NOTE TECHNIQUE

STORMSHIELD NETWORK SECURITY

# DESCRIPTION DES JOURNAUX D'AUDIT (LOGS)

Produits concernés : SNS 4.x

Date : 9 décembre 2019

Référence : sns-fr-description_des_journaux_d'audit_note_technique-v4

# Table of contents

# Avant de commencer

Les firewalls Stormshield Network Security journalisent l'activité des différents services activés lors de leur fonctionnement. Par défaut, les événements générés (ou logs) sont stockés dans des fichiers de journaux d'audit en local sur le disque dur ou sur une carte mémoire SD pour les plus petits équipements. Ils sont également affichés dans l'interface Web d'administration, regroupés par thématique, par exemple Trafic réseau, Alarmes, Web, etc.

Consultez les logs pour vérifier l'activité du firewall, ou pour résoudre d'éventuels problèmes. Le Support technique Stormshield s'appuie aussi sur ces logs pour vous dépanner en cas de besoin.

Ce document décrit comment consulter et configurer les logs, ainsi que les bonnes pratiques à adopter pour optimiser leur stockage et leur utilisation.

# Consulter les logs

Vous pouvez consulter les logs dans l'interface Web d'administration ou directement dans les fichiers stockés sur le disque ou la carte SD. Si les logs sont envoyés vers un serveur Syslog ou via un collecteur IPFIX, vous pouvez aussi les consulter par ce biais-là.

Dans un contexte Haute disponibilité (HA), les logs ne sont pas répliqués sur tous les noeuds. C'est le firewall actif qui écrit les logs sur son disque dur. Si le firewall devient passif, l'autre firewall actif reprend à son tour l'écriture des logs. Par conséquent, aucun des firewalls du cluster ne contient la totalité des logs, et l'interface web d'administration n'affiche que les logs se trouvant sur le firewall auquel elle est connectée. Pour consulter plus facilement tous les logs dans un contexte HA, envoyez-les vers un serveur Syslog.

Pour appliquer le Règlement Général sur la Protection des Données (RGPD), l'accès aux logs des firewalls a été restreint par défaut pour tous les administrateurs. Le super administrateur *admin* peut accéder facilement aux logs complets mais les autres administrateurs doivent demander un code d'accès temporaire. Chaque demande d'accès aux logs complets produit un log. Pour plus d'informations, reportez-vous à la note technique Se conformer aux règlements sur les données personnelles.

## Consulter les logs dans l'interface Web d'administration

1. Dans la partie supérieure de l'interface Web d'administration, cliquez sur l'onglet **Monitoring**.
2. Dans le menu de gauche, choisissez **Logs-Journaux d'audit**.
3. Pour afficher tous les logs, cliquez sur **Tous les journaux**. Sinon, choisissez la vue à consulter. Les logs sont affichés dans l'ordre chronologique, le premier étant le plus récent. Par défaut seuls les logs de l'heure précédente sont affichés, mais vous pouvez modifier la plage horaire en cliquant sur la liste déroulante.
4. Cliquez sur **Actions > Afficher tous les éléments** si vous souhaitez afficher toutes les colonnes disponibles.
5. Pour filtrer les logs, saisissez du texte dans le champ **Rechercher** ou cliquez sur **Recherche avancée**, puis **Ajouter un critère**, pour combiner différents critères de recherche.

Pour plus d'informations sur l'affichage des logs ou la recherche, reportez-vous aux sections Les vues et Les interactions du Manuel utilisateur.

## Consulter les logs dans les fichiers journaux

- Connectez-vous au firewall en SSH pour consulter les journaux stockés dans le répertoire */log*. Ceux-ci sont constitués des fichiers suivants :

| | |
|---|---|
| **l_alarm** | Événements liés aux fonctions de prévention d'intrusion (IPS) et ceux tracés avec le niveau d'alarme mineure ou majeure de la politique de filtrage. |
| **l_auth** | Événements liés à l'authentification des utilisateurs sur le firewall. |
| **l_connection** | Événements liés aux connexions TCP/UDP vers/depuis le firewall, non traités par un plugin applicatif. |
| **l_count** | Statistiques concernant le nombre d'exécutions d'une règle. La génération de ces logs n'est pas activée par défaut. Pour plus d'informations, voir Ajouter des logs sur les règles de filtrage et de NAT |
| **l_date** | Événements liés aux changements d'heure du Firewall. |
| **l_filter** | Événements liés aux règles de filtrages et/ou de NAT. La génération de ces logs n'est pas activée par défaut. Pour plus d'informations, voir Ajouter des logs sur les règles de filtrage et de NAT |
| **l_filterstat** | Statistiques concernant l'utilisation du firewall et de ses ressources. |
| **l_ftp** | Événements liés aux connexions traversant le proxy FTP. |
| **l_monitor** | Statistiques pour la création de graphes de performances et rapports de sécurité (Interface Web d'administration et Stormshield Network Realtime Monitor). |
| **l_plugin** | Événements liés aux traitements effectués par les plugins applicatifs (FTP, SIP, etc.). |
| **l_pop3** | Événements liés aux connexions traversant le proxy POP3. |
| **l_pvm** | Événements liés à l'option Stormshield Network Vulnerability Manager. |
| **l_sandboxing** | Événements liés à l'analyse sandboxing des fichiers lorsque cette option a été souscrite et activée. |
| **l_server** | Événements liés à l'administration du firewall. |
| **l_smtp** | Événements liés aux connexions traversant le proxy SMTP. |
| **l_ssl** | Événements liés aux connexions traversant le proxy SSL. |
| **l_system** | Événements liés directement au système (arrêt/redémarrage du Firewall, erreur système, fonctionnement des services …). |
| **l_vpn** | Événements liés à la phase de négociation d'un tunnel VPN IPSEC. |
| **l_web** | Événements liés aux connexions traversant le proxy HTTP. |
| **l_xvpn** | Événements liés à l'établissement de VPN SSL (mode tunnel ou portail). |

Pour plus d'informations sur les différents champs contenus dans ces fichiers, reportez-vous à la section Comprendre les journaux d'audit.

## Consulter les archives des logs

Dès qu'un fichier journal atteint une taille supérieure à 20 Mo, il est clôturé au profit d'un nouveau. Il est toujours consultable dans le répertoire */log* sous un nouveau nom.

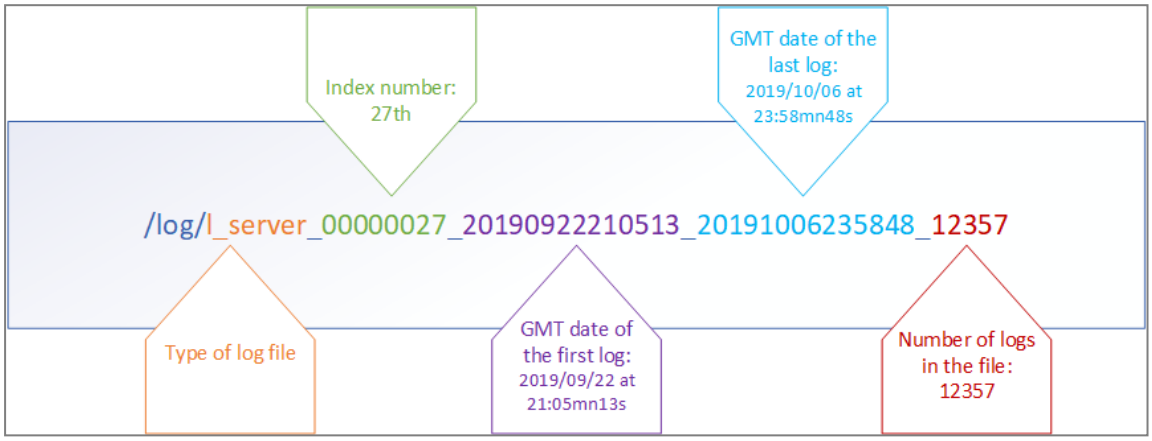
### Nom des archives

Le nom des fichiers journaux clôturés respecte la structure suivante :

- Type de fichier journal concerné (Exemple : l_filter, l_alarm…),
- Numéro d'indexation sur 8 chiffres (commence à 0),
- Date de création : date GMT du premier log contenu dans le fichier,

- Date de clôture : date GMT du dernier log contenu dans le fichier,
- Nombre de traces stockées dans le fichier.

**Exemple** :




L'indexation des fichiers (gérée de manière incrémentale et commençant à 0) permet de ne pas se baser uniquement sur leur date de création ou de clôture, car ces dernières peuvent être faussées par un changement d'heure du firewall.

## Gestion du stockage des logs

Par défaut, en cas de saturation de l'espace de stockage dédié à un type de logs, le fichier archive correspondant le plus ancien est effacé pour libérer de l'espace.

Deux autres comportements sont disponibles, que vous pouvez activer pour chaque type de fichier journal à l'aide de la commandes *serverd CONFIG LOG* :

- La génération des logs s'interrompt lorsque l'espace dédié est plein,
- Le firewall s'éteint lorsque l'espace dédié est plein.

Pour plus d'informations, reportez-vous au GuideCLI Serverd Commands Reference Guide (en anglais uniquement).

# Configurer les logs

Vous pouvez définir quels journaux vous souhaitez que le firewall génère, leur emplacement de stockage, et le niveau de logs à générer.

Il est important de configurer la journalisation de manière optimale pour éviter des logs inutiles. En effet, quand les logs générés sont plus nombreux que les capacités d'écriture sur leur espace de stockage, un espace tampon permet de temporiser cette écriture, mais celui-ci peut également arriver à saturation. Pour anticiper ou résoudre ce type de problèmes, vous pouvez aussi consulter l'article de la base de connaissances Comment résoudre un problème de débordement de logs (en anglais) et ses articles connexes.

## Comprendre les types de logs

Il existe deux types de logs :

- Les logs d'activité standard qui sont activés par défaut et que vous pouvez configurer via le menu **Notifications > Traces - Syslog - IPFIX**.
- Les logs de filtrage et de NAT qui sont désactivés par défaut et que vous pouvez configurer via le menu **Général > Niveau de trace** de la fenêtre d'édition d'une règle de filtrage ou le menu **Options > Niveau de trace** de la fenêtre d'édition d'une règle de NAT. Ces logs ne doivent être activés que temporairement pour diagnostiquer des problèmes.

## Choisir l'emplacement des logs

Par défaut les logs sont stockés en local sur le disque dur ou une carte SD. Ils peuvent aussi être envoyés vers un serveur Syslog ou un collecteur IPFIX.

1. Dans l'onglet **Configuration**, choisissez le menu **Notifications > Traces - Syslog - IPFIX**.
2. Activez l'interrupteur ON/OFF 

pour chaque emplacement vers lequel vous souhaitez envoyer les logs : local, Syslog et/ou IPFIX. Par exemple, si vous choisissez de visualiser les logs uniquement à travers un outil de type SIEM, activez un profil Syslog et désactivez le stockage local et le collecteur IPFIX.

   Si vous désactivez le stockage local, seuls les logs les plus récents qui sont stockés dans la RAM (environ 200 logs par catégorie) seront visibles dans l'interface Web d'administration du firewall. Les logs plus anciens ne seront pas affichés.

## Choisir les journaux à générer

Par défaut, tous les journaux d'activité standard sont activés et visibles dans l'interface Web d'administration. Seuls les logs de filtrage et de NAT sont désactivés par défaut. Il est recommandé de désactiver les journaux dont vous n'avez pas besoin.

Cette fonctionnalité n'est pas disponible pour les collecteurs IPFIX.

1. Dans l'onglet **Configuration**, choisissez le menu **Notifications > Traces - Syslog - IPFIX**.
2. Pour le stockage local, désactivez certaines familles de logs en double-cliquant dans la colonne **Activé** du tableau **Configuration de l'espace réservé pour les traces**. Vous pouvez aussi ajuster les pourcentages d'espace disque à votre convenance.
   Pour le serveur Syslog, désactivez certaines familles de logs en double-cliquant dans la colonne **État** dans **Configuration avancée**.

   Les logs désactivés pour le stockage local ne s'affichent pas dans l'interface Web d'administration du firewall.

Pour plus d'informations, reportez-vous à la section Traces-Syslog-IPFIX du Manuel utilisateur.

## Ajouter des logs sur les règles de filtrage et de NAT

Par défaut, les flux traités par une règle de filtrage ou de NAT génèrent des logs dans le journal **Connexions réseau**, ou dans le journal **Connexions applicatives** si une analyse applicative est menée par un plugin en mode, IPS, IDS. Seules sont journalisées les connexions avec l'action "Autoriser" et ayant leur couche de transport en TCP/UDP.

Afin de vérifier le bon fonctionnement d'une règle de filtrage ou de NAT, vous pouvez générer des logs supplémentaires qui ne sont pas présents dans les autres journaux :

- Les logs de tous les flux bloqués par une règle de filtrage,
- Les logs de tous les flux traités par une translation d'adresses (NAT),
- Les logs des flux directement au-dessus d'IP qui correspondent à une règle de filtrage, qu'ils soient autorisés ou bloqués.

Activez ce mode verbeux avec précaution et seulement le temps de réaliser la vérification, car il génère une grande quantité de logs, dont certains en doublon avec les logs d'activité standard. Il peut entraîner un débordement des logs et des baisses de performances du firewall.

Ce type de logs s'affiche dans le menu de monitoring **Logs - Journaux d'audit > Filtrage** de l'interface Web d'administration et est stocké dans le fichier journal *l_filter*.

1. Dans l'onglet **Configuration**, choisissez le menu **Politique de sécurité > Filtrage et NAT**.
2. Double-cliquez dans la colonne **Action** de votre règle de filtrage. La fenêtre **Édition de la Règle** s'affiche.
3. Dans l'onglet **Général**, choisissez le niveau de traces **Verbeux (journal de filtrage)**.
4. Dans l'onglet **Configuration avancée >Traces**, choisissez l'emplacement de stockage des logs de la règle. Décochez **Disque** si vous ne souhaitez pas stocker ce type de logs en local.
5. Dans la zone **Configuration avancée**, cochez la case **Compter** pour produire des statistiques sur le nombre d'exécutions de la règle dans le fichier journal *l_count*.
6. Réalisez votre vérification en consultant les vues **Trafic réseau** ou **Filtrage** dans l'interface Web d'administration, ou dans le fichier */log/l_filter*.
7. Dans l'onglet **Général**, remettez le niveau de traces sur la valeur par défaut **Standard (journal de connexions)**.

# Comprendre les journaux d'audit

Les logs sont écrits dans le fichier journal correspondant.

Les journaux d'audit sont des fichiers texte au format UTF-8 respectant le standard WELF. Le format WELF est une suite d'éléments, écrits sous la forme *champ=valeur* et séparés par des espaces. Les valeurs sont éventuellement délimitées par des guillemets doubles.

Un log (ou trace) correspond à une ligne terminée par un retour chariot (CRLF).

**Exemple**

```
id=firewall time="2019-01-27 13:24:28" fw="V50XXA0G0000002" tz=+0000
startime="2011-01-27 13:24:28" pri=4 srcif="Ethernet0" srcifname="out"
ipproto=tcp proto=ssh src=192.168.0.1 srcport=54937 srcportname=ephemeral_fw
dst=192.168.1.1 dstport=22 dstportname=ssh dstname=Firewall_out action=pass
msg="Interactive connection detected" class=protocol classification=0 alarmid=85
```

Dans les sections Champs communs à tous les journaux et Champs spécifiques, la description des logs se présente de la manière suivante :

| | |
|---|---|
| **Nom du champ** | Description du champ<br>Format du champ. Exemple : « valeur brute »<br>Valeur si celle-ci est différente de la valeur brute. |

Les journaux *l_server*, *l_auth*, *l_vpn* et *l_system* contiennent des champs spécifiques au firewall Stormshield Network. Ces champs particuliers n'appartenant pas au format WELF, sont décrits dans la section Champs spécifiques.

Certains fichiers de traces, comme *l_filterstat* et *l_count*, ayant pour vocation le calcul de statistiques, comportent un grand nombre de champs spécifiques.

Ils correspondent donc à un instantané de l'état du firewall. Ils sont calculés et écrits à intervalle régulier.

## Changement d'heure

Lorsque le firewall subit un changement d'heure, une ligne spécifique est écrite dans tous les journaux.

Elle contient notamment les champs `datechange` et `duration`. La valeur de `datechange` est dans ce cas égale à « 1 » pour refléter le changement d'heure. Le champ `duration` donne quant à lui, l'écart (en secondes) entre l'heure du firewall, avant et après ce changement.

Les autres champs de ce log particulier sont communs (décrits dans la section suivante).

**Exemple**

```
id=firewall time="2019-01-01 01:00:00" fw="U800SXXXXXXXXXX" tz=+0100
startime="2019-01-01 01:00:17" datechange=1 duration=-18
```

Dans le menu **Logs - Journaux d'audit** de l'interface Web d'administration, ce log apparaît dans l'ensemble des modules, surligné en jaune.

## Champs communs à tous les journaux

| | |
|---|---|
| **id** | Type de produit.<br>Ce champ a constamment la valeur « firewall » pour les traces du Firewall. |

| | |
|---|---|
| **time** | Heure « locale » d'enregistrement de la trace dans le fichier de log (heure configurée sur le Firewall).<br>Chaîne au format « YYYY-MM-DD HH:MM:SS ».<br>Disponible depuis : SNS v1.0.0.<br>*Enregistré à*<br>Le format d'affichage dépend de la langue du système d'exploitation sur lequel est installée la suite d'administration. Exemple : « JJ/MM/AAAA » et « HH:MM:SS » pour le français ; « AAAA/MM/JJ » et « HH:MM:SS » pour l'anglais. |
| **fw** | Identifiant du Firewall. Il s'agit du nom renseigné par l'administrateur ou, par défaut, de son numéro de série.<br>Chaîne de caractères au format UTF-8.<br>Exemple : « nom_firewall » ou « V50XXXXXXXXXXX »<br>Disponible depuis : SNS v1.0.0. |
| **tz** | Décalage de l'heure du Firewall par rapport à l'heure GMT. Dépend du fuseau horaire utilisé.<br>Chaîne au format « +HHMM » ou « -HHMM ».<br>Disponible depuis : SNS v1.0.0.<br>*Décalage GMT*<br>Exemple : « gmt +01:00 » |
| **startime** | Heure « locale » du début de l'événement tracé (heure configurée sur le Firewall).<br>Chaîne au format « YYYY-MM-DD HH:MM:SS ».<br>Disponible depuis : SNS v1.0.0<br>*Date et heure*<br>Le format d'affichage dépend de la langue du système d'exploitation sur lequel est installée la suite d'administration. Exemple : « JJ/MM/AAAA » et « HH:MM:SS » pour le français ; « AAAA/MM/JJ » et « HH:MM:SS » pour l'anglais. |

## Champs spécifiques

Les champs présentés ci-après peuvent être communs à un ensemble de journaux ou propres à un journal unique.

### Champs propres aux journaux « l_filter », « l_alarm », « l_connection », « l_plugin »

Les champs décrits ci-dessous sont présentés au sein de l'interface Web d'administration du firewall dans les vues **Tous les journaux**, **Trafic réseau**, **Filtrage**, **Web**, **E-mails** et **Événements systèmes** du menu **Logs - Journaux d'audit**.

| | |
|---|---|
| **pri** | Représente le niveau d'alarme.<br>Valeurs (non personnalisables): « 0 » (emergency), « 1 » (alert), « 2 » (critical), « 3 » (error), « 4 » (warning), « 5 » (notice), « 6 » (information) ou « 7 » (debug).<br>Disponible depuis : SNS v1.0.0.<br>*Priorité* |
| **confid** | Index du Profil d'inspection de sécurité utilisé.<br>Valeur de « 0 » à « 9 ».<br>Disponible depuis : SNS v1.0.0.<br>*Config* |
| **slotlevel** | Indique le type de règle ayant déclenché la trace.<br>Valeurs : « 0 » (implicite), « 1 » (globale), ou « 2 » (locale).<br>Disponible depuis : SNS v1.0.0<br>*Niveau règles*<br>Valeurs : « Implicite », « Global » ou « Local » |

| | |
|---|---|
| **ruleid** | Numéro de la règle de filtrage appliquée.<br>Exemple : « 1 », « 2 » …<br>Disponible depuis : SNS v1.0.0.<br>*Règle* |
| **srcif** | Nom interne de l'interface source du flux.<br>Chaîne de caractères au format UTF-8. Exemple : « Ethernet0 »<br>Disponible depuis : SNS v1.0.0<br>*Interf. source (ID)* |
| **srcifname** | Nom de l'objet représentant l'interface source du flux.<br>Chaîne de caractères au format UTF-8. Exemple : « out »<br>Disponible depuis : SNS v1.0.0<br>*Interf. source* |
| **srcmac** | Adresse MAC de la machine source.<br>Peut être affichée de manière anonyme selon les droits d'accès de l'administrateur.<br>Disponible depuis : SNS v1.0.0<br>*Adresse MAC Source* |
| **ipproto** | Nom du protocole au-dessus d'IP (couche transport).<br>Chaîne de caractères au format UTF-8. Exemple : « tcp »<br>Disponible depuis : SNS v1.0.0.<br>*Protocole Internet* |
| **ipv** | Version du protocole IP utilisé dans le flux.<br>Valeurs : « 4 » ou « 6 »<br>Disponible depuis : SNS v1.0.0.<br>*Version IP* |
| **proto** | Nom du plugin associé. A défaut, nom du service standard correspondant au port de destination. Chaîne de caractères au format UTF-8. Exemple : « http », « ssh »<br>Disponible depuis : SNS v1.0.0.<br>*Protocole* |
| **src** | Adresse IP de la machine source.<br>Format décimal. Exemple : « 192.168.0.1 »<br>Peut être affichée de manière anonyme selon les droits d'accès de l'administrateur.<br>Disponible depuis : SNS v1.0.0<br>*Source* |
| **srcport** | Numéro du port TCP/UDP source.<br>Exemple : « 49753 »<br>Disponible depuis : SNS v1.0.0<br>*Port source* |
| **srcportname** | Nom du port « source » si celui-ci est connu.<br>Chaîne de caractères au format UTF-8. Exemple : « http », « ephemeral_fw_tcp »…<br>Disponible depuis : SNS v1.0.0<br>*Nom du port source* |
| **srcname** | Nom de l'objet correspondant à la machine source.<br>Chaîne de caractères au format UTF-8. Exemple : « poste_client ».<br>Peut être affiché de manière anonyme selon les droits d'accès de l'administrateur.<br>Disponible depuis : SNS v1.0.0<br>*Nom de la source* |
| **modsrc** | Adresse IP translatée de la machine source.<br>Peut être affiché de manière anonyme selon les droits d'accès de l'administrateur.<br>Format décimal. Exemple : « 192.168.0.1 »<br>Disponible depuis : SNS v1.0.0.<br>*Adresse source translatée* |
| **modsrcport** | Numéro du port source TCP/UDP translaté. Exemple : « 80 »<br>Disponible depuis : SNS v1.0.0.<br>*Port source translaté* |

| | |
|---|---|
| **dst** | Adresse IP de la machine destinataire.<br>Format décimal. Exemple : « 192.168.0.2 »<br>Disponible depuis : SNS v1.0.0.<br>*Destination* |
| **dstport** | Numéro du port TCP/UDP destination.<br>Exemple : « 22 »<br>Disponible depuis : SNS v1.0.0.<br>*Port destination* |
| **dstportname** | Nom de l'objet correspondant au port de destination.<br>Chaîne de caractères au format UTF-8. Exemple : « ssh »<br>Disponible depuis : SNS v1.0.0.<br>*Nom du port dest.* |
| **dstname** | Nom ne l'objet correspondant à l'adresse IP de la machine de destination.<br>Chaîne de caractères au format UTF-8. Exemple : « serveur_intranet »<br>Disponible depuis : SNS v1.0.0.<br>*Nom de destination* |
| **origdst** | Adresse IP originale de la machine de destination (avant translation ou application d'une connexion virtuelle).<br>Format décimal. Exemple : « 192.168.0.1 »<br>Disponible depuis : SNS v1.0.0.<br>*Destination orig.* |
| **origdstport** | Numéro du port TCP/UDP destination original (avant translation ou application d'une connexion virtuelle). Exemple : « 80 »<br>Disponible depuis : SNS v1.0.0.<br>*Port destination orig.* |
| **dstif** | Nom de l'interface de destination.<br>Chaîne de caractères au format UTF-8. Exemple : « Ethernet 1 »<br>Disponible depuis : SNS v1.0.0.<br>*Interf. dest. (ID)* |
| **dstifname** | Nom de l'objet représentant l'interface destination du flux.<br>Chaîne de caractères au format UTF-8. Exemple : « dmz1 »<br>Disponible depuis : SNS v1.0.0.<br>*Interf. dest.* |
| **user** | Utilisateur authentifié par le Firewall.<br>Chaîne de caractères au format UTF-8. Exemple : « Jean.Dupont »<br>Peut être affiché de manière anonyme selon les droits d'accès de l'administrateur.<br>Disponible depuis : SNS v1.0.0.<br>*Utilisateur* |
| **dstcontinent** | Continent auquel appartient l'adresse IP de destination de la connexion.<br>Valeur : le code ISO du continent.<br>Exemple : dstcontinent=« eu »<br>Disponible depuis : SNS v3.0.0.<br>*Continent destination* |
| **dstcountry** | Pays auquel appartient l'adresse IP de destination de la connexion.<br>Format : le code ISO du pays.<br>Exemple : dstcountry=« fr »<br>Disponible depuis : SNS v3.0.0.<br>*Pays destination* |
| **dsthostrep** | Réputation des machines cibles de la connexion. Disponible uniquement si la gestion de réputation a été activée pour les machines concernées.<br>Format : entier non borné.<br>Exemple : dsthostrep=506<br>Disponible depuis : SNS v3.0.0.<br>*Réputation des machines destination* |

| | |
|---|---|
| **dstiprep** | Réputation de l'adresse IP de destination. Disponible uniquement si cette adresse IP est publique et référencée dans la base de réputation des adresses IP.<br>Valeur : « anonymizer », « botnet », « malware », « phishing », « tor », « scanner » ou « spam ».<br>Exemple : dstiprep=« spam »<br>Disponible depuis : SNS v3.0.0.<br>*Réputation publique de l'IP en destination* |
| **srccontinent** | Continent auquel appartient l'adresse IP source de la connexion.<br>Valeur : le code ISO du continent.<br>Exemple : srccontinent=« eu »<br>Disponible depuis : SNS v3.0.0<br>*Continent source* |
| **srccountry** | Pays auquel appartient l'adresse IP source de la connexion.<br>Format : le code ISO du pays.<br>Exemple : srccountry=« fr »<br>Disponible depuis : SNS v3.0.0<br>*Pays source* |
| **srchostrep** | Réputation des machines sources de la connexion. Disponible uniquement si la gestion de réputation a été activée pour les machines concernées.<br>Format : entier non borné.<br>Exemple : srchostrep=26123<br>Disponible depuis : SNS v3.0.0<br>*Réputation des machines sources* |
| **sriprep** | Réputation de l'adresse IP source. Disponible uniquement si cette adresse IP est publique et référencée dans la base de réputation des adresses IP.<br>Valeur : « anonymizer », « botnet », « malware », « phishing », « tor », « scanner » ou « spam ».<br>Exemple : sriprep=« anonymizer,tor »<br>Disponible depuis : SNS v3.0.0<br>*Réputation publique de l'IP source* |
| **dstmac** | Adresse MAC de la machine destination.<br>Format : Valeurs hexadécimales séparées par des ":".<br>Exemple : dstmac=00:25:90:01:ce:e7<br>Disponible depuis : SNS v4.0.0<br>*Adresse MAC destination* |
| **etherproto** | Type de protocole ethernet.<br>Format : Chaîne de caractères au format UTF-8.<br>Exemple : etherproto="profinet-rt"<br>Disponible depuis : SNS v4.0.0<br>*Protocole Ethernet* |

## Champs spécifiques au journal « l_filter »

Les champs décrits ci-dessous sont présentés au sein de l'interface Web d'administration du firewall dans les vues **Tous les journaux**, **Filtrage** et **Trafic réseau** du menu **Logs - Journaux d'audit**.

| | |
|---|---|
| **sent** | Nombre d'octets émis.<br>Format décimal. Exemple : « 14623 »<br>Disponible depuis : SNS v1.0.0.<br>*Envoyé*<br>Exemple : « 13Ko » |
| **action** | Comportement associé à la règle de filtrage.<br>Valeur : « Passer» ou « Bloquer » (champ vide pour l'action Tracer).<br>*Action* |

| | |
|---|---|
| **icmpcode** | Numéro de code du message icmp.<br>Exemple : « 1 » (signifiant « Destination host unreachable » ) …<br>Disponible depuis : SNS v1.0.0.<br>*Code ICMP* |
| **icmptype** | Numéro du type du message icmp.<br>Exemple : « 3 » (signifiant « Destination unreachable »).<br>Disponible depuis : SNS v1.0.0.<br>*Type ICMP* |
| **rcvd** | Nombre d'octets reçus.<br>Format décimal. Exemple : « 23631 »<br>Disponible depuis : SNS v1.0.0.<br>*Reçu*<br>Exemple : « 23Ko » |
| **target** | Indique si le champs src ou dst correspond à la cible du paquet ayant levé l'alarme.<br>Valeurs : « src »ou « dst »<br>Disponible depuis : SNS v3.0.0. |

## Champs spécifiques au journal « l_alarm »

Les champs décrits ci-dessous sont présentés au sein de l'interface Web d'administration du firewall dans les vues **Tous les journaux**, **Alarmes**, **Événements système** et **Filtrage** du menu **Logs - Journaux d'audit**.

| | |
|---|---|
| **action** | Comportement associé à la règle de filtrage.<br>Valeur : « pass » ou « block ».<br>*Action* |
| **msg** | Message textuel expliquant l'alarme.<br>Chaîne de caractères au format UTF-8. Exemple : « Sonde de port »<br>*Message* |
| **class** | Information sur la catégorie d'appartenance de l'alarme.<br>Chaîne au format UTF-8. Exemple : « protocol », « system », « filter »…<br>*Contexte* |
| **classification** | Numéro de code indiquant l'appartenance à une catégorie d'alarmes.<br>Exemple : « 0 »<br>*Classification*<br>Exemple : « Application » |
| **pktlen** | Taille en octets du paquet réseau à l'origine d'une remontée d'alarme.<br>Exemple : « 133 »<br>*Taille du paquet* |
| **pktdumplen** | Taille en octets du paquet capturé et destiné à une analyse approfondie par un outil tiers. Cette valeur peut différer de celle du champ « pktlen ».<br>Exemple : « 133 »<br>*Taille du paquet capturé* |
| **pktdump** | Paquet réseau capturé, encodé en hexadécimal, destiné à une analyse approfondie par un outil tiers.<br>Exemple : « 450000321fd240008011c2f50a00007b0a3c033d0035c »<br>*Paquet capturé* |
| **alarmid** | Identifiant Stormshield Network de l'alarme.<br>Format décimal. Exemple : « 85 »<br>*Alarme ID* |
| **repeat** | Nombre d'occurrences de l'alarme sur un temps donné.<br>Format décimal. Exemple : « 4 »<br>Disponible depuis : SNS v1.0.0.<br>*Répétition* |

| | |
|---|---|
| **icmpcode** | Numéro de code du message icmp.<br>Exemple : « 1 » (signifiant « Destination host unreachable »).<br>Disponible depuis : SNS v1.0.0. |
| | *Code ICMP* |
| **icmptype** | Numéro du type du message icmp.<br>Exemple : « 3 » (signifiant « Destination unreachable »).<br>Disponible depuis : SNS v1.0.0. |
| | *Type ICMP* |
| **domain** | Méthode d'authentification utilisée ou annuaire LDAP auquel appartient l'utilisateur authentifié par le Firewall.<br>Chaîne de caractères au format UTF-8.<br>Exemple : domain=« documentation.stormshield.eu »<br>Disponible depuis : SNS v3.0.0. |
| | *Méthode ou annuaire* |
| **risk** | Risque lié à la connexion. Cette valeur participe au calcul du score de réputation de la machine source de la connexion.<br>Valeur : entre 1 (risque faible) et 100 (risque très élevé).<br>Exemple : risk=20<br>Disponible depuis : SNS v3.0.0. |
| | *Risque* |
| **target** | Indique si le champs src ou dst correspond à la cible du paquet ayant levé l'alarme.<br>Valeurs : « src »ou « dst »<br>Disponible depuis : SNS v3.0.0. |

## Champs spécifiques au journal « l_connection »

Les champs décrits ci-dessous sont présentés au sein de l'interface Web d'administration du firewall dans les vues **Tous les journaux**, **Trafic réseau**, **Web** et **E-mails** du menu **Logs - Journaux d'audit**.

| | |
|---|---|
| **sent** | Nombre d'octets émis.<br>Format décimal. Exemple : « 14623 »<br>Disponible depuis : SNS v1.0.0. |
| | *Envoyé*<br>Exemple : « 13Ko » |
| **rcvd** | Nombre d'octets reçus.<br>Format décimal. Exemple : « 23631 »<br>Disponible depuis : SNS v1.0.0. |
| | *Reçu*<br>Exemple : « 23Ko » |
| **duration** | Durée de la connexion en secondes.<br>Format décimal. Exemple : « 173.15 » |
| | *Durée*<br>Exemple : « 2m 53s 15 » |
| **domain** | Méthode d'authentification utilisée ou annuaire LDAP auquel appartient l'utilisateur authentifié par le Firewall.<br>Chaîne de caractères au format UTF-8.<br>Exemple : domain=« documentation.stormshield.eu »<br>Disponible depuis : SNS v3.0.0. |
| | *Méthode ou annuaire* |
| **action** | Comportement associé à la règle de filtrage.<br>Valeur : « pass » ou « block » (champ vide pour l'action Tracer). |
| | *Action* |

| | |
|---|---|
| **clientappid** | Dernière application cliente détectée sur la connexion.<br>Chaîne de caractères.<br>Exemple : clientappid=firefox<br>Disponible depuis : SNS v3.2.0. |
| | *Application cliente* |
| **serverappid** | Dernière application serveur détectée sur la connexion.<br>Chaîne de caractères.<br>Exemple : serverappid=google<br>Disponible depuis : SNS v3.2.0. |
| | *Application serveur* |

## Champs spécifiques au journal « l_plugin »

Les champs décrits ci-dessous sont présentés au sein de l'interface Web d'administration du firewall dans les vues **Tous les journaux**, **Trafic réseau**, **Web** et **E-mails** du menu **Logs - Journaux d'audit**.

| | |
|---|---|
| **sent** | Nombre d'octets émis.<br>Format décimal. Exemple : « 14623 »<br>Disponible depuis : SNS v1.0.0. |
| | *Envoyé*<br>Exemple : « 13Ko ». |
| **rcvd** | Nombre d'octets reçus.<br>Format décimal. Exemple : « 23631 »<br>Disponible depuis : SNS v1.0.0. |
| | *Reçu*<br>Exemple : « 23Ko » |
| **duration** | Durée de la connexion en secondes.<br>Format décimal. Exemple : « 173.15 » |
| | *Durée*<br>Exemple : « 2m 53s 15 » |
| **action** | Comportement associé à la règle de filtrage.<br>Valeur : « pass ». |
| | *Action* |
| **domain** | Méthode d'authentification utilisée ou annuaire LDAP auquel appartient l'utilisateur authentifié par le Firewall.<br>Chaîne de caractères au format UTF-8.<br>Exemple : domain=« documentation.stormshield.eu »<br>Disponible depuis : SNS v3.0.0. |
| | *Méthode ou annuaire* |
| **error_class** | Numéro de la classe d'erreur dans une réponse S7.<br>Format numérique.<br>Disponible depuis : SNS v2.3.0. |
| **error_code** | Code de l'erreur dans la classe d'erreur précisée dans la réponse S7.<br>Disponible depuis : SNS v2.3.0. |
| **format** | Type de message du protocole IEC104.<br>Disponible depuis : SNS v3.1.0. |
| **group** | Code du groupe « *userdata* » pour un message S7.<br>Disponible depuis : SNS v2.3.4. |
| **unit_id** | Valeur du *"Unit Id"* d'un message Modbus.<br>Exemple : « 255».<br>Disponible depuis : SNS v2.3.0. |

| | |
|---|---|
| **clientappid** | Dernière application cliente détectée sur la connexion.<br>Chaîne de caractères.<br>Exemple : clientappid=firefox<br>Disponible depuis : SNS v3.2.0.<br>*Application cliente* |
| **serverappid** | Dernière application serveur détectée sur la connexion.<br>Chaîne de caractères.<br>Exemple : serverappid=google<br>Disponible depuis : SNS v3.2.0.<br>*Application serveur* |
| **cipservicecode** | Valeur du champ « Service Code » du message CIP.<br>Chaîne de caractères au format UTF-8.<br>Exemple : cipservicecode=Get_Attribute_List<br>Disponible depuis : SNS v3.5.0. |
| **cipclassid** | Valeur du champ « Class ID » du message CIP.<br>Chaîne de caractères au format UTF-8.<br>Exemple : cipclassid=Connection_Manager_Object<br>Disponible depuis : SNS v3.5.0. |
| **version** | Valeur du champ « Version number » pour le protocole NTP.<br>Format numérique.<br>Exemple : version=4.<br>Disponible depuis : SNS v3.8.0. |
| **requestmode** | Valeur du champ « Mode » pour une requête NTP.<br>Chaîne de caractères au format UTF-8.<br>Exemple : requestmode=client.<br>Disponible depuis : SNS v3.8.0. |
| **responsemode** | Valeur du champ « Mode » pour une réponse NTP.<br>Chaîne de caractères au format UTF-8.<br>Exemple : responsemode=server.<br>Disponible depuis : SNS v3.8.0. |

### Champs supplémentaires pour le plugin FTP

| | |
|---|---|
| **groupid** | Numéro d'identifiant permettant le suivi de connexions filles.<br>Exemple : « 3 »<br>*Groupe* |
| **op** | Opération FTP effectuée.<br>Chaîne de caractères ASCII. Exemple : « RETR », « LIST »…<br>*Opération* |
| **result** | Code de retour FTP.<br>Exemple : « 0 »<br>*Résultat* |
| **arg** | Argument FTP (nom du répertoire, du fichier, …).<br>Chaîne de caractères au format UTF-8. Exemple : « fichier.txt »<br>*Argument* |

### Champs supplémentaires pour le plugin HTTP

| | |
|---|---|
| **op** | Opération HTTP effectuée.<br>Chaîne de caractères ASCII. Exemple : « GET », « PUT », « POST » …<br>*Opération* |

| | |
|---|---|
| **result** | Code de retour HTTP.<br>Exemple : « 403 », « 404 »…<br>*Résultat* |
| **arg** | Argument HTTP (url, formulaire d'un POST, …).<br>Chaîne de caractères au format UTF-8. Exemple : « / », « /page.htm »…<br>*Argument* |

### Champs supplémentaires pour le plugin EDONKEY

| | |
|---|---|
| **op** | Opération réalisée.<br>Valeur : « SENDPART ».<br>*Opération* |
| **arg** | Argument EDONKEY (nom du fichier téléchargé).<br>Chaîne de caractères au format UTF-8. Exemple : « monfic.txt »<br>*Argument* |

### Champs supplémentaires pour les plugins RTP, RTCP_MEDIA_UDP et MEDIA_TCP

| | |
|---|---|
| **groupid** | Numéro d'identifiant permettant le suivi de connexions filles.<br>Exemple : « 3 »<br>*Groupe* |
| **caller** | Identifiant de l'appelant.<br>Chaîne de caractères au format UTF-8. Exemple : « "John" <sip:193@192.168.0.1> »<br>*Appelant* |
| **callee** | Identifiant de l'appelé.<br>Chaîne de caractères au format UTF-8.<br>Exemple : « <sip:192@192.168.1.1:5060;line=g842aca6eddb2a5> »<br>*Appelé* |
| **media** | Type de flux détecté (audio, vidéo, application, …).<br>Chaîne de caractères ASCII. Exemple : « control ».<br>*Média* |

### Champs supplémentaires pour le plugin YMSG

| | |
|---|---|
| **groupid** | Numéro d'identifiant permettant le suivi de connexions filles.<br>Exemple : « 3 »<br>*Groupe* |
| **op** | Opération réalisée.<br>Valeurs supportées : « V15 Proxy Transfer » et « V15 Inline Transfer »<br>*Opération* |
| **arg** | Argument YMSG : le nom de l'utilisateur et du fichier téléchargé.<br>Chaîne de caractères au format UTF-8. Exemple : « user@filename »<br>*Argument* |

### Champs supplémentaires pour le plugin MSN

| | |
|---|---|
| **groupid** | Identifiant permettant le suivi de connexions filles.<br>Format décimal. Exemple : « 1 »<br>*Groupe* |

| | |
|---|---|
| **op** | Opération réalisée.<br>Exemple : « VER », « USR » ….<br>*Opération* |
| **arg** | Argument MSN : nom du fichier téléchargé.<br>Chaîne de caractères au format UTF-8. Exemple : « fichier.txt »<br>*Argument* |

### Champs supplémentaires pour le plugin OSCAR

| | |
|---|---|
| **groupid** | Numéro d'identifiant permettant le suivi de connexions filles.<br>Exemple : « 3 »<br>*Groupe* |
| **op** | Opération réalisée.<br>Chaîne de caractères ASCII.<br>*Opération* |
| **arg** | Nom du fichier téléchargé.<br>Chaîne de caractères au format UTF-8. Exemple : « fichier.txt »<br>*Argument* |

### Champs supplémentaires pour le plugin TFTP

| | |
|---|---|
| **groupid** | Numéro d'identifiant permettant le suivi de connexions filles.<br>Exemple : « 3 »<br>*Groupe* |
| **op** | Opération réalisée.<br>Chaîne de caractères ASCII. Exemple : « read »<br>*Opération* |
| **result** | Code de retour. Exemple : « 0 »<br>*Résultat* |
| **arg** | Nom du fichier téléchargé.<br>Chaîne de caractères au format UTF-8. Exemple : « fichier.txt »<br>*Argument* |

### Champs supplémentaires pour le plugin MODBUS

| | |
|---|---|
| **unit_id** | Numéro d'identifiant (*Unit identifier*) permettant de préciser un automate esclave.<br>Exemple : « 255 » |
| **op** | Nom de la fonction Modbus.<br>Chaîne de caractères ASCII. Exemple : « Write_Single_Register», …<br>*Opération* |
| **result** | Valeur du code de fonction de la réponse Modbus.<br>Exemple : « 5 »<br>*Résultat* |
| **msg** | Informations complémentaires lorsque le firewall met fin à une connexion MODBUS.<br>Chaîne de caractères au format UTF-8. Valeurs : « timed out » (pas de réponse reçue pour une requête émise), « connexion closed » (connexion fermée par le firewall suite à la levée d'une alarme bloquante, par exemple) ou « no request » (aucune requête liée à une réponse reçue par le firewall).<br>*Message* |

### Champs supplémentaires pour le plugin S7

| | |
|---|---|
| **op** | Valeur du code de la fonction S7.<br>Exemple : « 4 », …<br>*Opération* |
| **error_class** | Classe d'erreur retournée dans une réponse S7.<br>Exemple : « 0 »<br>Disponible depuis : SNS v2.3.0. |
| **error_code** | Code d'erreur retourné dans une réponse S7.<br>Exemple : « 0 »<br>Disponible depuis : SNS v2.3.0. |
| **group** | Numéro de groupe auquel appartient le code de fonction S7 |
| **msg** | Informations complémentaires lorsque le firewall met fin à une connexion S7.<br>Chaîne de caractères au format UTF-8. Valeurs : « timed out » (pas de réponse reçue pour une requête émise), « connexion closed » (connexion fermée par le firewall suite à la levée d'une alarme bloquante, par exemple) ou « no request » (aucune requête liée à une réponse reçue par le firewall).<br>*Message* |

## Champs spécifiques au journal « l_pvm »

Les champs décrits ci-dessous sont présentés au sein de l'interface Web d'administration du firewall dans les vues **Tous les journaux** et **Vulnérabilités** du menu **Logs - Journaux d'audit**.

| | |
|---|---|
| **pri** | Niveau d'alarme (configurable dans certains cas par l'administrateur).<br>Valeurs : « 1 » (majeure) ou « 4 » (mineure).<br>Disponible depuis : SNS v1.0.0.<br>*Priorité* |
| **src** | Adresse IP de la machine source.<br>Format décimal. Exemple : « 192.168.0.1 »<br>Peut être affichée de manière anonyme selon les droits d'accès de l'administrateur.<br>Disponible depuis : SNS v1.0.0<br>*Source* |
| **srcname** | Nom de l'objet correspondant à l'adresse IP de la machine source.<br>Chaîne de caractères au format UTF-8. Exemple : « poste_client »<br>Peut être affiché de manière anonyme selon les droits d'accès de l'administrateur.<br>Disponible depuis : SNS v1.0.0<br>*Nom de la source* |
| **ipproto** | Type de protocole réseau (renseigné uniquement si une vulnérabilité est détectée).<br>Chaîne de caractères au format UTF-8. Exemple : « tcp »<br>Disponible depuis : SNS v1.0.0.<br>*Protocole Internet* |
| **proto** | Nom du plugin associé. A défaut, nom du service standard correspondant au port (renseigné uniquement si une vulnérabilité est détectée).<br>Chaîne de caractères au format UTF-8. Exemple : « ssh »<br>Disponible depuis : SNS v1.0.0.<br>*Protocole* |
| **port** | Numéro du port (renseigné uniquement si une vulnérabilité est détectée).<br>Exemple : « 22 »<br>*Port Source* |

| | |
|---|---|
| **portname** | Service standard correspondant au numéro du port (renseigné uniquement si une vulnérabilité est détectée).<br>Chaîne de caractères au format UTF-8. Exemple : « ssh »<br>*Nom du port source* |
| **vulnid** | Identifiant unique Stormshield Network de la vulnérabilité détectée.<br>Exemple : « 132710 »<br>*ID vuln* |
| **msg** | Libellé de la vulnérabilité.<br>Chaîne de caractères au format UTF-8. Exemple : « Samba SWAT Clickjacking Vulnerability »<br>*Message* |
| **arg** | Détails sur la vulnérabilité détectée (version du service, Système d'exploitation concerné …).<br>Chaîne de caractères au format UTF-8. Exemple : « Samba_3.6.3 »<br>*Argument* |
| **product** | Produit sur lequel la vulnérabilité a été détectée.<br>Chaîne de caractères au format UTF-8. Exemple : « JRE_1.6.0_27 »<br>*Produit* |
| **service** | Service (produit possédant un port dédié) sur lequel la vulnérabilité a été détectée.<br>Chaîne de caractères au format UTF-8. Exemple : « OpenSSH_5.4 »<br>*Service* |
| **detail** | Information additionnelle sur la version du logiciel vulnérable.<br>Chaîne de caractères au format UTF-8. Exemple : « PHP_5.2.3 »<br>*Détail* |
| **family** | Nom de la famille de la vulnérabilité (Web Client, Web Serveur, Mail Client...).<br>Chaîne de caractères au format UTF-8. Exemple : « SSH », « Web Client » ….<br>*Catégorie* |
| **severity** | Niveau de sévérité intrinsèque de la vulnérabilité.<br>Valeurs : « 0 » (Information), « 1 » (Faible), « 2 » (Moyen), « 3 » (Elevé) ou « 4 » (Critique).<br>*Sévérité*<br>Valeurs : « Information », « Faible », « Moyen », « Elevé » ou « Critique ». |
| **solution** | Indique si un correctif est disponible pour corriger la vulnérabilité détectée.<br>Valeurs : « 0 » (non disponible) ou « 1 » (disponible).<br>*Solution*<br>Valeurs : « Oui » ou « Non ». |
| **remote** | Indique si la vulnérabilité peut être exploitée à distance<br>Valeurs : « 0 » (faux) ou « 1 » (vrai).<br>*Exploit*<br>Valeurs : « Local » ou « A distance ». |
| **targetclient** | Indique si l'exploitation de la vulnérabilité nécessite l'utilisation d'un client sur la machine vulnérable.<br>Valeurs : « 0 » (faux) ou « 1 » (vrai).<br>*Cible client*<br>Valeurs : « Client» ou «  ». |
| **targetserver** | Indique si l'exploitation de la vulnérabilité nécessite qu'un serveur soit installé sur la machine vulnérable.<br>Valeurs : « 0 » (faux) ou « 1 » (vrai).<br>*Cible serveur*<br>Valeurs : « Serveur» ou «  ». |

| | |
|---|---|
| **discovery** | Date de publication de la vulnérabilité par les équipes de veille (uniquement en cas de sévérité supérieure à « 0 »)<br>Chaîne au format « YYYY-MM-DD ».<br>*Découvert le*<br>Format : dépend de la langue du système d'exploitation sur lequel est installée la suite d'administration. Exemple : « JJ/MM/AAAA » et « HH:MM:SS » pour le français ;<br>« AAAA/MM/JJ » et « HH:MM:SS » pour l'anglais. |

## Champs spécifiques au journal « l_system »

Les champs décrits ci-dessous sont présentés au sein de l'interface Web d'administration du firewall dans les vues **Tous les journaux**, **VPN** et **Evènements systèmes** du menu **Logs - Journaux d'audit**.

| | |
|---|---|
| **pri** | Figée à la valeur « 5 » signifiant « notice » pour assurer la compatibilité WELF.<br>Disponible depuis : SNS v1.0.0.<br>*Priorité* |
| **src** | Adresse IP de la machine source.<br>Format décimal. Exemple : « 192.168.0.1 »<br>Peut être affichée de manière anonyme selon les droits d'accès de l'administrateur.<br>Disponible depuis : SNS v1.0.0<br>*Source* |
| **dst** | Adresse IP de la machine destinataire.<br>Format décimal. Exemple : « 192.168.0.1 »<br>Disponible depuis : SNS v1.0.0.<br>*Destination* |
| **user** | Identifiant de l'administrateur ayant exécuté la commande.<br>Chaîne de caractères au format UTF-8. Exemple : « admin »<br>Peut être affiché de manière anonyme selon les droits d'accès de l'administrateur.<br>Disponible depuis : SNS v1.0.0.<br>*Utilisateur* |
| **msg** | Message de référence à l'action.<br>Chaîne de caractères au format UTF-8. Exemple : « Agent (ssoagent) is active »<br>*Message* |
| **service** | Nom du module ayant exécuté une action.<br>Chaîne de caractères ASCII. Exemple : « SSOAgent »<br>*Service* |

## Champs spécifiques au journal « l_server »

Les champs décrits ci-dessous sont présentés au sein de l'interface Web d'administration du firewall dans la vue **Tous les journaux** du menu **Logs - Journaux d'audit**.

| | |
|---|---|
| **error** | Numéro de code de retour de la commande<br>Exemple : « 0 », « 3 »…<br>*Etat*<br>Exemple : « ok », « Auth failed »… |
| **user** | Identifiant de l'administrateur ayant exécuté la commande.<br>Chaîne de caractères au format UTF-8. Exemple : « admin »<br>Peut être affiché de manière anonyme selon les droits d'accès de l'administrateur.<br>Disponible depuis : SNS v1.0.0.<br>*Utilisateur* |

| | |
|---|---|
| **address** | Adresse IP du poste client ayant initié la connexion.<br>Format décimal.<br>Exemple : address=192.168.0.2<br>*Source* |
| **sessionid** | Numéro d'identifiant de session permettant de différencier les connexions simultanées.<br>Exemple : « 18 »<br>*Session*<br>Exemple : « 01.0018 » |
| **msg** | Commande exécutée accompagnée éventuellement de ses paramètres.<br>Chaîne de caractères au format UTF-8. Exemple : « CONFIG FILTER ACTIVATE »<br>*Message* |
| **domain** | Méthode d'authentification utilisée ou annuaire LDAP auquel appartient l'utilisateur authentifié par le Firewall.<br>Chaîne de caractères au format UTF-8.<br>Exemple : domain=« documentation.stormshield.eu »<br>Disponible depuis : SNS v3.0.0.<br>*Méthode ou annuaire* |

## Champs spécifiques au journal « l_vpn »

Les champs décrits ci-dessous sont présentés au sein de l'interface Web d'administration du firewall dans les vues **Tous les journaux** et **VPN** du menu **Journaux d'audit**.

| | |
|---|---|
| **pri** | Fixé à la valeur « 5 » (« notice ») pour assurer la compatibilité avec le format WELF.<br>Disponible depuis : SNS v1.0.0.<br>*Priorité* |
| **error** | Niveau d'erreur de la trace.<br>Valeurs : « 0 » (Information), « 1 » (Avertissement) ou « 2 » (Erreur).<br>*Résultat*<br>Exemple : « Info » |
| **phase** | Numéro de la phase de négociation du tunnel VPN IPSec.<br>Valeurs : « 0 » (pas de phase), « 1 » (phase 1) ou « 2 » (phase 2).<br>*Phase* |
| **src** | Adresse IP de l'extrémité locale du tunnel VPN.<br>Format décimal. Exemple : « 192.168.0.1 »<br>Disponible depuis : SNS v1.0.0<br>*Source* |
| **srcname** | Nom de l'objet correspondant à l'extrémité locale du tunnel VPN.<br>Chaîne de caractères au format UTF-8.<br>Exemple : « Pub_FW »<br>Disponible depuis : SNS v1.0.0<br>*Nom de la source* |
| **dst** | Adresse IP de l'extrémité distante du tunnel VPN.<br>Format décimal.<br>Exemple : « 192.168.1.1 »<br>Disponible depuis : SNS v1.0.0.<br>*Destination* |
| **dstname** | Nom ne l'objet correspondant à l'extrémité distante du tunnel VPN.<br>Chaîne de caractères au format UTF-8.<br>Exemple : « fw_distant »<br>Disponible depuis : SNS v1.0.0.<br>*Nom de destination* |

| | |
|---|---|
| **user** | Identifiant de l'utilisateur distant utilisé pour la négociation.<br>Chaîne de caractères au format UTF-8.<br>Exemple : « jean.dupont »<br>Peut être affiché de manière anonyme selon les droits d'accès de l'administrateur.<br>Disponible depuis : SNS v1.0.0.<br>*Utilisateur* |
| **usergroup** | Groupe, défini dans les droits d'accès VPN, auquel appartient l'utilisateur ayant établi un tunnel.<br>Chaîne de caractères au format UTF-8.<br>Exemple : usergroup=« ipsec-group »<br>Disponible depuis : SNS v3.3.0.<br>*Groupe* |
| **msg** | Description de l'opération réalisée.<br>Chaîne de caractères au format UTF-8. Exemple : « Phase established »<br>*Message* |
| **side** | Rôle du Firewall dans la négociation du tunnel.<br>Valeurs : « initiator » ou « responder ».<br>*Rôle* |
| **cookie_i** | Marqueur d'identité temporaire de l'initiateur de la négociation.<br>Chaine de caractères en hexadécimal. Exemple : « 0xae34785945ae3cbf »<br>*Cookie initiateur* |
| **cookie_r** | Marqueur d'identité temporaire du correspondant de la négociation.<br>Chaine de caractères en hexadécimal. Exemple : « 0x56201508549a6526 ».<br>*Cookie réception* |
| **localnet** | Réseau local négocié durant la phase2.<br>Format décimal. Exemple : « 192.168.0.1 »<br>*Réseau local* |
| **remotenet** | Réseau distant négocié durant la phase2.<br>Format décimal. Exemple : « 192.168.1.1 »<br>*Réseau distant* |
| **spi_in** | Numéro de SPI (Security Parameter Index) de la SA (Security Association) entrante négociée. Chaine de caractères en hexadécimal. Exemple : « 0x01ae58af »<br>*Spi entrant* |
| **spi_out** | Numéro de SPI de la SA sortante négociée.<br>Chaine de caractères en hexadécimal. Exemple : « 0x003d098c »<br>*Spi sortant* |
| **ike** | Version du protocole IKE utilisé.<br>Valeurs : « 1 » ou « 2 »<br>*Version IKE* |
| **remoteid** | Identifiant du correspondant utilisé lors de la négociation de l'IKE SA.<br>Il peut s'agir d'une adresse e-mail ou d'une adresse IP.<br>*Identifiant distant* |

## Champs spécifiques au journal « l_monitor »

| | |
|---|---|
| **security** | Indicateur de l'état de sécurité du Firewall.<br>Cette valeur est utilisée par l'outil de gestion de parc (Stormshield Network Unified Manager) afin d'informer sur l'état sécuritaire (alarme mineures, majeures, ...).<br>Format décimal représentant un pourcentage. |

| | |
|---|---|
| **system** | Indicateur d'état du système du Firewall.<br>Cette valeur est utilisée par l'outil de gestion de parc (Stormshield Network Unified Manager) afin d'informer sur l'état du système (RAM disponible, utilisation CPU, bande passante, interfaces, remplissage des journaux d'audit, ...).<br>Format décimal représentant un pourcentage. |
| **CPU** | Consommation CPU du Firewall :<br>• temps alloué à la gestion des processus utilisateurs,<br>• temps consommé par le noyau,<br>• temps alloué aux interruptions du système.<br>Format : 3 valeurs numériques séparées par des virgules.<br>Exemple : CPU=1,0,2<br>*Supervision du système / Consommation CPU* |
| **Pvm** | Ensemble d'indicateurs concernant le management des vulnérabilités :<br>• nombre total de vulnérabilités détectées,<br>• nombre de vulnérabilités pouvant être exploitées à distance,<br>• nombre de vulnérabilités nécessitant qu'un serveur soit installé sur la machine vulnérable pour être exploitées,<br>• nombre de vulnérabilités classées au niveau critique,<br>• nombre de vulnérabilités classées au niveau mineur,<br>• nombre de vulnérabilités classées au niveau majeur,<br>• nombre de vulnérabilités faisant l'objet d'un correctif,<br>• nombre total d'informations (tous niveaux),<br>• nombre d'informations de niveau mineur,<br>• nombre d'informations de niveau majeur,<br>• nombre de machines pour lesquelles PVM a collecté des informations,<br>Format : 11 valeurs numériques séparées par des virgules. Exemple :<br>« 0,0,0,0,0,0,0,2,0,0,2 » |
| **EthernetXX** | Indicateurs de bande passante utilisée pour chacune des interfaces réseau actives :<br>• nom de l'interface. Chaîne de caractères au format UTF-8,<br>• débit entrant (bits/seconde),<br>• débit entrant maximum sur une période donnée (bits/seconde),<br>• débit sortant (bits/seconde),<br>• débit sortant maximum sur une période donnée (bits/seconde),<br>• nombre de paquets acceptés,<br>• nombre de paquets bloqués.<br>Format : 7 valeurs séparées par des virgules.<br>Exemple : « in,61515,128648,788241,1890520,2130,21 »<br>*Supervision des interfaces / Utilisation de la bande passante*. |

**VlanXX**

Indicateurs de bande passante utilisée pour chacun des VLAN définis :

- nom du Vlan. Chaîne de caractères au format UTF-8,
- débit entrant (bits/seconde),
- débit entrant maximum sur une période donnée (bits/seconde),
- débit sortant (bits/seconde),
- débit sortant maximum sur une période donnée (bits/seconde),
- nombre de paquets acceptés,
- nombre de paquets bloqués.

Format : 7 valeurs séparées par des virgules.
Exemple : « Vlan_Servers,61515,128648,788241,1890520 »

*Supervision des interfaces / Utilisation de la bande passante*.

**QidXX**

Indicateurs de bande passante utilisée pour chacune des files d'attentes QoS :

- nom de la file d'attente. Chaîne de caractères au format UTF-8,
- débit entrant (bits/seconde),
- débit maximum entrant sur une période donnée (bits/seconde),
- débit sortant (bits/seconde),
- débit maximum sortant sur une période donnée (bits/seconde),
- nombre de paquets acceptés,
- nombre de paquets bloqués.

Format : 7 valeurs séparées par des virgules.
Exemple : « http,5467,20128,1988,11704 »

*Supervision de la QoS / Utilisation de la bande passante*.

**WifiXX**

Ne concerne que les firewalls équipés d'antennes Wi-Fi (modèles W).
Indicateurs de bande passante utilisée pour chacun des points d'accès Wi-Fi actifs :

- nom du point d'accès. Chaîne de caractères au format UTF-8,
- débit entrant (bits/seconde),
- débit entrant maximum sur une période donnée (bits/seconde),
- débit sortant (bits/seconde),
- débit sortant maximum sur une période donnée (bits/seconde),
- nombre de paquets acceptés,
- nombre de paquets bloqués.

Format : 7 valeurs séparées par des virgules.
Exemple : « Public_WiFi,61515,128648,788241,1890520,2130,21 »

**wldev0**

Ne concerne que les firewalls équipés d'antennes Wi-Fi (modèles W).
Indicateurs de bande passante utilisée par l'interface physique supportant les points d'accès Wi-Fi du firewall :

- nom de l'interface. Chaîne de caractères au format UTF-8,
- débit entrant (bits/seconde),
- débit entrant maximum sur une période donnée (bits/seconde),
- débit sortant (bits/seconde),
- débit sortant maximum sur une période donnée (bits/seconde),
- nombre de paquets acceptés,
- nombre de paquets bloqués.

Format : 7 valeurs séparées par des virgules.
Exemple : « Physic_WiFi,61515,128648,788241,1890520,2130,21 »

**sslvpnX**

Indicateurs de bande passante utilisée par le trafic VPN SSL. :

- nom de l'interface. Chaîne de caractères au format UTF-8,
- débit entrant (bits/seconde),
- débit entrant maximum sur une période donnée (bits/seconde),
- débit sortant (bits/seconde),
- débit sortant maximum sur une période donnée (bits/seconde),
- nombre de paquets acceptés,
- nombre de paquets bloqués.

sslvpn0 représente le trafic VPN SSL basé sur TCP.
sslvpn1 représente le trafic VPN SSL basé sur UDP.

Format : 7 valeurs séparées par des virgules.
Exemple : « sslvpn_udp,61515,128648,788241,1890520,2130,21 »

**ipsecXX**

Indicateurs de bande passante utilisée par les interface IPSec :

- nom de l'interface. Chaîne de caractères au format UTF-8,
- débit entrant (bits/seconde),
- débit entrant maximum sur une période donnée (bits/seconde),
- débit sortant (bits/seconde),
- débit sortant maximum sur une période donnée (bits/seconde),
- nombre de paquets acceptés,
- nombre de paquets bloqués.

ipsec représente le trafic associé à l'interface IPSec native (non virtuelle).
ipsec1, ipsec2 ... représente le trafic associé aux interfaces virtuelles IPSec définies sur le firewall.

Format : 7 valeurs séparées par des virgules.
Exemple : « Primary_VTI,61515,128648,788241,1890520,2130,21 »

| | |
|---|---|
| **aggXX** | Indicateurs de bande passante utilisée par les agrégats d'interfaces :<br>• nom de l'interface. Chaîne de caractères au format UTF-8,<br>• débit entrant (bits/seconde),<br>• débit entrant maximum sur une période donnée (bits/seconde),<br>• débit sortant (bits/seconde),<br>• débit sortant maximum sur une période donnée (bits/seconde),<br>• nombre de paquets acceptés,<br>• nombre de paquets bloqués.<br>Format : 7 valeurs séparées par des virgules.<br>Exemple : « Production_LACP,61515,128648,788241,1890520,2130,21 » |

## Champs propres aux journaux « l_smtp », « l_pop3 », « l_ftp », « l_web » et « l_ssl »

Les champs décrits ci-dessous sont présentés au sein de l'interface Web d'administration du firewall dans les vues **Tous les journaux**, **Trafic réseau**, **Web** et **E-mails** du menu **Logs - Journaux d'audit**.

| | |
|---|---|
| **contentpolicy** | Numéro de la politique de filtrage SSL utilisée.<br>Chaîne de caractères au format UTF-8. Exemple : « 3 »<br>Disponible depuis : SNS v1.0.0.<br>ID Politique |
| **pri** | Fixé à la valeur « 5 » (« notice ») pour assurer la compatibilité avec le format WELF.<br>Disponible depuis : SNS v1.0.0.<br>*Priorité* |
| **proto** | Nom du service standard correspondant au port de destination.<br>Chaîne de caractères au format UTF-8. Exemple : « smtp »<br>Disponible depuis : SNS v1.0.0.<br>*Protocole* |
| **src** | Adresse IP de la machine source.<br>Format décimal. Exemple : « 192.168.0.1 »<br>Peut être affichée de manière anonyme selon les droits d'accès de l'administrateur.<br>Disponible depuis : SNS v1.0.0<br>*Source* |
| **srcport** | Numéro de port source du service.<br>Exemple : « 51166 »<br>Disponible depuis : SNS v1.0.0<br>*Port source* |
| **srcportname** | Nom du port « source », si celui-ci est connu.<br>Chaîne de caractères au format UTF-8. Exemple : « ephemeral_fw_tcp »<br>Disponible depuis : SNS v1.0.0<br>*Nom du port source* |
| **srcname** | Nom de l'objet correspondant à la machine source.<br>Chaîne de caractères au format UTF-8. Exemple : « poste_client »<br>Peut être affiché de manière anonyme selon les droits d'accès de l'administrateur.<br>Disponible depuis : SNS v1.0.0<br>*Nom de la source* |
| **srcmac** | Adresse MAC de la machine source<br>Peut être affichée de manière anonyme selon les droits d'accès de l'administrateur.<br>*Adresse MAC Source* |

| | |
|---|---|
| **modsrc** | Adresse IP de la machine source translatée.<br>Peut être affiché de manière anonyme selon les droits d'accès de l'administrateur.<br>Format décimal. Exemple : « 192.168.15.1 »<br>Disponible depuis : SNS v1.0.0.<br>*Adresse source translatée* |
| **modsrcport** | Numéro de port source TCP/UDP translaté.<br>Exemple : « 49690 »<br>Disponible depuis : SNS v1.0.0.<br>*Port source translaté* |
| **dst** | Adresse IP de la machine destinataire.<br>Format décimal. Exemple : « 192.168.100.1 »<br>Disponible depuis : SNS v1.0.0.<br>*Destination* |
| **dstport** | Numéro de port du service destination.<br>Exemple : « 465 »<br>Disponible depuis : SNS v1.0.0.<br>*Port destination* |
| **dstportname** | Nom de l'objet correspondant au port de destination.<br>Chaîne de caractères au format UTF-8. Exemple : « smtps »<br>Disponible depuis : SNS v1.0.0.<br>*Nom du port dest.* |
| **origdst** | Adresse IP originale de la machine de destination (avant translation ou application d'une connexion virtuelle).<br>Format décimal. Exemple : « 192.168.200.1 »<br>Disponible depuis : SNS v1.0.0.<br>*Destination orig.* |
| **origdstport** | Numéro du port TCP/UDP original de destination (avant translation ou application d'une connexion virtuelle).<br>Exemple : « 465 »<br>Disponible depuis : SNS v1.0.0.<br>*Port destination orig.* |
| **sent** | Volume de données applicatives émises (octets).<br>Exemple : « 26657 »<br>Disponible depuis : SNS v1.0.0.<br>*Envoyé*<br>Exemple : « 26 Ko » |
| **rcvd** | Volume de données applicatives reçues (octets).<br>Exemple : « 26657 »<br>Disponible depuis : SNS v1.0.0.<br>*Reçu*<br>Exemple : « 26 Ko » |
| **duration** | Durée de la connexion (secondes).<br>Exemple : « 0.5 »<br>*Durée*<br>Exemple : « 500 ms » |
| **action** | Comportement associé à la règle de filtrage.<br>Valeurs : « pass » ou « block ».<br>Action |
| **risk** | Risque lié à la connexion. Cette valeur participe au calcul du score de réputation de la machine source de la connexion.<br>Valeur : entre 1 (risque faible) et 100 (risque très élevé).<br>Exemple : risk=20<br>Disponible depuis : SNS v3.0.0.<br>*Risque* |

| | |
|---|---|
| **slotlevel** | Indique le type de règle ayant déclenché la trace.<br>Valeurs : « 0 » (implicite), « 1 » (globale), ou « 2 » (locale).<br>Disponible depuis : SNS v1.0.0<br>*Niveau règles*<br>Valeurs : « Implicite », « Global » ou « Local » |
| **rulename** | Nom de la règle de filtrage appliquée<br>Chaîne de caractères<br>Exemple : rulename=« myrule »<br>Disponible depuis : SNS v3.2.0.<br>*Nom de la règle* |

## Champs spécifiques aux journaux « l_smtp », « l_pop3 », « l_ftp », « l_web »

Les champs décrits ci-dessous sont présentés au sein de l'interface Web d'administration du firewall dans les vues **Tous les journaux**, **Trafic réseau**, **Web** et **E-mails** du menu **Logs - Journaux d'audit**.

| | |
|---|---|
| **filename** | Nom du fichier analysé par l'option sandboxing.<br>Chaîne de caractères au format UTF-8. Exemple : « mydocument.doc »<br>*Nom du fichier* |
| **filetype** | Type de fichier analysé par l'option sandboxing. Il peut s'agir d'un document (traitement de texte, tableur, présentation,...), d'un fichier de type Portable Document Format (PDF - Adobe Acrobat), d'un fichier exécutable ou d'une archive.<br>Valeur : « document », « pdf », « executable », « archive ».<br>*Type de fichier* |
| **hash** | Résultat du hachage du contenu du fichier (méthode SHA2)<br>Chaîne de caractères au format UTF-8.<br>Exemple :<br>« f4d1be410a6102b9ae7d1c32612bed4f12158df3cd1ab6440a9ac0cad417446d »<br>*Hash* |
| **sandboxinglevel** | Indique sur une échelle de 0 à 100 le niveau d'infection du fichier.<br>Valeur de : «0» (clean) à «100» (malicious).<br>*Score sandboxing* |
| **sandboxing** | Classification du fichier selon l'option sandboxing.<br>Valeur : « clean », « suspicious », « malicious », « unknown », «forward », « failed ».<br><br>L'état « clean », « suspicious » ou « malicious » est retourné par sandboxing lorsque le fichier a déjà fait l'objet d'une analyse et d'une classification. L'état « unknown » est retourné lorsque le fichier concerné est inconnu de sandboxing. Dans ce cas, le fichier complet est transmis par le firewall pour analyse.<br>*Sandboxing* |

## Champs spécifiques au journal « l_smtp »

Les champs décrits ci-dessous sont présentés au sein de l'interface Web d'administration du firewall dans les vues **Tous les journaux**, **Trafic réseau** et **E-mails** du menu **Logs - Journaux d'audit**.

| | |
|---|---|
| **ruleid** | Numéro de la règle de filtrage appliquée.<br>Exemple : «  1 », «  2 » …<br>Disponible depuis : SNS v1.0.0.<br>*Règle* |

| | |
|---|---|
| ***user*** | Adresse mail de l'émetteur. Chaîne de caractères au format UTF-8.<br>Exemple : « john.doe@compagnie1.com »<br>Peut être affichée de manière anonyme selon les droits d'accès de l'administrateur.<br>Disponible depuis : SNS v1.0.0.<br>*Utilisateur* |
| **dstname** | Adresse mail du destinataire.<br>Chaîne de caractères au format UTF-8. Exemple : « john.doe@compagnie2.com »<br>Disponible depuis : SNS v1.0.0.<br>*Nom de destination* |
| **msg** | Message associé à la commande SMTP passée.<br>Chaîne de caractères au format UTF-8. Exemple : « Connection interrupted »<br>*Message* |
| **spamlevel** | Résultat du traitement Anti spam sur le message.<br>Valeurs :<br>« X » : erreur dans le traitement du message.<br>« ? » : la nature du message n'a pu être déterminée.<br>« 0 » : message non-spam.<br>« 1 », « 2 » ou « 3 » : niveau de criticité du spam, 3 étant le plus critique.<br>Disponible depuis : SNS v1.0.0<br>*Spam* |
| **virus** | Message indiquant si un virus a été détecté (l'Antivirus doit être actif)<br>Exemple : « clean »<br>*Virus*<br>Exemple : « propre » |
| **ads** | Indique si l'Anti spam a détecté un e-mail comme étant une publicité<br>Valeurs : « 0 » ou « 1 ».<br>*Publicité* |
| **dstcontinent** | Continent auquel appartient l'adresse IP de destination de la connexion.<br>Valeur : le code ISO du continent.<br>Exemple : dstcontinent=« eu »<br>Disponible depuis : SNS v3.0.0.<br>*Continent destination* |
| **dstcountry** | Pays auquel appartient l'adresse IP de destination de la connexion.<br>Format : le code ISO du pays.<br>Exemple : dstcountry=« fr »<br>Disponible depuis : SNS v3.0.0.<br>*Pays destination* |
| **dsthostrep** | Réputation de la machine cible de la connexion. Disponible uniquement si la gestion de réputation a été activée pour la machine concernée.<br>Format : entier non borné.<br>Exemple : dsthostrep=506<br>Disponible depuis : SNS v3.0.0.<br>*Réputation des machines destination* |
| **dstiprep** | Réputation de l'adresse IP de destination. Disponible uniquement si cette adresse IP est publique et référencée dans la base de réputation des adresses IP.<br>Valeur : « anonymizer », « botnet », « malware », « phishing », « tor », « scanner » ou « spam ».<br>Exemple : dstiprep=« spam »<br>Disponible depuis : SNS v3.0.0.<br>*Réputation publique de l'IP en destination* |
| **srccontinent** | Continent auquel appartient l'adresse IP source de la connexion.<br>Valeur : le code ISO du continent.<br>Exemple : srccontinent=« eu »<br>Disponible depuis : SNS v3.0.0<br>*Continent source* |

| | |
|---|---|
| **srccountry** | Pays auquel appartient l'adresse IP source de la connexion.<br>Format : le code ISO du pays.<br>Exemple : srccountry=« fr »<br>Disponible depuis : SNS v3.0.0 |
| | *Pays source* |
| **srchostrep** | Réputation de la machine source de la connexion. Disponible uniquement si la gestion de réputation a été activée pour la machine concernée.<br>Format : entier non borné.<br>Exemple : srchostrep=26123<br>Disponible depuis : SNS v3.0.0 |
| | *Réputation des machines sources* |
| **sriprep** | Réputation de l'adresse IP source. Disponible uniquement si cette adresse IP est publique et référencée dans la base de réputation des adresses IP.<br>Valeur : « anonymizer », « botnet », « malware », « phishing », « tor », « scanner » ou « spam ».<br>Exemple : sriprep=« anonymizer,tor »<br>Disponible depuis : SNS v3.0.0 |
| | *Réputation publique de l'IP source* |
| **mailruleid** | Numéro de la règle de filtrage mail appliquée.<br>Format numérique<br>Exemple : mailruleid=48<br>Disponible depuis : SNS v3.2.0. |

## Champs spécifiques au journal « l_pop3 »

Les champs décrits ci-dessous sont présentés au sein de l'interface Web d'administration du firewall dans les vues **Tous les journaux**, **Trafic réseau** et **E-mails** du menu **Logs - Journaux d'audit**.

| | |
|---|---|
| **ruleid** | Numéro de la règle de filtrage appliquée.<br>Exemple : « 1 », « 2 » …<br>Disponible depuis : SNS v1.0.0. |
| | *Règle* |
| **spamlevel** | Résultat du traitement Anti spam sur le message.<br>Valeurs :<br>« X » : erreur dans le traitement du message.<br>« ? » : la nature du message n'a pu être déterminée.<br>« 0 » : message non-spam.<br>« 1 », « 2 » ou « 3 » : niveau de criticité du spam, 3 étant le plus critique.<br>Disponible depuis : SNS v1.0.0 |
| | *Spam* |
| **op** | Opération sur le serveur POP3 (RETR, LIST, ...)<br>Exemple : « USER » |
| | *Opération* |
| **virus** | Message indiquant si un virus a été détecté (l'Antivirus doit être actif)<br>Exemple : « clean » |
| | *Virus*<br>Exemple : « propre » |
| **msg** | Message associé à la commande POP3 passée.<br>Chaîne de caractères au format UTF-8. Exemple : « Username rejected » |
| | *Message* |

| | |
|---|---|
| **user** | Login de l'utilisateur.<br>Chaîne de caractères au format UTF-8. Exemple : « jean.dupont@compagnie.com »<br>Peut être affiché de manière anonyme selon les droits d'accès de l'administrateur.<br>Disponible depuis : SNS v1.0.0. |
| | *Utilisateur* |
| **ads** | Indique si l'Anti spam a détécté un e-mail comme étant une publicité<br>Valeurs : « 0 » ou « 1 ». |
| | *Publicité* |
| **dstcontinent** | Continent auquel appartient l'adresse IP de destination de la connexion.<br>Valeur : le code ISO du continent.<br>Exemple : dstcontinent=« eu »<br>Disponible depuis : SNS v3.0.0. |
| | *Continent destination* |
| **dstcountry** | Pays auquel appartient l'adresse IP de destination de la connexion.<br>Format : le code ISO du pays.<br>Exemple : dstcountry=« fr »<br>Disponible depuis : SNS v3.0.0. |
| | *Pays destination* |
| **dsthostrep** | Réputation de la machine cible de la connexion. Disponible uniquement si la gestion de réputation a été activée pour la machine concernée.<br>Format : entier non borné.<br>Exemple : dsthostrep=506<br>Disponible depuis : SNS v3.0.0. |
| | *Réputation des machines destination* |
| **dstiprep** | Réputation de l'adresse IP de destination. Disponible uniquement si cette adresse IP est publique et référencée dans la base de réputation des adresses IP.<br>Valeur : « anonymizer », « botnet », « malware », « phishing », « tor », « scanner » ou « spam ».<br>Exemple : dstiprep=« spam »<br>Disponible depuis : SNS v3.0.0. |
| | *Réputation publique de l'IP en destination* |
| **srccontinent** | Continent auquel appartient l'adresse IP source de la connexion.<br>Valeur : le code ISO du continent.<br>Exemple : srccontinent=« eu »<br>Disponible depuis : SNS v3.0.0 |
| | *Continent source* |
| **srccountry** | Pays auquel appartient l'adresse IP source de la connexion.<br>Format : le code ISO du pays.<br>Exemple : srccountry=« fr »<br>Disponible depuis : SNS v3.0.0 |
| | *Pays source* |
| **srchostrep** | Réputation de la machine source de la connexion. Disponible uniquement si la gestion de réputation a été activée pour la machine concernée.<br>Format : entier non borné.<br>Exemple : srchostrep=26123<br>Disponible depuis : SNS v3.0.0 |
| | *Réputation des machines sources* |
| **sriprep** | Réputation de l'adresse IP source. Disponible uniquement si cette adresse IP est publique et référencée dans la base de réputation des adresses IP.<br>Valeur : « anonymizer », « botnet », « malware », « phishing », « tor », « scanner » ou « spam ».<br>Exemple : sriprep=« anonymizer,tor »<br>Disponible depuis : SNS v3.0.0 |
| | *Réputation publique de l'IP source* |

## Champs spécifiques au journal « l_ftp »

Les champs décrits ci-dessous sont présentés au sein de l'interface Web d'administration du firewall dans les vues **Tous les journaux** et **Trafic réseau** du menu **Logs - Journaux d'audit**.

| | |
|---|---|
| **arg** | Argument de la commande FTP (fichier transféré,...).<br>Chaîne de caractères au format UTF-8. Exemple : « mon_fichier.txt »<br>*Argument* |
| **op** | Opération effectuée sur le serveur FTP.<br>Exemple : « LIST », « RETR », « QUIT »....<br>*Opération* |
| **groupid** | Numéro d'indicateur de suivi de connexions filles.<br>Exemple : « 0 », « 1 », «2 »...<br>*Groupe* |
| **user** | Identifiant utilisé pour se connecter sur le serveur FTP.<br>Chaîne de caractères au format UTF-8. Exemple : « jean.dupont »<br>Peut être affiché de manière anonyme selon les droits d'accès de l'administrateur.<br>Disponible depuis : SNS v1.0.0.<br>*Utilisateur* |
| **virus** | Message indiquant si un virus a été détecté (l'antivirus doit être actif)<br>Exemple : « clean »<br>*Virus*<br>Exemple : « propre » |
| **msg** | Message d'erreur ou complément d'information sur le virus détecté.<br>Chaîne de caractères au format UTF-8. Exemple : « virus:EICAR-Test-File »<br>*Message* |

## Champs spécifiques au journal « l_web »

Les champs décrits ci-dessous sont présentés au sein de l'interface Web d'administration du firewall dans les vues **Tous les journaux**, **Trafic réseau** et **Web** du menu **Logs - Journaux d'audit**.

| | |
|---|---|
| **arg** | Argument de la commande HTTP.<br>Chaîne de caractères au format UTF-8. Exemple : « / », « /mapage.htm »...<br>*Argument* |
| **op** | Opération sur le serveur http.<br>Exemple : « GET », « PUT » ...<br>*Opération* |
| **result** | Code de retour du serveur HTTP.<br>Exemple : « 403 », « 404 »...<br>*Résultat* |
| **virus** | Message indiquant si un virus a été détecté (l'antivirus doit être actif)<br>Exemple : « clean »<br>Virus<br>Exemple : « propre » |
| **cat_site** | Catégorie web (filtrage d'URL) du site consulté.<br>Chaîne de caractères au format UTF-8.<br>Exemple : « {bank} », « {news} »...<br>Disponible depuis : SNS v1.0.0.<br>*Catégorie* |

| | |
|---|---|
| **user** | Nom de l'utilisateur (lorsque l'authentification est activée).<br>Chaîne de caractères au format UTF-8. Exemple : « Jean.Dupont »<br>Peut être affiché de manière anonyme selon les droits d'accès de l'administrateur.<br>Disponible depuis : SNS v1.0.0.<br>*Utilisateur* |
| **ruleid** | Numéro de la règle de filtrage appliquée.<br>Exemple : « 4 »<br>Disponible depuis : SNS v1.0.0.<br>*Règle* |
| **dstname** | Nom du site web cible.<br>Chaîne de caractères au format UTF-8. Exemple : « serveurweb.compagnie.com »<br>Disponible depuis : SNS v1.0.0.<br>*Nom de destination* |
| **msg** | Message complémentaire de l'action réalisée.<br>Chaîne de caractères au format UTF-8. Exemple : « Blocked url »<br>*Message* |
| **domain** | Méthode d'authentification utilisée ou annuaire LDAP auquel appartient l'utilisateur authentifié par le Firewall.<br>Chaîne de caractères au format UTF-8.<br>Exemple : domain=« documentation.stormshield.eu »<br>Disponible depuis : SNS v3.0.0.<br>*Méthode ou annuaire* |
| **dstcontinent** | Continent auquel appartient l'adresse IP de destination de la connexion.<br>Valeur : le code ISO du continent.<br>Exemple : dstcontinent=« eu »<br>Disponible depuis : SNS v3.0.0.<br>*Continent destination* |
| **dstcountry** | Pays auquel appartient l'adresse IP de destination de la connexion.<br>Format : le code ISO du pays.<br>Exemple : dstcountry=« fr »<br>Disponible depuis : SNS v3.0.0.<br>*Pays destination* |
| **dsthostrep** | Réputation de la machine cible de la connexion. Disponible uniquement si la gestion de réputation a été activée pour la machine concernée.<br>Format : entier non borné.<br>Exemple : dsthostrep=506<br>Disponible depuis : SNS v3.0.0.<br>*Réputation des machines destination* |
| **dstiprep** | Réputation de l'adresse IP de destination. Disponible uniquement si cette adresse IP est publique et référencée dans la base de réputation des adresses IP.<br>Valeur : « anonymizer », « botnet », « malware », « phishing », « tor », « scanner » ou « spam ».<br>Exemple : dstiprep=« spam »<br>Disponible depuis : SNS v3.0.0.<br>*Réputation publique de l'IP en destination* |
| **srccontinent** | Continent auquel appartient l'adresse IP source de la connexion.<br>Valeur : le code ISO du continent.<br>Exemple : srccontinent=« eu »<br>Disponible depuis : SNS v3.0.0<br>*Continent source* |
| **srccountry** | Pays auquel appartient l'adresse IP source de la connexion.<br>Format : le code ISO du pays.<br>Exemple : srccountry=« fr »<br>Disponible depuis : SNS v3.0.0<br>*Pays source* |

| | |
|---|---|
| **srchostrep** | Réputation de la machine source de la connexion. Disponible uniquement si la gestion de réputation a été activée pour la machine concernée.<br>Format : entier non borné.<br>Exemple : srchostrep=26123<br>Disponible depuis : SNS v3.0.0<br>*Réputation des machines sources* |
| **sriprep** | Réputation de l'adresse IP source. Disponible uniquement si cette adresse IP est publique et référencée dans la base de réputation des adresses IP.<br>Valeur : « anonymizer », « botnet », « malware », « phishing », « tor », « scanner » ou « spam ».<br>Exemple : srciprep=« anonymizer,tor »<br>Disponible depuis : SNS v3.0.0<br>*Réputation publique de l'IP source* |
| **urlruleid** | Numéro de la règle de filtrage d'URL appliquée.<br>Format numérique.<br>Exemple : urlruleid=12<br>Disponible depuis : SNS v3.2.0. |

## Champs spécifiques au journal « l_ssl »

Les champs décrits ci-dessous sont présentés au sein de l'interface Web d'administration du firewall dans les vues **Tous les journaux** et **Trafic réseau** du menu **Logs - Journaux d'audit**.

| | |
|---|---|
| **user** | Identifiant de l'utilisateur (lorsque la phase d'authentification est achevée).<br>Chaîne de caractères au format UTF-8. Exemple : « Jean.Dupont »<br>Peut être affiché de manière anonyme selon les droits d'accès de l'administrateur.<br>Disponible depuis : SNS v1.0.0.<br>*Utilisateur* |
| **msg** | Message associé à l'action réalisée.<br>Chaîne de caractères au format UTF-8. Exemple : « Connection not deciphered (rule matches : Nodecrypt) »<br>*Message* |
| **arg** | Informations complémentaires concernant la négociation SSL.<br>Exemple : « Subject%... Issuer%... »<br>*Argument* |
| **domain** | Méthode d'authentification utilisée ou annuaire LDAP auquel appartient l'utilisateur authentifié par le Firewall.<br>Chaîne de caractères au format UTF-8.<br>Exemple : domain=« documentation.stormshield.eu »<br>Disponible depuis : SNS v3.0.0.<br>*Méthode ou annuaire* |
| **dstcontinent** | Continent auquel appartient l'adresse IP de destination de la connexion.<br>Valeur : le code ISO du continent.<br>Exemple : dstcontinent=« eu »<br>Disponible depuis : SNS v3.0.0.<br>*Continent destination* |
| **dstcountry** | Pays auquel appartient l'adresse IP de destination de la connexion.<br>Format : le code ISO du pays.<br>Exemple : dstcountry=« fr »<br>Disponible depuis : SNS v3.0.0.<br>*Pays destination* |

| | |
|---|---|
| **dsthostrep** | Réputation de la machine cible de la connexion. Disponible uniquement si la gestion de réputation a été activée pour la machine concernée.<br>Format : entier non borné.<br>Exemple : dsthostrep=506<br>Disponible depuis : SNS v3.0.0.<br>*Réputation des machines destination* |
| **dstiprep** | Réputation de l'adresse IP de destination. Disponible uniquement si cette adresse IP est publique et référencée dans la base de réputation des adresses IP.<br>Valeur : « anonymizer », « botnet », « malware », « phishing », « tor », « scanner » ou « spam ».<br>Exemple : dstiprep=« spam »<br>Disponible depuis : SNS v3.0.0.<br>*Réputation publique de l'IP en destination* |
| **srccontinent** | Continent auquel appartient l'adresse IP source de la connexion.<br>Valeur : le code ISO du continent.<br>Exemple : srccontinent=« eu »<br>Disponible depuis : SNS v3.0.0<br>*Continent source* |
| **srccountry** | Pays auquel appartient l'adresse IP source de la connexion.<br>Format : le code ISO du pays.<br>Exemple : srccountry=« fr »<br>Disponible depuis : SNS v3.0.0<br>*Pays source* |
| **srchostrep** | Réputation de la machine source de la connexion. Disponible uniquement si la gestion de réputation a été activée pour la machine concernée.<br>Format : entier non borné.<br>Exemple : srchostrep=26123<br>Disponible depuis : SNS v3.0.0<br>*Réputation des machines sources* |
| **srciprep** | Réputation de l'adresse IP source. Disponible uniquement si cette adresse IP est publique et référencée dans la base de réputation des adresses IP.<br>Valeur : « anonymizer », « botnet », « malware », « phishing », « tor », « scanner » ou « spam ».<br>Exemple : srciprep=« anonymizer,tor »<br>Disponible depuis : SNS v3.0.0<br>*Réputation publique de l'IP source* |
| **cnruleid** | Numéro de la règle de filtrage SSL appliquée.<br>Format numérique.<br>Exemple : cnruleid=3<br>Disponible depuis : SNS v3.2.0.<br>*Règle* |

## Champs spécifiques au journal « l_auth »

Les champs décrits ci-dessous sont présentés au sein de l'interface Web d'administration du firewall dans la vue **Tous les journaux** du menu **Logs - Journaux d'audit**.

| | |
|---|---|
| **user** | Identifiant de l'utilisateur (lorsque la phase d'authentification est achevée).<br>Chaîne de caractères au format UTF-8. Exemple : « Jean.Dupont »<br>Peut être affiché de manière anonyme selon les droits d'accès de l'administrateur.<br>Disponible depuis : SNS v1.0.0.<br>*Utilisateur* |

| | |
|---|---|
| **src** | Adresse IP de la machine source.<br>Format décimal. Exemple : « 192.168.0.1 »<br>Peut être affichée de manière anonyme selon les droits d'accès de l'administrateur.<br>Disponible depuis : SNS v1.0.0 |
| | *Source* |
| **error** | Code retour de l'authentification.<br>Format décimal. Exemple : « 0 », « 3 », « 4 »…. |
| | *Etat*<br>Exemple : « ok », « Auth failed », « Level denied »… |
| **msg** | Message associé au code retour de l'authentification.<br>Chaîne de caractères au format UTF-8. Exemple : « User logged in » |
| | *Message* |
| **ruleid** | Numéro de la règle d'authentification appliquée (aucune valeur en cas de méthode « AGENT »).<br>Exemple : « 1 »<br>Disponible depuis : SNS v1.0.0. |
| | *Règle* |
| **agentid** | Identifiant de l'agent SSO.<br>Valeur : de 0 à 5.<br>Exemple : agentid=0<br>Disponible depuis : SNS v3.0.0. |
| | Agent SSO |
| **domain** | Méthode d'authentification utilisée ou annuaire LDAP auquel appartient l'utilisateur authentifié par le Firewall.<br>Chaîne de caractères au format UTF-8.<br>Exemple : domain=« documentation.stormshield.eu »<br>Disponible depuis : SNS v3.0.0. |
| | *Méthode ou annuaire* |
| **confid** | Index du Profil d'inspection de sécurité utilisé.<br>Valeur de « 0 » à « 9 ».<br>Disponible depuis : SNS v1.0.0. |

## Champs spécifiques au journal « l_xvpn »

Les champs décrits ci-dessous sont présentés au sein de l'interface Web d'administration du firewall dans les vues **Tous les journaux**, **Trafic réseau** et **VPN** du menu **Logs - Journaux d'audit**.

| | |
|---|---|
| **user** | Nom de l'utilisateur accédant au VPN-SSL.<br>Chaîne de caractères au format UTF-8. Exemple : « jean.dupont »<br>Peut être affiché de manière anonyme selon les droits d'accès de l'administrateur.<br>Disponible depuis : SNS v1.0.0. |
| | *Utilisateur* |
| **arg** | Argument de la commande émise.<br>Chaîne de caractères au format UTF-8. Exemple : « /documentation » |
| | *Argument* |
| **error** | Code retour de l'accès au VPN-SSL.<br>Exemple : « 0 », « 5 », « 8 »… |
| | *Résultat*<br>Exemple : « Success », « Access denied », « Connect to host failed »… |
| **msg** | Message associé au code retour.<br>Chaîne de caractères au format UTF-8. Exemple : « Access to host », « Bad or no cookie found »… |
| | *Message* |

| | |
|---|---|
| **src** | Adresse IP de la machine source.<br>Format décimal. Exemple : « 192.168.0.1 »<br>Peut être affichée de manière anonyme selon les droits d'accès de l'administrateur.<br>Disponible depuis : SNS v1.0.0<br>*Source* |
| **srcname** | Nom de l'objet correspondant à la machine source.<br>Chaîne de caractères au format UTF-8. Exemple : « poste_client »<br>Peut être affiché de manière anonyme selon les droits d'accès de l'administrateur.<br>Disponible depuis : SNS v1.0.0<br>*Nom de la source* |
| **localnet** | Adresse réseau utilisée par le Firewall pour établir le tunnel VPN SSL.<br>Format décimal. Exemple : « 192.168.53.2 »<br>*Réseau local* |
| **remotenet** | Adresse réseau attribuée au client pour établir le tunnel VPN SSL.<br>Format décimal. Exemple : « 192.168.53.3 »<br>*Réseau distant* |
| **dst** | Adresse IP de la machine destinataire.<br>Format décimal. Exemple : « 192.168.50.1 »<br>Disponible depuis : SNS v1.0.0.<br>*Destination* |
| **dstport** | Numéro du port de destination.<br>Format décimal. Exemple : « 80 »<br>Disponible depuis : SNS v1.0.0.<br>*Port destination* |
| **dstportname** | Nom de l'objet correspondant au port de destination.<br>Chaîne de caractères au format UTF-8. Exemple : « http »<br>Disponible depuis : SNS v1.0.0.<br>*Nom du port dest.* |
| **dstname** | Nom ne l'objet (nom FQDN) correspondant à la machine de destination.<br>Chaîne de caractères au format UTF-8. Exemple : « serveur.compagnie.com »<br>Disponible depuis : SNS v1.0.0.<br>*Nom de destination* |
| **domain** | Méthode d'authentification utilisée ou annuaire LDAP auquel appartient l'utilisateur authentifié par le Firewall.<br>Chaîne de caractères au format UTF-8.<br>Exemple : domain=« documentation.stormshield.eu »<br>Disponible depuis : SNS v3.0.0.<br>*Méthode ou annuaire* |

## Champs spécifiques au journal « l_sandboxing »

Les champs décrits ci-dessous sont présentés au sein de l'interface Web d'administration du firewall dans les vues **Tous les journaux** et **Analyse sandboxing** du menu **Logs - Journaux d'audit**.

| | |
|---|---|
| **hash** | Résultat du hachage du contenu du fichier (méthode SHA2)<br>Chaîne de caractères au format UTF-8.<br>Exemple :<br>« f4d1be410a6102b9ae7d1c32612bed4f12158df3cd1ab6440a9ac0cad417446d »<br>*Hash* |
| **sandboxinglevel** | Indique sur une échelle de 0 à 100 le niveau d'infection du fichier.<br>Valeur de : « 0 » (clean) à « 100 » (malicious).<br>*Score sandboxing* |

| | |
|---|---|
| **sandboxing** | Classification du fichier selon l'option sandboxing.<br>Valeur : « clean », « suspicious », « malicious », « unknown », «forward », « failed ».<br><br>L'état « clean », « suspicious » ou « malicious » est retourné par l'option sandboxing lorsque le fichier a déjà fait l'objet d'une analyse et d'une classification. L'état « unknown » est retourné lorsque le fichier concerné est inconnu de sandboxing. Dans ce cas, le fichier complet est transmis par le firewall pour analyse.<br>*Sandboxing* |
| **msg** | Message associé au résultat d'analyse sandboxing.<br>Chaîne de caractères au format UTF-8. Exemple : « Virus name: thisvirus ».<br>*Message* |
| **dstcontinent** | Continent auquel appartient l'adresse IP de destination de la connexion.<br>Valeur : le code ISO du continent.<br>Exemple : dstcontinent=« eu »<br>Disponible depuis : SNS v3.0.0.<br>*Continent destination* |
| **dstcountry** | Pays auquel appartient l'adresse IP de destination de la connexion.<br>Format : le code ISO du pays.<br>Exemple : dstcountry=« fr »<br>Disponible depuis : SNS v3.0.0.<br>*Pays destination* |
| **dsthostrep** | Réputation de la machine cible de la connexion. Disponible uniquement si la gestion de réputation a été activée pour la machine concernée.<br>Format : entier non borné.<br>Exemple : dsthostrep=506<br>Disponible depuis : SNS v3.0.0.<br>*Réputation des machines destination* |
| **dstiprep** | Réputation de l'adresse IP de destination. Disponible uniquement si cette adresse IP est publique et référencée dans la base de réputation des adresses IP.<br>Valeur : « anonymizer », « botnet », « malware », « phishing », « tor », « scanner » ou « spam ».<br>Exemple : dstiprep=« spam »<br>Disponible depuis : SNS v3.0.0.<br>*Réputation de l'IP en destination* |
| **risk** | Risque lié à la connexion. Cette valeur participe au calcul du score de réputation de la machine source de la connexion.<br>Valeur : entre 1 (risque faible) et 100 (risque très élevé).<br>Exemple : risk=20<br>Disponible depuis : SNS v3.0.0.<br>*Risque* |
| **srccontinent** | Continent auquel appartient l'adresse IP source de la connexion.<br>Valeur : le code ISO du continent.<br>Exemple : srccontinent=« eu »<br>Disponible depuis : SNS v3.0.0<br>*Continent source* |
| **srccountry** | Pays auquel appartient l'adresse IP source de la connexion.<br>Format : le code ISO du pays.<br>Exemple : srccountry=« fr »<br>Disponible depuis : SNS v3.0.0<br>*Pays source* |

| | |
|---|---|
| **srchostrep** | Réputation de la machine source de la connexion. Disponible uniquement si la gestion de réputation a été activée pour la machine concernée.<br>Format : entier non borné.<br>Exemple : srchostrep=26123<br>Disponible depuis : SNS v3.0.0<br>*Réputation des machines sources* |
| **srciprep** | Réputation de l'adresse IP source. Disponible uniquement si cette adresse IP est publique et référencée dans la base de réputation des adresses IP.<br>Valeur : « anonymizer », « botnet », « malware », « phishing », « tor », « scanner » ou « spam ».<br>Exemple : srciprep=« anonymizer,tor »<br>Disponible depuis : SNS v3.0.0<br>*Réputation de l'IP en source* |
| **proto** | Nom du plugin associé. A défaut, nom du service standard correspondant au port de destination. Chaîne de caractères au format UTF-8. Exemple : « http », « ssh »<br>Disponible depuis : SNS v1.0.0.<br>*Protocole* |
| **service** | Service (produit possédant un port dédié) sur lequel la vulnérabilité a été détectée. Chaîne de caractères au format UTF-8. Exemple : « OpenSSH_5.4 »<br>*Management de vulnérabilités / Service* |

## Champs spécifiques au journal « l_filterstat »

| | |
|---|---|
| **SavedEvaluation** | Nombre d'évaluations de règles n'ayant pas eu recours à la technologie de prévention d'intrusion. |
| **DynamicMem** | Pourcentage de mémoire dynamique de l'ASQ en cours d'utilisation.<br>Valeur de « 0 » à « 100 ». |
| **HostMem** | Pourcentage de la mémoire allouée à une machine traitée par le Firewall.<br>Valeur de « 0 » à « 100 ». |
| **FragMem** | Pourcentage de la mémoire allouée pour le traitement des paquets fragmentés.<br>Valeur de « 0 » à « 100 ». |
| **ICMPMem** | Pourcentage de la mémoire allouée pour le protocole ICMP.<br>Valeur de « 0 » à « 100 ». |
| **ConnMem** | Pourcentage de la mémoire allouée pour les connexions.<br>Valeur de « 0 » à « 100 ». |
| **DtrackMem** | Pourcentage de la mémoire utilisée pour le suivi des données (paquets TCP/UDP).<br>Valeur de « 0 » à « 100 ». |
| **IPStateMem** | Pourcentage de la mémoire allouée pour le traitement des pseudo-connexions liées aux protocoles autres que TCP, UDP ou ICMP (exemple : GRE) ayant transité par le firewall. |
| **IPStateConn** | Nombre de pseudo-connexions actives liées aux protocoles autres que TCP, UDP ou ICMP (exemple : GRE). |
| **IPStateConnNatDst** | Nombre de pseudo-connexions actives avec translation d'adresses sur la destination. |
| **IPStateConnNatSrc** | Nombre de pseudo-connexions actives avec translation d'adresses sur la source. |
| **IPStateConnNoNatDst** | Nombre de pseudo-connexions actives incluant explicitement une directive "No NAT" sur la destination. |
| **IPStateConnNoNatSrc** | Nombre de pseudo-connexions actives incluant explicitement une directive "No NAT" sur la source. |
| **IPStatePacket** | Nombre de paquets réseau issus de protocoles autres que TCP, UDP ou ICMP (exemple : GRE) et ayant transité par le firewall. |
| **IPStateByte** | Nombre d'octets échangés pour les pseudo-connexions. Cette valeur inclus les octets entrants et sortants. |

| | |
|---|---|
| **Logged** | Nombre de lignes de traces générées par le moteur de prévention d'intrusion. |
| **LogOverflow** | Nombre de lignes de traces n'ayant pu être générées par le moteur de prévention d'intrusion. |
| **PvmFacts** | Nombre d'événements transmis par l'ASQ au processus de management de vulnérabilités. |
| **PvmOverflow** | Nombre d'événements destinés au processus de management de vulnérabilités ayant été ignorés par l'ASQ. |
| **Accepted** | Nombre de paquets correspondant à l'application de règles passantes.<br>Exemple : Accepted=2430. |
| **Blocked** | Nombre de paquets correspondant à l'application de règles bloquantes.<br>Exemple : Blocked=1254. |
| **Byte(i/o)** | Nombre d'octets ayant transité (entrée/sortie) par le Firewall.<br>Exemple : Byte (i/o)=527894/528486. |
| **Fragmented** | Nombre de paquets fragmentés ayant transité par le Firewall. |
| **TCPPacket** | Nombre de paquets TCP ayant transité par le Firewall. |
| **TCPByte(i/o)** | Nombre d'octets TCP ayant transité (entrée/sortie) par le Firewall.<br>Exemple : TCPByte (i/o)=527894/528486. |
| **TCPConn** | Nombre de connexions TCP ayant transité par le Firewall. |
| **TCPConnNatSrc** | Nombre de connexions TCP dont la source est translatée. |
| **TCPConnNatDst** | Nombre de connexions TCP dont la destination est translatée. |
| **UDPPacket** | Nombre de paquets UDP ayant transité par le Firewall. |
| **UDPByte(i/o)** | Nombre d'octets UDP ayant transité (entrée/sortie) par le Firewall.<br>Exemple : «527894/528486» |
| **UDPConn** | Nombre de connexions UDP ayant transité par le Firewall. |
| **UDPConnNatSrc** | Nombre de connexions UDP dont la source est translatée. |
| **UDPConnNatDst** | Nombre de connexions UDP dont la destination est translatée. |
| **ICMPPacket** | Nombre de paquets ICMP ayant transité par le Firewall. |
| **ICMPByte(i/o)** | Nombre d'octets ICMP ayant transité (entrée/sortie) par le Firewall.<br>Exemple : ICMPByte(i/o) =527894/528486 |
| **HostrepScore** | Moyenne des scores de réputation des machines supervisées.<br>Valeur : entier décimal entre 0 et 65535.<br>Exemple : HostrepScore=1234<br>Disponible depuis : SNS v3.0.0. |
| **HostrepMax** | Score de réputation maximum des hosts supervisés.<br>Valeur : entier décimal entre 0 et 65535.<br>Exemple : HostrepMax=6540<br>Disponible depuis : SNS v3.0.0. |
| **HostrepRequests** | Nombre de requêtes de scores de réputation effectuées.<br>Valeur : entier décimal, non borné.<br>Exemple : HostrepRequests=445<br>Disponible depuis : SNS v3.0.0. |
| **SCTPAssocPacket** | Nombre de paquets échangés pour une association SCTP.<br>Format numérique.<br>Exemple : SCTPAssocPacket=128<br>Disponible depuis : SNS v3.9.0. |
| **SCTPAssocByte(i/o)** | Nombre d'octets (entrant / sortant) ayant transité par le firewall pour une association SCTP.<br>Format numérique.<br>Exemple : SCTPAssocByte(i/o)=9728/9576.<br>Disponible depuis : SNS v3.9.0. |
| **SCTPAssoc** | Nombre d'associations SCTP.<br>Format numérique.<br>Exemple : SCTPAssoc=2.<br>Disponible depuis : SNS v3.9.0. |

| | |
|---|---|
| **EtherStatePacket** | Nombre de paquets pour un trafic Ethernet sans couche IP.<br>Format numérique.<br>Exemple : EtherStatePacket=128<br>Disponible depuis : SNS v4.0.0. |
| **EtherStateByte(i/o)** | Nombre d'octets en (entrant / sortant) pour un trafic Ethernet sans couche IP.<br>Format numérique.<br>Exemple : EtherStateByte(i/o)=9728/9576<br>Disponible depuis : SNS v4.0.0. |
| **EtherStateConn** | Nombre d'états stateful pour des échanges de type Ethernet sans couche IP.<br>Format numérique.<br>Exemple : EtherStateConn=0<br>Disponible depuis : SNS v4.0.0. |

## Champs spécifiques au journal « l_count »

| | |
|---|---|
| **RuleX:Y** | Indique le nombre d'octets ayant transité par la règle désignée.<br>• X : correspond à une catégorie<br>  • « 0 » : règle de filtrage implicite.<br>  • « 1 » : règle de filtrage globale.<br>  • « 2 » : règle de filtrage locale.<br>  • « 3 » : règle de NAT implicite.<br>  • « 4 » : règle de NAT globale.<br>  • « 5 » : règle de NAT locale.<br>• Y : correspond au numéro de la règle dans la politique active.<br>Exemple : « Rule2:8=1612 » signifie que 1612 octets ont transité par la 8ème règle de filtrage locale de la politique active. |

documentation@stormshield.eu