



**STORMSHIELD**



TECHNICAL NOTE

**STORMSHIELD NETWORK SECURITY**

# DESCRIPTION OF AUDIT LOGS

Product concerned: SNS 4.3.43 QS

Document last updated: May 18, 2026

Reference: [sns-en-description\\_of\\_audit\\_logs\\_technical\\_note\\_v4.3-QS](#)



# Table of contents

Getting started .....	3
Reading logs .....	4
Reading logs in the web administration interface .....	4
Reading logs in log files .....	4
Reading log archives .....	5
Archive names .....	5
Managing log storage .....	6
Configuring logs .....	7
Understanding log types .....	7
Choosing where to save logs .....	7
Choosing which logs to generate .....	7
Adding logs to filter and NAT rules .....	8
Understanding audit logs .....	9
Specific fields .....	10
Fields classified in alphabetical order and their descriptions .....	11
A .....	11
B .....	12
C .....	12
D .....	14
E .....	16
F .....	18
G .....	18
H .....	19
I .....	19
J .....	21
L .....	22
M .....	22
O .....	23
P .....	24
Q .....	26
R .....	26
S .....	28
T .....	33
U .....	35
V .....	36
W .....	37
Further reading .....	38



## 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:

<b><i>l_alarm</i></b>	Events relating to intrusion prevention functions (IPS) and those logged with a minor or major alarm level in the filter policy.
<b><i>l_auth</i></b>	Events relating to user authentication on the firewall
<b><i>l_connection</i></b>	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.
<b><i>l_count</i></b>	Statistics regarding the number of times a rule has been executed. Such logs are not generated by default. For further information, see <a href="#">Adding logs to filter rules</a> .
<b><i>l_date</i></b>	Events relating to time changes on the firewall.
<b><i>l_filter</i></b>	Events relating to filter and/or NAT rules. Such logs are not generated by default. For further information, see <a href="#">Adding logs to filter rules</a> .



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

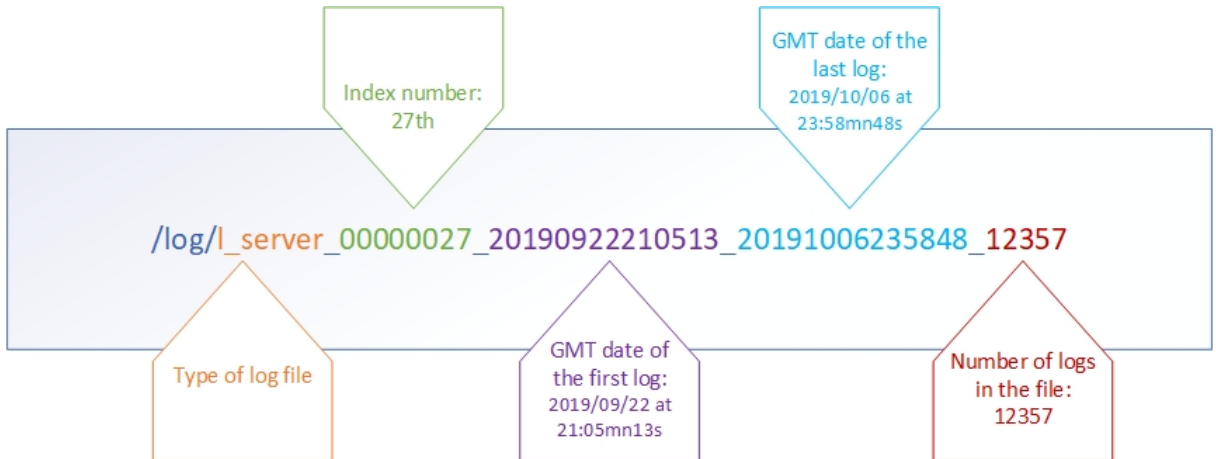
### Archive names

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 */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 */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/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"
starttime="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="U800SXXXXXXXXXXXX" tz="+0100"
starttime="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:

<b>fw</b>	<p>Firewall ID. This is the name entered by the administrator or, by default, its serial number. String of characters in UTF-8 format. Example: “<i>firewall_name</i>” or “<i>V50XXXXXXXXXXXX</i>” Available from: v1.0.0 SNS Affected logs: <i>l_alarm</i>, <i>l_auth</i>, <i>l_connection</i>, <i>l_count</i>, <i>l_date</i>, <i>l_filter</i>, <i>l_filterstat</i>, <i>l_ftp</i>, <i>l_monitor</i>, <i>l_plugin</i>, <i>l_pop3</i>, <i>l_pvm</i>, <i>l_sandboxing</i>, <i>l_server</i>, <i>l_smtp</i>, <i>l_ssl</i>, <i>l_system</i>, <i>l_vpn</i>, <i>l_web</i>, <i>l_xvpn</i> and <i>l_routerstat</i>.</p>
<b>starttime</b>	<p>“<i>Local</i>” time at the beginning of the logged event (time configured on the firewall). String in “<i>YYYY-MM-DD HH:MM:SS</i>” format. Available from: v1.0.0 SNS Affected logs: <i>l_alarm</i>, <i>l_auth</i>, <i>l_connection</i>, <i>l_count</i>, <i>l_date</i>, <i>l_filter</i>, <i>l_filterstat</i>, <i>l_ftp</i>, <i>l_monitor</i>, <i>l_plugin</i>, <i>l_pop3</i>, <i>l_pvm</i>, <i>l_sandboxing</i>, <i>l_server</i>, <i>l_smtp</i>, <i>l_ssl</i>, <i>l_system</i>, <i>l_vpn</i>, <i>l_web</i>, <i>l_xvpn</i> and <i>l_routerstat</i>.</p> <p><i>Date and time</i></p> <p>The display format depends on the language of the operating system on which the administration suite has been installed. Example: “<i>DD/MM/YYYY</i>” and “<i>HH:MM:SS</i>” for French; “<i>YYYY/MM/DD</i>” and “<i>HH:MM:SS</i>” for English.</p>
<b>time</b>	<p>“<i>Local</i>” time at which the log was recorded in the log file (time configured on the firewall). String in “<i>YYYY-MM-DD HH:MM:SS</i>” format. Available from: v1.0.0 SNS Affected logs: <i>l_alarm</i>, <i>l_auth</i>, <i>l_connection</i>, <i>l_count</i>, <i>l_date</i>, <i>l_filter</i>, <i>l_filterstat</i>, <i>l_ftp</i>, <i>l_monitor</i>, <i>l_plugin</i>, <i>l_pop3</i>, <i>l_pvm</i>, <i>l_sandboxing</i>, <i>l_server</i>, <i>l_smtp</i>, <i>l_ssl</i>, <i>l_system</i>, <i>l_vpn</i>, <i>l_web</i>, <i>l_xvpn</i> and <i>l_routerstat</i>.</p> <p><i>Saved at</i></p> <p>The display format depends on the language of the operating system on which the administration suite has been installed. Example: “<i>DD/MM/YYYY</i>” and “<i>HH:MM:SS</i>” for French; “<i>YYYY/MM/DD</i>” and “<i>HH:MM:SS</i>” for English.</p>
<b>tz</b>	<p>Time difference between the firewall’s time and GMT. This depends on the time zone used. String in “<i>+HHMM</i>” or “<i>-HHMM</i>” format. Available from: v1.0.0 SNS Affected logs: <i>l_alarm</i>, <i>l_auth</i>, <i>l_connection</i>, <i>l_count</i>, <i>l_date</i>, <i>l_filter</i>, <i>l_filterstat</i>, <i>l_ftp</i>, <i>l_monitor</i>, <i>l_plugin</i>, <i>l_pop3</i>, <i>l_pvm</i>, <i>l_sandboxing</i>, <i>l_server</i>, <i>l_smtp</i>, <i>l_ssl</i>, <i>l_system</i>, <i>l_vpn</i>, <i>l_web</i>, <i>l_xvpn</i> and <i>l_routerstat</i>.</p> <p><i>Time difference between local time and GMT time</i> Example: “<i>gmt +01:00</i>”</p>



# Fields classified in alphabetical order and their descriptions

---

## A

<b>Accepted</b>	Number of packets corresponding to the application of "Pass" rules. Example: Accepted=2430. Affected logs: <code>_filterstat</code> .
<b>action</b>	Behavior associated with the filter rule. Value: "Pass" or "Block" (empty field for "Log"). Example: action=block. Affected logs: <code>_alarm</code> , <code>_connection</code> , <code>_filter</code> , <code>_ftp</code> , <code>_plugin</code> , <code>_pop3</code> , <code>_smtp</code> , <code>_ssl</code> and <code>_web</code> .  <i>Action</i>
<b>address</b>	IP address of the client workstation that initiated the connection. Decimal format. Example: address=192.168.0.2. Affected logs: <code>_server</code> .  <i>Source</i>
<b>ads</b>	Indicates whether the antispam has detected an e-mail as an advertisement. Values: "0" or "1". Example: ads=1. Affected logs: <code>_pop3</code> and <code>_smtp</code> .  <i>Advertisement</i>
<b>agentid</b>	SSO agent ID. Value: from 0 to 5. Example: agentid=0 Available from: SNS v3.0.0. Affected logs: <code>_auth</code> .  <i>SSO Agent</i>
<b>aggXX</b>	Indicators of bandwidth used by interface aggregates: <ul style="list-style-type: none"><li>• Name of the interface. String of characters in UTF-8 format.</li><li>• Incoming throughput (bits/second),</li><li>• Maximum incoming throughput for a given period (bits/second),</li><li>• Outgoing throughput (bits/second),</li><li>• Maximum outgoing throughput for a given period (bits/second),</li><li>• Number of packets accepted,</li><li>• Number of packets blocked.</li></ul> Format: 7 values separated by commas. Example: agg01=Production_LACP,61515,128648,788241,1890520,2130,21. Affected logs: <code>_monitor</code> .



<b>alarmid</b>	Stormshield Network alarm ID Decimal format. Example: "85". Affected logs: <code>_alarm</code> and <code>_system</code> .
	<i>Alarm ID</i>
<b>arg</b>	Argument of the HTTP command. String of characters in UTF-8 format. Example: "/", "/mypage.htm" ... Affected logs: <code>_ftp</code> , <code>_plugin</code> , <code>_pvm</code> , <code>_sandboxing</code> , <code>_ssl</code> , <code>_web</code> and <code>_xvpn</code> .
	<i>Argument</i>
<b>B</b>	
<b>Blocked</b>	Number of packets corresponding to the application of "Block" rules. Example: Blocked=1254. Affected logs: <code>_filterstat</code> .
<b>Byte(i/o)</b>	Number of bytes (incoming/outgoing) that have passed through the Firewall. Example: Byte [i/o]=527894/528486. Affected logs: <code>_filterstat</code> .
<b>C</b>	
<b>caller</b>	Caller ID. String of characters in UTF-8 format. Example: ""John" <sip:193@192.168.0.1>". Affected logs: <code>_plugin</code> (RTP, RTCP, Media_UDP and Media_UDP).
	<i>Caller</i>
<b>callee</b>	Callee ID. String of characters in UTF-8 format. Example: "sip:192@192.168.1.1:5060;line=g842aca6eddb2a5". Affected logs: <code>_plugin</code> (RTP, RTCP, Media_UDP and Media_UDP).
	<i>Callee</i>
<b>cat_site</b>	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: <code>_ssl</code> and <code>_web</code> .
	<i>Category</i>
<b>class</b>	Information about the alarm's category. String of characters in UTF-8 format. Example: "protocol", "system", "filter", ... Affected logs: <code>_alarm</code> .
	<i>Context</i>



---

<b>cipclassid</b>	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.
<b>cipservicecode</b>	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.
<b>clientappid</b>	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.
	<i>Client application</i>
<b>cnruleid</b>	Number of the SSL filter rule applied. Digital format. Example: cnruleid=3. Available from: SNS v3.2.0. Affected logs: l_ssl.
	<i>Rule</i>
<b>confid</b>	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.
<b>ConnMem</b>	Percentage of memory allocated to connections. Value from "0" to "100". Example: ConnMem=1. Affected logs: l_filterstat.
<b>contentpolicy</b>	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.
<b>cookie_i</b>	Temporary identity marker of the initiator of the negotiation. Character string in hexadecimal. Example: cookie_i=0xae34785945ae3cbf Affected logs: l_vpn.
	<i>Initiating cookie</i>
<b>cookie_r</b>	Temporary identity marker of the peer of the negotiation. Character string in hexadecimal. Example: cookie_r=0x56201508549a6526. Affected logs: l_vpn.
	<i>Receiving cookie</i>

---



---

<b>CPU</b>	Firewall's CPU consumption: <ul style="list-style-type: none"><li>• Time allocated to the management of user processes,</li><li>• Time consumed by the kernel,</li><li>• Time allocated to system disruptions.</li></ul> Format: 3 numeric values separated by commas. Example: CPU=1,0,2 Affected logs: <code>l_monitor</code> .
------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

---

System monitoring / CPU load

---

## D

---

<b>detail</b>	Additional information on the vulnerable software version. String of characters in UTF-8 format. Example: detail="PHP_5.2.3". Affected logs: <code>l_pvm</code> .
---------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------

---

### *Details*

---

<b>discovery</b>	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. Example: discovery="2023-10-12". Affected logs: <code>l_pvm</code> .
------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

---

### *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.

---

---

<b>domain</b>	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: <code>l_alarm</code> , <code>l_auth</code> , <code>l_connection</code> , <code>l_plugin</code> , <code>l_server</code> , <code>l_ssl</code> , <code>l_web</code> and <code>l_xvpn</code> .
---------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

---

### *Method or directory*

---

<b>downrate</b>	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: <code>l_routerstat</code> .
-----------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

---

---

<b>dst</b>	IP address of the destination host Decimal format. Example: "192.168.0.2" Available from: v1.0.0 SNS Affected logs: <code>l_alarm</code> , <code>l_connection</code> , <code>l_filter</code> , <code>l_ftp</code> , <code>l_plugin</code> , <code>l_pop3</code> , <code>l_sandboxing</code> , <code>l_smtp</code> , <code>l_ssl</code> , <code>l_vpn</code> and <code>l_web</code> .
------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

---

### *Destination*

---



---

<b>dstcontinent</b>	<p>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: <code>_alarm</code>, <code>_connection</code>, <code>_filter</code>, <code>_plugin</code>, <code>_pop3</code>, <code>_sandboxing</code>, <code>_smtp</code>, <code>_ssl</code> and <code>_web</code>.</p> <hr/> <p><i>Destination continent</i></p>
<b>dstcountry</b>	<p>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: <code>_alarm</code>, <code>_connection</code>, <code>_filter</code>, <code>_ftp</code>, <code>_plugin</code>, <code>_pop3</code>, <code>_sandboxing</code>, <code>_smtp</code>, <code>_ssl</code>, <code>_vpn</code> and <code>_web</code>.</p> <hr/> <p><i>Destination country</i></p>
<b>dsthostrep</b>	<p>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: <code>_alarm</code>, <code>_connection</code>, <code>_filter</code>, <code>_plugin</code>, <code>_pop3</code>, <code>_sandboxing</code>, <code>_smtp</code>, <code>_ssl</code> and <code>_web</code>.</p> <hr/> <p><i>Destination host reputation</i></p>
<b>dstif</b>	<p>Name of the destination interface. String of characters in UTF-8 format. Example: dstif=Ethernet 1. Available from: SNS v1.0.0. Affected logs: <code>_alarm</code>, <code>_connection</code>, <code>_filter</code> and <code>_plugin</code>.</p> <hr/> <p><i>Dest. interf. (ID)</i></p>
<b>dstifname</b>	<p>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: <code>_alarm</code>, <code>_connection</code>, <code>_filter</code> and <code>_plugin</code>.</p> <hr/> <p><i>Dest. interf.</i></p>
<b>dstiprep</b>	<p>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: <code>_alarm</code>, <code>_connection</code>, <code>_filter</code>, <code>_plugin</code>, <code>_pop3</code>, <code>_sandboxing</code>, <code>_smtp</code>, <code>_ssl</code> and <code>_web</code>.</p> <hr/> <p><i>Public reputation of the destination IP address</i></p>

---



---

<b>dstmac</b>	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: <code>_alarm</code> , <code>_connection</code> and <code>_plugin</code> .
	<i>Destination MAC address</i>
<b>dstname</b>	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: <code>_alarm</code> , <code>_connection</code> , <code>_filter</code> , <code>_ftp</code> , <code>_plugin</code> , <code>_pop3</code> , <code>_sandboxing</code> , <code>_smtp</code> , <code>_ssl</code> , <code>_vpn</code> , <code>_web</code> and <code>_xvpn</code> .
	<i>Destination name</i>
<b>dstport</b>	Destination TCP/UDP port number. Example: dstport=22. Available from: SNS v1.0.0. Affected logs: <code>_alarm</code> , <code>_connection</code> , <code>_filter</code> , <code>_ftp</code> , <code>_plugin</code> , <code>_pop3</code> , <code>_sandboxing</code> , <code>_smtp</code> , <code>_ssl</code> , <code>_web</code> and <code>_xvpn</code> .
	<i>Destination port</i>
<b>dstportname</b>	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: <code>_alarm</code> , <code>_connection</code> , <code>_filter</code> , <code>_ftp</code> , <code>_plugin</code> , <code>_pop3</code> , <code>_sandboxing</code> , <code>_smtp</code> , <code>_ssl</code> , <code>_web</code> and <code>_xvpn</code> .
	<i>Dest. port name</i>
<b>DtrackMem</b>	Percentage of memory used for data tracking (TCP/UDP packets). Value from "0" to "100". Affected logs: <code>_filterstat</code> .
<b>duration</b>	Duration of the connection in seconds. Decimal format. Example: "173.15"
	<i>Duration</i> Example: "2m 53s 15"
<b>DynamicMem</b>	Percentage of the ASQ's dynamic memory in use. Value from "0" to "100". Affected logs: <code>_filterstat</code> .
<b>E</b>	
<b>error</b>	Return code from the authentication attempt or command. Example: error=1. Affected logs: <code>_auth</code> , <code>_server</code> and <code>_xvpn</code> .
	<i>Result</i> Example: "Success", "Access denied", "Connect to host failed" ...

---



---

<b>error_class</b>	Number of the error class in an S7 response. Digital format. Example: error_class=0. Available from: SNS v2.3.0. Affected logs: I_plugin.
<b>error_code</b>	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: I_plugin.
<b>EthernetXX</b>	Indicators of bandwidth used for each of the active network interfaces: <ul style="list-style-type: none"><li>• name of the interface. String of characters in UTF-8 format.</li><li>• incoming throughput (bits/second),</li><li>• maximum incoming throughput for a given period (bits/second),</li><li>• outgoing throughput (bits/second),</li><li>• maximum outgoing throughput for a given period (bits/second),</li><li>• number of packets accepted,</li><li>• number of packets blocked,</li></ul> Format: 7 values separated by commas. Example: "in,61515,128648,788241,1890520,2130,21". Affected logs: I_monitor.
	<i>Interface monitoring / Bandwidth use</i>
<b>etherproto</b>	Type of Ethernet protocol. Format: String of characters in UTF-8 format. Example: etherproto="profinet-rt" Available from: SNS v4.0.0. Affected logs: I_alarm, I_connection and I_plugin.
	<i>Ethernet protocol</i>
<b>EtherStateByte (i/o)</b>	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: I_filterstat.
<b>EtherStateConn</b>	Number of stateful statuses for Ethernet exchanges without IP layer. Digital format. Example: EtherStateConn=0. Available from: SNS v4.0.0. Affected logs: I_filterstat.
<b>EtherStatePacket</b>	Number of packets for Ethernet traffic without IP layer. Digital format. Example: EtherStatePacket=128. Available from: SNS v4.0.0. Affected logs: I_filterstat.

---



## F

<b>family</b>	Name of the vulnerability family (Web Client, Web Server, Mail Client...). String of characters in UTF-8 format. Example: family=Web Client. Affected logs: l_pvm.
	<i>Category</i>
<b>filename</b>	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.
	<i>File name</i>
<b>filetype</b>	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.
	<i>File type</i>
<b>format</b>	Type of message for IEC104 Character in UTF-8 format. Example: format=U. Available from: SNS v3.1.0. Affected logs: l_plugin.
<b>FragMem</b>	Percentage of memory allocated to the treatment of fragmented packets. Value from "0" to "100". Example: FragMem=2. Affected logs: l_filterstat.
<b>Fragmented</b>	Number of fragmented packets that have passed through the Firewall. Example: Fragmented=12. Affected logs: l_filterstat.

## G

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



## H

---

<b>hash</b>	Results of the file content hash (SHA2 method) String of characters in UTF-8 format. Example: hash= f4d1be410a6102b9ae7d1c32612bed4f12158df3cd1ab6440a9ac0cad417446d. Affected logs: <code>_ftp</code> , <code>_pop3</code> , <code>_sandboxing</code> , <code>_smtp</code> and <code>_web</code> .
	<i>Hash</i>
<b>HostMem</b>	Percentage of memory allocated to a host processed by the Firewall. Value from "0" to "100". Example: HostMem=4 Affected logs: <code>_filterstat</code> .
<b>HostrepScore</b>	Average reputation score of monitored hosts. Value: decimal integer between 0 and 65535. Example: HostrepScore=1234 Available from: SNS v3.0.0. Affected logs: <code>_filterstat</code> .
<b>HostrepMax</b>	Highest reputation score of monitored hosts. Value: decimal integer between 0 and 65535. Example: HostrepMax=6540 Available from: SNS v3.0.0. Affected logs: <code>_filterstat</code> .
<b>HostrepRequests</b>	Number of reputation score requests submitted. Value: unrestricted decimal integer. Example: HostrepRequests=445 Available from: SNS v3.0.0. Affected logs: <code>_filterstat</code> .

---

**I**

---

<b>ICMPByte(i/o)</b>	Number of ICMP bytes (incoming/outgoing) that have passed through the firewall. Example: ICMPByte(i/o) =527894/528486 Affected logs: <code>_filterstat</code> .
<b>icmpcode</b>	Code number of the ICMP message, based on ICMP type. Digital format. See the list of ICMP parameters at: <a href="http://www.iana.org/assignments/icmp-parameters/icmp-parameters.xhtml">http://www.iana.org/assignments/icmp-parameters/icmp-parameters.xhtml</a> . Example: icmpcode=1 (meaning "Host unreachable"). Available from: SNS v1.0.0. Affected logs: <code>_alarm</code> and <code>_filter</code> .
	<i>ICMP code</i>

---



---

<b>icmp<sub>type</sub></b>	<p>ICMP message type number. Digital format. See the list of ICMP parameters at: <a href="http://www.iana.org/assignments/icmp-parameters/icmp-parameters.xhtml">http://www.iana.org/assignments/icmp-parameters/icmp-parameters.xhtml</a>. Example: icmp<sub>type</sub>=3 (meaning "Destination unreachable"). Available from: SNS v1.0.0. Affected logs: <code>I_alarm</code> and <code>I_filter</code>.</p> <hr/> <p><i>ICMP type</i></p>
<b>ICMPMem</b>	<p>Percentage of memory allocated to ICMP. Value from "0" to "100". Example: ICMPMem=2 Affected logs: <code>I_filterstat</code>.</p>
<b>ICMPPacket</b>	<p>Number of ICMP packets that have passed through the Firewall. Example: ICMPPacket=0. Affected logs: <code>I_filterstat</code>.</p>
<b>id</b>	<p>Type of product. This field constantly has the value "<i>firewall</i>" for logs on the firewall. Affected logs: <code>I_alarm</code>, <code>I_auth</code>, <code>I_connection</code>, <code>I_count</code>, <code>I_date</code>, <code>I_filter</code>, <code>I_filterstat</code>, <code>I_ftp</code>, <code>I_monitor</code>, <code>I_plugin</code>, <code>I_pop3</code>, <code>I_pvm</code>, <code>I_sandboxing</code>, <code>I_server</code>, <code>I_smtp</code>, <code>I_ssl</code>, <code>I_system</code>, <code>I_vpn</code>, <code>I_web</code>, <code>I_xvpn</code> and <code>I_routerstat</code>.</p>
<b>ikev</b>	<p>Version of the IKE protocol used Values: "1" or "2". Example: ikev=1. Affected logs: <code>I_vpn</code>.</p> <hr/> <p><i>IKE version</i></p>
<b>ipproto</b>	<p>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: <code>I_alarm</code>, <code>I_connection</code>, <code>I_filter</code>, <code>I_plugin</code> and <code>I_pvm</code>.</p> <hr/> <p><i>Internet Protocol</i></p>
<b>ipsecXX</b>	<p>Indicators of bandwidth used by IPSec interfaces:</p> <ul style="list-style-type: none"><li>• name of the interface. String of characters in UTF-8 format.</li><li>• incoming throughput (bits/second),</li><li>• maximum incoming throughput for a given period (bits/second),</li><li>• outgoing throughput (bits/second),</li><li>• maximum outgoing throughput for a given period (bits/second),</li><li>• number of packets accepted,</li><li>• number of packets blocked,</li></ul> <p>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.</p> <p>Format: 7 values separated by commas. Example: ipsec=ipsec,61515,128648,788241,1890520,2130,21. Affected logs: <code>I_vpn</code>.</p>

---



<b>IPStateByte (i/o)</b>	Number of bytes exchanged for pseudo-connections. This value includes incoming and outgoing bytes. Example: IPStateByte(i/o)=0/40. Affected logs: I_filterstat.
<b>IPStateConn</b>	Number of active pseudo-connections relating to protocols other than TCP, UDP or ICMP (e.g.: GRE). Example: IPStateConn=0. Affected logs: I_filterstat.
<b>IPStateConnNatDst</b>	Number of active pseudo-connections with address translation on the destination. Example: IPStateConnNatDst=0. Affected logs: I_filterstat.
<b>IPStateConnNatSrc</b>	Number of active pseudo-connections with address translation on the source. Example: IPStateConnNatSrc=0. Affected logs: I_filterstat.
<b>IPStateConnNoNatDst</b>	Number of active pseudo-connections that explicitly include "No NAT" instructions on the destination. Example: IPStateConnNoNatDst=0. Affected logs: I_filterstat.
<b>IPStateConnNoNatSrc</b>	Number of active pseudo-connections that explicitly include "No NAT" instructions on the source. Example: IPStateConnNoNatSrc=0. Affected logs: I_filterstat.
<b>IPStateMem</b>	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: I_filterstat.
<b>IPStatePacket</b>	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: I_filterstat.
<b>ipv</b>	Version of the IP protocol used in the traffic Values: "4" or "6". Example: ipv=4. Available from: SNS v1.0.0. Affected logs: I_alarm, I_connection, I_filter, I_ftp, I_plugin, I_pop3, I_pvm, I_sntp, I_ssl and I_web.  <i>IP version</i>

**J**

<b>jitter</b>	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: I_routerstat.
---------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------



## L

---

<b>latency</b>	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.
<b>localnet</b>	Local network negotiated in phase2. Decimal format. Example: localnet=192.168.0.1/24. Affected logs: l_vpn and l_xvpn.
	<i>Local network</i>
<b>LogOverflow</b>	Number of log lines that could not be generated by the intrusion prevention engine. Example: LogOverflow=0. Affected logs: l_filterstat.
<b>Logged</b>	Number of log lines generated by the intrusion prevention engine. Example: Logged=461634616. Affected logs: l_filterstat.
<b>loopbackXX</b>	Indicators of bandwidth used by loopback interfaces: <ul style="list-style-type: none"><li>• Name of the interface. String of characters in UTF-8 format.</li><li>• Incoming throughput (bits/second),</li><li>• Maximum incoming throughput for a given period (bits/second),</li><li>• Outgoing throughput (bits/second),</li><li>• Maximum outgoing throughput for a given period (bits/second),</li><li>• Number of packets accepted,</li><li>• Number of packets blocked.</li></ul> Format: 7 values separated by commas. Example: loopback1=loopback1,61515,128648,788241,1890520,2130,21.
<b>lossrate</b>	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

---

<b>mailruleid</b>	Number of the mail filter rule applied. Digital format. Example: mailruleid=48 Available from: SNS v3.2.0. Affected logs: l_smtp.
-------------------	-----------------------------------------------------------------------------------------------------------------------------------------------

---



<b>media</b>	Type of traffic detected (audio, video, application, etc). ASCII character string. Example: media=control. Affected logs: l_plugin (RTP, RTCP, Media_UDP and Media_UDP).
	<i>Media</i>
<b>modsrc</b>	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.
	<i>Translated source address</i>
<b>modsrcport</b>	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.
	<i>Translated source port</i>
<b>msg</b>	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" ... Affected logs: l_alarm, l_auth, l_ftp, l_pvm, l_sandboxing, l_server, l_pop3, l_smtp, l_ssl, l_system, l_vpn, l_web, l_xvpn and l_plugin.
	<i>Message</i>
<b>0</b>	
<b>op</b>	Operation performed on the server (FTP, HTTP, etc.). Example: op="GET", op="LIST" ... Associated logs: l_ftp, l_plugin, l_sandboxing and l_web.
	<i>Operation</i>
<b>origdst</b>	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.
	<i>Orig. destination</i>
<b>origdstport</b>	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.
	<i>Orig. destination port</i>



## P

---

<b>phase</b>	Number of the IPSec VPN tunnel negotiation phase. Values: "0" (no phase), "1" (phase 1) or "2" (phase 2). Example: phase=1. Affected logs: <code>l_vpn</code> .
	<i>Phase</i>
<b>pktdump</b>	Network packet captured and encoded in hexadecimal for deeper analysis by a third-party tool. Example: pktdump="450000321fd240008011c2f50a00007b0a3c033d0035c" Affected logs: <code>l_alarm</code> .
	<i>Captured packet</i>
<b>pktdumplen</b>	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: <code>l_alarm</code> .
	<i>Size of the packet captured</i>
<b>pktlen</b>	Size of the network packet that activated the alarm (in bytes). Example: pktlen=33. Affected logs: <code>l_alarm</code> .
	<i>Packet size</i>
<b>port</b>	Port number (entered only if a vulnerability has been detected). Example: port=22. Affected logs: <code>l_pvm</code> .
	<i>Source port</i>
<b>portname</b>	Standard service corresponding to the port number (entered only if a vulnerability has been detected). String of characters in UTF-8 format. Example: "ssh". Affected logs: <code>l_pvm</code> .
	<i>Source port name</i>
<b>pri</b>	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: <code>l_smtp</code> , <code>l_pop3</code> , <code>l_ftp</code> , <code>l_web</code> , <code>l_ssl</code> , <code>l_system</code> and <code>l_vpn</code> . Possible values: "1" ("alert") or "4" ("warning") in the <code>l_pvm</code> log. Example: pri=1. Available from: SNS v1.0.0. Affected logs: <code>l_alarm</code> , <code>l_connection</code> , <code>l_filter</code> , <code>l_ftp</code> , <code>l_plugin</code> , <code>l_pvm</code> , <code>l_pop3</code> , <code>l_smtp</code> , <code>l_ssl</code> , <code>l_system</code> , <code>l_vpn</code> and <code>l_web</code> .
	<i>Priority</i>

---



---

<b>product</b>	Product on which the vulnerability was detected. String of characters in UTF-8 format. Example: product="JRE_1.6.0_27". Affected logs: <code>l_pvm</code> .
	<i>Product</i>
<b>proto</b>	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: <code>l_alarm</code> , <code>l_connection</code> , <code>l_filter</code> , <code>l_ftp</code> , <code>l_plugin</code> , <code>l_pvm</code> , <code>l_sandboxing</code> , <code>l_pop3</code> , <code>l_smtp</code> , <code>l_ssl</code> and <code>l_web</code> .
	<i>Protocol</i>
<b>Pvm</b>	All indicators regarding vulnerability management: <ul style="list-style-type: none"><li>• Total number of vulnerabilities detected,</li><li>• Number of vulnerabilities that can be exploited remotely,</li><li>• Number of vulnerabilities requiring the installation of a server on the vulnerable host in order to be exploited,</li><li>• Number of vulnerabilities classified as critical,</li><li>• Number of vulnerabilities classified as minor,</li><li>• Number of vulnerabilities classified as major,</li><li>• Number of vulnerabilities that have a bug fix,</li><li>• Total amount of information [all levels],</li><li>• Amount of minor data,</li><li>• Amount of major data,</li><li>• Number of hosts for which PVM has gathered information,</li></ul> Format: 11 numeric values separated by commas. Example: "0,0,0,0,0,0,0,2,0,0,2". Example: Pvm=1804,1588,1471,38,685,1119,1730,817,0,817,561. Affected logs: <code>l_monitor</code> .
<b>PvmFacts</b>	Number of events sent by IPS to the vulnerability management process. Example: PvmFacts=0. Affected logs: <code>l_filterstat</code> .
<b>PvmOverflow</b>	Number of events intended for the vulnerability management process that were ignored by IPS. Example: PvmOverflow=1. Affected logs: <code>l_filterstat</code> .

---

**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"

**remote**

Indicates whether the vulnerability can be exploited remotely

Values: "0" (false) or "1" (true).

Example: `remote=1`.

Affected logs: `l_pvm`.

*Exploit*

Values: "Local" or "Remote".

**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*



---

<b>repeat</b>	Number of occurrences of the alarm over a given period. Decimal format. Example: repeat=4. Available from: SNS v1.0.0. Affected logs: <code>_alarm</code> .
	<i>Repeat</i>
<b>requestmode</b>	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: <code>_plugin</code> .
<b>responsemode</b>	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: <code>_plugin</code> .
<b>result</b>	Return code of the server or of a function (example: Modbus protocol). Example: result=403. Affected logs:
	<i>Result</i>
<b>risk</b>	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: <code>_alarm</code> , <code>_ftp</code> , <code>_pop3</code> , <code>_sandboxing</code> , <code>_smtp</code> , <code>_ssl</code> and <code>_web</code> .
	<i>Risk</i>
<b>router</b>	Name of the monitored router. String of characters in UTF-8 format. Example: router=router CMP. Available from: SNS v4.3.0. Affected logs: <code>_routerstat</code> .
<b>rt</b>	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: <code>_alarm</code> , <code>_connection</code> , <code>_filter</code> and <code>_plugin</code> .
<b>rtname</b>	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: <code>_alarm</code> , <code>_connection</code> , <code>_filter</code> and <code>_plugin</code> .

---



**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: `I_count`.

**ruleid** Number of the filter rule or authentication rule (`I_auth log`) applied.  
Example: `ruleid=4`.  
Available from: SNS v1.0.0.  
Affected logs: `I_alarm`, `I_auth`, `I_connection`, `I_filter`, `I_plugin`, `I_pop3`, `I_smtp`, `I_ssl` and `I_web`.

---

*Rule*

**rulename** Name of the filter rule applied.  
Character string.  
Example: `rulename="myrule"`.  
Available from: SNS v3.2.0.  
Affected logs: `I_pop3`, `I_smtp`, `I_ssl`, `I_web` and `I_ftp`.

---

*Rule name*

**ruletype** Type of IPsec rule used.  
Character string.  
Values: "mobile", "gateway".  
Example: `ruletype=mobile`.  
Available from: SNS v4.2.  
Affected logs: `I_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: `I_ftp`, `I_sandboxing`, `I_pop3`, `I_smtp` and `I_web`.

---

*Sandboxing*



<b>sandboxinglevel</b>	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: <code>_ftp</code> , <code>_sandboxing</code> , <code>_pop3</code> and <code>_smtp</code> .
	<i>Sandboxing score</i>
<b>SavedEvaluation</b>	Number of rule evaluations that did not use intrusion prevention technology. Example: SavedEvaluation=2. Affected logs: <code>_filterstat</code> .
<b>SCTPAssoc</b>	Number of SCTP associations. Digital format. Example: SCTPAssoc=2. Available from: SNS v3.9.0. Affected logs: <code>_filterstat</code> .
<b>SCTPAssocByte (i/o)</b>	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: <code>_filterstat</code> .
<b>SCTPAssocPacket</b>	Number of packets exchanged for an SCTP association. Digital format. Example: SCTPAssocPacket=128 Available from: SNS v3.9.0. Affected logs: <code>_filterstat</code> .
<b>security</b>	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: <code>_monitor</code> .
<b>sent</b>	Number of bytes sent over the connection. Decimal format. Example: sent=14623. Available from: SNS v1.0.0. Affected logs: <code>_connection</code> , <code>_filter</code> , <code>_ftp</code> , <code>_plugin</code> , <code>_pop3</code> , <code>_smtp</code> , <code>_ssl</code> and <code>_web</code> .
	<i>Sent</i> Example: "13 KB"
<b>serverappid</b>	Last server application detected on the connection. Character string. Example: serverappid=google. Available from: SNS v3.2.0. Affected logs: <code>_connection</code> and <code>_plugin</code> .
	<i>Server application</i>
<b>service</b>	Name of the module that executed an action. ASCII character string. Example: service="SSOAgent". Affected logs: <code>_pvm</code> , <code>_sandboxing</code> and <code>_system</code> .
	<i>Service</i>



<b>sessionid</b>	Session ID number allowing simultaneous connections to be differentiated. Example: sessionid=18. Affected logs: l_server.  <i>Session</i> Example: "01.0018"
<b>severity</b>	Vulnerability's intrinsic level of severity. Values: "0" (Information), "1" (Weak), "2" (Moderate), "3" (High) or "4" (Critical). Example: severity=3. Affected logs: l_pvm.  <i>Severity</i> Values: "Information", "Weak", "Moderate", "High" or "Critical".
<b>side</b>	Role of the Firewall in the negotiation of the tunnel. Values: "initiator" or "responder". Example: side=initiator. Affected logs: l_vpn.  <i>Role</i>
<b>slotlevel</b>	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.  <i>Rule level</i> Values: "Implicit", "Global" or "Local".
<b>solution</b>	Indicates whether a fix is available in order to correct the detected vulnerability. Values: "0" (not available) or "1" (available). Example: solution=1. Affected logs: l_pvm.  <i>Solution</i> Values: "Yes" or "No".
<b>spamlevel</b>	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  <i>Spam</i>
<b>spi_in</b>	SPI (Security Parameter Index) number of the negotiated incoming SA (Security Association). Character string in hexadecimal. Example: spi_in=0x01ae58af. Affected logs: l_vpn.  <i>Incoming spi</i>
<b>spi_out</b>	SPI number of the negotiated outgoing SA. Character string in hexadecimal. Example: spi_out=0x003d098c. Affected logs: l_vpn.  <i>Outgoing spi</i>



---

<b>src</b>	<p>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: <code>_alarm</code>, <code>_auth</code>, <code>_connection</code>, <code>_filter</code>, <code>_ftp</code>, <code>_plugin</code>, <code>_pop3</code>, <code>_pvm</code>, <code>_sandboxing</code>, <code>_smtp</code>, <code>_ssl</code>, <code>_vpn</code>, <code>_web</code> and <code>_xvpn</code>.</p>
	<p><i>Source</i></p>
<b>srccontinent</b>	<p>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: <code>_alarm</code>, <code>_connection</code>, <code>_filter</code>, <code>_plugin</code>, <code>_pop3</code>, <code>_sandboxing</code>, <code>_smtp</code>, <code>_ssl</code> and <code>_web</code>.</p>
	<p><i>Source continent</i></p>
<b>srccountry</b>	<p>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: <code>_alarm</code>, <code>_connection</code>, <code>_filter</code>, <code>_plugin</code>, <code>_pop3</code>, <code>_sandboxing</code>, <code>_smtp</code>, <code>_ssl</code> and <code>_web</code>.</p>
	<p><i>Source country</i></p>
<b>srchostrep</b>	<p>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: <code>_alarm</code>, <code>_connection</code>, <code>_filter</code>, <code>_plugin</code>, <code>_pop3</code>, <code>_sandboxing</code>, <code>_smtp</code>, <code>_ssl</code> and <code>_web</code>.</p>
	<p><i>Source host reputation</i></p>
<b>srcif</b>	<p>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: <code>_alarm</code>, <code>_connection</code>, <code>_filter</code> and <code>_plugin</code>.</p>
	<p><i>Source interf. (ID)</i></p>
<b>srcifname</b>	<p>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: <code>_alarm</code>, <code>_connection</code>, <code>_filter</code> and <code>_plugin</code>.</p>
	<p><i>Source interf.</i></p>

---



---

<b>srciprep</b>	<p>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: <code>_alarm</code>, <code>_connection</code>, <code>_filter</code>, <code>_plugin</code>, <code>_pop3</code>, <code>_sandboxing</code>, <code>_smtp</code>, <code>_ssl</code> and <code>_web</code>.</p> <hr/> <p><i>Public reputation of the source IP address</i></p>
<b>srcmac</b>	<p>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: <code>_alarm</code>, <code>_connection</code>, <code>_filter</code>, <code>_ftp</code>, <code>_plugin</code>, <code>_sandboxing</code>, <code>_smtp</code>, <code>_ssl</code> and <code>_web</code>.</p> <hr/> <p><i>Source MAC address</i></p>
<b>srcname</b>	<p>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: <code>_alarm</code>, <code>_connection</code>, <code>_filter</code>, <code>_ftp</code>, <code>_plugin</code>, <code>_pop3</code>, <code>_pvm</code>, <code>_sandboxing</code>, <code>_smtp</code>, <code>_ssl</code>, <code>_vpn</code>, <code>_web</code> and <code>_xvpn</code>.</p> <hr/> <p><i>Source name</i></p>
<b>srcport</b>	<p>Source port number of the service. Example: srcport=51166. Available from: SNS v1.0.0. Affected logs: <code>_alarm</code>, <code>_connection</code>, <code>_filter</code>, <code>_ftp</code>, <code>_plugin</code>, <code>_pop3</code>, <code>_sandboxing</code>, <code>_smtp</code>, <code>_ssl</code> and <code>_web</code>.</p> <hr/> <p><i>Source port</i></p>
<b>srcportname</b>	<p>"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: <code>_alarm</code>, <code>_connection</code>, <code>_filter</code>, <code>_ftp</code>, <code>_plugin</code>, <code>_pop3</code>, <code>_sandboxing</code>, <code>_smtp</code>, <code>_ssl</code> and <code>_web</code>.</p> <hr/> <p><i>Source port name</i></p>

---



<b>sslvpnX</b>	<p>Indicators of bandwidth used by SSL VPN traffic. :</p> <ul style="list-style-type: none"> <li>• Name of the interface. String of characters in UTF-8 format.</li> <li>• Incoming throughput (bits/second),</li> <li>• Maximum incoming throughput for a given period (bits/second),</li> <li>• Outgoing throughput (bits/second),</li> <li>• Maximum outgoing throughput for a given period (bits/second),</li> <li>• Number of packets accepted,</li> <li>• Number of packets blocked.</li> </ul> <p>sslvpn0 represents TCP-based SSL VPN traffic. sslvpn1 represents UDP-based SSL VPN traffic.</p> <p>Format: 7 values separated by commas. Example: sslvpn1=sslvpn_udp,61515,128648,788241,1890520,2130,21. Affected logs: <code>I_monitor</code>.</p>
<b>system</b>	<p>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: <code>I_monitor</code>.</p>

T

<b>target</b>	<p>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: <code>I_alarm</code> and <code>I_filter</code>.</p> <p><i>Target</i></p>
<b>targetclient</b>	<p>Indicates whether the exploitation of the vulnerability requires the use of a client on the vulnerable host. Values: "0" (false) or "1" (true). Example: targetclient=1. Affected logs: <code>I_pvm</code>.</p> <p><i>Target client</i> Values: "Client" or "".</p>
<b>targetserver</b>	<p>Indicates whether the exploitation of the vulnerability requires the installation of a server on the vulnerable host. Values: "0" (false) or "1" (true). Example: targetserver=0. Affected logs: <code>I_pvm</code>.</p> <p><i>Target server</i> Values: "Server" or "".</p>



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



<b>TLSCertCachePurgedNb</b>	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: I_filterstat.
<b>TLSCertCachePurgeOp</b>	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: I_filterstat.
<b>U</b>	
<b>UDPByte(i/o)</b>	Number of UDP bytes (incoming/outgoing) that have passed through the firewall. Example: "527894/528486". Affected logs: I_filterstat.
<b>UDPConn</b>	Number of UDP connections that have passed through the Firewall. Example: UDPConn=527894. Affected logs: I_filterstat.
<b>UDPConnNatDst</b>	Number of UDP connections with a translated destination. Example: UDPConnNatDst=12. Affected logs: I_filterstat.
<b>UDPConnNatSrc</b>	Number of UDP connections with a translated source. Example: UDPConnNatSrc=15. Affected logs: I_filterstat.
<b>UDPPacket</b>	Number of UDP packets that have passed through the Firewall. Example: UDPPacket=6164646. Affected logs: I_filterstat.
<b>UI</b>	Sofbus/Lacbus information unit String of characters in UTF-8 format. Example: UI=Instruction. Available from: SNS v4.3.0. Affected logs: I_plugin.
<b>unitid</b>	Value of the "Unit Id" in a Modbus message that specifies a PLC. Example: unitid=255. Available from: SNS v2.3.0. Affected logs: I_plugin.
<b>unreachrate</b>	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: I_routerstat.



---

<b>uprate</b>	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: <code>_routerstat</code> .
<b>urlruleid</b>	Number of the URL filter rule applied. Digital format. Example: urlruleid=12 Available from: SNS v3.2.0. Affected logs: <code>_web</code> .
<b>user</b>	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: <code>_alarm</code> , <code>_auth</code> , <code>_connection</code> , <code>_ftp</code> , <code>_plugin</code> , <code>_pop3</code> , <code>_sandboxing</code> , <code>_server</code> , <code>_smtp</code> , <code>_ssl</code> , <code>_web</code> and <code>_xvpn</code> .
	<i>User</i>
<b>usergroup</b>	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: <code>_vpn</code> .
	<i>Group</i>

---

## V

---

<b>version</b>	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: <code>_connection</code> and <code>_plugin</code> .
	<i>Protocol version</i>

---

<b>VlanXX</b>	Indicators of bandwidth used for each of the VLANs defined: <ul style="list-style-type: none"><li>• Name of the VLAN. String of characters in UTF-8 format.</li><li>• Incoming throughput (bits/second),</li><li>• Maximum incoming throughput for a given period (bits/second),</li><li>• Outgoing throughput (bits/second),</li><li>• Maximum outgoing throughput for a given period (bits/second),</li><li>• Number of packets accepted,</li><li>• Number of packets blocked.</li></ul> Format: 7 values separated by commas. Example: "Vlan_Servers,61515,128648,788241,1890520". Affected logs: <code>_monitor</code> .
	<i>Interface monitoring / Bandwidth use</i>

---



---

<b>virus</b>	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.
	<i>Virus</i> Example: "clean".
<b>vulnid</b>	Unique Stormshield Network ID of the detected vulnerability. Example: vulnid=148262. Affected logs: l_pvm.
	<i>Vuln ID</i>

---

## W

---

<b>WifiXX</b>	Concerns only firewalls equipped with Wi-Fi antennas (W models). Indicators of bandwidth used for each active Wi-Fi access points: <ul style="list-style-type: none"><li>• Access point name. String of characters in UTF-8 format.</li><li>• Incoming throughput (bits/second),</li><li>• Maximum incoming throughput for a given period (bits/second),</li><li>• Outgoing throughput (bits/second),</li><li>• Maximum outgoing throughput for a given period (bits/second),</li><li>• Number of packets accepted,</li><li>• Number of packets blocked.</li></ul> Format: 7 values separated by commas. Example: Wifi01=Public_WiFi,61515,128648,788241,1890520,2130,21. Affected logs: l_monitor.
<b>wldev0</b>	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: <ul style="list-style-type: none"><li>• Name of the interface. String of characters in UTF-8 format.</li><li>• Incoming throughput (bits/second),</li><li>• Maximum incoming throughput for a given period (bits/second),</li><li>• Outgoing throughput (bits/second),</li><li>• Maximum outgoing throughput for a given period (bits/second),</li><li>• Number of packets accepted,</li><li>• Number of packets blocked.</li></ul> 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).



**STORMSHIELD**

[documentation@stormshield.eu](mailto:documentation@stormshield.eu)

*All images in this document are for representational purposes only, actual products may differ.*

*Copyright © Stormshield 2026. All rights reserved. All other company and product names contained in this document are trademarks or registered trademarks of their respective companies.*