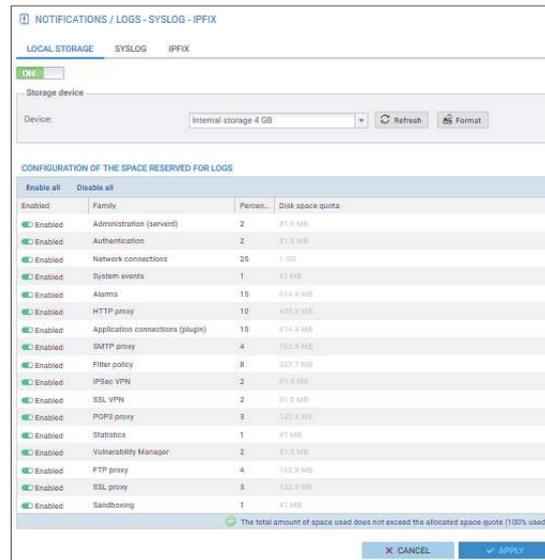


CONFIGURATION ET VISUALISATION DES TRACES

- Configuration du stockage local



6

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.

CONFIGURATION ET VISUALISATION DES TRACES

- Visualisation des traces

The screenshot displays the 'LOG / NETWORK TRAFFIC' section of the Stormshield interface. It features a search bar with 'Last hour' selected and a table of logs. The table has columns for 'Logs', 'Saved at', 'Action', 'Source Name', 'Destination country', 'Destination Name', 'Dest. Port Name', 'Protocol', 'Rule name', and 'Argument'. The logs are sorted by time, with the most recent at the top. A red box highlights the 'Actions' menu, which includes options like 'Expand all the elements', 'Export data', 'Print', 'Copy to clipboard', and 'Reset columns'. A blue box highlights the 'Columns' menu, which includes 'Group by this field' and 'Show in Groups'. A green box highlights the 'LOG LINE DETAILS' button on the right side of the table.

Logs	Saved at	Action	Source Name	Destination country	Destination Name	Dest. Port Name	Protocol	Rule name	Argument	Message
connection	11:10:44 AM	pass			Firewall_in	https	ssl			
plugin	11:10:36 AM	pass			www.perdu.com	http	http	fqn_perdu.com	/	
filter	11:10:20 AM	pass	www.stormshield.eu				icmp	ping_verbose		
filter	11:10:19 AM	pass	www.stormshield.eu				icmp	ping_verbose		
filter	11:10:18 AM	pass	www.stormshield.eu				icmp	ping_verbose		
connection	11:09:58 AM	pass			Firewall_in	https	ssl			

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).

CONFIGURATION ET VISUALISATION DES TRACES

- Filtre de recherche simple

LOG / NETWORK TRAFFIC

Today Refresh verbose Advanced search

SEARCH FROM - 09/06/2019 12:00:00 AM - TO - 09/06/2019 12:40:01 PM

Logs	Action	Source Name	De	Destination Name	Dest. Port Name	Protocol	Rule name	Message
filter	pass			www.stormshield.eu		icmp	ping_verbose	

Search for this value in the "All logs" view

- Check this host
- Show host details
- Blacklist this object
- Add this value as a search criterion
- Add the host to the objects base and/or add it to a group
- Copy the selected line to the clipboard
- Add the URL to a group
- Go to the corresponding security rule

ADD URL TO A GROUP

Characters allowed

* , / , _ [a-z] are allowed. URL examples:
www.google.com/*
* yahoo.com/*

URL to add: www.stormshield.eu

Comments: Added from activity reports on 09/06/2019

GROUP TO WHICH THE OBJECT WILL BE ADDED:

Group: White List

Send Cancel

8

Pour filtrer les journaux, une barre de recherche simple permet de rechercher une chaîne de caractères dans toutes les colonnes de tous 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.

CONFIGURATION ET VISUALISATION DES TRACES

- Filtre de recherche avancé

LOG / NETWORK TRAFFIC

Today Refresh Search... Advanced search

FILTER

+ Add a criterion

Critère 1

NEW FILTER

Field: Destination Name (dstname)

Criterion: contains

Value: stormshield

CLOSE ADD APPLY

Critère 2

NEW FILTER

Field: Protocol (proto)

Criterion: equal to

Value: icmp

CLOSE ADD APPLY

Résultat :

LOG / NETWORK TRAFFIC

Today Refresh No predefined filter Save Delete Simple search

FILTER SEARCH FROM - 09/06/2019 12:00:00 AM - TO - 09/06/2019 04:13:03 PM

Destination Name contains stormshield	Loga	Action	De	Destination Name	Protocol
Protocol equal to icmp	filter	pass	www.stormshield.eu	icmp	
	filter	pass	www.stormshield.eu	icmp	
	filter	pass	www.stormshield.eu	icmp	
	filter	pass	www.stormshield.eu	icmp	

+ Add a criterion

9

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.

CONFIGURATION ET VISUALISATION DES TRACES

- Accès restreint aux logs

Saved at	Action	User	Source Name	Destination Name	Dest. Port Name	Protocol	Message	Received
04:27:39 PM	Allow	admin	Anonymized	dns1.google.com		icmp		
04:27:34 PM	Allow	admin	Anonymized	dns1.google.com		icmp		
04:26:28 PM	Allow	admin	Anonymized	Firewall_in	https	ssl		11.69 KB

- Release writing privileges
- Obtain the access privilege for private data (logs)
- Preferences
- Log out

- Accès complet aux logs

Saved at	Action	User	Source Name	Destination Name	Dest. Port Name	Protocol	Message	Received
04:27:39 PM	Allow	bob.sponge	192.168.1.2	dns1.google.com		icmp		
04:27:34 PM	Allow	bob.sponge	192.168.1.2	dns1.google.com		icmp		
04:26:28 PM	Allow	bob.sponge	192.168.1.2	Firewall_in	https	ssl		

10

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)**.

CONFIGURATION ET VISUALISATION DES TRACES

- Création des codes d'accès temporaires pour un accès complet aux logs

TICKET CONFIGURATION

Start date: 10/07/2019 05:00:00 PM

Valid until: 10/08/2019 12:00:00 AM

SYSTEM / ADMINISTRATORS

ADMINISTRATORS ADMINISTRATOR ACCOUNT **TICKET MANAGEMENT**

Searching...

Ticket ID	Valid from	Valid until	Code for access to private data
MECH	10/07/2019 05:00:00 PM	10/08/2019 12:00:00 AM	MECHAFIDI5X0X8H2 <input type="button" value="🔗"/>

STORMSHIELD

11

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.