STORMSHIELD

TECHNICAL NOTE

STORMSHIELD NETWORK SECURITY

COMPLYING WITH PRIVACY REGULATIONS

Product concerned: SNS 3.4 and higher versions, SNS 4.x

Document last updated: April 14, 2020

Reference: sns-en-complying_with_privacy_regulations_technical_note

Table of contents

Getting started

SNS helps you to apply the provisions of the privacy regulations, including European General Data Protection Regulation (GDPR) within your infrastructure. In particular, under this regulation, users' personal data must remain confidential, and any processing of their data must be logged. SNS guarantees the anonymization - therefore, the confidentiality - of personal data found in logs, reports, monitoring screens (e.g., user identity, host name, source IP address), etc. By default, only supervisors can view such information. Other administrators (operators) are only allowed full access to logs for justifiable purposes, and after having requested an individual and temporary code. All operations performed after this code has been activated will be logged.

Levels of responsibility

SNS allows you to define various roles and levels of responsibility in order to ensure that you comply with the privacy regulations.

Supervisors

Supervisors are SNS administrators who hold *Access to private data* and *Management of access to private data* privileges. This means that they can view private data contained in logs. Whenever necessary, they can grant access to operators in the form of temporary tickets.

Operators

Operators are SNS administrators who can only view anonymized data by default and do not have access to private data. Whenever necessary, they can request a ticket for temporary access from their supervisor. A system event will be generated in alarms and on the dashboard when such tickets are used.

End users

Every user can be assured that access to private data pertaining to him is protected and monitored. Detailed logs provide information every time such data is accessed: date, identity of the operator, actions performed, etc.

Use case

The various privacy regulation compliance scenarios are covered by SNS features. In both examples described below, the client has decided to delegate the configuration and maintenance of the firewall to a service provider.

Modifying the firewall's configuration

Take for example a client who asks his service provider to modify the configuration of his firewall.

The operator who makes these changes does not have access to any private data: all user names, source IP addresses, host names, etc., are hidden.

Troubleshooting a network issue

Take for example a client who asks his service provider to resolve a network issue.

The operator must be entitled to full access to logs in order to troubleshoot effectively. He must therefore request a temporary access ticket from his supervisor, who will then issue one in the form of a 16-digit code. The operator then proceeds to resolve the issue before releasing the temporary ticket. All actions that the operator performs will be recorded and can be monitored.

Event manager (SIEM)

SNS does not anonymize private data for logs that are exported to SIEM (Security Information and Event Management) event collection and management tools. If you are using a SIEM tool, you will need to configure it so that it complies with the privacy regulations. However, SNS makes it possible to encrypt all connections between the firewall and the SIEM.

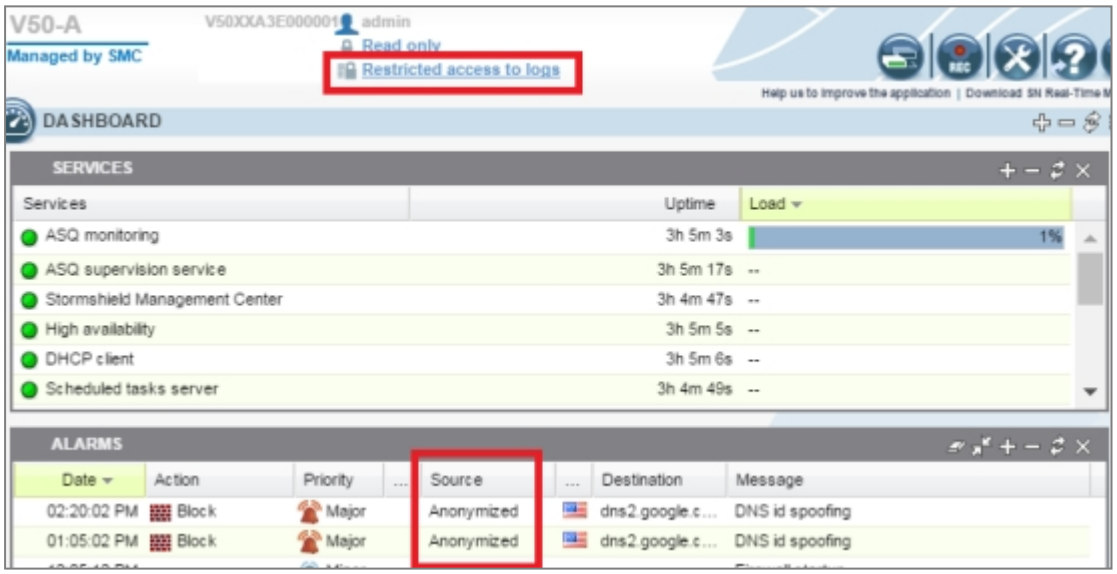
As a supervisor

If you are the firewall supervisor, you would have been logged on to the web administration interface with the *admin* account. The following are the operations that you will need to perform in order to comply with the privacy regulations:

- Accessing full logs,
- Creating operators,
- Allowing operators full access to logs,
- Checking operators' actions.

Accessing full logs

1. Log on to the web administration interface using the *admin* account. The dashboard will then appear. As implied by the link **Restricted access to logs** in the upper banner of the window, private data is hidden by default.



2. Click on **Restricted access to logs** in the banner. A dialog box will open to indicate that this action will be recorded in logs.
3. Click on **Obtain**.
   You will now be able to view private data, as shown by the link **Full access to logs (private data)** in the upper banner.

Creating operators

You can create administrators acting as operators, who will be able to perform maintenance operations without viewing private data.

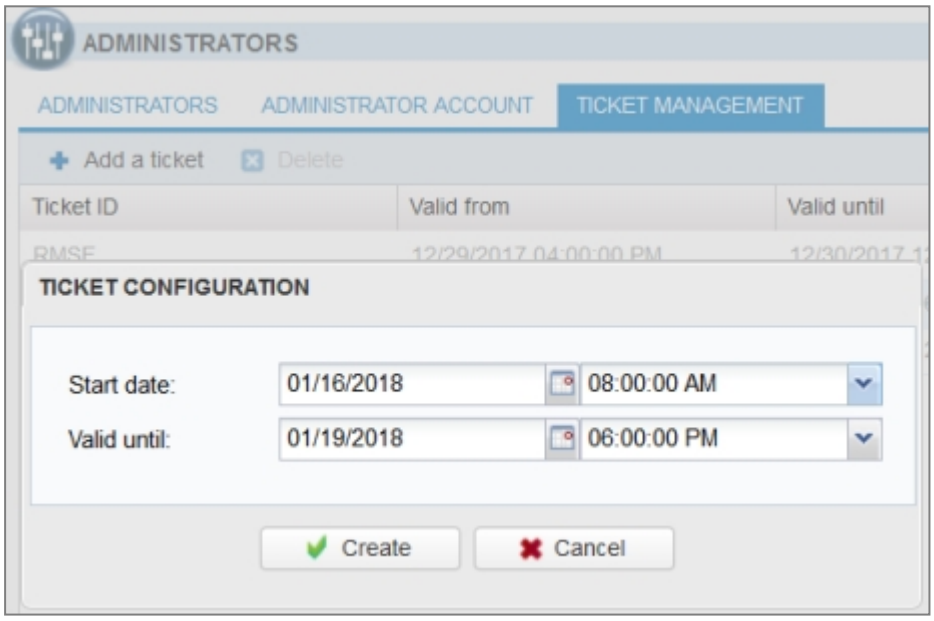
1. Log on to the web administration interface with the *admin* account.
2. In the module **Configuration > System > Administrators**, add an administrator without access to private data. By default, this administrator only has privileges to view logs and reports.
3. You may grant other privileges if you wish to, except for **Access to private data** and **Management of access to private data**.

4. Repeat the same steps for each operator that you wish to create.
5. Click on **Apply**.

Allowing operators full access to logs

Where necessary, you can issue access tickets to operators in order to allow them to view private data contained in logs, on a temporary basis.

1. Log on to the web administration interface using a supervisor account (i.e., an administrator with *Access to private data* and *Management of access to private data* privileges.
2. In the module **Configuration > System > Administrators**, click on **Ticket management**, then on **Add a ticket**.
3. In the **Ticket configuration** window, enter the dates and times to and from which the ticket remains valid.

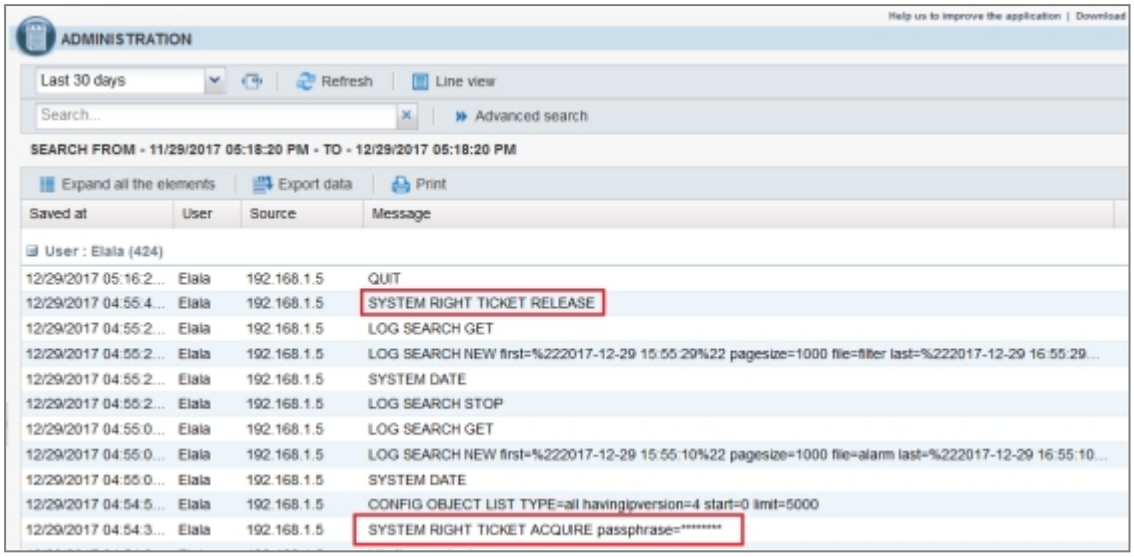


4. Click on **Create,** then on **Apply**.
5. In the **Code for access to private data** column, copy the code by clicking on the icon.
6. Give the operator the 16-digit code that will allow full access to logs.

Checking operators' actions

It is possible to check the actions performed by an operator to whom you have issued a ticket for temporary access to private data.

1. Log on to the web administration interface with the *admin* account.
2. In the upper banner of the page, click on **Restricted access to logs** and confirm.
3. Select the module **Audit logs > Logs > Administration**.
4. In the **User** column header, click on the arrow then on **Group by this field** to view only logs matching the operator whose actions you wish to check.
5. In the logs, the entry *SYSTEM RIGHT TICKET ACQUIRE passphrase=********* indicates when the ticket started being used, while the entry *SYSTEM RIGHT TICKET RELEASE* indicates the end of its use. In between both events, the operator was able to view private data.


Help us to improve the application | Download
ADMINISTRATION
Last 30 days
Refresh
Line view
Search...
Advanced search
SEARCH FROM - 11/29/2017 05:18:20 PM - TO - 12/29/2017 05:18:20 PM
Expand all the elements
Export data
Print
Saved at
User
Source
Message
User : Elala (424)
12/29/2017 05:16:2... Elala 192.168.1.5 QUIT
12/29/2017 04:55:4... Elala 192.168.1.5 SYSTEM RIGHT TICKET RELEASE
12/29/2017 04:55:2... Elala 192.168.1.5 LOG SEARCH GET
12/29/2017 04:55:2... Elala 192.168.1.5 LOG SEARCH NEW first=%222017-12-29 15:55:29%22 pagesize=1000 file=filter last=%222017-12-29 16:55:29...
12/29/2017 04:55:2... Elala 192.168.1.5 SYSTEM DATE
12/29/2017 04:55:2... Elala 192.168.1.5 LOG SEARCH STOP
12/29/2017 04:55:0... Elala 192.168.1.5 LOG SEARCH GET
12/29/2017 04:55:0... Elala 192.168.1.5 LOG SEARCH NEW first=%222017-12-29 15:55:10%22 pagesize=1000 file=alarm last=%222017-12-29 16:55:10...
12/29/2017 04:55:0... Elala 192.168.1.5 SYSTEM DATE
12/29/2017 04:54:5... Elala 192.168.1.5 CONFIG OBJECT LIST TYPE=all havingipversion=4 start=0 limit=5000
12/29/2017 04:54:3... Elala 192.168.1.5 SYSTEM RIGHT TICKET ACQUIRE passphrase=********

Operators

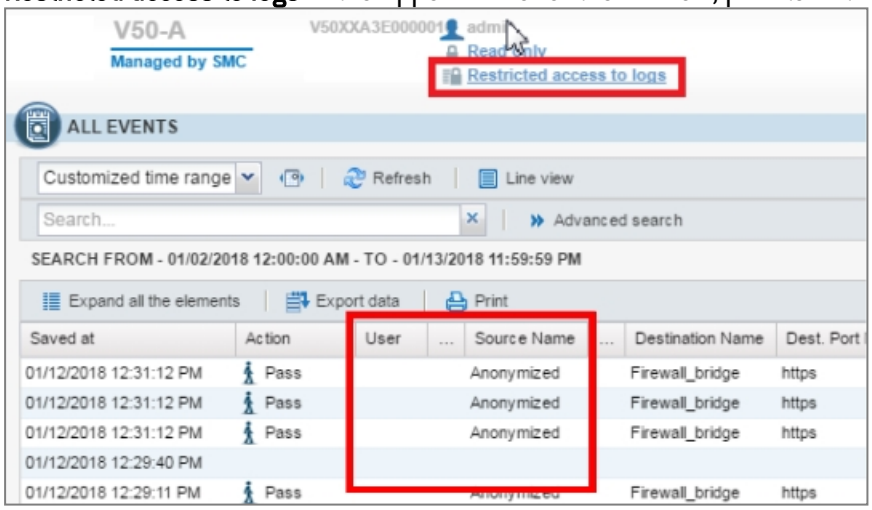
Operators are users to whom the super-administrator of the firewall (*admin*) has granted certain administration privileges. By default, they do not have access to private data, but may request such access from the supervisor when the need arises.

If you log on to the web administration interface as an operator, private data will be hidden, as shown by the **Restricted access to logs** link in the upper banner.

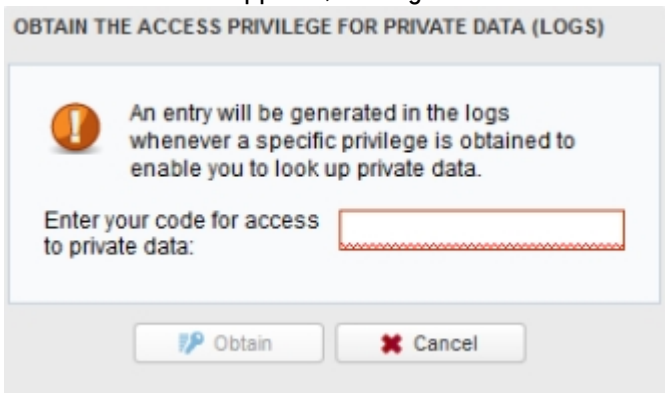
Accessing full logs

For certain maintenance or troubleshooting operations, you may require full access to logs as well as all reports and monitoring screens that contain private data.

1. Request a ticket from the firewall supervisor to obtain full access to logs. The supervisor will then send you a 16-digit code that enables access to private data.
2. Log on to the web administration interface to view these logs. As implied by the link **Restricted access to logs** in the upper banner of the window, private data is hidden.



3. Click on **Restricted access to logs** in the banner.
4. In the window that appears, enter your code for access to private data.



5. Click on **Obtain**.
   You will now be able to view private data in all modules, as shown by the link **Full access to logs (private data)** in the upper banner.

If you wish to view reports and monitoring screens containing private data, you may also enter your code when you access these screens.

Disabling full access to logs

The ticket enabling full access to logs is valid for a duration defined by the administrator. Once the ticket reaches its expiration date, the access code will no longer function.

You are advised to manually disable full access to logs when you no longer need it.

1. In the upper banner of the web administration interface, click on **Full access to logs (private data)**. A confirmation window will appear.
2. Click on **Release** to disable full access to logs.

You will no longer be able to view private data, as shown by the link **Restricted access to logs** in the upper banner.

Further reading

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

documentation@stormshield.eu