1. Fiche savoirs technologiques : Prise en main et configuration initiale du SNS

La configuration d'usine par défaut du pare-feu SNS (boîtier ou appliance VM laboratoire) est la suivante :

- la première interface du pare-feu SNS physique est nommée « OUT »,
- la seconde « IN »
- et le reste des interfaces « DMZx ».

L'interface **OUT** est une interface **externe** qui est utilisée pour connecter le pare-feu SNS à **Internet**.

Le reste des interfaces sont **internes** et servent principalement à connecter le pare-feu SNS à des **réseaux locaux** internes.

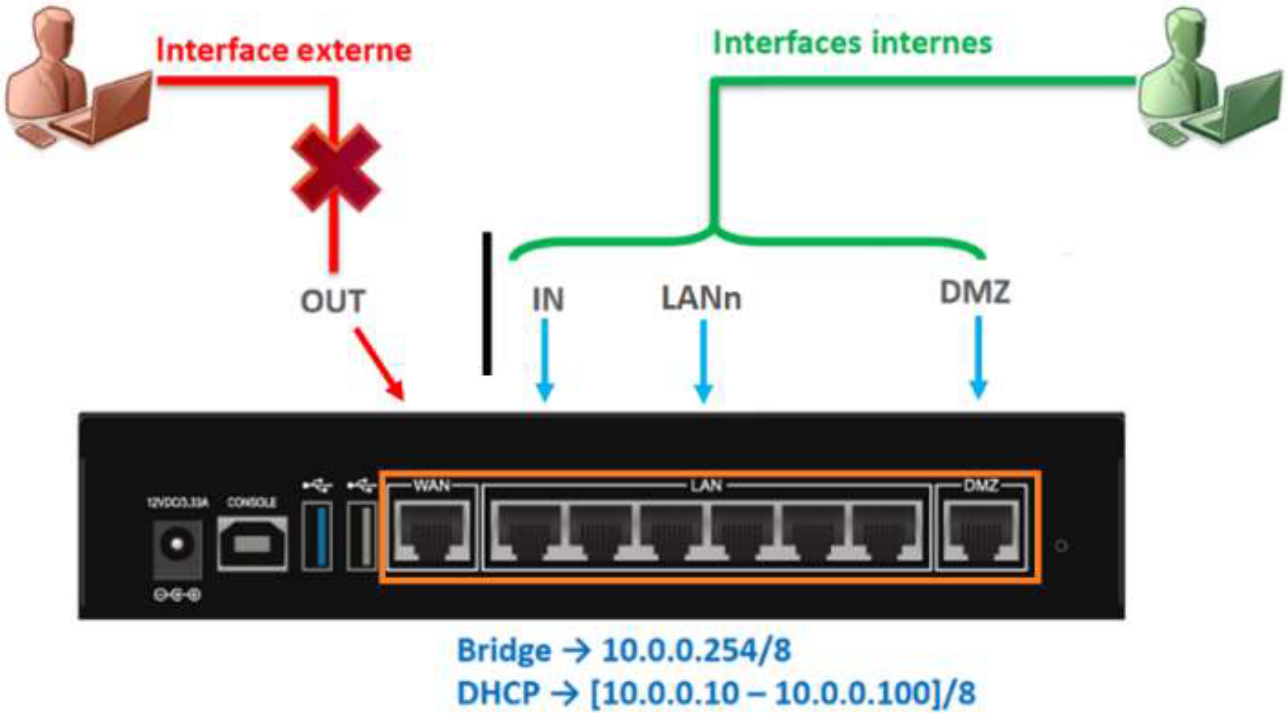
La distinction **interne/externe** pour les interfaces du SNS permet de se protéger contre les attaques d'usurpation d'adresse IP.

Toutes les interfaces sont incluses dans un **bridge** dont l'adresse est **10.0.0.254/8**.

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

Par défaut, seul le compte système **admin** (mot de passe par défaut **admin**), disposant de tous les privilèges sur le boîtier, existe et peut se connecter.



1.1. Connexion au pare-feu SNS

Pour accéder à l'interface d'administration du pare-feu SNS, il est indispensable de connecter votre client sur une interface interne (IN ou DMZ1) 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.

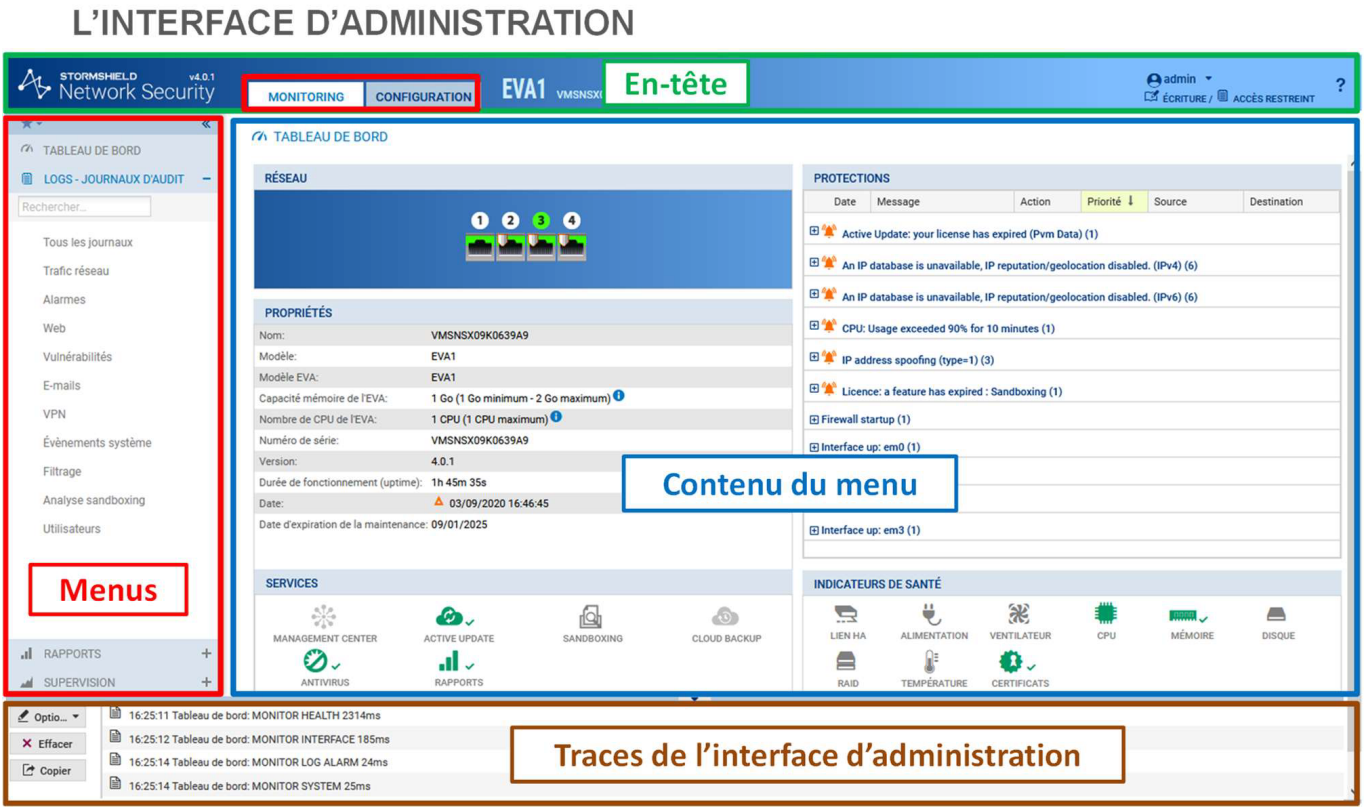
Vérifiez que votre machine hôte a bien obtenu une adresse IP dans la plage 10.0.0.0/24. Le cas échéant utilisez le script de configuration ou configurez-la manuellement.

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). Le compte par défaut est **admin** et le mot de passe **admin**.

Pour des raisons évidentes de sécurité, il conviendra de modifier ce mot de passe lorsque le pare-feu SNS est 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 le **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 :

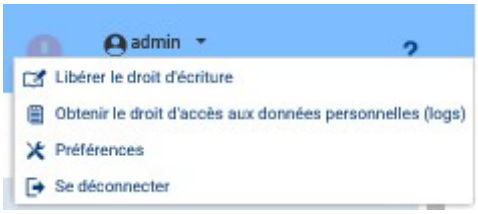
1.2.1. Partie 1 l'en-tête (partie encadrée en vert)

- 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, ses droits d'accès à la configuration : lecture seule

ou écriture et ses droits d'accès aux logs : restreint ou complet,



- 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 à plusieurs fonctionnalités :
  - Acquérir ou **libérer le droit d'écriture**. Notez qu'à un instant donné, un seul utilisateur peut disposer du droit d'écriture sur le pare-feu SNS ;
  - **Obtenir le droit d'accès aux données personnelles** ;
  - 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.

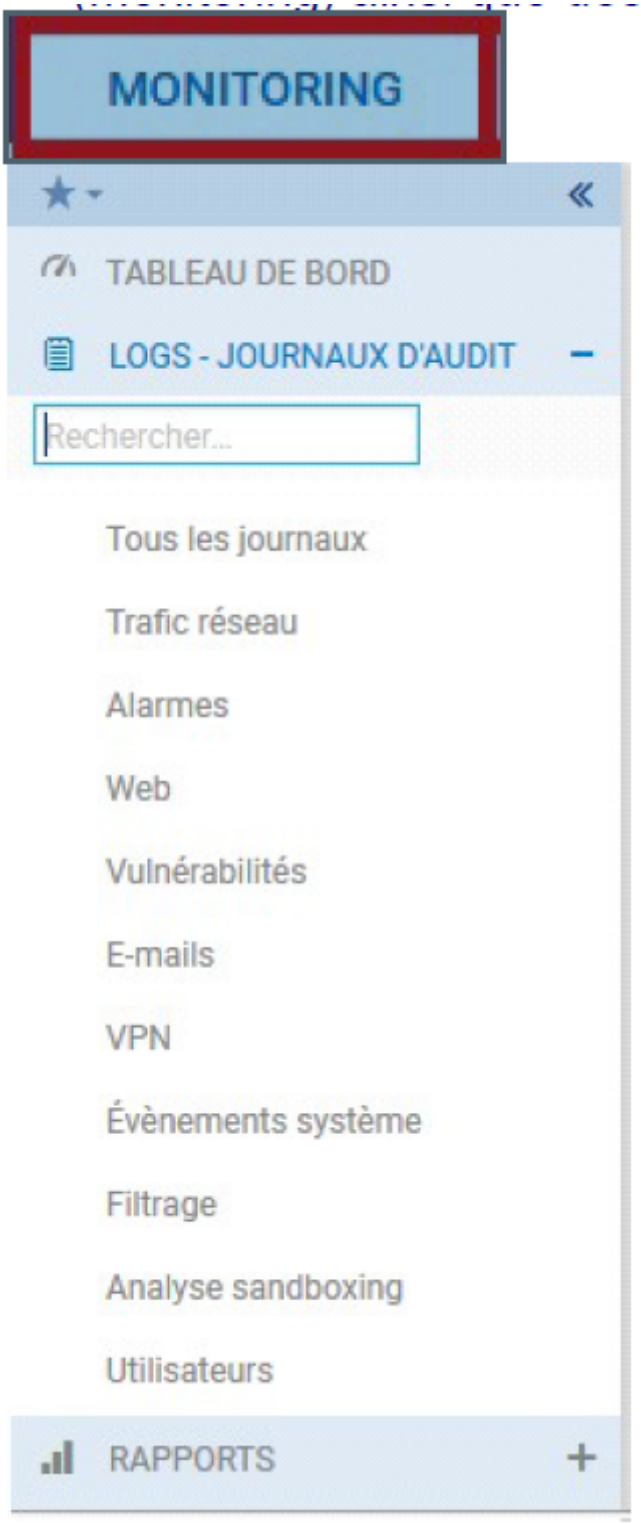


1.2.2. Partie 2 Les menus (partie encadrée en rouge)

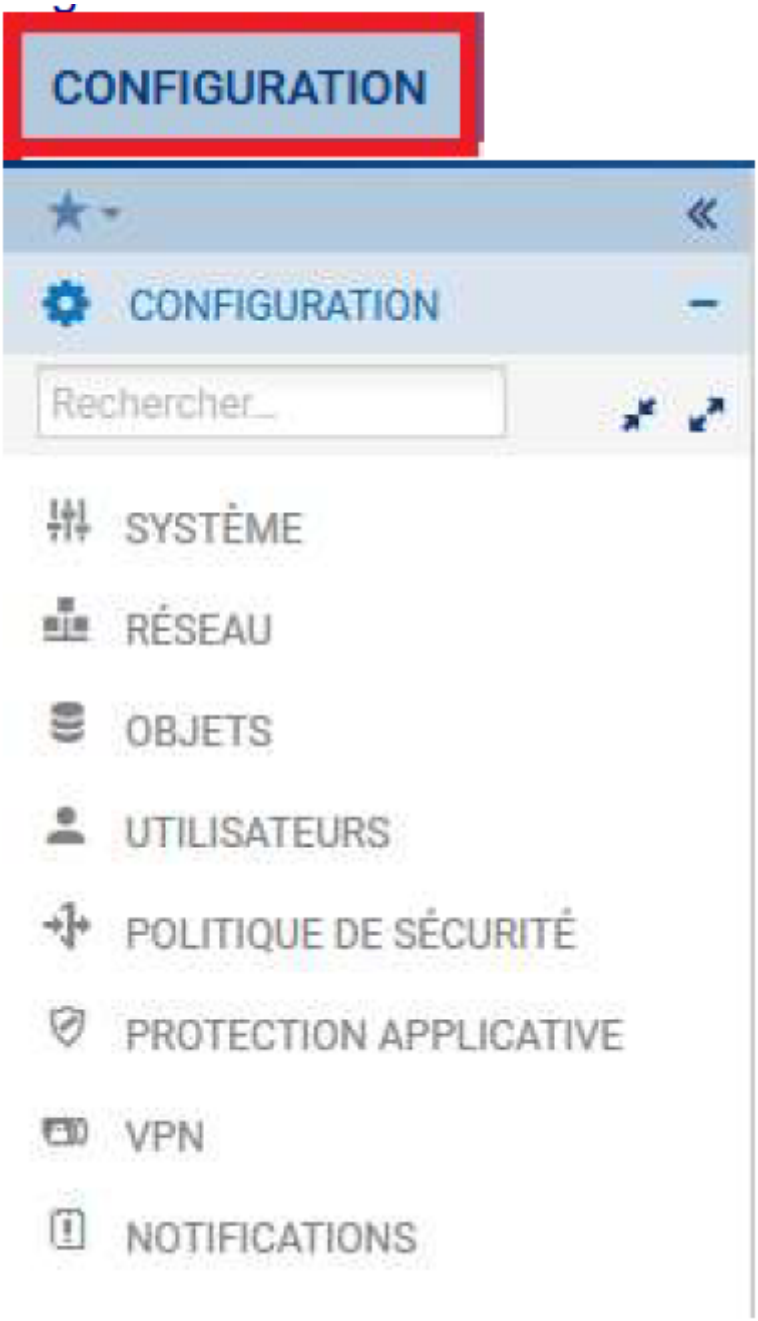
- Regroupe les menus de configuration, de supervision (Monitoring) ainsi que des raccourcis organisés sous forme de listes rétractables.

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.

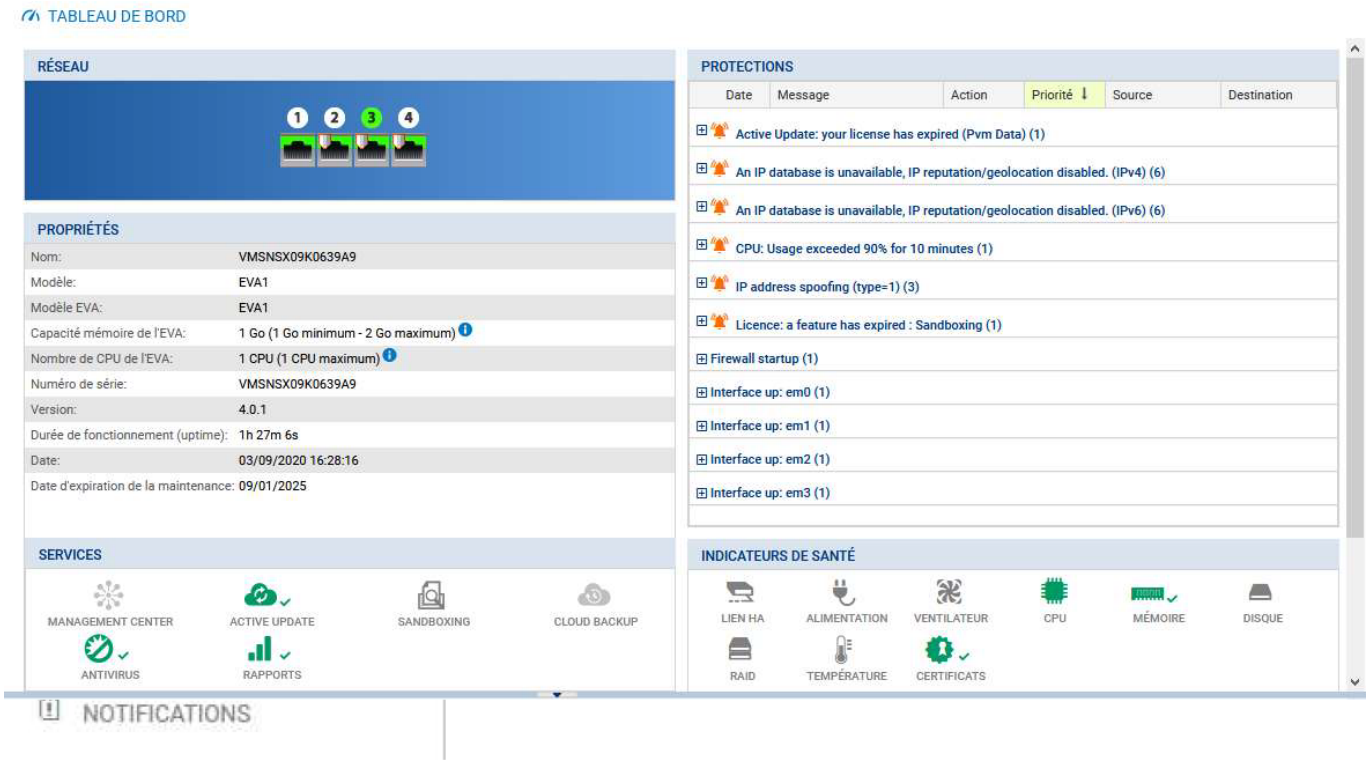


1.2.3. Partie 3 Le contenu du menu (partie encadrée en bleu)

- Affiche le contenu du menu sélectionné.

1.2.4. Partie 4 Les traces de l'interface d'administration (partie encadrée en marron)

* Affiche 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.

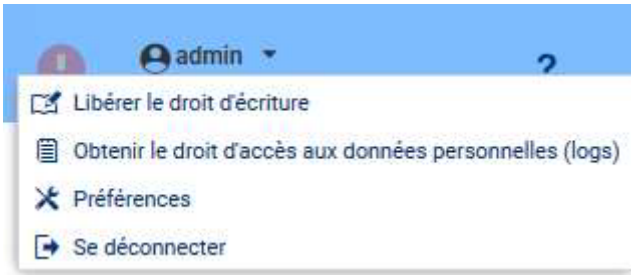
1.3. Configuration générale

Voici un certain nombre d'éléments de configuration générale utiles pour la bonne mise en oeuvre 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 activités 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.



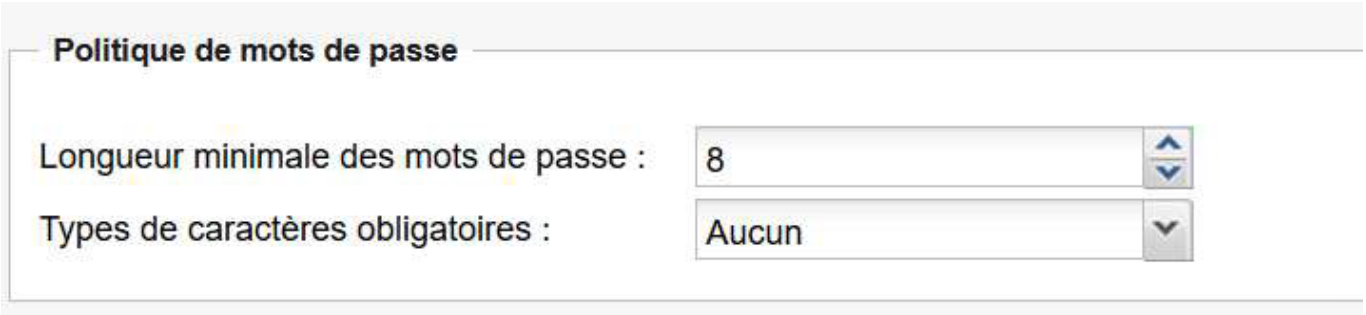
- Cliquez sur l'icône **Préférences** ;
- Dans la zone **Paramètres de connexion**, sélectionnez dans la liste **Déconnexion en cas d'inactivité :** la valeur **Toujours rester connecté**.



- 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. Laissez les logs en anglais.



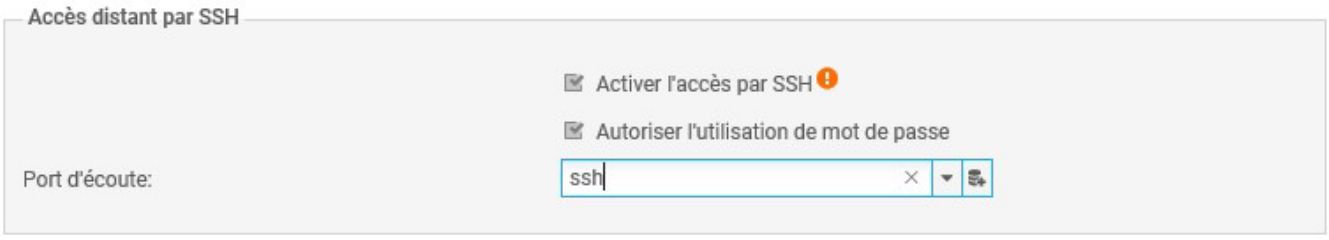
- La zone **Politique de mots de passe** permet de définir la longueur du mot de passe (8 par défaut) et la zone **Types de caractères** obligatoires permet de gérer la complexité du mot de passe (Aucun, Alphanumériques, alphabétiques et spéciaux).



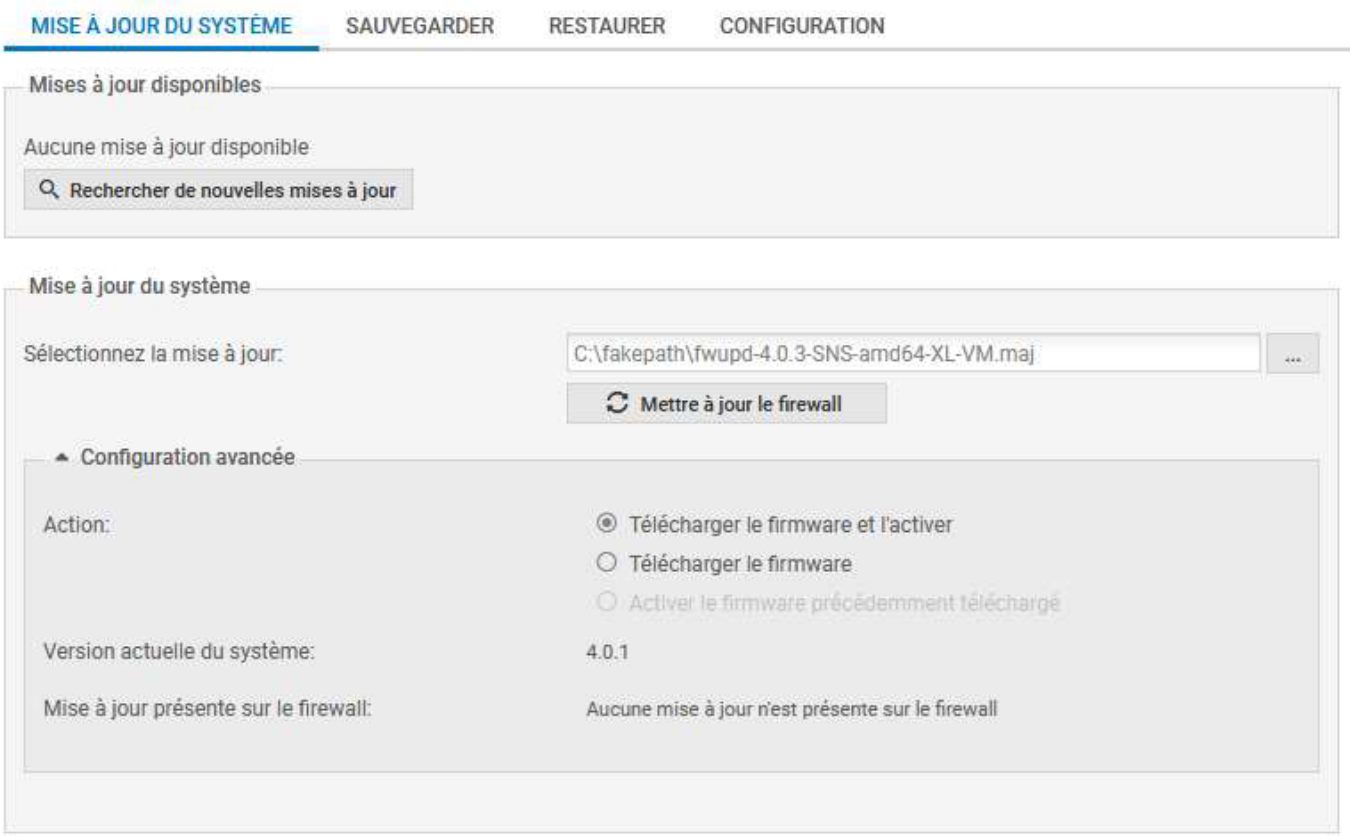
- Modifiez le fuseau horaire dans la zone **Date et heure (Europe/Paris)**.
- Cliquez **Synchroniser avec votre machine** ou **Maintenir le firewall à l'heure (NTP)** pour que les mises à jour d'heure d'été/heure d'hiver soient également effectives.
- Cliquez le bouton **Appliquer** pour sauvegarder la configuration et **Redémarrer plus tard**.

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

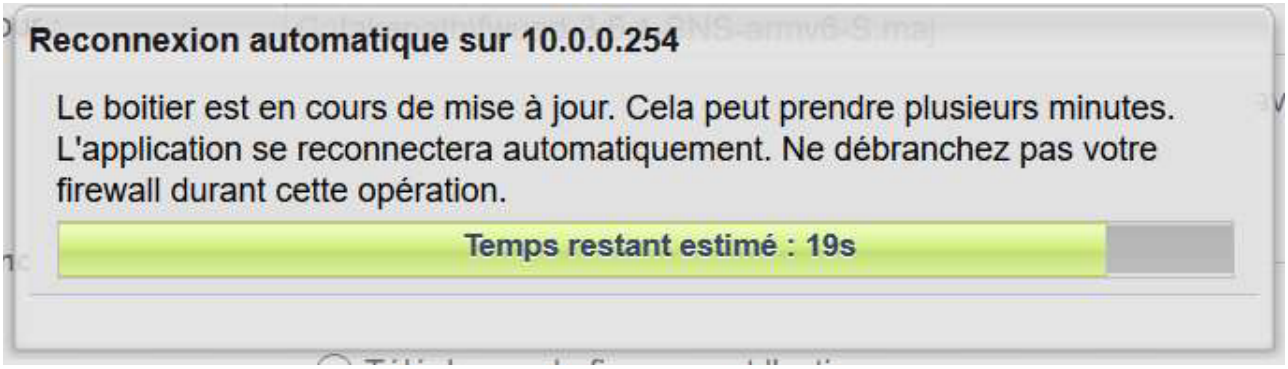
- La **modification du mot de passe** admin (recommandée) se fait dans le menu **Configuration** / **Système** / **Administrateurs** onglet **Compte ADMIN**. Le mot de passe doit par défaut, comporter au moins 5 caractères. La force du mot de passe choisit s'affiche alors. Les boutons **Exporter la clé privée** et **Exporter la clé publique** du firewall permettent respectivement de télécharger la clé privée et clé publique du compte admin.
- La **sauvegarde de la configuration** se fait dans le menu **Configuration** / **Système** / **Maintenance** onglet **Sauvegarder**. La sauvegarde automatique du fichier de configuration peut être mise en place et effectuée sur le Cloud Stormshield.
- L'accès SSH s'active depuis le menu **Configuration** / **Système** / **Configuration** onglet **Administration du firewall**, cochez **Activer l'accès par SSH** et **Autoriser l'utilisation de mot de passe**, puis choisissez **ssh** dans **Port d'écoute**.



- 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 firmware, vous devrez le télécharger sur l'UTM (soit directement via le lien **Rechercher de nouvelles mises à jour**, soit en allant le télécharger sur le site https://mystormshield.eu). Nous allons procéder à la mise à jour vers la dernière version disponible que vous aurez au préalable téléchargée.
- Cliquez **Configuration** / **Système** / **Maintenance** onglet **Mise à jour du système**.



- Sélectionnez le fichier de mise à jour présent sur votre poste de travail.
- 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 *Metre à jour le firewall**.**



* 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).**

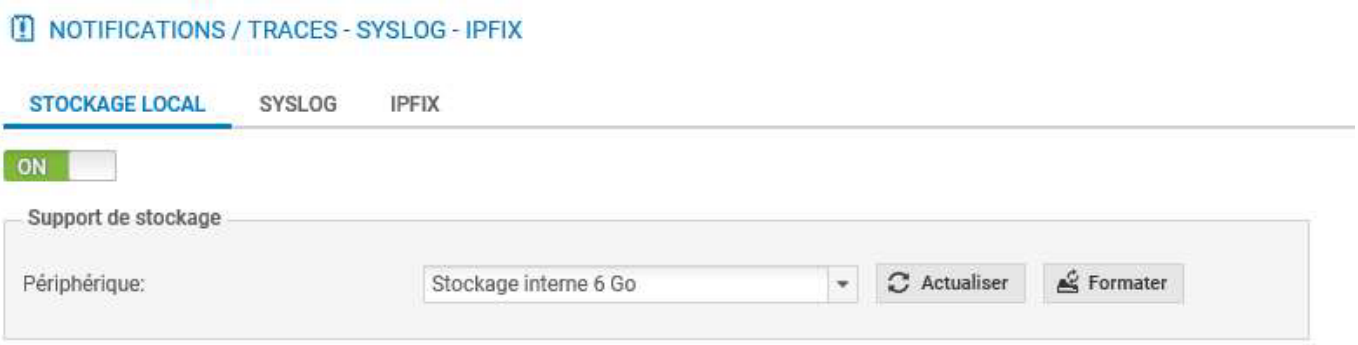
* Le menu

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. Vous pouvez le cas échéant les désactiver mais au contraire vérifiez qu'elles sont bien toutes activées. * 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).**

==== Stockage des logs : onglet

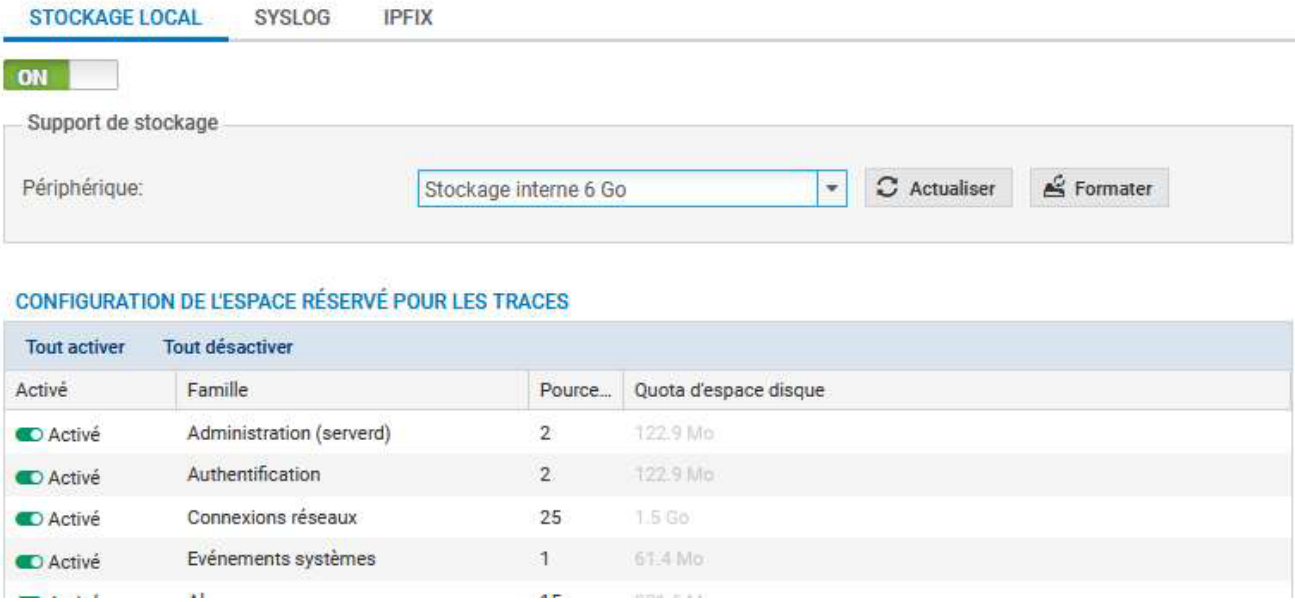
Configuration / Notifications / Traces – Syslog - IPFIX ====

- L'activation du stockage local des logs s'effectue dans l'onglet **Configuration / Notifications / Traces – Syslog - IPFIX / Stockage local**
- Sur une machine virtuelle, celui-ci est activé par défaut et occupe un espace disque de 6Go.





Une fois 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 des journaux.
- Le cas échéant, cliquez Conserver les rapports d'activité désactivés.

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%.

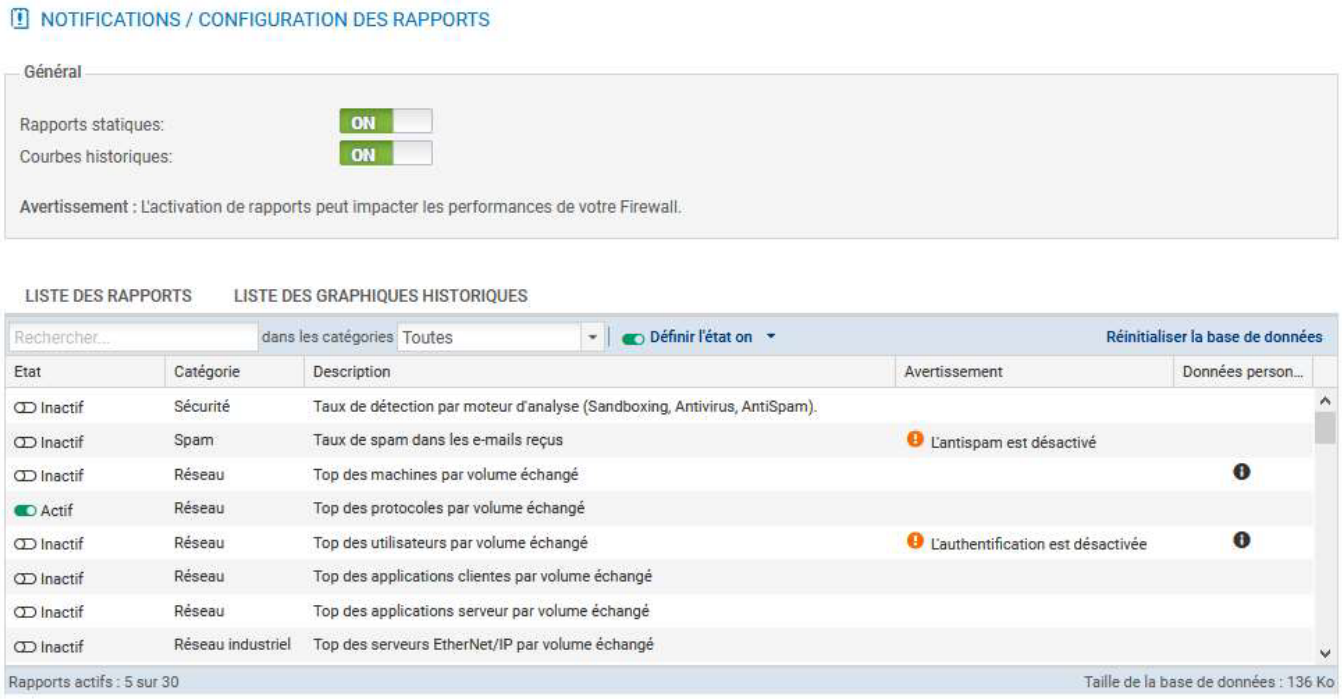
La taille réelle de l'espace disque réservé à une famille de traces est indiquée dans la partie **Quota** d'espace disque.

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).



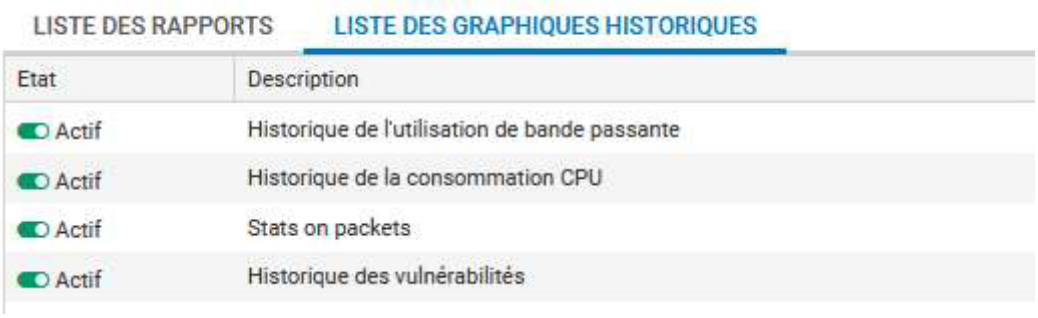
L'activation des rapports s'effectue depuis le menu **Configuration / Notifications / Configuration des rapports**

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



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 voir et modifier les graphiques qui sont activés par défaut.



1.4. Traces et Journaux

Les fichiers journaux sont organisés en plusieurs catégories décrites 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.

Dans le contexte **Monitoring**, le menu **LOGS - JOURNAUX D'AUDIT** permet de visualiser des traces sauvegardées en local sur le pare-feu SNS, regroupées 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).

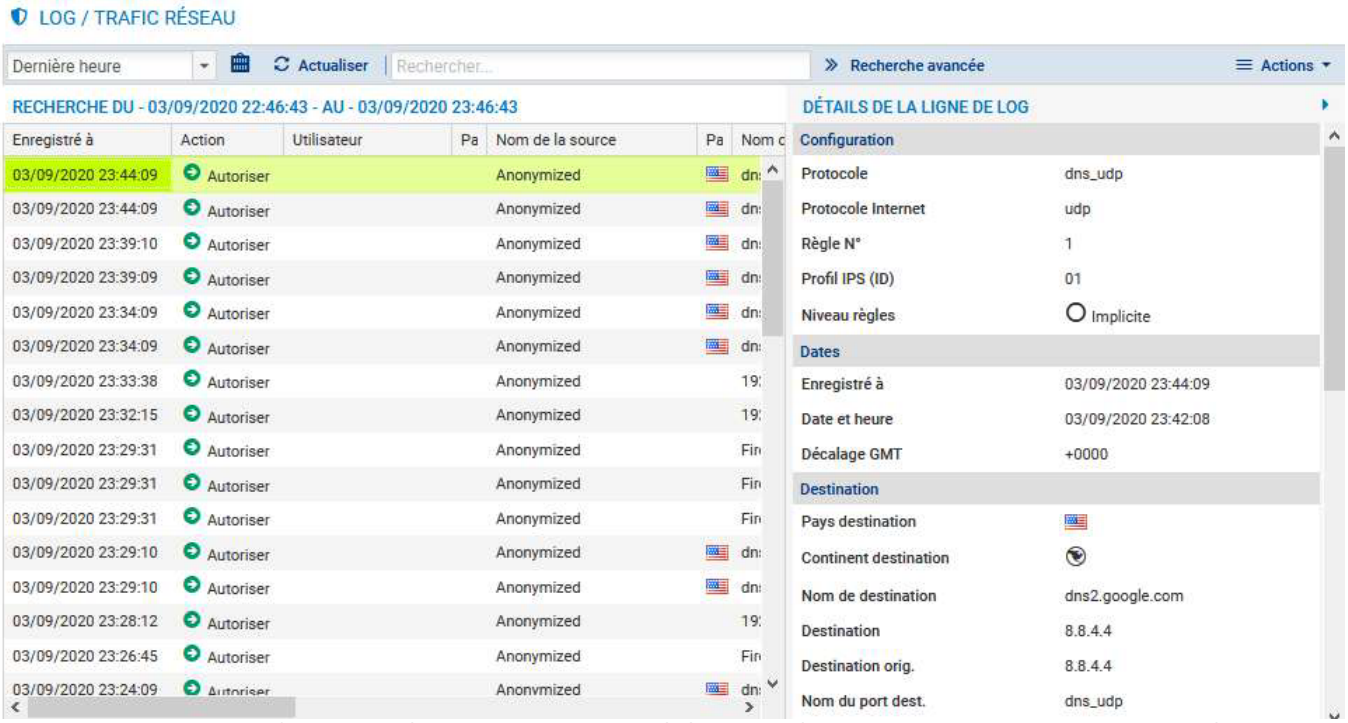
Pour appliquer la nouvelle réglementation européenne sur les données personnelles, le RGPD (Règlement Général sur la Protection des Données), l'accès aux logs des firewalls SNS est restreint par défaut pour tous les administrateurs.

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.

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



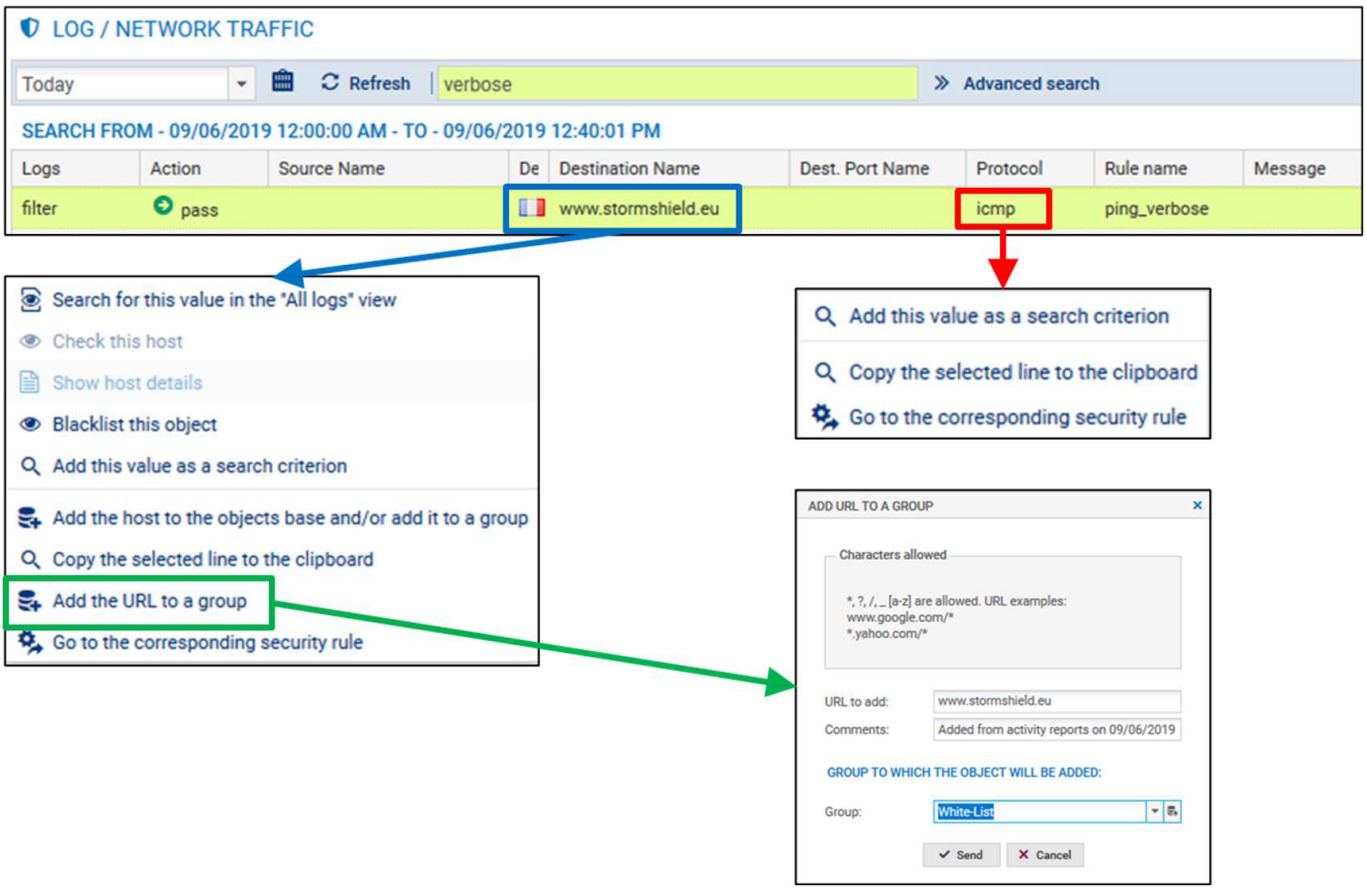
- Pour voir l'ensemble des données relatives à une trace, mettez la ligne désirée en surbrillance et cliquez sur la flèche en haut à droite **Détails de la ligne de log**.



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**.



1.5. Retour Accueil Stormshield

- Stormshield

From:
https://siocours.lycees.nouvelle-aquitaine.pro/ - **Les cours du BTS SIO**

Permanent link:
https://siocours.lycees.nouvelle-aquitaine.pro/doku.php/reseau/stormshield/phase1?rev=1631563016

Last update: **2021/09/13 19:56**