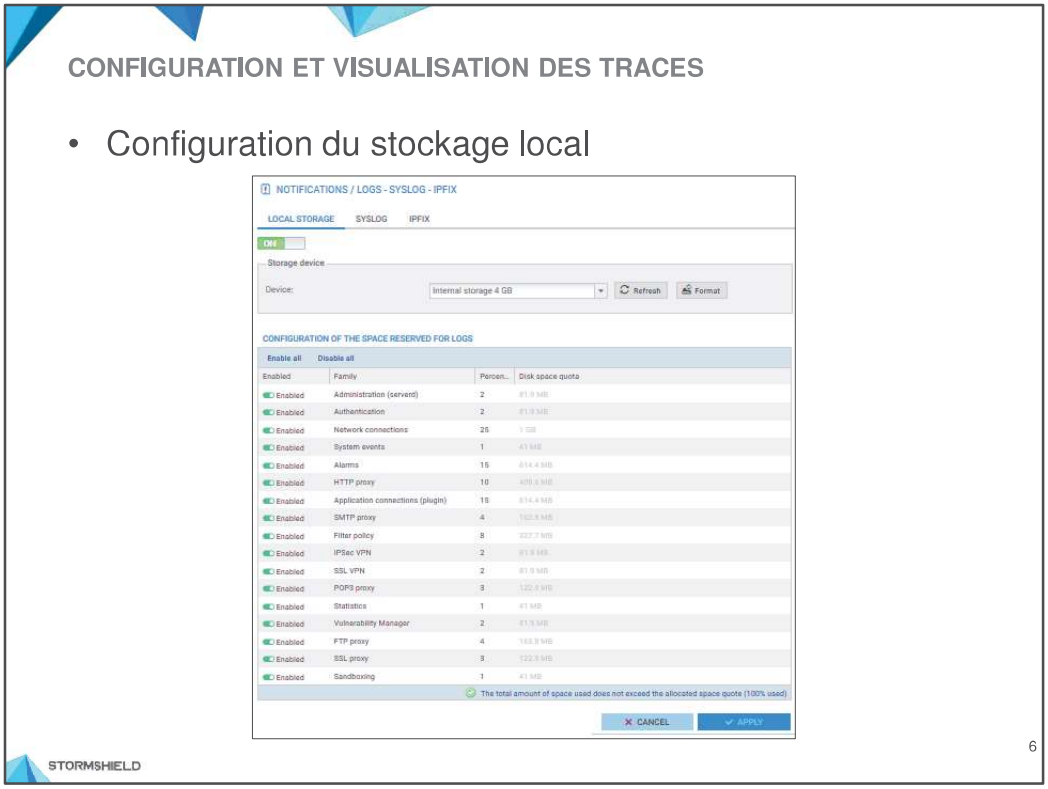
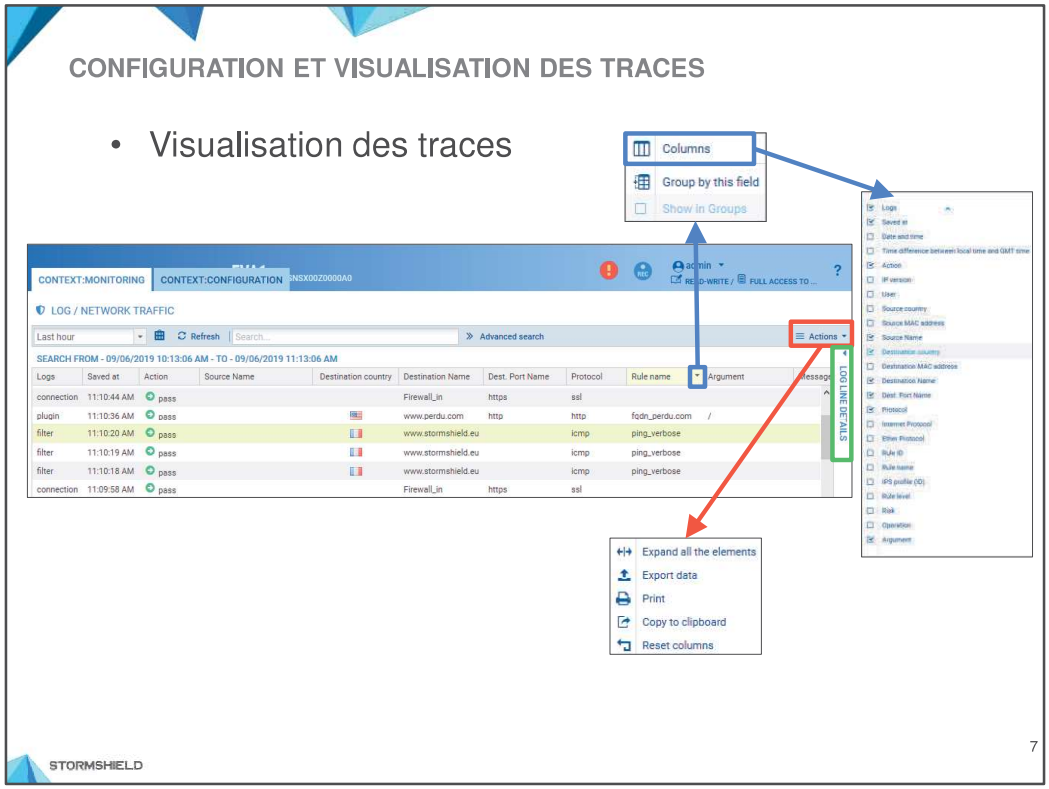


Le stockage local des traces est géré dans le menu **CONFIGURATION ⇒ NOTIFICATIONS ⇒ Traces - Syslog - IPFIX ⇒ onglet STOCKAGE LOCAL**. Les fichiers journaux sont enregistrés sur le disque dur (si le firewall en est équipé) ou sur une carte mémoire SD (si le firewall dispose d'un emplacement prévu à cet effet et si l'administrateur a souscrit à l'option « stockage externe »). Chaque journal occupe un espace réservé sur le support de stockage. L'onglet est composé de:

- **Bouton ON/OFF** : Permet d'activer/désactiver l'enregistrement des journaux. Il est activé par défaut et tous les journaux sont actifs.
- **Support de stockage** : Permet de sélectionner le support de stockage disque dur interne ou carte mémoire SD.
- **Bouton Actualiser** : Actualise les supports de stockage disponibles.
- **Bouton Formater** : Permet de formater le support de stockage sélectionné.
- **Configuration de l'espace réservé pour les traces** : Permet d'activer ou de désactiver l'écriture des traces pour un journal donné en double-cliquant dans la colonne **État** correspondante. Elle permet également de configurer le pourcentage de l'espace disque réservé pour chaque journal 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 un journal 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.



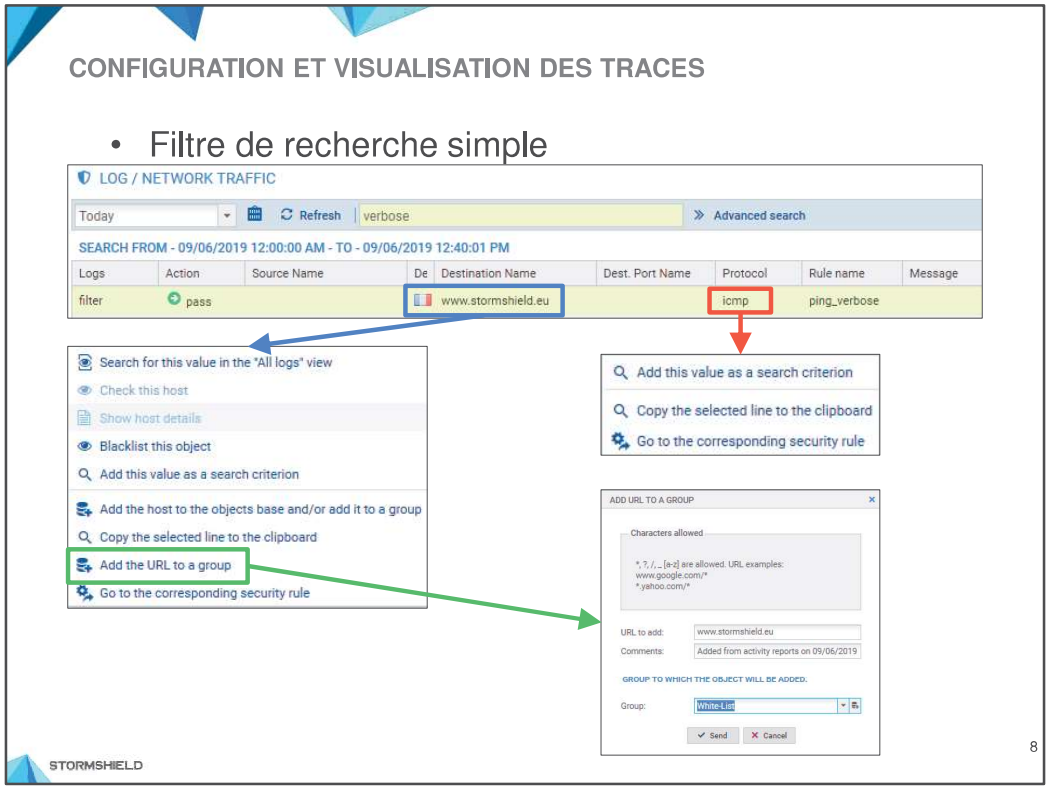
Le menu **JOURNAUX D'AUDIT**, dans le **CONTEXTE : SUPERVISION**, permet de visualiser les journaux sauvegardés en local sur le firewall, dans le cas où celui-ci dispose de disque dur (ou d'une carte mémoire SD avec l'option « stockage externe »), regroupés par famille de journaux : trafic réseau, alarmes, 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.

L'affichage des journaux peut être restreint à une plage temporelle prédéfinie (dernière heure, aujourd'hui, hier, semaine dernière ou mois dernier) ou personnalisée.

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

Le nombre de colonnes affiché par défaut est limité, cependant, toutes les colonnes peuvent être affichées en un clic grâce à l'option Afficher tous les éléments du menu Actions (encadré rouge). Pour ajouter manuellement une colonne à la fois, cliquez sur la flèche encadrée en bleu et ensuite sur « Colonnes ».

Pour voir l'ensemble des données relatives à une trace, mettez la ligne désirée en surbrillance et cliquez sur la flèche Détails de la ligne (encadré vert).

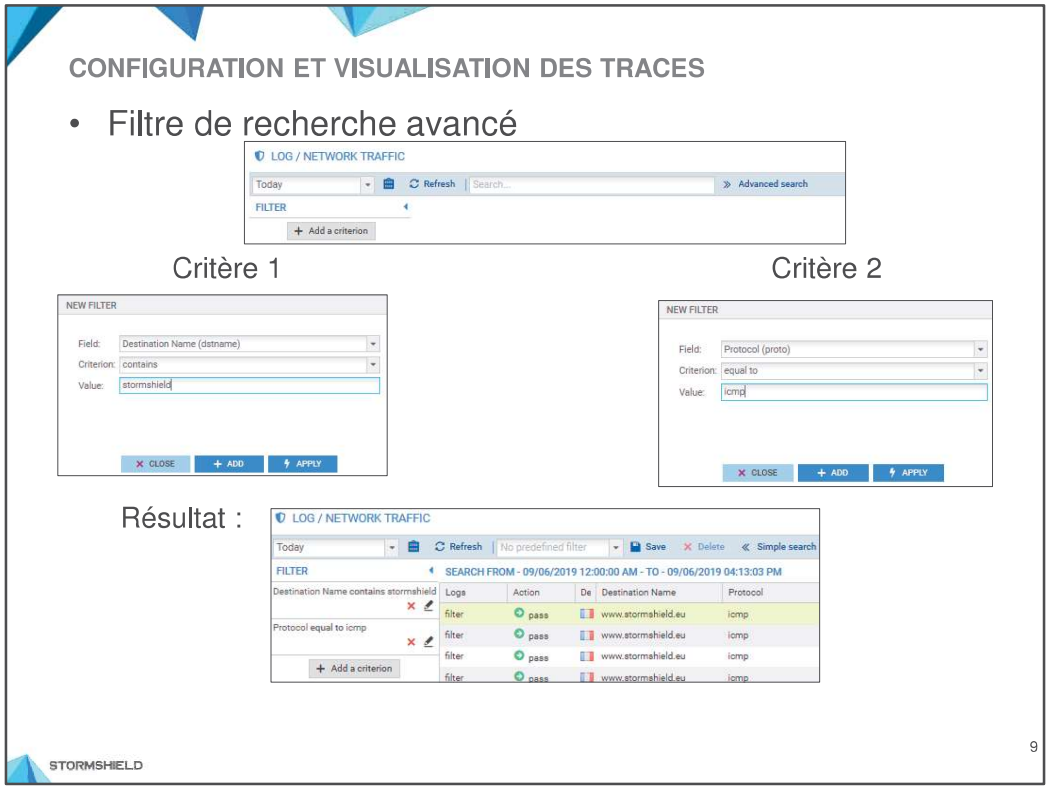


Pour filtrer les journaux, une barre de recherche simple permet de rechercher une chaine de caractères dans toutes les colonnes de tout les journaux, dans l'exemple ci-dessus, la recherche porte sur une partie du nom donné à une règle de filtrage ICMP. Le résultat est affiché, que la colonne concernant les informations soit visible à l'écran ou pas.

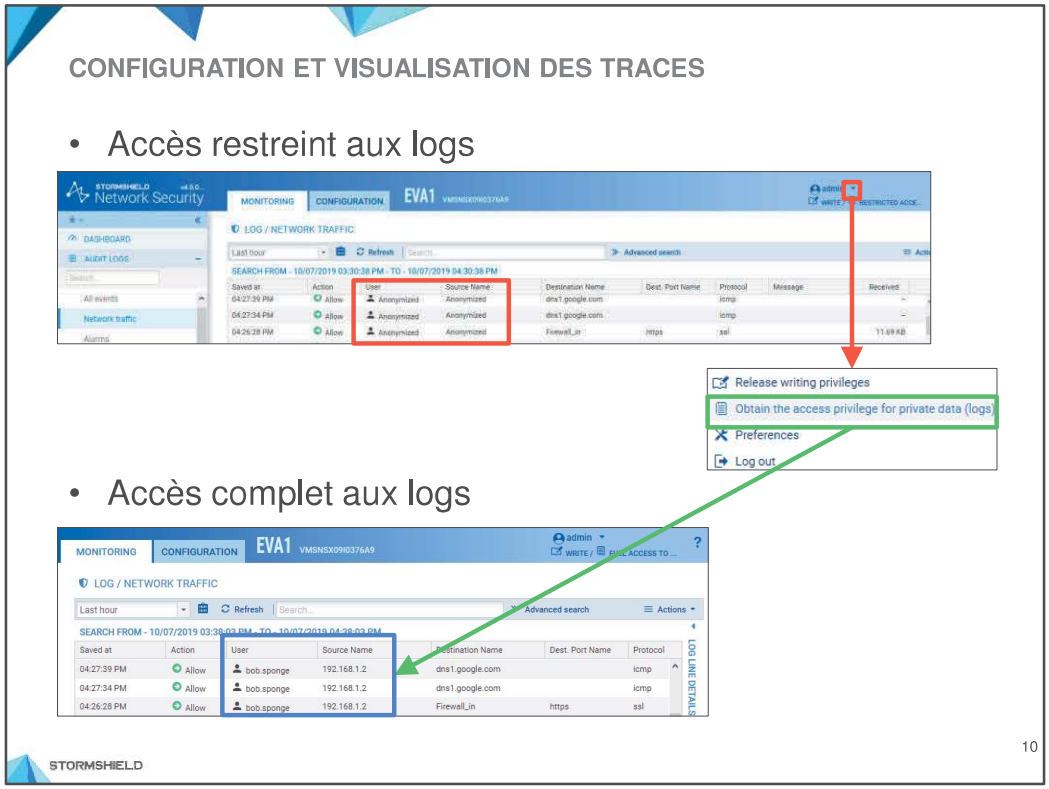
En cliquant droit sur un élément d'une ligne de trace, une fenêtre s'affiche pour offrir des raccourcis vers plusieurs fonctionnalités qui diffèrent suivant le type d'élément choisi, dans l'exemple ci-dessus :

- Différentes options permettent de gérer l'objet de type URL, comme de l'ajouter à une liste d'URL définie par l'administrateur (encadrés bleu puis vert),
- Le protocole ICMP (encadré rouge) peut être ajouté comme critère de recherche (il remplacera le critère **verbose** dans l'exemple ci-dessus), où la règle de filtrage correspondante peut être directement mise en surbrillance dans la politique de sécurité active.

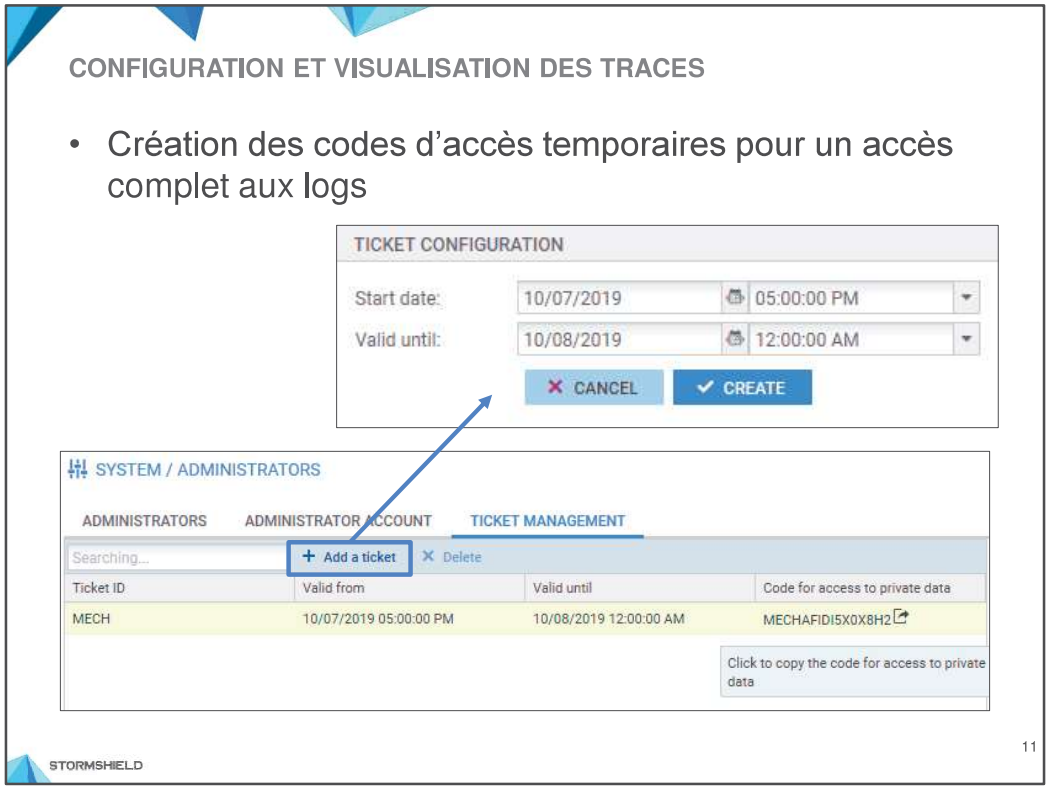
Ces manipulations permettent à l'administrateur de s'appuyer sur les journaux pour affiner sa politique de sécurité, d'enrichir la base objets du firewall, et de vérifier la configuration effectuée de manière intuitive.



La recherche avancée permet de créer des filtres complexes en combinant plusieurs critères de sélection.
Les filtres créés peuvent être enregistrés (bouton **Sauvegarder**), et réutilisés dans la même famille de journaux.



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)**.



Un administrateur n'ayant pas le droit « Accès aux données personnelles », peut également avoir un accès complet, grâce à un code d'accès temporaire, généré par un autre administrateur ayant le droit « Gestion des accès aux données personnelles ».

La création d'un code d'accès temporaire s'effectue dans le menu **CONFIGURATION ⇒ SYSTÈME ⇒ Administrateurs ⇒ onglet GESTION DES TICKETS**. Un ticket d'accès possède une date de début et une date de fin. Le ticket peut être copié et transmis à l'administrateur qui le renseigne dans la fenêtre qui s'affiche lorsqu'il clique sur le bouton **Accès restreint aux logs**.

NOTE : un ticket peut être utilisé par plusieurs administrateurs.