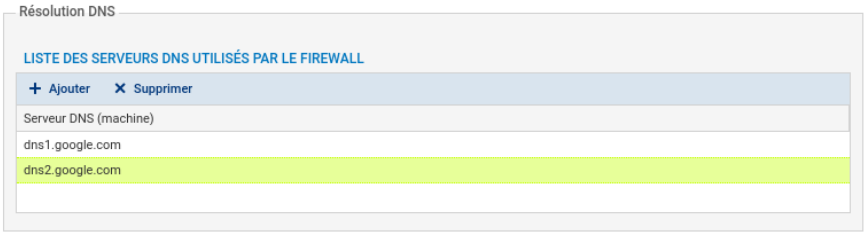
- Cliquez sur l'icône pour **ajouter un objet réseau,** choisissez **`Machine`** et renseignez les champs **`Nom`** (Ex : **FWOUT_Siege**) et **`Adresse IPv4`** du pare-feu SNS **Siège** : *192.36.253.1* puis cliquez le bouton **`Créer`**.



2.3 - Configuration du proxy cache DNS

Le proxy cache DNS doit être activé pour permettre la résolution de noms DNS de façon correcte pour la mise en œuvre des activités (labs).

- Dans le volet **`Système / Configuration`**, ouvrez l'onglet **`Paramètres réseaux`** pour visualiser les options de configuration réseau du pare-feu.



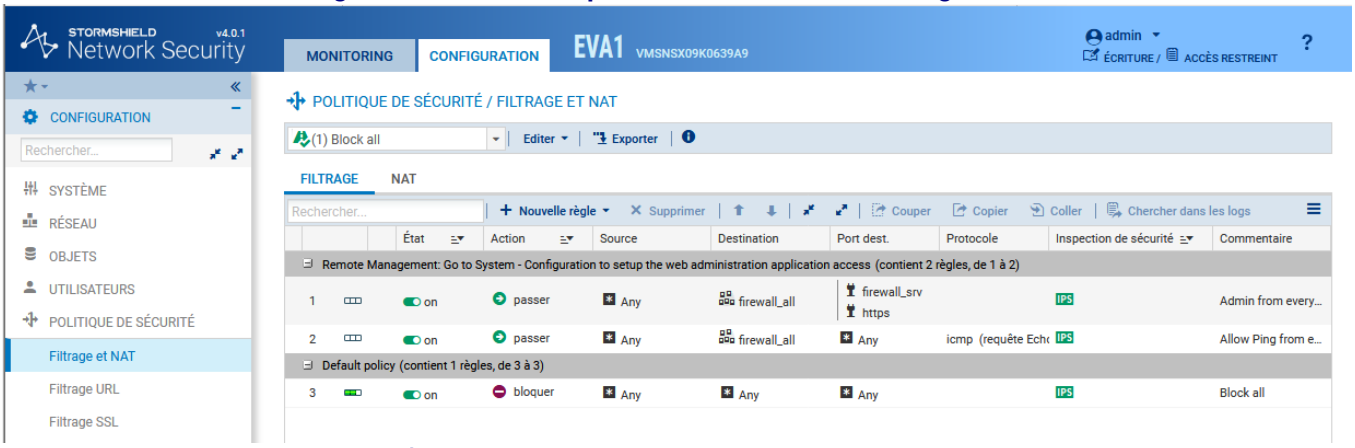
La liste des serveurs DNS utilisés par le firewall doit permettre la résolution DNS vers des serveurs de l'Internet, vous pouvez conserver les serveurs de google (par défaut) ou les remplacer par d'autres.
Le firewall intercepte les requêtes DNS à destination d'Internet, et effectue lui-même la requête vers le serveur DNS configuré.
Si le nom demandé est dans son cache, le firewall répond directement à la demande selon les informations qu'il possède. Nous allons configurer le proxy cache afin que le serveur DNS présent sur la DMZ puisse l'interroger.

- Dans le volet **`Configuration / Réseau,`** ouvrez **`Proxy cache DNS`**.
- Cliquez sur **OFF** pour activer le cache DNS, il passe à **ON**.
- Dans la « liste des clients autorisés à utiliser le cache DNS », cliquez **+ Ajouter** puis cliquez sur l'icône  pour ajouter un objet **Machine**, dans **Nom de l'objet**, tapez **srv_dns_priv**, dans **Adresse IPv4** saisir l'adresse 172.16.x.10 puis **Créer** pour l'ajouter puis **Appliquer**.

2.4 - Mise en œuvre de la traduction d'adresses pour l'accès à Internet (NAT/PAT)

Pour cette activité, nous considérons le réseau externe inter-entreprises comme un réseau public dans lequel aucune adresse IP privée n'est tolérée. De plus, le pare-feu SNS du **Siège** (ou enseignant) est connecté à internet via un réseau autre que ceux utilisés dans l'architecture du LAB.

- Ouvrez le menu **`Configuration`** / **`Politique de sécurité`** / **`Filtrage et NAT.`**

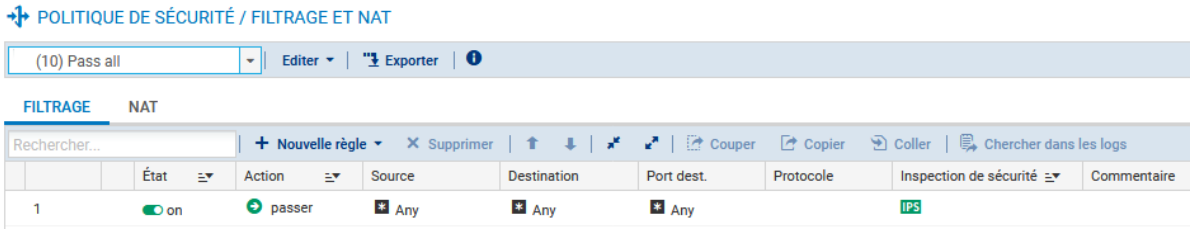


Dans les pare-feu SNS, les règles de filtrage et NAT (traduction d'adresses) sont regroupées sous une même politique. Il est possible de définir 10 politiques différentes mais une seule politique est active à la fois, identifiée par l'icône : 

La politique de sécurité active en configuration usine est **(1) `Block all`**, elle n'autorise que le ping des interfaces du firewall et l'accès en https à l'administration du boitier.
Une politique implicite **`Block all`** est également configurée sur le pare-feu SNS.
Pour réaliser les activités, nous allons choisir une politique plus permissive que nous durcirons progressivement.

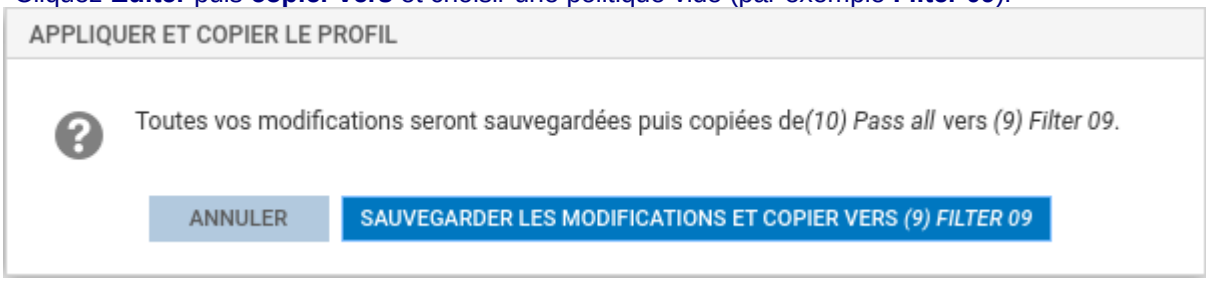
Étape 1 : Copiez la politique de filtrage/NAT (10) **`Pass all`** vers une la politique vide numéro 9, que vous renommerez « **`NAT Internet_Pass all`** ». Ensuite, **activez cette politique**.

- Dans la liste déroulante des politiques de sécurité, choisissez **(10) Pass all.**

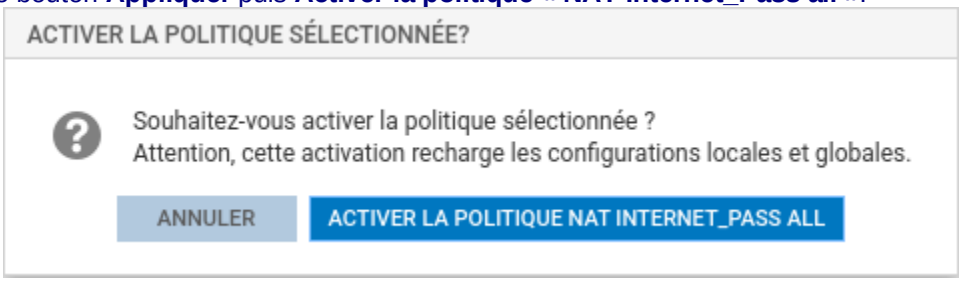


Cette politique laisse explicitement passer tous les flux.

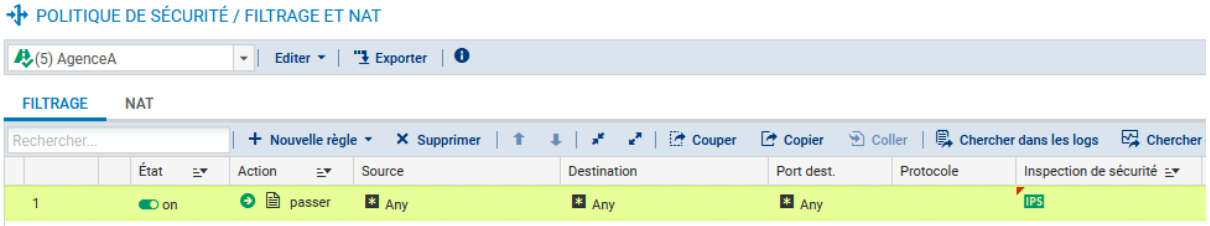
- Cliquez **Éditer** puis **copier vers** et choisir une politique vide (par exemple **Filter 09**).



- Cliquez **Sauvegarder les modifications…**
- Dans la liste déroulante des politiques de sécurité, choisissez la politique copiée **(09) Pass all.**
- Cliquez **Éditer** puis **Renommer** et renommez-la en « **NAT Internet_Pass all** », puis **Mettre à jour**.
- Cliquez le bouton **Appliquer** puis **Activer la politique** « **NAT Internet_Pass all** ».



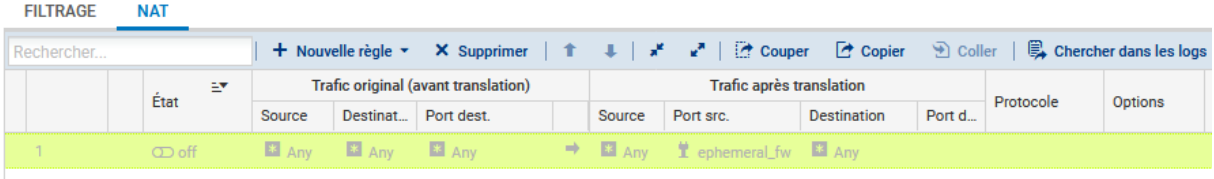
La politique « **NAT Internet_Pass all** » est activée :



Étape 2 : Ajoutez une règle de NAT dynamique NAPT afin que les machines de votre réseau interne (**Network_internals**) puissent accéder au réseau externe (**Network_Out**) et à Internet. Testez l'accès au réseau externe et l'accès à Internet depuis le client sur le réseau interne **IN** de votre agence.

La règle de **NAT dynamique** est créée avec le bouton **Nouvelle règle / règle de partage d'adresse source (masquerading)** qui ajoute automatiquement la plage de ports prédéfinie **ephemeral_fw** [20000-59999] au niveau du port source dans le trafic après traduction. Par défaut, les ports sont choisis séquentiellement dans cette plage, cependant une option est disponible pour permettre un choix aléatoire du numéro de port pour chaque nouvelle connexion et le rendre ainsi moins prédictible.

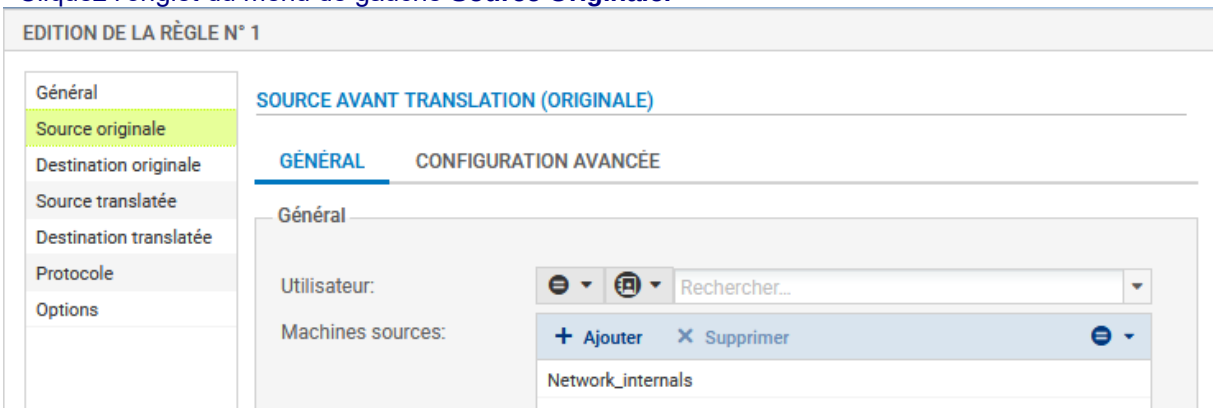
- Dans votre politique **(9)**, sélectionnez l'onglet NAT puis **Nouvelle règle / règle de partage d'adresse source (masquerading)**



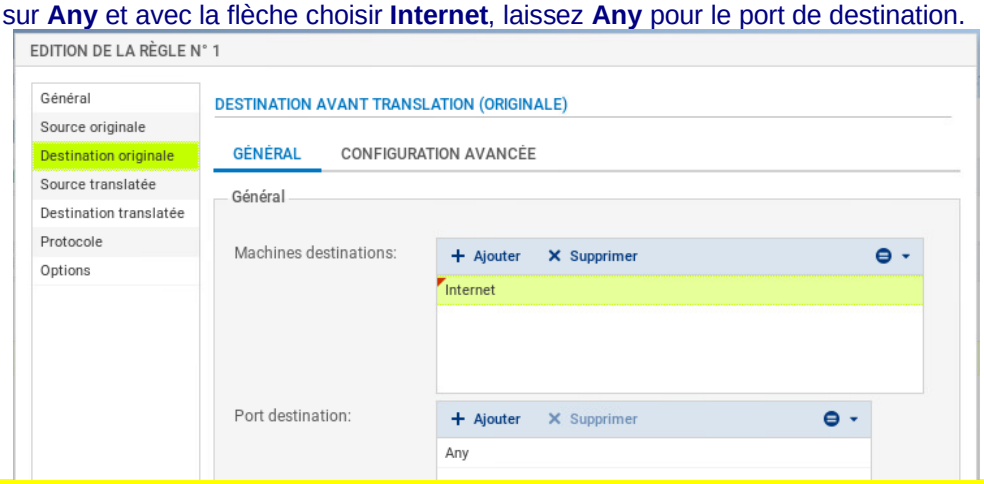
Une nouvelle règle non activée apparaît avec des valeurs par défaut any, any. Dans la section **Trafic après translation**, le port source sera traduit par un numéro de port choisi dans la plage **ephemeral_fw**.
La configuration du **Trafic original (avant translation)** permet de renseigner les valeurs des paramètres avant traduction (par défaut any, any). **Source Originale** permet de définir l'adresse IP d'un hôte ou du réseau source. **Destination Originale** permet de définir l'adresse IP d'un hôte ou du réseau le réseau destination. La configuration du **Trafic après translation** permet de renseigner les nouvelles valeurs des paramètres après

traduction (par défaut any, any). **Source** translatée définit l'adresse IP ou le réseau source et le **port** source vus de l'extérieur. **Destination** translatée définit l'adresse IP ou le réseau destination et **Port destination** translatée le port de destination.
Nous allons détailler chaque élément de la configuration de la règle.

- Double-cliquez sur une zone vide de la règle pour ouvrir la fenêtre de configuration détaillée« **Edition de la règle N°1** ».
- Cliquez l'onglet du menu de gauche **Général**, dans la zone **Commentaire,** saisir « Configuration de la règle de NAT/PAT de base pour la sortie internet ».
- Cliquez l'onglet du menu de gauche **Source Originale.**

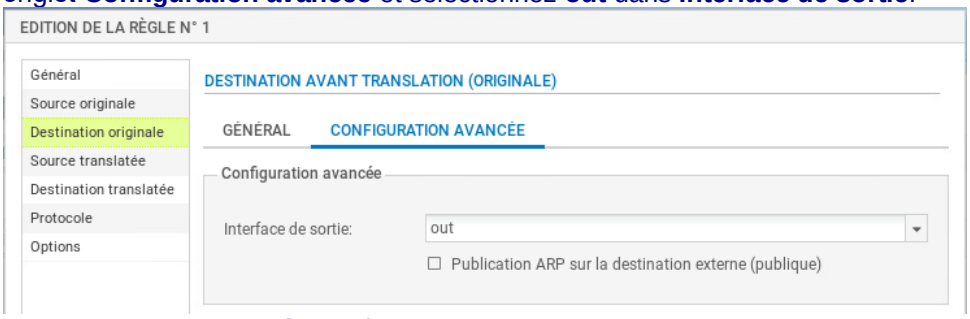


- Cliquez sur **Any** et avec la flèche choisir **Network_internals**, dans l'onglet **Configuration avancée**, laissez **Any** pour le port de destination.
- Cliquez l'onglet du menu de gauche **Destination Originale.**
- Cliquez sur **Any** et avec la flèche choisir **Internet**, laissez **Any** pour le port de destination.

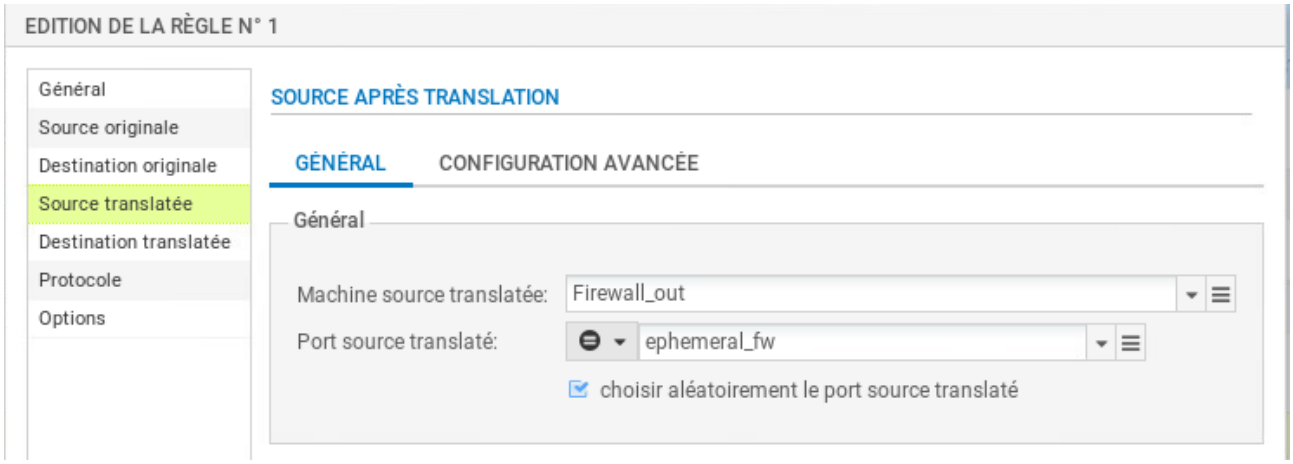


Attention : si dans la zone **destination originale**, vous laissez **Any**, plutôt qu'**Internet** qui désigne tous les réseaux sauf ceux internes au pare-feu SNS, le pare-feu SNS bloquera les flux d'administration (en ssh et en https). En effet, les flux d'administration subiront également une traduction NAT vers l'interface **OUT** qui l'interprétera comme une tentative d'intrusion et les bloquera.
Vous pouvez rendre cette règle plus restrictive en choisissant explicitement l'interface de sortie.

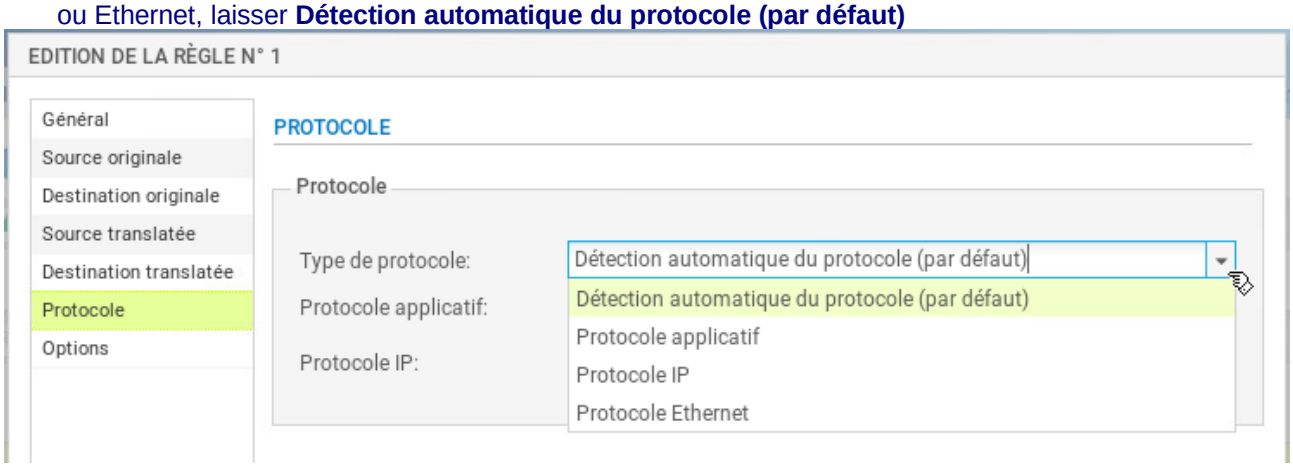
- Cliquez l'onglet **Configuration avancée** et sélectionnez **out** dans **Interface de sortie**.



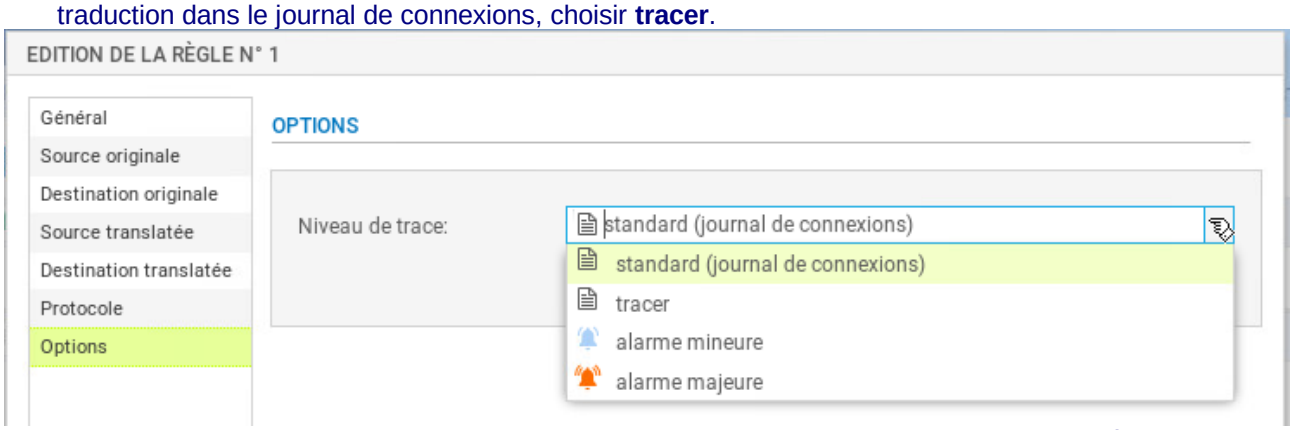
- Cliquez l'onglet **Source translatée** et sélectionnez **Firewall_Out** dans **Machine source translatée**.
- Dans **Port source translaté**, laisser **ephemeral_fw** et cochez **choisir aléatoirement le port source translaté**.
  Cette option **choisir aléatoirement le port source translaté**, permet d'éviter les attaques utilisant la prédictibilité des ports utilisés. Ainsi si le premier port est 10000, le suivant ne sera pas 10001. Cette précaution n'empêche pas les attaques, elle permet de les rendre plus complexes.



- Cliquez l'onglet du menu de gauche **Protocole**, cela permet de définir le type de protocole : applicatif, IP ou Ethernet, laisser **Détection automatique du protocole (par défaut)**



- Cliquez l'onglet du menu de gauche **Options**, cela permet de tracer le trafic qui correspond à la règle de traduction dans le journal de connexions, choisir **tracer**.



NB : La NAT ne laisse jamais de traces dans le journal de connexions, pour tracer une règle de NAT, il faut choisir l'option « tracer », sinon, aucune journalisation de NAT ne sera effectuée.

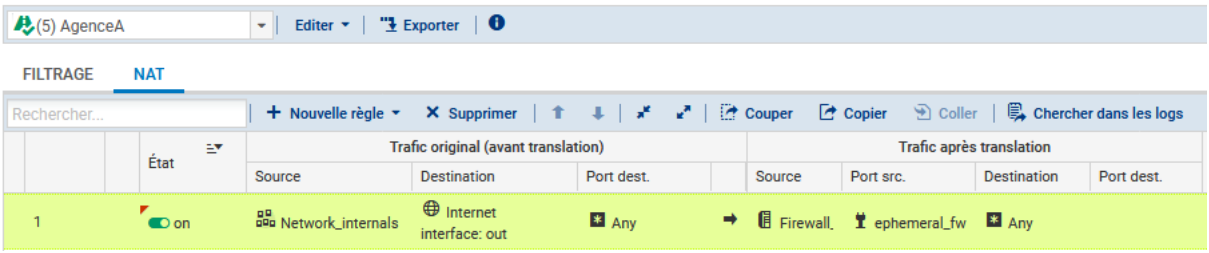
L'onglet **Options** permet également d'activer le NAT dans le tunnel IPSec (voir VPN IPSec).

- Cliquez **OK** pour sauvegarder les modifications de la règle de NAT dynamique que vous venez de créer.
- Dans la colonne **État**, sélectionner avec la flèche 

Définir l'état on

  La règle passe à 

- Cliquez **Appliquer** puis **Oui, Activer la politique** puis confirmer.



NB : L'accès à Internet est normalement possible via la passerelle NAT si la traduction NAPT (Network Address and Port Translation) est configurée comme ci-dessus. Les adresses IP internes ne seront pas visibles (SNAT) dans les flux sortants.

Pour tester, configurez une machine virtuelle cliente dans le réseau interne de votre agence côté interface IN (LAN_IN_*X*) comme suit :

- Adresse IP : 192.168.x.100/24
- Passerelle par défaut : 192.168.x.254
- Serveurs DNS : 172.16.x.10
  et en second le serveur DNS du réseau du BTSSIO ou 9.9.9.9

- Effectuez des tests de connectivité vers un serveur extérieur à votre plateforme, par exemple la passerelle par défaut : **ping 192.36.253.1** puis un serveur externe par exemple le DNS 9.9.9.9. **ping 9.9.9.9** doit renvoyer une réponse.
- Testez l'accès à un site web, par exemple https://www.debian.org/ ou https://allocine.fr doivent renvoyer une réponse.

NB : Le serveur DNS fourni avec le serveur debian effectue la résolution DNS pour vos adresses locales, la résolution vers Internet est également mise en place via la configuration DNS du pare-feu.

NB : À ce stade, nous vous conseillons d'effectuer à nouveau une sauvegarde de votre configuration.

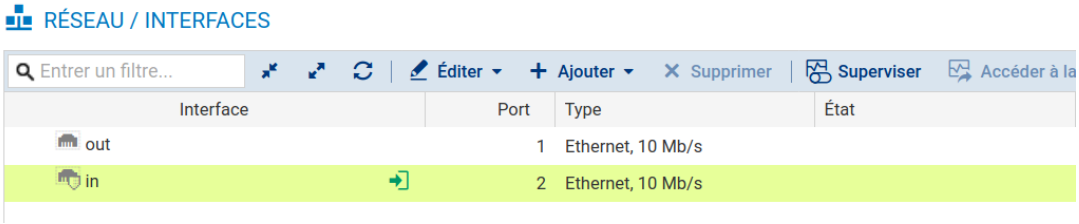
2.5 - Création de sous-interfaces pour la gestion des trames étiquetées (802.1q) et des VLAN

Lorsque le pare-feu doit également gérer le routage inter-vlan, il est nécessaire de créer à partir d'une interface physique des sous-interfaces à même d'interpréter des trames Ethernet étiquetées **802.1q** en fonction des VLAN créés.

Attention ! Les manipulations décrites ci-après ne sont pas nécessaires pour réaliser les activités, elles sont données à titre d'exemple, nous vous conseillons de les réaliser dans un second temps.

Attention ! Si l'interface **IN** est celle utilisée pour se connecter à la page web d'administration du pare-feu mais également pour la création de sous-interfaces, il est **indispensable** d'avoir un accès à cette même application par une autre interface telle que DMZ. Sans cela, il ne sera plus possible de se connecter au firewall pour l'administrer.

- Pour créer une sous-interface, il est nécessaire de se rendre dans le menu **Configuration / Réseau / Interfaces**.

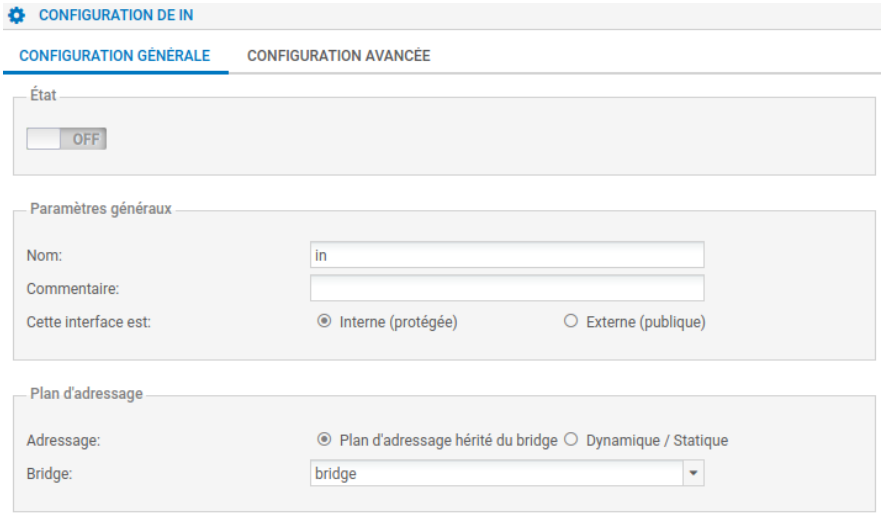


Contrairement à la création de sous-interfaces sur des routeurs Cisco qui consiste à activer l'interface réseau physique sans lui attribuer de configuration IP, Stormshield recommande de désactiver 

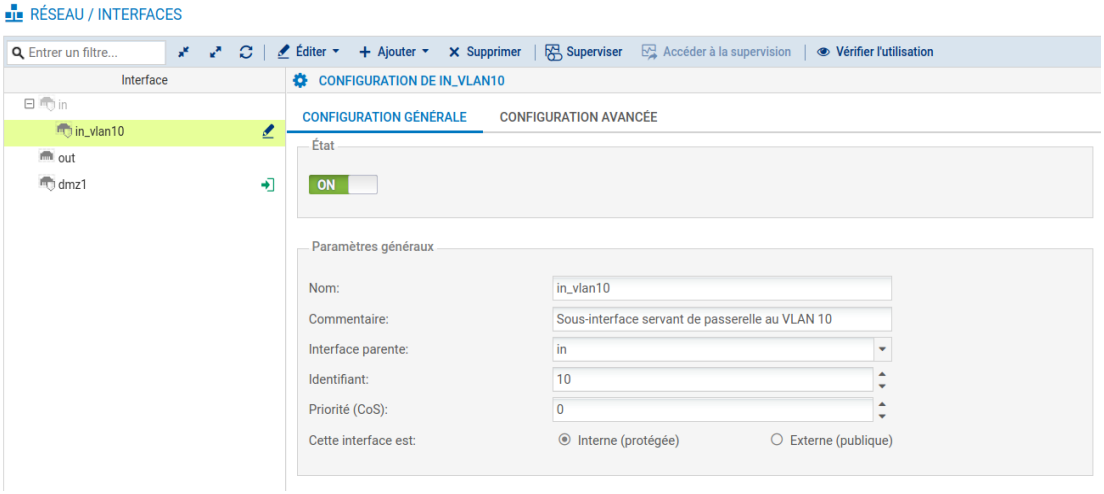
l'interface parente qui servira à la création des sous-interfaces associées à chaque VLAN.

Voir la section **Interface virtuelle : VLAN par port (802.1q)** du support CSNA (p162).

- Double-cliquer sur l'interface physique concernée par le routage inter-vlan (**in** la plupart du temps) puis dans l'onglet **Configuration Générale** pour la désactiver, passer l'**Etat** à **Off**.



- Sélectionner ensuite l'interface physique que vous venez de désactiver puis cliquer sur **Ajouter / VLAN / Pour in** (ou toute autre interface concernée).



- Définir un nom pour la sous-interface en respectant une convention de nommage cohérente puis un commentaire permettant d'expliciter l'utilité de celle-ci.
- Le cas échéant, choisir l'interface parente correspondante et définir un identifiant correspondant au VID du VLAN concerné (10, 100, 200…).
- Cette sous-interface est interne puisque les VLAN sont très souvent implémentés sur le réseau local de l'entreprise.
- En tant que passerelle, l'utilisation d'une adresse IP fixe est fortement conseillée.

Remarque : La norme 802.1q prévoit un VLAN administratif (VLAN 1 sur Cisco), seul VLAN non étiqueté 802.1q entre deux éléments actifs. Pour des raisons de sécurité, ce comportement est désactivé sur les pare-feu Stormshield qui ajoutent un en-tête 802.1q à chaque trame sur un port étiqueté.

Fiche pratique n°2 : Configuration des Objets Réseau

Dans cette partie, vous allez configurer les objets réseau nécessaires à la mise en place de règles de filtrage et de NAT permettant d'accéder à vos services serveurs en DMZ et à ceux de vos voisins.

Phase 3 Configuration des Objets Réseau

3.1 - Présentation des Objets

Les menus de configuration des pare-feu Stormshield Network utilisent des objets qui représentent des valeurs (adresse IP, adresse réseau, URL, événement temporel, etc.). L'utilisation d'objets au lieu de valeurs présente deux avantages majeurs :
1. Cela permet à l'administrateur de manipuler des noms, plus parlants que des valeurs.
2. Dans le cas où une valeur change, il suffira de modifier la valeur au niveau de l'objet et non dans tous les menus où l'objet est utilisé.
La création et la configuration des objets s'effectuent :

- Dans le menu : CONFIGURATION / OBJETS
- Dans le menu raccourci : 

- Depuis n'importe quel autre menu via le bouton 

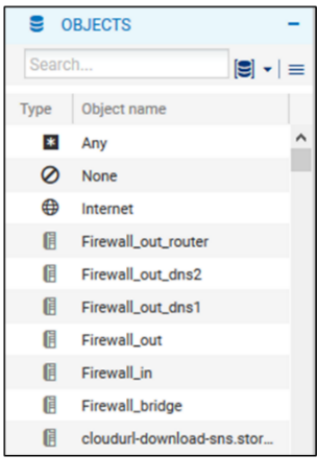
  Les objets sont classés en 3 catégories :
  1. **Objets Réseau :** Regroupe tous les objets en relation avec les valeurs réseaux (adresse IP, numéro de port, numéro de protocole, etc.) et les objets temps.
  2. **Objets Web :** Groupes d'URL (ou groupes de catégories) et groupes de noms de certificats.
  3. **Certificats et PKI :** Permet la création et la gestion des autorités de certification et de tous les certificats (de type serveur, utilisateur, ou smartcard) qui en découlent.

Nous nous intéresserons principalement aux objets réseaux. Les objets Web seront abordés dans le chapitre « Filtrage applicatif ». Les objets Certificats et PKI seront abordés dans le chapitre « PKI ».
Lors de la création de la passerelle par défaut (Fiche N°1, phase 2), vous avez créé l'**objet Machine FWOUT_Siege.**
On peut distinguer deux types d'objets particuliers en plus des objets qui peuvent être créés par l'administrateur :
• **Objets implicites :** Ils sont créés automatiquement par le firewall et dépendent de la configuration réseau. Ces objets sont en lecture seule et ne peuvent être ni modifiés ni supprimés par l'administrateur. Par exemple, l'objet **« Firewall_out »**, créé automatiquement lorsqu'une adresse IP est associée à l'interface « OUT » ou l'objet **« Network_internals »** qui regroupe tous les réseaux accessibles via les interfaces internes.
• **Objets préconfigurés :** Ils sont présents par défaut dans la liste des objets. Ils représentent des valeurs de paramètres réseaux standardisées (ports, protocoles, réseaux) et des valeurs nécessaires pour le fonctionnement du firewall (adresse IP des serveurs Stormshield pour les mises à jour). On trouvera par exemple le protocole ICMP et l'objet « **Internet** » ; ce dernier regroupe l'ensemble des machines ne faisant pas partie des réseaux internes.
NOTE : Il est conseillé d'utiliser les objets implicites et préconfigurés et d'éviter de créer d'autres objets portant les mêmes valeurs.

La syntaxe des noms des objets doit respecter quelques restrictions définies dans le tableau ci-dessous. De plus, elle est insensible à la casse.
Recommandations :

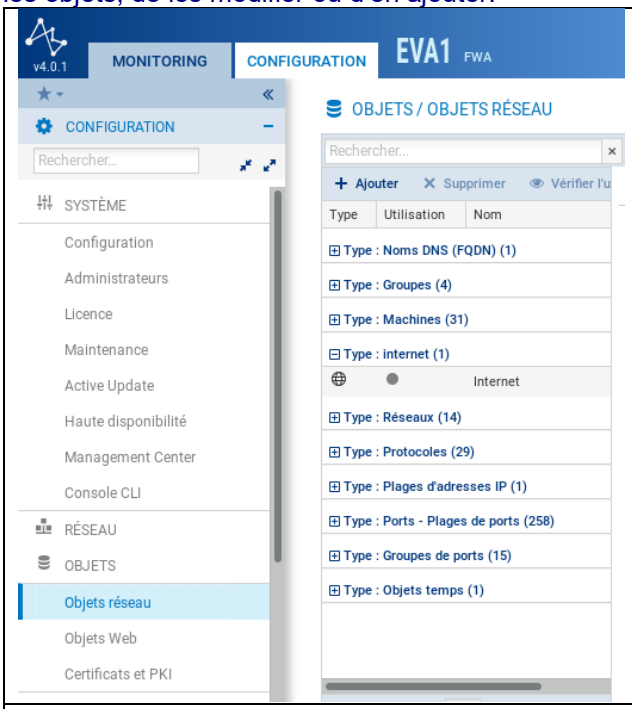
- ✓ **utiliser les objets implicites** ou pré-configurés ;
- ✓ **suivre une convention de nommage** des objets bien définie et l'appliquer strictement évite la création de doublons et facilite la lecture des objets ;
- ✓ utiliser un **groupe d'objet d'administration** contenant l'ensemble des IP et des réseaux d'administration permet de réutiliser ce groupe dans toutes les règles de filtrage liées à l'administration et donc de maintenir leur cohérence tout en facilitant leur modification ;
- ✓ limiter l'usage des objets dynamiques (type FQDN et Dynamic Host) : ils génèrent des requêtes DNS régulières. Cela sollicite le réseau et le pare-feu, utilisez cette fonctionnalité lorsqu'elle est nécessaire ;
- ✓ limiter le nombre d'objets inutilisés : ils chargent l'affichage et sont bien souvent oubliés et recréés ;
- ✓ **éviter les doublons**, ils doivent être traqués et supprimés car c'est une source d'erreur courante lors de la modification de règles de filtrage. On se retrouve dans un cas où la modification d'un objet n'impacte pas toutes les règles qui auraient dû l'être, créant ainsi des trous dans la sécurité.

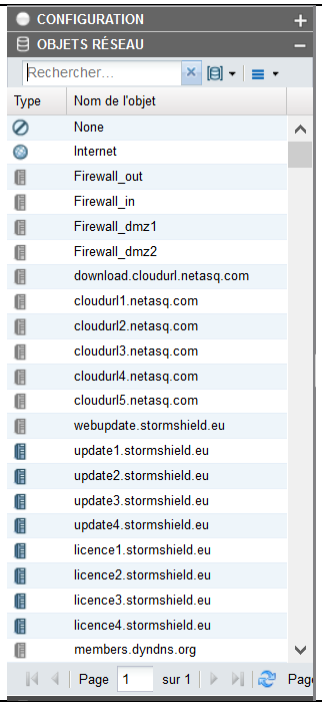
Préfixes interdits	Caractères interdis dans le nom	Noms d'objets interdis	Caractères interdits dans la description
firewall_	<tabulation>	Any	<tabulation>
Network_	<espace>	None	#
Ephemeral_	!	Anonymous	@
Global_	"	Broadcast	"
Vlan_	#	Internet	
Bridge_	,		
	=		
	@		
	[		
	]		
	\		



3.2 - Création des Objets Réseaux

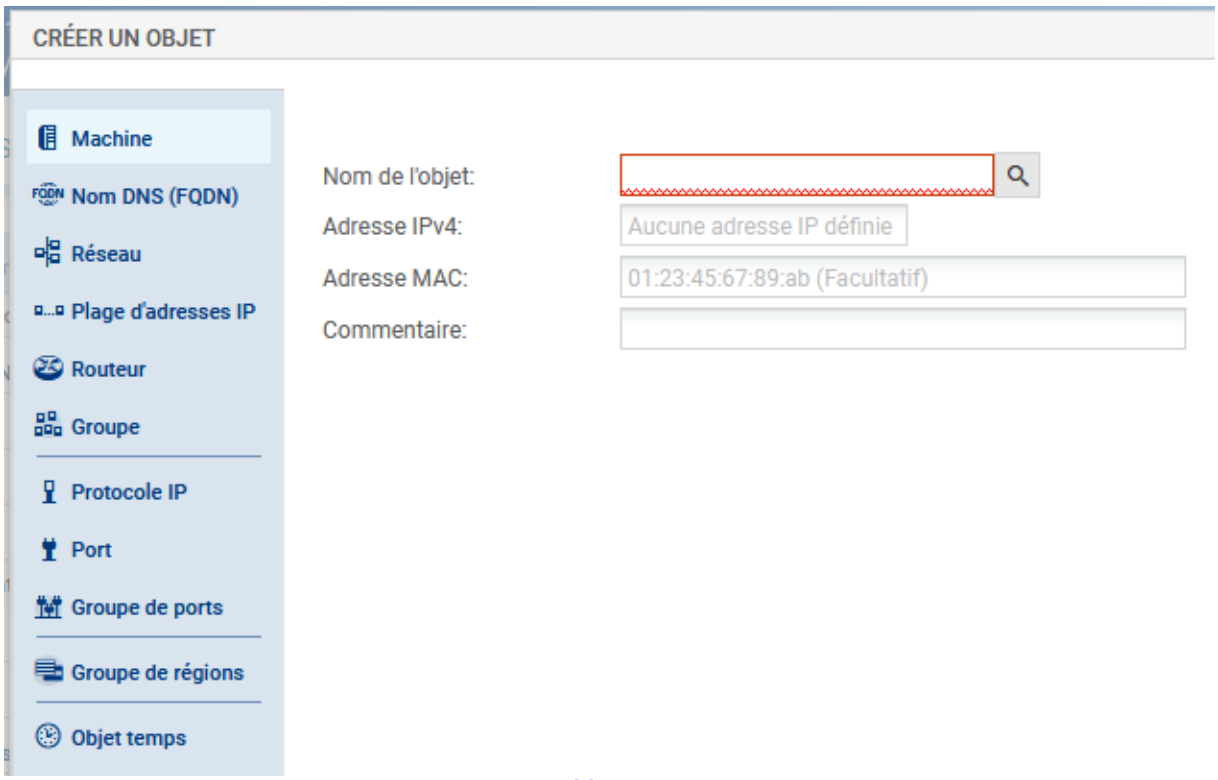
Le menu **`Configuration`** / **`Objets`** / **`Objets réseau`** ou le menu **`Objets réseau`** permettent de visualiser les objets, de les modifier ou d'en ajouter.





Menu **Configuration** / **Objets** Onglet **Objets réseaux**	Afficher les objets existants dans la base d'objets réseau

💻 Ouvrez **`Configuration`** / **`Objets`** / **`Objets réseau`** et cliquez le bouton **Ajouter** pour ajouter les objets souhaités.



Les types d'objets suivants peuvent être créés :

- **Machine** : Une adresse IP,
- **Nom DNS (FQDN)** : Toutes les adresses IP associées à un nom FQDN par résolution DNS,
- **Réseau** : Une adresse réseau,
- **Plage d'adresses IP** : Une plage d'adresses,
- **Routeur** : Permet de renseigner une ou plusieurs passerelles pour un routage par répartition de charge avec ou sans passerelle de secours.
- **Groupe** : Un groupe d'objets portant une ou plusieurs adresses IP : machines, plages d'adresses IP, réseaux ou d'autres groupes,
- **Protocole IP** : l'ID du protocole au niveau IP,
- **Port - Plage de ports** : Un port ou une plage de ports. Il/Elle peut être limité(e) à un protocole de transport particulier (TCP ou UDP),
- **Groupe de ports** : Un groupe d'objets portant des ports ou des plages de ports, ainsi que d'autres groupes de ports,
- **Groupe de régions** : Un groupe de pays ou de continents. Ce type d'objet peut être utilisé dans la géolocalisation des adresses IP,
- **Objet temps** : Un événement temporel (ponctuel, jour de l'année, jour(s) de la semaine ou plage(s) horaire(s)).

Veillez à utiliser un typage d'objets adéquat (objet réseau pour les réseaux, objet machine pour les pare-feu , etc.).

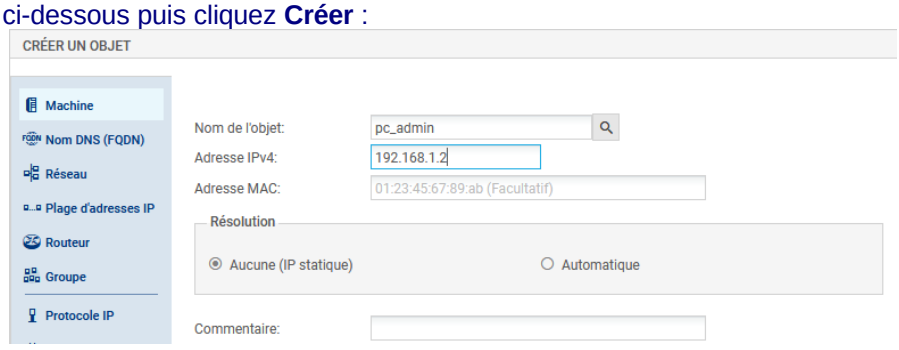
Note : Dans ce qui suit, le « x » correspond à l'agence considérée, A⇒1, B⇒2, C⇒3, D⇒4, etc.

3.2.1 - Créer des Objets Machines et Réseaux

Vous allez maintenant créer les objets correspondants à vos machines et réseaux internes.

a. Créez un objet **Machine** de nom "pc_admin" avec l'adresse 192.168.x.2

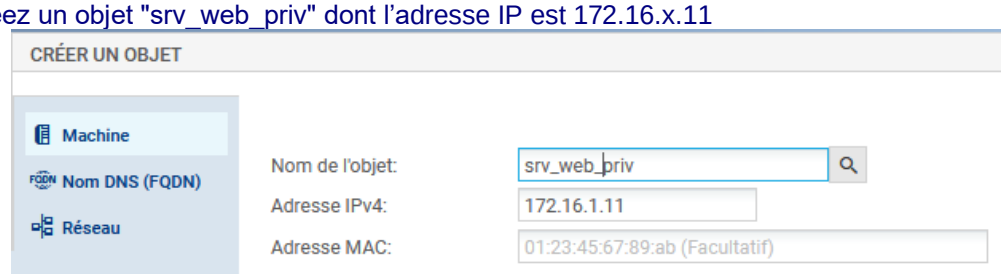
💻 Dans **`Configuration`** / **`Objets`** / **`Objets réseau`** cliquez le bouton **Ajouter** et saisissez les valeurs ci-dessous puis cliquez **Créer** :



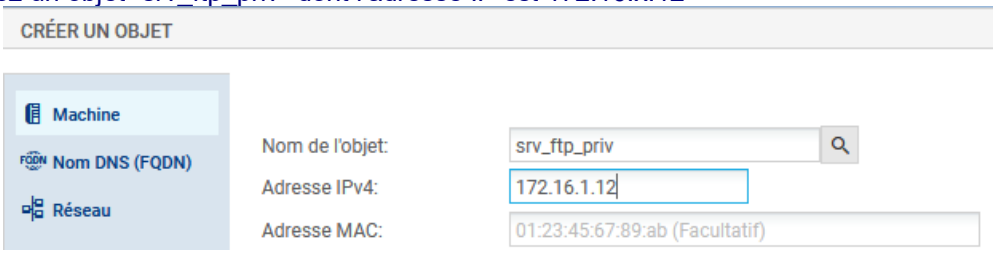
b. Créez un objet "srv_dns_priv" dont l'adresse IP est 172.16.x.10

Vous pouvez utiliser le bouton **Créer et dupliquer** pour la création des objets de même type.

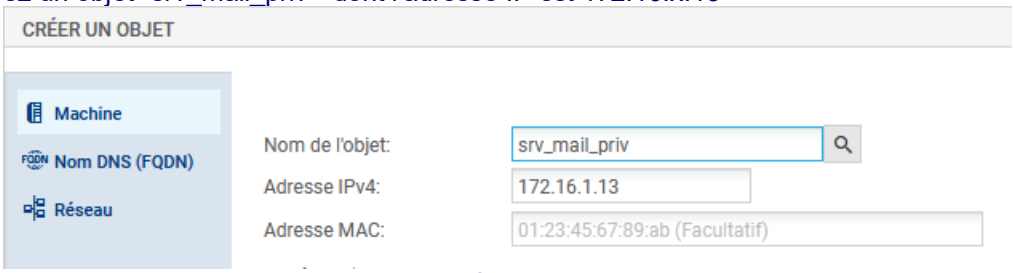
c. Créez un objet "srv_web_priv" dont l'adresse IP est 172.16.x.11



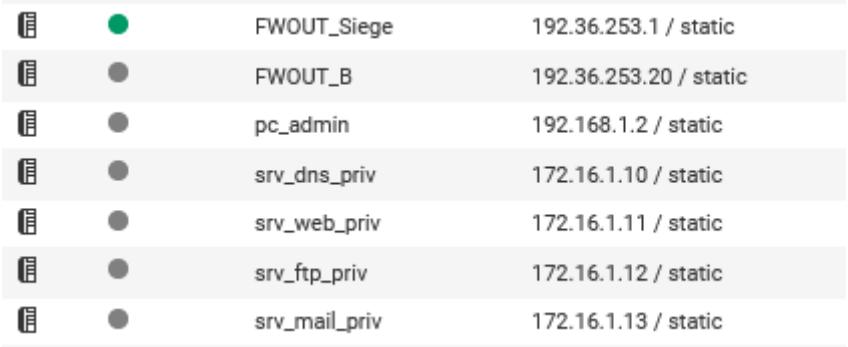
d. Créez un objet "srv_ftp_priv" dont l'adresse IP est 172.16.x.12



e. Créez un objet "srv_mail_priv " dont l'adresse IP est 172.16.x.13

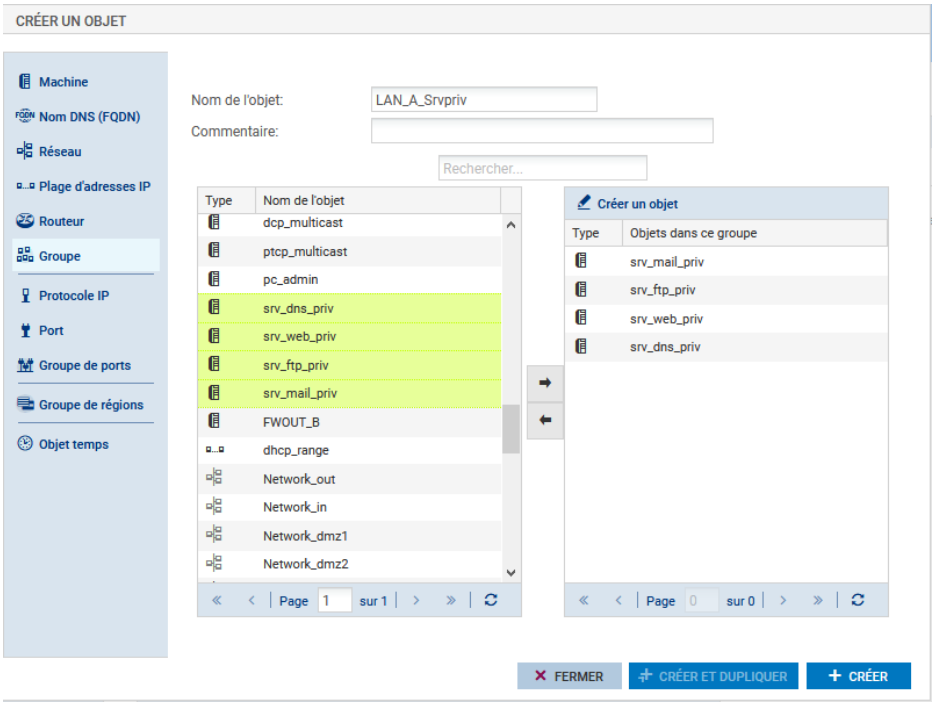


💻 Cliquez la liste **Type** : **Machines** pour déplier et visualiser son contenu.
Vous devez avoir à la fin de la liste des objets **Machines**, les nouveaux objets créés :



f. Créez un groupe d'objets qui contiendra les 4 serveurs que vous venez de définir de nom **LAN_A_Srvpriv**

💻 Cliquez **Ajouter** puis **Groupe,** dans la zone **Nom de l'objet** saisissez **LAN_A_Srvpriv** puis sélectionnez les 4 objets serveurs et à l'aide de la flèche ➡ déplacez les dans la zone de droite **Objets dans ce groupe** puis cliquez **Créer**.

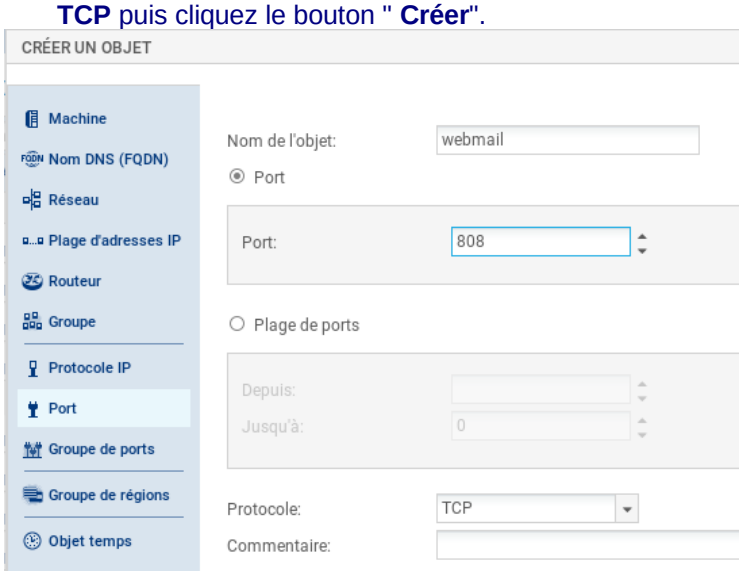


En suivant le même procédé, **créez les objets machines et réseaux** pour l'agence de votre « binôme » et pour le réseau DMZ du siège :
– Firewalls distants (adresse des interfaces externes), exemple : **FWOUT_x,** en 192.36.253.x0
– Réseaux distants (adresse des réseaux internes), exemple : **LAN_x** en 192.168.x.0 / 255.255.255.0
– Réseau DMZ distant du siège : **DMZ_Siege** en 172.16.250.0 / 255.255.255.0

3.2.2 – Créer un objet Port

Ajoutez un nouvel objet **Port** basé sur **TCP** fonctionnant sur le port **808**, appelé **webmail**

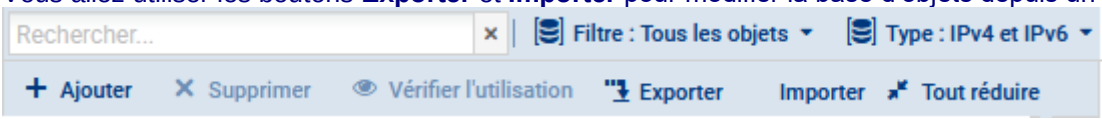
Cliquez le bouton "**Ajouter**" « **Port** », choisir le type **Port**, Nom de l'objet : **webmail**, Port : 808, Protocole : **TCP** puis cliquez le bouton " **Créer**".



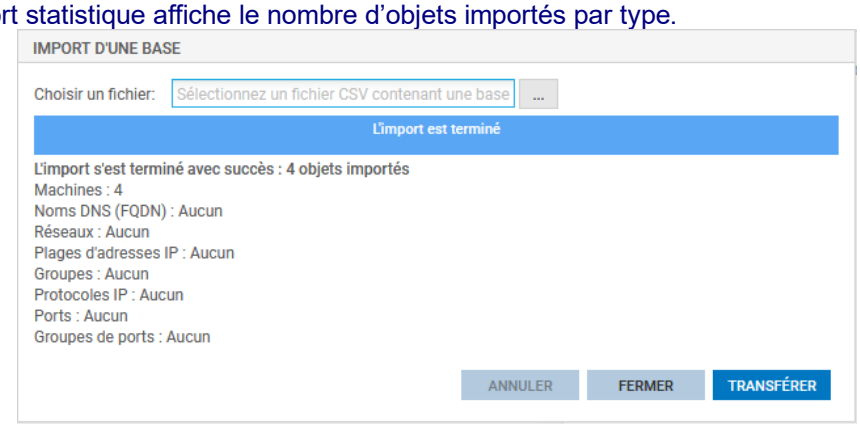
3.3 - Import/Export des Objets Réseaux

Il est possible d'exporter la base d'objets du pare-feu SNS dans un fichier CSV en cliquant sur le bouton « **Exporter** ». Le fichier CSV généré contient les objets machines, plages d'adresses IP, réseaux, FQDN, ports – plages de ports, protocoles, groupes et groupes de ports.
Les objets sont organisés par catégorie et séparés par des lignes contenant les noms des paramètres : #type, #name, #IP, etc… (les paramètres diffèrent en fonction des catégories d'objets). Les attributs d'un objet, quand à eux, sont séparés par des virgules.
Il est possible d'importer des objets depuis un fichier CSV possédant le même format que le fichier exporté.
Un rapport statistique affiche le nombre d'objets importés par type. En cas d'erreur d'import, la base d'objets n'est pas modifiée.

NOTE : Les objets du fichier importé écrasent ceux du firewall s'ils portent le même nom. Les autres objets ne sont pas affectés.
Vous allez utiliser les boutons **Exporter** et **Importer** pour modifier la base d'objets depuis un fichier csv.



- Cliquez **Exporter**, pour exporter la base d'objets précédemment créés dans un fichier CSV.
- En vous basant sur le format de ce fichier, créez un autre fichier CSV « ObjetsSNSPub.csv » contenant quatre nouveaux objets machines correspondant à l'adresse publique de vos serveurs privés :
  « srv_dns_pub » : 192.36.253.x0
  « srv_web_pub » : 192.36.253.x1
  « srv_ftp_pub » : 192.36.253.x2
  « srv_mail_pub » : 192.36.253.x3
  Vous allez importer le fichier CSV dans la base d'objets réseaux.
- Cliquez **Importer**, puis choisissez le fichier « ObjetsSNSPub.csv » et cliquez **Transférer** pour commencer l'import puis **Fermer**. Une barre d'avancement permet de visualiser le déroulement de l'import. Et une fois fini, un rapport statistique affiche le nombre d'objets importés par type.



NB : En cas de problème à l'importation, encodez le fichier en UTF-8 avec des retours à la ligne type Unix (LF).
Vous devez avoir les nouveaux objets machine dans la liste :

- Copiez le fichier CSV ver un nouveau fichier : **ObjetsSNSPub_X.csv**, remplacez les noms et les adresses IP par les adresses IP publiques des machines de votre binôme
  « srv_dns_pub_X » : 192.36.253.y0
  « srv_web_pub_X » : 192.36.253.y1
  « srv_ftp_pub_X » : 192.36.253.y2
  « srv_mail_pub_X » : 192.36.253.y3
- Cliquez **Importer**, puis choisissez le fichier « ObjetsSNSPub_X.csv » et cliquez **Transférer** puis **Fermer**.

Les objets ainsi créés seront utilisés dans les règles de filtrage et de NAT.

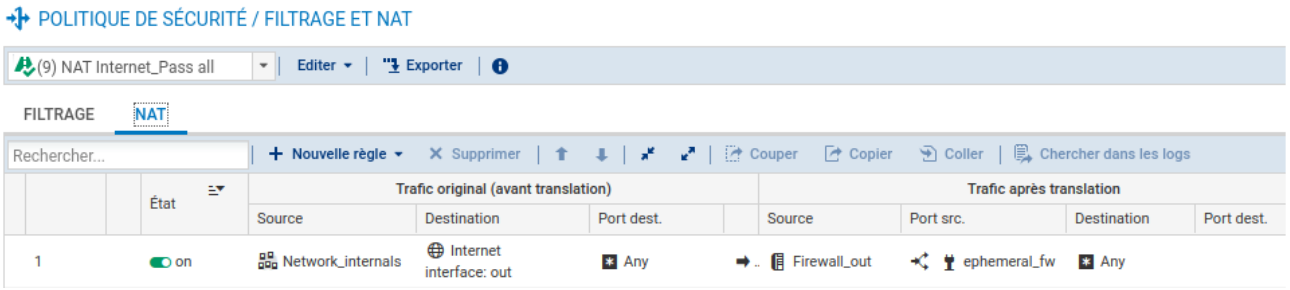
Fiche pratique n°3 : Configuration de la NAT

Dans cette partie, vous allez reprendre l'architecture présentée dans la fiche N°1 et mettre en place des règles de redirection de ports NAT qui vont permettre d'accéder aux serveurs en DMZ via des adresses IP « publiques ».

Phase 4 Traduction d'adresses (NAT/PAT)

En phase 2 vous avez mis en place une règle de NAPT pour permettre l'accès à Internet à vos réseaux internes via la passerelle par défaut du siège.

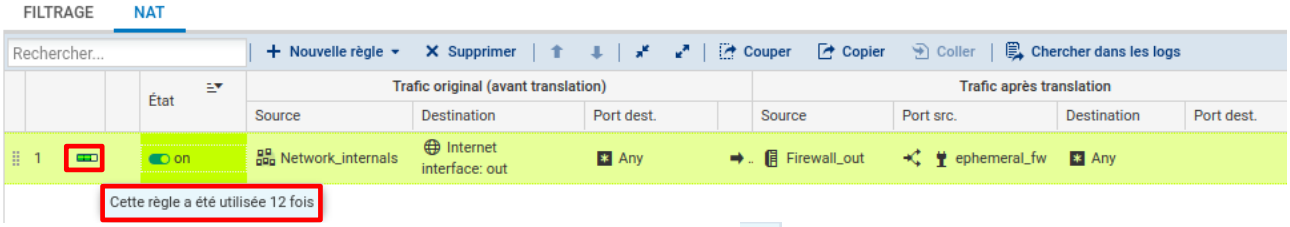
- Ouvrez **Configuration / Politique de sécurité / Filtrage et NAT** sur le pare-feu de votre agence.
- Dans la liste déroulante des politiques de sécurité, choisissez la politique **(09) NAT Internet_Pass all** puis **onglet NAT .**



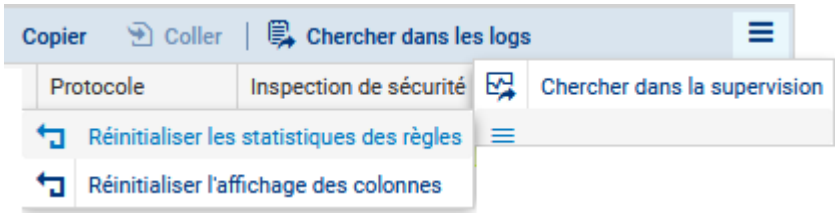
- Au besoin, cliquez le bouton **Appliquer** puis **Activer la politique « NAT Internet_Pass all ».**

Étape 1 : Testez l'application de la règle de NAT en envoyant un ping vers la passerelle par défaut.

- Depuis votre client et depuis la machine serveur debian de votre agence, tapez : **ping 192.36.253.1**
  Dans la liste des règles la barre devient verte quand les règles s'appliquent et une info-bulle indique le nombre de fois où la règle a été appliquée :



- Dans le bandeau d'affichage des règles, dépliez le menu ☰ cliquez sur **Réinitialiser les statistiques des règles** pour remettre les compteurs à zéro.



4.1 - Mise en œuvre de la NAT statique

Étape 2 : Copiez la politique de filtrage/NAT **(09) NAT Internet_Pass all** vers la politique **(04)** et la renommer « **Lab4_NAT** ».

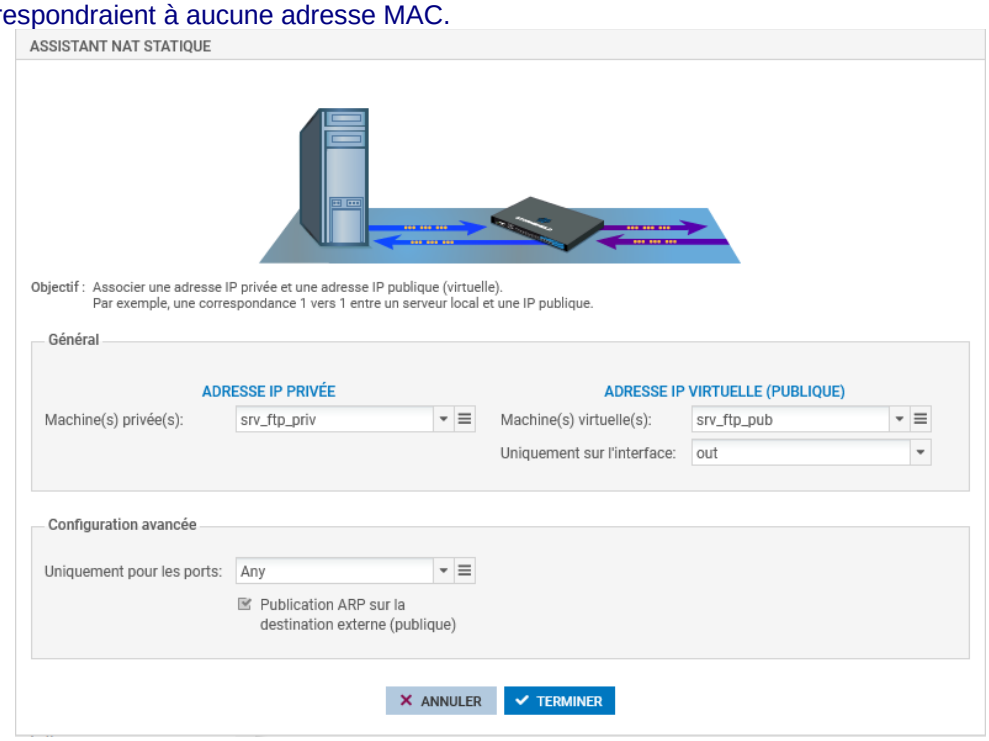
- Dans la liste déroulante des politiques de sécurité, choisissez la politique **(09) NAT Internet_Pass all .**
- Cliquez **Éditer** puis **copier vers** et choisir une politique vide (par exemple **Filter 04**).
- Cliquez **Sauvegarder les modifications…**
- Dans la liste déroulante des politiques de sécurité, choisissez la politique copiée **(04) NAT Internet_Pass all .**
- Cliquez **Éditer** puis **Renommer** et renommez-là en « Lab4_NAT », puis **Mettre à jour**.
- Cliquez le bouton **Appliquer** puis **Activer la politique** « Lab4_NAT ».

Votre agence dispose de 2 adresses IP publiques « 192.36.253.x2 » et « 192.36.253.x3 » réservées respectivement à vos serveurs FTP et MAIL (au besoin ajoutez ces 2 objets créés Phase 3).

Vous allez configurer des règles de redirections de ports (NAT statique) afin de rendre accessible vos services hébergés par le serveur Debian de la DMZ.

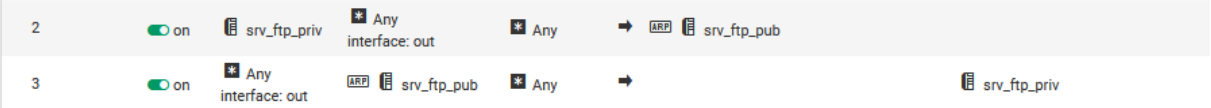
Étape 3 : Vous allez ajouter les règles de NAT statique qui permettent de joindre chaque serveur depuis le réseau externe grâce à son adresse IP publique.

- Dans votre politique **(04) Lab4_NAT**, sélectionnez l'onglet **NAT** puis **Nouvelle règle/ règle de NAT statique (bimap)**, un assistant s'ouvre :
  - **Machine(s) privée(s)** : L'adresse IP privée du serveur en interne
  - **Machine(s) virtuelle(s)** : L'adresse IP publique virtuelle dédiée au serveur interne
  - **Uniquement sur l'interface** : L'interface externe depuis laquelle le serveur est accessible avec son adresse IP publique virtuelle.
  - **Uniquement pour les ports** : La règle de NAT statique permet de translater tous les ports, cependant, il est possible de la restreindre en spécifiant un ou une plage de ports au niveau de ce paramètre. Il est conseillé de laisser cette valeur à **Any** et de restreindre le port directement dans les règles de filtrage.
  - **publication ARP** : cochez **Activer la publication ARP** pour l'adresse IP publique. Cette publication permet de faire correspondre les différentes IP publiques virtuelles utilisées à l'adresse MAC de l'interface WAN (out) du firewall. Sans l'activation de cette option, les adresses IP virtuelles ne correspondraient à aucune adresse MAC.

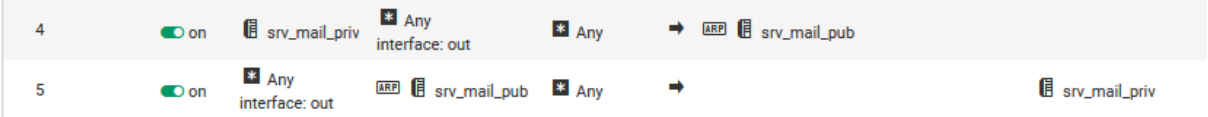


- Dans **Adresse IP Privée**, **Machine(s) privée(s),** choisissez l'adresse privée de la machine FTP : objet **srv_ftp_priv**.
- Dans **Adresse IP Virtuelle**, **Machine(s) virtuelle (s),** choisissez l'adresse publique de la machine FTP : objet **srv_ftp_pub**.
- Choisissez **out** dans **Uniquement sur l'interface** et laissez **Any** dans **Uniquement pour les ports** et cochez **Publication ARP** et cliquez **Terminer**.

L'assistant ajoute deux règles NATs. La première règle pour la traduction du **flux sortant** du serveur interne **vers le réseau public** et la deuxième pour le **flux entrant** à destination de l'adresse IP publique virtuelle. Les deux règles peuvent être modifiées par la suite indépendamment l'une de l'autre.



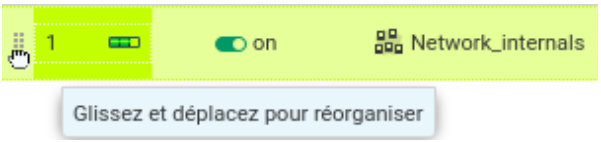
- Procédez de manière identique pour le serveur mail : objet **srv_mail_priv** et objet **srv_mail_pub**



Afin que les règles de redirection de ports s'appliquent avant la règle de NAT dynamique, il est nécessaire de déplacer la règle **N°1 de NAT dynamique** en dernière position. Dans le cas contraire, les flux des serveurs

FTP et SMTP dirigés vers Internet auraient après translation l'IP publique du firewall au lieu de leur IP publique dédiée.

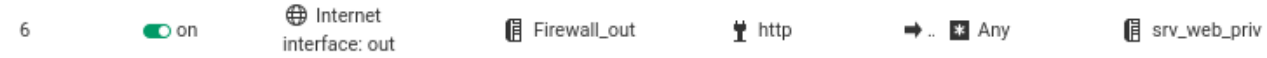
- Sélectionnez la règle N°1 de NAT dynamique et pointez la zone pointillée à gauche, une main apparaît et vous pouvez déplacer la règle en bas de la liste.



4.2 - Mise en œuvre de la redirection de ports

Étape 3 : Vous allez ajouter une règle de NAT afin que votre serveur WEB (objet srv_web_priv, protocole http) soit joignable grâce à une redirection de port via l'adresse IP publique OUT de votre firewall : « 192.36.253.x0 ».

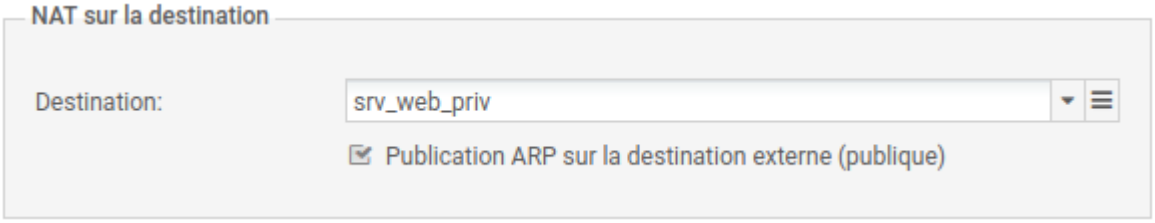
- Dans votre politique **(04) Lab4_NAT**, sélectionnez l'onglet **NAT** puis **Nouvelle règle / règle simple**, modifiez avec les paramètres suivants :
  Source originale = **Internet**, Interface d'entrée = **out**
  Destination originale = **Firewall_Out**, Port dest= **http**
  Source translatée = **Any**, Destination translatée = **srv_web_priv**, Port destination translaté = **none**.



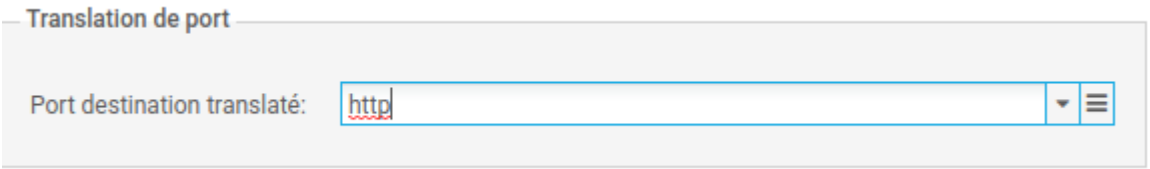
- Cliquez **Appliquer** puis **Oui, Activer la politique** puis confirmer.

NB : Il est également possible de réaliser une redirection de ports directement lors de la création d'une règle de filtrage. L'intérêt d'intégrer le filtrage et la redirection dans une règle unique est d'optimiser les performances puisque le pare-feu réalise un seul traitement au lieu de deux. Voici un exemple ci-dessous équivalent à la règle précédente :

*Dans l'onglet **Destination** de la règle de filtrage, choisissez l'onglet **Configuration avancée**, puis dans **NAT sur la destination**, sélectionnez l'objet correspondant à votre serveur web privé :*



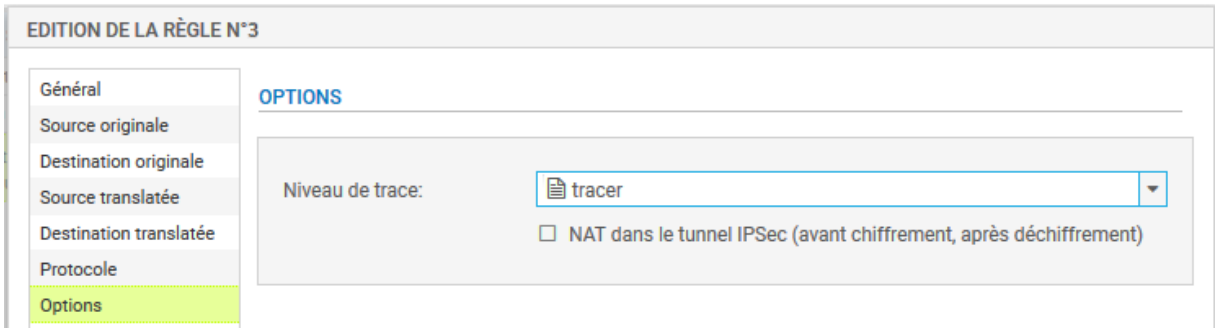
Puis dans l'onglet Port/Protocole, choisir http dans la zone Port destination translaté.



4.3 - Traçage des règles de NAT

Étape 4 : Vous allez activer le traçage des règles de NAT pour les flux entrants, ceci permet d'avoir les informations visibles dans les Journaux d'audit (logs).

- Double-cliquez une règle (par ex la règle n°3), et choisissez l'onglet **Options**, et dans niveau de trace **tracer** puis **OK.** Répétez l'opération pour les autres règles **entrantes**.



Vous pouvez tester l'accès à l'ensemble de vos ressources et vérifier le traçage des règles demandées (flux entrants) dans les logs du firewall (journal **standard** et journal **Filtrage**). Vous pouvez par exemple tenter d'accéder via des ping d'un serveur debian à l'autre.

Cliquez l'onglet **Monitoring** puis **LOGS - Journaux d'audit / Vues / Trafic réseau** : vous devriez voir apparaître les ping vers la passerelle par défaut ou vers 1.1.1.1 effectués précédemment.

LOG / TRAFIC RÉSEAU

Dernière heure | Actualiser | Rechercher... | Recherche avancée

RECHERCHE DU - 11/12/2021 17:51:52 - AU - 11/12/2021 18:51:52

Enregistré à	Action	Utilisateur	P..	Nom de la source	P..	Nom de destination	Nom du port dest.
18:51:52	Autoriser			Anonymized		www.a.net	http
18:51:52				Anonymized		www.google.fr	https
18:51:52	Autoriser			Anonymized		www.google.fr	https
18:51:46	Autoriser			Anonymized		3.debian.pool.ntp.org	ntp
18:51:45	Autoriser			Anonymized		0.debian.pool.ntp.org	ntp
18:51:41	Autoriser			Anonymized		www.b.net	http
18:51:41				Anonymized		webmail.b.net	http
18:51:39				Anonymized		www.b.net	http
18:51:39	Autoriser			Anonymized		www.b.net	http
18:51:29				Anonymized		FW_B	
18:51:17				Anonymized		1.1.1.1	
18:51:10				Anonymized		gw_default	

À faire : rédiger un rapport de test répondant aux points ci-dessous

- Concevez le plan de test des règles de redirection de port que vous avez implémenté, vous le testerez à partir d'une machine virtuelle cliente de chaque agence et en démarrant les serveurs debian de chaque agence. Vous devrez dans un tableau pour chaque règle décrire les machines impliquées, la nature du test (protocole, sens…) et les résultats.
- Testez les trafics sortants depuis un client dans l'agence A et tester les trafics entrants depuis l'agence B.
- En consultant les traces, confirmez :
  - Le traitement de chaque flux par la règle de NAT qui lui correspond.
  - Le traçage des règles demandées.

Fiche pratique n°4 : Configuration du filtrage protocolaire

Dans cette partie, vous allez reprendre l'architecture présentée dans la fiche N°1 et mettre en place des règles de filtrage afin de sécuriser l'accès à votre réseau local, à votre serveur en DMZ et interdire certains flux.

Phase 5 Filtrage protocolaire

La mise en place d'une politique de filtrage, permet à l'administrateur de définir les règles qui permettront d'autoriser ou de bloquer les flux au travers du pare-feu SNS. Selon les flux, certaines inspections de sécurité (analyse antivirale, analyse antispam, filtrage URL, …) peuvent être activées (nous détaillerons ces analyses dans le chapitre « Filtrage applicatif »). Les règles de filtrage définies doivent respecter la politique de sécurité de l'entreprise.

5.1 - Présentation des fonctionnalités

Pour définir un flux, une règle de filtrage se base sur de nombreux critères ; ce qui offre un haut niveau de granularité. Parmi ces critères, il est notamment possible de préciser :

- l'adresse IP source et/ou destination ;
- la réputation et la géolocalisation de l'adresse IP source et/ou destination ;
- l'interface d'entrée et/ou sortie ;
- l'adresse réseau source et/ou destination ;
- le FQDN source et/ou destination ;
- la valeur du champ DSCP ;
- le service TCP/UDP (n° de port de destination) ;
- le protocole IP (dans le cas d'ICMP, le type de message ICMP peut être précisé) ;
- l'utilisateur ou le groupe d'utilisateurs devant être authentifié.

Le nombre de règles de filtrage actives dans une politique est limité. Cette limite dépend exclusivement du modèle de firewall SNS.
Le premier paquet appartenant à chaque nouveau flux reçu par le pare-feu est confronté aux règles de filtrage de la première à la dernière ligne. Il est donc recommandé d'ordonner au mieux les règles de la plus restrictive à la plus généraliste.
Par défaut, tout trafic qui n'est pas autorisé explicitement par une règle de filtrage est bloqué.

NB : Dans les recommandations pour la définition d'une politique de filtrage réseau d'un pare-feu publiées par l'ANSSI le 30 mars 2013, il est précisé que la règle finale qui consiste à bloquer et journaliser tout ce qui n'est pas autorisé par les règles précédentes doit apparaître explicitement à la fin de la politique de filtrage appliquée. L'ajout de cette règle explicite garantit l'application du modèle de sécurité positif (tout ce qui n'a pas été autorisé précédemment est interdit) et permet de s'assurer que la trace des flux non légitimes est conservée.

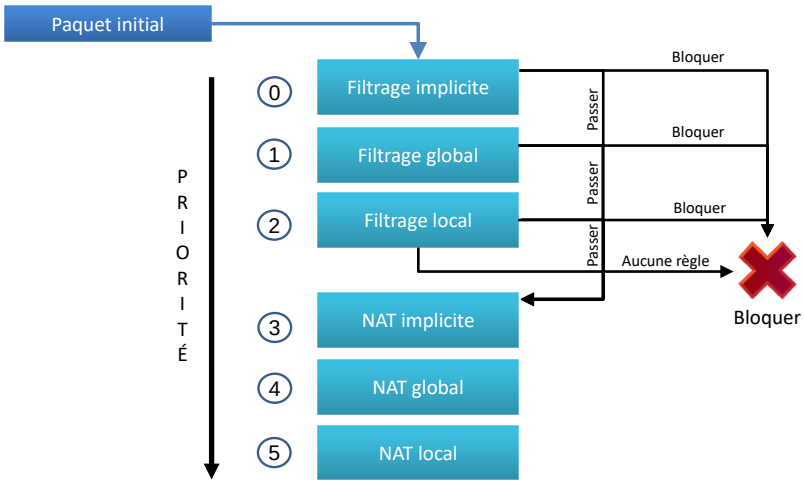
Les firewalls SNS utilisent la technologie SPI (Stateful Packet Inspection) qui leur permet de garder en mémoire l'état des connexions TCP (et SCTP) et des pseudo-connexions UDP et ICMP afin d'en assurer le suivi et de détecter d'éventuelles anomalies ou attaques. La conséquence directe de ce suivi « Stateful » est l'autorisation d'un flux par une règle de filtrage uniquement dans le sens de l'initiation de la connexion ; les réponses faisant partie de la même connexion sont automatiquement autorisées. Ainsi, nous n'avons nul besoin d'une règle de filtrage supplémentaire pour autoriser les paquets réponse d'une connexion établie au travers du firewall.
La figure suivante présente l'ordre d'application des règles de filtrage et de NAT, il est important de noter que les paquets sont filtrés **avant** que la phase de traduction (NAPT) n'ait lieu c'est pourquoi nous avons mis au point les règles de NAT avec une politique **Pass all**.
Le premier paquet reçu est confronté aux règles de filtrage des différents niveaux suivant l'ordre présenté dans la figure ci-après. Dès que les éléments du paquet correspondent à une règle dans un niveau, l'action de la règle (bloquer ou autoriser) est appliquée et le paquet n'est plus confronté aux règles suivantes. Si aucune règle de filtrage ne correspond, **le paquet est bloqué par défaut**.
Dans le cas où le paquet est autorisé, il est confronté aux règles de NAT des différents niveaux toujours suivant l'ordre présenté ci-après.

- **Le filtrage implicite :** Regroupe les règles de filtrage préconfigurées ou ajoutées dynamiquement par le firewall pour autoriser ou bloquer certains flux après l'activation d'un service. Par exemple, une règle implicite autorise les connexions à destination des interfaces internes du pare-feu SNS sur le port HTTPS (443/TCP) afin d'assurer un accès continu à l'interface d'administration Web. Autre

exemple, dès l'activation du service SSH, un ensemble de règles implicites sera ajouté pour autoriser ces connexions depuis toutes les machines des réseaux internes.

- **Le filtrage global :** Regroupe les règles de filtrage injectées au firewall depuis l'outil d'administration « Stormshield Management Server » (SMC) ou après affichage des politiques globales.
- **Le filtrage local :** Représente les règles de filtrage ajoutées par l'administrateur depuis l'interface d'administration du pare-feu SNS.

L'ORDONNANCEMENT DES RÈGLES DE FILTRAGE ET DE NAT



Les règles implicites sont accessibles depuis le menu **CONFIGURATION / POLITIQUE DE SÉCURITÉ / Règles implicites**. Chaque règle peut être activée/désactivée.
NB : La modification de l'état de ces règles a un impact direct sur le fonctionnement des services du firewall. Pour que le service concerné fonctionne toujours, il faut s'assurer au préalable que le flux est autorisé par les règles de priorité moindre telles que globales ou locales.

Les règles de filtrage font partie d'une politique présentée précédemment dans le chapitre « Traduction d'adresses ».

💻 Ouvrez le menu **Configuration / Politique de sécurité / Filtrage et NAT / Filtrage**

L'onglet **FILTRAGE** est composé d'un en-tête pour la gestion des règles de filtrage :

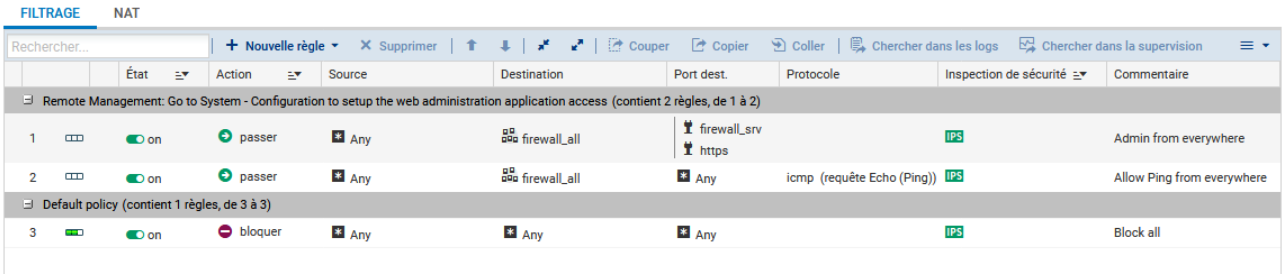
❖ Nouvelle règle :
- **Règle simple** : Ajoute une règle de filtrage standard. Par défaut, une nouvelle règle est désactivée et tous ses critères sont paramétrés à **Any**.
- **Séparateur – regroupement de règles** : Ajoute un séparateur qui regroupe toutes les règles se trouvant au-dessous (ou jusqu'au prochain séparateur). Cela permet de faciliter l'affichage d'une politique contenant un nombre de règles important. Le séparateur peut être personnalisé par une couleur et un commentaire.
- **Règle d'authentification** : Démarre un assistant qui facilite l'ajout d'une règle dont le rôle est de rediriger les connexions des utilisateurs non-authentifiés vers le portail captif.
- **Règle d'inspection SSL** : Démarre un assistant qui facilite l'ajout de règles pour l'activation du proxy SSL.
- **Règle de proxy HTTP explicite** : Démarre un assistant qui facilite l'ajout de règles pour l'activation du proxy HTTP explicite.

❖ **Supprimer** : Supprimer une règle.
❖ **Monter** / **Descendre** : Monter ou descendre la/les règle(s) sélectionnée(s) d'une position dans la liste.

5.2 - Analyse des politiques prédéfinies de filtrage

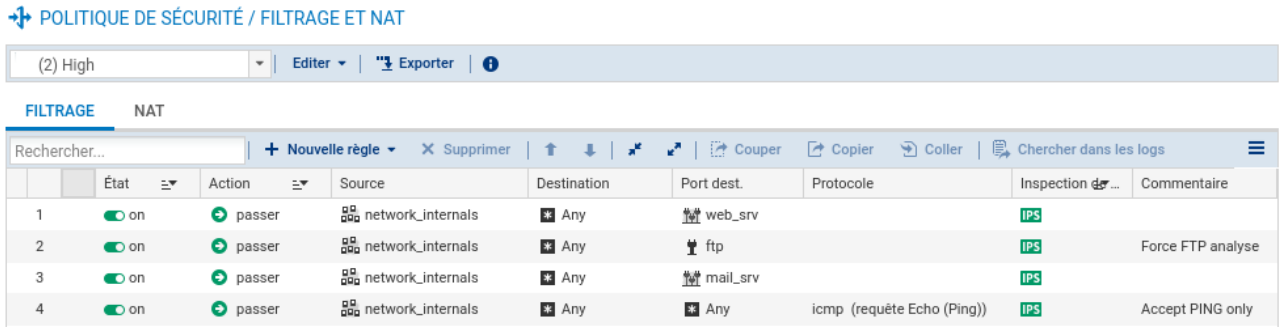
Vous allez dans un premier temps découvrir à travers les règles déjà définies dans les politiques prédéfinies de filtrage, le fonctionnement des règles de filtrage sur un pare-feu Stormshield.

💻 Ouvrez le menu **Configuration / Politique de sécurité / Filtrage et NAT / Filtrage**
💻 Dans la liste déroulante des politiques de sécurité, choisissez **(1) Block all.**



Cette politique bloque presque tous les flux (règle N°3) sauf ceux définis par les règles 1 et 2.
La règle numéro 1 autorise l'accès en **https** (443) et sur le port prédéfini **1300 firewall_srv** à toutes les interfaces du firewall, elle permet donc l'administration à distance depuis n'importe quel réseau.
La règle numéro 2 autorise les requêtes **ICMP Echo** vers toutes les interfaces du firewall, afin de pouvoir vérifier la présence du firewall à l'aide des commandes ICMP. Attention : un ping vers la passerelle par défaut échoue car il n'est pas explicitement autorisé.

Dans la liste déroulante des politiques de sécurité, choisissez **`(2) High.`**



Cette politique est un peu moins restrictive que la précédente, elle autorise certains protocoles à partir des réseaux internes.
La règle numéro 1 autorise l'accès à des services web en **http, https, dns** elle permet l'accès à des sites web.
La règle numéro 2 autorise l'accès à des services **ftp**.
La règle numéro 3 autorise l'accès à des services de messagerie en **imap, smtp, pop3** elle permet l'envoi et la réception de messages.
La règle numéro 4 autorise les requêtes **ICMP Echo** vers n'importe quelle destination des réseaux internes, afin de pouvoir vérifier la présence du firewall et des services en DMZ à l'aide des commandes ICMP. Attention : un ping vers la passerelle par défaut échoue car il n'est pas explicitement autorisé.
Vous remarquerez que pour toutes ces règles la colonne « Inspection de sécurité » stipule **IPS (Intrusion Prevention System)** qui est le niveau le plus élevé de filtrage avec inspection du contenu et le cas échéant blocage si l'on suspecte un comportement anormal ou une tentative d'intrusion.

5.3 - Mise en place des règles de filtrage

Vous allez mettre en place une nouvelle politique de sécurité basée sur vos règles de redirection NAT/PAT. Il faudra commencer par désactiver la règle de filtrage **Pass all** et ajouter les règles de filtrage qui respecteront le cahier des charges décrit ci-après.

Le cas échéant, ajoutez les adresses IP privées de vos serveurs et les IP publiques des serveurs de vos voisins dans les **Objets Réseaux** (cf Phase 3 Objets réseau).

« srv_dns_priv » : 172.16.x.x0	« srv_dns_pub_Y » : 192.36.253.y0
« srv_web_priv » : 172.16.x.x1	« srv_web_pub_Y » : 192.36.253.y1
« srv_ftp_priv » : 172.16.x.x2	« srv_ftp_pub_Y » : 192.36.253.y2
« srv_mail_priv » : 172.16.x.x3	« srv_mail_pub_Y » : 192.36.253.y3

Étape 1 : Copiez la politique de filtrage/NAT **(04) Lab4_NAT** vers une politique vide (05 par exemple).

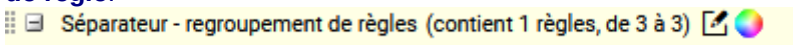
- Dans la liste déroulante des politiques de sécurité, choisissez la politique précédente **(04) Lab4_NAT.**
- Cliquez **Éditer** puis **copier vers** et choisir une politique vide (par exemple **Filter 05**).
- Cliquez **Sauvegarder les modifications…**
- Dans la liste déroulante des politiques de sécurité, choisissez la politique copiée **(05) Lab4_NAT**.
- Cliquez **Éditer** puis **Renommer** et renommez-là en « **Lab5_Filtrage_NAT »**, puis **Mettre à jour**.
- Désactivez la règle numéro 1 **Pass all (Passer any any any)** en double-cliquant sur **On** (=>Off) afin de pouvoir ajouter les règles de filtrage qui respecteront le cahier des charges défini.
- Cliquez le bouton **Appliquer** puis **Activer la politique** « **Lab5_Filtrage_NAT** ».

Attention : la règle implicite par défaut étant **Block all**, les tests de connectivité précédemment réalisés ne seront plus opérationnels puisque vous avez désactivé la règle de filtrage numéro 1 **Pass all**.

Étape 2 : Nous allons mettre en place une première série de règles sur le **Trafic sortant**. Nous vous proposons d'utiliser les bandeaux séparateurs en indiquant le rôle de chaque règle pour plus de lisibilité.

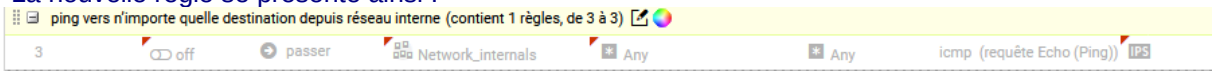
a) Votre réseau interne doit pouvoir émettre un **ping vers n'importe quelle destination**.

- Cliquez la règle numéro 2 qui passe en surbrillance et choisissez **Nouvelle règle / séparateur – Regroupement de règle**.



- Cliquez le symbole du crayon et modifiez le nom du séparateur en **ping vers n'importe quelle destination**.
- Cliquez **Nouvelle règle / règle simple**
  - **Action** : **Passer**
  - **Source** : L'adresse IP ou le réseau source, ici **Network_internals**
  - **Protocole dest** : Port destination, ici **ICMP**.
- Double-cliquez sur **Protocole** et remplir les champs comme ci-dessous :
  - **Type de protocole** : **Protocole IP**
  - **Protocole IP** : **icmp**
  - **Message ICMP** : choisir au milieu de la liste **requête Echo (Ping, type 8, code 0)**

La nouvelle règle se présente ainsi :



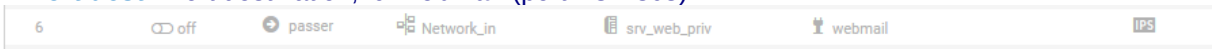
- Double-cliquez sur le bouton **off** pour passer la règle à l'état **on**, puis cliquez **Appliquer** puis **Oui, activer la politique.**

b) Votre réseau interne doit pouvoir accéder aux serveurs privés de la DMZ (DNS, WEB (ports 80 et 808 pour le webmail), FTP et SMTP).

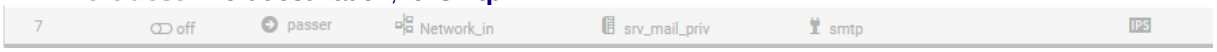
- Ajoutez un séparateur nommé **Accès aux serveurs DMZ**, choisissez **Nouvelle règle / séparateur – Regroupement de règle** puis éditez-le.
- Cliquez **Nouvelle règle /règle simple**
  - **Action** : **Passer**
  - **Source** : **Network_in**
  - **Destination** : **srv_ftp_priv**
  - **Port dest** : Port destination, ici **ftp**.

- Cliquez sur **Copier** puis **Coller** pour créer la deuxième règle à partir de la précédente :
  - **Action** : **Passer**
  - **Source** : **Network_in**
  - **Destination** : **srv_web_priv**
  - **Port dest** : Port destination, ici **http**

- Cliquez sur **Copier** puis **Coller** pour créer la troisième règle pour le webmail à partir de la précédente :
  - **Action** : **Passer**
  - **Source** : **Network_in**
  - **Destination** : **srv_web_priv**
  - **Port dest** : Port destination, ici **webmail** (port **TCP 808**)

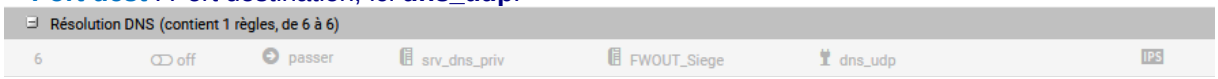


- Cliquez sur **Copier** puis **Coller** pour créer la quatrième règle pour le serveur mail smtp à partir de la précédente :
  - **Action** : **Passer**
  - **Source** : **Network_in**
  - **Destination** : **srv_mail_priv**
  - **Port dest** : Port destination, ici **smtp**

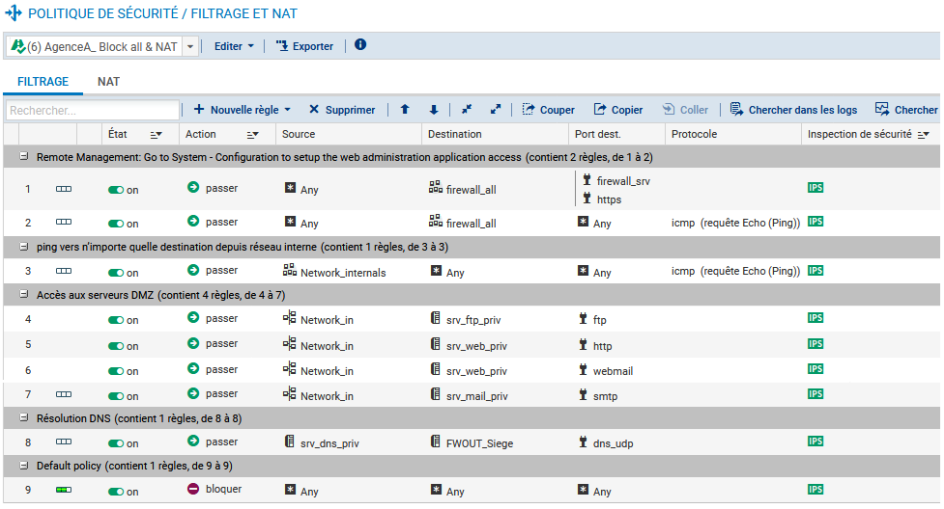


c) Seul votre serveur DNS interne (**srv_dns_priv** 172.16.x.10) sera autorisé à résoudre les requêtes DNS vers l'extérieur, et plus précisément vers l'IP publique du siège (192.36.253.1).

- Cliquez **Nouvelle règle /règle simple**
  - **Action** : **Passer**
  - **Source** : **srv_dns_priv**
  - **Destination** : **FWOUT_Siege**
  - **Port dest** : Port destination, ici **dns_udp**.



- Double cliquez sur le symbole **off** des règles pour les passer à l'état **on**, puis cliquez **Appliquer** et **Oui, activer la politique.**
  Les règles actuellement mises en place sont les suivantes :



Maintenant que vous avez vu comment construire les règles de filtrage sur un pare-feu SNS Stormshield, vous allez ajouter les 2 règles ci-dessous qui concernent le trafic sortant.

d) Votre réseau interne (DMZ incluse) doit pouvoir joindre les serveurs Web et FTP externes.

e) Votre serveur de messagerie peut envoyer des mails vers n'importe quel serveur de mail externe.

Étape 3 : Vous allez mettre en place une deuxième série de règles sur les trafics entrants (utilisez les séparateurs en indiquant le rôle de chaque règle).

Trafics entrants :

1. Les réseaux externes (dont ceux de l'agence voisine) peuvent joindre vos serveurs Web et FTP ; ces événements doivent être tracés.
2. Les serveurs mails externes sont autorisés à transmettre des e-mails à votre serveur de messagerie
3. Les réseaux externes (dont ceux de l'agence voisine) sont autorisés à pinger l'interface externe de votre SNS ; cet événement devra lever une alarme mineure.
4. Un poste sur le réseau OUT est autorisé à pinger l'interface externe de votre SNS.
5. Les réseaux externes (dont ceux de l'agence voisine) peuvent se connecter à votre SNS : via l'interface web et en SSH. Ces événements devront lever des alarmes majeures.

À faire : rédiger un rapport de test répondant aux points ci-dessous

- Concevez le plan de test des différentes règles (entrantes et sortantes) que vous avez implémenté, vous le testerez à partir d'une machine virtuelle cliente de chaque agence et en démarrant les serveurs debian de chaque agence. Vous devrez dans un tableau pour chaque règle décrire les machines impliquées, la nature du test (protocole, sens…) et les résultats.
- Testez les trafics sortants et faites tester les trafics entrants par les voisins.
- En consultant les traces, confirmez :
  • Le traitement de chaque flux par la règle de filtrage qui lui correspond.
  • Le traçage et la levée des alarmes pour les règles demandées.

Fiche pratique n°6 : Configuration du filtrage applicatif

Dans cette partie, vous allez reprendre l'architecture virtuelle présentée dans la fiche N°1 et mettre en place des règles de filtrage au niveau applicatif afin de mieux sécuriser l'accès à votre réseau.

Phase 6 Filtrage applicatif (URL, SSL…)

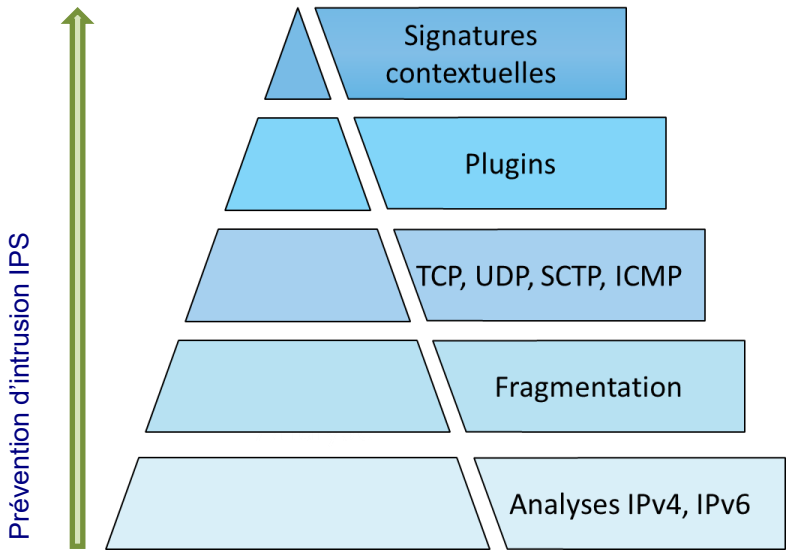
La mise en place d'une politique de filtrage, permet à l'administrateur de définir les règles qui permettront d'autoriser ou de bloquer des flux au travers du pare-feu SNS. Selon les flux, certaines inspections de sécurité (analyse antivirale, analyse antispam, filtrage URL, …) peuvent être activées sur les pare-feu SNS afin de :

- Contrôler les accès à certains sites web d'Internet (filtrage d'URL et filtrage SSL)
- Créer une politique anti-relais et antispam (filtrage SMTP)
- Effectuer une analyse antivirale sur les flux DATA (HTTP, SMTP, FTP, POP3,…)
- Bloquer les maliciels à l'aide d'une analyse comportementale sur des machines de détonation (sandboxing Breachfighter)

6.1 - Présentation du moteur de prévention d'intrusion ASQ

a) Présentation du moteur de prévention d'intrusion ASQ

Les équipements Stormshield Network Security sont équipés nativement d'un **module de prévention d'intrusion** nommé **ASQ (Active Security Qualification**). Chaque paquet reçu par le pare-feu SNS sera soumis à un ensemble d'analyses à commencer par la vérification du protocole IP. Le rôle principal de l'ASQ est de s'assurer de la conformité du paquet par rapport aux protocoles utilisés de la couche IP jusqu'à la couche applicative (grâce aux plugins) et aux signatures contextuelles (ou Patterns). C'est également l'ASQ qui est en charge de filtrer les flux et d'appliquer une opération de NAT si nécessaire.



Intégré à la pile réseau du système d'exploitation FreeBSD, le moteur de prévention d'intrusion **ASQ** dispose d'un accès privilégié aux ressources matérielles (CPU, mémoire et carte réseau).
Ce **système de prévention d'intrusion** assure le filtrage des flux ainsi que leur analyse ; dès les couches de transport et jusqu'aux couches applicatives, il applique des contrôles génériques de conformité, ainsi que des contrôles ciblés et comportementaux. Les opérations de NAT ainsi que certaines opérations de routage spécifique sont également prises en charge par ce moteur.
Ces analyses sont appliquées directement sur les connexions cherchant à traverser la pile réseau du système.

Le **système de prévention d'intrusion** ou **IPS** (Intrusion Prevention System) **détecte** et **bloque** les tentatives d'attaques des applicatifs grâce à des analyses contextuelles et comportementales complétées par une identification par signatures. Cette association présente deux bénéfices majeurs :

- Il permet de réaliser un traitement préventif sur toutes les couches de communication (du réseau à l'application) fournissant ainsi une réelle protection 0-day,
- L'usage des contextes applicatifs limite le nombre de signatures à examiner et réduit ainsi les risques de faux positifs tout en optimisant les temps de traitements pour procurer des performances optimales.

Les signatures utilisées par le moteur de prévention d'intrusion SNS sont construites pour détecter des attaques identifiables mais également leurs variantes potentielles. À titre d'exemple, la signature contextuelle sur une injection SQL par une commande SELECT (http:url:decoded:95) permet de contrer plus de 1 540 variantes d'attaques. En plus de maintenir un espace de stockage contenu, cette technique permet d'optimiser les temps de traitement et propose une protection contre de futures attaques basées sur les mêmes principes.
La **mise à jour des bases de signatures du moteur de prévention** Stormshield Network Security est assurée indépendamment de la mise à jour du firmware pour garantir une actualisation périodique et automatique afin de rester constamment protégé contre les nouvelles attaques.

Cette fonctionnalité de mise à jour automatique se nomme « Active Update » ; elle permet également d'ajouter de nouveaux contextes pour intégrer de nouvelles catégories de signatures contextuelles.

b) Les différents types d'analyses

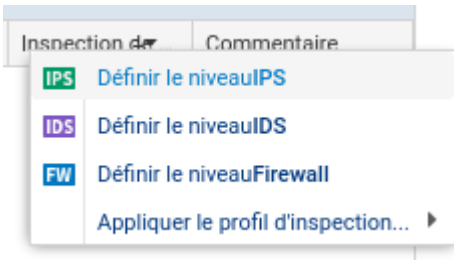
Au-delà du simple classement [niveau réseau][niveau applicatif], un firewall SNS protège le réseau selon trois familles d'analyses :

- **l'analyse protocolaire** : elle assure la conformité des flux réseau vis-à-vis des standards de communication (IP, TCP, UDP, ...) ainsi que la conformité aux protocoles applicatifs (HTTP, FTP, …) grâce aux contrôles appliqués par les contextes applicatifs,
- **l'analyse statistique** : basée sur des études statistiques du trafic transitant par le firewall, cette analyse détecte des comportements assimilables à du scan de ports, à du SYN flooding, ou encore à des tentatives de DoS (Denial of Service) par maintien de multiples connexions annonçant des petites fenêtres (SockStress),
- **l'analyse par signatures contextuelles** : elle vient compléter les contrôles de conformité sur le trafic. Cette analyse permet de se protéger de tentatives d'attaques visant spécifiquement un protocole et une implémentation cliente ou serveur, mais sans toutefois recourir à une inconformité au standard de communication. Elle s'appuie sur des bases de signatures construites par Stormshield, maintenues quotidiennement et mises à disposition sur les serveurs Active Update.

NB : Le fonctionnement détaillé de l'ASQ ainsi que ses options sont abordés dans la formation Expert (CSNE).

c) Les niveaux d'inspection de sécurité

Chaque paquet reçu par le pare-feu SNS est soumis à la politique de filtrage. Par défaut, l'analyse **IPS** (Intrusion Prevention System : système de prévention d'intrusion) est appliquée, ce qui signifie que le pare-feu SNS est capable de détecter une anomalie et de bloquer le paquet correspondant.
D'autres niveaux d'inspections peuvent être utilisés, à des fins de tests ou par nécessité ; par exemple si on contacte un serveur ne respectant pas la RFC des protocoles qu'il gère.
Ces niveaux sont à sélectionner dans la colonne **Inspection de sécurité** de la règle de filtrage concernée.



IPS : **Détecter et bloquer** (choix par défaut). L'ASQ va soumettre le paquet à l'ensemble des couches qu'il est capable d'analyser et le bloquer en cas d'anomalie.
IDS : **Détecter**. L'ASQ effectue une analyse similaire à l'IPS sauf que le paquet est toujours autorisé. C'est un profil permettant de faire un audit rapide pour une règle de filtrage donnée.
Firewall : **Ne pas inspecter.** L'ASQ ne va effectuer que très peu d'analyses sur le paquet reçu. Il se comporte comme un simple routeur filtrant.

L'ASQ est composé de 10 configurations (également nommées **profils IPS**). Chacune de ces configuration peut être éditée en fonction des besoins de l'administrateur.
La configuration par défaut, comme indiqué dans le menu **Configuration ⇒ Protection applicative ⇒ Profils d'inspection**, applique les profils **IPS_00** et **IPS_01** respectivement aux connexions **entrantes** (paquet dont l'adresse IP source ne fait pas partie d'un réseau protégé) et aux connexions **sortantes** (paquet dont l'adresse IP source fait partie d'un réseau protégé).
Si des flux sains déclenchent des alarmes, il sera sûrement nécessaire de modifier les paramètres de l'ASQ pour ne pas bloquer la production. Dans ce cas, les modifications doivent être faites au plus spécifique. De préférence dans un profil dédié qui sera appliqué sur les règles identifiant précisément le trafic concerné.
Il est alors possible, dans la table de filtrage, de forcer l'utilisation d'un profil ASQ spécifique depuis la colonne **Inspection de sécurité**. Les profils sont ensuite configurables et administrables depuis les menus **Protocoles et Applications et protections** sous **Configuration ⇒ Protection applicative**.
Enfin, par défaut, l'IPS est actif sur toutes les règles de filtrage en mode de **détection automatique du protocole**. Afin de mieux inspecter les flux, il est recommandé de qualifier manuellement le type de protocole si le port utilisé n'est pas standard. L'IPS risquerait de ne pas détecter correctement l'application.

d) Mode Proxy transparent du pare-feu

Selon les flux, certaines inspections de sécurité applicatives (analyse antivirale, analyse antispam, filtrage URL, …) peuvent être activées. L'analyse applicative complète des flux, qu'ils soient initialement chiffrés ou pas, induit l'utilisation d'un mode Proxy sur les firewalls Stormshield. L'activation d'une inspection applicative sur une règle de filtrage du firewall entraîne ainsi le démarrage des analyses en mode Proxy transparent :

- Le firewall se fait passer pour le client auprès du serveur et pour le serveur auprès du client,

- La configuration du poste client n'est pas modifiée (c'est le principe du mode transparent), par exemple, le port d'écoute et l'adresse IP du Proxy n'ont pas à être configurés sur son navigateur Internet.

NB : Une analyse sur une règle de filtrage en mode **IPS** seulement n'utilise pas de mécanisme de type Proxy.

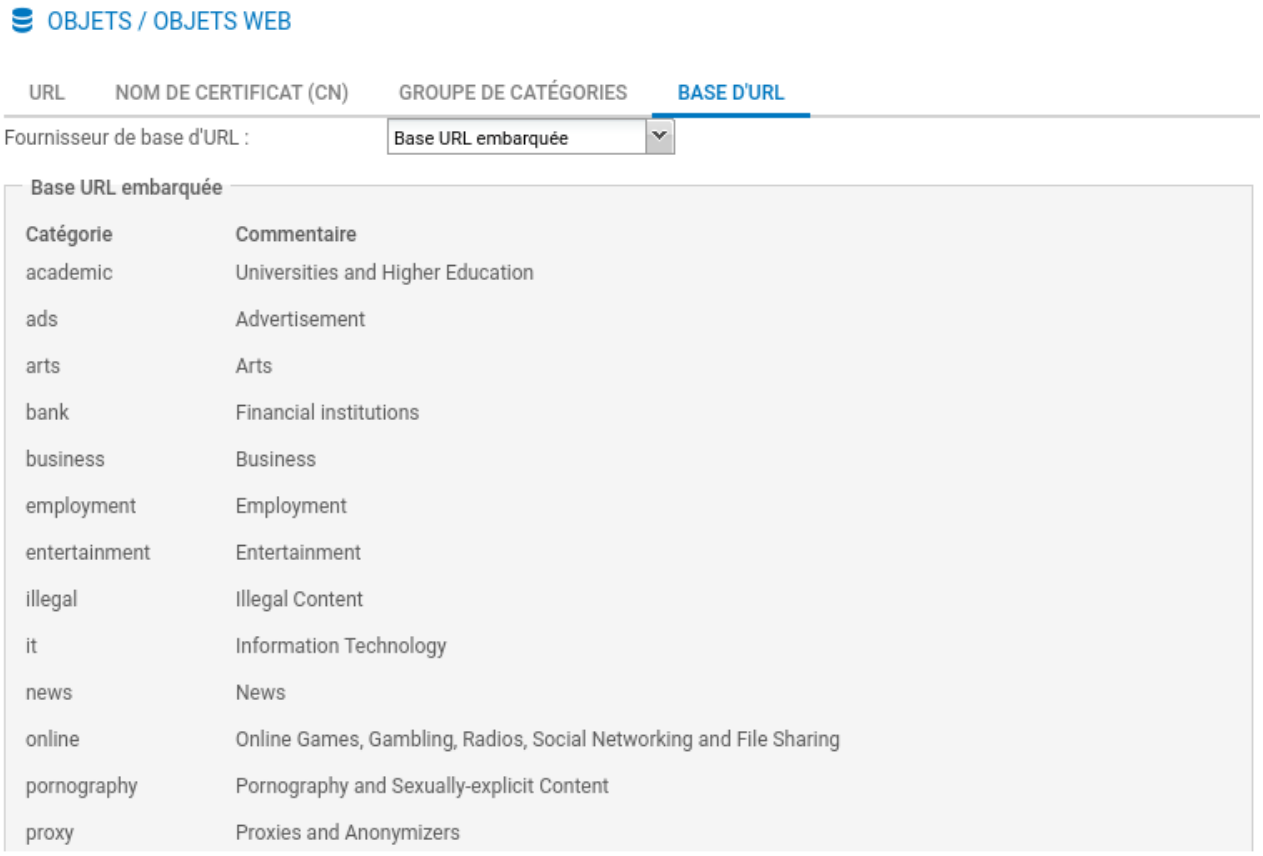
6.2 - Présentation des bases de catégories d'URL

La fonction de filtrage des URL permet de contrôler l'accès aux sites web d'Internet pour l'ensemble des utilisateurs. Pour contrôler ces accès, la politique de filtrage URL va se baser sur une liste d'URL classées en catégories ou de mots clés personnalisés.
Deux fournisseurs de base URL sont disponibles sur les pare-feu SNS :

1. Base URL embarquée composée de 16 catégories téléchargées sur les serveurs de mise à jour,
2. Base Extended Web Control (EWC) constituée de 65 catégories, toutes hébergées dans le Cloud.

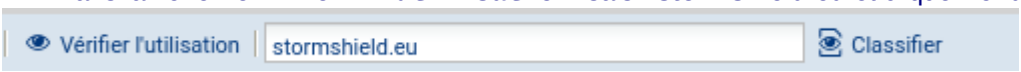
NB : La base étendue EWC est disponible en option payante, elle est néanmoins incluse dans les VM du partenariat Stormshield Academy.

- Ouvrez **Configuration** / **Objets** / **Objets Web** onglet **Base d'URL**. La base par défaut est la Base URL embarquée.

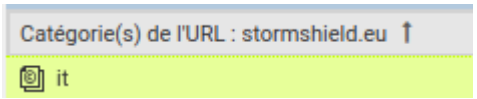


Les catégories prédéfinies pour la **Base URL embarquée** sont disponibles. Le contenu des catégories ne peut pas être consulté, cependant, l'appartenance d'une URL à un groupe peut être vérifiée par le biais des champs de classification. Ces champs sont disponibles depuis le menu Objets Web ou au sein d'une politique de filtrage URL. Nous allons vérifier l'appartenance de Stormshield à une des catégories de la base.

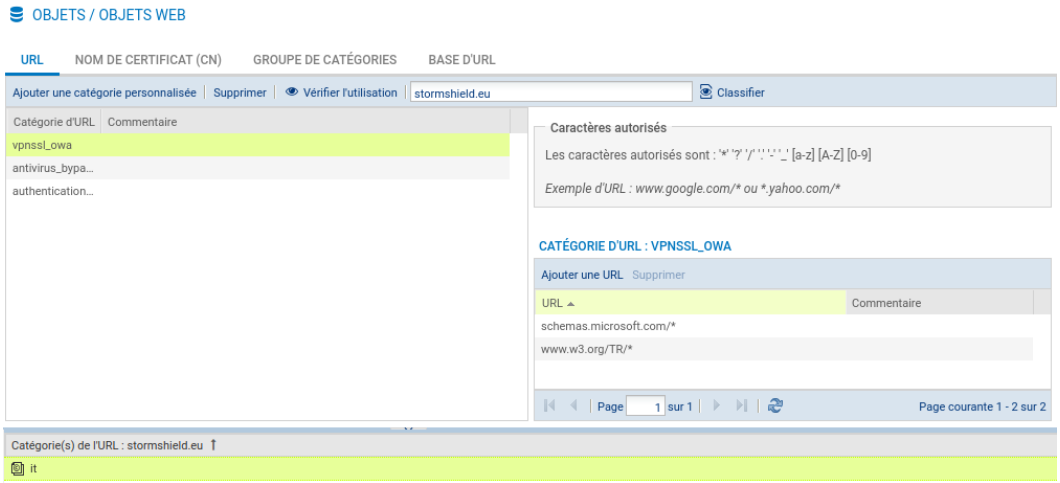
- Ouvrez **Configuration** / **Objets** / **Objets Web** onglet **URL**.
- Dans la zone **Vérifier l'utilisation** saisir **stormshield.eu** et cliquer **Classifier**.



Le résultat s'affiche dans la zone de commentaires, l'URL **stormshield.eu** fait partie de la catégorie **IT** :



- Au besoin cliquer le symbole au bas de l'écran pour déplier la zone de commentaires.



Si les catégories de sites web prédéfinies par votre base d'URL ne sont pas exactement adaptées à vos besoins, vous pouvez créer vos propres catégories pour y mettre les URL que vous souhaitez bloquer ou autoriser. Nous vous recommandons ainsi de prévoir une catégorie white_list et une catégorie black_list.

Étape 1 : Nous allons créer une catégorie personnalisée black_list pour y mettre les URL à blacklister.

- Dans l'onglet **URL**, cliquer **Ajouter une catégorie personnalisée** puis donnez-lui le nom **black_list**.
- Dans la zone **Catégorie d'URL** cliquer **Ajouter une URL** saisir *.**badssl.com/***

Le site *badssl.com* permet d'effectuer de nombreux tests de configuration des navigateurs Internet. En particulier l'url *http.badssl.com* permet de tester l'affichage d'une page web en htpp.
Afin de bien comprendre les éléments nécessaires à ces analyses applicatives, nous créerons les règles de filtrage & NAT minimales pour tester les règles de filtrage d'URL.

Étape 2 : Nous allons créer une nouvelle politique de filtrage basée sur (09) NAT Internet_Pass all et la renommer « Lab6_URL_NAT ».

Nous allons créer une règle pour autoriser toutes les requêtes de résolution DNS, et une autre pour autoriser les requêtes http et https. Nous supprimerons ensuite la règle **Pass all** de cette politique.

- Ouvrez **Configuration / Politique de sécurité / Filtrage et NAT.**
- Copiez la politique de filtrage/NAT **(09) NAT Internet_Pass all** vers la politique **(06)** et la renommer « **Lab6_URL_NAT**». Cliquez **Appliquer** pour activer la politique (**06**).
- Dans l'onglet Filtrage, cliquez Nouvelle règle / règle simple
  - Action : Passer
  - Source : Network_internals
  - Destination : Any
  - Protocole dest : Port destination, ici dns_udp.
- Cliquez Nouvelle règle / règle simple
  - Action : Passer
  - Source : Network_internals
  - Destination : Internet
  - Protocole dest : Port destination, ici http.
- Sélectionnez la règle précédente qui autorise l'accès à Internet avec le protocole http. Cliquez **Copier** puis **Coller** pour la dupliquer, modifiez **Port destination**, par **https**.
- Sélectionnez la règle **Pass all** puis cliquer sur **x Supprimer**. La règle implicite Block_all est réactivée.

Les règles suivantes doivent être créées :

	État	Action	Source	Destination	Port dest.
1	on	passer	network_internals	Any	dns_udp
2	on	passer	Network_internals	Internet	http
3	on	passer	Network_internals	Internet	https

À ce stade vous pouvez tester que vous pouvez accéder à n'importe quel site web depuis votre poste client configuré selon le plan d'adressage de l'agence **A** : Adresse IP : 192.168.**1**.100/24,Passerelle par défaut : 192.168.**1**.254, Serveurs DNS : 172.16.**1**.10.

Ouvrez la page web **http.badssl.com** depuis le navigateur de votre poste client, elle doit s'afficher correctement.

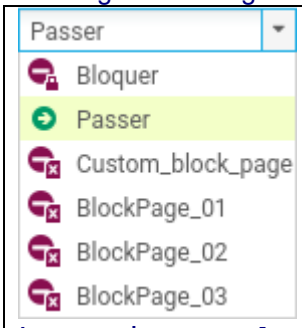
6.3 - Présentation des politiques de filtrage d'URL

Vous allez dans un premier temps découvrir à travers les règles déjà définies dans les politiques prédéfinies de filtrage, le fonctionnement des règles de filtrage sur un pare-feu Stormshield.

Ouvrez le menu **Configuration / Politique de sécurité / Filtrage URL**

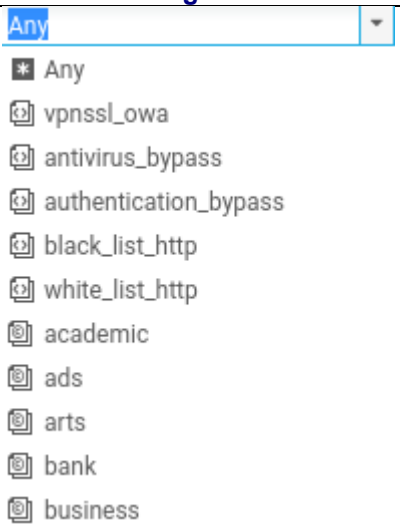
Dans la liste déroulante des politiques de sécurité, choisissez **(0) URLFilter_00.**

La règle numéro 1 (non activée) autorise les URL qui font partie du groupe **authentication_bypass** qui peut être consulté dans le menu **Objets Web**, il s'agit des sites qui permettent les mises à jour Microsoft.
La règle numéro 2 laisse explicitement passer tous les flux.
Les règles de filtrage d'URL sont composées d'une colonne **Action** et d'une colonne **Catégorie d'URL**.



La colonne **Action permet de Bloquer ou de Passer ou** de rediriger vers l'une des 4 pages de blocage personnalisables.

La colonne **Catégorie d'URL** contient la liste des catégories prédéfinies de la base **URL embarquée** et les catégories personnalisées que vous avez créées.



Il convient ensuite de choisir les catégories de sites à autoriser, bloquer ou à rediriger vers l'une des 4 pages de blocage personnalisables. Le contrôle de cohérence en temps réel affiche les erreurs détectées dans votre politique.

Étape 3 : Nous allons créer une règle de blocage pour la catégorie personnalisée black_list.

Dans la liste déroulante des politiques de sécurité, choisissez **(0) URLFilter_00**, cliquez **Éditer** puis **Renommer** « **LAB6_URL** » puis **Mettre à jour**.

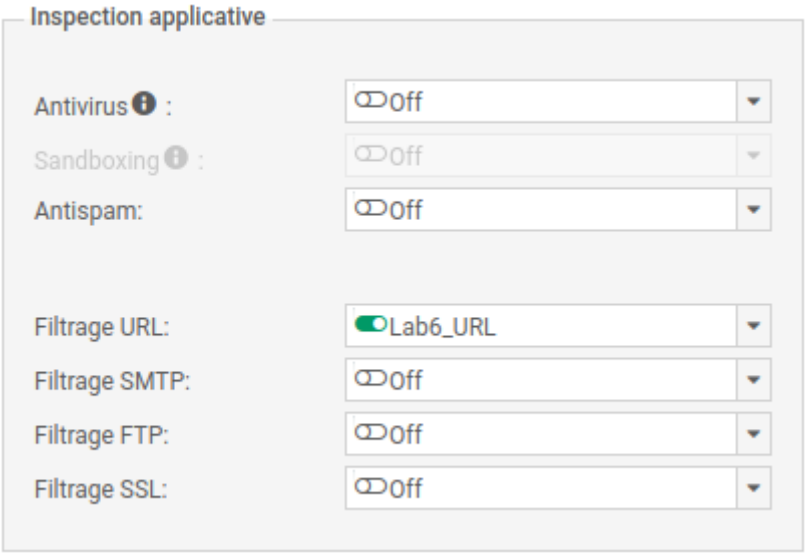
Positionnez-vous sur la règle 1 (désactivée) et cliquez **+ Ajouter** pour ajouter une nouvelle règle de filtrage d'URL.

	État	Action	Catégorie d'URL	Commentaire
1	off	Passer	authenticati...	authorize the URLs of authentication_bypass group
2	on	BlockPage_00	Any	
3	on	Passer	any	default rule (pass all)

- Dans la règle 2, dans **Action**, laissez **BlockPage_00**, dans la colonne **Catégorie d'URL**, choisissez **black_list,** cliquez **Appliquer** puis **Sauvegarder**.

Les pages de blocage par défaut, ici **BlockPage_00** peuvent être éditées depuis le menu **Configuration ⇒ Notifications ⇒ Messages de blocage ⇒** Onglet **Page de blocage HTTP**. Les modifications peuvent s'effectuer grâce à l'éditeur HTML, cela permet de personnaliser la page.

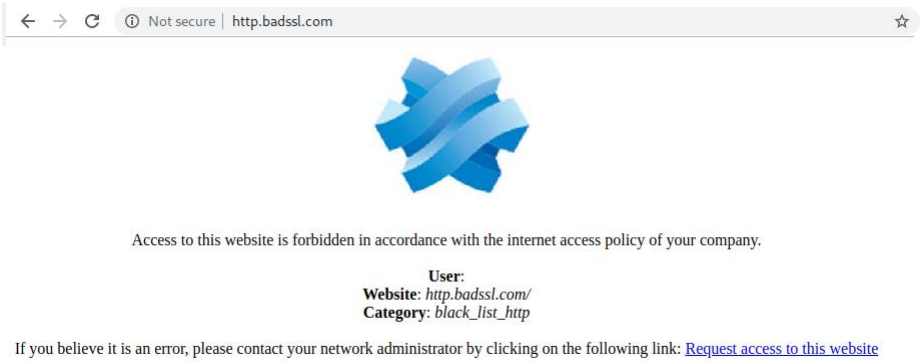
- Ouvrez **Configuration / Politique de sécurité / Filtrage et NAT**, au besoin choisir la politique **(06) Lab6_URL_NAT**.
- Dans l'onglet **Filtrage**, ouvrez la règle 2 qui autorise l'accès à Internet avec le protocole **http**. Dans l'onglet **Inspection de sécurité**, dans la zone **Inspection applicative** choisir **LAB6_URL** dans la liste **Filtrage URL**.



Vous devez obtenir la règle suivante :

			État	Action	Source	Destination	Port dest.	Protocole	Inspection de sécurité
1			on	passer	network_internals	Any	dns_udp		IPS
2			on	passer	Network_in	Internet	http		IPS Filtrage URL : Lab6_URL

- Ouvrez la page web **http.badssl.com** depuis votre navigateur, elle ne doit pas s'afficher correctement. Vous devez voir le message de blocage ci-dessous :



La règle de filtrage a été utilisée et la barre de comptage est passée en bleu pour indiquer que du filtrage applicatif a été appliqué.

1		on	passer	network_internals	Any	dns_udp	IPS
2		on	passer	Network_in	Internet	http	IPS Filtrage URL : LAB_6
3		on	passer	Network_internals	Internet	https	IPS

Ouvrez la page web **https://badssl.com/** depuis votre navigateur, elle s'affiche correctement car l'url est en https et n'est donc pas déchiffrée par la règle précédente.

La majorité des url d'Internet étant en **https**, il faudra d'abord déchiffrer le flux pour pouvoir décider du blocage ou non, ce qui nécessite l'utilisation d'un proxy SSL.

6.4 - Mise en place du Proxy SSL pour le filtrage des services sécurisés

De nombreux services réseau tels que le web, la messagerie, la messagerie instantanée etc. utilisent le protocole TLS (plus connu sous le nom de son prédécesseur SSL) pour authentifier les correspondants et chiffrer leurs communications.

Les firewalls SNS sont capables de filtrer et déchiffrer les connexions HTTPS, ce qui permet de :

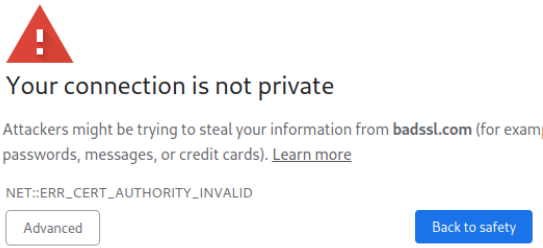
- Bloquer des sites web HTTPS ou des catégories de sites web HTTPS inappropriés,
- Analyser les flux HTTPS pour les fonctions de protection applicative (e.g., anti-virus, sandboxing, filtrage URL, Google SafeSearch, etc.).

Pour activer ces fonctionnalités sur votre pare-feu SNS, vous devez configurer le proxy SSL.

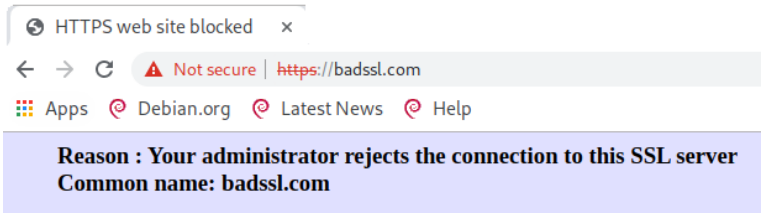
a) Méthodes de filtrage pour HTTPS

Deux méthodes sont envisageables pour filtrer les connexions HTTPS : **avec** ou **sans** déchiffrement des flux SSL. Ces deux méthodes peuvent être combinées en fonction de différents critères, tels que l'authentification ou le réseau IP source. Nous étudierons ici uniquement le **Filtrage SANS déchiffrement des flux SSL.**

Cette méthode permet de bloquer les sites web HTTPS indésirables en vérifiant seulement leur certificat sans déchiffrer le flux. Ainsi, lorsqu'un client initie une connexion vers un site en HTTPS, il envoie en clair au serveur le nom de domaine du site demandé. Ce mécanisme appelé **Server Name Indication** (SNI) permet au serveur de sélectionner le bon certificat à présenter au client. Stormshield Network Security s'appuie sur ce système pour contrôler l'accès à ces sites web sans déchiffrer le flux. Avec ce type de filtrage, les pare-feu SNS sont compatibles avec les extensions SNI (Server Name Indication), permettant de décrire explicitement le nom de l'hôte avec lequel une session TLS est en négociation. Un message de certificat invalide apparaîtra en cas de blocage puis une page de blocage non personnalisable.



Si vous choisissez **Advanced** et **Proceed**, vous aurez accès à la page de blocage du pare-feu SNS :

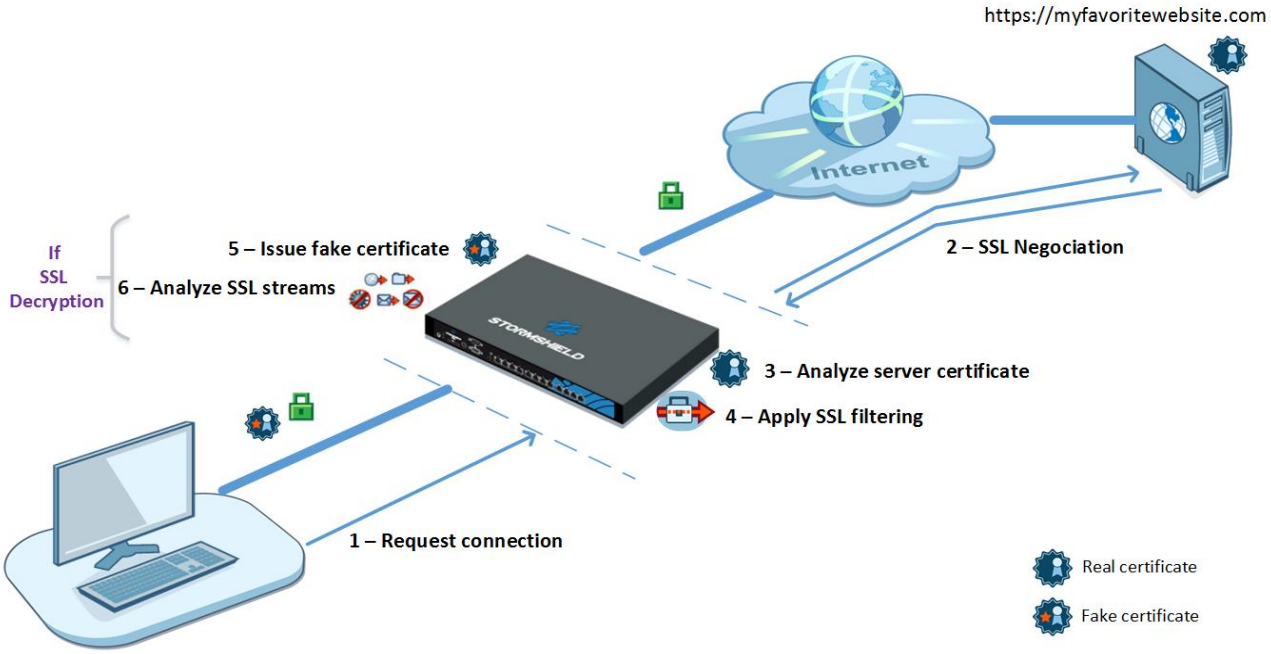


En revanche, cette méthode ne permet pas d'analyser les connexions HTTPS avec les protections applicatives tels que l'anti-virus, le sandboxing, Google SafeSearch, etc.

Le déchiffrement des données personnelles étant encadré par la loi dans la majorité des pays, le filtrage SSL doit prendre en compte cette législation. Vous devez exclure les sites qui ne doivent pas être déchiffrés en leur appliquant l'action **Passer sans déchiffrer** (e.g., en France les sites bancaires). Pour la France, les aspects juridiques liés au déchiffrement SSL sont détaillés en annexe du document *Recommandations de sécurité concernant l'analyse des flux HTTPS* de l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Informations).

b) Fonctionnement du proxy SSL

Le proxy SSL est positionné en « homme du milieu » (Man in the middle) sur le trafic SSL entre le client et le serveur web. Il se charge des négociations SSL et sécurise ainsi les connexions proxy SSL/serveur, et proxy SSL/client. Entre les deux, il autorise ou bloque les connexions selon la politique de filtrage, et si besoin, il déchiffre les flux SSL.



Les différentes étapes du filtrage SSL sont les suivantes :
1. Le proxy SSL intercepte les connexions du client sur le port TCP/443.
2. Il effectue les négociations SSL avec le serveur web au nom du client.
3. Il analyse le certificat envoyé par le serveur. En cas de non-conformité du certificat, l'accès au serveur est bloqué.
4. Si le certificat est conforme, le proxy SSL consulte les règles de filtrage SSL :
   - **Bloquer sans déchiffrer** : il bloque les connexions,
   - **Passer sans déchiffrer** : il laisse passer les connexions,
   - **Déchiffrer** : il déchiffre le flux qui est ensuite évalué par les règles de filtrage suivantes.
5. Si l'action est **Déchiffrer**, le proxy SSL génère un certificat usurpé (fake certificate) et le présente au client qui vérifie le certificat. Si le certificat de l'autorité signataire n'a pas été installé dans le navigateur ou dans le système et déclaré comme autorité de confiance, un message d'erreur s'affiche.
6. Si le certificat est présent, le trafic est sécurisé. Les protections applicatives sont appliquées (e.g., anti-virus, antispam, sandboxing).

NOTE : Les étapes 5 et 6 ont lieu uniquement si vous appliquez la méthode de filtrage AVEC déchiffrement des flux SSL.

c) Configuration du proxy SSL pour le filtrage des site https

Étape 4 : Nous allons créer une catégorie personnalisée black_list_https.

- Ouvrez le menu **`Configuration`** / **`Politique de sécurité`** / **`Filtrage SSL`**
- Dans la liste déroulante des politiques de sécurité, choisissez **`(0) SSLFilter_00`**.

POLITIQUE DE SÉCURITÉ / FILTRAGE SSL

(0) SSLFilter_00 | Editer | Fournisseur de base URL : Base URL embarquée

+ Ajouter | Supprimer | Monter | Descendre | Couper | Copier | Coller | + Ajouter toutes les catégories

	État	Action	URL - CN	Commentaire
1	on	Passer sans déchiffrer	proxyssl_bypass	don't decrypt some specific ssl servers
2	on	Déchiffrer	any	default rule (decrypt all)

Deux règles sont déjà présentes par défaut. La règle numéro 1 spécifie de **Passer sans déchiffrer** les **URL-CN** qui font partie de la catégorie **proxyssl_bypass**. En effet, ces serveurs détectent que le proxy SSL génère un certificat usurpé et sont susceptibles de refuser les connexions (c'est le cas par exemple de mozilla.org). La règle numéro 2 spécifie de déchiffrer tous les autres..

Les règles de filtrage SSL sont composées d'une colonne **Action** et d'une colonne **URL-CN**. Cette dernière correspond au nom que l'on retrouve dans le certificat du serveur concerné.

- Ouvrez **`Configuration`** / **`Objets`** / **`Objets Web`** onglet **`NOM DE CERTIFICAT (CN)`**.

On retrouve la catégorie par défaut **proxyssl_bypass** qui contient une liste de noms de certificats que Stormshield recommande de laisser passer sans déchiffrer.
Pour faciliter l'élaboration de règles de filtrage SSL nous vous recommandons de créer les catégories suivantes pour les sites https :

- Une catégorie de **liste blanche** (white_list_https) contenant toutes les URL que vous estimez fiables. Par exemple les sites que la législation ne vous autorise pas à déchiffrer, vos sites internes, ainsi que les sites de mise à jour des systèmes et des logiciels (e.g., Microsoft, antivirus etc.). Appliquez à cette nouvelle catégorie l'action **Passer sans déchiffrer**.
- Une catégorie de **liste noire** (black_list_https) contenant des URL que vous estimez malveillantes et que vous ne trouvez pas dans les catégories prédéfinies. Appliquez à cette nouvelle catégorie l'action **Bloquer sans déchiffrer**.

- Dans l'onglet **`NOM DE CERTIFICAT (CN)`**, cliquer **Ajouter une catégorie personnalisée** puis donnez-lui le nom **black_list_https**.
- Dans la zone **Catégorie d'URL** cliquer **Ajouter un nom de certificat URL** saisir *.**badssl.com**, puis saisir également **badssl.com**.

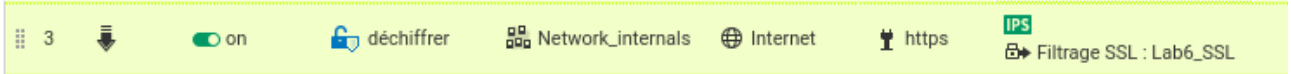
Étape 5 : Nous allons créer une règle de filtrage SSL pour la catégorie personnalisée black_list_https.

- Ouvrez le menu **`Configuration`** / **`Politique de sécurité`** / **`Filtrage SSL`**
- Dans la liste déroulante des politiques de sécurité, choisissez **`(0) SSLFilter_00`**, cliquez **Éditer** puis **Renommer** « **Lab6_SSL** » puis **Mettre à jour**.
- Positionnez-vous sur la règle 1 et cliquez **+ Ajouter** pour ajouter une nouvelle règle de filtrage SSL.
- Dans la règle 2, dans **Action**, choisir **Bloquer sans déchiffrer**, dans la colonne **URL-CN**, choisissez **black_list_https,** cliquez **Appliquer** puis **Sauvegarder**.

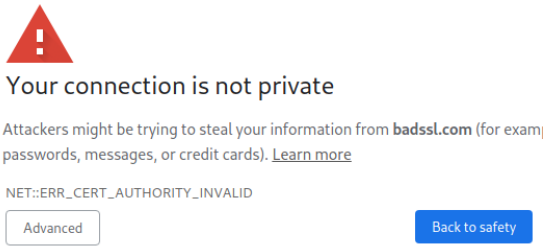
Étape 6 : Nous allons activer dans une règle de filtrage classique le déchiffrement pour le protocole https.

Une fois la politique de filtrage SSL définie, il convient de l'appliquer, ainsi que l'action **Déchiffrer**, à une règle de filtrage autorisant les flux HTTPS sortants, comme le montre l'exemple ci-après.
Cette manière de procéder permet d'activer plusieurs politiques de filtrage SSL simultanément afin de gérer les accès de différents réseaux ou machines sources.

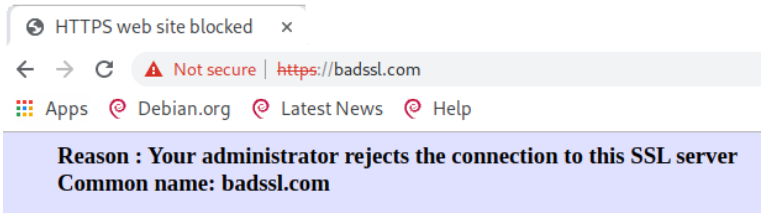
- Ouvrez **Configuration / Politique de sécurité / Filtrage et NAT**, au besoin choisir la politique **(06) Lab6_URL_NAT_Pass all**.
- Dans l'onglet **Filtrage**, ouvrez la règle 3 qui autorise l'accès à Internet avec le protocole **https**. Dans l'onglet **Action** choisir **Déchiffrer**.
- Dans l'onglet **Inspection de sécurité**, dans la zone **Inspection applicative** choisir **LAB6_SSL** dans la liste **Filtrage SSL**.
  Vous devez obtenir la règle suivante :



- Videz le cache de votre navigateur, afin de purger le cache des sites des essais précédents.
- Ouvrez la page web **https://badssl.com/** depuis votre navigateur, un message de certificat invalide apparaît.



- Si vous choisissez **Advanced** et **Proceed**, vous aurez accès à la page de blocage du pare-feu SNS :



Le filtrage SSL a donc bien correctement fonctionné.

6.5 - Mise en place des règles de filtrage d'URL

Étape 1 : Mettre en place une première série de règles de filtrage standard pour les sites web.

Trafics sortants :

1. Votre réseau interne, doit pouvoir naviguer sur les sites web d'Internet en HTTP et HTTPS (cf lab 5), sauf sur les sites de la République de Corée (tester avec www.visitkorea.or.kr).
2. L'accès au site https://www.cnn.com doit être bloqué depuis le réseau interne. Pour cela vous créerez et utiliserez un objet FQDN.

- Ouvrez **Configuration / Politique de sécurité / Filtrage et NAT**, au besoin choisir la politique **(06) Lab6_URL_NAT_Pass all**.
- Ajouter les deux règles ci-dessous, juste après la règle 1 qui autorise la résolution DNS.

		Status	Action	Source	Destination	Dest. port	Protocol	Security inspection
1		on	pass	network_internals	Any	dns_udp		IPS
2		on	block	Network_in	Internet geo Republic of Ko	http https		IPS
3		on	block	Network_in	www.cnn.com	http https		IPS

  - Tester ces nouvelles règles, vérifier que vous obtenez bien le comportement attendu.

Étape 2 : Mettre en place le filtrage d'url selon un cahier des charges.

3. Trouvez les catégories dans lesquelles sont classées les URL www.netbsd.org, neverssl.com, twitter.com, allocine.fr.
4. Configurez une politique de filtrage URL, permettant l'accès à tous les sites Web sauf les sites http listés au point précédent.
5. Configurez une politique de filtrage SSL, permettant l'accès à tous les sites Web sauf les sites listés au point 3 et les sites des catégories « shopping » et « news ». Cependant, assurez-vous que le site bbc.com reste joignable.
6. Tentez d'accéder au site cnn.com et ensuite à euronews.com. Pourquoi la page de rejet du trafic SSL ne s'affiche pas pour cnn.com ?

À faire : rédiger un rapport répondant aux questions ci-dessus.

Fiche pratique n°7 : Mise en place d'un VPN SSL pour les clients nomades

Dans cette activité, vous allez reprendre l'architecture virtuelle présentée dans la fiche N°1 et mettre en place un VPN SSL pour les clients nomades.

Phase 7 Création d'un accès VPN SSL/TLS pour les clients nomades

Chaque utilisateur souhaitant utiliser le VPN SSL du firewall SNS doit disposer d'un compte d'annuaire : soit Active Directory, soit interne au firewall.
Une fois le service d'annuaire correctement configuré, les utilisateurs concernés pourront récupérer après authentification le fichier de configuration du client nomade sur le portail captif du pare-feu activé temporairement sur l'interface externe. Le client VPN SSL utilisé peut être celui fourni par Stormshield ou par OpenVPN.

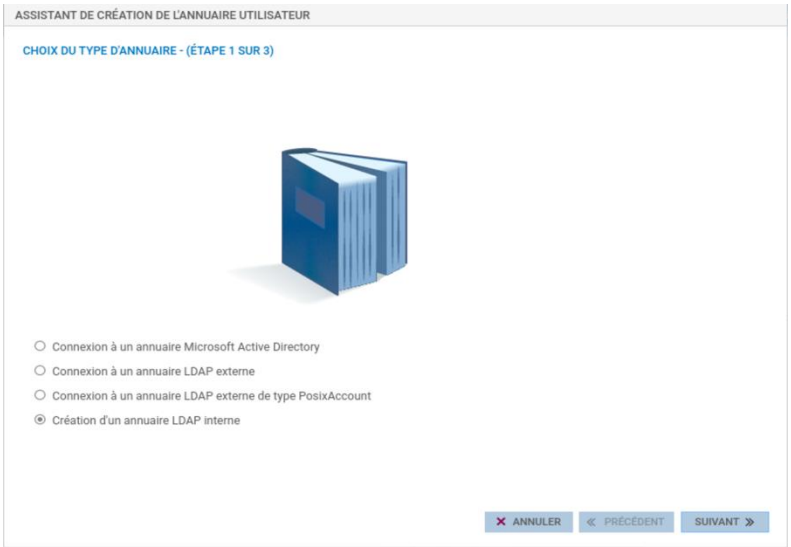
7.1 – Mise en place de l'activité

- Le cas échéant, effectuer la mise à jour vers le firmware 4.2.5 minimum pour pouvoir restaurer les configurations fournies dans le client linux graphique Stormshield.
- Restaurer la configuration du LAB 5 de l'agence A (fichier 5A_LAB5_FILTER_V4.5.2.na)
  NB : les fichiers de configuration sont dans le dossier **Documents**, archive **TRAINEE_A_CSNA_NA_FILES.zip** de la machine virtuelle cliente Linux (Graphical_client1) et disponibles sur le site du réseau certa (https://www.reseaucerta.org/partenaires/stormshield/stormshield-ressources).
  Rappel : La restauration d'une configuration se fait dans le menu **`Configuration / Système / Maintenance /`** onglet **`Restaurer.`** Sélectionnez le fichier à restaurer en cliquant sur le bouton **...**
- Ouvrez le menu **`Configuration`** / **`Politique de sécurité`** / **`Filtrage et NAT`** / **`Filtrage`**
- Dans la liste déroulante des politiques de sécurité, activer la politique **10 Pass all** pour mettre en place les règles de VPN.

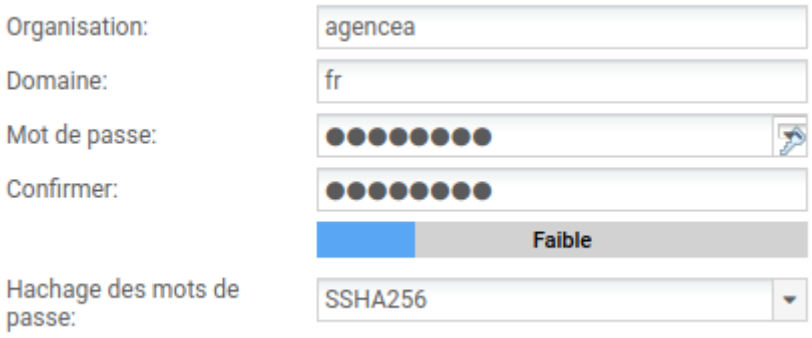
7.2 - Configuration de l'annuaire interne

La configuration de l'annuaire interne s'effectue à partir du menu **`Configuration / Utilisateurs.`**

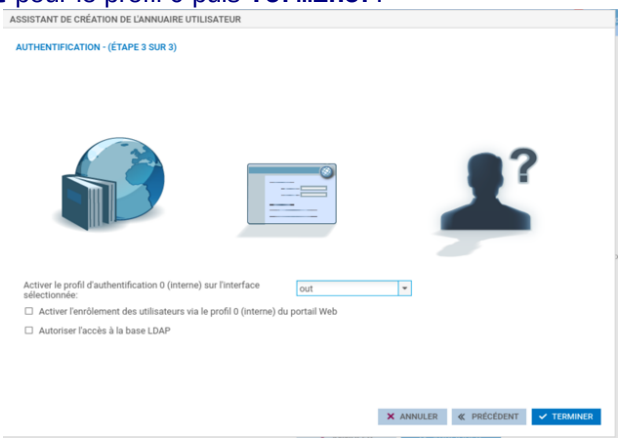
- **`Configuration => Utilisateurs => configuration des annuaires`** puis **`Création d'un annuaire LDAP interne`** et **`Suivant`**.



- Renseignez les champs demandés comme ci-dessous, avec pour mot de passe « password », puis **`Suivant`**.



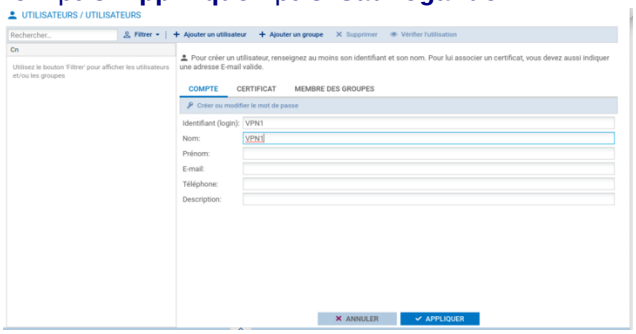
- Choisissez l'interface **`out`** pour le profil 0 puis **`Terminer`**.



Un résumé de la configuration de l'annuaire s'affiche :

Une fois l'annuaire créé, nous allons créer un **groupe VPN** qui contiendra les utilisateurs qui auront le droit de se connecter au VPN.
Nous allons d'abord créer un **utilisateur VPN1** qui sera l'utilisateur qui aura accès à notre VPN (en cas de besoin vous pouvez bien sûr créer autant d'utilisateurs que nécessaire).

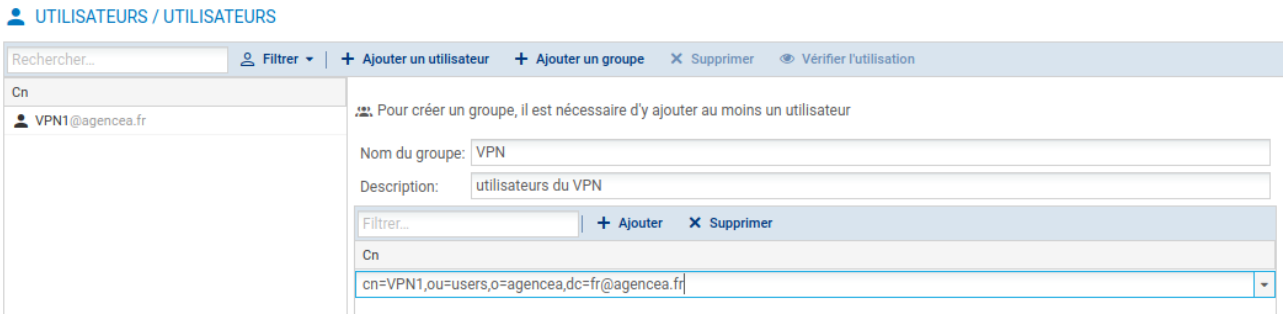
- **`Configuration => Utilisateurs => utilisateurs => ajouter un utilisateur,`** saisir **`VPN1`** comme identifiant et nom puis **`Appliquer`** puis **`Sauvegarder.`**



- Une fois validé, entrez le mot de passe « password » et le confirmer puis **`OK`**.

Vous devez maintenant créer un groupe pour les utilisateurs du VPN, VPN et y intégrer l'utilisateur VPN1.

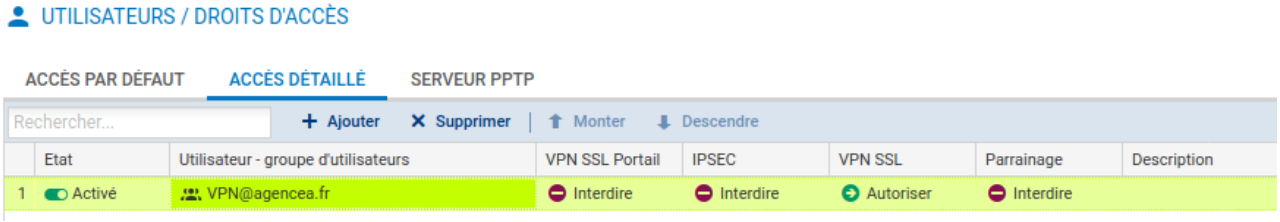
- **`Configuration => Utilisateurs => utilisateurs => ajouter un groupe,`** saisir **`VPN`** comme identifiant.



- Cliquer **+Ajouter** pour rajouter l'utilisateur VPN1 en recherchant son nom dans la zone Cn (sinon vous aurez un message d'erreur lors de la création du groupe) puis **`Appliquer`** puis **`Sauvegarder`**.

Maintenant vous devez donner les droits d'accès au groupe VPN.

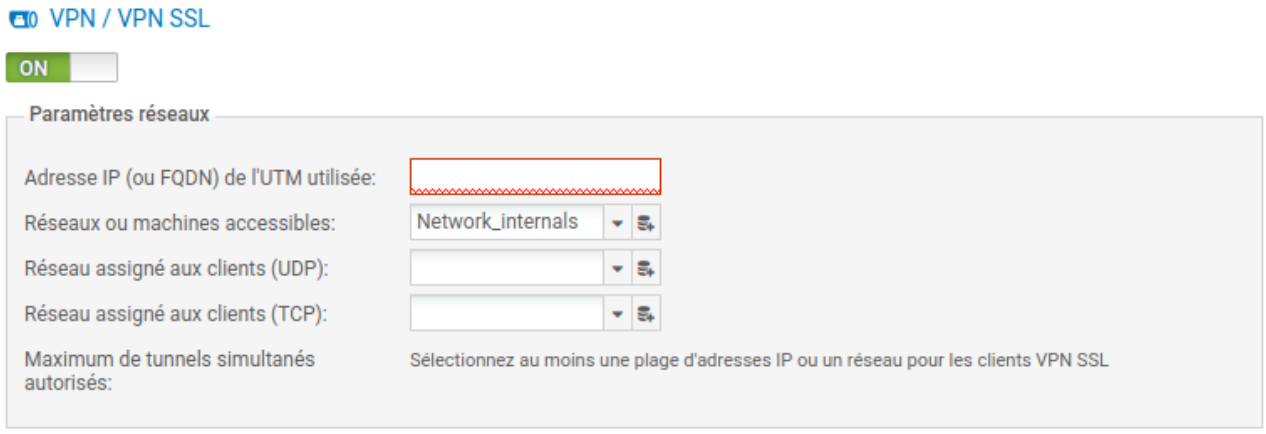
- **`Configuration => Utilisateurs => droits d'accès`**
- Choisir l'onglet **`accès détaillé`**, cliquer **+Ajouter** et rajouter le groupe VPN et choisir **Autoriser** dans la colonne VPN SSL pour donner l'accès au VPN SSL et double-cliquer sur **État** pour activer la règle puis **`Appliquer`** puis **`Sauvegarder`**.



7.3 – Configuration du VPN SSL

Vous allez maintenant configurer le VPN SSL.

- **`Configuration => VPN => VPN SSL`** puis **`ON`** pour le configurer.



Vous allez créer 2 objets réseaux qui vont servir pour les clients VPN en UDP ou TCP.

- Pour UDP : **Net-SSLVPN_UDP** 172.30.1.0/24
- Pour TCP : **Net-SSLVPN_TCP** 172.31.1.0/24

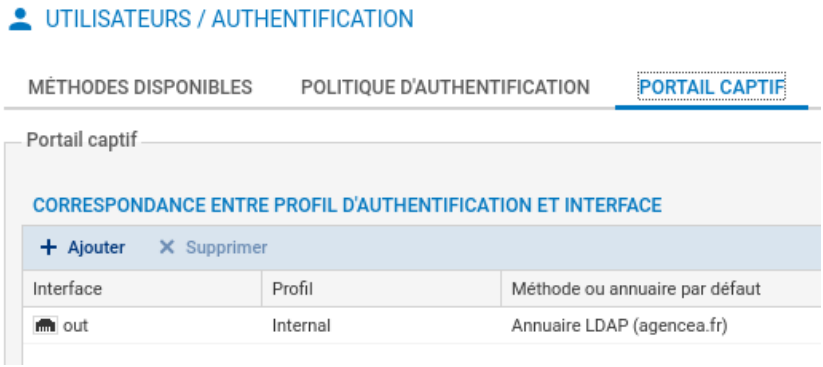
- Renseignez les informations suivantes dans la zone **Paramètres réseaux** :
  - **Adresse IP de l'UTM utilisée** : **192.36.253.10** (l'adresse IP de l'interface out).
  - **Réseaux ou machines accessibles** : Network_internals.
  - **Réseau assigné aux clients (UDP)** : créez l'objet réseau **Net-SSLVPN_UDP** 172.30.1.0/24.
  - **Réseau assigné aux clients (TCP)** : créez l'objet réseau **Net-SSLVPN_TCP** 172.31.1.0/24.
- Renseignez les informations suivantes dans la zone **Paramètres DNS** :
  - **Nom de domaine** : agencea.net.
  - **Serveur DNS primaire** : srv_dns_priv (172.16.1.10).
- Appliquez la configuration, choisir **`Appliquer`** puis **`Sauvegarder`**.

Étape 1 : Activer le portail captif pour permettre la récupération des certificats du client VPN.

Vous allez vérifier l'activation du portail captif pour que l'utilisateur **vpn1** puisse se connecter pour récupérer les certificats ainsi que le client VPN.

💻 **`Configuration => utilisateurs => authentification => portail captif`**

Vérifier que l'interface **out** est bien activée sinon il faut la rajouter.



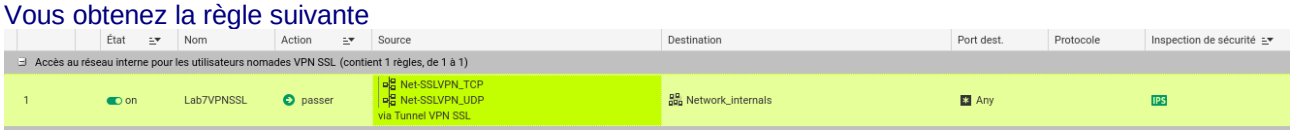
NB : L'activation du portail captif sur l'interface externe est à limiter dans la mesure du possible afin de limiter la surface d'attaque du site. Elle doit être ponctuelle en fonction des besoins. La meilleure solution est, le plus souvent, que le service informatique paramètre le matériel (logiciel client et certificat utilisateur) avant que l'utilisateur ne devienne nomade. Cela évite la possibilité que les certificats soient récupérés par un individu malveillant.

Étape 2 : Copiez la politique de filtrage/NAT **(06) Company_A_Filter_NAT** vers la politique **(07)** et la renommer « **Lab7_VPNSSL** ».

Il convient d'ajouter une règle de filtrage qui autorise l'accès aux réseaux internes pour les réseaux du VPN SSL : Net-SSLVPN_TCP et Net-SSLVPN_UDP.

- 💻 Au début de la liste des règles de l'onglet **Filtrage**, créer un nouveau séparateur : **Accès au réseau interne pour les utilisateurs nomades VPN SSL**
- 💻 Cliquez **Nouvelle règle / règle simple**
  - **Action** : **Passer**
  - **Source** : les 2 réseaux VPN **Net-SSLVPN_TCP** et **Net-SSLVPN_UDP**
  - **Source / Configuration Avancée**, ajouter dans **Via** : **Tunnel VPN SSL**
  - **Destination / Général** : Network_internals
  - **Général** : Etat **On,** Nom : **Lab7VPNSSL**
- 💻 Cliquez **OK** pour valider puis **Appliquer.**

Vous obtenez la règle suivante



7.4 – Configuration du client VPN nomade

Vous devez configurer une machine virtuelle ou votre hôte physique pour qu'il puisse se connecter au portail captif du pare-feu de l'agence A (https://192.36.253.10) et simuler l'accès VPN nomade. Plusieurs possibilité s'offrent à vous :

1. Ajouter une machine virtuelle Windows ou Linux sur le réseau externe (Réseau virtuel :Nat Network), avec une IP dans le réseau 192.36.253.0/24.
2. Utiliser la VM client graphique Stormshield sur le réseau de l'entreprise B avec le firewall de l'entreprise B configuré au moins avec la NAT pour l'accès à Internet.
3. Utiliser la VM client graphique Stormshield sur le réseau externe (Réseau virtuel :Nat Network), avec une IP dans le réseau 192.36.253.0/24 (nécessite une modification du script de configuration, voir annexe).
4. Utiliser votre machine hôte Windows avec une IP dans le réseau 192.36.253.0/24, vous configurerez un réseau privé hôte virtualbox « Virtual Host-only Ethernet Adapter #X » sur le réseau externe et vous mettrez l'interface **out** de votre pare-feu SNS sur ce réseau pour faire les tests.

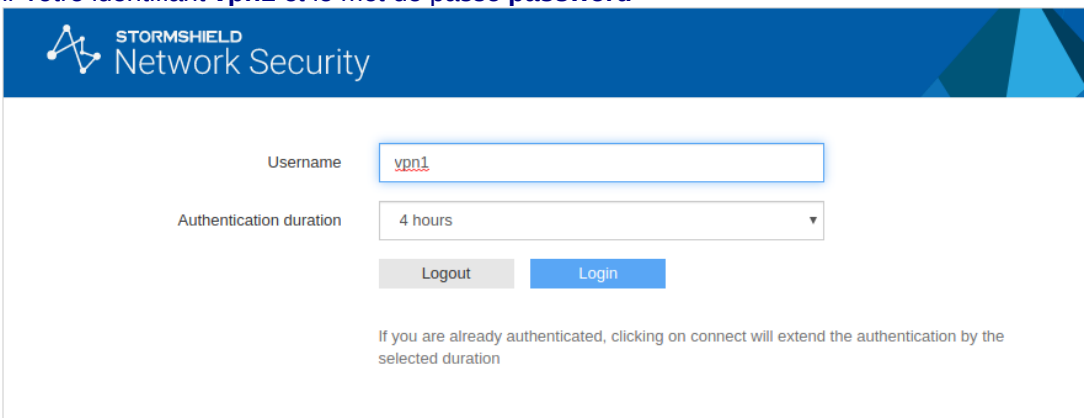
Étape 1 : Récupérer les certificats client OpenVpn pour l'utilisateur vpn1

Vous devez configurer une machine virtuelle ou votre hôte physique pour qu'il puisse se connecter au portail captif du pare-feu de l'agence A (https://192.36.253.10), voir paragraphe 7.4.1 pour la configuration du client Linux.

- 💻 Configurez la machine cliente pour qu'elle appartienne au réseau externe **OUT** 192.36.253.0/24
- 💻 Ouvrez le navigateur de la machine cliente avec **https://192.36.253.10.**

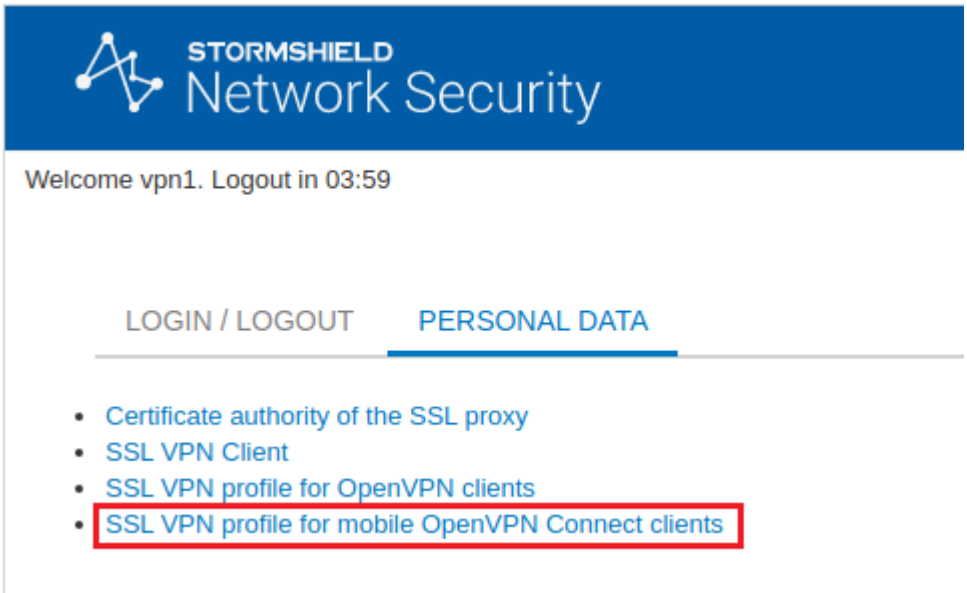
Le portail captif du pare-feu de l'agence A s'ouvre.

- Saisir votre identifiant **vpn1** et le mot de passe **password**



Une seconde page web s'ouvre et vous permet de télécharger les fichiers nécessaires.

- Téléchargez l'archive **SSL VPN profile for mobile OpenVPN Connect clients** qui contient un fichier unique **openvpn_mobile_client.ovpn**.



En fonction de votre choix de machine cliente Linux ou Windows, vous réaliserez les étapes du 7.4.1 ou 7.4.2

7.4.1 – Configuration du client VPN nomade sur le client graphique Linux

Le plus simple est d'utiliser la VM client graphique Stormshield pour avoir à termes votre client nomade sur le réseau interne de l'agence B avec le pare-feu de l'agence B configuré avec le NAT pour l'accès à Internet.

Dans un premier temps, vous allez utiliser le client graphique sur le réseau externe OUT, afin de pouvoir télécharger les fichiers du portail captif.

- Ajouter dans le fichier **network_config.sh** le paragraphe si dessous à la fin après le paragraphe sns et juste avant l'instruction **esac**

```
out)
  IPPREFIX=192.36
  IPMASQ=24
  X=253 ;;
```

- Exécuter ensuite le script **network_config.sh** modifié et tapez **Y** puis **out** pour vous placer sur le réseau externe, vérifiez avec **ip addr** que vous obtenez bien une adresse en 192.36.253.2.

Étape 2 : Configurer le client OpenVpn sur la machine virtuelle Linux

- Ouvrez le navigateur de la machine cliente avec **https://192.36.253.10** et téléchargez le certificat SSL pour OpenVpn, il sera stocké par défaut dans `/home/user/Downloads`.
- Ouvrir un terminal et effectuer les commandes suivantes

```
su -  (password = toor)
cd /home/user/Downloads
openvpn openvpn_mobile_client.ovpn
```

Vous devez entrer le nom d'utilisateur et le mot de passe pour vous connecter, vous obtenez le résultat ci-après.

```
root@client-training:/home/user/Downloads# openvpn openvpn_mobile_client.ovpn
Enter Auth Username: vpn1
Enter Auth Password: ********
Mon Jan 24 01:41:01 2022 WARNING: No server certificate verification method has
been enabled.  See http://openvpn.net/howto.html#mitm for more info.
```

Vous pouvez vérifier l'adresse obtenue par le VPN, elle doit se trouver dans le réseau VPNSSL configuré sur le firewall : 172.30 ou 172.31.

- Ouvrir un second terminal et taper la commande **ip addr**, une nouvelle interface **tun0** est présente.

```
user@client-training:~$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default
 qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP g
roup default qlen 1000
    link/ether 08:00:27:23:35:92 brd ff:ff:ff:ff:ff:ff
    inet 192.36.253.2/24 scope global enp0s3
       valid_lft forever preferred_lft forever
4: tun0: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast stat
e UNKNOWN group default qlen 100
    link/none
    inet 172.30.1.10 peer 172.30.1.9/32 scope global tun0
       valid_lft forever preferred_lft forever
```

Vous pouvez également vérifier sur votre machine que de nouvelles routes ont été créées et que la connexion est toujours ouverte.

- Ouvrir un second terminal et taper la commande **ip route show**

```
user@client-training:~$ ip route show
default via 192.36.253.254 dev enp0s3
172.16.1.0/24 via 172.30.1.5 dev tun0
172.30.1.0/24 via 172.30.1.5 dev tun0
172.30.1.1 via 172.30.1.5 dev tun0
172.30.1.5 dev tun0 proto kernel scope link src 172.30.1.6
172.31.1.0/24 via 172.30.1.5 dev tun0
172.31.1.1 via 172.30.1.5 dev tun0
192.36.253.0/24 dev enp0s3 proto kernel scope link src 192.36.253.2
192.36.253.1 via 172.30.1.5 dev tun0
192.168.1.0/24 via 172.30.1.5 dev tun0
```

- Vous pouvez tester un ping vers le serveur DNS interne :

```
user@client-training:~$ ping 172.16.1.10
PING 172.16.1.10 (172.16.1.10) 56(84) bytes of data.
64 bytes from 172.16.1.10: icmp_seq=1 ttl=64 time=3.95 ms
64 bytes from 172.16.1.10: icmp_seq=2 ttl=64 time=5.40 ms
```

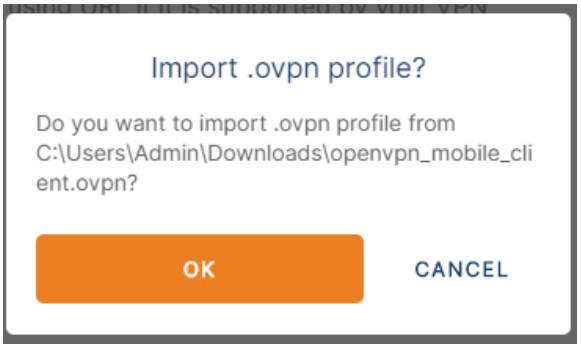
- Vous pouvez effectuer de nouveaux tests en positionnant votre client nomade sur le réseau interne de l'agence B (LAN_IN_B) avec le pare-feu de l'agence B configuré avec le NAT pour l'accès à Internet.

7.4.2 – Configuration du client VPN nomade Windows

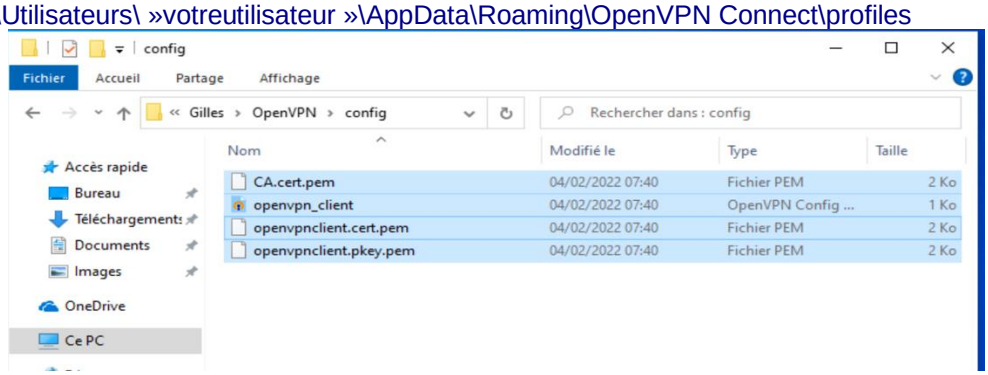
Étape 2bis : Installer le client OpenVpn sur une machine virtuelle Windows

- Sur votre machine cliente, installer OpenVPN (https://openvpn.net/client-connect-vpn-for-windows/). Faire l'installation.

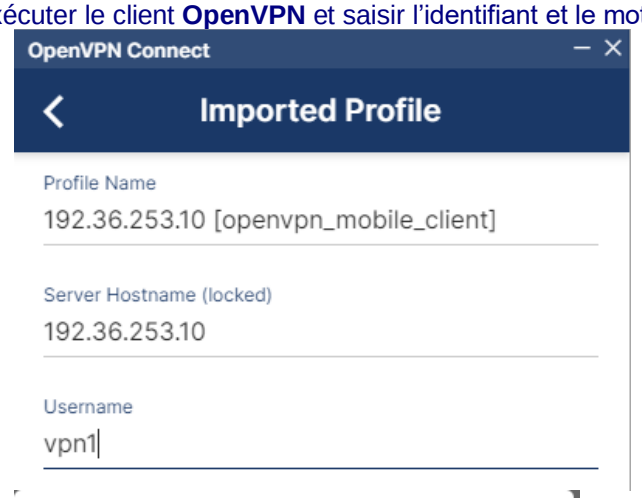
Au démarrage vous allez peut-être avoir un message d'erreur indiquant que vous n'avez pas de fichiers de configuration. Il faut que vous téléchargiez sur le portail captif du Stormshield (voir plus haut) le **Profil VPN SSL pour clients mobiles OpenVPN**. Sinon il va détecter le fichier que vous avez téléchargé :

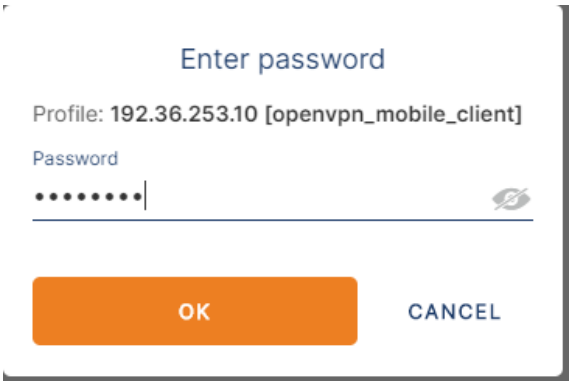


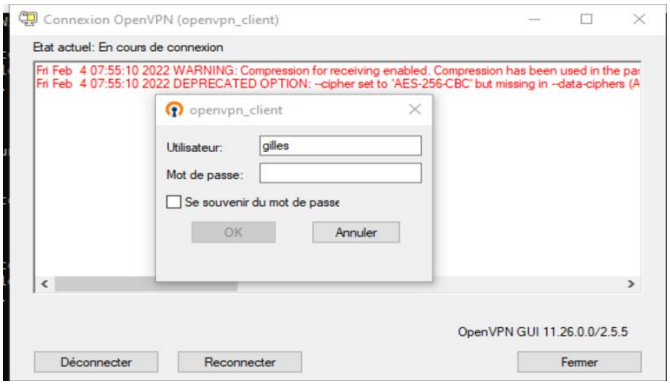
- Au besoin copier le fichier téléchargé **openvpn_mobile_client.ovpn**.dans le répertoire suivant : « c:\Utilisateurs\ »votreutilisateur »\AppData\Roaming\OpenVPN Connect\profiles



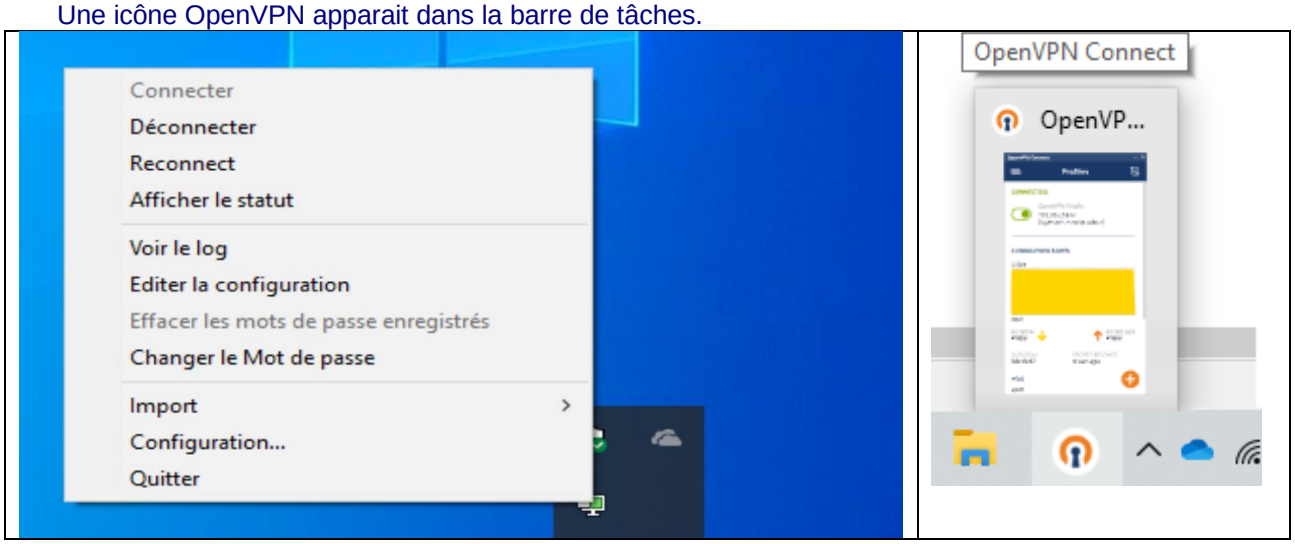
- Exécuter le client **OpenVPN** et saisir l'identifiant et le mot de passe de l'utilisateur précédemment créé.







Valider avec **OK** et vous êtes connecté au serveur VPN.
Une icône OpenVPN apparait dans la barre de tâches.



- Vous pouvez vérifier l'adresse qui vous est donnée avec la commande **ipconfig /all** au niveau de la carte réseau OpenVPN **TAP-Windows**.

```
Carte inconnue Connexion au réseau local :

   Suffixe DNS propre à la connexion. . . :
   Description. . . . . . . . . . . . . . : TAP-Windows Adapter V9 for OpenVPN Connect
   Adresse physique . . . . . . . . . . . : 00-FF-77-A5-94-0C
   DHCP activé. . . . . . . . . . . . . . : Non
   Configuration automatique activée. . . : Oui
   Adresse IPv6 de liaison locale. . . . .: fe80::5513:d3fe:1976:f975%73(préféré)
   Adresse IPv4. . . . . . . . . . . . . .: 172.30.1.6(préféré)
   Masque de sous-réseau. . . . . . . . . : 255.255.255.252
```

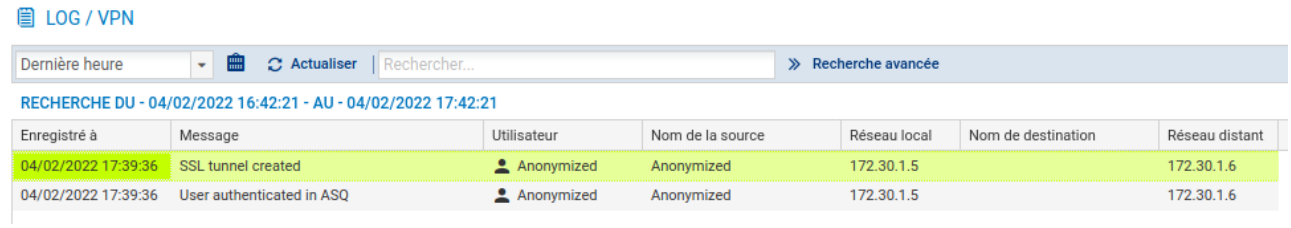
- Effectuer des tests de connectivité à l'aide de la commande ping pour vérifier que vous avez bien accès au réseau de l'agence A : tester l'accès aux différents serveurs de la DMZ et à l'IP interne du firewall sur le réseau LAN.

```
C:\Users\Admin>ping 172.16.1.10

Envoi d'une requête 'Ping'  172.16.1.10 avec 32 octets de données :
Réponse de 172.16.1.10 : octets=32 temps=4 ms TTL=64
Réponse de 172.16.1.10 : octets=32 temps=4 ms TTL=64
```

7.5 – Visualisation dans les logs des connexions VPN

- Vous pouvez vérifier qu'il y a bien l'utilisateur connecté depuis la supervision dans le menu **Monitoring / Logs VPN.**



Remarque : les logs étant par défaut anonymisés, il faut modifier les préférences de l'administrateur et passer en LOGS : ACCES COMPLET pour afficher les utilisateurs connectés dans les menu LOGS/VPN.

- Activer la **politique de Filtrage 7** et vérifiez que vous pouvez toujours accéder aux serveurs de la DMZ, vous pouvez également tester un accès à l'interface d'administration du pare-feu https://192.168.1.254/admin, cela doit fonctionner comme avec la politique **10 Pass_all**.

Fiche pratique n°8 : Mise en place d'un VPN site-à-site IPSec

Dans cette activité, vous allez reprendre l'architecture présentée dans la fiche N°1 et mettre en place un tunnel VPN IPSec site-à-site entre vos deux agences.

Phase 8 - Mise en place du VPN site-à-site IPSec

8.1 - Détails de la technologie VPN site-à-site IPSec

Le tunnel VPN IPSec site-à-site peut s'établir entre le firewall SNS et n'importe quel équipement compatible VPN IPSec. La négociation du tunnel s'effectue avec le protocole ISAKMP (Internet Security Association Key Management Protocol), appelé également IKE (Internet Key Exchange), qui existe actuellement en deux versions V1 (RFC 2409) et V2 (RFC 7296).
La négociation s'effectue entre les extrémités de tunnel qui correspondent aux adresses IP publiques des équipements (@IP FWA_OUT et @IP FWB_OUT). Le protocole IKE est transmis via le protocole UDP sur le port 500.
Une fois le tunnel établi entre les deux équipements, les extrémités de trafic correspondantes aux réseaux privés peuvent communiquer via le protocole ESP (Encapsulating Security Payload) qui assure la confidentialité et l'intégrité des données. Le protocole ESP (ID=50) est encapsulé directement dans un paquet IP.
Dans le cas où une extrémité de tunnel est située dans un réseau translaté, le port **UDP/4500** sera utilisé pour finaliser la négociation IKE et pour transmettre les paquets ESP.

8.2 - Mise en place de l'activité

- Implanter le prototype sur votre infrastructure virtuelle (voir fiche installation de la plateforme)
- Le cas échéant, effectuer la mise à jour vers le firmware 4.2.5 minimum pour pouvoir restaurer les configurations fournies.

💻 Restaurer la configuration du LAB 5 de l'agence A (fichier 5A_LAB5_FILTER_V4.5.2.na)
NB : les fichiers de configuration sont dans le dossier **Documents**, archive **TRAINEE_A_CSNA_NA_FILES.zip** de la machine virtuelle cliente Linux (Graphical_client1).
Rappel : La restauration d'une configuration se fait dans le menu **`Configuration / Système / Maintenance /`** onglet **`Restaurer.`** Sélectionnez le fichier à restaurer en cliquant sur le bouton **...**

💻 Ouvrez le menu **`Configuration`** / **`Politique de sécurité`** / **`Filtrage et NAT`** / **`Filtrage`**

💻 Dans la liste déroulante des politiques de sécurité, activer la politique **10 Pass all** pour mettre en place les règles de VPN.

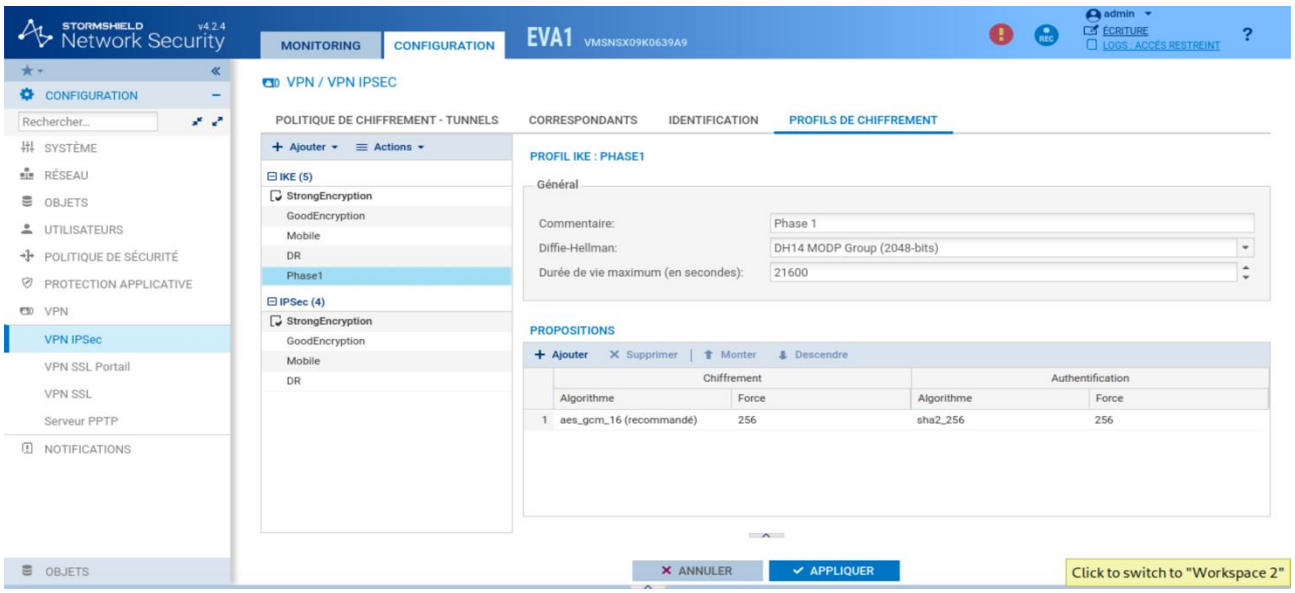
8.3 - Configuration du VPN site-à-site IPSec

Le menu **`Configuration => VPN => VPN IPSEC`** permet de configurer les différents éléments de votre réseau privé virtuel. On utilisera la première politique (1) IPsec 01.

8.3.1. Profils de chiffrement.

Afin de configurer un tunnel VPN IPSEC site-à-site, il faut commencer par créer des profils de chiffrement.

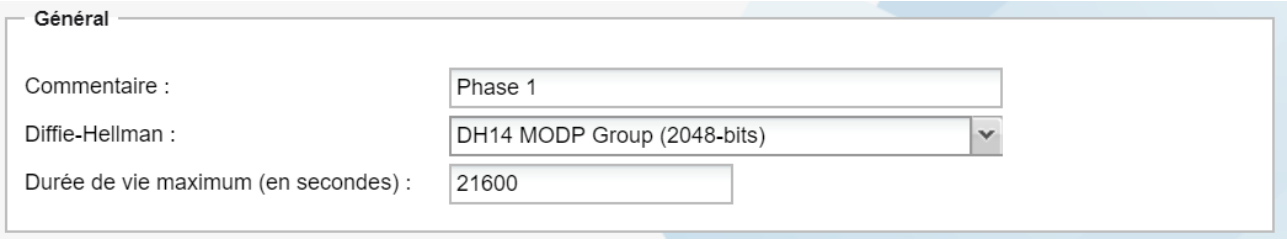
💻 **`Configuration => VPN => VPN IPSEC => Profils de chiffrement`**.



Nous allons créer un nouveau profil de chiffrement pour chaque phase mais il est également possible simplement d'utiliser les deux profils prédéfinis **Strong Encryption**.

Étape 1 : Configurer le profil IKE Phase 1 : Diffie-Hellman (Group 14), Durée de vie maximum (21600 s, algorithme d'authentification (sha 256bits) et algorithme de chiffrement (AES 256bits).

- Cliquer **`Ajouter`** puis **`Profil de phase 1 (IKE)`**
- Dans la zone **`Général`**, dans **`Commentaire`** saisir **`Phase 1`**, dans **`Diffie-Hellman`** saisir **`DH 14 MODP Group (20148-bits)`**



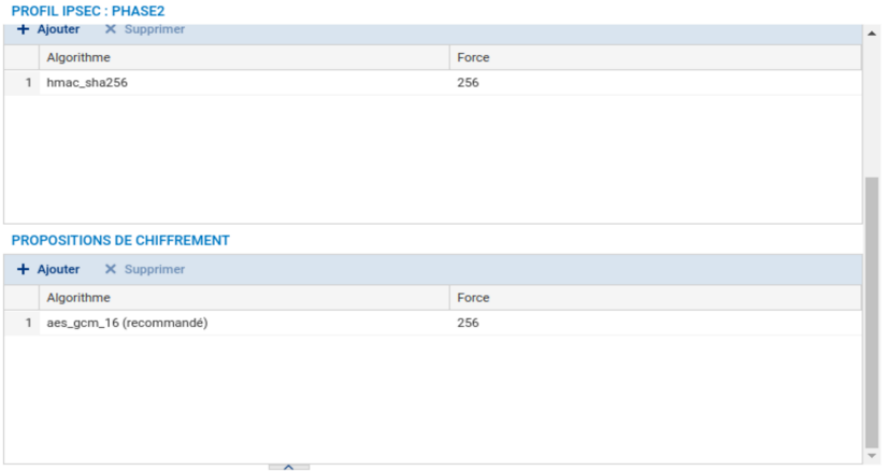
- Dans la zone **`PROPOSITIONS`** choisir dans **`Authentification Algorithme sha2_256`** force 256 bits et dans **`Chiffrement Algorithme AES`** force **`256`** bits

	Authentification		Chiffrement	
	Algorithme	Force	Algorithme	Force
1	sha2_256	256	aes	256

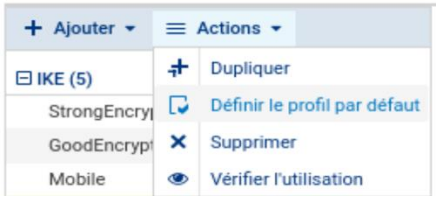
- Cliquer **`Enregistrer`** puis **`Sauvegarder`** puis **`Plus tard`** pour ne pas activer tout de suite les changements.

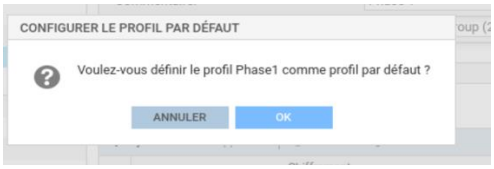
Étape 2 : Configurer le profil IPSEC Phase 2 : PFS (Group 14), durée de vie (3600s), algorithme d'authentification (hmac_sha2 256bits) et algorithme de chiffrement (AES 256bits).

- Dans la zone **`Général`**, dans **`Commentaire`** saisir Phase **`2`**, dans **`Perfect Forward Secrecy (PFS)`** saisir **`DH 14 MODP Group (20148-bits)`**
- Dans la zone **`PROPOSITIONS`** choisir dans **`Authentification Algorithme hmac_sha2256`** force 256 bits et dans **`Chiffrement Algorithme AES_GCM_16`** force **`256`** bits, puis **`Enregistrer`** puis **`Sauvegarder`**.



Sélectionner **Phase 1**, puis aller dans **Actions** et choisir **Définir le protocole par défaut**.





Idem pour **IPsec (phase 2)** puis **`Appliquer`**, **`Sauvegarder`** puis **`Appliquer la politique`**.

8.3.2. Configuration du tunnel IPsec avec clé partagée

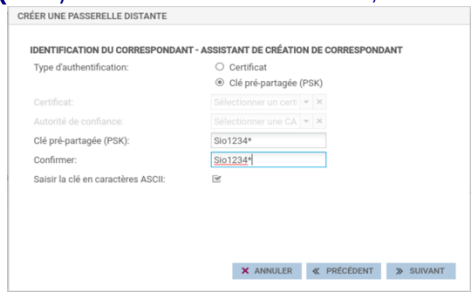
Étape 3 : Configurez un tunnel IPsec avec une authentification par clé partagée (PSK) pour relier votre réseau interne « 192.168.1.0/24 » à celui de l'agence voisine (agence B). Vous utiliserez comme clé PSK : **Sio1234***.

Dans le menu **`Configuration => VPN => VPN IPSEC => politique de chiffrement – tunnels => site à site (gateway-gateway)`**, cliquer **`Ajouter`** => **`Tunnel site à site simple`**

Un assistant de configuration s'affiche :

- Dans **Réseau local** indiquer votre réseau interne (objets prédéfinis **Network_in ou Network_internals** qui comprend également la DMZ).
- Dans **Réseau distant** indiquer le réseau interne de votre correspondant : **LANx**
- Dans la zone **Choix du correspondant** cliquer sur le lien **Créer un correspondant Ikev2**
- Dans **Passerelle distante** indiquer l'adresse IP publique du firewall de votre correspondant : **FW_B**, dans **Nom**, par défaut le nom **Site_FW_B** est créé, puis **Suivant.**

- Choisir **Clé prépartagée (PSK**) entrer une clé : **Sio1234***, la confirmer puis **Suivant**.



- Un résumé s'affiche, cliquer **Terminer**.

- Vérifier que les trois paramètres (**Réseau local**, **correspondant** et **Réseau distant**) sont bien renseignés puis cliquer **Terminer** pour enregistrer la configuration.

Le tunnel VPN IPSec est ajouté sur une nouvelle ligne de la politique par défaut **(1)IPSec 01**.

La configuration n'est pas terminée, il faut utiliser les protocoles de chiffrement précédemment configurés pour les phases 1 et 2.

8.3.3. Ajout des protocoles de chiffrement dans la configuration du VPN IPsec

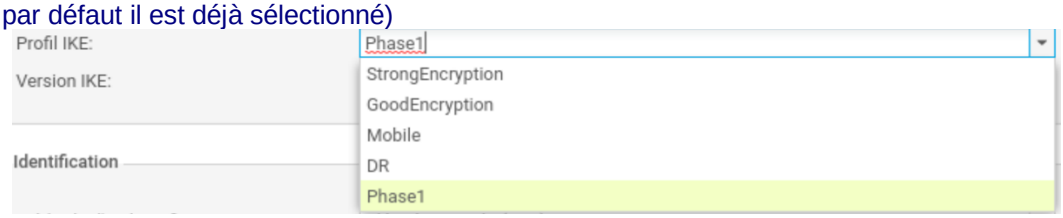
Étape 4 : utiliser les protocoles de chiffrement précédemment configurés pour les phases 1 et 2.

- Dans la zone **`Profil de chiffrement`**, le cas échéant, sélectionnez dans la liste déroulante **Phase 2** (comme nous l'avons configuré dans les profils par défaut il est déjà présent).

  La sélection du profil de chiffrement pour la **phase 1** s'effectue dans l'onglet **`Correspondants`**.

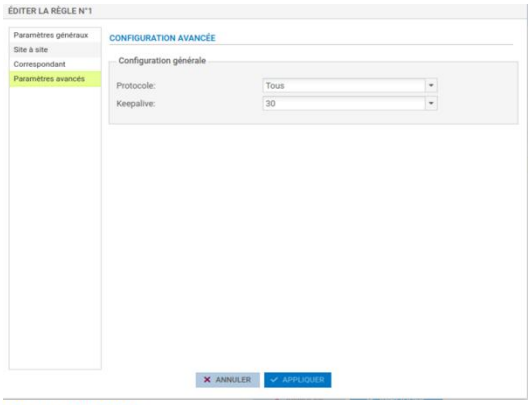
- Cliquer l'onglet **`Correspondants`**, dans le volet de droite les éléments du correspondant s'affichent. Vérifier les paramètres (il faut que le **profil phase1** soit sélectionné et que la clé partagée soit la même).

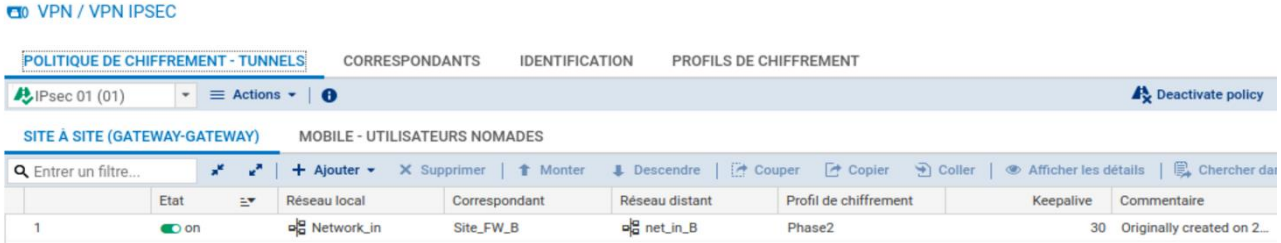
- Dans **`Profil IKE`** choisir, le cas échéant, le profil **Phase 1** (comme nous l'avons configuré dans les profils par défaut il est déjà sélectionné)



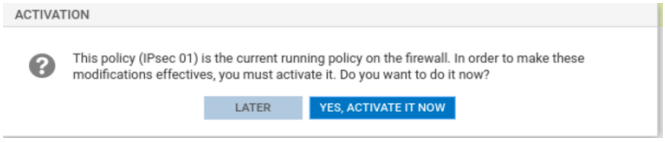
- Cliquer **`Enregistrer`** puis **`Sauvegarder`** puis **`Plus tard`**.

Pour garder le tunnel « en vie » vous pouvez mettre une valeur dans le champ « keepalive ». Ici la valeur est mise à 30 secondes.



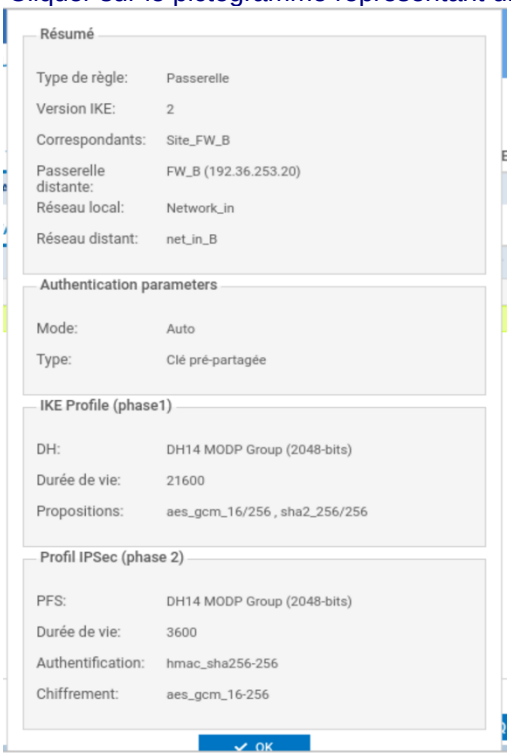


- **Au niveau de la règle `(1) IPsec01`** cliquer **`Activer cette politique`** puis confirmer pour activer le tunnel.



Un résumé détaillé des paramètres de configuration peut être affiché par un simple **clic** sur le pictogramme représentant un **œil** au niveau de l'**Etat on** de la politique **`Site-à-Site`**. Tous les éléments nécessaires sont affichés et vous permettront de vérifier que votre correspondant a bien une configuration identique.

- Cliquer sur le pictogramme représentant un **œil**

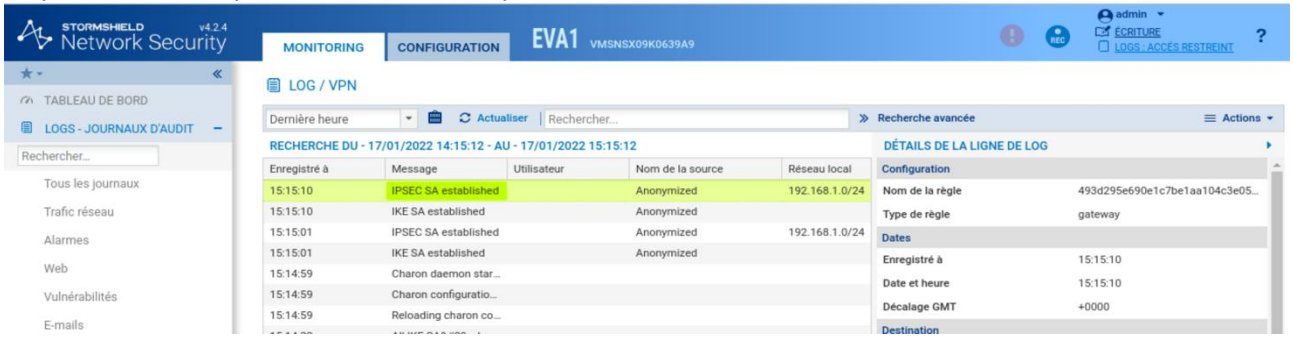


8.3.4. Configuration du VPN IPsec sur le pare-feu de l'agence B et tests

- Procéder de manière identique sur le pare-feu stormshield du site B, vous pouvez à cet effet partir du fichier de configuration de l'agence B (**AgenceB_ConfLabVPN2.na**) fournit dans l'archive **TRAI-NEE_B_CSNA_NA_FILES.zip**.

Pour vérifier que tout fonctionne, vous pouvez aller voir sur les logs :

- **Onglet Monitoring -> VPN** et vous devez obtenir ceci :
  La phase 1 établie (IKE SA established)
  La phase 2 établie (IPSEC SA established)



- Pour vérifier que vous avez bien une connexion VPN établie vous pouvez faire un ping entre vos deux clients graphiques situés respectivement dans les réseaux internes de l'agence A et de l'agence B.
  NB : pour vérifier que c'est bien grâce au tunnel que vous pouvez vous pinguer, désactivez la règle de tunnel, vérifiez que les pings ne fonctionnent pas puis réactivez la règle.

Annexe 1 – Correction Phase 5 Filtrage protocolaire - Étape 3

Étape 3 : Vous allez mettre en place une deuxième série de règles sur les trafics entrants et sortants qui respecteront le cahier des charges ci-dessous (utilisez les séparateurs en indiquant le rôle de chaque règle).

Trafics sortants :

1. Votre réseau interne, à l'exception de vos serveurs en DMZ, doit pouvoir naviguer sur les sites web d'Internet en HTTP et HTTPS, sauf sur les sites de la République de Corée (test avec www.visitkorea.or.kr).
2. L'accès au site https://www.cnn.com doit être bloqué depuis le réseau interne, en utilisant un objet FQDN.
3. Un stagiaire, nouvellement arrivé dans l'entreprise, a l'interdiction d'effectuer la moindre requête FTP. L'adresse IP de sa machine est 192.168.x.200.
4. Votre réseau interne (DMZ incluse) doit pouvoir joindre les serveurs FTP et Web de vos voisins.
5. Votre serveur de messagerie peut envoyer des mails vers les serveurs publiés par vos voisins.

Trafics entrants :

6. Les voisins peuvent joindre vos serveurs Web et FTP ; ces événements doivent être tracés.
7. Les serveurs mails voisins sont autorisés à transmettre des e-mails à votre serveur de messagerie
8. Les voisins sont autorisés à pinger l'interface externe de votre SNS ; cet événement devra lever une alarme mineure.
9. Les réseaux externes sont autorisés à pinger l'interface externe de votre SNS.
10. Les voisins peuvent se connecter à votre SNS : via l'interface web et en SSH. Ces événements devront lever des alarmes majeures.

Voici l'ensemble des règles que vous devez obtenir :

POLITIQUE DE SÉCURITÉ / FILTRAGE ET NAT

(6) Company_A_Filter_NAT | Editer | Exporter

FILTRAGE NAT

Rechercher... | + Nouvelle règle | Supprimer | Couper | Copier | Coller | Chercher dans les logs

	État	Nom	Action	Source	Destination	Port dest.	Protocole	Inspection de sécurité
FW Administration from Admin PC (contient 1 règles, de 1 à 1)								
1	on	Q12_Webadmin_from_PC_...	passer	pc_admin	Firewall_in	https		IPS
Internal traffic IN to DMZ (contient 6 règles, de 2 à 7)								
2	on	Q1_Internal_dns	passer	Network_in	srv_dns_priv	dns		IPS
3	on	Q1_Internal_http	passer	Network_in	srv_web_priv	http		IPS
4	on	Q1_Internal_webmail	passer	Network_in	srv_web_priv	webma		IPS
5	on	Q4_block_noob_ftp	bloquer	pc_200	Any	ftp		IPS
6	on	Q1_internal_ftp	passer	Network_in	srv_ftp_priv	ftp		IPS
7	on	Q1_Internal_smtp	passer	Network_in	srv_mail_priv	smtp		IPS
Outgoing traffic (contient 7 règles, de 8 à 14)								
8	on	Q2_block_korea	bloquer	Network_in	Internet geo Republic of Korea	http https		IPS
9	on	Q3_block_cnn	bloquer	Network_in	www.cnn.com	http https		IPS
10	on	Q2_allow_http	passer	Network_in	Internet	http		IPS
11	on	Q2_allow_https	passer	Network_in	Internet	https		IPS
12	on	Q5_allow_ftp_to_internet	passer	Network_internals	Internet	ftp		IPS
13	on	Q6_allow_ping_to_any	passer	Network_in	Any	Any	icmp (requête Echo (Ping))	IPS
14	on	Q8_allow_smtp_internet	passer	srv_mail_priv	Internet	smtp		IPS
Incoming traffic (contient 5 règles, de 15 à 19)								
15	on	Q9_allow_internet_to_http	passer	Internet	Firewall_out	http		IPS
16	on	Q9_allow_internet_to_ftp	passer	Internet	srv_ftp_pub	ftp		IPS
17	on	Q10_allow_internet_to_smtp	passer	Internet	srv_mail_pub	smtp		IPS
18	on	Q11_allow_internet_to_ping	passer	Internet	Firewall_out	Any	icmp (requête Echo (Ping))	IPS
19	on	Q12_allow_internet_to_ssh	passer	Internet	Firewall_out	https ssh		IPS

Vous trouverez ci-après les détails pour certaines règles

1. Votre réseau interne doit pouvoir joindre les serveurs FTP et Web de vos voisins.

💻 Ajoutez un séparateur nommé **Accès aux serveurs voisins**, choisissez **Nouvelle règle / séparateur – Regroupement de règle** puis éditez-le.

💻 Cliquez **Nouvelle règle /règle simple**

- **Action** : **Passer**

- **Source** : **Network_internals**
- **Destination** : **srv_ftp_pub_X**
- **Port dest** : Port destination, ici **ftp**.

Cliquez sur **Copier** puis **Coller** pour créer la deuxième règle à partir de la précédente :

- **Action** : **Passer**
- **Source** : **Network_internals**
- **Destination** : **srv_web_pub_X**
- **Port dest** : Port destination, ici **http**

3. Au préalable, vous devrez créer un objet de type machine nommé "stagiaire", portant l'adresse IP 192.168.x.200.

10. Pour autoriser, les voisins à se connecter à votre firewall via l'interface web, il faut ajouter leurs adresses IP publiques dans l'encadré **Accès aux pages d'administration du firewall** du menu **`Système => Configuration => onglet Administration du firewall.`**

Annexe 2 – Correction Phase 6 Filtrage applicatif (6.5)

Étape 1 : Mettre en place une première série de règles de filtrage standard pour les sites web.

Trafics sortants :

1. Votre réseau interne, doit pouvoir naviguer sur les sites web d'Internet en HTTP et HTTPS (cf lab 5), sauf sur les sites de la République de Corée (tester avec www.visitkorea.or.kr).
2. L'accès au site https://www.cnn.com doit être bloqué depuis le réseau interne. Pour cela vous créerez et utiliserez un objet FQDN.

💻 Ouvrez **Configuration / Politique de sécurité / Filtrage et NAT**, au besoin choisir la politique **(06) Lab6_URL_NAT_Pass all**.

💻 Ajouter les deux règles ci-dessous, juste après la règle 1 qui autorise la résolution DNS.

		Status	Action	Source	Destination	Dest. port	Protocol	Security inspection
1		on	pass	network_internals	Any	dns_udp		IPS
2		on	block	Network_in	Internet geo Republic of Ko	http https		IPS
3		on	block	Network_in	www.cnn.com	http https		IPS

➢ Tester ces nouvelles règles, vérifier que vous obtenez bien le comportement attendu.

Étape 2 : Mettre en place le filtrage d'url selon un cahier des charges.

3. Trouvez les catégories dans lesquelles sont classées les URL www.netbsd.org, neverssl.com, twitter.com, allocine.fr

Pour déterminer les groupes dans lesquels les URL sont classées, rendez-vous dans le menu Objets WEB puis entrez ces valeurs dans le champ « Vérifier la classification d'une URL ».

💻 Dans **`Configuration`** / **`Objets`** / **`Objets Web`** onglet **`URL`**, dans la zone **`Vérifier l'utilisation`** saisir netbsd.org et cliquer **`Classifier`**.

4. Configurez une politique de filtrage URL, permettant l'accès à tous les sites Web sauf les sites http listés au point précédent.

Le site neverssl.com est en http et netbsd.org en http et en HTTPS. Il faut donc ajouter neverssl.com et netbsd.org dans la liste **blacklist** de l'onglet URL et appliquer la règle 2 déjà mise en place pour http.

💻 Dans **Configuration => Objets => Objets web => onglet URL**, modifiez la catégorie personnalisée de type URL, nommée « blacklist » et ajoutez « *neverssl.com/* » « *netbsd.org /* ».

💻 Ouvrez **Configuration / Politique de sécurité / Filtrage et NAT**, au besoin choisir la politique **(06) Lab6_URL_NAT_Pass all**.

💻 Dans l'onglet **Filtrage**, ouvrez la règle 2 qui autorise l'accès à Internet avec le protocole **http**. Dans l'onglet **Inspection de sécurité**, dans la zone **Inspection applicative** choisir **LAB6_URL** dans la liste **Filtrage URL**.

Vous pouvez tester en tentant d'accéder au site neverssl.com après avoir vidé le cache du navigateur

5. Configurez une politique de filtrage, permettant l'accès à tous les sites Web sauf les sites listés au point 3 et les sites des catégories « shopping » et « news ». Cependant, assurez-vous que le site bbc.com reste joignable.

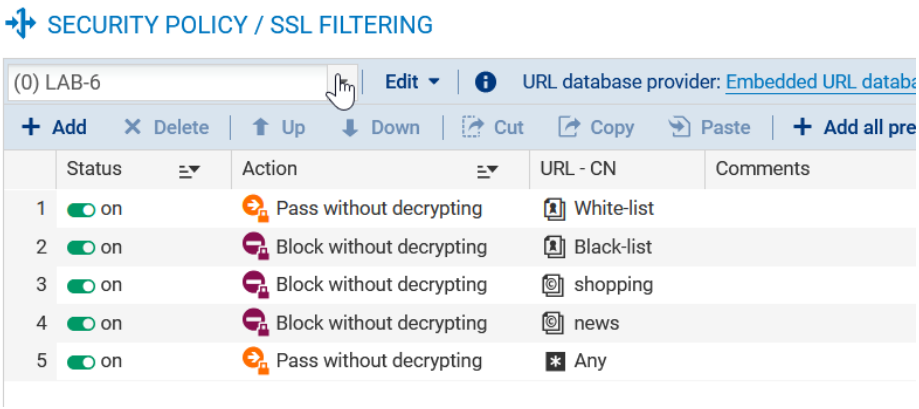
Tous les sites cités sauf neverssl.com sont en HTTPS. En plus de la politique de filtrage SSL à mettre en place pour les gérer, il faut faire une politique de filtrage URL pour bloquer les catégories demandées.

a) Commencer par créer des objets web dans le menu **Configuration => Objets => Objets web** => onglet **Nom de certificat (CN)** , deux catégories personnalisées de CN doivent être créées :

- Une catégorie personnalisée nommée « White_list_https », contenant les CN « *.bbc.com ; *.bbci.co.uk ; *.bbc.co.uk ».
- Une catégorie personnalisée nommée « Black_list_https », contenant les CN « *. netbsd.org ; *.allocine.fr; *.twitter.com ».

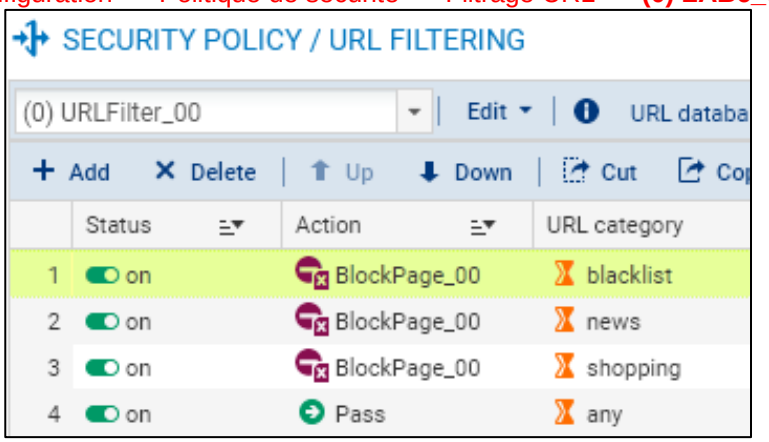
b) Modifier les règles de filtrage SSL

- Ouvrez le menu **`Configuration`** / **`Politique de sécurité`** / **`Filtrage SSL`** choisissez **`(0) Lab6_SSL`**.
- Vous devez ajouter les règles de filtrage SSL suivantes :



c) Pour ce qui concerne le filtrage URL, modifiez le contenu afin que celui-ci comporte la politique suivante :

- Configuration => Politique de sécurité => Filtrage URL => **(0) LAB6_URL**



6. Tentez d'accéder au site cnn.com et ensuite à euronews.com. Pourquoi la page de rejet du trafic SSL ne s'affiche pas pour cnn.com ?

Le site www.cnn.com est déjà bloqué par une règle de filtrage avec un objet FQDN, ce qui bloque les requêtes HTTP sans qu'aucune réponse ne soit renvoyée au navigateur. En revanche, le site www.euronews.com est bloqué par le filtrage d'URL (catégorie news) ; si vous tentez de le joindre en HTTP (la page de blocage apparaît), ou par le filtrage SSL si vous tentez de le joindre en HTTPS.

À faire : rédiger un rapport répondant aux questions ci-dessus.

Annexe 3 – Prise en main du serveur Debian

L'archive contient une machine virtuelle serveur debian qui permet de tester les protocoles utilisés dans les règles de filtrage des ateliers.

- Au besoin vérifiez que votre machine virtuelle serveur est bien sur le réseau interne LAN_DMZ1_A.
- Au démarrage de la machine virtuelle vous devez sélectionner la lettre de votre entreprise afin d'obtenir la configuration correspondante pour votre serveur qui sera en DMZ, sélectionnez **A**.

Voici les informations de configuration que vous obtenez pour l'agence A :

```
Your WEB server is "www.a.net" on 172.16.1.11
Your FTP server is "ftp.a.net" on 172.16.1.12
Your DNS server is on 172.16.1.10
Your DOMAIN NAME is a.net
Your MAIL server is "mail.a.net" on 172.16.1.13
Your WEBMAIL server is "webmail.a.net" on 172.16.1.11:808
Your USERNAME for mails is "user" and his password is "user"
The administrator of this server is "root" with password "root"
```

Serveur WEB	"www.a.net"	172.16.1.11
Serveur FTP	"ftp.a.net"	172.16.1.12
Serveur DNS		172.16.1.10
Serveur MAIL	"mail.a.net"	172.16.1.13
Serveur WEBMAIL	"webmail.a.net"	172.16.1.11:808
NOM DE DOMAINE	a.net	

Pour la messagerie, l'utilisateur est "user" et le mot de passe "user".
Le compte administrateur sur ce serveur est "root" et le mot de passe "root".

- Au besoin, vérifiez que votre machine virtuelle cliente de l'agence A est bien sur le réseau interne LAN_IN_A.
- Testez la commande ping 172.16.1.10, puis ping www.a.net, vous devriez avoir une réponse.
- Lancez dans le navigateur : www.a.net vous devriez avoir la page web ci-dessous :*

Annexe 4 – Procédure de Remise à zéro des Pare-feu SNS

Un RAZ du firewall peut être fait via la console (sur les VM ou les boitiers physiques), ceci nécessite un redémarrage (reboot). Un appui sur le bouton reset pour les boitiers physiques permet de restaurer la configuration d'usine et redémarrer en bridge sur toutes les interfaces.

```
ASQ Initialization...Done

Pattern checking...Done

Starting daemons... logd monitord hardwared asqd userreqd modem service dns ldap
 voucher filter network dialup ha snmp bird ipsec sl openvpn antivirus dhcp ntp
smcrouting event cad thind alived telemetryd hostapd.

SN210W16K0683A7: FW SN210W (S / EUROPE)
Firewall software version 4.0.2 RELEASE

port       name       NS-BSD   state  addressIPv4         addressIPv6
   1        out      mvneta0 no-link  10.0.0.254/8
   2         in      mvneta2      up  10.0.0.254/8
   3       dmz1      mvneta1 no-link  10.0.0.254/8


System is now ready.


NS-BSD/arm (SN210W16K0683A7) (ttyu0)
```

Pour les VM sur une ferme de serveurs, il faut pouvoir disposer d'un vlan commun à tous les pare-feu reliant leurs interfaces OUT. Or dans la configuration par défaut des VM du laboratoire Stormshield, toutes les interfaces appartiennent à un « bridge » et ont la même adresse IP, ce qui fonctionne avec des boitiers physiques ou avec les labs individuels sur VirtualBox mais génère du trafic que chaque pare-feu va bloquer en le reconnaissant comme une tentative d'intrusion si tous les pare-feu de la ferme de serveurs sont au démarrage sur le même VLAN/réseau.

La **remise-à-zéro des VM** va consister dans un premier temps à supprimer le bridge et mettre des adresses en DHCP (ou fixes) pour faciliter le paramétrage ensuite par l'interface web.

- Démarrez la machine virtuelle ou le boitier et accédez à la console en administrateur (admin/admin).
- Tapez la commande **defaultconfig –f –r –p –c -L** (anciennement **cleanfw -c**)

```
VMSNSX09K0639A9>cleanfw -c
Kill all test process
Remove local backup (autobackup)
Remove previous faulty fwtest traces...
Restore default configuration
Restoration done, reboot recommended
Clear History
VMSNSX09K0639A9>
```

NB : Pour plus d'informations sur la commande **defaultconfig***, voir l'annexe sur les commandes console.*

- Redémarrez la machine virtuelle à l'aide de la commande **reboot** et répondez aux questions de configuration initiale.

```
Pattern checking...Done

Starting daemons... logd monitord hardwared asqd userreqd modem service dns ldap
 voucher filter network dialup ha snmp bird ipsec sl openvpn antivirus dhcp ntp
smcrouting event cad thind alived telemetryd.
Setting boot partition to Main
No BACKUP partition found
mount_cd9660: /dev/cd0: No such file or directory

################################
## Configure keyboard mapping ##
################################

Current keyboard mapping: us.iso

The available choices are:
        1 - ch
        2 - de
        3 - es
        4 - fr
        5 - it
        6 - pl
        7 - us
Select your keyboard mapping number:
```

⇨ Sélectionner **4** pour fr *(sur le clavier le chiffre 4 sans utiliser la touche Maj).*

```
New keyboard mapping is fr

##########################################
## Change SRP/SSH password for admin ##
##########################################
setting password for admin
enter password:
```

⇨ Entrez un mot de passe de 8 caractères minimum avec Maj/min, pour éviter les soucis de clavier américain sur certaines consoles d'hyperviseur, utilisez par exemple **SioSioSio** ou **Sio2022*** puis confirmez.

```
########################################
## Change SRP/SSH password for admin ##
########################################
setting password for admin
enter password:
verify:
Modify SRP/SSH password of user 'admin' successful
```

Passons à la configuration des interfaces réseau :

```
Current network settings:
 1st interface (out): DHCP
 2nd interface (in): DHCP

Change 1st network interface (out) settings ? [y|N]:
```

⇨ Pour ce premier démarrage on va laisser les interfaces en DHCP, répondre N ou Entrée même si aucun serveur DHCP n'est relié à ces réseaux.

```
Current network settings:
 1st interface (out): DHCP
 2nd interface (in): DHCP

Change 1st network interface (out) settings ? [y|N]:
Change 2nd network interface (in) settings ? [y|N]:
Will you configure your virtual appliance through its first interface (out) ?
[Y/n]:
```

⇨ Répondre N, en effet il n'est pas recommandé d'autoriser l'administration sur votre interface OUT

```
VMSNSX09K0639A9: FW EVA1 (XL / EUROPE)
Firewall software version 4.0.1

port       name       NS-BSD   state  addressIPv4         addressIPv6
   1        out          em0      up  169.254.30.115/16
   2         in          em1      up  192.168.239.128/24
   3       dmz1          em2      up  192.168.229.132/24
   4       dmz2          em3      up  192.168.230.138/24


System is now ready.


NS-BSD/amd64 (VMSNSX09K0639A9) (ttyv0)

login:
```

Votre système est installé avec les valeurs rappelées ci-dessus, vous pouvez tester que la configuration du clavier a bien été prise en compte en saisissant votre login/mdp.

Annexe 5 – Commandes utiles de console des Pare-feu SNS

defaultconfig

```
Usage: [options]
        -f:     Force
        -r:     Reboot after defaultconfig
        -D:     Only Restore the data partition
        -p:     Reset password
        -u:     Check usb token boot restoration
        -d:     Dump root partition after defaultconfig
        -k:        Keep autoupdate data (Pattern, Pvm, Clamav, Kaspersky,
URLFiltering), default SSL proxy authority, default sslvpn full authority and
ssh host keys
        -l:     Keep network configuration file
        -n:     Do not mark firewall as having a defaultconfig configuration
        -c:     No backup files (.old)
        -L:     Remove logs
        -s:       Safe mode. Restore network configuration with only first
interface enabled.
        -t:     Reset TPM (TPM password required)
```

- taper **defaultconfig –f –r –p –c -L** pour redémarrer en configuration usine.