

### Table des matières

I Configuration du stockage des journaux (logs).....	1
II Les Journaux.....	4
III Consultation des Journaux.....	4

Le stockage des journaux (logs) des pare-feu Stormshield peut être configuré en local et/ou vers un serveur Syslog et/ou avec le protocole IPFIX. Les journaux, rapports d'activités et graphiques d'historiques sont disponibles sur les pare-feu 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.

### I 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.

- Sélectionner 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** :

NOTIFICATIONS / TRACES - SYSLOG - IPFIX

STOCKAGE LOCAL    SYSLOG    IPFIX

ON

Support de stockage

Périphérique:

Stockage interne 6 Go

Actualiser

Formater

Sur un **boîtier physique**, le stockage local des logs n'est pas activé par défaut.

- 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.

NOTIFICATIONS / TRACES - SYSLOG - IPFIX

STOCKAGE LOCAL    SYSLOG    IPFIX

OFF

Support de stockage

Périphérique:

Support de stockage manquant ou débranché

Actualiser

Formater

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

- cocher le bouton **ON** ;
- dans la zone **Support de stockage** sélectionner dans la liste **Périphérique** la carte SD comme support de stockage.

ON

● N'ajoutez pas la carte SD lorsque le service de stockage des traces est activé. Rappel: il est nécessaire de désactiver le stockage des traces et d'appliquer la configuration avant d'insérer la carte SD.

● Le support de stockage doit être formaté.

Support de stockage

Périphérique:

Carte SD 28.32 Go (non formaté)

Actualiser

Formater

Le système vous propose de la formater avant utilisation.

➤ Cliquer **Formater Carte SD**. Cette opération prend quelques secondes.

#### ERREUR



Carte SD (28.32 Go) n'est pas formaté.  
Voulez-vous le formater maintenant ?

ANNULER

FORMATER CARTE SD (28.32 GO)



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 pré-configurés est activée avec pour chaque journal un espace dédié. Vous pouvez désactiver certains journaux si vous le souhaitez.

STOCKAGE LOCAL   SYSLOG   IPFIX

ON

● N'injectez pas la carte SD lorsque le service de stockage des traces est activé. Rappel: il est nécessaire de désactiver le stockage des traces et d'appliquer la configuration avant d'insérer la carte SD.

Support de stockage

Périphérique:

Carte SD 28.33 Go

Actualiser

Formater

#### CONFIGURATION DE L'ESPACE RÉSERVÉ POUR LES TRACES

Tout activer	Tout désactiver		
Activé	Famille	Pourcentage	Quota d'espace disque
<input checked="" type="checkbox"/> Activé	Administration (serveur)	2	580.1 Mo
<input checked="" type="checkbox"/> Activé	Authentification	2	580.1 Mo

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

#### ACTIVER LES RAPPORTS D'ACTIVITÉS



Le stockage externe va être activé.  
Vous voulez également activer les rapports d'activités ?

CONSERVER LES RAPPORTS D'ACTIVITÉS DÉSACTIVÉS

ACTIVER LES RAPPORTS D'ACTIVITÉS

➤ Le cas échéant, cliquer **Conserver les rapports d'activité désactivés**.

#### CONFIGURATION DE L'ESPACE RÉSERVÉ POUR LES TRACES

Tout activer	Tout désactiver		
Activé	Famille	Pourcentage	Quota d'espace disque
<input checked="" type="checkbox"/> Activé	Administration (serveur)	2	—
<input checked="" type="checkbox"/> Activé	Authentification	2	—
<input checked="" type="checkbox"/> Activé	Connexions réseaux	25	—
<input checked="" type="checkbox"/> Activé	Événements systèmes	1	—
<input checked="" type="checkbox"/> Activé	Alarmes	15	—
<input checked="" type="checkbox"/> Activé	Proxy HTTP	10	—
<input checked="" type="checkbox"/> Activé	Connexions applicatives (plugin)	15	—
<input checked="" type="checkbox"/> Activé	Proxy SMTP	4	—
<input checked="" type="checkbox"/> 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**. Si l'on désactive une trace mais qu'on laisse le pourcentage actif, cela maintiendra un espace disque alloué à cette trace malgré tout.

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**.

- Cliquer **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	<input checked="" type="checkbox"/> Définir l'état on	Réinitialiser la base de données
État	Catégorie	Description	Avertissement	Données person...
<input type="checkbox"/> Inactif	Sécurité	Taux de détection par moteur d'analyse (Sandboxing, Antivirus, AntiSpam).		
<input type="checkbox"/> Inactif	Spam	Taux de spam dans les e-mails reçus	L'anti-spam est désactivé	
<input type="checkbox"/> Inactif	Réseau	Top des machines par volume échangé		
<input checked="" type="checkbox"/> Actif	Réseau	Top des protocoles par volume échangé		
<input type="checkbox"/> Inactif	Réseau	Top des utilisateurs par volume échangé	L'authentification est désactivée	
<input type="checkbox"/> Inactif	Réseau	Top des applications clientes par volume échangé		
<input type="checkbox"/> Inactif	Réseau	Top des applications serveur par volume échangé		
<input type="checkbox"/> 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		
<input checked="" type="checkbox"/> Actif	Historique de l'utilisation de bande passante		
<input checked="" type="checkbox"/> Actif	Historique de la consommation CPU		
<input checked="" type="checkbox"/> Actif	Stats on packets		
<input checked="" type="checkbox"/> Actif	Historique des vulnérabilités		

## II Les Journaux

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

- **Administration** : regroupe les événements liés à l'administration du pare-feu SNS. Ainsi, toutes les modifications de configuration effectuées sur le pare-feu sont journalisées.
- **Authentification** : regroupe les événements liés à l'authentification des utilisateurs sur le pare-feu SNS.
- **Connexions réseaux** : regroupe les événements liés aux connexions TCP/UDP traversant ou à destination du pare-feu SNS non traitées par un plugin applicatif.
- **Événements systèmes** : regroupe les événements 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 événements liés aux fonctions de prévention d'intrusions (IPS) et les événements tracés avec le niveau alarme mineure ou majeure de la politique de filtrage.
- **Proxy HTTP** : regroupe les événements liés aux connexions traversant le proxy HTTP.
- **Connexions applicatives (plugin)** : regroupe les événements liés aux connexions traitées par un plugin applicatif (HTTP, FTP, SIP, etc).
- **Politique de filtrage** : regroupe les événements liés aux règles de filtrages et/ou de NAT, lorsque la journalisation des règles est en mode verbeux.

**NB** : Il est recommandé de libérer les quotas alloués à des catégories de logs correspondants à des fonctionnalités non utilisées (pour cause de licence non souscrite ou fonction non activée comme proxy POP3,...) et ré-allouer l'espace disque ainsi libéré aux autres catégories qui en aurait davantage besoin afin de retarder l'entrée en rotation des catégories les plus consommatrices (Connexions réseau / connexions applicatives / alarmes / captures réseau...).

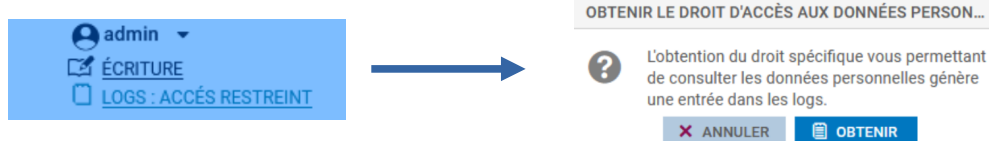
Dans le contexte **Monitoring**, le menu **LOGS - JOURNAUX D'AUDIT** permet de visualiser les journaux et traces sauvegardés en local sur le pare-feu SNS, regroupés par famille de journaux : trafic réseau, alarmes, web, etc.

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 anti chronologique (la trace la plus récente est en tête de liste).

**Pour appliquer le règlement général sur la protection des données (RGPD)**, l'accès aux logs des pare-feus 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.



## III Consultation des Journaux

➤ Cliquer **Monitoring** puis **LOGS – JOURNAUX D'AUDIT** puis, par exemple, **Trafic réseau**.

LOG / TOUS LES JOURNAUX

Demière heure Actualiser Rechercher... Recherche avancée Actions

RECHERCHE DU - 06/09/2020 22:22:06 - AU - 06/09/2020 23:22:06

Enregistré à	Action	Utilisateur	P.	Nom de la source	P.	Nom de destination	Nom du port dest.	Argument	Message
06/09/2020 23:20:24		Anonymous		172.16.2.200					LOG SEARCH GET
06/09/2020 23:20:24		Anonymous		172.16.2.200					LOG SEARCH NEW Filter=222020 09 06 ...
06/09/2020 23:20:23		Anonymous		172.16.2.200					SYSTEM DATE
06/09/2020 23:20:27		Anonymous		172.16.2.200					SYSTEM CLONE start=0 limit=25
06/09/2020 23:20:16	Authoriser	Anonymous				Firewall_Ldm21	https		
06/09/2020 23:20:16	Authoriser	Anonymous				Firewall_Ldm21	https		
06/09/2020 23:20:08		Anonymous		172.16.2.200					SYSTEM UPDATE CHECK start=0 limit=25

DÉTAILS DE LA LIGNE DE LOG

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**.

The screenshot shows the 'LOG / TRAFIC RÉSEAU' interface. On the left, a table lists log entries with columns: Enregistré à, Action, Utilisateur, Pa, Nom de la source, Pa, and Nom c. The entry for '03/09/2020 23:44:09' is highlighted. On the right, the 'DÉTAILS DE LA LIGNE DE LOG' panel is open, showing configuration details for the selected log entry.

Enregistré à	Action	Utilisateur	Pa	Nom de la source	Pa	Nom c
03/09/2020 23:44:09	Autoriser			Anonymized	dn	
03/09/2020 23:44:09	Autoriser			Anonymized	dn	
03/09/2020 23:39:10	Autoriser			Anonymized	dn	
03/09/2020 23:39:09	Autoriser			Anonymized	dn	
03/09/2020 23:34:09	Autoriser			Anonymized	dn	
03/09/2020 23:34:09	Autoriser			Anonymized	dn	
03/09/2020 23:33:38	Autoriser			Anonymized	19	
03/09/2020 23:32:15	Autoriser			Anonymized	19	
03/09/2020 23:29:31	Autoriser			Anonymized	Fin	
03/09/2020 23:29:31	Autoriser			Anonymized	Fin	
03/09/2020 23:29:31	Autoriser			Anonymized	Fin	
03/09/2020 23:29:10	Autoriser			Anonymized	dn	
03/09/2020 23:29:10	Autoriser			Anonymized	dn	
03/09/2020 23:28:12	Autoriser			Anonymized	19	
03/09/2020 23:26:45	Autoriser			Anonymized	Fin	
03/09/2020 23:24:09	Autoriser			Anonymized	dn	

**DÉTAILS DE LA LIGNE DE LOG**

**Configuration**

- Protocole: dns\_udp
- Protocole Internet: udp
- Règle N°: 1
- Profil IPS (IP): 01
- Niveau règles: ☐ Implicite

**Détails**

- Enregistré à: 03/09/2020 23:44:09
- Date et heure: 03/09/2020 23:42:08
- Décalage GMT: +0000

**Destination**

- Pays destination:
- Continent destination:
- Nom de destination: dns2.google.com
- Destination: 8.8.4.4
- Destination orig.: 8.8.4.4
- Nom du port dest.: dns\_udp

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 chaîne de caractères dans toutes les colonnes de toutes les traces, voir l'exemple ci-dessous pour **ICMP**.

The screenshot shows the 'LOG / NETWORK TRAFFIC' interface. A search filter is applied to the 'Protocol' column, showing 'icmp'. A context menu is open over the filter, with the option 'Add the URL to a group' highlighted. A dialog box titled 'ADD URL TO A GROUP' is also shown, with the URL 'www.stormshield.eu' entered.

**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	

**Context Menu Options:**

- 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:

Send Cancel