TECHNICAL NOTE
STORMSHIELD NETWORK SECURITY

DESCRIPTION OF AUDIT LOGS

Product concerned: SNS 5.0.1 Beta

Document last updated: May 20, 2025

Reference: sns-en-description_of_audit_logs_technical_note_v5

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_dmrouting	Events related to the dynamic multicast routing service: traffic, receiver subscription/unsubscription ...

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_routing	Routing service events: changes to dynamic routes, adjacency states, etc.
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).

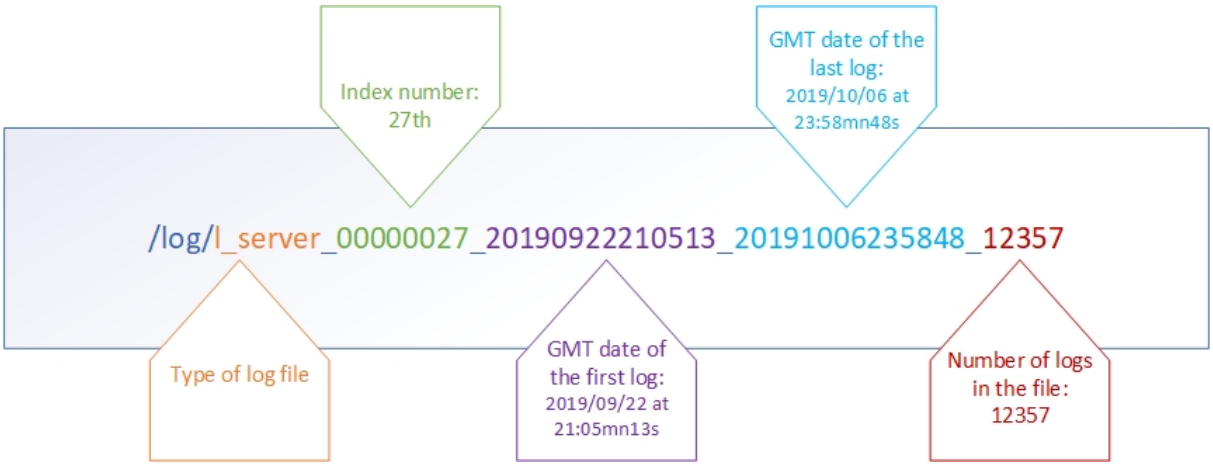
Archive names

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, please 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 **Monitoring > Logs - Audit logs > Filtering** module 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

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="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
```

Log fields are classified in alphabetical order in the following sections. Their descriptions are presented in this format:

Field name	Description of the field Format of the field. Example: "*raw value*". Example. SNS version number in which the field appeared.
	Name of the field in the administration interface, if different from the name that appears in log files.

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

Some log files, such as *l_filterstat*, *l_routerstat* and *l_count*, which are used for the calculation of statistics, contain a very large number of 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="2019-01-01 01:00:00" fw="U800SXXXXXXXXXX" tz=+0100
startime="2019-01-01 01:00:17" datechange=1 duration=-18
```

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

Specific fields

The logs *"l_server"*, *"l_auth"*, *"l_vpn"* and *"l_system"* contain fields that are specific to Stormshield Network firewalls.

These special fields, which are not in WELF format, are described below:

fw	Firewall 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: v1.0.0 SNS Affected logs: l_alarm, l_auth, l_connection, l_count, l_date, l_filter, l_filterstat, l_ftp, l_monitor, l_plugin, l_pop3, l_sandboxing, l_server, l_smtp, l_ssl, l_system, l_vpn, l_web, l_xvpn and l_routerstat, l_dmrouting.
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: v1.0.0 SNS Affected logs: l_alarm, l_auth, l_connection, l_count, l_date, l_filter, l_filterstat, l_ftp, l_monitor, l_plugin, l_pop3, l_sandboxing, l_server, l_smtp, l_ssl, l_system, l_vpn, l_web, l_xvpn and l_routerstat, l_dmrouting, l_routing.
	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.
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: v1.0.0 SNS Affected logs: l_alarm, l_auth, l_connection, l_count, l_date, l_filter, l_filterstat, l_ftp, l_monitor, l_plugin, l_pop3, l_sandboxing, l_server, l_smtp, l_ssl, l_system, l_vpn, l_web, l_xvpn and l_routerstat, l_dmrouting, l_routing.
	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.
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: v1.0.0 SNS Affected logs: l_alarm, l_auth, l_connection, l_count, l_date, l_filter, l_filterstat, l_ftp, l_monitor, l_plugin, l_pop3, l_sandboxing, l_server, l_smtp, l_ssl, l_system, l_vpn, l_web, l_xvpn and l_routerstat, l_dmrouting, l_routing.
	Time difference between local time and GMT time Example: "*gmt +01:00*"

Fields classified in alphabetical order and their descriptions

A

Accepted	Number of packets corresponding to the application of "Pass" rules. Example: Accepted=2430. Affected logs: l_filterstat.
action	Behavior associated with the filter rule. Value: "*Pass*" or "*Block*" (empty field for "Log"). Example: action=block. Affected logs: l_alarm, l_connection, l_filter, l_ftp, l_plugin, l_pop3, l_smtp, l_ssl and l_web.
	Action
address	IP address of the client workstation that initiated the connection. Decimal format. Example: address=192.168.0.2. Affected logs: l_server.
	Source
ads	Indicates whether the antispam has detected an e-mail as an advertisement. Values: "0" or "1". Example: ads=1. Affected logs: l_pop3 and l_smtp.
	Advertisement
agentid	SSO agent ID. Value: from 0 to 5. Example: agentid=0 Available from: SNS v3.0.0. Affected logs: l_auth.
	SSO Agent
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: agg01=Production_LACP,61515,128648,788241,1890520,2130,21. Affected logs: l_monitor.

alarmid	Stormshield Network alarm ID Decimal format. Example: "*85*". Affected logs: l_alarm and l_system.
	Alarm ID
arg	Argument of the HTTP command. String of characters in UTF-8 format. Example: "/", "/mypage.htm"… Affected logs: l_ftp, l_plugin, l_sandboxing, l_ssl, l_web and l_xvpn.
	Argument

B

Blocked	Number of packets corresponding to the application of "Block" rules. Example: Blocked=1254. Affected logs: l_filterstat.
Byte(i/o)	Number of bytes (incoming/outgoing) that have passed through the Firewall. Example: Byte (i/o)=527894/528486. Affected logs: l_filterstat.

C

caller	Caller ID. String of characters in UTF-8 format. Example: ""John" <sip:193@192.168.0.1>". Affected logs: l_plugin (RTP, RTCP, Media_UDP and Media_UDP).
	Caller
callee	Callee ID. String of characters in UTF-8 format. Example: "sip:192@192.168.1.1:5060;line=g842aca6eddb2a5". Affected logs: l_plugin (RTP, RTCP, Media_UDP and Media_UDP).
	Callee
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. Affected logs: l_ssl and l_web.
	Category
class	Information about the alarm's category. String of characters in UTF-8 format. Example: "*protocol*", "*system*", "*filter*", … Affected logs: l_alarm.
	Context

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. Affected logs: l_plugin.
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. Affected logs: l_plugin.
clientappid	Last client application detected on the connection. Character string. Example: clientappid=*firefox* Available from: v3.2.0 SNS Affected logs: l_connection and l_plugin.
	Client application
cnruleid	Number of the SSL filter rule applied. Digital format. Example: cnruleid=3. Available from: SNS v3.2.0. Affected logs: l_ssl.
	Rule
clientversion	Version of SSL VPN client used to establish SSL VPN tunnel (only when Hostchecking is enabled). Format : major.minor.build Example : clientversion=4.0.3 Available from: SNS v4.8.0. Affected logs: l_xvpn.
confid	Index of the security inspection profile used. Value from "00" to "09 ". Example: confid=01. Available from: SNS v1.0.0. Affected logs: l_alarm, l_auth, l_connection, l_filter, l_ftp, l_plugin, l_pop3, l_smtp, l_ssl and l_web.
ConnMem	Percentage of memory allocated to connections. Value from “0” to “100”. Example: ConnMem=1. Affected logs: l_filterstat.
contentpolicy	Index of the filter profile used. Value from "00" to "09 ". Example: contentpolicy=00 Available from: SNS v1.0.0. Affected logs: l_pop3, l_smtp, l_ssl and l_web.
cookie_i	Temporary identity marker of the initiator of the negotiation. Character string in hexadecimal. Example: cookie_i=0xae34785945ae3cbf Affected logs: l_vpn.
	Initiating cookie

cookie_r	Temporary identity marker of the peer of the negotiation. Character string in hexadecimal. Example: cookie_r=0x56201508549a6526. Affected logs: l_vpn.
	Receiving cookie
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 Affected logs: l_monitor.
	System monitoring / CPU load

D

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. Affected logs: l_alarm, l_auth, l_connection, l_plugin, l_server, l_ssl, l_web and l_xvpn.
	Method or directory
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. Affected logs: l_routerstat.
drcompliant	Indicates whether the correspondent is compatible with DR mode. Values : 0 or 1. Example : drcompliant=1. Available from: SNS v5.0.1 Affected logs: l_vpn.
	DR compliant
dst	IP address of the destination host Decimal format. Example: "*192.168.0.2*" Available from: v1.0.0 SNS Affected logs: l_alarm, l_connection, l_filter, l_ftp, l_plugin, l_pop3, l_sandboxing, l_smtp, l_ssl, l_vpn and l_web, l_dmrouting.
	Destination

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. Affected logs: l_alarm, l_connection, l_filter, l_plugin, l_pop3, l_sandboxing, l_smtp, l_ssl and l_web.
	Destination continent
dstcountry	Country to which the destination IP address of the connection belongs. Format: country's ISO code Example: dstcountry="fr" Available from: v3.0.0 SNS Affected logs: l_alarm, l_connection, l_filter, l_ftp, l_plugin, l_pop3, l_sandboxing, l_smtp, l_ssl, l_vpn and l_web.
	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=41 Available from: v3.0.0 SNS Affected logs: l_alarm, l_connection, l_filter, l_plugin, l_pop3, l_sandboxing, l_smtp, l_ssl and l_web.
	Destination host reputation
dstif	Name of the destination interface. String of characters in UTF-8 format. Example: dstif=Ethernet 1. Available from: SNS v1.0.0. Affected logs: l_alarm, l_connection, l_filter and l_plugin, l_dmrouting.
	Dest. interf. (ID)
dstifname	Name of the object representing the traffic's destination interface. String of characters in UTF-8 format. Example: dstifname=dmz1. Available from: SNS v1.0.0. Affected logs: l_alarm, l_connection, l_filter and l_plugin, l_dmrouting.
	Dest. interf.
dstiprep	Reputation of the destination IP address. Available only if this IP address is public and listed in the IP address reputation base. Values: "*anonymizer*", "*botnet*", "*malware*", "*phishing*", "*tor*", "*scanner*" or "*spam*". Example: dstiprep=spam. Available from: SNS v3.0.0. Affected logs: l_alarm, l_connection, l_filter, l_plugin, l_pop3, l_sandboxing, l_smtp, l_ssl and l_web.
	Public reputation of the destination 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. Affected logs: l_alarm, l_connection and l_plugin.
	Destination MAC address
dstname	Name of the object corresponding to the IP address of the destination host. String of characters in UTF-8 format. Example: dstname=intranet_server. Available from: SNS v1.0.0. Affected logs: l_alarm, l_connection, l_filter, l_ftp, l_plugin, l_pop3, l_sandboxing, l_smtp, l_ssl, l_vpn, l_web and l_xvpn, l_dmrouting.
	Destination name
dstport	Destination TCP/UDP port number. Example: dstport=22. Available from: SNS v1.0.0. Affected logs: l_alarm, l_connection, l_filter, l_ftp, l_plugin, l_pop3, l_sandboxing, l_smtp, l_ssl, l_web and l_xvpn.
	Destination port
dstportname	Name of the object corresponding to the destination port. String of characters in UTF-8 format. Example: dstportname=ssh. Available from: SNS v1.0.0. Affected logs: l_alarm, l_connection, l_filter, l_ftp, l_plugin, l_pop3, l_sandboxing, l_smtp, l_ssl, l_web and l_xvpn.
	Dest. port name
DtrackMem	Percentage of memory used for data tracking (TCP/UDP packets). Value from "0" to "100". Affected logs: l_filterstat.
duration	Duration of the connection in seconds. Decimal format. Example: "*173.15*"
	Duration Example: "*2m 53s 15*"
DynamicMem	Percentage of the ASQ's dynamic memory in use. Value from "0" to "100". Affected logs: l_filterstat.

E

error	Return code from the authentication attempt or command. Example: error=1. Affected logs: l_auth, l_server and l_xvpn.
	Result Example: "Success", "Access denied", "Connect to host failed"…

error_class	Number of the error class in an S7 response. Digital format. Example: error_class=0. Available from: SNS v2.3.0. Affected logs: l_plugin.
error_code	Error code in the error class specified in the S7 response. Digital format. Example: error_code=0. Available from: SNS v2.3.0. Affected logs: l_plugin.
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". Affected logs: l_monitor.
	Interface monitoring / Bandwidth use
etherproto	Type of Ethernet protocol. Format: String of characters in UTF-8 format. Example: etherproto="profinet-rt" Available from: SNS v4.0.0. Affected logs: l_alarm, l_connection and l_plugin.
	Ethernet protocol
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. Affected logs: l_filterstat.
EtherStateConn	Number of stateful statuses for Ethernet exchanges without IP layer. Digital format. Example: EtherStateConn=0. Available from: SNS v4.0.0. Affected logs: l_filterstat.
EtherStatePacket	Number of packets for Ethernet traffic without IP layer. Digital format. Example: EtherStatePacket=128. Available from: SNS v4.0.0. Affected logs: l_filterstat.

F

filename	Name of the file scanned by the sandboxing option. String of characters in UTF-8 format. Example: filename="mydocument.doc". Affected logs: l_ftp, l_pop3, l_sandboxing, l_smtp and l_web.
	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". Example: filetype=archive. Affected logs: l_ftp, l_pop3, l_sandboxing, l_smtp and l_web.
	File type
format	Type of message for IEC104 Character in UTF-8 format. Example: format=U. Available from: SNS v3.1.0. Affected logs: l_plugin.
FragMem	Percentage of memory allocated to the treatment of fragmented packets. Value from “0” to “100”. Example: FragMem=2. Affected logs: l_filterstat.
Fragmented	Number of fragmented packets that have passed through the Firewall. Example: Fragmented=12. Affected logs: l_filterstat.

G

gw	Name of the monitored gateway. String of characters in UTF-8 format. Example: gw=Inet_gw. Available from: SNS v4.3.0. Affected logs: l_routerstat.
group	Code of the *"userdata"* group for an S7 message. Digital value. Example: group=4. Available from: SNS v2.3.4. Affected logs: l_plugin.
groupid	ID number allowing the tracking of child connections. Example: groupid=1. Affected logs: l_ftp and l_plugin.
	Group

H

hash	Results of the file content hash (SHA2 method) String of characters in UTF-8 format. Example: hash= f4d1be410a6102b9ae7d1c32612bed4f12158df3cd1ab6440a9ac0cad417446d. Affected logs: l_ftp, l_pop3, l_sandboxing, l_smtp and l_web.
	Hash
hotschecking	Status during authentication by the SSL VPN service associated with Hostchecking. Values: • "conforming" whether Hostchecking requirements have been met, • "non conforming" if requirements are not met, • "disabled" if Hostchecking is disabled. Example : hotschecking=conforming. Available from: SNS v4.8.0. Affected logs: l_xvpn.
hotscheckingdetails	Origin of the error during authentication by the SSL VPN service associated with Hostchecking. String of characters in UTF-8 format. Example : hotscheckingdetails="Invalid criteria: criterion=[OsVersion]windows_version='1';". Available from: SNS v4.8.0. Affected logs: l_xvpn.
HostMem	Percentage of memory allocated to a host processed by the Firewall. Value from “0” to “100”. Example: HostMem=4 Affected logs: l_filterstat.
HostrepScore	Average reputation score of monitored hosts. Value: decimal integer between 0 and 65535. Example: HostrepScore=1234 Available from: SNS v3.0.0. Affected logs: l_filterstat.
HostrepMax	Highest reputation score of monitored hosts. Value: decimal integer between 0 and 65535. Example: HostrepMax=6540 Available from: SNS v3.0.0. Affected logs: l_filterstat.
HostrepRequests	Number of reputation score requests submitted. Value: unrestricted decimal integer. Example: HostrepRequests=445 Available from: SNS v3.0.0. Affected logs: l_filterstat.

I

ICMPByte(i/o)	Number of ICMP bytes (incoming/outgoing) that have passed through the Firewall. Example: ICMPByte(i/o) =527894/528486 Affected logs: l_filterstat.
icmpcode	Code number of the ICMP message, based on ICMP type. Digital format. See the list of ICMP parameters at: http://www.iana.org/assignments/icmp-parameters/icmp-parameters.xhtml. Example: icmpcode=1 (meaning "*Host unreachable*"). Available from: SNS v1.0.0. Affected logs: l_alarm and l_filter.
	ICMP code
icmptype	ICMP message type number. Digital format. See the list of ICMP parameters at: http://www.iana.org/assignments/icmp-parameters/icmp-parameters.xhtml. Example: icmptype=3 (meaning "*Destination unreachable*"). Available from: SNS v1.0.0. Affected logs: l_alarm and l_filter.
	ICMP type
ICMPMem	Percentage of memory allocated to ICMP. Value from “0” to “100”. Example: ICMPMem=2 Affected logs: l_filterstat.
ICMPPacket	Number of ICMP packets that have passed through the Firewall. Example: ICMPPacket=0. Affected logs: l_filterstat.
id	Type of product. This field constantly has the value"*firewall*" for logs on the firewall. Affected logs: l_alarm, l_auth, l_connection, l_count, l_date, l_filter, l_filterstat, l_ftp, l_monitor, l_plugin, l_pop3, l_sandboxing, l_server, l_smtp, l_ssl, l_system, l_vpn, l_web, l_xvpn and l_routerstat, l_dmrouting.
ikev	Version of the IKE protocol used Values: “1” or “2”. Example: ikev=1. Affected logs: l_vpn.
	IKE version
ipproto	Name of the protocol above IP (transport layer). String of characters in UTF-8 format. Example: ipproto=tcp. Available from: v1.0.0 SNS Affected logs: l_alarm, l_connection, l_filter, l_plugin.
	Internet Protocol

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: ipsec=ipsec,61515,128648,788241,1890520,2130,21. Affected logs: l_vpn.
IPStateByte (i/o)	Number of bytes exchanged for pseudo-connections. This value includes incoming and outgoing bytes. Example: IPStateByte(i/o)=0/40. Affected logs: l_filterstat.
IPStateConn	Number of active pseudo-connections relating to protocols other than TCP, UDP or ICMP (e.g.: GRE). Example: IPStateConn=0. Affected logs: l_filterstat.
IPStateConnNatDst	Number of active pseudo-connections with address translation on the destination. Example: IPStateConnNatDst=0. Affected logs: l_filterstat.
IPStateConnNatSrc	Number of active pseudo-connections with address translation on the source. Example: IPStateConnNatSrc=0. Affected logs: l_filterstat.
IPStateConnNoNatDst	Number of active pseudo-connections that explicitly include "No NAT" instructions on the destination. Example: IPStateConnNoNatDst=0. Affected logs: l_filterstat.
IPStateConnNoNatSrc	Number of active pseudo-connections that explicitly include "No NAT" instructions on the source. Example: IPStateConnNoNatSrc=0. Affected logs: l_filterstat.
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. Example: IPStateMem=1. Affected logs: l_filterstat.
IPStatePacket	Number of network packets originating from protocols other than TCP, UDP or ICMP (e.g.: GRE) that have passed through the firewall. Example: IPStatePacket=2. Affected logs: l_filterstat.

ipv	Version of the IP protocol used in the traffic Values: "*4*" or "*6*". Example: ipv=4. Available from: SNS v1.0.0. Affected logs: l_alarm, l_connection, l_filter, l_ftp, l_plugin, l_pop3, l_smtp, l_ssl and l_web.
	IP version

J

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. Affected logs: l_routerstat.

L

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. Affected logs: l_routerstat.
localnet	Local network negotiated in phase2. Decimal format. Example: localnet=192.168.0.1/24. Affected logs: l_vpn and l_xvpn.
	Local network
LogOverflow	Number of log lines that could not be generated by the intrusion prevention engine. Example: LogOverflow=0. Affected logs: l_filterstat.
Logged	Number of log lines generated by the intrusion prevention engine. Example: Logged=461634616. Affected logs: l_filterstat.

loopbackXX	Indicators of bandwidth used by loopback 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: loopback1=loopback1,61515,128648,788241,1890520,2130,21.
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. Affected logs: l_routerstat.

M

mailruleid	Number of the mail filter rule applied. Digital format. Example: mailruleid=48 Available from: SNS v3.2.0. Affected logs: l_smtp.
mc_cat	Multicast event category. String of characters in UTF-8 format. Example: mc_cat="receiver". Available from: SNS v4.8.0. Affected logs: l_dmrouting.
mc_grp	IP address of event-related multicast group. Decimal format. Example: mc_grp="231.1.1.2". Available from: SNS v4.8.0. Affected logs: l_dmrouting.
mc_grpname	Name of the object corresponding to the multicast group linked to the event. String of characters in UTF-8 format. Example: mc_grpname="mc_ssm_test_grp". Available from: SNS v4.8.0. Affected logs: l_dmrouting.
mc_src	IP address of event-related multicast source. Decimal format. Example: mc_src="10.50.30.91". Available from: SNS v4.8.0. Affected logs: l_dmrouting.
media	Type of traffic detected (audio, video, application, etc). String of characters in ASCII format. Example: media=control. Affected logs: l_plugin (RTP, RTCP, Media_UDP and Media_UDP).

modsrc	Translated IP address of the source host. May be displayed anonymously depending on the administrator's access privileges. Decimal format. Example: modsrc=192.168.0.1. Available from: SNS v1.0.0. Affected logs: l_connection, l_ftp, l_plugin, l_pop3, l_smtp, l_ssl and l_web.
	Translated source address
modsrcport	Number of the translated TCP/UDP source port. Example: modsrcport=49690. Available from: SNS v1.0.0. Affected logs: l_connection, l_ftp, l_plugin, l_pop3, l_smtp, l_ssl and l_web.
	Translated source port
msg	Additional message. String of characters in UTF-8 format. Example: msg="Access to host", msg="Bad or no cookie found", msg="Blocked url", msg="Phase established", msg="Asynchronous reload is enabled|disabled"… Affected logs: l_alarm, l_auth, l_ftp, l_sandboxing, l_server, l_pop3, l_smtp, l_ssl, l_system, l_vpn, l_web, l_xvpn and l_plugin, l_dmrouting, l_routing.
	Message

O

op	Operation performed on the server (FTP, HTTP, etc.). Example: op="GET", op="LIST"... Affected logs: l_ftp, l_plugin, l_sandboxing and l_web.
	Operation
origdst	Original IP address of the destination host (before translation or the application of a virtual connection). Decimal format. Example : origdst=192.168.200.1. Available from: SNS v1.0.0. Affected logs: l_alarm, l_connection, l_ftp, l_plugin, l_pop3, l_smtp, l_ssl and l_web.
	Orig. destination
origdstport	Original port number of the destination TCP/UDP port (before translation or the application of a virtual connection). Example: origdstport=53. Available from: SNS v1.0.0. Affected logs: l_alarm, l_connection, l_ftp, l_plugin, l_pop3, l_smtp, l_ssl and l_web.
	Orig. destination port
ostype	Operating system of the user. String of characters in UTF-8 format. Example: ostype="Windows" Available from: SNS v4.8.3. Affected logs: l_xvpn.

P

phase	Number of the IPSec VPN tunnel negotiation phase. Values: “0” (no phase), “1” (phase 1) or “2” (phase 2). Example: phase=1. Affected logs: l_vpn.
	Phase
pktdump	Network packet captured and encoded in hexadecimal for deeper analysis by a third-party tool. Example: pktdump="*450000321fd240008011c2f50a00007b0a3c033d0035c*" Affected logs: l_alarm.
	Captured packet
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: pktdumplen=28. Affected logs: l_alarm.
	Size of the packet captured
pktlen	Size of the network packet that activated the alarm (in bytes). Example: pktlen=33. Affected logs: l_alarm.
	Packet size
ppkid	Identifier of the post-quantum pre-shared key (ppk) used to establish the IPsec tunnel. String of characters in UTF-8 format. Example: « identifier_of_the_ppk_used ». Affected logs: l_vpn.
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). Set to “5” (“notice”) to ensure WELF compatibility in the following logs: l_smtp, l_pop3, l_ftp, l_web, l_ssl, l_system and l_vpn. Example: pri=1. Available from: SNS v1.0.0. Affected logs: l_alarm, l_connection, l_filter, l_ftp, l_plugin, l_pop3, l_smtp, l_ssl, l_system, l_vpn and l_web, l_routing.
	Priority
proto	Name of the standard service corresponding to the destination port. String of characters in UTF-8 format. Example: proto=http. Available from: SNS v1.0.0. Affected logs: l_alarm, l_connection, l_filter, l_ftp, l_plugin, l_sandboxing, l_pop3, l_smtp, l_ssl and l_web, l_routing.
	Protocol

Q

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”. Affected logs: l_monitor.
	QoS monitoring / Bandwidth use

R

rcvd	Number of bytes received. Decimal format. Example: rcvd=23631. Available from: v1.0.0 SNS Affected logs: l_connection, l_filter, l_ftp, l_plugin, l_pop3, l_smtp, l_ssl and l_web.
	Received Example: "*23 KB*"
remoteid	ID of the peer used during the negotiation of the IKE SA. This may be an e-mail address or IP address. Example: remoteid=10.3.0.202. Affected logs: l_vpn.
	Remote identifier
remotenet	Peer's network address. Decimal format. Example: "192.168.53.3". Affected logs: l_vpn and l_xvpn.
	Remote network
repeat	Number of occurrences of the alarm over a given period. Decimal format. Example: repeat=4. Available from: SNS v1.0.0. Affected logs: l_alarm.
	Repeat
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. Affected logs: l_plugin.

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. Affected logs: l_plugin.
result	Return code of the server or of a function (example: Modbus protocol). Example: result=403. Affected logs: *Result*
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. Affected logs: l_alarm, l_ftp, l_pop3, l_sandboxing, l_smtp, l_ssl and l_web. *Risk*
router	Name of the monitored router. String of characters in UTF-8 format. Example: router=routerICMP. Available from: SNS v4.3.0. Affected logs: l_routerstat.
rt	Name of the gateway used for the connection. Appears only if the gateway does not match the default route. String of characters in UTF-8 format. Example: rt="my_gateway". Available from: SNS v4.3.0. Affected logs: l_alarm, l_connection, l_filter and l_plugin.
rtname	Name of the router object used for the connection. Appears only if the router does not match the default route. String of characters in UTF-8 format. Example: rtname="my_router". Available from: SNS v4.3.0. Affected logs: l_alarm, l_connection, l_filter and l_plugin.

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.
	Affected logs: l_count.

ruleid	Number of the filter rule or authentication rule (l_auth log) applied. Example: ruleid=4. Available from: SNS v1.0.0. Affected logs: l_alarm, l_auth, l_connection, l_filter, l_plugin, l_pop3, l_smtp, l_ssl and l_web.
	Rule
rulename	Name of the filter rule applied. Character string. Example: rulename="myrule". Available from: SNS v3.2.0. Affected logs: l_pop3, l_smtp, l_ssl, l_web and l_ftp.
	Rule name
ruletype	Type of IPsec rule used. Character string. Values: "mobile", "gateway". Example: ruletype=mobile. Available from: SNS v4.2. Affected logs: l_vpn.

S

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 in question. In this case, the whole file will be sent to the firewall to be scanned. Example: sandboxing=forward. Affected logs: l_ftp, l_sandboxing, l_pop3, l_smtp and l_web.
	Sandboxing
sandboxinglevel	Indicates the level of the file's infection on a scale of 0 to 100. Value of "0" (clean) to "100" (malicious). Example: sandboxinglevel=20. Affected logs: l_ftp, l_sandboxing, l_pop3 and l_smtp.
	Sandboxing score
SavedEvaluation	Number of rule evaluations that did not use intrusion prevention technology. Example: SavedEvaluation=2. Affected logs: l_filterstat.
SCTPAssoc	Number of SCTP associations. Digital format. Example: SCTPAssoc=2. Available from: SNS v3.9.0. Affected logs: l_filterstat.

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. Affected logs: l_filterstat.
SCTPAssocPacket	Number of packets exchanged for an SCTP association. Digital format. Example: SCTPAssocPacket=128 Available from: SNS v3.9.0. Affected logs: l_filterstat.
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. Example: security=70. Affected logs: l_monitor.
sent	Number of bytes sent over the connection. Decimal format. Example: sent=14623. Available from: SNS v1.0.0. Affected logs: l_connection, l_filter, l_ftp, l_plugin, l_pop3, l_smtp, l_ssl and l_web.
	Sent Example: "*13 KB*"
serverappid	Last server application detected on the connection. Character string. Example: serverappid=google. Available from: SNS v3.2.0. Affected logs: l_connection and l_plugin.
	Server application
service	Name of the module that executed an action. ASCII character string. Example: service="SSOAgent". Affected logs: l_sandboxing and l_system, l_routing.
	Service
sessionid	Session ID number allowing simultaneous connections to be differentiated. Example: sessionid=18. Affected logs: l_server.
	Session Example: "01.0018"
side	Role of the Firewall in the negotiation of the tunnel. Values: "initiator" or "responder". Example: side=initiator. Affected logs: l_vpn.
	Role

slotlevel	Indicates the type of rule that activated logging. Values: “0” (implicit), “1” (global), or “2” (local). Example: slotlevel=1. Available from: v1.0.0 SNS Affected logs: l_alarm, l_connection, l_filter, l_ftp, l_plugin, l_pop3, l_smtp, l_ssl and l_web.
	Rule level Values: “Implicit”, “Global” or “Local”.
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: v1.0.0 SNS
	Spam
spi_in	SPI (Security Parameter Index) number of the negotiated incoming SA (Security Association). Character string in hexadecimal. Example: spi_in=0x01ae58af. Affected logs: l_vpn.
	Incoming spi
spi_out	SPI number of the negotiated outgoing SA. Character string in hexadecimal. Example: spi_out=0x003d098c. Affected logs: l_vpn.
	Outgoing spi
src	IP address of the source host. Decimal format. Example: src=192.168.0.1. May be displayed anonymously depending on the administrator's access privileges. Available from: SNS v1.0.0. Affected logs: l_alarm, l_auth, l_connection, l_filter, l_ftp, l_plugin, l_pop3, l_sandboxing, l_smtp, l_ssl, l_vpn, l_web and l_xvpn, l_dmrouting.
	Source
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. Affected logs: l_alarm, l_connection, l_filter, l_plugin, l_pop3, l_sandboxing, l_smtp, l_ssl and l_web.
	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. Affected logs: l_alarm, l_connection, l_filter, l_plugin, l_pop3, l_sandboxing, l_smtp, l_ssl and l_web.
	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. Affected logs: l_alarm, l_connection, l_filter, l_plugin, l_pop3, l_sandboxing, l_smtp, l_ssl and l_web.
	Source host reputation
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. Affected logs: l_alarm, l_connection, l_filter and l_plugin, l_dmrouting.
	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. Affected logs: l_alarm, l_connection, l_filter and l_plugin, l_dmrouting.
	Source interf.
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. Affected logs: l_alarm, l_connection, l_filter, l_plugin, l_pop3, l_sandboxing, l_smtp, l_ssl and l_web.
	Public reputation of the source IP address
srcmac	MAC address of the source host. May be displayed anonymously depending on the administrator's access privileges. Example: srcmac=00:25:90:01:ce:e7. Affected logs: l_alarm, l_connection, l_filter, l_ftp, l_plugin, l_sandboxing, l_smtp, l_ssl and l_web.
	Source MAC address
srcname	Name of the object corresponding to the source host. May be displayed anonymously depending on the administrator's access privileges. String of characters in UTF-8 format. Example: srcname=client laptop. Available from: SNS v1.0.0. Affected logs: l_alarm, l_connection, l_filter, l_ftp, l_plugin, l_pop3, l_sandboxing, l_smtp, l_ssl, l_vpn, l_web and l_xvpn, l_dmrouting.
	Source name

srcport	Source port number of the service. Example: srcport=51166. Available from: SNS v1.0.0. Affected logs: l_alarm, l_connection, l_filter, l_ftp, l_plugin, l_pop3, l_sandboxing, l_smtp, l_ssl and l_web.
	Source port
srcportname	"Source" port name if it is known. String of characters in UTF-8 format. Example: srcportname=ad2003-dyn_tcp. Available from: SNS v1.0.0. Affected logs: l_alarm, l_connection, l_filter, l_ftp, l_plugin, l_pop3, l_sandboxing, l_smtp, l_ssl and l_web.
	Source port name
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: sslvpn1=sslvpn_udp,61515,128648,788241,1890520,2130,21. Affected logs: l_monitor.
system	Indicator of the Firewall's system status. This value is used by the fleet management tool (Stormshield Management Center) to provide information on the system status (available RAM, CPU use, bandwidth, interfaces, fullness of audit logs, etc). Decimal format representing a percentage. Example: system=0. Affected logs: l_monitor.

T

target	Shows whether the src or dst fields correspond to the target of the packet that had raised the alarm. Values: "*src*" or "*dst*". Example: target=src. Available from: SNS v3.0.0. Affected logs: l_alarm and l_filter.
	Target

TCPByte(i/o)	Number of TCP bytes (incoming/outgoing) that have passed through the firewall. Example: TCPByte (i/o)=527894/528486. Affected logs: l_filterstat.
TCPConn	Number of TCP connections that have passed through the Firewall. Example: TCPConn=13246. Affected logs: l_filterstat.
TCPConnNatDst	Number of TCP connections with a translated destination. Example: TCPConnNatDst=654565. Affected logs: l_filterstat.
TCPConnNatSrc	Number of TCP connections with a translated source. Example: TCPConnNatSrc=3432. Affected logs: l_filterstat.
TCPPacket	Number of TCP packets that have passed through the Firewall. Example: TCPPacket=654364646. Affected logs: l_filterstat.
TLSCertCacheEntriesNb	Number of entries currently in the TLS certificate cache. Digital format. Example: TLSCertCacheEntriesNb=3456. Available from: SNS v4.3.0. Affected logs: l_filterstat.
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. Affected logs: l_filterstat.
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. Affected logs: l_filterstat.
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. Affected logs: l_filterstat.
TLSCertCacheInsert	Number of entries inserted in the TLS certificate cache. Digital format. Example: TLSCertCacheInsert=789. Available from: SNS v4.3.0. Affected logs: l_filterstat.
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. Affected logs: l_filterstat.

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. Affected logs: l_filterstat.
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. Affected logs: l_filterstat.
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. Affected logs: l_auth, l_xvpn.
	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. Affected logs: l_auth and l_system.

U

UDPByte(i/o)	Number of UDP bytes (incoming/outgoing) that have passed through the firewall. Example: "527894/528486". Affected logs: l_filterstat.
UDPConn	Number of UDP connections that have passed through the Firewall. Example: UDPConn=527894. Affected logs: l_filterstat.
UDPConnNatDst	Number of UDP connections with a translated destination. Example: UDPConnNatDst=12. Affected logs: l_filterstat.
UDPConnNatSrc	Number of UDP connections with a translated source. Example: UDPConnNatSrc=15. Affected logs: l_filterstat.
UDPPacket	Number of UDP packets that have passed through the Firewall. Example: UDPPacket=6164646. Affected logs: l_filterstat.
UI	Sofbus/Lacbus information unit String of characters in UTF-8 format. Example: UI=Instruction. Available from: SNS v4.3.0. Affected logs: l_plugin.

unitid	Value of the *"Unit Id"* in a Modbus message that specifies a PLC. Example: unitid=255. Available from: SNS v2.3.0. Affected logs: l_plugin.
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. Affected logs: l_routerstat.
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. Affected logs: l_routerstat.
urlruleid	Number of the URL filter rule applied. Digital format. Example: urlruleid=12 Available from: SNS v3.2.0. Affected logs: l_web.
user	User authenticated by the firewall. String of characters in UTF-8 format. Example: user="john.doe", user="john.doe@company.com" May be displayed anonymously depending on the administrator's access privileges. Available from: SNS v1.0.0. Affected logs: l_alarm, l_auth, l_connection, l_ftp, l_plugin, l_pop3, l_sandboxing, l_server, l_smtp, l_ssl, l_web and l_xvpn.
	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. Affected logs: l_vpn.
	Group

V

version	Version number of the protocol. String of characters in UTF-8 format. Example: version=TLSv1.2, version=4. Available from: v4.2.1 SNS Affected logs: l_connection and l_plugin.
	Protocol version

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". Affected logs: l_monitor.
	Interface monitoring / Bandwidth use
virus	Message indicating whether a virus has been detected (the antivirus has to be enabled) Example: virus=clean. Affected logs: l_ftp, l_pop3, l_smtp and l_web.
	Virus Example: “clean”.

W

WifiXX	Concerns only firewalls equipped with Wi-Fi antennas (W models). Indicators of bandwidth used for each active Wi-Fi access points: • Access point name. 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: Wifi01=Public_WiFi,61515,128648,788241,1890520,2130,21. Affected logs: l_monitor.

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: wldev0=Physic_WiFi,61515,128648,788241,1890520,2130,21. Affected logs: l_monitor.

Further reading

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

documentation@stormshield.eu