NOTE TECHNIQUE

STORMSHIELD NETWORK SECURITY

DESCRIPTION DES JOURNAUX D'AUDIT (LOGS)

Produits concernés : SNS 4.8.4

Dernière mise à jour du document : 12 novembre 2024

Référence : sns-fr-description_des_journaux_d'audit_note_technique-v4

Table des matières

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 autorisées vers/depuis le firewall, non traités par un plugin applicatif. Le log est écrit à la fin de la connexion.
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.

l_date	Événements liés aux changements d'heure du firewall.
l_dmrouting	Événements liés au service de routage dynamique multicast : trafic, abonnement / désabonnement de récepteur...
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.
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).
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_routing	Événements liés au service de routage : changement de routes dynamiques, d'états d'adjacence...
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).
l_routerstat	Statistiques liées aux objets routeur (SD-WAN).

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. Le nombre de fichiers journaux conservés pour chaque catégorie de logs dépend de l'espace disque attribué à cette catégorie de journaux (module **Configuration** > **Notifications** > **Traces - Syslog - IPFIX** > onglet **Stockage Local**).

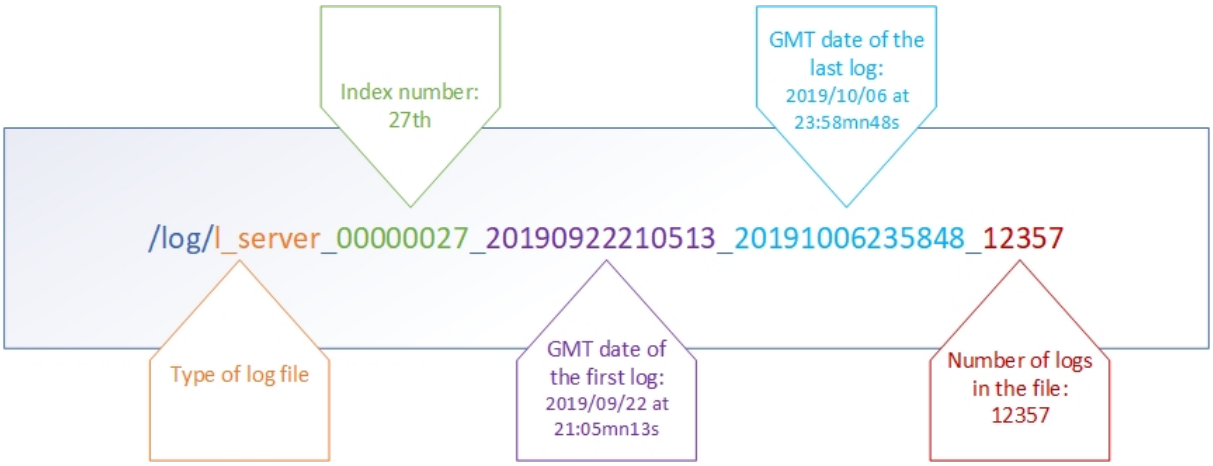
EXEMPLE
Un espace de stockage de 3,2 Go pour la catégorie de journaux VPN IPsec autorise une rétention de 160 fichiers journaux IPsec (20 Mo * 160 = 3.2 Go).

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 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 des commandes CLI / 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 concernant la syntaxe de ces commandes, veuillez vous référer au Guide de référence des commandes CLI / Serverd.

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 module **Configuration > Notifications > Traces - Syslog - IPFIX**.
- Les logs de filtrage et de NAT qui sont désactivés par défaut et que vous pouvez configurer via le module **Configuration > Politique de sécurité > Filtrage et NAT** :
  - Dans la fenêtre d'édition d'une règle de filtrage, menu **Action**, onglet *Général*, champ **Niveau de trace**,
  - Dans la fenêtre d'édition d'une règle de NAT, menu **Options**, champ **Niveau de trace**.

  Les logs de filtrage et de NAT 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. Rendez-vous dans le module **Configuration > 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. Rendez-vous dans le module **Configuration > 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 module **Monitoring > Logs - Journaux d'audit > Filtrage** de l'interface Web d'administration et est stocké dans le fichier journal *l_filter*.

1. Rendez-vous dans le module **Configuration > 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 le menu **Action** :
   - Onglet *Général*, choisissez le niveau de traces **Verbeux (journal de filtrage)**,
   - Onglet *Configuration avancée*, zone **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.
   - Onglet *Configuration avancée*, zone **Traces**, cochez la case **Compter** pour produire des statistiques sur le nombre d'exécutions de la règle dans le fichier journal *l_count*.
4. Validez l'édition de la règle en cliquant sur **OK**, puis cliquez sur **Appliquer**.
5. Réalisez votre vérification en consultant les vues **Trafic réseau** ou **Filtrage** dans l'interface Web d'administration, ou dans le fichier */log/l_filter*.
6. Dans l'onglet **Général** de la fenêtre d'édition d'une règle de filtrage, remettez le niveau de traces sur la valeur par défaut **Standard (journal de connexions)**.

Comprendre les journaux d'audit

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
```

Les champs de logs sont classés par ordre alphabétique dans les sections qui suivent. Leur description se présente de la manière suivante :

Nom du champ	Description du champ. Format du champ. Exemple : "*valeur brute*". Exemple. N° de version SNS dans laquelle est apparue le champ.
	Nom du champ dans l'interface d'administration si celui-ci diffère du nom présent dans le fichier de logs.

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 Les champs spécifiques.

Certains fichiers de traces, comme *l_filterstat* , *l_routerstat* 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 module **Logs - Journaux d'audit** de l'interface Web d'administration, ce log apparaît dans l'ensemble des modules, surligné en jaune.

Les champs spécifiques

Les journaux *l_server*, *l_auth*, *l_vpn* et *l_system* contiennent des champs spécifiques au firewall Stormshield Network.

Ces champs particuliers, qui ne sont pas au format WELF, sont décrits ci-dessous :

fw	Identifiant du firewall. Il s'agit du nom renseigné par l'administrateur ou, par défaut, de son numéro de série. Chaîne de caractères au format UTF-8. Exemple : "*nom firewall*" ou "*V50XXXXXXXXXXX*" Disponible depuis : SNS v1.0.0 Journaux concernés : l_alarm, l_auth, l_connection, l_count, l_date, l_filter, l_filterstat, l_ftp, l_monitor, l_plugin, l_pop3, l_pvm, l_sandboxing, l_server, l_smtp, l_ssl, l_system, l_vpn, l_web, l_xvpn, l_routerstat, l_dmrouting.
startime	Heure "*locale*" du début de l'événement tracé (heure configurée sur le firewall). Chaîne au format "*YYYY-MM-DD HH:MM:SS*". Disponible depuis : SNS v1.0.0 Journaux concernés : l_alarm, l_auth, l_connection, l_count, l_date, l_filter, l_filterstat, l_ftp, l_monitor, l_plugin, l_pop3, l_pvm, l_sandboxing, l_server, l_smtp, l_ssl, l_system, l_vpn, l_web, l_xvpn, l_routerstat, l_dmrouting, l_routing.
	Date et heure 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.
time	Heure "*locale*" d'enregistrement de la trace dans le fichier de log (heure configurée sur le firewall). Chaîne au format "*YYYY-MM-DD HH:MM:SS*". Disponible depuis : SNS v1.0.0 Journaux concernés : l_alarm, l_auth, l_connection, l_count, l_date, l_filter, l_filterstat, l_ftp, l_monitor, l_plugin, l_pop3, l_pvm, l_sandboxing, l_server, l_smtp, l_ssl, l_system, l_vpn, l_web, l_xvpn, l_routerstat, l_dmrouting, l_routing.
	Enregistré à 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.
tz	Décalage de l'heure du firewall par rapport à l'heure GMT. Dépend du fuseau horaire utilisé. Chaîne au format "*+HHMM*" ou "*-HHMM*". Disponible depuis : SNS v1.0.0 Journaux concernés : l_alarm, l_auth, l_connection, l_count, l_date, l_filter, l_filterstat, l_ftp, l_monitor, l_plugin, l_pop3, l_pvm, l_sandboxing, l_server, l_smtp, l_ssl, l_system, l_vpn, l_web, l_xvpn, l_routerstat, l_dmrouting, l_routing.
	Décalage GMT Exemple : "*gmt +01:00*"

Les champs classés par ordre alphabétique et leur description

A

Accepted	Nombre de paquets correspondant à l'application de règles passantes. Exemple : Accepted=2430. Journaux concernés : l_filterstat.
action	Comportement associé à la règle de filtrage. Valeur : "*Passer*" ou "*Bloquer*" (champ vide pour l'action Tracer). Exemple : action=block. Journaux concernés : l_alarm, l_connection, l_filter, l_ftp, l_plugin, l_pop3, l_smtp, l_ssl, l_web.
	Action
address	Adresse IP du poste client ayant initié la connexion. Format décimal. Exemple : address=192.168.0.2. Journaux concernés : l_server.
	Source
ads	Indique si l'Anti spam a détécté un e-mail comme étant une publicité Valeurs : « 0 » ou « 1 ». Exemple : ads=1. Journaux concernés : l_pop3, l_smtp.
	Publicité
agentid	Identifiant de l'agent SSO. Valeur : de 0 à 5. Exemple : agentid=0 Disponible depuis : SNS v3.0.0. Journaux concernés : l_auth.
	Agent SSO
aggXX	Indicateurs de bande passante utilisée par les agrégats d'interfaces : • 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 : agg01=Production LACP,61515,128648,788241,1890520,2130,21. Journaux concernés : l_monitor.

alarmid	Identifiant Stormshield Network de l'alarme. Format décimal. Exemple : "*85*". Journaux concernés : l_alarm, l_system.
	Alarme ID
arg	Argument de la commande HTTP. Chaîne de caractères au format UTF-8. Exemple : « / », « /mapage.htm »… Journaux concernés : l_ftp, l_plugin, l_pvm, l_sandboxing, l_ssl, l_web, l_xvpn.
	Argument

B

Blocked	Nombre de paquets correspondant à l'application de règles bloquantes. Exemple : Blocked=1254. Journaux concernés : l_filterstat.
Byte(i/o)	Nombre d'octets ayant transité (entrée/sortie) par le Firewall. Exemple : Byte (i/o)=527894/528486. Journaux concernés : l_filterstat.

C

caller	Identifiant de l'appelant. Chaîne de caractères au format UTF-8. Exemple : « "John" <sip:193@192.168.0.1> ». Journaux concernés = l_plugin (RTP, RTCP, Media_UDP, Media_UDP).
	Appelant
callee	Identifiant de l'appelé. Chaîne de caractères au format UTF-8. Exemple : « <sip:192@192.168.1.1:5060;line=g842aca6eddb2a5> ». Journaux concernés = l_plugin (RTP, RTCP, Media_UDP, Media_UDP).
	Appelé
cat_site	Catégorie web (filtrage d'URL) du site consulté. Chaîne de caractères au format UTF-8. Exemple : « {bank} », « {news} »… Disponible depuis : SNS v1.0.0. Journaux concernés : l_ssl, l_web.
	Catégorie
class	Information sur la catégorie d'appartenance de l'alarme. Chaîne au format UTF-8. Exemple : "*protocol*", "*system*", "*filter*", … Journaux concernés : l_alarm.
	Contexte

cipclassid	Valeur du champ "*Class ID*" du message CIP. Chaîne de caractères au format UTF-8. Exemple : cipclassid=Connection Manager Object. Disponible depuis : SNS v3.5.0. Journaux concernés : l_plugin.
cipservicecode	Valeur du champ "*Service Code*" du message CIP. Chaîne de caractères au format UTF-8. Exemple : cipservicecode=Get Attribute List. Disponible depuis : SNS v3.5.0. Journaux concernés : l_plugin.
clientappid	Dernière application cliente détectée sur la connexion. Chaîne de caractères. Exemple : clientappid=*firefox* Disponible depuis : SNS v3.2.0 Journaux concernés : l_connection, l_plugin.
	Application cliente
clientversion	Version du client VPN SSL utilisé pour établir le tunnel VPN SSL (uniquement si le *Hostchecking* est activé). Format : major.minor.build Exemple : clientversion=4.0.3 Disponible depuis : SNS v4.8.0. Journaux concernés : l_xvpn.
cnruleid	Numéro de la règle de filtrage SSL appliquée. Format numérique. Exemple : cnruleid=3. Disponible depuis : SNS v3.2.0. Journaux concernés : l_ssl.
	Règle
confid	Index du Profil d'inspection de sécurité utilisé. Valeur de « 00» à « 09 ». Exemple : confid=01. Disponible depuis : SNS v1.0.0. Journaux concernés : l_alarm, l_auth, l_connection, l_filter, l_ftp, l_plugin, l_pop3, l_smtp, l_ssl, l_web.
ConnMem	Pourcentage de la mémoire allouée pour les connexions. Valeur de « 0 » à « 100 ». Exemple : ConnMem=1. Journaux concernés : l_filterstat.
contentpolicy	Index du profil de filtrage utilisé. Valeur de « 00» à « 09 ». Exemple : contentpolicy=00 Disponible depuis : SNS v1.0.0. Journaux concernés : l_pop3, l_smtp, l_ssl, l_web.
cookie_i	Marqueur d'identité temporaire de l'initiateur de la négociation. Chaîne de caractères en hexadécimal. Exemple : cookie_i=0xae34785945ae3cbf Journaux concernés : l_vpn.
	Cookie initiateur

cookie_r	Marqueur d'identité temporaire du correspondant de la négociation. Chaîne de caractères en hexadécimal. Exemple : cookie_r=0x56201508549a6526. Journaux concernés : l_vpn.
	Cookie réception
CPU	Consommation CPU du Firewall : • temps alloué à la gestion des processus utilisateurs, • temps consommé par le noyau, • temps alloué aux interruptions du système. Format : 3 valeurs numériques séparées par des virgules. Exemple : CPU=1,0,2 Journaux concernés : l_monitor.
	Supervision du système / Consommation CPU

D

detail	Information additionnelle sur la version du logiciel vulnérable. Chaîne de caractères au format UTF-8. Exemple : detail="PHP 5.2.3". Journaux concernés : l_pvm.
	Détail
discovery	Date de publication de la vulnérabilité par les équipes de veille (uniquement en cas de sévérité supérieure à « 0 ») Chaîne au format « YYYY-MM-DD ». Exemple : discovery="2023-10-12". Journaux concernés : l_pvm.
	Découvert le 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 ; « AAAA/MM/JJ » et « HH:MM:SS » pour l'anglais.
domain	Méthode d'authentification utilisée ou annuaire LDAP auquel appartient l'utilisateur authentifié par le Firewall. Chaîne de caractères au format UTF-8. Exemple : domain=« documentation.stormshield.eu » Disponible depuis : SNS v3.0.0. Journaux concernés : l_alarm, l_auth, l_connection, l_plugin, l_server, l_ssl, l_web, l_xvpn.
	Méthode ou annuaire
downrate	Indique le pourcentage de temps pendant lequel la passerelle était en état injoignable au cours des 15 dernières minutes. Chaîne de caractères au format UTF-8. Exemple : downrate=0. Disponible depuis : SNS v4.3.0. Journaux concernés : l_routerstat.

dst	Adresse IP de la machine destinataire. Format décimal. Exemple : "*192.168.0.2*" Disponible depuis : SNS v1.0.0 Journaux concernés : l_alarm, l_connection, l_filter, l_ftp, l_plugin, l_pop3, l_sandboxing, l_smtp, l_ssl, l_vpn, l_web, l_dmrouting.
	Destination
dstcontinent	Continent auquel appartient l'adresse IP de destination de la connexion. Valeur : le code ISO du continent. Exemple : dstcontinent="eu" Disponible depuis : SNS v3.0.0. Journaux concernés : l_alarm, l_connection, l_filter, l_plugin, l_pop3, l_sandboxing, l_smtp, l_ssl, l_web.
	Continent destination
dstcountry	Pays auquel appartient l'adresse IP de destination de la connexion. Format : le code ISO du pays. Exemple : dstcountry="fr" Disponible depuis : SNS v3.0.0 Journaux concernés : l_alarm, l_connection, l_filter, l_ftp, l_plugin, l_pop3, l_sandboxing, l_smtp, l_ssl, l_vpn, l_web.
	Pays destination
dsthostrep	Réputation des machines cibles de la connexion. Disponible uniquement si la gestion de réputation a été activée pour les machines concernées. Format : entier non borné. Exemple : dsthostrep=41 Disponible depuis : SNS v3.0.0 Journaux concernés : l_alarm, l_connection, l_filter, l_plugin, l_pop3, l_sandboxing, l_smtp, l_ssl, l_web.
	Réputation des machines destination
dstif	Nom de l'interface de destination. Chaîne de caractères au format UTF-8. Exemple : dstif=Ethernet 1. Disponible depuis : SNS v1.0.0. Journaux concernés : l_alarm, l_connection, l_filter, l_plugin, l_dmrouting.
	Interf. dest. (ID)
dstifname	Nom de l'objet représentant l'interface destination du flux. Chaîne de caractères au format UTF-8. Exemple : dstifname=dmz1. Disponible depuis : SNS v1.0.0. Journaux concernés : l_alarm, l_connection, l_filter, l_plugin, l_dmrouting.
	Interf. dest.

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. Valeurs : "*anonymizer*", "*botnet*", "*malware*", "*phishing*", "*tor*", "*scanner*" ou "*spam*". Exemple : dstiprep=spam. Disponible depuis : SNS v3.0.0. Journaux concernés : l_alarm, l_connection, l_filter, l_plugin, l_pop3, l_sandboxing, l_smtp, l_ssl, l_web.
	Réputation publique de l'IP en destination
dstmac	Adresse MAC de la machine destination. Format : Valeurs hexadécimales séparées par des ":". Exemple : dstmac=00:25:90:01:ce:e7 Disponible depuis : SNS v4.0.0. Journaux concernés : l_alarm, l_connection, l_plugin.
	Adresse MAC destination
dstname	Nom ne l'objet correspondant à l'adresse IP de la machine de destination. Chaîne de caractères au format UTF-8. Exemple : dstname=intranet_server. Disponible depuis : SNS v1.0.0. Journaux concernés : l_alarm, l_connection, l_filter, l_ftp, l_plugin, l_pop3, l_sandboxing, l_smtp, l_ssl, l_vpn, l_web, l_xvpn, l_dmrouting.
	Nom de destination
dstport	Numéro du port TCP/UDP destination. Exemple : dstport=22. Disponible depuis : SNS v1.0.0. Journaux concernés : l_alarm, l_connection, l_filter, l_ftp, l_plugin, l_pop3, l_sandboxing, l_smtp, l_ssl, l_web, l_xvpn.
	Port destination
dstportname	Nom de l'objet correspondant au port de destination. Chaîne de caractères au format UTF-8. Exemple : dstportname=ssh. Disponible depuis : SNS v1.0.0. Journaux concernés : l_alarm, l_connection, l_filter, l_ftp, l_plugin, l_pop3, l_sandboxing, l_smtp, l_ssl, l_web, l_xvpn.
	Nom du port dest.
DtrackMem	Pourcentage de la mémoire utilisée pour le suivi des données (paquets TCP/UDP). Valeur de « 0 » à « 100 ». Journaux concernés : l_filterstat.
duration	Durée de la connexion en secondes. Format décimal. Exemple : "*173.15*"
	Durée Exemple : "*2m 53s 15*"
DynamicMem	Pourcentage de mémoire dynamique de l'ASQ en cours d'utilisation. Valeur de « 0 » à « 100 ». Journaux concernés : l_filterstat.

E

error	Code retour de la tentative d'authentification ou de la commande. Exemple : error=1. Journaux concernés : l_auth, l_server, l_xvpn.
	Résultat Exemple : « Success », « Access denied », « Connect to host failed »…
error_class	Numéro de la classe d'erreur dans une réponse S7. Format numérique. Exemple : error_class=0. Disponible depuis : SNS v2.3.0. Journaux concernés : l_plugin.
error_code	Code de l'erreur dans la classe d'erreur précisée dans la réponse S7. Format numérique. Exemple : error_code=0. Disponible depuis : SNS v2.3.0. Journaux concernés : l_plugin.
EthernetXX	Indicateurs de bande passante utilisée pour chacune des interfaces réseau actives : • 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 : « in,61515,128648,788241,1890520,2130,21 ». Journaux concernés : l_monitor.
	Supervision des interfaces / Utilisation de la bande passante.
etherproto	Type de protocole ethernet. Format : Chaîne de caractères au format UTF-8. Exemple : etherproto="profinet-rt" Disponible depuis : SNS v4.0.0. Journaux concernés : l_alarm, l_connection, l_plugin.
	Protocole Ethernet
EtherStateByte (i/o)	Nombre d'octets en (entrant / sortant) pour un trafic Ethernet sans couche IP. Format numérique. Exemple : EtherStateByte(i/o)=9728/9576. Disponible depuis : SNS v4.0.0. Journaux concernés : l_filterstat.
EtherStateConn	Nombre d'états stateful pour des échanges de type Ethernet sans couche IP. Format numérique. Exemple : EtherStateConn=0. Disponible depuis : SNS v4.0.0. Journaux concernés : l_filterstat.

EtherStatePacket	Nombre de paquets pour un trafic Ethernet sans couche IP. Format numérique. Exemple : EtherStatePacket=128. Disponible depuis : SNS v4.0.0. Journaux concernés : l_filterstat.

F

family	Nom de la famille de la vulnérabilité (Web Client, Web Serveur, Mail Client...). Chaîne de caractères au format UTF-8. Exemple : family=Web Client. Journaux concernés : l_pvm.
	Catégorie
filename	Nom du fichier analysé par l'option sandboxing. Chaîne de caractères au format UTF-8. Exemple : filename=«mydocument.doc». Journaux concernés : l_ftp, l_pop3, l_sandboxing, l_smtp, l_web.
	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. Valeur : « document », « pdf », « executable », « archive ». Exemple : filetype=archive. Journaux concernés : l_ftp, l_pop3, l_sandboxing, l_smtp, l_web.
	Type de fichier
format	Type de message du protocole IEC104. Caractère au format UTF-8. Exemple : format=U. Disponible depuis : SNS v3.1.0. Journaux concernés : l_plugin.
FragMem	Pourcentage de la mémoire allouée pour le traitement des paquets fragmentés. Valeur de « 0 » à « 100 ». Exemple : FragMem=2. Journaux concernés : l_filterstat.
Fragmented	Nombre de paquets fragmentés ayant transité par le Firewall. Exemple : Fragmented=12. Journaux concernés : l_filterstat.

G

gw	Nom de la passerelle supervisée. Chaîne de caractères au format UTF-8. Exemple : gw=Inet_gw. Disponible depuis : SNS v4.3.0. Journaux concernés : l_routerstat.

group	Code du groupe "*userdata*" pour un message S7. Valeur numérique. Exemple : group=4. Disponible depuis : SNS v2.3.4. Journaux concernés : l_plugin.
groupid	Numéro d'indicateur de suivi de connexions filles. Exemple : groupid=1. Journaux concernés : l_ftp, l_plugin.
	Groupe

H

hash	Résultat du hachage du contenu du fichier (méthode SHA2) Chaîne de caractères au format UTF-8. Exemple : hash= f4d1be410a6102b9ae7d1c32612bed4f12158df3cd1ab6440a9ac0cad417446d. Journaux concernés : l_ftp, l_pop3, l_sandboxing, l_smtp, l_web.
	Hash
hotschecking	État lors de l'authentification par le service VPN SSL associé au *Hostchecking*. Valeurs : • "conforming" si les exigences Hostchecking sont respectées, • "non conforming" si les exigences ne sont pas respectées, • "disabled" si le Hostchecking est désactivé. Exemple : hotschecking=conforming. Disponible depuis : SNS v4.8.0. Journaux concernés : l_xvpn.
hotscheckingdetails	Origine de l'erreur lors de l'authentification par le service VPN SSL associé au *Hostchecking.* Chaîne de caractères au format UTF-8. Exemple : hotscheckingdetails="Invalid criteria: criterion=[OsVersion]windows_version='1';". Disponible depuis : SNS v4.8.0. Journaux concernés : l_xvpn.
HostMem	Pourcentage de la mémoire allouée à une machine traitée par le Firewall. Valeur de « 0 » à « 100 ». Exemple : HostMem=4 Journaux concernés : l_filterstat.
HostrepScore	Moyenne des scores de réputation des machines supervisées. Valeur : entier décimal entre 0 et 65535. Exemple : HostrepScore=1234 Disponible depuis : SNS v3.0.0. Journaux concernés : l_filterstat.

HostrepMax	Score de réputation maximum des hosts supervisés. Valeur : entier décimal entre 0 et 65535. Exemple : HostrepMax=6540 Disponible depuis : SNS v3.0.0. Journaux concernés : l_filterstat.
HostrepRequests	Nombre de requêtes de scores de réputation effectuées. Valeur : entier décimal, non borné. Exemple : HostrepRequests=445 Disponible depuis : SNS v3.0.0. Journaux concernés : l_filterstat.

I

ICMPByte(i/o)	Nombre d'octets ICMP ayant transité (entrée/sortie) par le Firewall. Exemple : ICMPByte(i/o) =527894/528486 Journaux concernés : l_filterstat.
icmpcode	Numéro de code du message ICMP en foncion du type ICMP. Format numérique. Voir la listes des paramètres ICMP : http://www.iana.org/assignments/icmp-parameters/icmp-parameters.xhtml. Exemple : icmpcode=1 (signifiant "*Host unreachable*"). Disponible depuis : SNS v1.0.0. Journaux concernés : l_alarm, l_filter. *Code ICMP*
icmptype	Numéro du type du message ICMP. Format numérique. Voir la listes des paramètres ICMP : http://www.iana.org/assignments/icmp-parameters/icmp-parameters.xhtml. Exemple : icmptype=3 (signifiant "*Destination unreachable*"). Disponible depuis : SNS v1.0.0. Journaux concernés : l_alarm, l_filter. *Type ICMP*
ICMPMem	Pourcentage de la mémoire allouée pour le protocole ICMP. Valeur de « 0 » à « 100 ». Exemple : ICMPMem=2 Journaux concernés : l_filterstat.
ICMPPacket	Nombre de paquets ICMP ayant transité par le Firewall. Exemple : ICMPPacket=0. Journaux concernés : l_filterstat.
id	Type de produit. Ce champ a constamment la valeur "*firewall*" pour les traces du firewall. Journaux concernés : l_alarm, l_auth, l_connection, l_count, l_date, l_filter, l_filterstat, l_ftp, l_monitor, l_plugin, l_pop3, l_pvm, l_sandboxing, l_server, l_smtp, l_ssl, l_system, l_vpn, l_web, l_xvpn, l_routerstat, l_dmrouting.

ikev	Version du protocole IKE utilisé. Valeurs : « 1 » ou « 2 ». Exemple : ikev=1. Journaux concernés : l_vpn.
	Version IKE
ipproto	Nom du protocole au-dessus d'IP (couche transport). Chaîne de caractères au format UTF-8. Exemple : ipproto=tcp. Disponible depuis : SNS v1.0.0 Journaux concernés : l_alarm, l_connection, l_filter, l_plugin, l_pvm.
	Protocole Internet
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 : ipsec=ipsec,61515,128648,788241,1890520,2130,21. Journaux concernés : l_vpn.
IPStateByte (i/o)	Nombre d'octets échangés pour les pseudo-connexions. Cette valeur inclut les octets entrants et sortants. Exemple : IPStateByte(i/o)=0/40. Journaux concernés : l_filterstat.
IPStateConn	Nombre de pseudo-connexions actives liées aux protocoles autres que TCP, UDP ou ICMP (exemple : GRE). Exemple : IPStateConn=0. Journaux concernés : l_filterstat.
IPStateConnNatDst	Nombre de pseudo-connexions actives avec translation d'adresses sur la destination. Exemple : IPStateConnNatDst=0. Journaux concernés : l_filterstat.
IPStateConnNatSrc	Nombre de pseudo-connexions actives avec translation d'adresses sur la source. Exemple : IPStateConnNatSrc=0. Journaux concernés : l_filterstat.
IPStateConnNoNatDst	Nombre de pseudo-connexions actives incluant explicitement une directive "No NAT" sur la destination. Exemple : IPStateConnNoNatDst=0. Journaux concernés : l_filterstat.

IPStateConnNoNatSrc	Nombre de pseudo-connexions actives incluant explicitement une directive "No NAT" sur la source. Exemple : IPStateConnNoNatSrc=0. Journaux concernés : l_filterstat.
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. Exemple : IPStateMem=1. Journaux concernés : l_filterstat.
IPStatePacket	Nombre de paquets réseau issus de protocoles autres que TCP, UDP ou ICMP (exemple : GRE) et ayant transité par le firewall. Exemple : IPStatePacket=2. Journaux concernés : l_filterstat.
ipv	Version du protocole IP utilisé dans le flux. Valeurs : "*4*" ou "*6*". Exemple : ipv=4. Disponible depuis : SNS v1.0.0. Journaux concernés : l_alarm, l_connection, l_filter, l_ftp, l_plugin, l_pop3, l_pvm, l_smtp, l_ssl, l_web.
	Version IP

J

jitter	Indique la gigue (variation de la latence) moyenne, minimale et maximale sur un intervalle régulier dépendant de la configuration (ms). Chaîne de caractères au format UTF-8. Exemple : jitter=5,0,20. Disponible depuis : SNS v4.3.0. Journaux concernés : l_routerstat.

L

latency	Indique la latence moyenne, minimale et maximale sur un intervalle régulier dépendant de la configuration (ms). Chaîne de caractères au format UTF-8. Exemple : latency=70,50,100. Disponible depuis : SNS v4.3.0. Journaux concernés : l_routerstat.
localnet	Réseau local négocié durant la phase2. Format décimal. Exemple : localnet=192.168.0.1/24. Journaux concernés : l_vpn, l_xvpn.
	Réseau local

LogOverflow	Nombre de lignes de traces n'ayant pu être générées par le moteur de prévention d'intrusion. Exemple : LogOverflow=0. Journaux concernés : l_filterstat.
Logged	Nombre de lignes de traces générées par le moteur de prévention d'intrusion. Exemple : Logged=461634616. Journaux concernés : l_filterstat.
loopbackXX	Indicateurs de bande passante utilisée par les interfaces loopback : • 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 : loopback1=loopback1,61515,128648,788241,1890520,2130,21.
lossrate	Indique le taux moyen (%) de perte de paquets sur les 15 dernières minutes. Chaîne de caractères au format UTF-8. Exemple : lossrate=10. Disponible depuis : SNS v4.3.0. Journaux concernés : l_routerstat.

M

mailruleid	Numéro de la règle de filtrage mail appliquée. Format numérique. Exemple : mailruleid=48 Disponible depuis : SNS v3.2.0. Journaux concernés : l_smtp.
mc_cat	Catégorie d'événement multicast. Chaîne de caractères au format UTF-8. Exemple : mc_cat="receiver". Disponible depuis : SNS v4.8.0. Journaux concernés : l_dmrouting.
mc_grp	Adresse IP du groupe multicast lié à l'événement. Format décimal. Exemple : mc_grp="231.1.1.2". Disponible depuis : SNS v4.8.0. Journaux concernés : l_dmrouting.
mc_grpname	Nom de l'objet correspondant au groupe multicast lié à l'événement. Chaîne de caractères au format UTF-8. Exemple : mc_grpname="mc_ssm_test_grp". Disponible depuis : SNS v4.8.0. Journaux concernés : l_dmrouting.

mc_src	Adresse IP de la source multicast liée à l'événement. Format décimal. Exemple : mc_src="10.50.30.91". Disponible depuis : SNS v4.8.0. Journaux concernés : l_dmrouting.
mc_srcname	Nom de l'objet correspondant à la source multicast liée à l'événement. Chaîne de caractères au format UTF-8 (peut être "any"). Exemple : mc_srcname="any". Disponible depuis : SNS v4.8.0. Journaux concernés : l_dmrouting.
media	Type de flux détecté (audio, vidéo, application, …). Chaîne de caractères ASCII. Exemple : media=control. Journaux concernés : l_plugin (RTP, RTCP, Media_UDP, Media_UDP).
modsrc	Adresse IP translatée de la machine source. Peut être affiché de manière anonyme selon les droits d'accès de l'administrateur. Format décimal. Exemple : modsrc=192.168.0.1. Disponible depuis : SNS v1.0.0. Journaux concernés : l_connection, l_ftp, l_plugin, l_pop3, l_smtp, l_ssl, l_web.
	Adresse source translatée
modsrcport	Numéro de port source TCP / UDP translaté. Exemple : modsrcport=49690. Disponible depuis : SNS v1.0.0. Journaux concernés : l_connection, l_ftp, l_plugin, l_pop3, l_smtp, l_ssl, l_web.
	Port source translaté
msg	Message complémentaire. Chaîne de caractères au format UTF-8. Exemple : msg=« Access to host », msg=« Bad or no cookie found », msg=« Blocked url », msg=« Phase established » … Journaux concernés : l_alarm, l_auth, l_ftp, l_pvm, l_sandboxing, l_server, l_pop3, l_smtp, l_ssl, l_system, l_vpn, l_web, l_xvpn, l_plugin, l_dmrouting, l_routing.
	Message

O

op	Opération réalisée sur le serveur (FTP, HTTP...). Exemple : op=« GET », op=« LIST » ... Journaux associés : l_ftp, l_plugin, l_sandboxing, l_web.
	Opération

origdst	Adresse IP originale de la machine de destination (avant translation ou application d'une connexion virtuelle). Format décimal. Exemple : origdst=192.168.200.1. Disponible depuis : SNS v1.0.0. Journaux concernés : l_alarm, l_connection, l_ftp, l_plugin, l_pop3, l_smtp, l_ssl, l_web.
	Destination orig.
origdstport	Numéro du port TCP/UDP original de destination (avant translation ou application d'une connexion virtuelle). Exemple : origdstport=53. Disponible depuis : SNS v1.0.0. Journaux concernés : l_alarm, l_connection, l_ftp, l_plugin, l_pop3, l_smtp, l_ssl, l_web.
	Port destination orig.

P

phase	Numéro de la phase de négociation du tunnel VPN IPSec. Valeurs : « 0 » (pas de phase), « 1 » (phase 1) ou « 2 » (phase 2). Exemple : phase=1. Journaux concernés : l_vpn.
	Phase
pktdump	Paquet réseau capturé, encodé en hexadécimal, destiné à une analyse approfondie par un outil tiers. Exemple : pktdump="*450000321fd240008011c2f50a00007b0a3c033d0035c*". Journaux concernés : l_alarm.
	Paquet capturé
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". Exemple : pktdumplen=28. Journaux concernés : l_alarm.
	Taille du paquet capturé
pktlen	Taille en octets du paquet réseau à l'origine d'une remontée d'alarme. Exemple : pktlen=33. Journaux concernés : l_alarm.
	Taille du paquet
port	Numéro du port (renseigné uniquement si une vulnérabilité est détectée). Exemple : port=22. Journaux concernés : l_pvm.
	Port Source

portname	Service standard correspondant au numéro du port (renseigné uniquement si une vulnérabilité est détectée). Chaîne de caractères au format UTF-8. Exemple : « ssh ». Journaux concernés : l_pvm.
	Nom du port source
ppkid	Identifiant de la clé pré-partagée post-quantique (ppk) utilisée pour l'établissement du tunnel IPsec. Chaîne de caractères au format UTF-8. Exemple : « identifier of the ppk used ». Journaux concernés : l_vpn.
pri	Représente le niveau d'alarme. Valeurs (non personnalisables) : "*0*" (emergency), "*1*" (alert), "*2*" (critical), "*3*" (error), "*4*" (warning), "*5*" (notice), "*6*" (information) ou "*7*" (debug). Fixé à la valeur « 5 » (« notice ») pour assurer la compatibilité avec le format WELF dans les journaux suivants : l_smtp, l_pop3, l_ftp, l_web, l_ssl, l_system, l_vpn. Valeurs possibles : « 1 » (« alert ») ou « 4 » (« warning ») dans le journal l_pvm. Exemple : pri=1. Disponible depuis : SNS v1.0.0. Journaux concernés : l_alarm, l_connection, l_filter, l_ftp, l_plugin, l_pvm, l_pop3, l_smtp, l_ssl, l_system, l_vpn, l_web, l_routing.
	Priorité
product	Produit sur lequel la vulnérabilité a été détectée. Chaîne de caractères au format UTF-8. Exemple : product=« JRE 1.6.0_27 ». Journaux concernés : l_pvm.
	Produit
proto	Nom du service standard correspondant au port de destination. Chaîne de caractères au format UTF-8. Exemple : proto=http. Disponible depuis : SNS v1.0.0. Journaux concernés : l_alarm, l_connection, l_filter, l_ftp, l_plugin, l_pvm, l_sandboxing, l_pop3, l_smtp, l_ssl, l_web, l_routing.
	Protocole

Pvm	Ensemble d'indicateurs concernant le management des vulnérabilités : • Nombre total de vulnérabilités détectées, • Nombre de vulnérabilités pouvant être exploitées à distance, • Nombre de vulnérabilités nécessitant qu'un serveur soit installé sur la machine vulnérable pour être exploitées, • Nombre de vulnérabilités classées au niveau critique, • Nombre de vulnérabilités classées au niveau mineur, • Nombre de vulnérabilités classées au niveau majeur, • Nombre de vulnérabilités faisant l'objet d'un correctif, • Nombre total d'informations (tous niveaux), • Nombre d'informations de niveau mineur, • Nombre d'informations de niveau majeur, • Nombre de machines pour lesquelles PVM a collecté des informations, Format : 11 valeurs numériques séparées par des virgules. Exemple : « 0,0,0,0,0,0,0,2,0,0,2 ». Exemple : Pvm=1804,1588,1471,38,685,1119,1730,817,0,817,561. Journaux concernés : l_monitor.
PvmFacts	Nombre d'événements transmis par l'IPS au processus de management de vulnérabilités. Exemple : PvmFacts=0. Journaux concernés : l_filterstat.
PvmOverflow	Nombre d'événements destinés au processus de management de vulnérabilités ayant été ignorés par l'IPS. Exemple : PvmOverflow=1. Journaux concernés : l_filterstat.

Q

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 ». Journaux concernés : l_monitor. *Supervision de la QoS / Utilisation de la bande passante*.

R

rcvd	Nombre d'octets reçus. Format décimal. Exemple : rcvd=23631. Disponible depuis : SNS v1.0.0 Journaux concernés : l_connection, l_filter, l_ftp, l_plugin, l_pop3, l_smtp, l_ssl, l_web.
	Reçu Exemple : "*23 Ko*"
remote	Indique si la vulnérabilité peut être exploitée à distance Valeurs : « 0 » (faux) ou « 1 » (vrai). Exemple : remote=1. Journaux concernés : l_pvm.
	Exploit Valeurs : « Local » ou « A distance ».
remoteid	Identifiant du correspondant utilisé lors de la négociation de l'IKE SA. Il peut s'agir d'une adresse e-mail ou d'une adresse IP. Exemple : remoteid=10.3.0.202. Journaux concernés : l_vpn.
	Identifiant distant
remotenet	Adresse réseau du correspondant. Format décimal. Exemple : « 192.168.53.3 ». Journaux concernés : l_vpn, l_xvpn.
	Réseau distant
repeat	Nombre d'occurrences de l'alarme sur un temps donné. Format décimal. Exemple : repeat=4. Disponible depuis : SNS v1.0.0. Journaux concernés : l_alarm.
	Répétition
requestmode	Valeur du champ "*Mode*" pour une requête NTP. Chaîne de caractères au format UTF-8. Exemple : requestmode=client. Disponible depuis : SNS v3.8.0. Journaux concernés : l_plugin.
responsemode	Valeur du champ "*Mode*" pour une réponse NTP. Chaîne de caractères au format UTF-8. Exemple : responsemode=server. Disponible depuis : SNS v3.8.0. Journaux concernés : l_plugin.
result	Code de retour du serveur ou code de retour d'une fonction (exemple : protocole Modbus). Exemple : result=403. Journaux concernés :
	Résultat

risk	Risque lié à la connexion. Cette valeur participe au calcul du score de réputation de la machine source de la connexion. Valeur : entre 1 (risque faible) et 100 (risque très élevé). Exemple : risk=20. Disponible depuis : SNS v3.0.0. Journaux concernés : l_alarm, l_ftp, l_pop3, l_sandboxing, l_smtp, l_ssl, l_web.
	Risque
router	Nom du routeur supervisé. Chaîne de caractères au format UTF-8. Exemple : router=routerICMP. Disponible depuis : SNS v4.3.0. Journaux concernés : l_routerstat.
rt	Nom de la passerelle utilisée pour la connexion. Présent seulement si la passerelle ne correspond pas à la route par défaut. Chaîne de caractères au format UTF-8. Exemple : rt="my_gateway". Disponible depuis : SNS v4.3.0. Journaux concernés : l_alarm, l_connection, l_filter, l_plugin.
rtname	Nom de l'objet routeur utilisé pour la connexion. Présent seulement si le routeur ne correspond pas à la route par défaut. Chaîne de caractères au format UTF-8. Exemple : rtname="my_router". Disponible depuis : SNS v4.3.0. Journaux concernés : l_alarm, l_connection, l_filter, l_plugin.

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

ruleid	Numéro de la règle de filtrage ou d'authentification (journal l_auth) appliquée. Exemple : ruleid=4. Disponible depuis : SNS v1.0.0. Journaux concernés : l_alarm, l_auth, l_connection, l_filter, l_plugin, l_pop3, l_smtp, l_ssl, l_web.
	Règle

rulename	Nom de la règle de filtrage appliquée. Chaîne de caractères. Exemple : rulename=« myrule ». Disponible depuis : SNS v3.2.0. Journaux concernés : l_pop3, l_smtp, l_ssl, l_web, l_ftp.
	Nom de la règle
ruletype	Type de règle IPSec utilisée. Chaîne de caractères. Valeurs : « mobile », « gateway ». Exemple : ruletype=mobile. Disponible depuis : SNS v4.2. Journaux concernés : l_vpn.

S

sandboxing	Classification du fichier selon l'option sandboxing. Valeur : « clean », « suspicious », « malicious », « unknown », «forward », « failed ». 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. Exemple : sandboxing=forward. Journaux concernés : l_ftp, l_sandboxing, l_pop3, l_smtp, l_web.
	Sandboxing
sandboxinglevel	Indique sur une échelle de 0 à 100 le niveau d'infection du fichier. Valeur : de «0» (clean) à «100» (malicious). Exemple : sandboxinglevel=20. Journaux concernés : l_ftp, l_sandboxing, l_pop3, l_smtp.
	Score sandboxing
SavedEvaluation	Nombre d'évaluations de règles n'ayant pas eu recours à la technologie de prévention d'intrusion. Exemple : SavedEvaluation=2. Journaux concernés : l_filterstat.
SCTPAssoc	Nombre d'associations SCTP. Format numérique. Exemple : SCTPAssoc=2. Disponible depuis : SNS v3.9.0. Journaux concernés : l_filterstat.
SCTPAssocByte (i/o)	Nombre d'octets (entrant / sortant) ayant transité par le firewall pour une association SCTP. Format numérique. Exemple : SCTPAssocByte(i/o)=9728/9576. Disponible depuis : SNS v3.9.0. Journaux concernés : l_filterstat.

SCTPAssocPacket	Nombre de paquets échangés pour une association SCTP. Format numérique. Exemple : SCTPAssocPacket=128 Disponible depuis : SNS v3.9.0. Journaux concernés : l_filterstat.
security	Indicateur de l'état de sécurité du Firewall. 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, ...). Format décimal représentant un pourcentage. Exemple : security=70. Journaux concernés : l_monitor.
sent	Nombre d'octets émis sur la connexion. Format décimal. Exemple : sent=14623. Disponible depuis : SNS v1.0.0. Journaux concernés : l_connection, l_filter, l_ftp, l_plugin, l_pop3, l_smtp, l_ssl, l_web.
	Envoyé Exemple : "*13 Ko*"
serverappid	Dernière application serveur détectée sur la connexion. Chaîne de caractères. Exemple : serverappid=google. Disponible depuis : SNS v3.2.0. Journaux concernés : l_connection, l_plugin.
	Application serveur
service	Nom du module ayant exécuté une action. Chaîne de caractères ASCII. Exemple : service=« SSOAgent ». Journaux concernés : l_pvm, l_sandboxing, l_system, l_routing.
	Service
sessionid	Numéro d'identifiant de session permettant de différencier les connexions simultanées. Exemple : sessionid=18. Journaux concernés : l_server.
	Session Exemple : « 01.0018 »
severity	Niveau de sévérité intrinsèque de la vulnérabilité. Valeurs : « 0 » (Information), « 1 » (Faible), « 2 » (Moyen), « 3 » (Élevé) ou « 4 » (Critique). Exemple : severity=3. Journaux concernés : l_pvm.
	Sévérité Valeurs : « Information », « Faible », « Moyen », « Élevé» ou « Critique ».
side	Rôle du Firewall dans la négociation du tunnel. Valeurs : « initiator » ou « responder ». Exemple : side=initiator. Journaux concernés : l_vpn.
	Rôle

slotlevel	Indique le type de règle ayant déclenché la trace. Valeurs : « 0 » (implicite), « 1 » (globale), ou « 2 » (locale). Exemple : slotlevel=1. Disponible depuis : SNS v1.0.0 Journaux concernés : l_alarm, l_connection, l_filter, l_ftp, l_plugin, l_pop3, l_smtp, l_ssl, l_web.
	Niveau règles Valeurs : « Implicite », « Global » ou « Local »
solution	Indique si un correctif est disponible pour corriger la vulnérabilité détectée. Valeurs : « 0 » (non disponible) ou « 1 » (disponible). Exemple : solution=1. Journaux concernés : l_pvm.
	Solution Valeurs : « Oui » ou « Non ».
spamlevel	Résultat du traitement Antispam sur le message. Valeurs : « X » : erreur dans le traitement du message. « ? » : la nature du message n'a pu être déterminée. « 0 » : message non-spam. « 1 », « 2 » ou « 3 » : niveau de criticité du spam, 3 étant le plus critique. Disponible depuis : SNS v1.0.0
	Spam
spi_in	Numéro de SPI (Security Parameter Index) de la SA (Security Association) entrante négociée. Chaine de caractères en hexadécimal. Exemple : spi_in=0x01ae58af. Journaux concernés : l_vpn.
	Spi entrant
spi_out	Numéro de SPI de la SA sortante négociée. Chaine de caractères en hexadécimal. Exemple : spi_out=0x003d098c. Journaux concernés : l_vpn.
	Spi sortant
src	Adresse IP de la machine source. Format décimal. Exemple : src=192.168.0.1. Peut être affichée de manière anonyme selon les droits d'accès de l'administrateur. Disponible depuis : SNS v1.0.0. Journaux concernés : l_alarm, l_auth, l_connection, l_filter, l_ftp, l_plugin, l_pop3, l_pvm, l_sandboxing, l_smtp, l_ssl, l_vpn, l_web, l_xvpn, l_dmrouting.
	Source
srccontinent	Continent auquel appartient l'adresse IP source de la connexion. Valeur : le code ISO du continent. Exemple : srccontinent=« eu » Disponible depuis : SNS v3.0.0. Journaux concernés : l_alarm, l_connection, l_filter, l_plugin, l_pop3, l_sandboxing, l_smtp, l_ssl, l_web.
	Continent source

srccountry	Pays auquel appartient l'adresse IP source de la connexion. Format : le code ISO du pays. Exemple : srccountry=« fr ». Disponible depuis : SNS v3.0.0. Journaux concernés : l_alarm, l_connection, l_filter, l_plugin, l_pop3, l_sandboxing, l_smtp, l_ssl, l_web.
	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. Format : entier non borné. Exemple : srchostrep=26123 Disponible depuis : SNS v3.0.0. Journaux concernés : l_alarm, l_connection, l_filter, l_plugin, l_pop3, l_sandboxing, l_smtp, l_ssl, l_web.
	Réputation des machines sources
srcif	Nom interne de l'interface source du flux. Chaîne de caractères au format UTF-8. Exemple : "Ethernet0". Disponible depuis : SNS v1.0.0. Journaux concernés : l_alarm, l_connection, l_filter, l_plugin, l_dmrouting.
	Interf. source (ID)
srcifname	Nom de l'objet représentant l'interface source du flux. Chaîne de caractères au format UTF-8. Exemple : "out" Disponible depuis : SNS v1.0.0. Journaux concernés : l_alarm, l_connection, l_filter, l_plugin, l_dmrouting.
	Interf. source
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. Valeur : « anonymizer », « botnet », « malware », « phishing », « tor », « scanner » ou « spam ». Exemple : srciprep=« anonymizer,tor ». Disponible depuis : SNS v3.0.0. Journaux concernés : l_alarm, l_connection, l_filter, l_plugin, l_pop3, l_sandboxing, l_smtp, l_ssl, l_web.
	Réputation publique de l'IP source
srcmac	Adresse MAC de la machine source Peut être affichée de manière anonyme selon les droits d'accès de l'administrateur. Exemple : srcmac=00:25:90:01:ce:e7. Journaux concernés : l_alarm, l_connection, l_filter, l_ftp, l_plugin, l_sandboxing, l_smtp, l_ssl, l_web.
	Adresse MAC Source

srcname	Nom de l'objet correspondant à la machine source. Peut être affiché de manière anonyme selon les droits d'accès de l'administrateur. Chaîne de caractères au format UTF-8. Exemple : srcname=client_laptop. Disponible depuis : SNS v1.0.0. Journaux concernés : l_alarm, l_connection, l_filter, l_ftp, l_plugin, l_pop3, l_pvm, l_sandboxing, l_smtp, l_ssl, l_vpn, l_web, l_xvpn, l_dmrouting.
	Nom de la source
srcport	Numéro de port source du service. Exemple : srcport=51166. Disponible depuis : SNS v1.0.0. Journaux concernés : l_alarm, l_connection, l_filter, l_ftp, l_plugin, l_pop3, l_sandboxing, l_smtp, l_ssl, l_web.
	Port source
srcportname	Nom du port « source », si celui-ci est connu. Chaîne de caractères au format UTF-8. Exemple : srcportname=ad2003-dyn_tcp. Disponible depuis : SNS v1.0.0. Journaux concernés : l_alarm, l_connection, l_filter, l_ftp, l_plugin, l_pop3, l_sandboxing, l_smtp, l_ssl, l_web.
	Nom du port source
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 : sslvpn1=sslvpn_udp,61515,128648,788241,1890520,2130,21. Journaux concernés : l_monitor.
system	Indicateur d'état du système du Firewall. Cette valeur est utilisée par l'outil de gestion de parc (Stormshield Management Center) afin d'informer sur l'état du système (RAM disponible, utilisation CPU, bande passante, interfaces, remplissage des journaux d'audit, ...). Format décimal représentant un pourcentage. Exemple : system=0. Journaux concernés : l_monitor.

T

target	Indique si le champs src ou dst correspond à la cible du paquet ayant levé l'alarme. Valeurs : "*src*" ou "*dst*". Exemple : target=src. Disponible depuis : SNS v3.0.0. Journaux concernés : l_alarm,l_filter.
	Cible
targetclient	Indique si l'exploitation de la vulnérabilité nécessite l'utilisation d'un client sur la machine vulnérable. Valeurs : « 0 » (faux) ou « 1 » (vrai). Exemple : targetclient=1. Journaux concernés : l_pvm.
	Cible client Valeurs : « Client» ou « ».
targetserver	Indique si l'exploitation de la vulnérabilité nécessite qu'un serveur soit installé sur la machine vulnérable. Valeurs : « 0 » (faux) ou « 1 » (vrai). Exemple : targetserver=0. Journaux concernés : l_pvm.
	Cible serveur Valeurs : « Serveur» ou « ».
TCPByte(i/o)	Nombre d'octets TCP ayant transité (entrée/sortie) par le Firewall. Exemple : TCPByte (i/o)=527894/528486. Journaux concernés : l_filterstat.
TCPConn	Nombre de connexions TCP ayant transité par le Firewall. Exemple : TCPConn=13246. Journaux concernés : l_filterstat.
TCPConnNatDst	Nombre de connexions TCP dont la destination est translatée. Exemple : TCPConnNatDst=654565. Journaux concernés : l_filterstat.
TCPConnNatSrc	Nombre de connexions TCP dont la source est translatée. Exemple : TCPConnNatSrc=3432. Journaux concernés : l_filterstat.
TCPPacket	Nombre de paquets TCP ayant transité par le Firewall. Exemple : TCPPacket=654364646. Journaux concernés : l_filterstat.
TLSCertCacheEntriesNb	Nombre d'entrées actuellement dans le cache de certificats TLS. Format numérique. Exemple : TLSCertCacheEntriesNb=3456. Disponible depuis : SNS v4.3.0. Journaux concernés : l_filterstat.

TLSCertCacheExpiredNb	Nombre d'entrées supprimées du cache de certificats TLS suite à une expiration du TTL. Format numérique. Exemple : TLSCertCacheExpiredNb=789. Disponible depuis : SNS v4.3.0. Journaux concernés : l_filterstat.
TLSCertCacheFlushedNb	Nombre d'entrées supprimées du cache de certificats TLS suite à une opération de type "flush". Format numérique. Exemple : TLSCertCacheFlushedNb=123. Disponible depuis : SNS v4.3.0. Journaux concernés : l_filterstat.
TLSCertCacheFlushOp	Nombre d'opérations de type "flush" (suppression manuelle d'entrées, ou suite à un rechargement de signatures) réalisées sur le cache de certificats TLS. Format numérique. Exemple : TLSCertCacheFlushOp=7. Disponible depuis : SNS v4.3.0. Journaux concernés : l_filterstat.
TLSCertCacheInsert	Nombre d'entrées insérées dans le cache de certificats TLS. Format numérique. Exemple : TLSCertCacheInsert=789. Disponible depuis : SNS v4.3.0. Journaux concernés : l_filterstat.
TLSCertCacheLookup (miss/total)	Nombre de recherches manquées / effectuées dans le cache de certificats TLS. Format numérique. Exemple : TLSCertCacheLookup(miss/total)=128/136. Disponible depuis : SNS v4.3.0. Journaux concernés : l_filterstat.
TLSCertCachePurgedNb	Nombre d'entrées supprimées du cache de certificats TLS suite à une opération de type "purge". Format numérique. Exemple : TLSCertCachePurgedNb=456. Disponible depuis : SNS v4.3.0. Journaux concernés : l_filterstat.
TLSCertCachePurgeOp	Nombre d'opérations de type "purge" (suppression automatique d'un pourcentage d'entrées lorsque la capacité maximale du cache est atteinte) réalisées sur le cache de certificats TLS. Format numérique. Exemple : TLSCertCachePurgeOp=4. Disponible depuis : SNS v4.3.0. Journaux concernés : l_filterstat.
totp	Indique si l'authentification a nécessité l'utilisation d'un code TOTP Valeurs : "yes" si un code TOTP a été utilisé, "no" si aucun code TOTP n'a été utilisé. Exemple : totp=yes Disponible depuis : SNS v4.5.0. Journaux concernés : l_auth, l_xvpn.
	Mot de passe à usage unique

tsagentname	Indique le nom de l'agent TS utilisé. Chaîne de caractères au format UTF-8. Exemple : tsagentname="agent_name_test" Disponible depuis : SNS v4.7.0. Journaux concernés : l_auth, l_system.

U

UDPByte(i/o)	Nombre d'octets UDP ayant transité (entrée / sortie) par le Firewall. Exemple : «527894/528486». Journaux concernés : l_filterstat.
UDPConn	Nombre de connexions UDP ayant transité par le Firewall. Exemple : UDPConn=527894. Journaux concernés : l_filterstat.
UDPConnNatDst	Nombre de connexions UDP dont la destination est translatée. Exemple : UDPConnNatDst=12. Journaux concernés : l_filterstat.
UDPConnNatSrc	Nombre de connexions UDP dont la source est translatée. Exemple : UDPConnNatSrc=15. Journaux concernés : l_filterstat.
UDPPacket	Nombre de paquets UDP ayant transité par le Firewall. Exemple : UDPPacket=6164646. Journaux concernés : l_filterstat.
UI	Unité d'Information Sofbus / Lacbus Chaîne de caractères au format UTF-8. Exemple : UI=Consigne. Disponible depuis : SNS v4.3.0. Journaux concernés : l_plugin.
unitid	Valeur du "*Unit Id*" d'un message Modbus permettant de préciser un automate. Exemple : unitid=255. Disponible depuis : SNS v2.3.0. Journaux concernés : l_plugin.
unreachrate	Indique le pourcentage de temps pendant lequel la passerelle n'était pas accessible au cours des 15 dernières minutes. Chaîne de caractères au format UTF-8. Exemple : unreachrate=0. Disponible depuis : SNS v4.3.0. Journaux concernés : l_routerstat.
uprate	Indique le pourcentage de temps pendant lequel la passerelle était en état actif au cours des 15 dernières minutes. Chaîne de caractères au format UTF-8. Exemple : uprate=0. Disponible depuis : SNS v4.3.0. Journaux concernés : l_routerstat.

urlruleid	Numéro de la règle de filtrage d'URL appliquée. Format numérique. Exemple : urlruleid=12 Disponible depuis : SNS v3.2.0. Journaux concernés : l_web.
user	Utilisateur authentifié par le firewall. Chaîne de caractères au format UTF-8. Exemple : user=« john.doe », user=« john.doe@company.com » Peut être affiché de manière anonyme selon les droits d'accès de l'administrateur. Disponible depuis : SNS v1.0.0. Journaux concernés : l_alarm, l_auth, l_connection, l_ftp, l_plugin, l_pop3, l_sandboxing, l_server, l_smtp, l_ssl, l_web, l_xvpn.
	Utilisateur
usergroup	Groupe, défini dans les droits d'accès VPN, auquel appartient l'utilisateur ayant établi un tunnel. Chaîne de caractères au format UTF-8. Exemple : usergroup=« ipsec-group » Disponible depuis : SNS v3.3.0. Journaux concernés : l_vpn.
	Groupe

V

version	Numéro de version du protocole. Chaîne de caractères au format UTF-8. Exemple : version=TLSv1.2, version=4. Disponible depuis : SNS v4.2.1 Journaux concernés : l_connection, l_plugin.
	Version de protocole
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 ». Journaux concernés : l_monitor.
	Supervision des interfaces / Utilisation de la bande passante.

virus	Message indiquant si un virus a été détecté (l'antivirus doit être actif) Exemple : virus=clean. Journaux concernés : l_ftp, l_pop3, l_smtp, l_web.
	Virus Exemple : « propre ».
vulnid	Identifiant unique Stormshield Network de la vulnérabilité détectée. Exemple : vulnid=148262. Journaux concernés : l_pvm.
	ID vuln

W

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 : Wifi01=Public_WiFi,61515,128648,788241,1890520,2130,21. Journaux concernés : l_monitor.
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 : wldev0=Physic_WiFi,61515,128648,788241,1890520,2130,21. Journaux concernés : l_monitor.

Pour aller plus loin

Des informations complémentaires et réponses à vos éventuelles questions sur les logs SNS sont disponibles dans la base de connaissances Stormshield (authentification nécessaire).

documentation@stormshield.eu