TECHNICAL NOTE
STORMSHIELD NETWORK SECURITY

DESCRIPTION OF AUDIT LOGS

Product concerned: SNS 4.7.5

Document last updated: April 10, 2024

Reference: sns-en-description_of_audit_logs_technical_note_v4

Table of contents

Getting started

Stormshield Network Security firewalls log the activity of the various enabled services while they are running. Generated events (logs) are saved locally by default in audit log files on the hard disk or in SD memory cards for smaller appliances. They also appear in the web administration interface, displayed by theme, e.g., Network traffic, Alarms, Web, etc.

Logs allow you to check the firewall's activity or fix potential issues. Stormshield's technical support team also relies on such logs for troubleshooting where necessary.

In this document, you will learn how to look up and configure logs, as well as the best practices to adopt when storing and using them.

Reading logs

Logs can be read in the web administration interface or directly in files stored on the hard disk or SD card. If logs are sent to a Syslog server or through an IPFix collector, they can also be read in these programs.

In a high availability (HA) cluster, logs are not replicated on all nodes. The active firewall writes logs to its hard disk. If the firewall becomes the passive firewall, the other active firewall will continue writing logs. As a result, neither firewall in the cluster contains all logs, and the web administration interface displays only logs found on the firewall to which it is connected. To read logs more easily in a HA setup, send them to a Syslog server.

In line with the General Data Protection Regulation (GDPR), access to firewall logs is restricted by default for all administrators. The *admin* super administrator can easily access full logs but other administrators must request a temporary access code. Every time a request is submitted for full access to logs, a log will be generated. For further information, refer to the Technical note Complying with privacy regulations.

Reading logs in the web administration interface

1. In the upper part of the web administration interface, click on the **Monitoring** tab.
2. In the menu on the left, select **Logs-Audit logs**.
3. To display all logs, click on **All logs**. Otherwise, select the desired view.
   Logs are displayed in chronological order, the first being the most recent. Only logs from the last hour are displayed by default, but the time range can be changed by clicking on the drop-down list.
4. Click on **Actions > Expand all elements** if you wish to display all available columns.
5. To filter logs, enter text in the **Search** field or click on **Advanced search**, then **Add a criterion** to combine various search criteria.

For further information on searches and displaying logs, refer to Views and Interactions in the User guide.

Reading logs in log files

- Log in to the firewall in SSH to read logs stored in the */log* folder. These logs consist of the following files:

l_alarm	Events relating to intrusion prevention functions (IPS) and those logged with a minor or major alarm level in the filter policy.
l_auth	Events relating to user authentication on the firewall
l_connection	Events relating to TCP/UDP connections allowed to and from the firewall, which have not been analyzed by an application plugin. The log is written when the connection ends.
l_count	Statistics regarding the number of times a rule has been executed. Such logs are not generated by default. For further information, see Adding logs to filter rules.
l_date	Events relating to time changes on the firewall.
l_filter	Events relating to filter and/or NAT rules. Such logs are not generated by default. For further information, see Adding logs to filter rules.

l_filterstat	Statistics regarding the use of the firewall and its resources.
l_ftp	Events relating to connections going through the FTP proxy.
l_monitor	Statistics to compile performance graphs and security reports (web administration interface).
l_plugin	Events relating to processes carried out by application plugins (FTP, SIP, etc.).
l_pop3	Events relating to connections going through the POP3 proxy.
l_pvm	Events relating to the option Stormshield Network Vulnerability Manager.
l_sandboxing	Events relating to file sandboxing if the subscription for this option has been activated.
l_server	Events relating to the administration of the firewall
l_smtp	Events relating to connections going through the SMTP proxy.
l_ssl	Events relating to connections going through the SSL proxy.
l_system	Events directly relating to the system (shutdown/reboot of the firewall, system error, service operation, etc).
l_vpn	Events relating to the IPSec VPN tunnel negotiation phase.
l_web	Events relating to connections going through the HTTP proxy.
l_xvpn	Events relating to the setup of an SSL VPN tunnel (tunnel or portal mode).
l_routerstat	Statistics relating to router objects (SD-WAN).

For more information on the various fields in these files, refer to the technical note Understanding audit logs.

Reading log archives

As soon as a log file exceeds 20 MB, it will be closed to make way for another. The closed file can be found in the */log* file under a new name. The number of log files that are retained for each log category depends on the amount of disk space assigned to the log category in question (**Configuration** > **Notifications** > **Logs - Syslog - IPFIX** > **Local storage** tab).

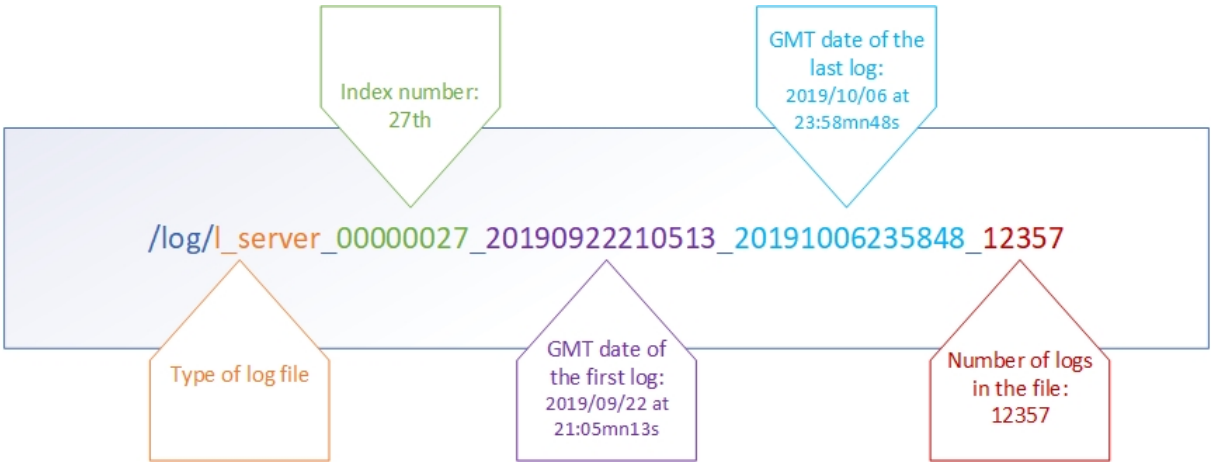
EXAMPLE
If 3.2 GB of storage space has been allocated to the IPsec VPN log category, 160 IPsec log files can be retained (20 MB * 160 = 3.2 GB).

Archive names

Closed log files are named according to the following structure:

- Type of log file (e.g.: l_filter, l_alarm, etc.),
- An 8-digit index number (starts from 0),
- Creation date: GMT date of the first log contained in the file,
- Closing date: GMT date of the last log contained in the file,
- The number of logs stored in the file.

Example:



File indexation (managed incrementally and starting from 0) makes it possible to not have to rely only on creation or closing dates, as these dates may be distorted when the time is changed on the firewall.

Managing log storage

By default, when the storage space reserved for a log type reaches full capacity, the oldest archive file will be erased to free up space.

Two other courses of action are available, and can be enabled for each type of log file using CLI/serverd *CONFIG LOG* commands:

- Logs stop being generated once the dedicated space reaches full capacity,
- The firewall shuts down once the dedicated space reaches full capacity.

For more information on the syntax of these commands, refer to the CLI SERVERD Commands Reference Guide.

Configuring logs

You can select the logs you want the firewall to generate, where logs will be saved, and the level of logs to generate.

Logging must be optimally configured so that only necessary logs will be generated. When the amount of logs generated exceeds the writing capacity on the storage medium, a buffer will allow writing to be delayed, but will eventually fill up. To anticipate or resolve such issues, refer to the knowledge base article How can I solve a log overflow issue? and its related articles.

Understanding log types

There are two types of logs:

- Standard activity logs that are enabled by default and which can be configured in the module **Configuration > Notifications > Logs - Syslog - IPFIX**.
- Filter and NAT logs that are disabled by default and which can be configured in the module **Configuration > Security policy > Filter - NAT**:
  - In the window to edit filter rules, **Action** menu, *General* tab, **Log level** field,
  - In the window to edit NAT rules, **Options** menu, **Log level** field.

  Filter and NAT logs must only be enabled temporarily to diagnose issues.

Choosing where to save logs

Logs are saved locally by default on the hard disk or on an SD card. They can also be sent to a Syslog server or an IPFix collector.

1. Go to **Configuration > Notifications > Logs - Syslog - IPFIX**.
2. Switch on the ON/OFF 

switch depending on where you wish to send logs: local, Syslog and/or IPFix. For example, if you choose to view logs only through SIEM tools, enable a Syslog profile and disable local storage and the IPFIX collector.

   If local storage is disabled, only the most recent logs stored in the RAM (about 200 logs per category) can be viewed in the web administration interface on the firewall. Older logs will not be displayed.

Choosing which logs to generate

All standard activity logs are enabled by default and can be viewed in the web administration interface. Only filter and NAT logs are disabled by default. Disable all logs that you do not need.

This feature is not available for IPFix collectors.

1. Go to **Configuration** > **Notifications** > **Logs - Syslog - IPFIX**.
2. For local storage, disable log families by double-clicking in the **Enabled** column in the table **Configuration of the space reserved for logs**. You can adjust the percentage of disk space according to your needs.
   For the Syslog server, disable log families by double-clicking in the **Status** column in **Advanced properties**.

   Logs disabled for local storage will not appear in the web administration interface of the firewall.

For more information, refer to the section Logs-Syslog-IPFIX in the User guide.

Adding logs to filter and NAT rules

Traffic that goes through a filter or NAT rule generate logs by default in the **Network connections** log, or in the **Application connections** log if a plugin conducts application analyses in IPS or IDS mode. Only connections with a "Pass" action and in TCP/UDP are logged

To check the effectiveness of a filter or NAT rule, you can generate additional logs that do not appear in other logs:

- Logs of all traffic that a filter rule has blocked,
- Logs of all traffic to which address translation (NAT) has been applied,
- Logs of all traffic directly above the IP layer that matches a filter rule, regardless of whether it has been passed or blocked.

Enable verbose mode with care and only for the duration of the check, as a large volume of logs will be generated, including duplicates of standard activity logs. This may cause a log overflow and slow down the performance of the firewall.

Such logs appear in the **Logs - Audit logs** > **Filtering** monitoring menu in the web administration interface and are saved in the *l_filter* log file.

1. Go to the menu **Configuration** > **Security policy** > **Filter - NAT**.
2. Double-click in the **Action** column of the filter rule. The **Editing rule** window appears.
3. In the **Action** menu:
   - *General* tab, choose the **Verbose (filter log)** log level,
   - *Advanced properties* tab, **Logs** section, select the location where logs for the rule will be saved. Do not check **Disk** if you do not wish to save such logs locally.
   - *Advanced properties* tab, **Logs** section, select **Count** to generate statistics in the *l_count* log on the number of times a rule has been executed.
4. Confirm changes to the rule by clicking on **OK**, then click on **Apply**.
5. Run your check by looking up the **Network traffic** or **Filtering** views in the web administration interface, or in the */log/l_filter* file.
6. In the **General** tab in the window to edit filter rules, reset the log level to the default value **Standard (connection log)**.

Understanding audit logs

Logs are written to their corresponding log files.

Audit logs are WELF-compatible UTF-8 text files. The WELF format is a sequence of items, written as *field=value* and separated by spaces. Values may be framed by double quotes.

A single log corresponds to a line ending with a return carriage (CRLF).

Example

```
id=firewall time="1/27/2019 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
```

In the sections Common fields in all logs and Specific fields, logs are described as follows:

Field name	Description of the field Format of the field. Example: "*raw value*"
	Value if different from the raw value.

The logs *l_server*, *l_auth*, *l_vpn* and *l_system* contain fields that are specific to Stormshield Network firewalls. These particular fields, which do not belong to the WELF format, will be described in the section Specific fields.

Some log files, such as *l_filterstat* , *l_routerstat* and *l_count*, which are used to calculate statistics, contain many specific fields.

They are therefore similar to snapshots of the state of the firewall. They are calculated and written at regular intervals.

Changing the time

When the time on the firewall is changed, a specific line will be written in all the logs.

This line contains the fields `datechange` and `duration`. The `datechange` value in this case will be "1" to reflect the time change. As for the `duration` field, it will indicate the difference (in seconds) between the time on the firewall before and after this change.

The other fields of this log are common to all logs (described in the following section).

Example

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

In the **Audit logs** menu in the web administration interface, this log will appear in all modules highlighted in yellow.

Common fields in all logs

id	Type of product. This field constantly has the value “firewall” for logs on the Firewall.

time	"Local" time at which the log was recorded in the log file (time configured on the Firewall). String in "YYYY-MM-DD HH:MM:SS" format. Available from: SNS v1.0.0.
	Saved at The display format depends on the language of the operating system on which the administration suite has been installed. Example: "DD/MM/YYYY" and "HH:MM:SS" for French; "YYYY/MM/DD" and "HH:MM:SS" for English.
fw	firewall's ID This is the name entered by the administrator or, by default, its serial number. String of characters in UTF-8 format. Example: "firewall_name" or "V50XXXXXXXXXXXX" Available from: SNS v1.0.0.
tz	Time difference between the Firewall's time and GMT. This depends on the time zone used. String in "+HHMM" or "-HHMM" format. Available from: SNS v1.0.0.
	GMT offset Example: "gmt +01:00"
startime	"Local" time at the beginning of the logged event (time configured on the Firewall). String in "YYYY-MM-DD HH:MM:SS" format. Available from: SNS v1.0.0.
	Date and time The display format depends on the language of the operating system on which the administration suite has been installed. Example: "DD/MM/YYYY" and "HH:MM:SS" for French; "YYYY/MM/DD"; and "HH:MM:SS" for English.

Specific fields

The fields presented below may be common to a set of logs or specific to a single log.

Fields specific to the "l_filter", "l_alarm", " l_connection" and "l_plugin" logs

The fields described below appear in the web administration interface of the firewall under the **Monitoring > Logs - Audit logs** module, in the views: **All logs**, **Network traffic**, **Filtering**, **Alarms**, **Web**, **E-mails** and **System events**.

pri	Represents the alarm level. Values (cannot be customized): "0 " (emergency), "1 " (alert), "2 " (critical), "3 " (error), "4 " (warning), "5 " (notice), "6 " (information) or "7 " (debug). Available from: SNS v1.0.0.
	Priority
confid	Index of the security inspection profile used. Value from "0" to "9". Available from: SNS v1.0.0.
	Config
slotlevel	Indicates the type of rule that activated logging. Values: "0" (implicit), "1" (global), or "2" (local). Available from: SNS v1.0.0.
	Rule level Values: "Implicit", "Global" or "Local".
ruleid	Number of the filter rule applied. Example: "1", "2" … Available from: SNS v1.0.0.
	Rule
srcif	Internal name of the interface at the source of the traffic. String of characters in UTF-8 format. Example: "Ethernet0" Available from: SNS v1.0.0.
	Source interf. (ID)
srcifname	Name of the object representing the interface at the source of the traffic. String of characters in UTF-8 format. Example: "out" Available from: SNS v1.0.0.
	Source interf.
srcmac	MAC address of the source host. May be displayed anonymously depending on the administrator's access privileges. Available from: SNS v1.0.0.
	Source MAC address
ipproto	Name of the protocol above IP (transport layer). String of characters in UTF-8 format. Example: "tcp" Available from: SNS v1.0.0.
	Internet Protocol

ipv	Version of the IP protocol used in the traffic Values: “4”, “6”… Available from: SNS v1.0.0.
	IP version
proto	Name of the associated plugin. If this is not available, the name of the standard service corresponding to the destination port. String of characters in UTF-8 format. Example: “http”, “ssh” Available from: SNS v1.0.0.
	Protocol
src	IP address of the source host. Decimal format. Example: ”192.168.0.1” May be displayed anonymously depending on the administrator's access privileges. Available from: SNS v1.0.0.
	Source
srcport	Source TCP/UDP port number. Example: "49753" Available from: SNS v1.0.0.
	Source port
srcportname	“Source” port name if it is known. String of characters in UTF-8 format. Example: “http”, “ephemeral_fw_tcp”… Available from: SNS v1.0.0.
	Source port name
srcname	Name of the object corresponding to the source host. String of characters in UTF-8 format. Example: “client_workstation” May be displayed anonymously depending on the administrator's access privileges. Available from: SNS v1.0.0.
	Source name
modsrc	Translated IP address of the source host. May be displayed anonymously depending on the administrator's access privileges. Decimal format. Example: ”192.168.0.1” Available from: SNS v1.0.0.
	Translated source address
modsrcport	Translated TCP/UDP source port number. Example: "80" Available from: SNS v1.0.0.
	Translated source port
dst	IP address of the destination host Decimal format. Example: ”192.168.0.2” Available from: SNS v1.0.0.
	Destination

dstport	Destination TCP/UDP port number. Example: "22" Available from: SNS v1.0.0.
	Destination port
dstportname	Name of the object corresponding to the destination port. String of characters in UTF-8 format. Example: “ssh” Available from: SNS v1.0.0.
	Dest. port name
dstname	Name of the object corresponding to the IP address of the destination host. String of characters in UTF-8 format. Example: “intranet_server” Available from: SNS v1.0.0.
	Destination name
origdst	Original IP address of the destination host (before translation or the application of a virtual connection). Decimal format. Example: ”192.168.0.1” Available from: SNS v1.0.0.
	Orig. destination
origdstport	Original port number of the destination TCP/UDP port (before translation or the application of a virtual connection). Example: "80" Available from: SNS v1.0.0.
	Orig. destination port
dstif	Name of the destination interface. String of characters in UTF-8 format. Example: “Ethernet 1” Available from: SNS v1.0.0.
	Dest. interf. (ID)
dstifname	Name of the object representing the traffic’s destination interface. String of characters in UTF-8 format. Example: “dmz1” Available from: SNS v1.0.0.
	Dest. interf.
user	User authenticated by the firewall. String of characters in UTF-8 format. Example: “John.smith” May be displayed anonymously depending on the administrator's access privileges. Available from: SNS v1.0.0.
	User
dstcontinent	Continent to which the destination IP address of the connection belongs. Value: continent's ISO code Example: dstcontinent="eu" Available from: SNS v3.0.0.
	Destination continent

dstcountry	Country to which the destination IP address of the connection belongs. Format: country's ISO code Example: dstcountry="fr" Available from: SNS v3.0.0.
	Destination country
dsthostrep	Reputation of the connection's target hosts Available only if reputation management has been enabled for the relevant hosts. Format: unrestricted integer. Example: dsthostrep=506 Available from: SNS v3.0.0.
	Destination host reputation
dstiprep	Reputation of the destination IP address. Available only if this IP address is public and listed in the IP address reputation base. Value: "anonymizer", "botnet", "malware", "phishing", "tor", "scanner" or "spam". Example: dstiprep="spam" Available from: SNS v3.0.0.
	Public reputation of the destination IP address
srccontinent	Continent to which the source IP address of the connection belongs. Value: continent's ISO code Example: srccontinent="eu" Available from: SNS v3.0.0.
	Source continent
srccountry	Country to which the source IP address of the connection belongs. Format: country's ISO code Example: srccountry="fr" Available from: SNS v3.0.0.
	Source country
srchostrep	Reputation of the connection's source hosts. Available only if reputation management has been enabled for the relevant hosts. Format: unrestricted integer. Example: srchostrep=26123 Available from: SNS v3.0.0.
	Source host reputation
srciprep	Reputation of the source IP address. Available only if this IP address is public and listed in the IP address reputation base. Value: "anonymizer", "botnet", "malware", "phishing", "tor", "scanner" or "spam". Example: srciprep="anonymizer,tor" Available from: SNS v3.0.0.
	Public reputation of the source IP address
dstmac	MAC address of the destination host. Format: Hexadecimal values separated by ":". Example: dstmac=00:25:90:01:ce:e7 Available from: SNS v4.0.0.
	Destination MAC address

etherproto	Type of Ethernet protocol. Format: String of characters in UTF-8 format. Example: etherproto="profinet-rt" Available from: SNS v4.0.0.
	Ethernet protocol
rt	Name of the gateway used for the connection. Present only if the gateway does not match the default route. String of characters in UTF-8 format. Example: "my_gateway" Available from: SNS v4.3.0.
rtname	Name of the router object used for the connection. Present only if the router does not match the default route. String of characters in UTF-8 format. Example: "my_gateway" Available from: SNS v4.3.0.

Fields specific to the "l_filter" log

The fields described below appear in the web administration interface of the firewall under the **Monitoring > Logs - Audit logs** module, in the views: **All logs**, **Network traffic** and **Filtering**.

sent	Number of bytes sent. Decimal format. Example: "*14623*" Available from: SNS v1.0.0.
	Sent Example: *13 KB*
action	Behavior associated with the filter rule. Value: "*Pass*" or "*Block*" (empty field for "Log").
	Action
icmpcode	Code number of the icmp message. Example: "*1*" (meaning "Destination host unreachable"). Available from: SNS v1.0.0.
	ICMP code
icmptype	Number of the type of icmp message. Example: "*3*" (meaning "Destination unreachable"). Available from: SNS v1.0.0.
	ICMP type
rcvd	Number of bytes received. Decimal format. Example: "*23631*" Available from: SNS v1.0.0.
	Received Example: *23 KB*

target	Shows whether the src or dst fields correspond to the target of the packet that had raised the alarm. Values: "*src*" or "*dst*" Available from: SNS v3.0.0.
	Target

Fields specific to the "l_alarm" log

The fields described below appear in the web administration interface of the firewall under the **Monitoring > Logs - Audit logs** module, in the views: **All logs**, **Alarms**, **Filtering** and **System events**.

action	Behavior associated with the filter rule. Value: "pass" or "block"
	Action
msg	Text message explaining the alarm. String of characters in UTF-8 format. Example: "Port probe"
	Message
class	Information about the alarm's category. String of characters in UTF-8 format. Example: "protocol", "system", "filter"…
	Context
classification	Code number indicating alarm category. Example: "0"
	Classification Example: "Application"
pktlen	Size of the network packet that activated the alarm (in bytes). Example: "133"
	Packet size
pktdumplen	Size of the packet captured for deeper analysis by a third-party tool. This value may differ from the value of the "pktlen" field. Example: "133"
	Size of the packet captured
pktdump	Network packet captured and encoded in hexadecimal for deeper analysis by a third-party tool. Example: "450000321fd240008011c2f50a00007b0a3c033d0035c"
	Captured packet
alarmid	Stormshield Network alarm ID Decimal format. Example: "85"
	Alarm ID

repeat	Number of occurrences of the alarm over a given period. Decimal format. Example: "4" Available from: SNS v1.0.0.
	Repeat
icmpcode	Code number of the icmp message. Example: “1” (meaning “Destination host unreachable”). Available from: SNS v1.0.0.
	ICMP code
icmptype	Number of the type of icmp message. Example: “3” (meaning “Destination unreachable”). Available from: SNS v1.0.0.
	ICMP type
domain	Authentication method used or LDAP directory of the user authenticated by the firewall. String of characters in UTF-8 format. Example: domain="documentation.stormshield.eu" Available from: SNS v3.0.0.
	Method or directory
risk	Risk relating to the connection. This value contributes to the reputation score of the connection's source host. Value: between 1 (low risk) and 100 (very high risk). Example: risk=20 Available from: SNS v3.0.0.
	Risk
target	Shows whether the src or dst fields correspond to the target of the packet that had raised the alarm. Values: "src" or "dst" Available from: SNS v3.0.0.
	Target

Fields specific to the “l_connection” log

The fields described below appear in the web administration interface of the firewall under the **Monitoring > Logs - Audit logs** module, in the views: **All logs**, **Network traffic**, **Web** and **E-mails**.

sent	Number of bytes sent. Decimal format. Example: "14623" Available from: SNS v1.0.0.
	Sent Example: “13KB”
rcvd	Number of bytes received. Decimal format. Example: "23631" Available from: SNS v1.0.0.
	Received Example: “23 KB”

duration	Duration of the connection in seconds. Decimal format. Example: "173.15" *Duration* Example: "2m 53s 15"
domain	Authentication method used or LDAP directory of the user authenticated by the firewall. String of characters in UTF-8 format. Example: domain="documentation.stormshield.eu" Available from: SNS v3.0.0. *Method or directory*
action	Behavior associated with the filter rule. Value: “pass” or “block” (empty field for “Log” action). *Action*
clientappid	Last client application detected on the connection. Character string. Example: clientappid=firefox Available from: SNS v3.2.0. *Client application*
serverappid	Last server application detected on the connection. Character string. Example: serverappid=google Available from: SNS v3.2.0. *Server application*
version	Protocol version number Character string in UTF-8 format. Example: version=TLSv1.2 Available from: SNS 4.2.1 *Protocol version*

Fields specific to the “l_plugin” log

The fields described below appear in the web administration interface of the firewall under the **Monitoring > Logs - Audit logs** module, in the views: **All logs, Network traffic, Web** and **E-mails.**

sent	Number of bytes sent. Decimal format. Example: "*14623*" Available from: SNS v1.0.0 *Sent* Example: "*13 KB*"

rcvd	Number of bytes received. Decimal format. Example: "*23631*" Available from: SNS v1.0.0
	Received Example: "*23 KB*"
duration	Duration of the connection in seconds. Decimal format. Example: "*173.15*"
	Duration Example: "*2m 53s 15*"
action	Behavior associated with the filter rule. Value: "*pass*".
	Action
domain	Authentication method used or LDAP directory of the user authenticated by the firewall. String of characters in UTF-8 format. Example: domain=*documentation.stormshield.eu* Available from: SNS v3.0.0
	Method or directory
error_class	Number of the error class in an S7 response. Digital format. Available from: SNS v2.3.0
error_code	Error code in the error class specified in the S7 response. Available from: SNS v2.3.0
format	Type of message for IEC104 Available from: SNS v3.1.0
group	Code of the *"userdata"* group for an S7 message. Available from: SNS v2.3.4
unit_id	Value of the *"Unit Id"* in a Modbus message. Example: "*255*". Available from: SNS v2.3.0
clientappid	Last client application detected on the connection. Character string. Example: clientappid=*firefox* Available from: SNS v3.2.0
	Client application
serverappid	Last server application detected on the connection. Character string. Example: serverappid=*google* Available from: SNS v3.2.0
	Server application

cipservicecode	Value of the "*Service Code*" field in the CIP message. String of characters in UTF-8 format. Example: cipservicecode=*Get_Attribute_List* Available from: SNS v3.5.0
cipclassid	Value of the "*Class ID*" field in the CIP message. String of characters in UTF-8 format. Example: cipclassid=*Connection_Manager_Object* Available from: SNS v3.5.0
version	Value of the "*Version number*" field for the NTP protocol. Digital format. Example: version=*4*. Available from: SNS v3.8.0
requestmode	Value of the "*Mode*" field for an NTP request. String of characters in UTF-8 format. Example: requestmode=*client.* Available from: SNS v3.8.0
responsemode	Value of the "*Mode*" field for an NTP response. String of characters in UTF-8 format. Example: responsemode=*server.* Available from: SNS v3.8.0
UI	Sofbus/Lacbus information unit String of characters in UTF-8 format. Example: UI=Instruction Available from: SNS v4.3.0

Additional fields for the FTP plugin

groupid	ID number allowing the tracking of child connections. Example: "3"
	Group
op	FTP operation performed. ASCII character string. Example: “RETR”, “LIST”…
	Operation
result	FTP return code. Example: "0"
	Result
arg	FTP argument (name of directory, file, etc). String of characters in UTF-8 format. Example: “file.txt”
	Argument

Additional fields for the HTTP plugin

op	HTTP operation performed. ASCII character string. Example: “GET”, “PUT”, “POST” …
	Operation
result	HTTP return code. Example: “403”, “404”…
	Result
arg	HTTP argument (URL, POST form, etc). String of characters in UTF-8 format. Example: “/”, “/page.htm”…
	Argument

Additional fields for the EDONKEY plugin

op	Operation performed. Value: “SENDPART”.
	Operation
arg	EDONKEY argument (name of the downloaded file). String of characters in UTF-8 format. Example: “myfile.txt”
	Argument

Additional fields for the RTP, RTCP_MEDIA_UDP and MEDIA_TCP plugins

groupid	ID number allowing the tracking of child connections. Example: "3"
	Group
caller	Caller ID. String of characters in UTF-8 format. Example: “"John" <sip:193@192.168.0.1>"
	Caller
callee	Callee ID. String of characters in UTF-8 format. Example: "sip:192@192.168.1.1:5060;line=g842aca6eddb2a5"
	Callee
media	Type of traffic detected (audio, video, application, etc). ASCII character string. Example: “control”.
	Media

Additional fields for the YMSG plugin

groupid	ID number allowing the tracking of child connections. Example: "3"
	Group
op	Operation performed. Values supported: “V15 Proxy Transfer” and “V15 Inline Transfer”.
	Operation
arg	YMSG argument: name of the user and downloaded file. String of characters in UTF-8 format. Example: “user@filename”
	Argument

Additional fields for the MSN plugin

groupid	ID number allowing the tracking of child connections. Decimal format. Example: "1"
	Group
op	Operation performed. Example: “VER”, “USR” ….
	Operation
arg	MSN argument: name of the downloaded file. String of characters in UTF-8 format. Example: “file.txt”
	Argument

Additional fields for the OSCAR plugin

groupid	ID number allowing the tracking of child connections. Example: "3"
	Group
op	Operation performed. ASCII character string.
	Operation
arg	Name of the downloaded file. String of characters in UTF-8 format. Example: “file.txt”
	Argument

Additional fields for the TFTP plugin

groupid	ID number allowing the tracking of child connections. Example: "3"
	Group
op	Operation performed. ASCII character string. Example: “read”
	Operation
result	Return code. Example: "0"
	Result
arg	Name of the downloaded file. String of characters in UTF-8 format. Example: “file.txt”
	Argument

Additional fields for the MODBUS plugin

unit_id	*Unit identifier* that allows specifying a slave automaton. Example: "255"
op	Name of the Modbus function. ASCII character string. Example: "Write_Single_Register", etc
	Operation
result	Value of the function code from the Modbus response. Example: "5"
	Result
msg	Additional information when the firewall ends a MODBUS connection String of characters in UTF-8 format. Values: "timed out" (no response received for a sent request), "connection closed" (connection shut down by the firewall after a block alarm was raised, for example) or "no request" (the firewall did not receive a request relating to a response it has received).
	Message

Additional fields for the S7 plugin

op	Value of the S7 function code. Example: "4", etc.
	Operation
error_class	Error class returned in an S7 response. Example: "0" Available from: SNS v2.3.0.
error_code	Error code returned in an S7 response. Example: "0" Available from: SNS v2.3.0.

group	Number of the group to which the S7 function code belongs
msg	Additional information when the firewall ends an S7 connection String of characters in UTF-8 format. Values: "timed out" (no response received for a sent request), "connection closed" (connection shut down by the firewall after a block alarm was raised, for example) or "no request" (the firewall did not receive a request relating to a response it has received).
	Message

Fields specific to the "l_pvm" log

The fields described below appear in the web administration interface of the firewall under the **Monitoring > Logs - Audit logs** module, in the views: **All logs**, **Alarms** and **Vulnerabilities**.

pri	Alarm level (configurable by the administrator in certain cases). Values: “1” (major) or “4” (minor). Available from: SNS v1.0.0.
	Priority
src	IP address of the source host. Decimal format. Example: ”192.168.0.1” May be displayed anonymously depending on the administrator's access privileges. Available from: SNS v1.0.0.
	Source
srcname	Name of the object corresponding to the IP address of the source host. String of characters in UTF-8 format. Example: “client_workstation” May be displayed anonymously depending on the administrator's access privileges. Available from: SNS v1.0.0.
	Source name
ipproto	Type of network protocol (entered only if a vulnerability has been detected). String of characters in UTF-8 format. Example: “tcp” Available from: SNS v1.0.0.
	Internet Protocol
proto	Name of the associated plugin. If this is not available, the name of the standard service corresponding to the port (entered only if a vulnerability has been detected). String of characters in UTF-8 format. Example: “ssh” Available from: SNS v1.0.0.
	Protocol
port	Port number (entered only if a vulnerability has been detected). Example: "22"
	Source port
portname	Standard service corresponding to the port number (entered only if a vulnerability has been detected). String of characters in UTF-8 format. Example: “ssh”
	Source port name

vulnid	Unique Stormshield Network ID of the detected vulnerability. Example: "132710"
	Vuln ID
msg	Name of the vulnerability. String of characters in UTF-8 format. Example: “Samba SWAT Clickjacking Vulnerability”
	Message
arg	Details of the detected vulnerability (version of service, operating system concerned, etc). String of characters in UTF-8 format. Example: “Samba_3.6.3”
	Argument
product	Product on which the vulnerability was detected. String of characters in UTF-8 format. Example: “JRE_1.6.0_27”
	Product
service	Service (product with a dedicated port) on which the vulnerability was detected. String of characters in UTF-8 format. Example: “OpenSSH_5.4”
	Service
detail	Additional information on the vulnerable software version. String of characters in UTF-8 format. Example: “PHP_5.2.3”
	Detail
family	Name of the vulnerability family (Web Client, Web Server, Mail Client...). String of characters in UTF-8 format. Example: “SSH”, “Web Client” ….
	Category of contact
severity	Vulnerability’s intrinsic level of severity. Values: “0” (Information), “1” (Weak), “2” (Moderate), “3” (High) or “4” (Critical).
	Severity Values: “Information”, “Weak”, “Moderate”, “High” or “Critical”.
solution	Indicates whether a fix is available in order to correct the detected vulnerability. Values: “0” (not available) or “1” (available).
	Workaround Values: “Yes” or “No”.
remote	Indicates whether the vulnerability can be exploited remotely Values: “0” (false) or “1” (true).
	Exploit Values: “Local” or “Remote”.
targetclient	Indicates whether the exploitation of the vulnerability requires the use of a client on the vulnerable host. Values: “0” (false) or “1” (true).
	Target client Values: "Client" or " ".

targetserver	Indicates whether the exploitation of the vulnerability requires the installation of a server on the vulnerable host. Values: “0” (false) or “1” (true).
	Target server Values: "Server" or " ".
discovery	Date on which the security watch team published the vulnerability (only if the level of severity is higher than “0”) String in “YYYY-MM-DD” format.
	Discovered on Format: depends on the language of the operating system on which the administration suite was installed. Example: “DD/MM/YYYY” and “HH:MM:SS” for French; “YYYY/MM/DD” and “HH:MM:SS” for English.

Fields specific to the "l_system" log

The fields described below appear in the web administration interface of the firewall under the **Monitoring > Logs - Audit logs** module, in the views: **All logs**, **VPN** and **System events**.

pri	Set to “5” meaning “notice” to ensure WELF compatibility. Available from: SNS v1.0.0.
	Priority
src	IP address of the source host. Decimal format. Example: ”192.168.0.1” May be displayed anonymously depending on the administrator's access privileges. Available from: SNS v1.0.0.
	Source
dst	IP address of the destination host Decimal format. Example: ”192.168.0.1” Available from: SNS v1.0.0.
	Destination
user	ID of the administrator who executed the command. String of characters in UTF-8 format. Example: ”admin” May be displayed anonymously depending on the administrator's access privileges. Available from: SNS v1.0.0.
	User
msg	Reference message regarding the action. String of characters in UTF-8 format. Example: “Agent (ssoagent) is active”
	Message
service	Name of the module that executed an action. ASCII character string. Example: “SSOAgent”
	Service

alarmid	Stormshield Network alarm ID Decimal format. Example: "85"
	Alarm ID
tsagentname	Indicates the name of the TS agent used. String of characters in UTF-8 format. Example: tsagentname="agent_name_test" Available from: SNS v4.7.0.

Fields specific to the "l_server" log

The fields described below appear in the web administration interface of the firewall under the **Monitoring > Logs - Audit logs** module, in the views: **All logs** .

error	Command's return code number Example: "0", "3"…
	State Example: "ok", "Auth failed"…
user	ID of the administrator who executed the command. String of characters in UTF-8 format. Example: "admin" May be displayed anonymously depending on the administrator's access privileges. Available from: SNS v1.0.0.
	User
address	IP address of the client workstation that initiated the connection. Decimal format. Example: address=192.168.0.2
	Source
sessionid	Session ID number allowing simultaneous connections to be differentiated. Example: "18"
	Session Example: "01.0018"
msg	Executed command accompanied by its parameters where applicable. String of characters in UTF-8 format. Example: "CONFIG FILTER ACTIVATE"
	Message
domain	Authentication method used or LDAP directory of the user authenticated by the firewall. String of characters in UTF-8 format. Example: domain="documentation.stormshield.eu" Available from: SNS v3.0.0.
	Method or directory

Fields specific to the "l_vpn" log

The fields described below appear in the web administration interface of the firewall under the **Monitoring > Logs - Audit logs** module, in the views: **All logs** and **VPN**.

pri	Set to “5” (“notice”) to ensure WELF compatibility. Available from: SNS v1.0.0.
	Priority
error	Error level of the log. Values: “0” (Information), “1” (Warning) or “2” (Error).
	Result Example: “Info”
phase	Number of the IPSec VPN tunnel negotiation phase. Values: “0” (no phase), “1” (phase 1) or “2” (phase 2).
	Phase
src	IP address of the VPN tunnel’s local endpoint. Decimal format. Example: ”192.168.0.1” Available from: SNS v1.0.0.
	Source
srcname	Name of the object corresponding to the VPN tunnel’s local endpoint. String of characters in UTF-8 format. Example: “Pub_FW” Available from: SNS v1.0.0.
	Source name
dst	IP address of the VPN tunnel’s remote endpoint. Decimal format. Example: ”192.168.1.1” Available from: SNS v1.0.0.
	Destination
dstname	Name of the object corresponding to the VPN tunnel’s remote endpoint. String of characters in UTF-8 format. Example: “fw_remote” Available from: SNS v1.0.0.
	Destination name
user	ID of the remote user used for the negotiation. String of characters in UTF-8 format. Example: “john.smith” May be displayed anonymously depending on the administrator's access privileges. c
	User
usergroup	The user that set up a tunnel belongs this group, defined in the VPN access privileges. String of characters in UTF-8 format. Example: usergroup="ipsec-group" Available from: SNS v3.3.0.
	Group

msg	Description of the operation performed. String of characters in UTF-8 format. Example: “Phase established”
	Message
side	Role of the Firewall in the negotiation of the tunnel. Values: “initiator” or “responder”.
	Role
cookie_i	Temporary identity marker of the initiator of the negotiation. Character string in hexadecimal. Example: “0xae34785945ae3cbf”
	Initiating cookie
cookie_r	Temporary identity marker of the peer of the negotiation. Character string in hexadecimal. Example: "0x56201508549a6526".
	Receiving cookie
localnet	Local network negotiated in phase2. Decimal format. Example: ”192.168.0.1”
	Local network
remotenet	Remote network negotiated in phase2. Decimal format. Example: ”192.168.1.1”
	Remote network
spi_in	SPI (Security Parameter Index) number of the negotiated incoming SA (Security Association). Character string in hexadecimal. Example: “0x01ae58af”
	Incoming spi
spi_out	SPI number of the negotiated outgoing SA. Character string in hexadecimal. Example: “0x003d098c”
	Outgoing spi
ike	Version of the IKE protocol used Values: “1”, “2”…
	IKE version
remoteid	ID of the peer used during the negotiation of the IKE SA. This may be an e-mail address or IP address.
	Remote identifier
ruletype	Type of IPSec rule. Character string. Values: mobile, gateway. Example: ruletype=mobile. Available from: SNS v4.2.1

Fields specific to the "l_monitor" log

Some of the fields described below are shown in the **Monitoring** > **Monitoring** module, in the views: **System**, **Interfaces** and **QoS**.

security	Indicator of the Firewall's security status. This value is used by the fleet management tool (Stormshield Network Unified Manager) to provide information on the security status (minor, major alarms, etc). Decimal format representing a percentage.
system	Indicator of the Firewall's system status. This value is used by the fleet management tool (Stormshield Network Unified Manager) to provide information on the system status (available RAM, CPU use, bandwidth, interfaces, fullness of audit logs, etc). Decimal format representing a percentage.
CPU	Firewall's CPU consumption: • Time allocated to the management of user processes, • Time consumed by the kernel, • Time allocated to system disruptions. Format: 3 numeric values separated by commas. Example: CPU=1,0,2 *System monitoring / CPU load*
Pvm	All indicators regarding vulnerability management: • Total number of vulnerabilities detected, • number of vulnerabilities that can be exploited remotely, • number of vulnerabilities requiring the installation of a server on the vulnerable host in order to be exploited, • number of vulnerabilities classified as critical, • number of vulnerabilities classified as minor, • number of vulnerabilities classified as major, • number of vulnerabilities that have a bug fix, • total amount of information (all levels), • number of minor data, • number of major data, • number of hosts for which PVM has gathered information, Format: 11 numeric values separated by commas. Example: "0,0,0,0,0,0,0,2,0,0,2"
EthernetXX	Indicators of bandwidth used for each of the active network interfaces: • name of the interface. String of characters in UTF-8 format. • incoming throughput (bits/second), • maximum incoming throughput for a given period (bits/second), • outgoing throughput (bits/second), • maximum outgoing throughput for a given period (bits/second), • number of packets accepted, • number of packets blocked, Format: 7 values separated by commas. Example: "in,61515,128648,788241,1890520,2130,21" *Interface monitoring / Bandwidth use*

VlanXX	Indicators of bandwidth used for each of the VLANs defined: • name of the VLAN. String of characters in UTF-8 format. • incoming throughput (bits/second), • maximum incoming throughput for a given period (bits/second), • outgoing throughput (bits/second), • maximum outgoing throughput for a given period (bits/second), • number of packets accepted, • number of packets blocked, Format: 7 values separated by commas. Example: "Vlan_Servers,61515,128648,788241,1890520"
	Interface monitoring / Bandwidth use
QidXX	Indicators of bandwidth used for each QoS queue: • name of the queue. String of characters in UTF-8 format. • incoming throughput (bits/second), • maximum incoming throughput for a given period (bits/second), • outgoing throughput (bits/second), • maximum outgoing throughput for a given period (bits/second), • number of packets accepted, • number of packets blocked, Format: 7 values separated by commas. Example: “http,5467,20128,1988,11704”
	QoS monitoring / Bandwidth use
WifiXX	Concerns only firewalls equipped with Wi-Fi antennas (W models). Indicators of bandwidth used for each active Wi-Fi access points: • name of the access point. String of characters in UTF-8 format. • incoming throughput (bits/second), • maximum incoming throughput for a given period (bits/second), • outgoing throughput (bits/second), • maximum outgoing throughput for a given period (bits/second), • number of packets accepted, • number of packets blocked, Format: 7 values separated by commas. Example: "Public_WiFi,61515,128648,788241,1890520,2130,21"

wldev0	Concerns only firewalls equipped with Wi-Fi antennas (W models). Indicators of bandwidth used for each physical interface that supports the firewall's Wi-Fi access points: • name of the interface. String of characters in UTF-8 format. • incoming throughput (bits/second), • maximum incoming throughput for a given period (bits/second), • outgoing throughput (bits/second), • maximum outgoing throughput for a given period (bits/second), • number of packets accepted, • number of packets blocked, Format: 7 values separated by commas. Example: "Physic_WiFi,61515,128648,788241,1890520,2130,21"
sslvpnX	Indicators of bandwidth used by SSL VPN traffic. : • name of the interface. String of characters in UTF-8 format. • incoming throughput (bits/second), • maximum incoming throughput for a given period (bits/second), • outgoing throughput (bits/second), • maximum outgoing throughput for a given period (bits/second), • number of packets accepted, • number of packets blocked, sslvpn0 represents TCP-based SSL VPN traffic. sslvpn1 represents UDP-based SSL VPN traffic. Format: 7 values separated by commas. Example: "sslvpn_udp,61515,128648,788241,1890520,2130,21"
ipsecXX	Indicators of bandwidth used by IPSec interfaces: • name of the interface. String of characters in UTF-8 format. • incoming throughput (bits/second), • maximum incoming throughput for a given period (bits/second), • outgoing throughput (bits/second), • maximum outgoing throughput for a given period (bits/second), • number of packets accepted, • number of packets blocked, ipsec represents traffic associated with the native IPSec interface (non virtual). ipsec1, ipsec2, etc. represent traffic associated with the virtual IPSec interfaces defined on the firewall. Format: 7 values separated by commas. Example: "Primary_VTI,61515,128648,788241,1890520,2130,21"

aggXX	Indicators of bandwidth used by interface aggregates: • name of the interface. String of characters in UTF-8 format. • incoming throughput (bits/second), • maximum incoming throughput for a given period (bits/second), • outgoing throughput (bits/second), • maximum outgoing throughput for a given period (bits/second), • number of packets accepted, • number of packets blocked, Format: 7 values separated by commas. Example: "Production_LACP,61515,128648,788241,1890520,2130,21"

Fields specific to the "l_smtp", "l_pop3", "l_ftp", "l_web", and "l_ssl" logs

The fields described below appear in the web administration interface of the firewall under the **Monitoring > Logs - Audit logs** module, in the views: **All logs**, **Network traffic**, **Web** and **E-mails**.

contentpolicy	Number of the SSL filter policy used. String of characters in UTF-8 format. Example: "3" Available from: SNS v1.0.0.
	Policy ID
pri	Set to “5” (“notice”) to ensure WELF compatibility. Available from: SNS v1.0.0.
	Priority
proto	Name of the standard service corresponding to the destination port. String of characters in UTF-8 format. Example: “smtp” Available from: SNS v1.0.0.
	Protocol
src	IP address of the source host. Decimal format. Example: ”192.168.0.1” May be displayed anonymously depending on the administrator's access privileges. Available from: SNS v1.0.0.
	Source
srcport	Source port number of the service. Example: "51166" Available from: SNS v1.0.0.
	Source port
srcportname	“Source” port name if it is known. String of characters in UTF-8 format. Example: “ephemeral_fw_tcp” Available from: SNS v1.0.0.
	Source port name

srcname	Name of the object corresponding to the source host. String of characters in UTF-8 format. Example: “client_workstation” May be displayed anonymously depending on the administrator's access privileges. Available from: SNS v1.0.0.
	Source name
srcmac	MAC address of the source host. May be displayed anonymously depending on the administrator's access privileges.
	Source MAC address
modsrc	Translated IP address of the source host. May be displayed anonymously depending on the administrator's access privileges. Decimal format. Example: ”192.168.15.1” Available from: SNS v1.0.0.
	Translated source address
modsrcport	Number of the translated TCP/UDP source port. Example: "49690" Available from: SNS v1.0.0.
	Translated source port
dst	IP address of the destination host Decimal format. Example: ”192.168.100.1” Available from: SNS v1.0.0.
	Destination
dstport	Service's destination port number. Example: "465" Available from: SNS v1.0.0.
	Destination port
dstportname	Name of the object corresponding to the destination port. String of characters in UTF-8 format. Example: "smtps " Available from: SNS v1.0.0.
	Dest. port name
origdst	Original IP address of the destination host (before translation or the application of a virtual connection). Decimal format. Example: ”192.168.200.1” Available from: SNS v1.0.0.
	Orig. destination
origdstport	Original port number of the destination TCP/UDP port (before translation or the application of a virtual connection). Example: "465" Available from: SNS v1.0.0.
	Orig. destination port

sent	Volume of application data sent (bytes). Example: "26657" Available from: SNS v1.0.0.
	Sent Example: "26 KB"
rcvd	Volume of application data received (bytes). Example: "26657" Available from: SNS v1.0.0.
	Received Example: "26 KB"
duration	Duration of the connection in seconds. Example: "0.5"
	Duration Example: “500 ms”
action	Behavior associated with the filter rule. Values: “pass” or “block”
	Action
risk	Risk relating to the connection. This value contributes to the reputation score of the connection's source host. Value: between 1 (low risk) and 100 (very high risk). Example: risk=20 Available from: SNS v3.0.0.
	Risk
slotlevel	Indicates the type of rule that activated logging. Values: “0” (implicit), “1” (global), or “2” (local). Available from: SNS v1.0.0.
	Rule level Values: “Implicit”, “Global” or “Local”.
rulename	Name of the filter rule applied Character string Example: rulename="myrule" Available from: SNS v3.2.0.
	Rule name

Fields specific to the "l_smtp", "l_pop3", "l_ftp" and "l_web" logs

The fields described below appear in the web administration interface of the firewall under the **Monitoring > Logs - Audit logs** module, in the views: **All logs**, **Network traffic**, **Web** and **E-mails**.

filename	Name of the file scanned by the sandboxing option. String of characters in UTF-8 format. Example: "mydocument.doc"
	File name

filetype	Type of file scanned by the sandboxing option. This may be a document (word processing, table, presentation, etc), a Portable Document Format file (PDF - Adobe Acrobat), and executable file or an archive. Value: "document", "pdf", "executable", "archive".
	File type
hash	Results of the file content hash (SHA2 method) String of characters in UTF-8 format. Example: "f4d1be410a6102b9ae7d1c32612bed4f12158df3cd1ab6440a9ac0cad417446d"
	Hash
sandboxinglevel	Indicates the level of the file's infection on a scale of 0 to 100. Value: "0" (clean) to "100" (malicious).
	Sandboxing score
sandboxing	Classification of the file according to the sandboxing option. Value: "clean", "suspicious", "malicious", "unknown", «forward", "failed". Sandboxing indicates a "clean", "suspicious" or "malicious" status if the file has already been scanned and classified. The "unknown" status is returned if sandboxing does not know the file concerned. In this case, the whole file will be sent to the firewall to be scanned.
	Sandboxing

Fields specific to the "l_smtp" log

The fields described below appear in the web administration interface of the firewall under the **Monitoring > Logs - Audit logs** module, in the views: **All logs**, **Network traffic** and **E-mails**.

ruleid	Number of the filter rule applied. Example: “1”, “2” … Available from: SNS v1.0.0.
	Rule
user	E-mail address of the sender. String of characters in UTF-8 format. Example: "john.doe@company1.com" May be displayed anonymously depending on the administrator's access privileges. Available from: SNS v1.0.0.
	User
dstname	E-mail address of the recipient. String of characters in UTF-8 format. Example: "john.doe@company2.com" Available from: SNS v1.0.0.
	Destination name
msg	Message associated with the SMTP command executed. String of characters in UTF-8 format. Example: “Connection interrupted”
	Message

spamlevel	Results of antispam processing on the message. Values: "X": error while processing the message. "? ": the nature of the message could not be determined. "0": non-spam message. "1", "2" or "3": criticality of the spam message, 3 being the most critical. Available from: SNS v1.0.0.
	Spam
virus	Message indicating whether a virus has been detected (the antivirus has to be enabled) Example: “clean”
	Virus Example: “clean”
ads	Indicates whether the antispam has detected an e-mail as an advertisement. Values: “0” or“1”.
	Advertisement
dstcontinent	Continent to which the destination IP address of the connection belongs. Value: continent's ISO code Example: dstcontinent="eu" Available from: SNS v3.0.0.
	Destination continent
dstcountry	Country to which the destination IP address of the connection belongs. Format: country's ISO code Example: dstcountry="fr" Available from: SNS v3.0.0.
	Destination country
dsthostrep	Reputation of the connection's target host. Available only if reputation management has been enabled for the relevant host. Format: unrestricted integer. Example: dsthostrep=506 Available from: SNS v3.0.0.
	Destination host reputation
dstiprep	Reputation of the destination IP address. Available only if this IP address is public and listed in the IP address reputation base. Value: "anonymizer", "botnet", "malware", "phishing", "tor", "scanner" or "spam". Example: dstiprep="spam" Available from: SNS v3.0.0.
	Public reputation of the destination IP address
srccontinent	Continent to which the source IP address of the connection belongs. Value: continent's ISO code Example: srccontinent="eu" Available from: SNS v3.0.0.
	Source continent

srccountry	Country to which the source IP address of the connection belongs. Format: country's ISO code Example: srccountry="fr" Available from: SNS v3.0.0.
	Source country
srchostrep	Reputation of the connection's source host. Available only if reputation management has been enabled for the relevant host. Format: unrestricted integer. Example: srchostrep=26123 Available from: SNS v3.0.0.
	Source host reputation
srciprep	Reputation of the source IP address. Available only if this IP address is public and listed in the IP address reputation base. Value: "anonymizer", "botnet", "malware", "phishing", "tor", "scanner" or "spam". Example: srciprep="anonymizer,tor" Available from: SNS v3.0.0.
	Public reputation of the source IP address
mailruleid	Number of the mail filter rule applied. Digital format Example: mailruleid=48 Available from: SNS v3.2.0.

Fields specific to the "l_pop3" log

The fields described below appear in the web administration interface of the firewall under the **Monitoring > Logs - Audit logs** module, in the views: **All logs**, **Network traffic** and **E-mails**.

ruleid	Number of the filter rule applied. Example: “1”, “2” … Available from: SNS v1.0.0.
	Rule
spamlevel	Results of antispam processing on the message. Values: "X": error while processing the message. "? ": the nature of the message could not be determined. "0": non-spam message. "1", "2" or "3": criticality of the spam message, 3 being the most critical. Available from: SNS v1.0.0.
	Spam
op	Operation on the POP3 server (RETR, LIST, ...) Example: “USER”
	Operation
virus	Message indicating whether a virus has been detected (the antivirus has to be enabled) Example: “clean”
	Virus Example: “clean”

msg	Message associated with the POP3 command executed. String of characters in UTF-8 format. Example: “Username rejected”
	Message
user	User’s login. String of characters in UTF-8 format. Example: "john.smith@company.com" May be displayed anonymously depending on the administrator's access privileges. Available from: SNS v1.0.0.
	User
ads	Indicates whether the antispam has detected an e-mail as an advertisement. Values: “0” or“1”.
	Advertisement
dstcontinent	Continent to which the destination IP address of the connection belongs. Value: continent's ISO code Example: dstcontinent="eu" Available from: SNS v3.0.0.
	Destination continent
dstcountry	Country to which the destination IP address of the connection belongs. Format: country's ISO code Example: dstcountry="fr" Available from: SNS v3.0.0.
	Destination country
dsthostrep	Reputation of the connection's target host. Available only if reputation management has been enabled for the relevant host. Format: unrestricted integer. Example: dsthostrep=506 Available from: SNS v3.0.0.
	Destination host reputation
dstiprep	Reputation of the destination IP address. Available only if this IP address is public and listed in the IP address reputation base. Value: "anonymizer", "botnet", "malware", "phishing", "tor", "scanner" or "spam". Example: dstiprep="spam" Available from: SNS v3.0.0.
	Public reputation of the destination IP address
srccontinent	Continent to which the source IP address of the connection belongs. Value: continent's ISO code Example: srccontinent="eu" Available from: SNS v3.0.0.
	Source continent
srccountry	Country to which the source IP address of the connection belongs. Format: country's ISO code Example: srccountry="fr" Available from: SNS v3.0.0.
	Source country

srchostrep	Reputation of the connection's source host. Available only if reputation management has been enabled for the relevant host. Format: unrestricted integer. Example: srchostrep=26123 Available from: SNS v3.0.0.
	Source host reputation
srciprep	Reputation of the source IP address. Available only if this IP address is public and listed in the IP address reputation base. Value: "anonymizer", "botnet", "malware", "phishing", "tor", "scanner" or "spam". Example: srciprep="anonymizer,tor" Available from: SNS v3.0.0.
	Public reputation of the source IP address

Fields specific to the "l_ftp" log

The fields described below appear in the web administration interface of the firewall under the **Monitoring > Logs - Audit logs** module, in the views: **All logs** and **Network traffic**.

arg	Argument of the FTP command (file forwarded, etc). String of characters in UTF-8 format. Example: “my_file.txt”
	Argument
op	Operation performed on the FTP server. Example: "LIST ", "RETR ", "QUIT "….
	Operation
groupid	ID number allowing the tracking of child connections. Example: “0”, “1”, “2” etc.
	Group
user	ID used for logging on to the FTP server. String of characters in UTF-8 format. Example: “john.smith” May be displayed anonymously depending on the administrator's access privileges. Available from: SNS v1.0.0.
	User
virus	Message indicating whether a virus has been detected (the antivirus has to be enabled) Example: “clean”
	Virus Example: “clean”
msg	Error message or additional information on the virus detected. String of characters in UTF-8 format. Example: “virus:EICAR-Test-File”
	Message

Fields specific to the "l_web" log

The fields described below appear in the web administration interface of the firewall under the **Monitoring > Logs - Audit logs** module, in the views: **All logs**, **Network traffic** and **Web**.

arg	Argument of the HTTP command. String of characters in UTF-8 format. Example: “/”, “/mapage.htm”…
	Argument
op	Operation on the http server. Example: “GET”, “PUT” ...
	Operation
result	Return code of the HTTP server. Example: “403”, “404”…
	Result
virus	Message indicating whether a virus has been detected (the antivirus has to be enabled) Example: “clean”
	Virus Example: “clean”
cat_site	Category (URL filtering) of the website visited. String of characters in UTF-8 format. Example: “{bank}”, “{news}”, etc. Available from: SNS v1.0.0.
	Category
user	Name of the user (when authentication is enabled). String of characters in UTF-8 format. Example: “John.smith” May be displayed anonymously depending on the administrator's access privileges. Available from: SNS v1.0.0.
	User
ruleid	Number of the filter rule applied. Example: "4" Available from: SNS v1.0.0.
	Rule
dstname	Name of the target website. String of characters in UTF-8 format. Example: “webserver.company.com” Available from: SNS v1.0.0.
	Destination name
msg	Additional message about the action performed. String of characters in UTF-8 format. Example: “Blocked url”
	Message
domain	Authentication method used or LDAP directory of the user authenticated by the firewall. String of characters in UTF-8 format. Example: domain="documentation.stormshield.eu" Available from: SNS v3.0.0.
	Method or directory

dstcontinent	Continent to which the destination IP address of the connection belongs. Value: continent's ISO code Example: dstcontinent="eu" Available from: SNS v3.0.0.
	Destination continent
dstcountry	Country to which the destination IP address of the connection belongs. Format: country's ISO code Example: dstcountry="fr" Available from: SNS v3.0.0.
	Destination country
dsthostrep	Reputation of the connection's target host. Available only if reputation management has been enabled for the relevant host. Format: unrestricted integer. Example: dsthostrep=506 Available from: SNS v3.0.0.
	Destination host reputation
dstiprep	Reputation of the destination IP address. Available only if this IP address is public and listed in the IP address reputation base. Value: "anonymizer", "botnet", "malware", "phishing", "tor", "scanner" or "spam". Example: dstiprep="spam" Available from: SNS v3.0.0.
	Public reputation of the destination IP address
srccontinent	Continent to which the source IP address of the connection belongs. Value: continent's ISO code Example: srccontinent="eu" Available from: SNS v3.0.0.
	Source continent
srccountry	Country to which the source IP address of the connection belongs. Format: country's ISO code Example: srccountry="fr" Available from: SNS v3.0.0.
	Source country
srchostrep	Reputation of the connection's source host. Available only if reputation management has been enabled for the relevant host. Format: unrestricted integer. Example: srchostrep=26123 Available from: SNS v3.0.0.
	Source host reputation
srciprep	Reputation of the source IP address. Available only if this IP address is public and listed in the IP address reputation base. Value: "anonymizer", "botnet", "malware", "phishing", "tor", "scanner" or "spam". Example: srciprep="anonymizer,tor" Available from: SNS v3.0.0.
	Public reputation of the source IP address

urlruleid	Number of the URL filter rule applied. Digital format. Example: urlruleid=12 Available from: SNS v3.2.0.

Fields specific to the "l_ssl" log

The fields described below appear in the web administration interface of the firewall under the **Monitoring > Logs - Audit logs** module, in the views: **All logs** and **Network traffic**.

user	ID of the user (when the authentication phase has ended). String of characters in UTF-8 format. Example: “John.smith” May be displayed anonymously depending on the administrator's access privileges. Available from: SNS v1.0.0.
	User
msg	Message associated with the action performed. String of characters in UTF-8 format. Example: "Connection not deciphered (rule matches: Nodecrypt)"
	Message
cat_site	*Category (URL filtering) of the website visited.* *String of characters in UTF-8 format.* *Example: “{bank}”, “{news}”, etc.* *Available from: SNS v1.0.0.*
	Category
arg	Additional information regarding the SSL negotiation Example: "Subject%... Issuer%... "
	Argument
domain	Authentication method used or LDAP directory of the user authenticated by the firewall. String of characters in UTF-8 format. Example: domain="documentation.stormshield.eu" Available from: SNS v3.0.0.
	Method or directory
dstcontinent	Continent to which the destination IP address of the connection belongs. Value: continent's ISO code Example: dstcontinent="eu" Available from: SNS v3.0.0.
	Destination continent
dstcountry	Country to which the destination IP address of the connection belongs. Format: country's ISO code Example: dstcountry="fr" Available from: SNS v3.0.0.
	Destination country

dsthostrep	Reputation of the connection's target host. Available only if reputation management has been enabled for the relevant host. Format: unrestricted integer. Example: dsthostrep=506 Available from: SNS v3.0.0.
	Destination host reputation
dstiprep	Reputation of the destination IP address. Available only if this IP address is public and listed in the IP address reputation base. Value: "anonymizer", "botnet", "malware", "phishing", "tor", "scanner" or "spam". Example: dstiprep="spam" Available from: SNS v3.0.0.
	Public reputation of the destination IP address
srccontinent	Continent to which the source IP address of the connection belongs. Value: continent's ISO code Example: srccontinent="eu" Available from: SNS v3.0.0.
	Source continent
srccountry	Country to which the source IP address of the connection belongs. Format: country's ISO code Example: srccountry="fr" Available from: SNS v3.0.0.
	Source country
srchostrep	Reputation of the connection's source host. Available only if reputation management has been enabled for the relevant host. Format: unrestricted integer. Example: srchostrep=26123 Available from: SNS v3.0.0.
	Source host reputation
srciprep	Reputation of the source IP address. Available only if this IP address is public and listed in the IP address reputation base. Value: "anonymizer", "botnet", "malware", "phishing", "tor", "scanner" or "spam". Example: srciprep="anonymizer,tor" Available from: SNS v3.0.0.
	Public reputation of the source IP address
cnruleid	Number of the SSL filter rule applied. Digital format. Example: cnruleid=3 Available from: SNS v3.2.0.
	Rule

Fields specific to the "l_auth" log

The fields described below appear in the web administration interface of the firewall under the **Monitoring > Logs - Audit logs** module, in the views: **All logs** and **Users**.

user	ID of the user (when the authentication phase has ended). String of characters in UTF-8 format. Example: “John.smith” May be displayed anonymously depending on the administrator's access privileges. Available from: SNS v1.0.0.
	User
src	IP address of the source host. Decimal format. Example: ”192.168.0.1” May be displayed anonymously depending on the administrator's access privileges. Available from: SNS v1.0.0
	Source
error	Authentication return code. Decimal format. Example: “0”, “3”, “4", etc.
	Status Example: “ok”, “Auth failed”, “Level denied”…
msg	Message associated with the authentication return code. String of characters in UTF-8 format. Example: ”User logged in”
	Message
ruleid	Number of the authentication rule applied (no value if the “AGENT” method is used). Example: "1" Available from: SNS v1.0.0.
	Rule
agentid	SSO agent ID. Value: from 0 to 5. Example: agentid=0 Available from: SNS v3.0.0.
	SSO Agent
domain	Authentication method used or LDAP directory of the user authenticated by the firewall. String of characters in UTF-8 format. Example: domain="documentation.stormshield.eu" Available from: SNS v3.0.0.
	Method or directory
confid	Index of the security inspection profile used. Value from “0” to “9”. Available from: SNS v1.0.0.
totp	Indicates whether authentication required a TOTP Values: "yes" if a TOTP was used, "no" if no TOTP was used. Example: totp=yes Available from: SNS v4.5.0.
	One-time password
tsagentname	Indicates the name of the TS agent used. String of characters in UTF-8 format. Example: tsagentname="agent_name_test" Available from: SNS v4.7.0.
	TS agent name

Fields specific to the "l_xvpn" log

The fields described below appear in the web administration interface of the firewall under the **Monitoring > Logs - Audit logs** module, in the views: **All logs**, **Network traffic** and **VPN**.

user	Name of the user accessing SSL VPN. String of characters in UTF-8 format. Example: “john.smith” May be displayed anonymously depending on the administrator's access privileges. Available from: SNS v1.0.0.
	User
arg	Argument of the executed command. String of characters in UTF-8 format. Example: “/documentation”
	Argument
error	Return code of the SSL VPN access. Example: “0”, “5”, “8", etc.
	Result Example: “Success”, “Access denied”, “Connect to host failed”…
msg	Message associated with the return code. String of characters in UTF-8 format. Example: “Access to host”, “Bad or no cookie found”…
	Message
src	IP address of the source host. Decimal format. Example: ”192.168.0.1” May be displayed anonymously depending on the administrator's access privileges. Available from: SNS v1.0.0.
	Source
srcname	Name of the object corresponding to the source host. String of characters in UTF-8 format. Example: “client_workstation” May be displayed anonymously depending on the administrator's access privileges. Available from: SNS v1.0.0.
	Source name
localnet	Network address used by the firewall to set up the SSL VPN tunnel Decimal format. Example: ”192.168.53.2”
	Local network
remotenet	Network address assigned to the client to set up the SSL VPN tunnel Decimal format. Example: ”192.168.53.3”
	Remote network
dst	IP address of the destination host Decimal format. Example: ”192.168.50.1” Available from: SNS v1.0.0.
	Destination

dstport	Destination port number. Decimal format. Example: "80" Available from: SNS v1.0.0.
	Destination port
dstportname	Name of the object corresponding to the destination port. String of characters in UTF-8 format. Example: “http” Available from: SNS v1.0.0.
	Dest. port name
dstname	Name of the object (FQDN name) corresponding to the destination host. String of characters in UTF-8 format. Example: “server.company.com” Available from: SNS v1.0.0.
	Destination name
domain	Authentication method used or LDAP directory of the user authenticated by the firewall. String of characters in UTF-8 format. Example: domain="documentation.stormshield.eu" Available from: SNS v3.0.0.
	Method or directory

Fields specific to the "l_sandboxing" log

The fields described below appear in the web administration interface of the firewall under the **Monitoring > Logs - Audit logs** module, in the views: **All logs** and **Sandboxing**.

hash	Results of the file content hash (SHA2 method) String of characters in UTF-8 format. Example: "f4d1be410a6102b9ae7d1c32612bed4f12158df3cd1ab6440a9ac0cad417446d"
	Hash
sandboxinglevel	Indicates the level of the file's infection on a scale of 0 to 100. Value: "0" (clean) to "100" (malicious).
	Sandboxing score
sandboxing	Classification of the file according to the sandboxing option. Value: "clean", "suspicious", "malicious", "unknown", «forward", "failed". The sandboxing option indicates a "clean", "suspicious" or "malicious" status if the file has already been scanned and classified. The "unknown" status is returned if sandboxing does not know the file concerned. In this case, the whole file will be sent to the firewall to be scanned.
	Sandboxing
msg	Message associated with the results of the sandboxing scan. String of characters in UTF-8 format. Example: "Virus name: thisvirus".
	Message

dstcontinent	Continent to which the destination IP address of the connection belongs. Value: continent's ISO code Example: dstcontinent="eu" Available from: SNS v3.0.0.
	Destination continent
dstcountry	Country to which the destination IP address of the connection belongs. Format: country's ISO code Example: dstcountry="fr" Available from: SNS v3.0.0.
	Destination country
dsthostrep	Reputation of the connection's target host. Available only if reputation management has been enabled for the relevant host. Format: unrestricted integer. Example: dsthostrep=506 Available from: SNS v3.0.0.
	Destination host reputation
dstiprep	Reputation of the destination IP address. Available only if this IP address is public and listed in the IP address reputation base. Value: "anonymizer", "botnet", "malware", "phishing", "tor", "scanner" or "spam". Example: dstiprep="spam" Available from: SNS v3.0.0.
	Reputation of the dest.
risk	Risk relating to the connection. This value contributes to the reputation score of the connection's source host. Value: between 1 (low risk) and 100 (very high risk). Example: risk=20 Available from: SNS v3.0.0.
	Risk
srccontinent	Continent to which the source IP address of the connection belongs. Value: continent's ISO code Example: srccontinent="eu" Available from: SNS v3.0.0.
	Source continent
srccountry	Country to which the source IP address of the connection belongs. Format: country's ISO code Example: srccountry="fr" Available from: SNS v3.0.0.
	Source country
srchostrep	Reputation of the connection's source host. Available only if reputation management has been enabled for the relevant host. Format: unrestricted integer. Example: srchostrep=26123 Available from: SNS v3.0.0.
	Source host reputation

srciprep	Reputation of the source IP address. Available only if this IP address is public and listed in the IP address reputation base. Value: "anonymizer", "botnet", "malware", "phishing", "tor", "scanner" or "spam". Example: srciprep="anonymizer,tor" Available from: SNS v3.0.0.
	Reputation of the src.
proto	Name of the associated plugin. If this is not available, the name of the standard service corresponding to the destination port. String of characters in UTF-8 format. Example: “http”, “ssh” Available from: SNS v1.0.0.
	Protocol
service	Service (product with a dedicated port) on which the vulnerability was detected. String of characters in UTF-8 format. Example: “OpenSSH_5.4”
	Vulnerability management / Service

Fields specific to the “l_filterstat” log

SavedEvaluation	Number of rule evaluations that did not use intrusion prevention technology.
DynamicMem	Percentage of the ASQ’s dynamic memory in use. Value from “0” to “100”.
HostMem	Percentage of memory allocated to a host processed by the Firewall. Value from “0” to “100”.
FragMem	Percentage of memory allocated to the treatment of fragmented packets. Value from “0” to “100”.
ICMPMem	Percentage of memory allocated to ICMP. Value from “0” to “100”.
ConnMem	Percentage of memory allocated to connections. Value from “0” to “100”.
DtrackMem	Percentage of memory used for data tracking (TCP/UDP packets). Value from “0” to “100”.
IPStateMem	Percentage of memory allocated to processing pseudo-connections relating to protocols other than TCP, UDP or ICMP (e.g.: GRE) that have passed through the firewall.
IPStateConn	Number of active pseudo-connections relating to protocols other than TCP, UDP or ICMP (e.g.: GRE).
IPStateConnNatDst	Number of active pseudo-connections with address translation on the destination.
IPStateConnNatSrc	Number of active pseudo-connections with address translation on the source.
IPStateConnNoNatDst	Number of active pseudo-connections that explicitly include "No NAT" instructions on the destination.

IPStateConnNoNatSrc	Number of active pseudo-connections that explicitly include "No NAT" instructions on the source.
IPStatePacket	Number of network packets originating from protocols other than TCP, UDP or ICMP (e.g.: GRE) that have passed through the firewall.
IPStateByte	Number of bytes exchanged for pseudo-connections. This value includes incoming and outgoing bytes.
Logged	Number of log lines generated by the intrusion prevention engine.
LogOverflow	Number of log lines that could not be generated by the intrusion prevention engine.
PvmFacts	Number of events sent by ASQ to the vulnerability management process.
PvmOverflow	Number of events intended for the vulnerability management process that were ignored by ASQ.
Accepted	Number of packets corresponding to the application of “Pass” rules. Example: Accepted=2430.
Blocked	Number of packets corresponding to the application of “Block” rules. Example: Blocked=1254.
Byte(i/o)	Number of bytes (incoming/outgoing) that have passed through the Firewall. Example: Byte (i/o)=527894/528486.
Fragmented	Number of fragmented packets that have passed through the Firewall.
TCPPacket	Number of TCP packets that have passed through the Firewall.
TCPByte(i/o)	Number of TCP bytes (incoming/outgoing) that have passed through the firewall. Example: TCPByte (i/o)=527894/528486.
TCPConn	Number of TCP connections that have passed through the Firewall.
TCPConnNatSrc	Number of TCP connections with a translated source.
TCPConnNatDst	Number of TCP connections with a translated destination.
UDPPacket	Number of UDP packets that have passed through the Firewall.
UDPByte(i/o)	Number of UDP bytes (incoming/outgoing) that have passed through the Firewall. Example: “527894/528486”
UDPConn	Number of UDP connections that have passed through the Firewall.
UDPConnNatSrc	Number of UDP connections with a translated source.
UDPConnNatDst	Number of UDP connections with a translated destination.
ICMPPacket	Number of ICMP packets that have passed through the Firewall.
ICMPByte(i/o)	Number of ICMP bytes (incoming/outgoing) that have passed through the Firewall. Example: ICMPByte(i/o) =527894/528486

HostrepScore	Average reputation score of monitored hosts. Value: decimal integer between 0 and 65535. Example: HostrepScore=1234 Available from: SNS v3.0.0.
HostrepMax	Highest reputation score of monitored hosts. Value: decimal integer between 0 and 65535. Example: HostrepMax=6540 Available from: SNS v3.0.0.
HostrepRequests	Number of reputation score requests submitted. Value: unrestricted decimal integer. Example: HostrepRequests=445 Available from: SNS v3.0.0.
SCTPAssocPacket	Number of packets exchanged for an SCTP association. Digital format. Example: SCTPAssocPacket=128 Available from: SNS v3.9.0.
SCTPAssocByte(i/o)	Number of bytes (incoming/outgoing) that have passed through the firewall for an SCTP association. Digital format. Example: SCTPAssocByte(i/o)=9728/9576. Available from: SNS v3.9.0.
SCTPAssoc	Number of SCTP associations. Digital format. Example: SCTPAssoc=2. Available from: SNS v3.9.0.
EtherStatePacket	Number of packets for Ethernet traffic without IP layer. Digital format. Example: EtherStatePacket=128 Available from: SNS v4.0.0.
EtherStateByte(i/o)	Number of bytes (incoming/outgoing) for Ethernet traffic without IP layer. Digital format. Example: EtherStateByte(i/o)=9728/9576 Available from: SNS v4.0.0.
EtherStateConn	Number of stateful statuses for Ethernet exchanges without IP layer. Digital format. Example: EtherStateConn=0 Available from: SNS v4.0.0.
TLSCertCacheEntriesNb	Number of entries currently in the TLS certificate cache. Digital format. Example: TLSCertCacheEntriesNb=3456 Available from: SNS v4.3.0
TLSCertCacheLookup (miss/total)	Number of lookups missed/performed in the TLS certificate cache. Digital format. Example: TLSCertCacheLookup(miss/total)=128/136 Available from: SNS v4.3.0
TLSCertCacheInsert	Number of entries inserted in the TLS certificate cache. Digital format. Example: TLSCertCacheInsert=789 Available from: SNS v4.3.0

TLSCertCacheFlushOp	Number of "flush" operations (manual deletion of entries, or after reloading signatures) performed on the TLS certificate cache. Digital format. Example: TLSCertCacheFlushOp=7 Available from: SNS v4.3.0
TLSCertCachePurgeOp	Number of "purge" operations (automatic deletion of a percentage of entries when the cache reaches full capacity) performed on the TLS certificate cache. Digital format. Example: TLSCertCachePurgeOp=4 Available from: SNS v4.3.0
TLSCertCacheFlushedNb	Number of entries deleted from the TLS certificate cache after a "flush" operation. Digital format. Example: TLSCertCacheFlushedNb=123 Available from: SNS v4.3.0
TLSCertCachePurgedNb	Number of entries deleted from the TLS certificate cache after a "purge" operation. Digital format. Example: TLSCertCachePurgedNb=456 Available from: SNS v4.3.0
TLSCertCacheExpiredNb	Number of entries deleted from the TLS certificate cache after a TTL expired. Digital format. Example: TLSCertCacheExpiredNb=789 Available from: SNS v4.3.0

Fields specific to the "l_count" log

RuleX:Y	Indicates the number of bytes that have passed through the designated rule.
	• X: corresponds to a category
	  • "0": implicit filter rule.
	  • "1": global filter rule.
	  • "2": local filter rule.
	  • "3": implicit NAT rule.
	  • "4": global NAT rule.
	  • "5": local NAT rule.
	• Y: corresponds to the number of the rule in the active policy.
	Example: "Rule2:8=1612e means that 1612 bytes have passed through the 8th local filter rule in the active policy.

Fields specific to the "l_routerstat" log

router	Name of the monitored router. String of characters in UTF-8 format. Example: router=routerICMP. Available from: SNS v4.3.0.

gw	Name of the monitored gateway. String of characters in UTF-8 format. Example: gw=gw123. Available from: SNS v4.3.0.
latency	Indicates the average, minimum and maximum latency over a regular interval, depending on the configuration (ms). String of characters in UTF-8 format. Example: latency=70,50,100. Available from: SNS v4.3.0.
jitter	Indicates the average, minimum and maximum jitter (variation in latency) over a regular interval, depending on the configuration (ms). String of characters in UTF-8 format. Example: jitter=5,0,20. Available from: SNS v4.3.0.
lossrate	Indicates the average rate of packet loss (%) over the last 15 minutes. String of characters in UTF-8 format. Example: lossrate=10. Available from: SNS v4.3.0.
unreachrate	Indicates the percentage of time the gateway could not be accessed over the last 15 minutes. String of characters in UTF-8 format. Example: unreachrate=0. Available from: SNS v4.3.0.
uprate	Indicates the percentage of time the status of the gateway was active over the last 15 minutes. String of characters in UTF-8 format. Example: uprate=0. Available from: SNS v4.3.0.
downrate	Indicates the percentage of time the gateway could not be reached over the last 15 minutes. String of characters in UTF-8 format. Example: downrate=0. Available from: SNS v4.3.0.

Further reading

Additional information and responses to questions you may have about the SNS logs are available in the Stormshield knowledge base (authentication required).

documentation@stormshield.eu