GUIDE

STORMSHIELD NETWORK SECURITY

REAL-TIME MONITOR - ADMINISTRATION GUIDE

Version 3

Document last updated: June 2, 2022

Reference: sns-en-sn_real-time_monitor-user_configuration_manual-v3

Foreword

Welcome to the Stormshield Network Real-Time Monitor v3 administration guide.

Products concerned

U30S, U70S, U150S, U250S, U500S, U800S,
SN150, SN160w, SN200 , SN210w, SN300, SN310,
SN500, SN510, SN700, SN710, SN900, SN910,
SN2000, SN3000, SN6000,
SNi40,
VS5, VS10, V50, V100, V200, V500 and VU.

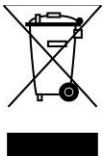
The contents of this document relate to the developments in Stormshield's technology at the time of its writing. With the exception of the mandatory applicable laws, no guarantee shall be made in any form whatsoever, expressly or implied, including but not limited to implied warranties as to the merchantability or fitness for a particular purpose, as to the accuracy, reliability or the contents of the document.

Stormshield reserves the right to revise this document, to remove sections or to remove this whole document at any moment without prior notice.

Liability

This manual has undergone several revisions to ensure that the information in it is as accurate as possible. The descriptions and procedures herein are correct where Stormshield Network firewalls are concerned. Stormshield rejects all liability directly or indirectly caused by errors or omissions in the manual as well as for inconsistencies between the product and the manual.

Warning



WEEE Directive

All Stormshield products that are subject to the WEEE directive will be marked with the mandated "crossed-out wheeled bin" symbol (as shown above) for items shipped on or after August 13, 2005. This symbol means that the product meets the requirements laid down by the WEEE directive with regards to the destruction and reuse of waste electrical and electronic equipment. For further details, please refer to the website at this address: https://www.stormshield.com/about-us/recycling/

Table of contents

1. Basic principles

This section explains:

- The basic knowledge required for the proper understanding of the information provided in this guide.
- The typographical conventions and specific terms used.
- Resources for obtaining additional help on how to operate SN Real-Time Monitor.

1.1 Who should read this?

This manual is intended for network administrators or, at the least, for users with IP knowledge.

In order to configure your Stormshield Network UTM firewall in the most efficient manner, you must be familiar with IP operation, its protocols and their specific features:

- ICMP (Internet Control Message Protocol).
- IP (Internet Protocol).
- TCP (Transmission Control Protocol).
- UDP (User Datagram Protocol).

Knowledge of the general operation of major TCP/IP services is also desirable:

- HTTP.
- FTP.
- Mail (SMTP, POP3, IMAP).
- Telnet.
- DNS.
- DHCP.
- SNMP.
- NTP.

If you do not possess this knowledge, don't worry: any general book on TCP/IP can provide you with the required elements.

1.2 Typographical conventions

1.2.1 Abbreviations

For the sake of clarity, the usual abbreviations have been kept. For example, **VPN** (*Virtual Private Network*).

1.2.2 Display

Names of windows, menus, sub-menus, buttons and options in the application will be represented in the following fonts:

Example: Interfaces Menu

1.2.3 Indications

Indications in this manual provide important information and are intended to attract your attention to important points. Among these, you will find:

NOTE/REMARKS

These messages provide a more detailed explanation on a particular point.

WARNING

These messages warn you about the risks involved in performing a certain manipulation or about how not to use your appliance.

TIP

Such messages give you ingenious ideas on using the options on your product.

DEFINITION

Describes technical terms relating to Stormshield Network or networking. These terms will also be covered in the glossary.

1.2.4 Messages

Messages that appear in the application are indicated in double quotes.

Example: "Delete this entry?"

1.2.5 Examples

Example: This allows you to have an example of a procedure explained earlier.

1.2.6 Command lines

Command lines

```
Indicates a command line (for example, an entry in the DOS command
window).
```

1.2.7 Recaps of general points

Reminders are indicated as follows:

- Reminder description.

1.2.8 Access

Access paths to features are indicated as follows:

- Go to the File\Firewall menu.

1.3 Vocabulary used in the manual

Dialup	Interface on which the modem is connected.
Firewall	Stormshield Network UTM device /product
Configuration slot	(or policy). Configuration files which allow generating filter and NAT policies, for example.
Logs	.

1.4 Getting help

To obtain help regarding your product and the different applications in it:

- Website: https://mystormshield.eu/. Your secure-access area allows you to access a wide range of documentation and other information.
- SNS User configuration manual and Stormshield Network Real-Time Monitor User manual.

1.5 Technical Assistance Center

Stormshield Network provides several resources and tools for resolving technical issues on your firewall.

- A knowledge base.
- A certified distribution network. You can therefore ask your reseller for advice,
- Documents: these can be accessed from your client or partner area. You will need a client account in order to access these documents.

For further information regarding technical assistance, please refer to the document "Support charter".

2. Software installation

This section provides you with the elements for installing the software suite that would allow you to administer your product. *For further information on the appliances and how to install them, please refer to the product installation guide.*

You will need the graphical interface installation file. This file can be found on the website (https://mystormshield.eu/). The installation file is in English and French. You will also need your firewall's internal IP address as well as its serial number.

2.1 Prerequisites

Stormshield Network Real-time Monitor v3 is supported on the following operating systems:

- Microsoft Windows 10 and 11.
- Microsoft Windows Server 2012 R2, 2016 and 2022.

2.2 Installing via your personal area

Download the necessary files from the website and execute the .EXE program corresponding to the administration suite. The installation information will appear in the same language as the version of Windows that has been installed.

2.2.1 Verification procedure

Signature verification procedure

When you download an application from your client or partner area on https://mystormshield.eu/, the following message will appear: "Open a file or save on your computer? ".

- If you choose "Open", your web browser will check the signature automatically and inform you about the results.
- If you choose "Save" (recommended option), you will need to perform the check manually.

Manual verification

To manually check the application's signature, follow the procedure below before installing the application:

1 Right-click on the Stormshield Network appliance whose signature you wish to check then select the **Properties** menu from the contextual menu that appears.

2 Select the *Digital signatures* tab then the name of the signer (NETASQ).

3 Click on **Details**: this window will indicate whether the digital signature is valid.

2.2.2 Registration

During installation, you will be asked to register your product. This registration is mandatory in order to obtain your product's license, to download updates and to access technical support.

3. SN Real-Time Monitor

Stormshield Network **Real-Time Monitor** allows you to visualize your Firewall's activity in real time and provides the information below:

- Use of the Firewall's internal resources (memory, CPU, etc.),
- List of raised alarms when vulnerabilities are detected,
- List of connected hosts and users,
- Real-time alarms,
- Number of connections, bandwidth use, throughput,
- List and status of gateways used by the firewall,
- Information on the status of interfaces and VPN tunnels,
- Last logs generated,
- Use of disk space allocated to logs.

With this tool, you can connect to several firewalls and supervise all of them.

Stormshield Network **Real-Time Monitor** provides a simple display of connections transiting via the firewall, along with any alarms it has generated.

By default, Monitor can only be run on a machine connected to the internal network and must be running permanently in order to avoid missing any alarms.

SN Real-Time Monitor logs on to firewalls using their web administration port (TCP/443 – HTTPS by default). In this way, they can benefit from the authentication methods and policies defined on the monitored firewalls. When this port is modified (Firewall administration tab in the Configuration module), the connection can be established by indicating the firewall's IP address and the customized administration port, separated by colons (":").

3.1 Access

There are 2 ways to launch the Stormshield Network **Real-Time Monitor** application:

- Via the shortcut **Applications\Launch Stormshield Network Real-Time-Monitor** in the menu bar on other applications in the Administration Suite.
- Via the menu **Start\Programs\Stormshield\Administration Suite 1.0\ Stormshield Network Real-Time Monitor.**

If this is your very first time connecting to your product, a message will prompt you to confirm the serial number (found on the underside of the firewall).

The **Overview** window will open upon connection:

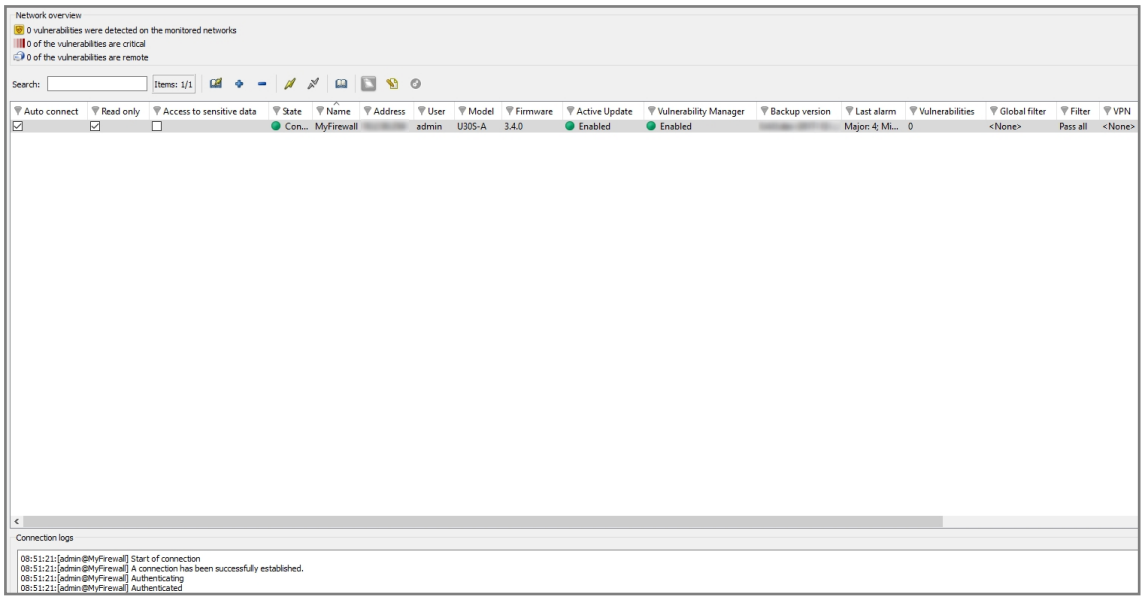


Figure 1: Overview

3.2 Connection

Stormshield Network Real-Time Monitor is opened differently depending on the option chosen in the *Behavior at startup* tab in **Application settings** (cf. Part 2/Section Behavior at startup).

The possible options are:

- Direct connection.
- Connect automatically to data sources.
- None.

3.2.1 Direct connection to a Stormshield Network multifunction Firewall

Direct connection allows you to enter connection information for a specific firewall.

To set up a direct connection, go to the menu **File\Direct connection**. Or, if Monitor has been configured to connect directly at startup, the following window will appear:

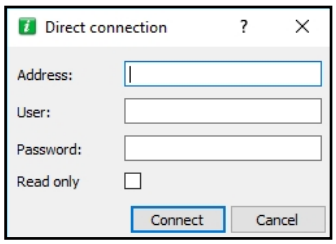


Figure 2: Direct connection

NOTE

For more information regarding connection, please refer to Behavior at startup.

1 Indicate the firewall's IP address in the **Address** field. If the firewall's web administration port has been modified, indicate the IP address followed by a colon, then the administration port.
Example: *192.168.0.1:3333*.

2. Enter the user login in the **User** field.

3. Enter the user password in the **Password** field.

> **REMARK**
>
> Select the option **Read only** to connect to the firewall in read-only mode.

4. Click on the **Connect** button.

5. A message prompting you to accept the firewall's certificate will then appear. Click on **Trust this certificate and log on** in order to finalize the connection to the firewall.

3.2.2 Opening the address book

Go to the menu **File\Address book** to open the address book. Or, if Monitor has been configured to open the address book at startup, the Address book window will appear:

> **NOTE**
>
> For more information regarding the address book, please refer to Address book.

3.2.3 Connect automatically to data sources.

If this option has been selected in **Behavior at startup\Application settings**, Monitor will directly open the "Overview" main window and the application will automatically connect to the existing firewalls. (cf. For more information regarding connection, please refer to Behavior at startup).

3.2.4 None

If this option has been selected in **Behavior at startup\ Application settings**, Monitor will directly open the "Overview" main window but no application will be connected to the firewall. Only the **Overview** menu will be enabled. The other menus in the directory will be grayed out. (cf. For more information regarding connection, please refer to Behavior at startup).

3.3 Address book

The address book can be accessed from the menu **File\Address book**.

> **REMARK**
>
> The address book can also be opened automatically upon the startup of the application if you have selected the option in **Application settings/Behavior at startup.** (cf. Section Behavior at startup).

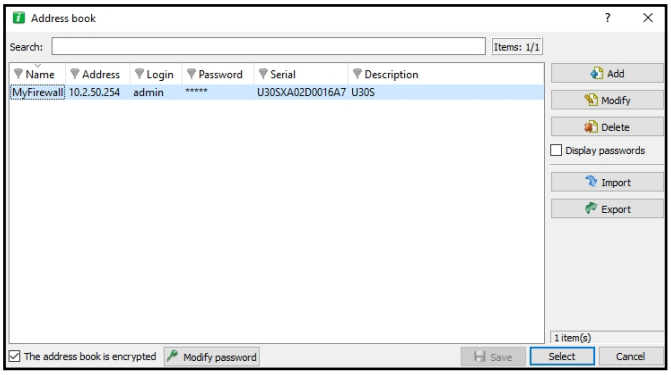


Figure 3: Address book

It is possible to store connection data on your different firewalls. This information is stored on the same client workstation on which the interface has been installed. It may be encrypted if you check the option **Address book is encrypted**. In this case, you will be asked to enter an encryption key. The information that is stored for each firewall includes the IP address, login name, connection password and the serial number of the firewall to which you wish to connect. This password belongs to an authorized user.

By specifying a serial number, you will protect yourself from "man-in-the-middle" attacks. If you attempt a connection on a firewall that does not meet the "serial number" criterion indicated in the address book, the monitor will inform you that you are attempting to connect to an unknown firewall. You will also be asked if you wish to add this serial number to the list of authorized firewalls. Verify the information displayed in the monitor before accepting such a request.

Once this information has been entered, you may save it using the **Save** button. To open a session on one of the firewalls from the address book, click on its name then on the **OK** button, or simply double click on the name of the firewall.

WARNING

If you modify the **Address book is encrypted** option, the address book has to be saved once more to apply the changes

Check the option **Display passwords** to check the passwords used for each Firewall saved in the address book (passwords are displayed in plaintext).

3.3.1 Adding an address

Click on the **Add** button to add an address to the address book. Other information to supply:

Name	The name of the firewall.
Address	IP address of the firewall. If the firewall's web administration port has been modified, indicate the IP address followed by a colon, then the administration port. **Example**: *192.168.0.1:3333*.
User	The user account.
Password	User password.
Confirm	Confirm the password.
Description	Description or comments regarding the firewall.

3.3.2 Modifying an address

The procedure for modifying an address in the address book is as follows:

1. Select the firewall to be modified.
2. Click on the **Modify** button. The following window will appear:

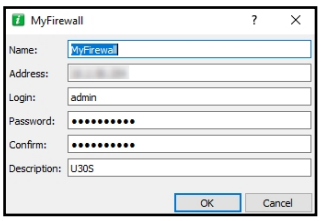


Figure 4: Modifying an address

3. Make the necessary changes.
4. Click on **OK** to confirm changes.

3.3.3 Deleting an address

The procedure for deleting a firewall from the address book is as follows:

1. Select the firewall to delete.
2. Click on the **Delete** button. The following message will appear:
"Delete this entry?"
3. Click on **Yes** or **No** to confirm whether to delete or cancel.

3.3.4 Importing an address book

The procedure for importing an existing address book is as follows:

1. Click on **Import**. The following window will appear:

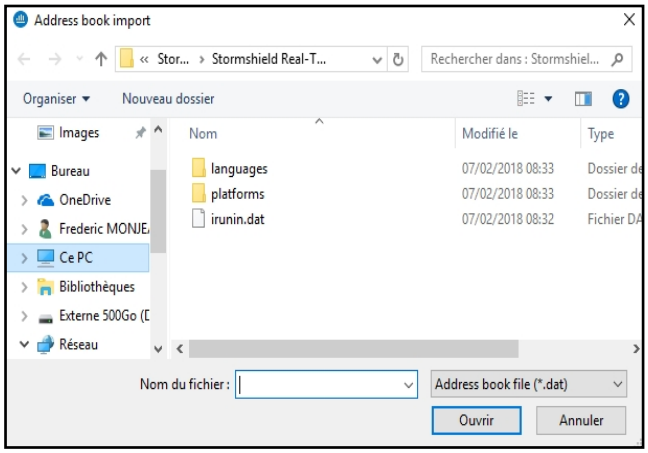


Figure 5: Importing the address book

2. Select the file to import.

REMARK

The file to import should be in .dat format.

3 Click on **Open**.

3.3.5 Exporting an address book

The procedure for exporting an existing address book is as follows:

1 Click on **Export**. The following window will appear:

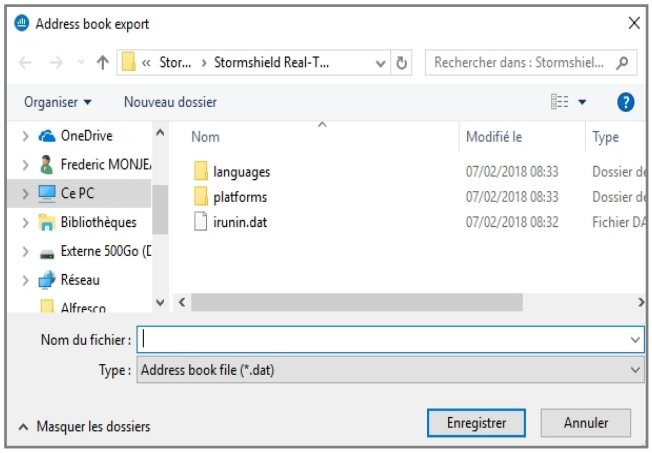


Figure 6: Exporting the address book

2 Select the file to export.

REMARK

The file to export should be in .dat format.

3 Click on **Save**.

3.3.6 Search

The search covers all information found in the columns.

Information can be filtered on a column and the search can then be refined.

Examples:

- Filter on the "Address" column containing 129: a list of results will appear; next, launch a global search by refining according to address.
- Filter on the "Address" column beginning with "10.2", then search from the displayed addresses, hosts with addresses beginning with "10.2.14" by entering only "14" in the search field.

3.4 Presentation of the interface

3.4.1 Main window

From this window, you can open several windows, each connected to different firewalls.

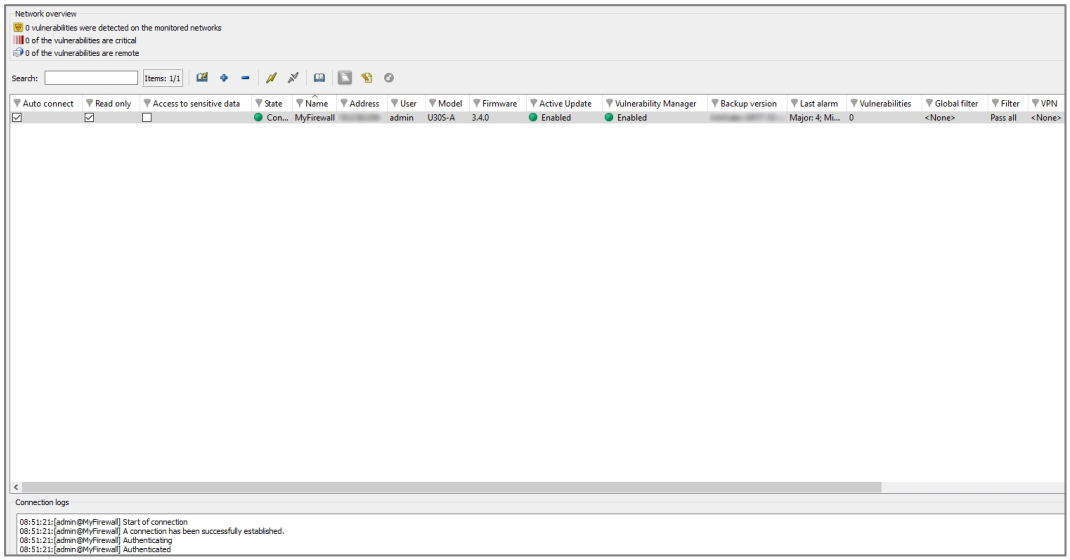


Figure 7: Overview

Once Monitor is connected, it will open a welcome window (Overview Menu) which will display various types of information on the firewall's activity.

It consists of five parts:

- A menu bar,
- A horizontal bar containing icons relating to connection and a search zone,
- A vertical bar containing a menu directory allowing **Stormshield Network Real-Time Monitor** options to be viewed and configured,
- A result display zone,
- A status bar.

REMARK

The other windows in the menu directory may contain a button bar or a checkbox:

- Refresh,
- Show / Hide help,
- Access to private data,
- Firewall,
- Duplicate.

3.4.2 Descriptions of icons

	Logs on via the address book.
	Connects directly to a firewall.
	Disconnects or deletes a connection.
	Connects to the selected firewall.
	Disconnects from the selected firewall.
	Edits the address book.
	Displays the dashboard of the selected firewall.
	Generates a web report for the selected firewall: • Summary of system resources, memory, CPU, etc. • List of connected hosts (IP address, interface to which the user is connected, amount of data transferred, number of connections, throughput used, etc.). • List of authenticated users (user name, IP, remaining time on authentication period, etc.). • List of alarms raised (major and minor). • List of active VPN tunnels. • List of active services. • Status of the Active Update module. • Statistics. • Vulnerability Manager.
	Logs on to the selected firewall's web administration.

3.4.3 Tabs

The main window contains the following menus: **File, Windows, Applications,** and **? (Help)**

File	Allows you to connect to firewalls and to access the application's general options.
Windows	Allows you to organize the connection windows on the screen.
? (Help)	Allows you to access the relevant Help file, and to know which version the monitor runs on.

3.4.4 Menu tree

Overview	This window lists the firewalls. Monitor opens in this window once the connection has been established. • The **Console** sub-menu: When the option Enable is selected in the menu **Application parameters\Miscellaneous** in the console zone, you will be able to access firewalls in console mode (CLI commands). When this window is validated, a **Console** menu will be added under the **Overview** menu directory.
Dashboard	This window gives you a summary of the main information relating to your product's activity.
Events	This window lists events that the firewall has raised.
Vulnerability management	This window allows you to view alarms being raised and to get help in the event of vulnerability.
Hosts	List of hosts on your network.
Interfaces	This screen makes it possible to obtain statistics on the use of QoS queues (bandwidth, connections, throughput, etc.).
Quality of Service	This window allows you to get statistics on bandwidth, connections and throughput.
Users	This window allows you to get information on users and session privileges on authentication.
Quarantine – ASQ Bypass	This window displays the list of dynamically quarantined hosts.
Routers	This window shows the status of routers used in the configuration of the firewall: default gateway and routers configured in filter rules (PBR: Policy Based Routing).
VPN tunnels	This window displays static information on the operation of VPN tunnels and on the source and destination.
Active Update	This window sets out the status of Active Update on the firewall for each type of update available.
Services	This window shows the active and inactive services on the firewall and how long they have been active/inactive.
Hardware	This window shows information on the initialization of high availability and RAID.
Filter policy	This window displays the active filter policy by grouping implicit and local rules.
VPN Policy	This window allows viewing the configuration of various VPN tunnel policies.
Logs	This window allows viewing the size of the log file in real time. • The VPN sub-menu provides information on VPN logs. • The System sub-menu provides system information.

3.4.5 Result display zone

Data and options from the selected menus in the horizontal bar appear in this zone. These windows will be explained in further detail in the corresponding sections.

Pop-up menu on columns

Right-clicking on a column header will display the following options:

Filter by this column	Isolates a set of events according to the criteria provided. For example, filtering by events with a "minor" protocol. When a filter has been applied to a column, the icon will appear in blue in the column label.
Clear column filter	Removes the filter that was previously set on the column.
Clear all filters	Removes the filters set on all the columns.
Clear all filters except this	Removes the filters set on all the columns except for the filter on the selected column.
Hide column	Hides the selected column.
Columns	Allows selecting the columns to display.
Adjust column width to fit contents	Columns will be resized according to the contents.

When the menu **Filter by this column** is selected, the following screen will appear:

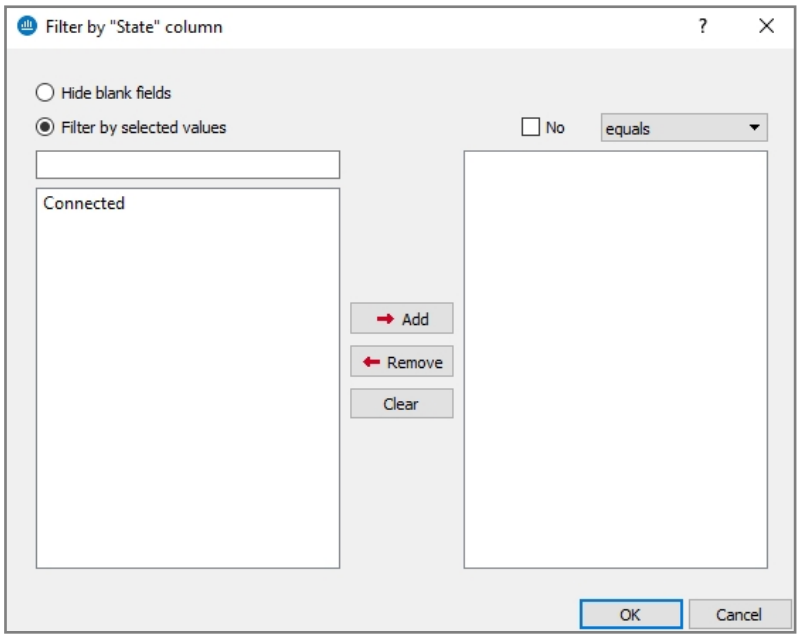


Figure 8: Filter by this column

The screen relates to the column that had been selected previously. (E.g.: *Filter by the "Details" column*).

- **Hide blank fields** option: allows displaying only fields that contain data.
- **Filter by selected values**: a value can be entered manually or selected from the suggested list.

To create a filter, you only need to select one or several values from the suggested list and add them in order for them to appear in the section to the right of the table.

You may use the following operators:

- **Equals**: the values found have to be equal to those selected.
- **Contains**: looks for a word in a phrase
- **Begins with**: looks for a phrase beginning with a string
- **Ends with**: looks for a phrase ending with a string.
- **Joker (Wildcard):** See the table below.
- **Regular expression**: cf. http://qt-project.org/doc/qt-4.8/qregexp.html

c	E.g., if "c" is entered, the system will search for all occurrences of "c".
?	Allows searching for a single character.
*****	Allows searching for one or several characters.
[…]	Allows entering several characters between square brackets. For example, if [ABCD] is selected, the search will be conducted for A or B or C or D. If [A-D] is entered, the search will be for ABCD, if [A-Z] is entered, the search will be for all capital letters.

Events can therefore be filtered according to one or several values. For example, displaying events using HTTP or HTTPS.

It is also possible to negate a criterion by selecting **No**. For example, display all entries unless the protocol used is HTTP.

- Columns can be resized according to their contents (option **Adjust columns to fit contents**).

Furthermore, the administrator can sort the table by clicking on the column by which he wishes to sort.

Pop-up menu on rows

Right-clicking against a line will display a pop-up menu that allows various operations. The options offered vary according to the table.

Overview

3 pop-up menus can be opened in this window:

- When right-clicking against a firewall
- When right-clicking against an empty zone in the list of firewalls
- When right-clicking against the "Connection logs" view

Pop-up menu relating to a firewall

Show dashboard…	Opens the Dashboard menu of the selected firewall.
Generate an instant web report…	Clicking on this button will generate a report in HTML. This report will contain the following information at any given moment: system information, memory, connected users, services, Active Update status, bandwidth statistics, connection statistics, vulnerabilities, number of hosts, authenticated users, number of major and minor alarms, quarantine, the number of VPN tunnels, filter rules and configured IPSec tunnels.

Launch Web administration interface	Allows logging on to the web administration interface of the selected firewall
Log off	Allows logging off from the selected firewall.
Remove this firewall from the connection list…	Enables disconnecting and deleting the entry that corresponds to this connection.
Add a new firewall to the connection list and connect to it	Displays the direct connection window to allow logging on to a firewall.
Add a firewall from the address book to the connection list	Opens the address book window to allow the selection of a registered firewall.
Add this firewall to the address book	Opens a window that will allow saving the selected firewall in the address book.
Edit the address book	Opens the address book window to enable editing.

Pop-up menu from right-clicking against an empty zone

Add a new firewall to the connection list and connect to it	Displays the direct connection window to allow logging on to a firewall.
Add a firewall from the address book to the connection list	Opens the address book window to allow the selection of a registered firewall.
Edit the address book	Opens the address book window to enable editing.

Pop-up menu relating to connection logs

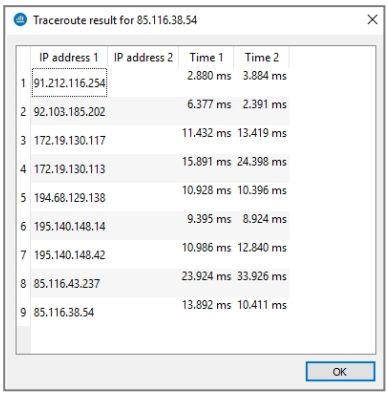
Copy	Copies the selected log line(s).
Copy link location	Copies the location of the link.
Select all	Selects all the log lines.
Clear logs	Deletes all log lines.

Events

Right-clicking against a line containing an event will bring you to the pop-up menu that will allow you to:

Filter by these criteria,	This option allows restricting the list of results to the selected field. For example, if the data is filtered by the priority "Major", the administrator will get all the lines containing "Major". **NOTE** Using this option will replace all the current filters on the columns
Filter only this column by this criterion,	This option allows restricting the list of results to the criteria under your cursor. **Example** If your cursor points to the destination / website consulted, the displayed list will only present the elements containing this destination / website.
View source host…	Indicates the name of the source host. If this option is selected, the Hosts menu will open.
View destination host…	Indicates the name of the destination host.
Add the source host to the Object base	This option allows: • Creating an object corresponding to the selected source IP address directly in the firewall's object base in Stormshield Network Real Time Monitor. • Adding this object to an existing group on the firewall. For further information regarding this option, please refer to the Technical Note "Stormshield Network Collaborative Security".
Add the destination host to the Object base	This option allows: • Creating an object corresponding to the selected destination IP address directly in the firewall's object base in Stormshield Network Real Time Monitor • Adding this object to an existing group on the firewall. For further information regarding this option, please refer to the Technical Note "Stormshield Network Collaborative Security".
Ping source host	Allows pinging the source host from the firewall and obtaining its response time as a result.

Traceroute to source host	Two `Traceroute` commands are used to determine and test all appliances traffic has to go through in order to reach the source host from the firewall. The results are presented in the form of a table containing four columns:



- IP address no. 1: nominal IP address of hosts encountered.
- IP address no. 2: alternative IP address of hosts encountered (appliances in load balancing, for example).
- Time 1: response time of each appliance during the first Traceroute.
- Time 2: response time of each appliance during the second Traceroute.

REMARK
When an appliance on the route does not respond to Traceroute requests, SN Real-Time Monitor will wait for the test packet to expire. The display time of the results window may then be longer.

Ping destination host	Allows `pinging` the destination host from the firewall and obtaining its response time as a result.
Traceroute to destination host,	Allows testing and listing (`Traceroute`) all appliances traffic has to go through in order to reach the selected destination host from the firewall. This action works in the same way as **Traceroute to source host.**
Send source to quarantine	Allows quarantining the source host for a fixed period of 1 minute, 5 minutes, 30 minutes or 3 hours.
View packet...	This will open the tool that will allow you to view malicious packets.
Flush alarms	Clears the list of alarms displayed.
Copy to the clipboard	Copies the selected line to the clipboard.

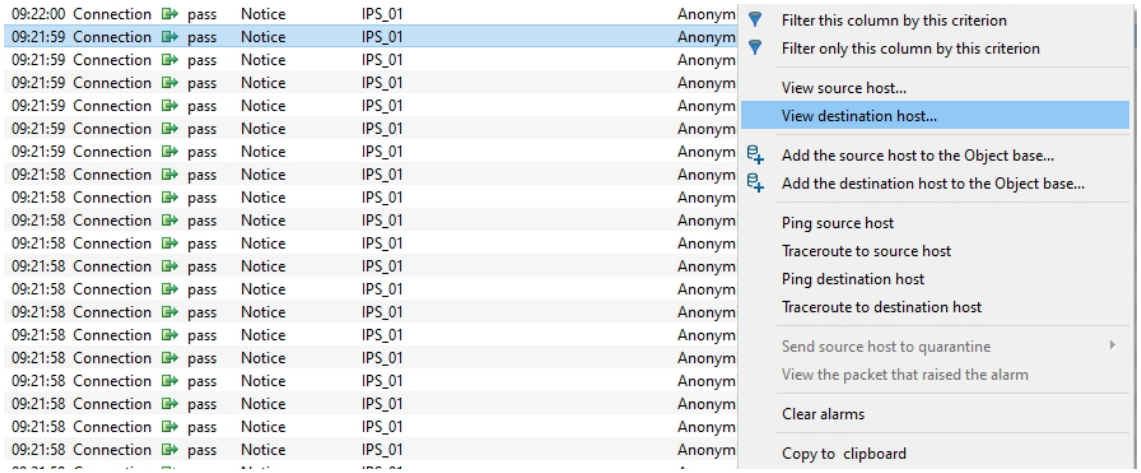


Figure 9: Pop-up menu

Vulnerability manager

In the Vulnerability tab, 3 pop-up menus can be opened:

- When right-clicking against a line detailing a vulnerability
- When right-clicking against a line detailing a host
- When right-clicking against the help zone,

Pop-up menu for a line containing a vulnerability

Right-clicking against a line containing vulnerability will bring you to the pop-up menu that will allow you to:

Filter by these criteria,	This option allows restricting the list of results to the selected field. For example, if the data is filtered by "Critical" priority, the administrator will get all the lines containing "Critical". **NOTE** Using this option will replace all the current filters on the columns
Filter only this column by this criterion,	This option allows restricting the list of results to the criteria under your cursor. **Example** If your cursor points to the destination / website consulted, the displayed list will only present the elements containing this destination / website.
Copy to the clipboard	Copies the selected line to the clipboard.

Pop-up menu for a line containing a host

Right-clicking against a line containing a host will bring you to the pop-up menu that will allow you to:

Filter by these criteria,	This option allows restricting the list of results to the selected field. For example, if the data is filtered by the "Client" priority, the administrator will get all the lines containing "Client" hosts. **NOTE** Using this option will replace all the current filters on the columns
Filter only this column by this criterion,	This option allows restricting the list of results to the criteria under your cursor. **Example** If your cursor points to the destination / website consulted, the displayed list will only present the elements containing this destination / website.
View host	The **Hosts** tree menu will open to display additional information on the detected host. During “pre-filtering”, the host concerned will be selected. The data will be filtered according to the host name if available, or by its address.
Add the host to the Object base,	This option allows: • Creating an object corresponding to the selected source IP address directly in the firewall’s object base in Stormshield Network Real Time Monitor. • Adding this object to an existing group on the firewall. For further information regarding this option, please refer to the Technical Note “Stormshield Network Collaborative Security”.
Copy to the clipboard	Copies the selected line to the clipboard. Data can be copied in two different ways: 1. A single line is selected: in this case, this line as well as the lines of details will be copied. 2. Several lines are selected: in this case, only these lines will be copied to the clipboard.

In the *Applications* tab, 2 pop-up menus can be opened:

- When right-clicking against a line detailing an application
- When right-clicking against a line detailing a host

Pop-up menu for a line containing an application

Right-clicking against a line containing an application will bring you to the pop-up menu that will allow you to:

Filter by these criteria,	This option allows restricting the list of results to the selected field. For example, if the data is filtered by the "Web server", the administrator will get all the lines containing the "Web server" family. **NOTE** Using this option will replace all the current filters on the columns
Filter only this column by this criterion,	This option allows restricting the list of results to the criteria under your cursor. **Example** If your cursor points to the destination / website consulted, the displayed list will only present the elements containing this destination / website.

Copy to the clipboard	Copies the selected line to the clipboard. Data can be copied in two different ways: 1. A single line is selected: in this case, this line as well as the lines of details will be copied. 2. Several lines are selected: in this case, only these lines will be copied to the clipboard.

Pop-up menu for a line containing a host

Filter by these criteria,	This option allows restricting the list of results to the selected field. For example, if the data is filtered by "Linux OS", the administrator will get all the lines containing the "Linux OS". **NOTE** Using this option will replace all the current filters on the columns
Filter only this column by this criterion,	This option allows restricting the list of results to the criteria under your cursor. **Example** If your cursor points to the destination / website consulted, the displayed list will only present the elements containing this destination / website.
View host	The **Hosts** tree menu will open to display additional information on the detected host. During “pre-filtering”, the host concerned will be selected. The data will be filtered according to the host name if available, or by its address.
Add the host to the Object base,	This option allows: • Creating an object corresponding to the selected IP address directly in the firewall’s object base in Stormshield Network Real Time Monitor. • Adding this object to an existing group on the firewall. For further information regarding this option, please refer to the Technical Note “Stormshield Network Collaborative Security”.

In the *Information* tab, 3 pop-up menus can be opened:

- When right-clicking against a line containing information
- When right-clicking against a line detailing a host
- When right-clicking against the help zone,

Pop-up menu for a line containing information

Filter by these criteria,	This option allows restricting the list of results to the selected field. For example, if the data is filtered by the "Web server", the administrator will get all the lines containing the "Web server" family. **NOTE** Using this option will replace all the current filters on the columns
Filter only this column by this criterion,	This option allows restricting the list of results to the criteria under your cursor. **Example** If your cursor points to the destination / website consulted, the displayed list will only present the elements containing this destination / website.

Copy to the clipboard	Copies the selected line to the clipboard. . Data can be copied in two different ways: 1. A single line is selected: in this case, this line as well as the lines of details will be copied. 2. Several lines are selected: in this case, only these lines will be copied to the clipboard.

Pop-up menu for a line containing hosts

Right-clicking against a line containing an event will bring you to the pop-up menu that will allow you to:

Filter by these criteria,	This option allows restricting the list of results to the selected field. For example, if the data is filtered by "Linux OS", the administrator will get all the lines containing the "Linux OS". **NOTE** Using this option will replace all the current filters on the columns
Filter only this column by this criterion,	This option allows restricting the list of results to the criteria under your cursor. **Example** If your cursor points to the destination / website consulted, the displayed list will only present the elements containing this destination / website.
View host	The **Hosts** tree menu will open to display additional information on the detected host. During “pre-filtering”, the host concerned will be selected. The data will be filtered according to the host name if available, or by its address.
Add the host to the Object base,	This option allows: • Creating an object corresponding to the selected IP address directly in the firewall’s object base in Stormshield Network Real Time Monitor. • Adding this object to an existing group on the firewall. For further information regarding this option, please refer to the Technical Note “Stormshield Network Collaborative Security”.
Copy to the clipboard	Copies the selected line to the clipboard. Data can be copied in two different ways: 1. A single line is selected: in this case, this line as well as the lines of details will be copied. 2. Several lines are selected: in this case, only these lines will be copied to the clipboard.

Hosts

Many pop-up menus can be opened in this window:

- When right-clicking against a host,
- When right-clicking against the “Vulnerabilities” tab,
- When right-clicking against the “Applications” tab,
- When right-clicking against the “Information” tab,
- When right-clicking against the “Connections” tab,
- When right-clicking against the “Events” tab,

- When right-clicking against the help zone,
- When right-clicking against a DHCP lease.

Pop-up menu relating to a host

Filter by these criteria,	This option allows restricting the list of results to the selected field. For example, if the data is filtered by "Linux OS", the administrator will get all the lines containing the "Linux OS". **NOTE** Using this option will replace all the current filters on the columns
Filter only this column by this criterion,	This option allows restricting the list of results to the criteria under your cursor. **Example** If your cursor points to the destination / website consulted, the displayed list will only present the elements containing this destination / website.
Remove host from ASQ…	Enables deleting the host's ASQ information. This may be useful especially if a host has been hacked. The "Monitor modify" privilege is necessary. A message will appear, asking you to confirm this action.
Reset Vulnerability Manager information	Resets Vulnerability Manager data for the selected host. The "Monitor modify" privilege is necessary. A message will appear, asking you to confirm this action. When you perform this reset, the host will be deleted from the Vulnerability Manager database and as well as from data counters (detected vulnerabilities, software, etc).
Send to quarantine	The quarantined host will be dynamically blocked for a duration to be specified. (This duration can either be 1 minute, 5 minutes, 30 minutes or 3 hours). The "Monitor modify" privilege is necessary. You will not be asked to confirm this action.

Manually set the Operating System

This option allows specifying a host's operating system when Stormshield Network Vulnerability Manager is unable to detect it automatically. The window will then offer several fields:

Current operating system: The OS that Stormshield Network Vulnerability Manager uses for detecting vulnerabilities on a host. The OS of a host may not be detected sometimes.

Detected operating system: OS that Stormshield Network Vulnerability Manager detects after performing a traffic scan on a host. The Restore button allows removing the OS indicated by the user and reverting to the OS detected by Stormshield Network Vulnerability Manager.

New OS name: In the event the host's OS is not detected by Stormshield Network Vulnerability Manager, it is possible to impose it by selecting it from the suggested list. In this case, 2 situations may arise:

1. You are unable to specify the correct version (examples: *Android, Blackberry, etc*). In this case, the "Version" field will remain grayed out. Click on OK in order to force the OS to accept this value.
2. You are able to specify the version (example: Linux). In this case, the "Version" field will be modifiable and you will be able to enter a version number (example: 2.6). Next, click on Validate. If Stormshield Network Vulnerability Manager detects the version, a name will appear (*example, Linux 2.6.14*). To finish, click on OK in order to confirm your selection.

Imposing the host's OS when it has not been detected will allow, in particular, viewing the vulnerabilities of services and products according to the system.

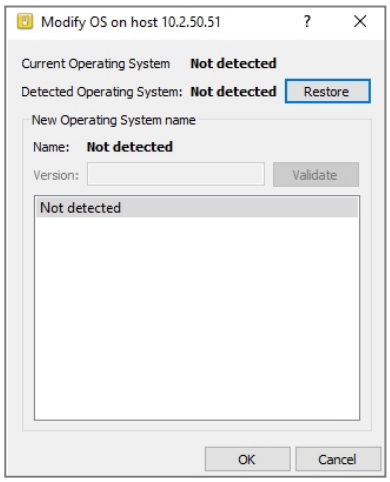


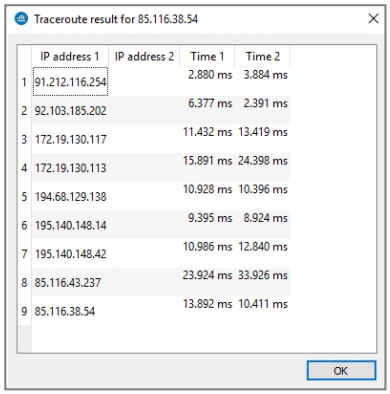
Figure 10: Manually set the Operating System

Add the host to the Object base,

This option allows:

- Creating an object corresponding to the selected IP address directly in the firewall's object base in Stormshield Network Real Time Monitor.
- Adding this object to an existing group on the firewall.

For further information regarding this option, please refer to the Technical Note *"Stormshield Network Collaborative Security"*.

Ping host	Allows `pinging` the host from the firewall and obtaining its response time as a result.
Traceroute to host	Two `Traceroute` commands are used to determine and test all appliances that traffic has to go through in order to reach the host from the firewall. The results are presented in the form of a table containing four columns:  • IP address no. 1: nominal IP address of hosts encountered. • IP address no. 2: alternative IP address of hosts encountered (appliances in load balancing, for example). • Time 1: response time of each appliance during the first `Traceroute`. • Time 2: response time of each appliance during the second `Traceroute`. **REMARK** When an appliance on the route does not respond to `Traceroute` requests, SN Real-Time Monitor will wait for the test packet to expire. The display time of the results window may then be longer.
Copy to the clipboard	Copies the selected line to the clipboard. Data can be copied in two different ways: 1. A single line is selected: in this case, this line as well as the lines of details will be copied. 2. Several lines are selected: in this case, only these lines will be copied to the clipboard.

Pop-up menu in the “Vulnerability” tab

Filter by these criteria,	This option allows restricting the list of results to the selected field. For example, if the data is filtered by "Critical" severity, the administrator will get all the lines containing "Critical" severity. **NOTE** Using this option will replace all the current filters on the columns

Filter only this column by this criterion,	This option allows restricting the list of results to the criteria under your cursor. **Example** If your cursor points to the destination / website consulted, the displayed list will only present the elements containing this destination / website.
View hosts with the same vulnerability	Allows displaying only hosts with a similar vulnerability.
Copy to the clipboard	Copies the selected line to the clipboard. . Data can be copied in two different ways: 1. A single line is selected: in this case, this line as well as the lines of details will be copied. 2. Several lines are selected: in this case, only these lines will be copied to the clipboard.

Pop-up menu in the “Applications” tab

Filter by these criteria,	This option allows restricting the list of results to the selected field. For example, if the data is filtered by "Unix", the administrator will get all the lines containing the "Unix" operating system. **NOTE** Using this option will replace all the current filters on the columns
Filter only this column by this criterion,	This option allows restricting the list of results to the criteria under your cursor. **Example** If your cursor points to the destination / website consulted, the displayed list will only present the elements containing this destination / website.
View all hosts that use this application	The Stormshield Network Vulnerability Manager menu appears with the name of the program concerned in pre-filtering.
View the vulnerabilities for this application	The “Vulnerabilities” tab is selected with the name of the program concerned in pre-filtering.
Impose a server application	The “Monitor modify” privilege is necessary. Only server programs can be modified.
Copy to the clipboard	Copies the selected line to the clipboard. . Data can be copied in two different ways: 1. A single line is selected: in this case, this line as well as the lines of details will be copied. 2. Several lines are selected: in this case, only these lines will be copied to the clipboard.

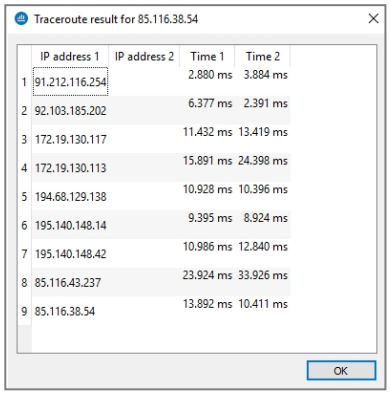
Pop-up menu in the “Information” tab

Filter by these criteria,	This option allows restricting the list of results to the selected field. For example, if the data is filtered by "Unix", the administrator will get all the lines containing the "Unix" operating system. **NOTE** Using this option will replace all the current filters on the columns
Filter only this column by this criterion,	This option allows restricting the list of results to the criteria under your cursor. **Example** If your cursor points to the destination / website consulted, the displayed list will only present the elements containing this destination / website.
View hosts with the same information	The Stormshield Network Vulnerability Manager menu appears with the name of the program concerned in pre-filtering.
Copy to the clipboard	Copies the selected line to the clipboard. . Data can be copied in two different ways: • A single line is selected: in this case, this line as well as the lines of details will be copied. • Several lines are selected: in this case, only these lines will be copied to the clipboard.

Pop-up menu in the “Connections” tab

Filter by these criteria,	This option allows restricting the list of results to the selected field. For example, if the data is filtered by "Unix", the administrator will get all the lines containing the "Unix" operating system. **NOTE** Using this option will replace all the current filters on the columns
Filter only this column by this criterion,	This option allows restricting the list of results to the criteria under your cursor. **Example** If your cursor points to the destination / website consulted, the displayed list will only present the elements containing this destination / website.
Ping source host	Allows pinging the source host from the firewall and obtaining its response time as a result.

Traceroute to source host	Two `Traceroute` commands are used to determine and test all appliances traffic has to go through in order to reach the source host from the firewall. The results are presented in the form of a table containing four columns:

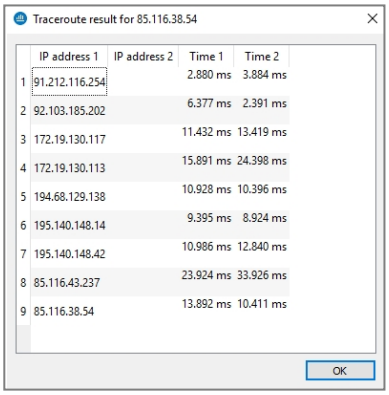


- IP address no. 1: nominal IP address of hosts encountered.
- IP address no. 2: alternative IP address of hosts encountered (appliances in load balancing, for example).
- Time 1: response time of each appliance during the first `Traceroute`.
- Time 2: response time of each appliance during the second `Traceroute`.

REMARK
When an appliance on the route does not respond to `Traceroute` requests, SN Real-Time Monitor will wait for the test packet to expire. The display time of the results window may then be longer.

Ping destination host	Allows pinging the destination host from the firewall and obtaining its response time as a result.
Traceroute to destination host,	Allows testing and listing (Traceroute) all appliances traffic has to go through in order to reach the destination host from the firewall. This action works in the same way as **Traceroute to source host.**
Send connection to quarantine	Allows quarantining the connection for a fixed period of 1 minute, 5 minutes, 30 minutes or 3 hours. This allows preventing certain downloads, for example.
Copy to the clipboard	Copies the selected line to the clipboard. . Data can be copied in two different ways: 1. A single line is selected: in this case, this line as well as the lines of details will be copied. 2. Several lines are selected: in this case, only these lines will be copied to the clipboard.

Pop-up menu in the “Events” tab

Filter by these criteria,	This option allows restricting the list of results to the selected field. For example, if the data is filtered by "Unix", the administrator will get all the lines containing the "Unix" operating system. **NOTE** Using this option will replace all the current filters on the columns
Filter only this column by this criterion,	This option allows restricting the list of results to the criteria under your cursor. **Example** If your cursor points to the destination / website consulted, the displayed list will only present the elements containing this destination / website.
View the packet that raised the alarm	This will open the tool that will allow you to view malicious packets.
Ping source host	Allows pinging the source host from the firewall and obtaining its response time as a result.
Traceroute to source host	Two `Traceroute` commands are used to determine and test all appliances traffic has to go through in order to reach the source host from the firewall. The results are presented in the form of a table containing four columns:  • IP address no. 1: nominal IP address of hosts encountered. • IP address no. 2: alternative IP address of hosts encountered (appliances in load balancing, for example). • Time 1: response time of each appliance during the first Traceroute. • Time 2: response time of each appliance during the second Traceroute. **REMARK** When an appliance on the route does not respond to `Traceroute` requests, SN Real-Time Monitor will wait for the test packet to expire. The display time of the results window may then be longer.

Ping destination host	Allows pinging the destination host from the firewall and obtaining its response time as a result.
Traceroute to destination host,	Allows testing and listing (Traceroute) all appliances traffic has to go through in order to reach the destination host from the firewall. This action works in the same way as **Traceroute to source host.**
Copy to the clipboard	Copies the selected line to the clipboard. . Data can be copied in two different ways: 1. A single line is selected: in this case, this line as well as the lines of details will be copied. 2. Several lines are selected: in this case, only these lines will be copied to the clipboard.

Pop-up menu relating to a DHCP lease

Filter by these criteria,	This option allows restricting the list of results to the selected field. For example, if the data is filtered by "Linux OS", the administrator will get all the lines containing the "Linux OS". **NOTE** Using this option will replace all the current filters on the columns
Filter only this column by this criterion,	This option allows restricting the list of results to the criteria under your cursor. **Example** If your cursor points to the destination / website consulted, the displayed list will only present the elements containing this destination / website.
Display host	Allows displaying details of the selected host.
Ping host	Allows pinging the host from the firewall and obtaining its response time as a result.
Traceroute to host	Allows testing and listing (Traceroute) all appliances traffic has to go through in order to reach the destination host from the firewall.
Copy to the clipboard	Copies the selected line to the clipboard. . Data can be copied in two different ways: 1. A single line is selected: in this case, this line as well as the lines of details will be copied. 2. Several lines are selected: in this case, only these lines will be copied to the clipboard.

Interfaces

Several pop-up menus can be opened in this window:

- When right-clicking against an interface,
- When right-clicking against the “Incoming connections” tab,
- When right-clicking against the “Outgoing connections” tab,

Pop-up menu relating to an interface

Filter by these criteria,	This option allows restricting the list of results to the selected field. For example, if the data is filtered by "Unix", the administrator will get all the lines containing the "Unix" operating system. **NOTE** Using this option will replace all the current filters on the columns
Filter only this column by this criterion,	This option allows restricting the list of results to the criteria under your cursor. **Example** If your cursor points to the destination / website consulted, the displayed list will only present the elements containing this destination / website.
Display hosts associated with this interface	This option allows displaying the list of hosts that have the same interface.

Pop-up menu in the “Incoming connections” tab

Filter by these criteria,	This option allows restricting the list of results to the selected field. For example, if the data is filtered by "Unix", the administrator will get all the lines containing the "Unix" operating system. **NOTE** Using this option will replace all the current filters on the columns
Filter only this column by this criterion,	This option allows restricting the list of results to the criteria under your cursor. **Example** If your cursor points to the destination / website consulted, the displayed list will only present the elements containing this destination / website.
View source host…	Indicates the name of the source host. If this option is selected, the **Hosts** menu will open.
View destination host…	Indicates the name of the destination host.
Send connection to quarantine	Allows quarantining the connection for a fixed period of 1 minute, 5 minutes, 30 minutes or 3 hours. This allows preventing certain downloads, for example.
Copy to the clipboard	Copies the selected line to the clipboard. . Data can be copied in two different ways: 1. A single line is selected: in this case, this line as well as the lines of details will be copied. 2. Several lines are selected: in this case, only these lines will be copied to the clipboard.

Pop-up menu in the "Outgoing connections" tab

Filter by these criteria,	This option allows restricting the list of results to the selected field. For example, if the data is filtered by "Unix", the administrator will get all the lines containing the "Unix" operating system. **NOTE** Using this option will replace all the current filters on the columns
Filter only this column by this criterion,	This option allows restricting the list of results to the criteria under your cursor. **Example** If your cursor points to the destination / website consulted, the displayed list will only present the elements containing this destination / website.
View source host…	Indicates the name of the source host. If this option is selected, the **Hosts** menu will open.
View destination host…	Indicates the name of the destination host.
Send connection to quarantine	Allows quarantining the connection for a fixed period of 1 minute, 5 minutes, 30 minutes or 3 hours. This allows preventing certain downloads, for example.
Copy to the clipboard	Copies the selected line to the clipboard. . Data can be copied in two different ways: 1. A single line is selected: in this case, this line as well as the lines of details will be copied. 2. Several lines are selected: in this case, only these lines will be copied to the clipboard.

Quality of Service

Refer to the section Quality of Service (QoS).

Users

2 pop-up menus can be opened in this window:

- When right-clicking against the "users" zone
- When right-clicking against an "administration sessions" zone

Pop-up menu in the "users" zone

Filter by these criteria,	This option allows restricting the list of results to the selected field. For example, if the data is filtered by a specific firewall address, the administrator will get all the lines containing this host. **NOTE** Using this option will replace all the current filters on the columns
Filter only this column by this criterion,	This option allows restricting the list of results to the criteria under your cursor. **Example** If your cursor points to the destination / website consulted, the displayed list will only present the elements containing this destination / website.

Remove user from ASQ	Enables deleting the user's ASQ information. This may be useful especially if a user has been affected by an attack. The "Monitor modify" privilege is necessary. A message will appear, asking you to confirm this action.
Copy to the clipboard	Copies the selected line to the clipboard. Data can be copied in two different ways: 1. A single line is selected: in this case, this line as well as the lines of details will be copied. 2. Several lines are selected: in this case, only these lines will be copied to the clipboard.

Pop-up menu in the "administration sessions" zone

Copy to the clipboard	Copies the selected line to the clipboard. Data can be copied in two different ways: 1. A single line is selected: in this case, this line as well as the lines of details will be copied. 2. Several lines are selected: in this case, only these lines will be copied to the clipboard.

Quarantine – ASQ Bypass

2 pop-up menus can be opened in this window:

- When right-clicking against the "Quarantine" zone
- When right-clicking against an "ASQ Bypass" zone

Pop-up menu in the "Quarantine" zone

Filter by these criteria,	This option allows restricting the list of results to the selected field. For example, when filtering by a particular firewall address, the administrator will obtain only all the relevant lines. **NOTE** Using this option will replace all the current filters on the columns
Filter only this column by this criterion,	This option allows restricting the list of results to the criteria under your cursor. **Example** If your cursor points to the destination / website consulted, the displayed list will only present the elements containing this destination / website.
Copy to the clipboard	Copies the selected line to the clipboard.

Pop-up menu in the "ASQ Bypass" zone

Filter by these criteria,	This option allows restricting the list of results to the selected field. For example, when filtering by a particular firewall address, the administrator will obtain only all the relevant lines. **NOTE** Using this option will replace all the current filters on the columns
Filter only this column by this criterion,	This option allows restricting the list of results to the criteria under your cursor. **Example** If your cursor points to the destination / website consulted, the displayed list will only present the elements containing this destination / website.
Copy to the clipboard	Copies the selected line to the clipboard.

VPN tunnels

This module now presents tunnels set up via IPSec VPN and SSL VPN under two separate tabs.

"SSL VPN Tunnels" tab

By right-clicking on a row of SSL VPN tunnels, you will access a pop-up menu that allows you to:

Filter by these criteria,	This option allows restricting the list of results to the selected field.
Filter only this column by this criterion,	This option allows restricting the list of results to the criteria under your cursor. **Example** If your cursor points to the user name, the displayed list will only present the elements containing this user.
View host	This option makes it possible to display all characteristics of the host corresponding to the IP addresses (vulnerabilities, applications, connections, etc) in the Host module of Stormshield Network Real Time Monitor.
Remove this tunnel	This option allows instantaneously shutting down the selected SSL VPN tunnel.

"IPSec VPN Tunnels" tab

Right-clicking against a line containing a VPN tunnel will bring you to the pop-up menu that will allow you to:

Filter by these criteria,	This option allows restricting the list of results to the selected field. For example, if the data is filtered by "mature" status, the administrator will get all the lines containing "mature" status.
Filter only this column by this criterion,	This option allows restricting the list of results to the criteria under your cursor. Example If your cursor points to a source address, the displayed list will only show the elements containing this source address.

View logs of outgoing SPIs	This option will allow displaying the SPIs of the negotiated outgoing SA.
View logs of incoming SPIs	This option will allow displaying the SPIs of the negotiated incoming SA.
View the outgoing policy	Hypertext link enabling the display of the outgoing policy visible in the VPN Policy menu.
View the incoming policy	Hypertext link enabling the display of the incoming policy visible in the VPN Policy menu.
Reset this tunnel	The selected tunnel will be deleted, but the configuration on the firewalls will still be active. The SAs matching the selected tunnel will be cleared; new SAs will have to be renegotiated so that the tunnel can be used again.
Reset all tunnels	All tunnels will be deleted.

Active Update

Right-clicking against a line in the Active Update section will bring you to the pop-up menu that will allow you to:

Copy to the clipboard	Data can be copied in two different ways: 1. A single line is selected: in this case, this line as well as the lines of details will be copied. 2. Several lines are selected: in this case, only these lines will be copied to the clipboard.

Services

Right-clicking against a line containing a service will bring you to the pop-up menu that will allow you to:

Filter by these criteria,	This option allows restricting the list of results to the selected field. For example, if the data is filtered by "Enabled" status, the administrator will get all the lines containing "Enabled" status. **NOTE** Using this option will replace all the current filters on the columns
Filter only this column by this criterion,	This option allows restricting the list of results to the criteria under your cursor. **Example** If your cursor points to the "Enabled" status, the displayed list will only show the elements containing this status.
Copy to the clipboard	Copies the selected line to the clipboard.

Hardware

This menu is dedicated to high availability. Refer to the Hardware section.

Filter policy

This menu allows you to view different types of rules:

- Implicit rules
- Global filter rules
- Local filter rules
- Local NAT rules

For more information, please refer to the Filter policy section.

VPN Policy

Right-clicking against a line containing a VPN policy will bring you to the pop-up menu that will allow you to:

Filter by these criteria,	This option allows restricting the list of results to the selected field. For example, if the data is filtered by "Firewall_bridge" as a destination router, the administrator will get all the lines containing the "Firewall_bridge" destination router.
Filter only this column by this criterion,	This option allows restricting the list of results to the criteria under your cursor.
View corresponding tunnels	Goes to the VPN tunnels menu with a filter.

Logs

VPN

Right-clicking against a line containing a VPN policy will bring you to the pop-up menu that will allow you to:

Filter by these criteria,	This option allows restricting the list of results to the selected field. For example, if the data is filtered by "Phase established" message, the administrator will get all the lines containing the "Phase established" message. **NOTE** Using this option will replace all the current filters on the columns
Filter only this column by this criterion,	This option allows restricting the list of results to the criteria under your cursor. **Example** If your cursor points to the destination / website consulted, the displayed list will only present the elements containing this destination / website.
Copy to the clipboard	Copies the selected line to the clipboard.

System

Right-clicking against a line in the System section will bring you to the pop-up menu that will allow you to:

Filter by these criteria,	This option allows restricting the list of results to the selected field. For example, if the data is filtered by the priority "Major", the administrator will get all the lines containing "Major". **NOTE** Using this option will replace all the current filters on the columns
Filter only this column by this criterion,	This option allows restricting the list of results to the criteria under your cursor.
Copy to the clipboard	Copies the selected line to the clipboard.

Status bar

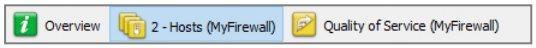


Figure 11: Status bar

The status bar contains menus from the tree that may have been opened during a session. Being able to do so is particularly useful when you are monitoring several firewalls at a time. You will be able to get back the same information window for each firewall and thus make simultaneous comparisons.

Button bar

Figure 12: Button bar

This bar appears in most menus in Monitor.

Refresh

This button allows you to reinitialize the list displayed (Alarms, Vulnerability Manager, Hosts, Interfaces, Quality of Service, Users, Quarantine, VPN Tunnels, Active Update, Services, Hardware, Filter Policy, VPN, Logs).

Show/Hide help

This button allows you to show or hide a help screen. Subsequently, you only need to click on the selected line to get help when necessary.

Access to private data

If this option is selected, the administrator who has logged on to Monitor will be able to obtain privileges to view private data shown in the current window (source IP addresses, host names, user names, etc.). Depending on the account used, a temporary access code provided by the firewall supervisor may be required before such data can be displayed.

When this option is not selected, private data will be replaced with the term *Anonymized*.

Firewall

This drop-down menu allows you to filter the list of alarms on a selected firewall.

Duplicate

The window can be duplicated using the button found in it. This comes in handy especially when you wish to change the target (firewall or <all>) and view.

3.4.6 Search zone

The search zone is presented in 2 different formats:

1st format: the bar shown below can be seen on all screens except for the “Events” screen.

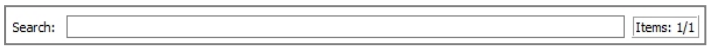


Figure 13: Search zone

2nd format: the bar below appears in the Events menu.

Figure 14: Search zone - Events

The **Filters** button contains the filters defined by the application and allows obtaining only the lines below:

- Alarm
- Virus
- Connection
- Web
- Mail
- FTP
- Filtering
- SSL
- SSL VPN
- Authentication
- Applications (alarm)
- Protection (alarm)
- Malware (alarm)

Search

In this zone, you will be able to conduct searches through items in the list. Items are filtered while search criteria are being entered.

3.5 Presentation of menus

3.5.1 File

The **File** menu concerns connections to the firewall and the application’s general options.

Address book…	Configures the firewalls’ address books.
Direct connection…	Opens a new firewall connection window. Enter the IP address of the firewall and the user's password.

Application settings…	Determines the behavior that Monitor should adopt at startup, enables getting a packet analyzer, defining a destination folder for reports, and the language used in the graphical interface.
Default monitoring settings…	Configures memory, connection timeout and the frequency with which different parameters will be refreshed.
Quit	Disconnects monitors and shuts down the application.

3.5.2 Windows

The **Windows** menu enables managing the display windows of the different connected firewalls:

Maximize	Opens the selected window.
Cascade	Arranges the various connection windows in cascade.
Title	Gives a global view of the main services offered by Monitor.
Duplicate current window	Duplicates the current window according to the firewall that you had selected earlier.
Overview	IP address of connected firewall(s).
Firewall address	The drop-down menu indicates the last windows visited and distinguishes the current window with a check.

3.5.3 Applications

The **Applications** menu enables connecting to other applications in the Stormshield Network Administration Suite. Using the two shortcuts provides the added advantage of not having to reauthenticate on both applications.

Run the configuration application	Allows accessing the selected firewall's web administration interface.

3.5.4 ? (Help)

Help	Opens a page that leads to your secure-access area, to allow you to obtain documentation.
About…	Provides information on the monitor in use (version number, credits).

3.6 Application settings

Certain parameters of the **Stormshield Network Real-Time Monitor** application can be configured.

- Select the **File\Application settings** menu : the window showing the parameters opens.

3.6.1 Behavior at startup

This tab offers the different options that enable configuring the application's behavior at startup.

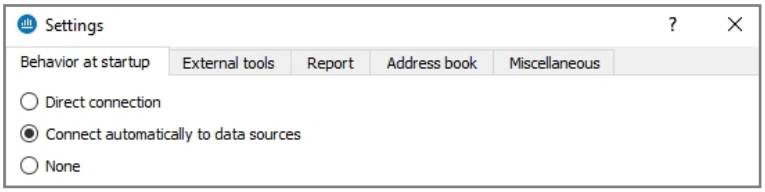


Figure 15: Behavior at startup

Direct connection	If this option is selected, the direct connection window will open when Monitor starts up. It will enable you to enter the IP address of the desired firewall and the user's password.
Connect automatically to data sources.	If this option is selected, the connection will be established automatically on different firewalls in the address book.
None	The **Overview** window will open but Monitor will not connect to any firewall.

3.6.2 External tools

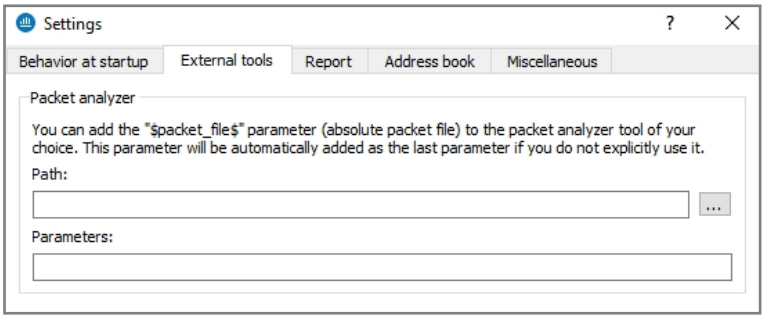


Figure 16: Settings – External tools

Packet analyzer	When an alarm is raised on a Stormshield Network Firewall, the packet that caused this alarm to be raised can be viewed. In order to do this, you need a packet viewing tool like **Ethereal** or **Packetyzer**. Specify the selected tool in the field "Packet analyzer", which the Monitor will use to display malicious packets.
Path	Indicates the location of the directory containing the application that allows analyzing packets.
Settings	The parameter "$packet_file$" can be added to the packet analyzer.

3.6.3 Report

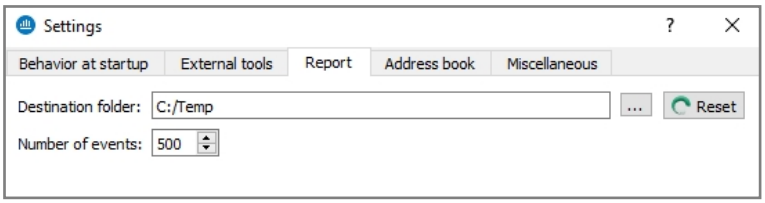


Figure 17: Settings – Report

Destination folder	Enables selecting the destination folder for the report. The **Reset** button allows you to reset the directory for storing reports.
Number of events	Allows defining the number of events desired when generating the report. By default, the value is set to 500 lines.

REMARK

The report can be generated by right-clicking on a line in the **Overview** menu and by selecting the option **Generate an instant web report...**

The report contains the following information:

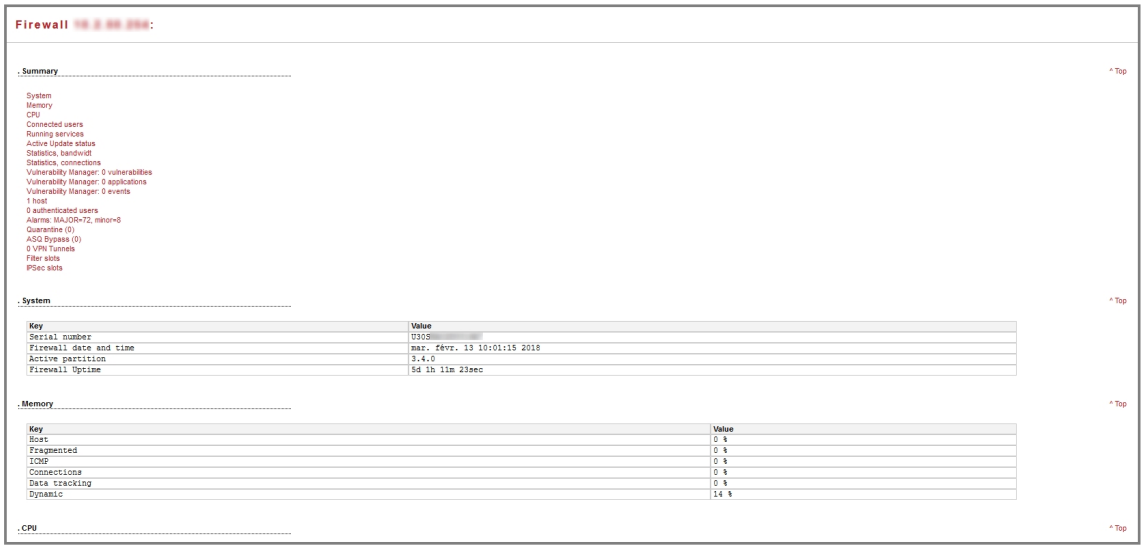


Figure 18: summary report

It displays information regarding the firewall for which you intended to generate a report. By clicking on a link in the list, the information will be displayed in table or graph form.

In the example below, information on memory is displayed.

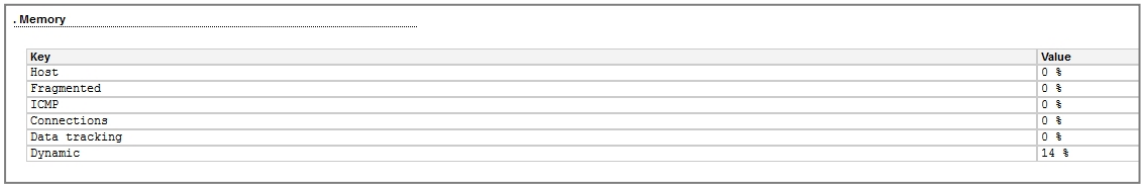


Figure 19: Memory information

3.6.4 Address book

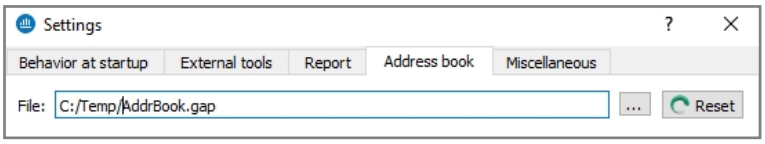


Figure 20: Settings – Address book

To retrieve a .gap file (Stormshield Network project file), simply click on **Browse**.

3.6.5 Miscellaneous

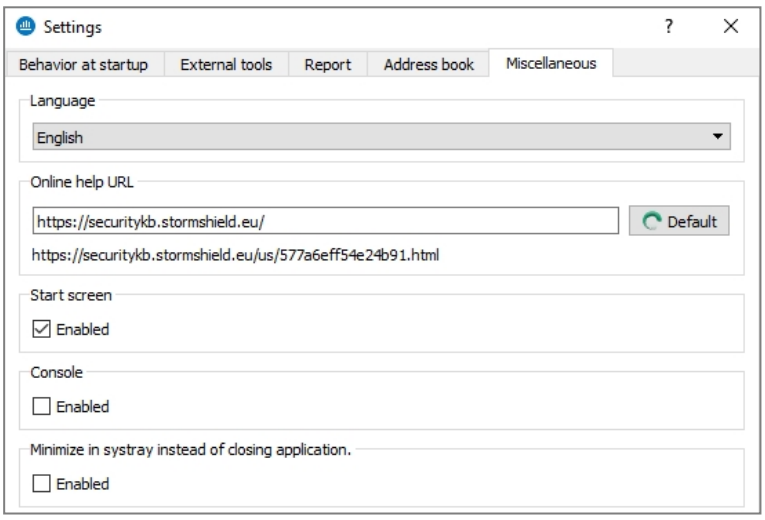


Figure 21: Settings – Miscellaneous

Language	You can select one of three languages for the interface's menus. English, French and Polish. Automatic selection will use the language of the version of Windows installed on the workstation. Whenever changes are made, the application must be restarted in order to apply the new language selected.
Online help URL	This option allows you to access the Stormshield Network knowledge base at any time.
Splash screen	If you select this option, the first window that appears on startup will contain the name, logo, version and loading status of the software. If it is not selected, the start screen will no longer be displayed.
Console	If the option **Enable** is selected, you will be able to access firewalls in console mode (CLI commands). When this window is validated, a **Console** menu will be added under the **Overview** menu directory.
Minimize in systray instead of closing application	If this option is selected, the application will be minimized in Systray instead of being shut down.

3.7 Default monitoring settings

This menu enables configuring when all information contained in Monitor will be refreshed. There are 6 parameters that regulate the frequency of data retrieval. You can define how long the different logs (in number of lines) and datagrams (in minutes) will be displayed.

➲ The default parameters for monitoring can be accessed from the menu **File\Default monitoring settings**.

3.7.1 Automatic

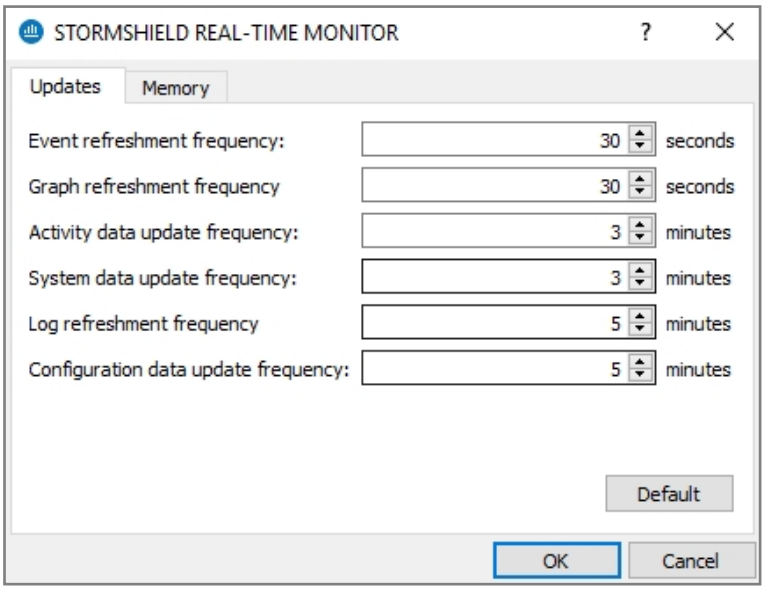


Figure 22: Monitor – Updates

Event refreshment frequency	Specifies in seconds when the list of detected events will be refreshed. The refreshment frequency is set to 30 seconds by default and may be a minimum of 1 second and a maximum of 3600 seconds.
Graph refreshment frequency	Specifies in seconds when graphs (Statistics, Interfaces, QoS and VPN SA) will be refreshed. The refreshment frequency is set to 30 seconds by default and may be a minimum of 10 seconds.
Activity data refreshment frequency	Specifies in minutes when activity data (hosts, authenticated users and Vulnerability Manager) will be refreshed. The refreshment frequency is set to 3 minutes by default and may be a minimum of 1 minute.
System data refreshment frequency	Specifies in minutes when system data (session data, high availability, RAID, cryptography card, quarantine, services and Active Update) will be refreshed. The refreshment frequency is set to 3 minutes by default and may be a minimum of 1 minute.
Log refreshment frequency	Specifies in minutes when log data will be refreshed. (Log space, filters, VPN, system, traffic and filter logs). The refreshment frequency is set to 5 minutes by default and may be a minimum of 1 minute.
Configuration data update frequency	Specifies in minutes when configuration data will be refreshed. (Antispam, antivirus, proxies, SPD and system properties). The refreshment frequency is set to 5 minutes by default and may be a minimum of 1 minute.

REMARK

The Default button allows you to reset the parameters to their default values.

3.7.2 Memory

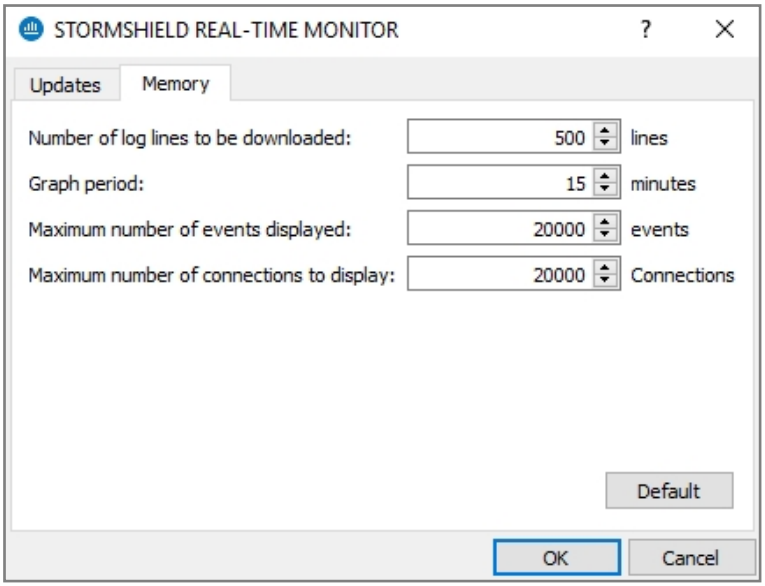


Figure 23: Monitor – Memory

Maximum number of the latest log lines to be downloaded	Configures the number of log lines you wish to display in the **Traffic** menu.
Graph period	Indicates how long graphs will be displayed (Statistics from the **Interfaces** menu).
Maximum number of events displayed	Configures the number of event lines that you wish to display in the **Events** menu. By default, the value is set to 20,000 events and may be a minimum of 1 events and a maximum of 2,000,000 events. The number of alarm lines indicated influences the memory used: The memory used for 150,000 event lines indicated for a firewall is about 220 MB. The memory used for 300,000 event lines indicated for a firewall is about 430 MB.
Maximum number of connections displayed	Configures the maximum number of connections that you wish to display in the **Hosts, Interfaces, Filter policy** and **Quality of Service** modules. If the value is zero, the function will be disabled. By default, the value is set to 20,000 events.

4. Information on firewalls

The information shown below will become available once the connection with the firewall is established.

4.1 Overview

4.1.1 Introduction

From the menu tree, the **Overview** menu allows you to display several types of information regarding your firewalls.

The **Overview** menu consists of five zones:

- The menu tree.
- A view providing information on vulnerabilities found on your network (corresponding to the **Vulnerability Manager** menu).
- A search and icon bar.
- A list of your firewalls.
- A view of connection logs.

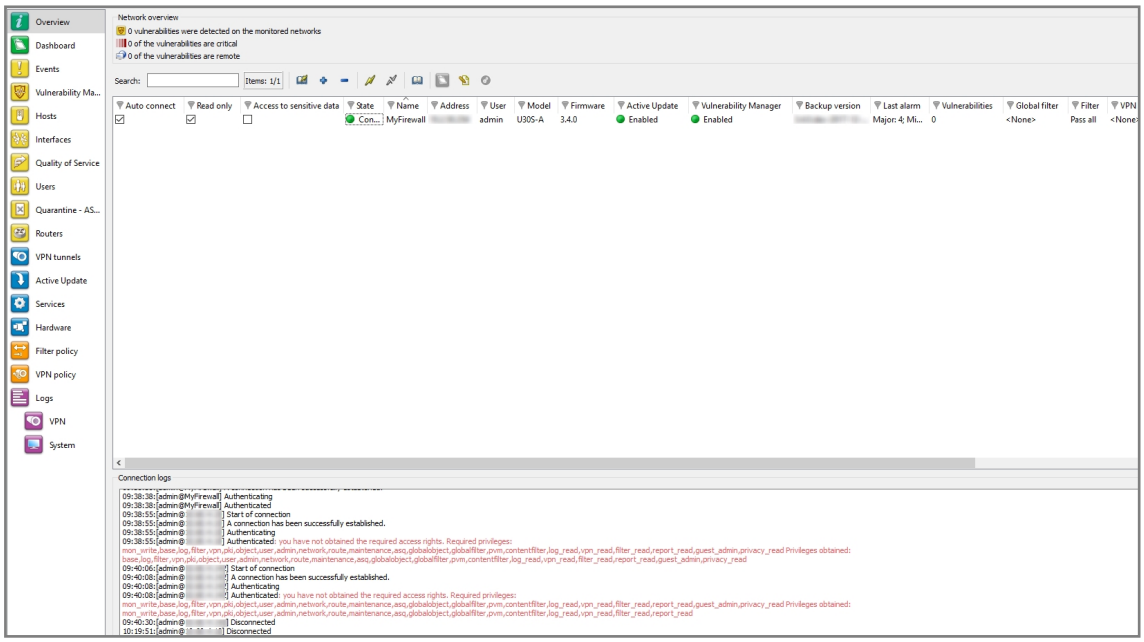


Figure 24: Overview

4.1.2 Overview of information on vulnerabilities

This view indicates the number of vulnerabilities found, the number of critical vulnerabilities and the number of vulnerabilities that are remotely accessible on your networks. These indications represent links that allowing access to these vulnerabilities (**Vulnerability Manager** menu).

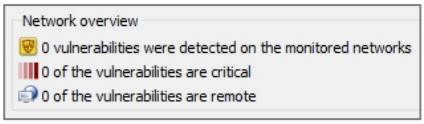


Figure 25: Network overview

4.1.3 List of firewalls

This view provides the following information on your product(s):

Auto connect.	Selecting this option allows you to activate automatic reconnection of **Stormshield Network Real-Time Monitor** in the event of a disconnection.
Read only	Select this option to activate read-only mode.
Access to private data	If this option is selected, the administrator who has logged on to Monitor will be able to display private data (source IP addresses, host names, user names, etc.) in all menus. Depending on the level of his permissions, he may be asked to enter a temporary access code in order to access private data. This code is provided by the firewall supervisor. When this option is not selected, such data will be replaced with the term *Anonymized*.
State	Indicates the product's connection status. Options: **Connected/Disconnected**.
Name	Product's name or IP address if the name has not been indicated.
Address	Firewall's IP address.
User	ID of the user connected to the firewall via **Stormshield Network Real-Time Monitor**.
Model	Product model: SN300, SN6000, etc
Firmware	Software version of the listed firewall.
Active Update	Indicates the update status of the Active Update module. **OK** or **x failure (s)**.
Vulnerability management	Indicates the status of the Vulnerability Manager service.
Antivirus	Indicates the status of the antivirus. The options are: **OK/Disabled**.
Backup version	Version number of the backup module or of the firmware on the passive partition.
Last alarms	Indicates the number of major and minor alarms for the latest alarms (over the past 15 minutes). The maximum value is 100 even if the number of alarms exceeds this value.
Vulnerabilities	Indicates the number of vulnerabilities.
Global filtering	Indicates whether a global filter rule has been activated. If so, "Global policy" will be indicated.
Filtering	Indicates the name of the active filter slot.
VPN	Indicates the name of the active VPN slot.
URL	Indicates the name of the active URL slot.

NAT	Indicates the name of the active NAT slot.
Uptime	Amount of time that the firewall has been running since the last startup.
Session	Indicates the number of sessions opened on the firewall.
Comments	Comments or descriptions of the firewall.

4.1.4 Connection logs

This window indicates logs of connections between Stormshield Network Real-Time Monitor and the firewall.

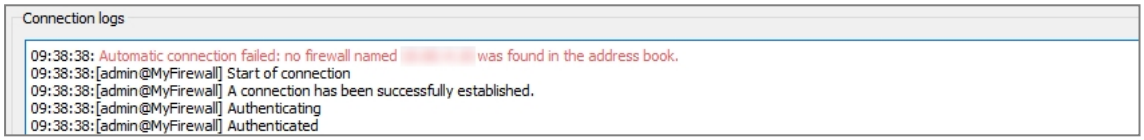


Figure 26: Connection logs

TIP
You can erase logs by right-clicking on the "Connection logs" view

4.2 Dashboard

4.2.1 Introduction

The **Dashboard** menu allows displaying on a single screen all the useful information concerning real-time monitoring.

It basically picks out useful information from some of the menus in the **Stormshield Network Real-Time Monitor** tree and adds on other additional information. The data displayed in this window are:

- System information
- Memory
- Temperature
- CPU
- Hardware
- Active network policies
- Alarms
- Vulnerabilities
- VPN tunnels
- Active Update
- Logs
- Services
- HTTP Cache
- Interfaces.
- Top 5 interfaces for incoming throughput
- Top 5 interfaces for outgoing throughput

- Top 5 hosts for incoming throughput
- Top 5 hosts for outgoing throughput

Checkboxes allow showing or hiding details of each category of information. The status of each checkbox (enabled/disabled) is remembered in order to display the dashboard with the same layout the next time **SN Real-Time Monitor** is started.

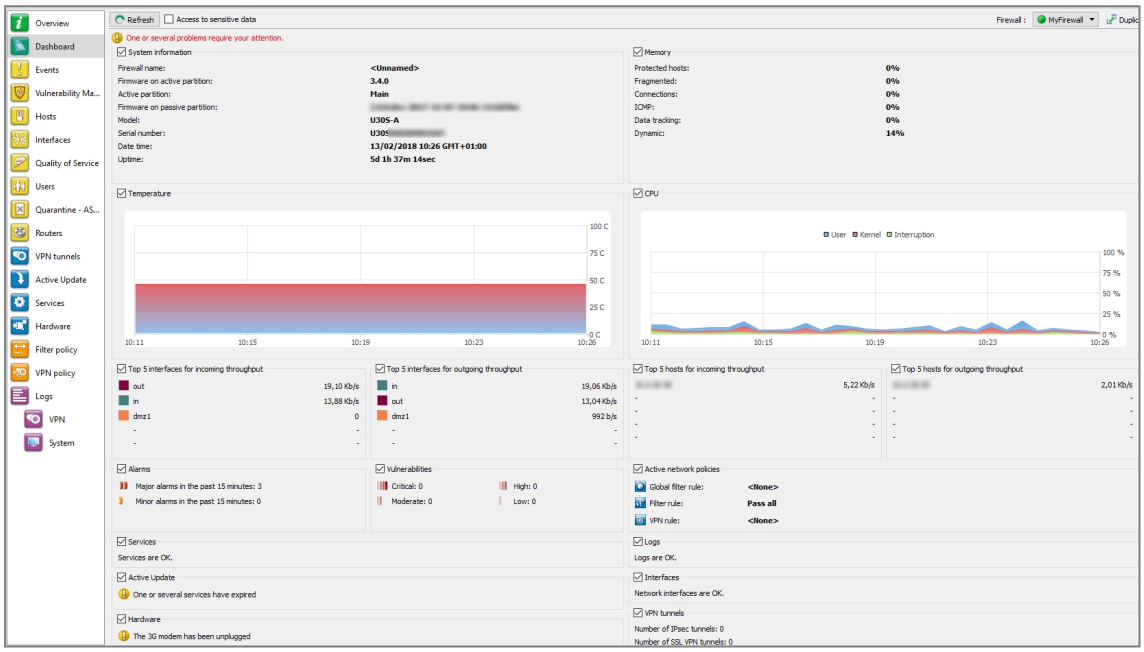


Figure 27: Dashboard

4.2.2 Selecting a product

When clicking in the **Dashboard** menu, a product selection window may appear if the Stormshield Network Real-Time Monitor is connected to several firewalls.

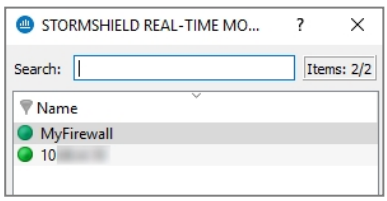


Figure 28: Selecting a firewall

1. If the list of firewalls is long, look for the desired firewall using the Search field.
2. Select the firewall.
3. Click on OK. The Dashboard of the desired firewall will appear.

4.2.3 System information

Firewall name	Name given to the product when it was registered in the address book.

Firmware on active partition	Version of the active partition's firmware.
Active Partition	Partition on which the firewall was booted.
Firmware on passive partition	Version of the passive partition's firmware.
Model	Firewall's model number.
Serial number	Firewall's serial number.
Date-time	Current date and time.
Uptime	Amount of time that the firewall has been running since the last startup.

4.2.4 Memory

This refers to the use (in percentage) of memory reserved for storing information (buffer). The buffer is linked to the *stateful* module and corresponds to the context being saved.

Protected host	Protected host stack
Fragmented	Fragmented packets
Connections	All TCP/IP connections.
ICMP	ICMP requests (ping, trace route, etc.).
Data tracking	Memory used for monitoring connections.
Dynamic	Percentage of ASQ memory being used.

Buffer sizes vary according to product type and product version.

Cleaning algorithms optimize the operation of "Hosts", "Fragmented", "ICMP" and "Connections" buffers. Entries in the "Fragmented" and "ICMP" buffers are initialized at fixed intervals (each entry has a limited lifetime: TTL).

This illustrates part of the firewall's activity. A high percentage may mean the firewall is overloaded or that an attack has been launched.

4.2.5 CPU

DEFINITION
Better known as a "processor", this is the internal firewall resource that performs the necessary calculations.

User:	CPU time allocated to the management of user processes.
Kernel:	CPU time that the kernel consumes
Interruption:	CPU time allocated for interruptions.

4.2.6 Temperature

This graph displays the temperature of the appliance in degrees Celsius (°C). This information is not available on virtual machines. For multi-core processors, the value displayed is the average of all the CPUs.

4.2.7 Hardware

DEFINITION OF "HIGH AVAILABILITY"

A specific architecture in which a backup firewall takes over when the "main" firewall breaks down while in use. This switch takes place seamlessly.

If high availability has been activated, an additional section will provide you with the information regarding high availability (status of firewalls, licenses, synchronization).

Click on the descriptive phrase in the "Hardware" zone in order to display the **Hardware** menu and to obtain information on high availability and the status of the firewall's components (S.M.A.R.T. peripherals, RAID volumes where possible, disks and power supply units).

If the backup firewall is not available, information on the active firewall can be viewed.

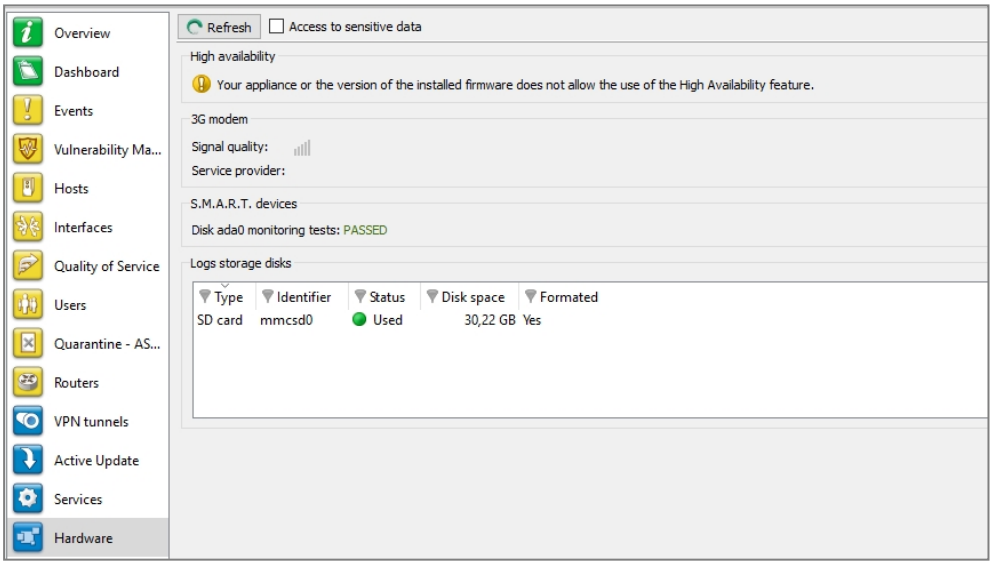


Figure 29: Hardware

4.2.8 Active network policies

This view indicates whether slots are active. If so, the name of the activated rule is indicated. The rules mentioned here are:

Global filter rules	Name of the activated global filter policy.
Filter rule	Name of the activated filter policy.
VPN rule	Name of the activated VPN rule.
Translation rule	Name of the activated translation policy.
URL filter rule	Name of the activated URL filter rule.

REMARK
<None> means that no policy has been activated for the rule that contains this indication.

4.2.9 Alarms

This view indicates the number of major and minor alarms during the past 15 minutes that the product has been connected. The maximum value indicated is 100 even if the number of alarms exceeds this value.

To view the alarms, click on either link of your choice – the **Events** menu will appear and will set out the list of alarms according to the selected criticality.

4.2.10 Vulnerabilities

This view indicates the number of vulnerabilities for a specific level. The 4 levels of vulnerability are: Critical, High, Moderate and Low.

To view a list of vulnerabilities, click on one of the levels, and the menu **Vulnerability management** will appear (*Cf.* section *Vulnerability Manager*).

4.2.11 VPN tunnels

This view indicates the number of configured VPN tunnels. To view a list of configured VPN tunnels, click on the link – the **VPN Tunnels** menu will appear.

4.2.12 Active Update

This view indicates the status of updates that have been performed (success or failure) as well as the last time the "Active Update" module had been launched (date and time). To view a list of updates and their status, click on the link – the **Active Update** menu will appear.

4.2.13 Logs

This window indicates whether there are problems with the logs. To view a graph that represents the current size of the log file in real time (Alarms, Authentication, Connections, Filters, Monitor, Plugins, POP3, Vulnerability Manager, Administration, SMTP, System, IPSec VPN, Web, SSL VPN) in relation to the space allocated to each log type on the firewall, click on the link. The **Logs** menu will appear.

4.2.14 Services

This zone indicates whether there are problems with the services. To view a list of services and their status (**Enabled/Disabled**), click on the link – the **Services** menu will appear.

4.2.15 Cache proxy

These 3 pie charts represent the use of the HTTP cache when it has been enabled in the filter rules:

- The first graph compares the number of cached requests and the number of requests that were not saved in memory.

- The second graph compares the amount of cached data and the amount of data not saved in memory.
- The third graph represents the distribution of cached data on the hard disk, data cached in RAM and data not saved in memory.

4.2.16 Interfaces

This zone indicates whether there are problems with the interfaces. To view information on bandwidth, connections and throughput, click on the link. The **Interfaces** menu will appear.

4.2.17 Top 5 interfaces for incoming throughput

This zone displays the list of the 5 interfaces that have registered the most incoming throughput. Click on any one of the interfaces to display the *Throughput* tab graph in the **Interfaces** menu.

4.2.18 Top 5 interfaces for outgoing throughput

This zone displays the list of the 5 interfaces that have registered the most outgoing throughput. Click on any one of the interfaces to display the *Throughput* tab graph in the **Interfaces** menu.

4.2.19 Top 5 hosts for incoming throughput

This zone displays the list of the 5 hosts that have registered the most incoming throughput. Click on any one of the interfaces to display the *Throughput* tab graph in the **Interfaces** menu.

4.2.20 Top 5 hosts for outgoing throughput

This zone displays the list of the 5 hosts that have registered the most outgoing throughput. Click on any one of the interfaces to display the *Throughput* tab graph in the **Interfaces** menu.

4.2.21 Stormshield Management Center

When the firewall is managed from Stormshield Management Center, this view will show several indicators relating to the connection to the SMC server and the version of the configuration currently deployed on the appliance:

Status of the connection	Indicates whether the connection between the firewall and the Synapse server has been established (Connected / Disconnected).
IP address	IP address of the Synapse server
Logged on/ Logged off since	Specifies the time/date from which the firewall has been logged on to or logged off from the Synapse server.
Deployment version	Indicates the number of the last configuration deployment carried out by the Synapse server on the firewall.
Last configuration update	Indicates the last date on which the configuration was sent by the Synapse server to the firewall.

5. Real-Time Information

Real-time information is given regarding:

- Events
- SN Vulnerability Manager
- Hosts monitored
- Interfaces
- QoS
- Users
- Quarantine
- Routers

5.1 Events

The alarms generated by the firewall will appear in this window.

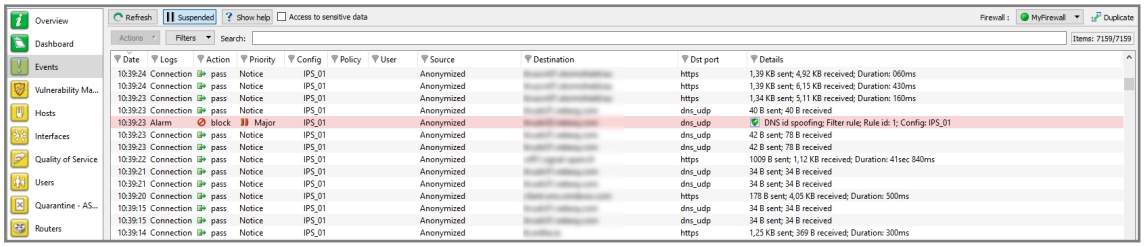


Figure 30: Events

In this module, the additional **Activated/Suspended** button allows switching the status of alarm refreshment. If this button is in a suspended status, the automatic refreshment will be disabled, making it easier to read logs.

When the **Events** menu in the tree on the left is selected, the data displayed by default are:

Date	Date and time the line was recorded in the log file at the firewall's local time.
Logs	Indicates the type of log. The possible types of logs are: Alarm, Plugin, Connection, Web, SMTP, FTP, POP3, Filter).
Action	Action associated with the filter rule and applied to the packet (**Examples**: Block/Pass, etc.)

Priority	Determines the alarm level. The possible values are: • 0: emergency • 1: alert • 2: critical • 3: error • 4: warning • 5: notice • 6: information • 7: debug
Config	Name of the application inspection profile that reported the event.
Policy	Name of the SMTP, URL or SSL filter policy that raised the alarm
User	Identifier for the authenticated user (ftp), e-mail address of the sender (SMTP), identifier for the user if authentication has been enabled (WEB).
Source (src/srcname)	IP address or name of the object corresponding to the source host of the packet that set off the alarm.
Src. port (num)	Source port number involved, displayed in digits.
Destination (dst/dstname)	IP address or name of the object corresponding to the destination host of the packet that set off the alarm.
Destination Port (dst port/dstportname)	Destination port number of the service or name of the object corresponding to the service port of the destination host if it exists and is requested for this connection.
Details	Describes the event relating to the log. This column groups some of the information gathered from the other columns. **Example** If an alarm log is concerned, information such as whether it was a sensitive alarm, the number of the filter rule, rule ID (already given in the columns "Sensitive alarm", "Rule" and "Rule ID") will be grouped in this column. This column displays the icon that specifies the type of detection according to the categories **Applications, Malware** and **Protections**.

Other available data includes:

Firewall (fw)	Serial number or name of the firewall (if known) that caused the event.
UTC Date (time+tz)	UTC date (replaces the GMT)
Start date (starttime)	“Local” date at the start of an event.
UTC start date (startime+tz)	UTC date at the start of an event (a connection).
Time zone (tz)	Firewall’s time zone.
Rule (ruleid)	Number of the filter rule involved in the raised alarm.

Protocol (proto)	Protocol of the packet that set off the alarm.
Connection group (groupid)	Identifier that would allow tracking child connections.
Source interface (srcif/srcifname)	Name of the firewall interface on which the event was raised (source interface network card).
Source address (src)	IP address of the source host of the packet that set off the event.
Source port (srcport/srcportname)	Source port number of the service or the name of the object corresponding to the service port of the source host (only if TCP/UDP).
Destination interface (dstif/dstifname)	Network card of the destination interface.
Destination address (dst)	IP address of the destination host of the packet that set off the event.
Authentication	Authentication method used.
Sensitive alarm (sensitive)	Indicates whether an alarm is sensitive. This alarm is raised whenever the intrusion prevention system detects a sensitive packet and for which it has been configured in intrusion detection mode. If the alarm is sensitive, an icon in the form of an exclamation mark followed by "Yes" will appear. Otherwise, "No" will be indicated. When the alarm is blocked, the icon will be grayed out (it is disabled). **NOTE** Only protocol alarms can be described as "sensitive". For alarms that are not in this class, the column will be empty.
Copy (repeat)	Indicates the number of an event's occurrences within a defined period.
Identifier (Id/alarmid)	Indicates the number of the alarm.
Context (class)	Text indicating the category to which the alarm belongs (system, protocol, filter, etc).
Alarm type (classification)	Code (number) indicating the alarm category. This column also displays the type of detection according to the categories **Applications, Malware** and **Protections**.
Caller	VoIP: Indicates the caller
Callee	VoIP: Indicates the callee
Duration	Connection time in seconds.
Sent	Number of KB sent during the connection.
Received (rcvd)	Number of KB received during the connection.
Operation (op)	Identified command of the protocol. • FTP: PUT, MPUT, GET, DELETE,… • HTTP: GET, PUT, POST,… • EDONKEY: SENDPART • POP3: RETR, LIST,… • FTP: DELETE, LIST,…

Result	Result of the operation in the protocol (example: 404 which indicates an error).
Parameter (arg)	Operation parameter.
Category (cat_site)	Web category of the requested website.
Spam level (spamlevel)	Spam level : 0 (Message not spam) 1,2 and 3 (spam) x (error while processing the message) and ? (the nature of the message could not be determined) if antispam has been enabled.
Virus (virus)	Indicates whether there is a virus (if the antivirus has been enabled).
IP (ipproto)	Internet protocol (tcp or udp).
Media	Type of traffic detected (audio, video, application,...)
Message (Msg)	Detailed description of the alarm. All commands sent by the client are found here. Sensitive information such as passwords is removed.
ICMP code (icmpcode)	ICMP code in the alarm logs.
ICMP type (icmptype)	ICMP type in the alarm logs.
Packet	Indicates the IP packet for which the alarm was raised. Right-clicking on this packet allows it to be viewed through a packet analyzer. The information displayed in this column shows the size of the IPv4 packets (value beginning with 45). The size of captured packets is 1536 bytes. **WARNING** To view a packet, a software program needs to be installed on your workstation.
Sandboxing	Indicates the result of sandboxing a file exchanged during the listed connection. The value of this result may be one of the following: Clean, Suspicious, Malicious, Unknown, Forwarded or Failure.
Hash	Hash applied to the analyzed file and allowing it to be identified in various log files.
Sandboxing criticality	This indicator will only be displayed when a file scanned by sandboxing has been deemed malicious. It will then be presented in the form of a score ranging from the detection threshold of a malicious file (set by default to 80) to 100.
Source IP reputation	Reputation category of the public IP address at the source of the traffic. This column will only contain data if this IP address is public and listed in the IP address reputation database. The possible values are: "anonymizer", "botnet", "malware", "phishing", "tor", "scanner" or "spam".
Source host reputation	Reputation score of the host at the source of the traffic. This column will only contain data when host reputation management has been enabled and the selected host is a monitored host.
Destination IP address reputation	Reputation category of the public IP address at the destination of the traffic. This column will only contain data if this IP address is public and listed in the IP address reputation database. The possible values are: "anonymizer", "botnet", "malware", "phishing", "tor", "scanner" or "spam".

Destination host reputation	Reputation score of the host at the destination of the traffic. This column will only contain data when host reputation management has been enabled and the selected host is a monitored host.

NOTE
The logs will now be displayed for models without hard drives.

The **Actions** button makes it possible to perform certain actions on the selected event (for further information, please refer to the section Pop-up menu on rows):

- View source host,
- View destination host,
- Add the source host to the Object base,
- Add the destination host to the Object base,
- Ping source host,
- Traceroute to source host,
- Ping destination host,
- Traceroute to destination host,
- Send source to quarantine,
- View packet,
- Flush alarms.

5.2 SN Vulnerability Manager (SNVM)

5.2.1 Introduction

Stormshield Network Vulnerability Manager is a module that allows network administrators to gather information in real time and to analyze it in order to spot possible vulnerabilities that may compromise the security of their networks. Among other things, it also allows raising alarms generated by the intrusion prevention engine and thus to maintain an optimal security policy.

Stormshield Network Vulnerability Manager collects and archives in particular, information relating to the operating system, to various active services as well as to the different applications that have been installed. As a result, descriptive profiles can be made of network elements.

Stormshield Network Vulnerability Manager aims to:

- Configure your company network's security policy.
- Analyze the status of the risk.
- Optimize the level of security.
- Report security events.

The procedure is as follows:

1 Stormshield Network's intrusion prevention engine (ASQ) extracts data in real time using network protocols that it knows.

2 Vulnerability Manager then combines and weights these data.

3 The vulnerability found can then be fixed using databases that have been indexed dynamically. Once all this information has been collected, they will be used in Monitor so that flaws on the network can be corrected, or prohibited software can be detected, or the real risk relating to the attack can be identified in real time.

4 The profile is therefore complete.

5 One or several solutions can thus be considered.

Example

A company has a public website that it updates twice a month via FTP. At a specific date and time, a vulnerability that affects FTP servers is raised and Monitor immediately takes it into account, enabling the network administrator to detect it at practically the same time.

This vulnerability is represented by a line that indicates the number of affected hosts and whether a solution is available.

By deploying this line, details of the hosts concerned will appear, as well as the service that has been affected by the vulnerability. Help, in the form of links, may be suggested to correct the detected flaw.

Once the network administrator becomes aware of the vulnerability, he can correct it at any moment, quarantine the affected host(s) and generate a report.

When you click on the **Vulnerability Manager** menu in the menu directory, the scan window will consist of the following:

- A *Vulnerabilities* tab.
- An *Applications* tab.
- An *Information* tab.

5.2.2 "Vulnerabilities" tab

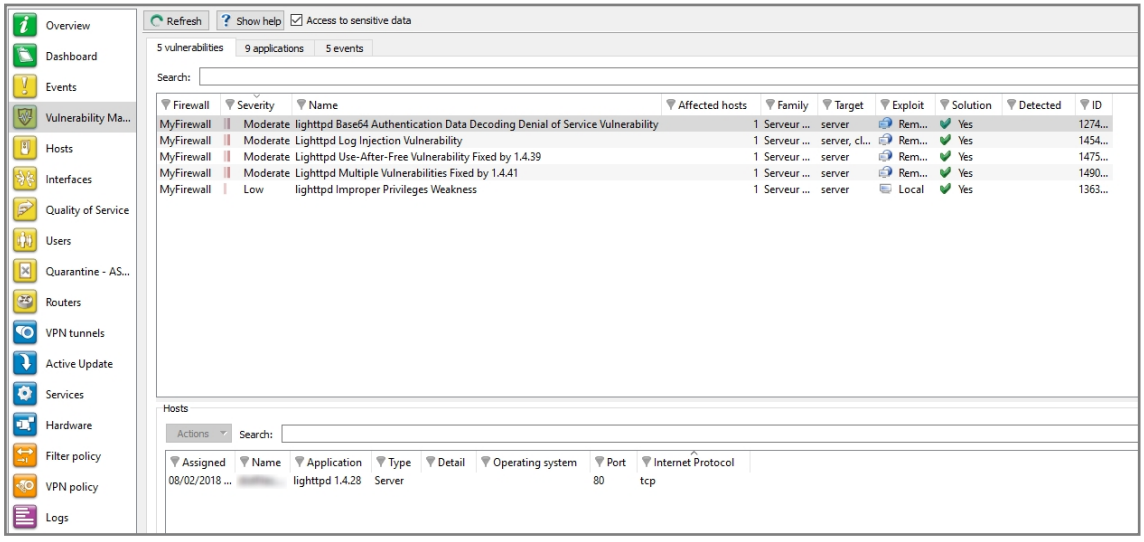


Figure 31: Vulnerability Manager

This screen consists of 3 views:

- A view of the list of vulnerabilities.
- A view of the list of hosts affected by this vulnerability.
- A hidden help view that you can display by clicking on "Show help" (top left of the screen). This allows working around the selected vulnerability, if a solution exists.

"Vulnerability(ies)" view

This view allows you to view all the vulnerabilities that the firewall has detected. Each line represents a vulnerability.

REMARK

The number of vulnerabilities is displayed in the tab's label.

The information provided in the "vulnerability" view is as follows:

Firewall	Serial number or name (if known) of the firewall at the source of the vulnerability.
Severity	Indicates the level of severity on the host(s) affected by the vulnerability. There are 4 levels of severity: Low, Moderate, High, Critical.
Name	Indicates the name of the vulnerability.
Affected hosts	Number of hosts affected by the vulnerability.
Family	Family to which the vulnerability belongs.
Target	One of 2 targets: **Client** or **Server**.
Exploit	Access may be local or remote (via the network). It allows exploiting the vulnerability.
Workaround	Indicates whether a workaround exists.
Discovered on	Date on which the vulnerability was detected. **WARNING** This refers to the date on which the vulnerability was discovered and not the date on which it appeared on the network.
ID	Allows a unique identification of the vulnerability.

"Hosts" view

This view allows you to view all the vulnerabilities for a given host. Every row represents a host.

The "Hosts" view displays the following data:

Assigned	Date on which the host was assigned.
Name	Name of the host affected by the attack (if it exists).
Address	IP address of the host affected by the attack.
Application	Name and version of the application (if available).
Type	Application type (Client/Server/Operating system).

Details	Name of the service prone to being affected by the vulnerability.
Operating system	Vulnerable host's operating system.
Port	Number of the port on which the vulnerability had been detected.
Internet Protocol	Name of the protocol used.

The **Actions** button makes it possible to perform certain actions on the selected event (for further information, please refer to the section Pop-up menu on rows):

- View host,
- Add the host to the Object base,

Help zone

The help zone allows you to get more details relating to the attack. Thus the administrator can correct the vulnerability.

Click on the **Show help** button to show or hide the help zone associated with a vulnerability.

Typically, help comes in the form of a descriptive file that contains explanations, links to the publisher's site or to bug fixes.

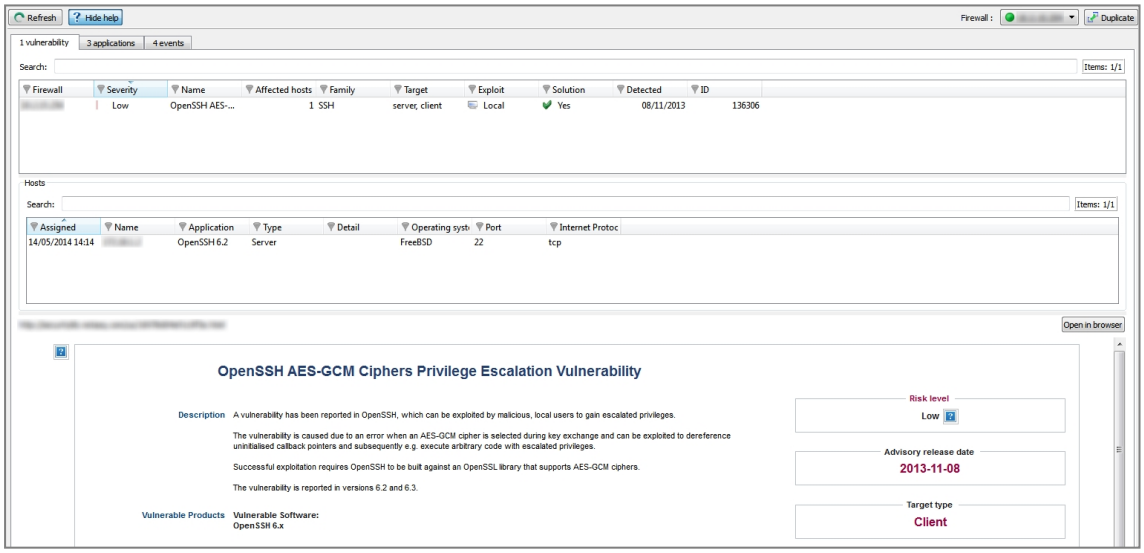


Figure 32: Help

5.2.3 "Applications" tab

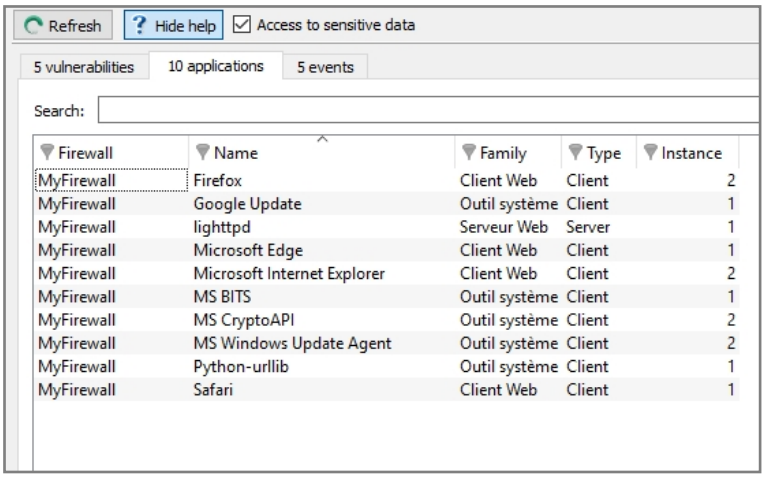


Figure 33: Vulnerability Manager - Applications

The *Applications* tab provides information on the application detected within the enterprise.

Two types of application may be detected:

- **Products**: these are client applications installed on the host (e.g.: Firefox).
- **Services**: these are server applications that are attached to a port (e.g.: lighttpd).

Using information detected by the ASQ engine, Stormshield Network Vulnerability Manager generates information about the detected applications. The design of this feature allows grouping applications by family, so by pairing such information with the vulnerability database, Stormshield Network Vulnerability Manager also suggests probable security loopholes linked to these applications.

This tab offers features that include filtering, optional column display, resizing to fit contents and copying of data to the clipboard. It displays information on the detected applications through the columns that can be seen in the window below:

This screen consists of 2 views:

- A view that lists the applications.
- A detailed view that lists the hosts.

"Application(s)" view

This view allows you to see the applications that the firewall detects. Each line represents an application.

REMARK

The number of applications is displayed in the tab's name.

The *Applications* tab displays the following data:

Firewall	Serial number or name (if known) of the firewall.

Name	Name of the software application. The version is not specified except for the operating systems.
Family	The software application's family (e.g.: "web client").
Type	Software type (Client: the software does not provide any service – Server: the software application provides a service – Operating system).
Instance	Number of software applications detected in the monitored networks. For a server, the same service may be suggested on several ports. E.g.: an Apache http server which provides its services on port 80 and port 8080 (web proxy) would appear twice.

"Hosts" view

This view allows you to see all the applications for a given host. Every row represents a host.

The "Hosts" view displays the following data:

Name	Host name.
IP address	IP address of the host.
Application	Name of the software as well as its version, if available.
Type	Software type (Client: the software does not provide any service – Server: the software application provides a service – Operating system).
Operating system	Host's operating system.
Port	Port that the software application uses (if it uses any).
Protocol	Internet protocol of the software (if it uses any).

The **Actions** button makes it possible to perform certain actions on the selected event (for further information, please refer to the section Pop-up menu on rows):

- View host,
- Add the host to the Object base,

5.2.4 "Events" tab

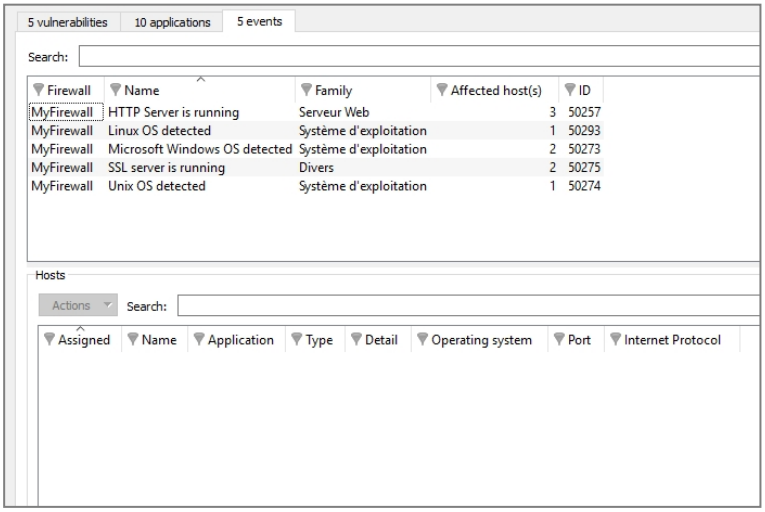


Figure 34: Vulnerability Manager - Events

The *Information* tab informs you of your network's activity. You can therefore see the programs that are at risk of generating attacks.

This screen consists of 3 views:

- List of programs.
- List of hosts.
- Help zone.

"Events" view

This view allows you to see all the events that the firewall detects. Each line represents an event.

REMARK
The number of events is displayed in the tab's name.

The "Information" view displays the following data:

Firewall	Serial number or name (if known) of the firewall.
Name	Name of the detected OS or a server (e.g.: SSH server).
Family	Host family. **Example** SSH
Affected hosts	Number of hosts affected. These hosts are identified in the Hosts view in this tab. **REMARK** The number of hosts indicated in the column "Affected hosts" is not always the same as the number of elements indicated in the "Hosts" zone in this window. In fact, the same service may use several ports. For example, the service thhtpd_server 2.25b can listen to 2 different ports, thus increasing the number of elements.
ID	Identifier.

"Hosts" view

This view allows you to see all the events for a given host. Every row represents a host.

The "Hosts" view displays the following data:

Assigned	Date and time of the event's occurrence.
Name	Host name.

Address	IP address of the host.
Application	Name of the software as well as its version, if available.
Type	Software type (Client: the software does not provide any service – Server: the software application provides a service – Operating system).
Details	Details about the operating system.
Operating system	Host's operating system.
Port	Port that the software application uses (if it uses any).
Internet Protocol	Internet protocol of the software (if it uses any).

The **Actions** button makes it possible to perform certain actions on the selected event (for further information, please refer to the section Pop-up menu on rows):

- View host,
- Add the host to the Object base,

Help zone

The help zone allows you to get more details relating to the attack. Thus the administrator can correct the vulnerability.

Click on the **Show help** button to show or hide the help zone associated with an event.

Typically, help comes in the form of a descriptive file that contains explanations, links to the publisher's site or to bug fixes.

REMARK
Refer to the Stormshield Network Security user guide to configure Vulnerability Manager.

5.3 Hosts

From the menu tree, click on **Hosts**.

This window lists the connected hosts.

5.3.1 "Hosts" tab

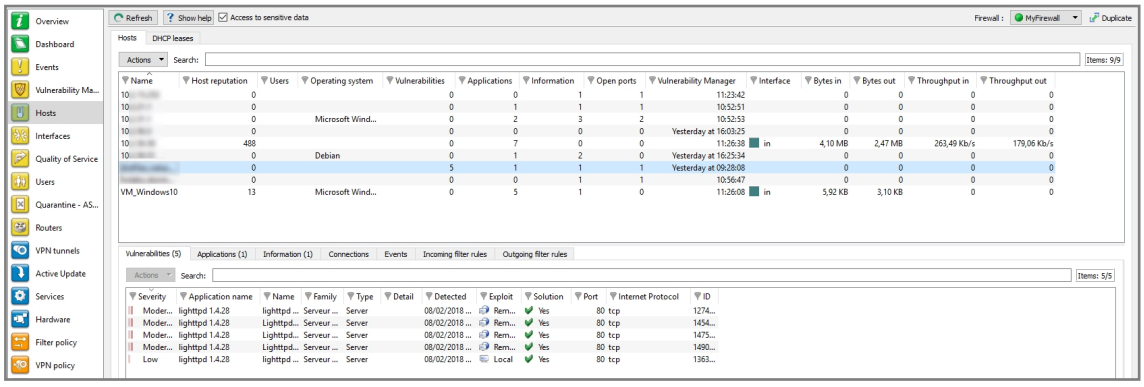


Figure 36: Hosts

This screen consists of 3 views:

- A view listing the hosts
- A view that lists the Vulnerabilities, Applications, Information, Connections and Events relating to the selected host
- A hidden help view that you can display by clicking on "Show help" (top left of the screen). This allows working around the selected vulnerability, if a solution exists.

"Hosts" view

This view shows all hosts detected by the firewall. Every row represents a host.

The "Hosts" view displays the following data:

Name	Name of the sending host (if declared in objects) or IP address of the host (if not declared).
Address	IP address of the host.
Users	User logged on to the host (if any).
MAC address	MAC address of the host.
Operating system	Operating system used on the host.
Vulnerabilities	Number of vulnerabilities detected.
Applications	Number of applications on the host (if there are any).
Events	Number of detected events.
Open ports	Number of open ports.
Vulnerability Manager	Indicates the date and time of the last Vulnerability Manager event.
Interface	Interface to which the user belongs.
Bytes in	Number of bytes that have passed through the firewall from the sending host ever since the firewall started running.
Bytes out	Number of bytes that have passed through the firewall towards the sending host ever since the firewall started running.
Incoming throughput	Actual throughput of traffic to the host passing through the firewall
Outgoing throughput	Actual throughput of traffic from the host passing through the firewall
Host reputation	Host's reputation score This column will only contain data when host reputation management has been enabled and the selected host is a monitored host.

The **Actions** button makes it possible to perform certain actions on the selected event (for further information, please refer to the section Pop-up menu on rows):

- Remove host from ASQ,
- Reset Vulnerability Manager information,
- Send to quarantine,
- Manually set the Operating System

- Add the host to the Object base,
- Ping host,
- Traceroute to source host.

"Vulnerabilities" view

For a selected host, this tab will describe the vulnerabilities detected. Each vulnerability can then later be viewed in detail.

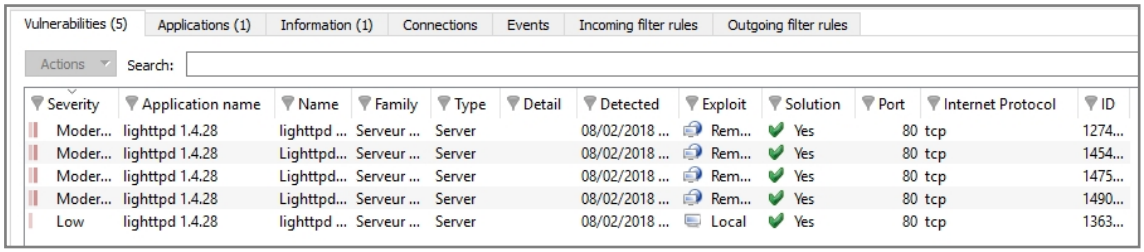


Figure 37: Hosts – Vulnerabilities

The "Vulnerabilities" view displays the following data:

Severity	Indicates the level of severity on the host(s) affected by the vulnerability. There are 4 levels of severity: "**Low**", "**Moderate**", "**High**", "**Critical**".
Name of the application	Name of the software as well as its version, if available.
Name	Indicates the name of the vulnerability.
Family	Number of hosts affected.
Type	Software type (Client: the software does not provide any service – Server: the software application provides a service).
Details	One of 2 targets: "**Client**" or "**Server**".
Assigned	Family to which the vulnerability belongs.
Exploit	Access may be local or remote (via the network). It allows exploiting the vulnerability.
Workaround	Indicates whether a workaround exists.
Port	Date on which the vulnerability was detected. **WARNING** This refers to the discovery date and not the date on which the vulnerability appeared on the network.
Internet Protocol	Name of the protocol used.
ID	Vulnerability ID

The **Actions** button makes it possible to perform certain actions on the selected event (for further information, please refer to the section Pop-up menu on rows):

- View hosts with the same vulnerability

"Application" view

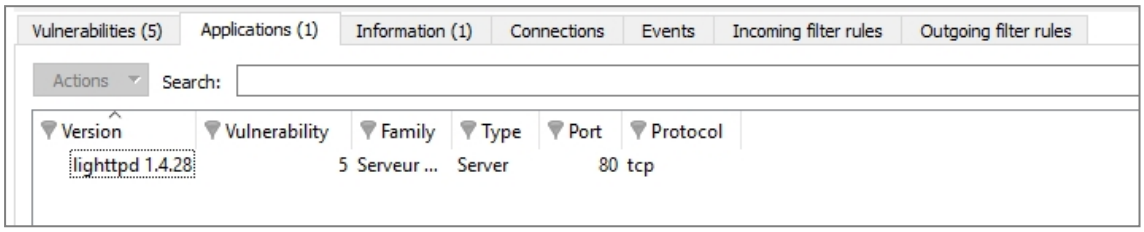


Figure 38: Hosts – Applications

For a selected host, this tab will describe the applications detected. It is possible to view applications in detail later.

The "**Application**" view displays the following data:

Version	Name and version of the application.
Vulnerability	Number of vulnerabilities detected on the application.
Family	The software application's family.
Type	Application type (Client: the software does not provide any service – Server: the software application provides a service).
Port	Port used by the application (if it uses one).
Protocol	Protocol used by the application

The **Actions** button makes it possible to perform certain actions on the selected event (for further information, please refer to the section Pop-up menu on rows):

- View all hosts that use this application,
- View the vulnerabilities for this application,
- Impose a server application.

"Information" view

This tab provides information relating to a given host.

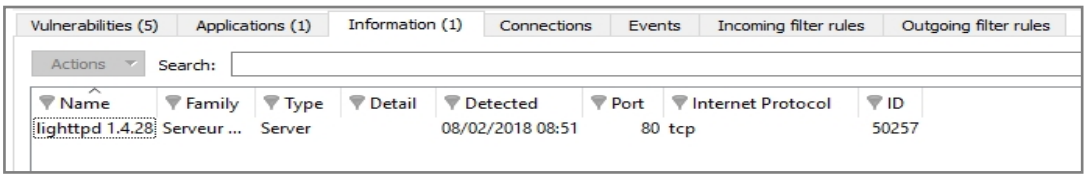


Figure 39: Hosts – Events

REMARK

The number of events is displayed in the tab's name.

The "**Information**" view displays the following data:

Name	Name of the detected OS.
Family	Family of the vulnerability that is likely to appear (Example: SSH).
Type	Application type (Client: the software does not provide any service – Server: the software application provides a service).
Details	Description of information.
Assigned	Date and time of detection.
Port	Number of the port on which the vulnerability had been detected.
Protocol	Name of the protocol used.
ID	Unique identifier of the vulnerability family.

The **Actions** button makes it possible to perform certain actions on the selected event (for further information, please refer to the section Pop-up menu on rows):

- View hosts with the same information.

"Connections" view

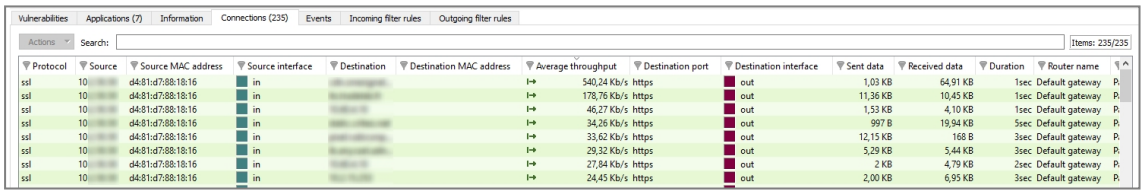


Figure 40: Hosts - Connections

This view shows all connections detected by the firewall. Every row represents a connection. The "**Connection**s" view displays the following data:

Time	Indicates the date and time of the object's connection.
Protocol	Communication protocol used for the connection.
Source	Name of the object that connected to the selected host.
Source MAC address	MAC address of the object at the source of the connection
Source port	Number of the source port used for the connection
Source interface	Name of the interface on the firewall on which the connection was set up.
Destination	Name of the object for which a connection has been established.
Destination MAC address	MAC address of the object at the destination of the connection.
Average throughput	Average value calculated by the amount of data exchanged divided by the length of the session.
Destination Port	Number of the destination port used for the connection

Destination interface	Name of the destination interface used by the connection on the firewall.
Data sent	Number of bits sent during the connection.
Data received	Number of bits received during the connection.
Duration	Connection time.
Router	ID assigned by the firewall to the router used by the connection
Router name	Name of the router saved in the objects database used by the connection
Policy	Name of the policy that allowed the connection
Rule	ID name of the rule that allowed the connection
Operation	Identified command of the protocol.
Parameter	Operation parameter.
Status	This parameter indicates the status of the configuration corresponding, for example, to its initiation, establishment or closure.

The **Actions** button makes it possible to perform certain actions on the selected event (for further information, please refer to the section Pop-up menu on rows):

- Ping source host,
- Traceroute to source host,
- Ping destination host,
- Traceroute to destination host,
- Send connection to quarantine.

"Events" view

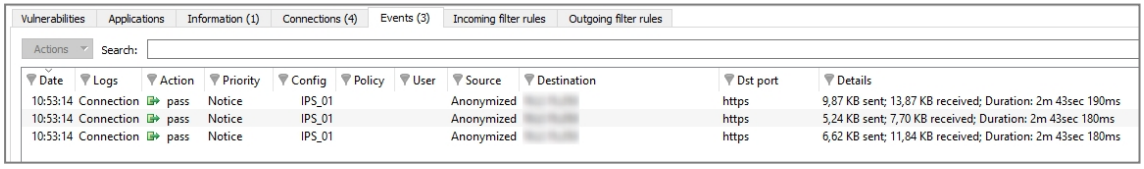


Figure 41: Hosts - Events

This view allows you to view all the events that the firewall has detected. Each line represents an alarm. The information provided in the "**Events**" view is as follows:

Date	Date and time the line was recorded in the log file at the firewall's local time.
Logs	Source of the event.
Action (action)	Action associated with the filter rule and applied to the packet (**Examples**: Block/Pass, etc.)

Priority	Determines the alarm level. The possible values are: 0: emergency 1: alert 2: critical 3: error 4: warning 5: notice 6: information 7: debug
Config	Name of the application inspection profile that reported the event.
Policy	Name of the SMTP, URL or SSL filter policy that raised the alarm.
User	Identifier of the user requesting authentication
Protocol	Protocol of the packet that set off the alarm.
Source	IP address or name of the object corresponding to the source host of the packet that set off the event.
Source MAC address	MAC address of the object at the source of the connection
Src prt num	Port number of the source (only if TCP/UDP).
Destination	IP address or name of the object corresponding to the destination host of the packet that set off the event.
Destination Port	Port requested for this connection (in letters, **e.g.**: http).
Dst. port (num)	Destination port requested for this connection (in numerals, **e.g.**: 80).
Details	Describes the event relating to the log. This description groups information from other columns in a single column. **Example**: *if it is an alarm log, information such as whether the alarm is sensitive, the filter rule number and rule identifier will be indicated in this column or will otherwise be new columns in order to enable filtering.* Please refer to the "*Audit logs*" technical note.
Source IP reputation	Reputation category of the public IP address at the source of the traffic. This column will only contain data if this IP address is public and listed in the IP address reputation database. The possible values are: "anonymizer", "botnet", "malware", "phishing", "tor", "scanner" or "spam".
Source host reputation	Reputation score of the host at the source of the traffic. This column will only contain data when host reputation management has been enabled and the selected host is a monitored host.
Destination IP address reputation	Reputation category of the public IP address at the destination of the traffic. This column will only contain data if this IP address is public and listed in the IP address reputation database. The possible values are: "anonymizer", "botnet", "malware", "phishing", "tor", "scanner" or "spam".
Destination host reputation	Reputation score of the host at the destination of the traffic. This column will only contain data when host reputation management has been enabled and the selected host is a monitored host.

For the description of additional data available by column title, please refer to the section EVENTS.

The **Actions** button makes it possible to perform certain actions on the selected event (for further information, please refer to the section Pop-up menu on rows):

- Ping source host,
- Traceroute to source host,
- Ping destination host,
- Traceroute to destination host,

"Incoming filter rules" view

This view allows listing the incoming filter rules that can be applied to the selected host. Block rules are shown in red. Ignored rules are grayed out.

"Outgoing filter rules" view

This view allows listing the outgoing filter rules that can be applied to the selected host. Block rules are shown in red. Ignored rules are grayed out.

5.3.2 "DHCP leases" tab

This tab displays all hosts that have a lease in progress or which has ended and specifies the state of this lease. The information provided in the *DHCP leases* tab is as follows:

IP address	IP address of the host.
Name	Name of the host that has a lease in progress or which has ended (if declared in objects) or host's IP address otherwise.
Status	The status of the lease can be: • **Active**: the address has been assigned to a host and the assignment is still in progress. • **Free**: the lease has expired, and the address can be reused for another lease.
From	Starting date and time of the lease assignment.
Until	Ending date and time of the lease assignment. This can be a date and time in the past or future
MAC address	Physical network identifier of the host with an ongoing or lapsed lease.

REMARK
The leases assigned by reservation (static IP address reserved exclusively for a MAC address) are not displayed on this screen.

REMARK
When a new host logs on to a network, it will send a first request (DHCPDISCOVER) to the whole network to find out where the DHCP servers are. Upon reception, the DHCP server will pre-reserve an IP address and sends it to the host (DHCPOFFER). It is possible, however, that this host already uses the address range of another DHCP server. During this pre-reservation period (2 minutes), the IP address will no longer be available but will appear in the list as "free". If many pre-reservations are made within a short period, the server may run out of available addresses while the screen continues displaying "free" addresses.

The **Actions** button makes it possible to perform certain actions on the selected event (for further information, please refer to the section Pop-up menu on rows):

- Display host,
- Ping source host,
- Traceroute to source host.

5.4 Interfaces

5.4.1 Introduction

DEFINITION
A zone, whether real or virtual, that separates two elements. The interface thus refers to what each element needs to know about the other in order to run correctly.

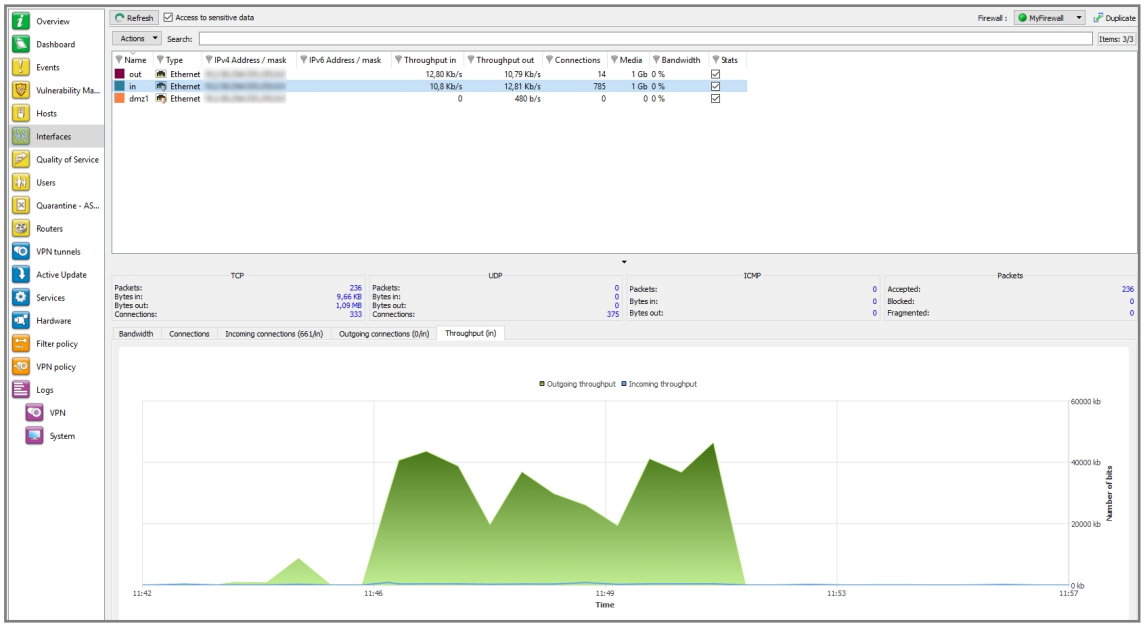


Figure 42: Interfaces

The **Interfaces** menu presents different statistics concerning:

- Bandwidth
- Connections
- Throughput

Statistics are displayed in the form of graphs. Both vertical and horizontal axes are graduated. The horizontal scale represents time. The vertical scale represents one of the following:

- Bandwidth percentage.
- The number of connections, or
- Throughput expressed in bytes, kilobytes or megabytes.

Interface types

- VLAN.
- Ethernet.
- PPTP.
- Dialup.

REMARK
The interfaces are grayed out or do not appear at all when they are disabled.

This screen consists of 3 views:

- A view of the interfaces in the form of a table (or legend)
- A details zone.
- A zone for viewing graphs.

5.4.2 Legend view (or tabular view of interfaces)

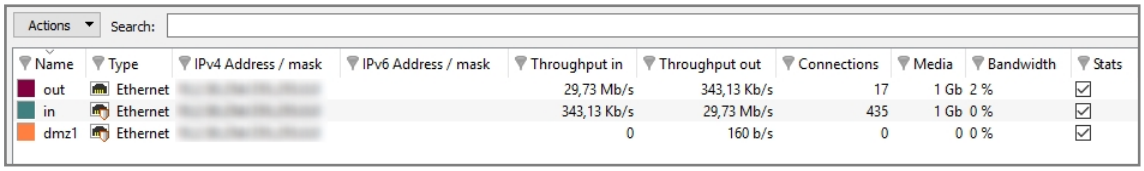


Figure 43: Interfaces – Legend

This view allows you to view all the interfaces that the firewall has detected. Each line represents an interface.

The information provided in the "**Legend**" view is as follows:

Name	Name and color assigned to the interface. The colors allow you to distinguish the interface in the various graphs.
Type	Type of interface with a matching icon.
IPv4 Address/ Mask	IPv4 address and subnet mask of the interface.
IPv6 Address/ Mask	IPv6 address and subnet mask of the interface.
Incoming throughput	Indicates the actual incoming throughput.
Outgoing throughput	Indicates the actual outgoing throughput.
Connections	Number of real-time connections on each interface of the firewall over a defined period.
Media	The default value is 0. The throughput of a network interface can be configured via the firewall's web administration interface.
Bandwidth	Indicates the percentage of bandwidth used for an interface.
Stats	If this option is selected, the graph corresponding to this interface will be displayed.

REMARK
Inactive interfaces are grayed out.

You will notice the colors of the visible interfaces at the top of the window. These colors are defined in the network parameters of the firewall for each interface (refer to the *Stormshield Network Security user manual)*.

The **Actions** button makes it possible to perform certain actions on the selected event (for further information, please refer to the section Pop-up menu on rows):

- Filter by these criteria,
- Filter only this column by this criterion,
- Display hosts associated with this interface.

5.4.3 "Details" view

Each table summarizes throughput statistics for each interface.

The details zone provides the following information:

- Name, IP address, subnet mask (American format), connection type (10 or 100Mbits, half duplex or full duplex).
- Instantaneous (left) and maximum (right) throughput.
- Number of packets and volume in bytes for TCP, UDP and ICMP.
- Number of TCP connections.
- Total number of packets accepted, blocked and fragmented by the Firewall.

5.4.4 "Bandwidth" tab

The bandwidth graph displays the percentage of use of the available bandwidth on each interface in real time.

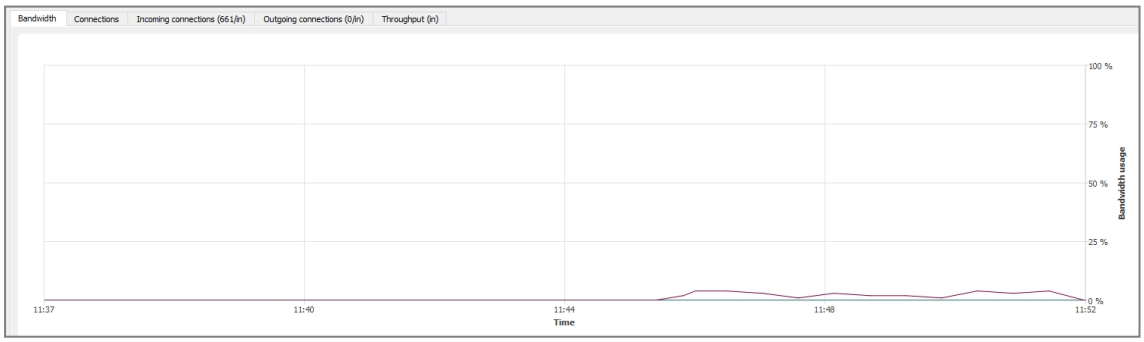


Figure 45: Interfaces - Bandwidth

Each interface is represented by a different color of which the legend may be found at the top of the graph. Maximum bandwidth represents the theoretical maximum throughput supported by the interface.

Example

For a 100Mbits/s line used in full duplex, this maximum is 200 Mbits/s, and for a 10Mbits/s line used in half duplex it is 10 Mbits/s.

5.4.5 "Connections" tab

The connection graph displays in real time the number of connections on each of the Firewall's interfaces during the defined period.

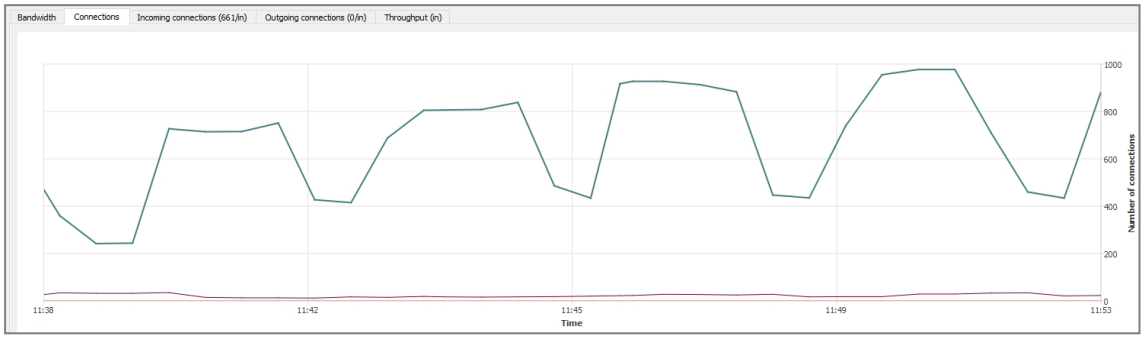


Figure 46: Interfaces - Connections

Each interface is represented by a different color of which the legend may be found at the top of the graph.

5.4.6 "Incoming connections" tab

The screen displays incoming connections in progress relating to the selected interface. To find out what data is offered, please refer to the section of the Hosts module, section *"Connections"* view for the *Hosts* tab.

The **Actions** button makes it possible to perform certain actions on the selected event (for further information, please refer to the section Pop-up menu on rows):

- View source host,
- View destination host,
- Send connection to quarantine

5.4.7 "Outgoing connections" tab

The screen displays outgoing connections in progress relating to the selected interface. To find out what data is offered, please refer to the section of the Hosts module, section *"Connections"* view for the *Hosts* tab.

The **Actions** button makes it possible to perform certain actions on the selected event (for further information, please refer to the section Pop-up menu on rows):

- View source host,
- View destination host,
- Send connection to quarantine

5.4.8 "Throughput" tab

The throughput graph represents the real throughput on each of the Firewall's interfaces. The throughput scale automatically adapts to the maximum throughput recorded during the period.

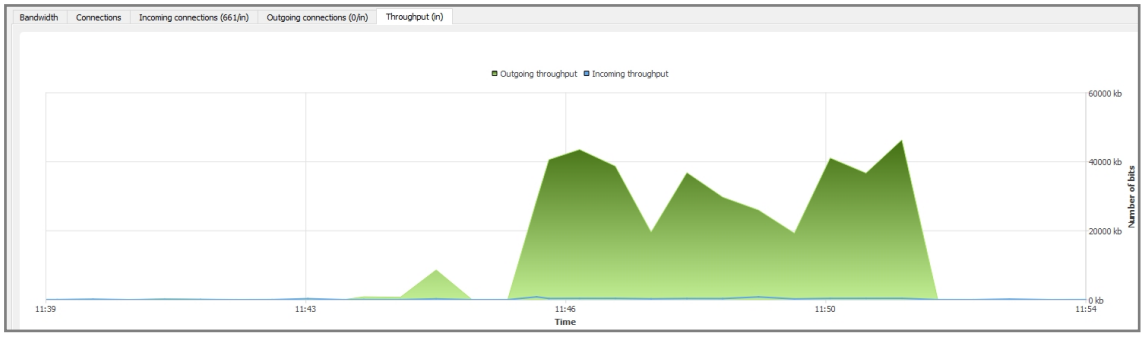


Figure 47: Interfaces - Throughput

For each interface, the throughput graph indicates the ingoing and outgoing throughput.

To modify the interface on which throughput is viewed, click on this interface in the legend at the top right section of the graph. The interface currently being viewed will be highlighted in blue.

5.5 Quality of service (QoS)

REMARKS

1. Quality of Service, which has a high level of abstraction, refers to the ability to provide a network service according to parameters defined in a Service Level Agreement (SLA). The "quality" of the service is therefore gauged by its availability, latency rate, fluctuations, throughput and rate of lost packets.
2. Where network resources are concerned, the "Quality of service" refers to a network element's ability to provide traffic prioritization services and bandwidth and latency time control.

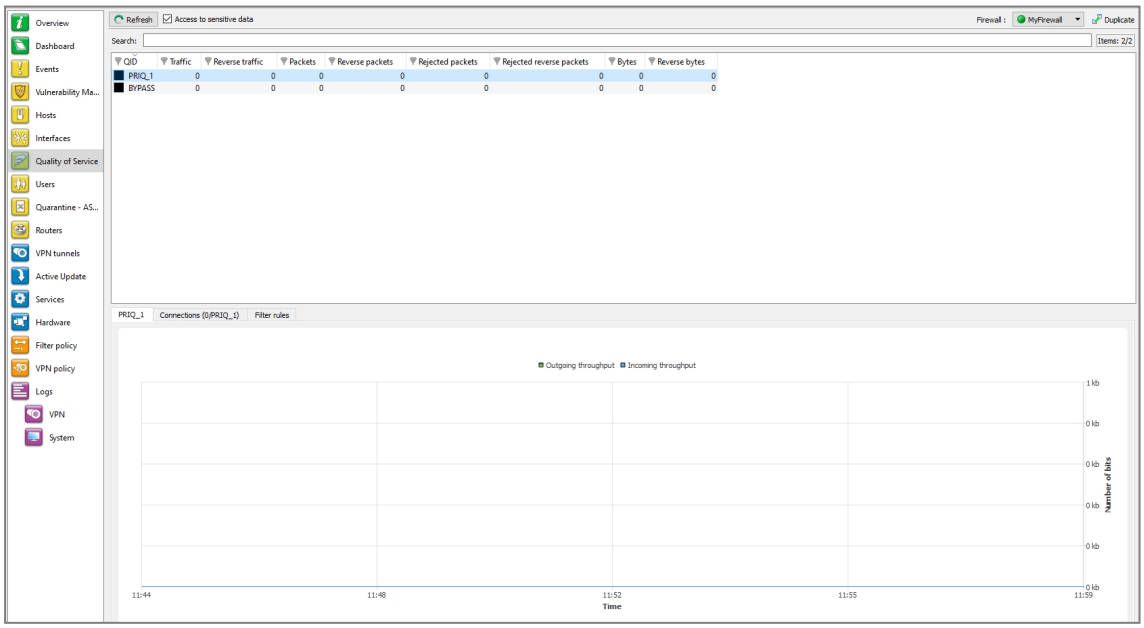


Figure 48: QoS

This window comprises 2 views:

- A table view
- A graph view

The following data is displayed when you click on the Quality of Service menu:

QID	Name of the policy defined for accepting or rejecting packets.
Throughput	Indicates in real time the incoming throughput that the QID manages.
Reverse traffic	Indicates in real time the outgoing throughput that the QID manages
Packets	Number of incoming packets in real time over a defined period.
Reverse packets	Number of outgoing packets in real time over a defined period
Rejected packets	Number of rejected incoming packets on the network.
Rejected reverse packets	Number of rejected outgoing packets.
Bytes	Value in Kbits or Mbits.
Reverse bytes	Value in Kbits or Mbits.

5.5.1 “Diagram” view

This view shows the incoming and outgoing throughput associated with the different QIDs defined on the firewall’s QoS policy.

5.5.2 "Connections" view

The Connections tab displays connections in progress going through the selected queue. To find out what data is offered, please refer to the section of the Hosts module, section *“Connections”* view for the *Hosts* tab.

5.5.3 “Filter rules” view

This view allows listing the incoming filter rules that can be applied to the selected service class. Block rules are shown in red. Ignored rules are grayed out.

5.6 Users

5.6.1 Introduction

The **User**s menu enables viewing, in the capacity of an administrator, the users who are currently connected on the Firewall.

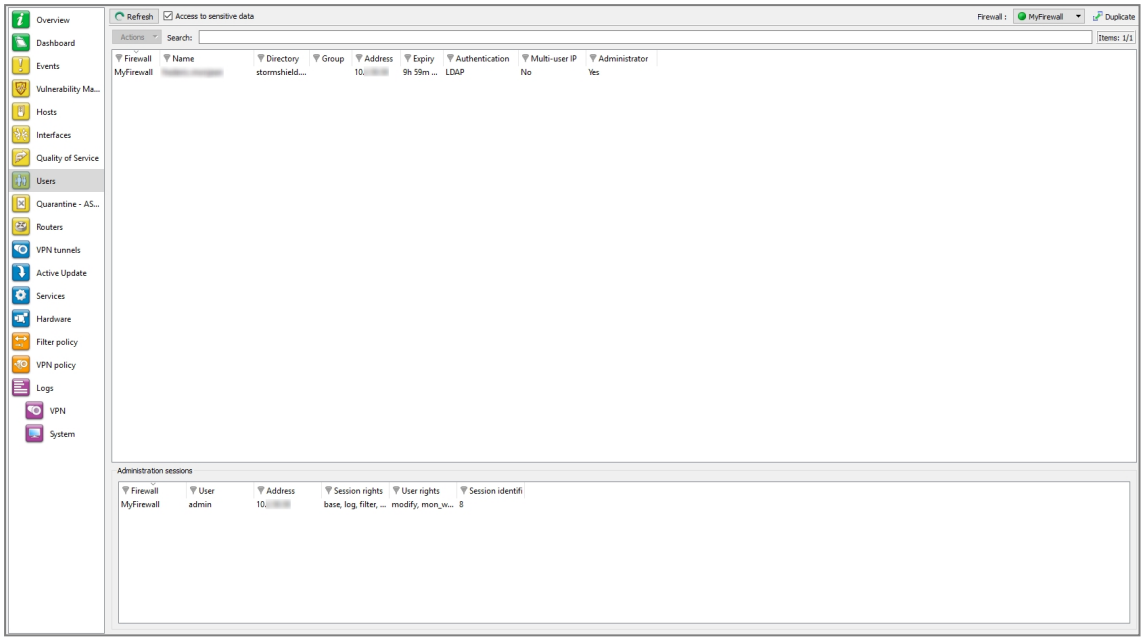


Figure 49: Users

This window comprises 2 views:

- A “Users” view.
- An “Administration sessions” view.

“Users” view

The information provided in the “Users” view is as follows:

Firewall	Serial number or name (if known) of the firewall.
Name	Name of the authenticated user.
Group	Name of the group to which the user belongs.
Address	User’s IP address.
Expires on	Remaining time in the authentication session. (Users are authenticated for a definite period).
Authentication	Authentication method used.
Multi-user IP	Indicates whether multi-user authentication is used (one IP address shared by several users). **REMARK** As the SSO Agent method only allows one authentication per IP address, the value will therefore not be available (value *<n/a>* displayed).
Administrator	Indicates the type of ‘Administrator” privileges granted to the connected user.

The **Actions** button makes it possible to perform certain actions on the selected event (for further information, please refer to the section Pop-up menu on rows):

- Remove user from ASQ

"Administration sessions" view

This window enables finding out the session privileges of the user connected to the firewall.

The information provided in the "administration sessions" view is as follows:

Firewall	Serial number or name (if known) of the firewall.
User	Authenticated user's identifier.
Address	IP address of the connected user's host.
Session privileges	Indicates the privileges for the current session. Only one administrator is allowed to make changes in each session (*modify* and *mon_write* privileges).
User privileges	Indicates privileges that have been given to the connected user (these privileges include adding, modifying, deleting or reading in different applications).
Session identifier	Session ID number.

5.7 Quarantine - ASQ Bypass

DEFINITIONS

1. **Dynamic quarantine**: the quarantine is manually done and for a set duration.
2. **Static quarantine**: the quarantine is automatic and for permanent.

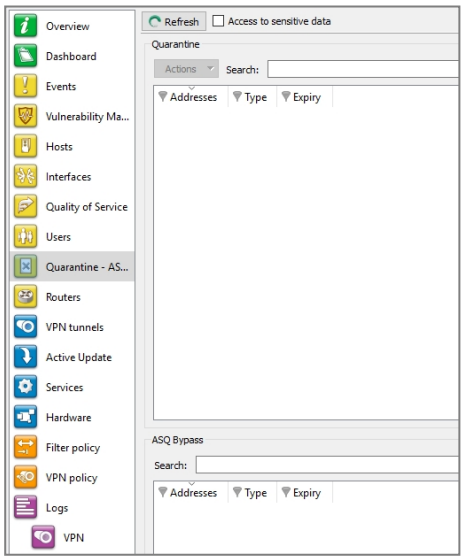


Figure 50: Quarantine

This window comprises 2 views:

- A "Quarantine" view.
- An "ASQ Bypass" view.

5.7.1 "Quarantine-ASQ Bypass" view

This window shows the hosts that have been dynamically quarantined. Hosts in static quarantine are not reflected in this list.

The information provided in the "Quarantine - ASQ Bypass" view is as follows:

Addresses	IP address of the host(s) affected by the quarantine.
Type	2 options are possible: **Host to host** and **Host to all**.
Expires on	Time at which the quarantine will expire.

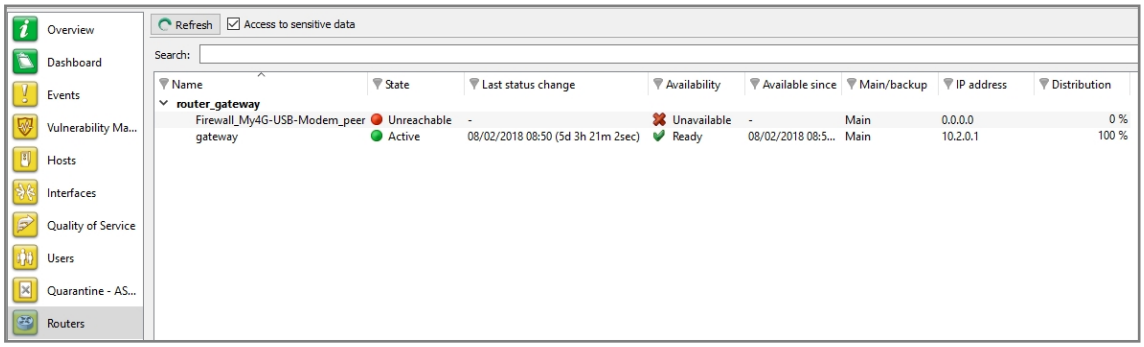
5.7.2 "ASQ Bypass" view

The information provided in the "Whitelist" view is as follows:

Addresses	IP address of the host(s) affected by the whitelist.
Type	2 options are possible: **Host to host** and **Host to all**.
Expires on	Time at which the whitelist will expire.

5.8 Routers

The **Routers** module shows the list of routers used in the configuration of the firewall: default gateway and routers configured in filter rules (PBR: Policy Based Routing).



When the **Routers** menu in the menu directory is selected, the data displayed by default are:

Name	Name of the router and the gateways that it includes.
Status	Indicates the status of each gateway. There are three possible values: • **Active**: when the gateway is in use, • **On standby**: when it is a backup gateway, • **Not reachable**: the gateway is not responding to pings
Last status change	Duration since the gateway's last change of status.
Availability	Indicates whether the gateway is available for use. There are two possible values: *Ready* or *Disabled*.

Available since	Time elapsed since the gateway's availability was last changed.
Main/backup	Indicates whether the gateway is in use (main) or is a backup gateway.
IP address	IP address of the gateway.
Fairness	Indicates the percentage of the gateway used in the router object.
Type	Specifies the type of configuration in which the gateway is used: filter rule or load balancing, etc.

6. Network activity

This module groups information regarding:

- VPN tunnels,
- Active Update,
- Services on the firewall,
- Hardware information.

6.1 VPN tunnels

The VPN Tunnels module presents IPSec VPN and SSL VPN tunnels under two separate tabs.

6.1.1 IPSec VPN Tunnels tab

The following window appears when you click on the **VPN Tunnels** menu:

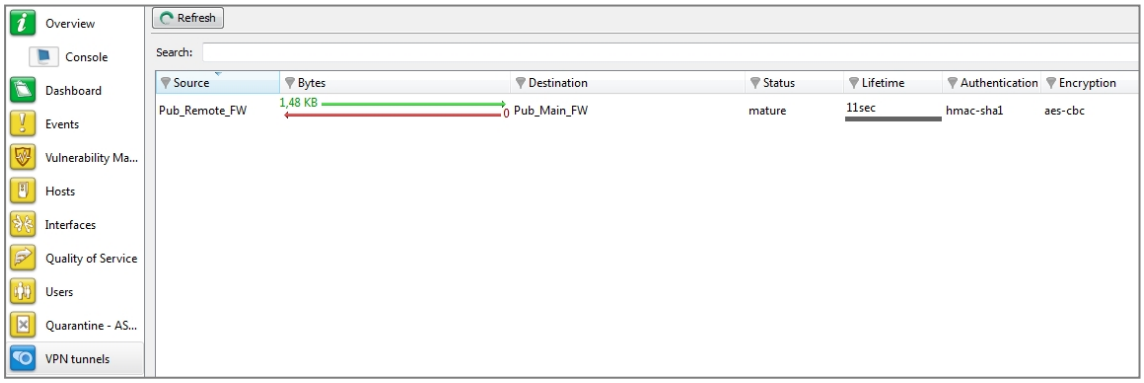


Figure 51: IPSec VPN tunnels

This section sets out the statistics of the tunnel's operation.

The following information is displayed in this window:

Source	IP address or name of the tunnel initiator
Source address	IP address of the tunnel initiator

Bytes	Incoming and outgoing throughput
Destination	Destination IP address
Status	Indicates the status of the tunnel. (Example: Mature).
Lifetime	The SA's (Security Association) lifetime in a graphical representation of the position in this lifetime as well as the value (expressed in hours, minutes and seconds).
Authentication	Name of the authentication algorithm
Encryption	Name of the encryption algorithm

The tunnel is made up of two sub-tunnels, one for each direction of the datagram transmission.

REMARK

The algorithms and limits have been configured in the firewall's web administration interface (refer to the *Stormshield Network Security user and configuration guide* for further details).

TIP

You will find other information regarding the parameters in this window in the RFCs.

Further information may be found in RFC 2401 IPSEC:

http://www.ietf.org/rfc/rfc2401.txt or on sites such as:
http://www.guill.net/reseaux/Ipsec.html

This status is color-coded. The line containing VPN information will use the color corresponding to the tunnel's status.

	Undetermined
	Larval: the SA is in the process of being negotiated or has not been completely negotiated.
	Mature: the SA has been established and is available; the VPN tunnel has been correctly set up.
	Dying: the SA will soon expire; a new SA is in the progress of being negotiated.
	Dead: the SA has expired and cannot be used; the tunnel has not been set up and is therefore no longer active.
	Orphan: a problem has occurred, in general this status means that the tunnel has been set up in only one direction.

The **Actions** button makes it possible to perform certain actions on the selected event (for further information, please refer to the section Pop-up menu on rows):

- View logs of outgoing SPIs,
- View logs of incoming SPIs,
- View the outgoing policy,
- View the incoming policy,

- Reset this tunnel,
- Reset all tunnels.

6.1.2 SSL VPN Tunnels tab

The following window appears when you click on the **VPN Tunnels** menu:

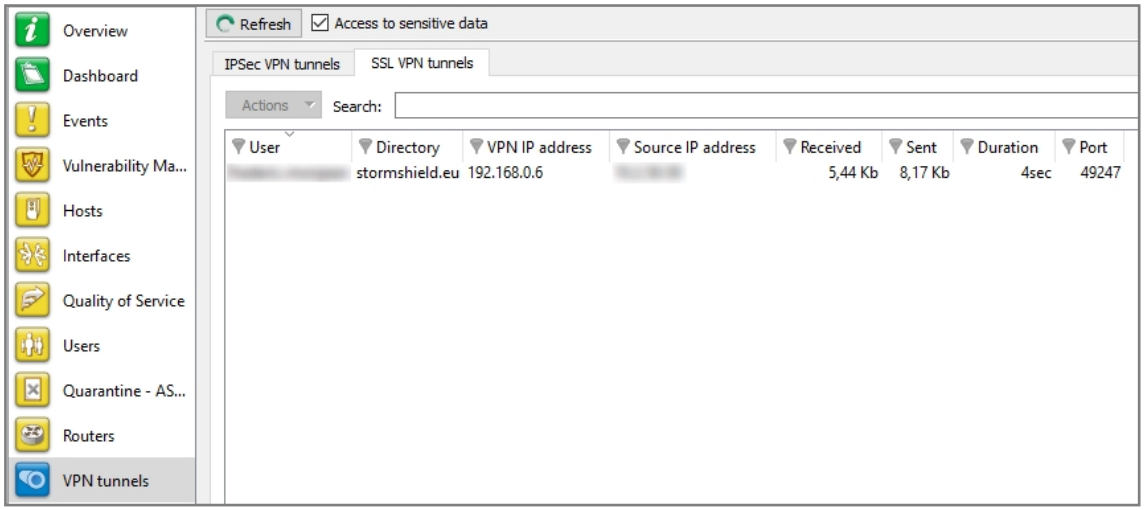


Figure 52: SSL VPN tunnels

It displays statistics on the operation of SSL VPN tunnels that have been set up.

The following information is displayed in this window:

User	Name of the user that initiated the tunnel.
VPN IP address	IP address assigned by the OpenVPN server to the client, for communications through the SSL VPN tunnel.
Source IP address	IP address of the client workstation outside the SSL VPN tunnel (local network address).
Received	Amount of data the client has received through the SSL VPN tunnel (unit: bits).
Sent	Amount of data the client has sent through the SSL VPN tunnel (unit: bits).
Duration	Time elapsed since the setup of the SSL VPN tunnel (expressed in days, hours, minutes and seconds).
Port	Source port used by the client to set up the SSL VPN tunnel.

The **Actions** button makes it possible to perform certain actions on the selected event (for further information, please refer to the section Pop-up menu on rows):

- View host,
- Remove this tunnel.

6.2 Active Update

DEFINITION: ACTIVE UPDATE

Enables updating the antivirus database, ASQ contextual signatures, the list of antispam servers, trusted root certification authorities and the URLs used for dynamic URL filtering.

This window displays the status of Active Update on the firewall for each type of update available (Antispam, Antivirus, Contextual signatures, Root certificates ...).

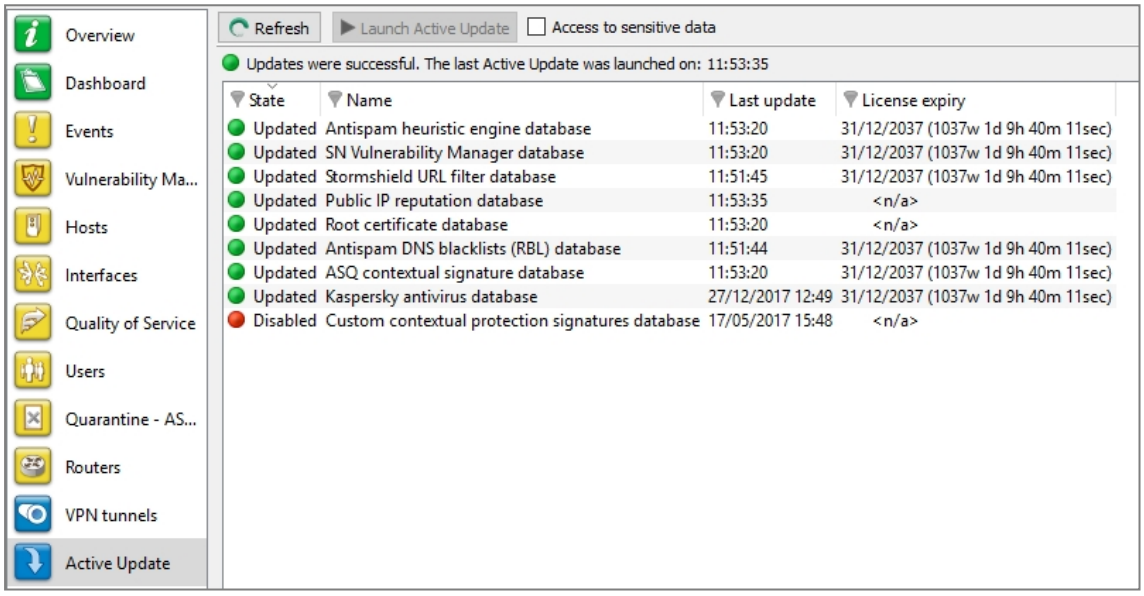


Figure 53: Active Update

Active Update is used for automatically keeping URL databases up to date by downloading them on servers such as updateX. stormshield.eu.

The Monitor screen indicates the result of the last update (successful or failed) and the date of the last update.

The following data will be displayed when you click on the Active Update menu:

Status	Indicates the status of the Active Update. 2 options are possible: **The last update failed / Updated**.
Name	Indicates the update data categories.
Last update	Indicates the date and time of the last update.
License expiry	Indicates the expiry date of the license option for this category.

6.3 Services

This window sets out the services (active and inactive) on the Firewall and for how long they have been active/inactive.

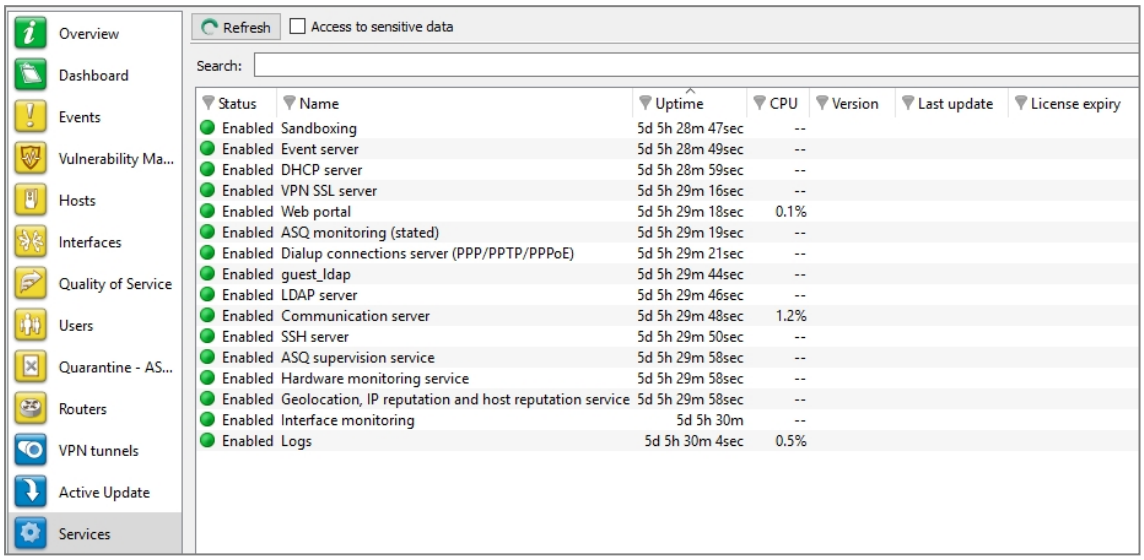


Figure 54: Services

This screen also contains information regarding the antivirus (activity, version, last update, license expiry).

The following data is displayed when you click on the **Services** menu:

Status	Indicates whether services are active or inactive.
Name	Indicates the names of services.
Uptime	Indicates the number of number of days the service has been running and the time of activation.
CPU	Portion of processor resources used by the service (percentage).
Version	Version number of the service.
Last update	Date of the last time the service was updated.
License expiry	Expiry date of the license.

6.4 Hardware

6.4.1 High Availability

This window displays information concerning the initialization of high availability.

DEFINITION OF HIGH AVAILABILITY

High availability is an option that allows two firewalls (identified through a MasterHA and BackupHA license) to exchange information on their statuses, via a dedicated link in

order to ensure service continuity in the event one of the firewalls breaks down. Firewalls in high availability have the same configuration – only their serial numbers, licenses (Master or Backup) and most of all, their status (active or passive) differ.

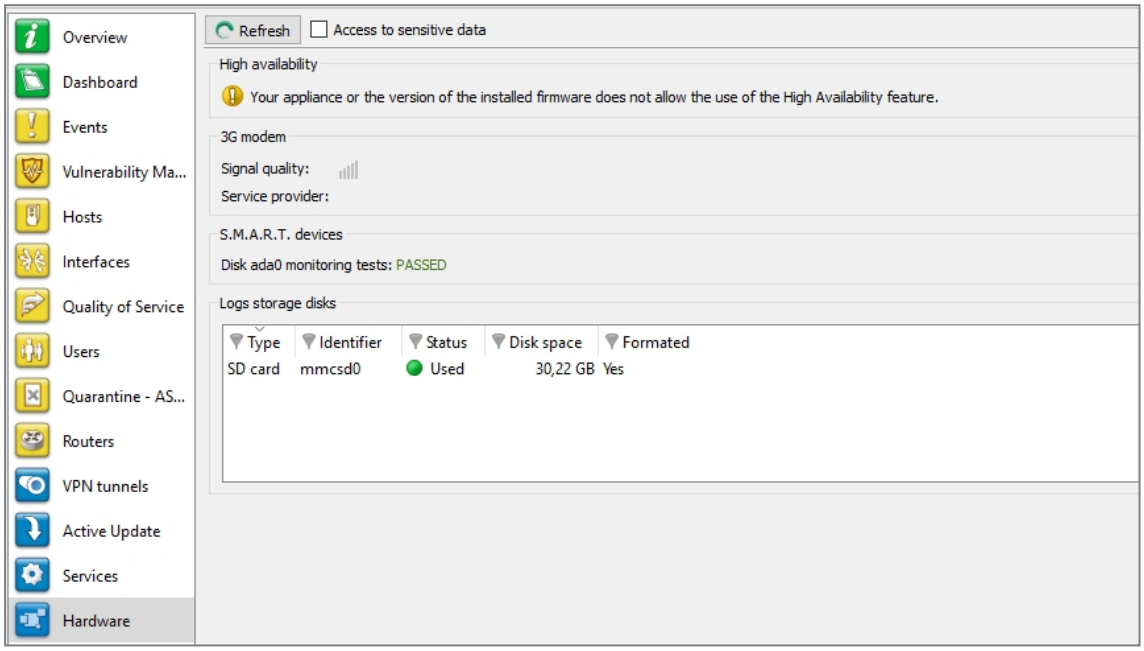


Figure 55: Hardware

NOTE

Version 1 of Stormshield Network multifunction firewalls allows you to benefit from high availability support and a new-generation display with the date of the last synchronization.

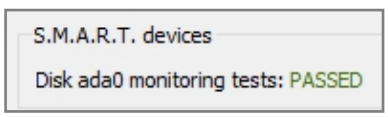
You will also notice changes to RAID support.

6.4.2 Power supply

If your firewall model supports redundant power supply modules (high-end models SN3000 and SN6000), the power supply statut will be displayed.

6.4.3 S.M.A.R.T. devices

The results of monitoring tests that have been conducted will be displayed for each S.M.A.R.T. peripheral detected.



6.4.4 RAID

The following is the information relating to the status of RAID volumes and the disks that it comprises:

Disk type	Indication of the type of RAID volume or type of disk that makes up a RAID volume. **Example**: Mirrored array (Raid1) for a RAID volume.
Disk address	Physical location of the disk contributing to a RAID volume. **Example**: Upper slot.
Disk status	Status of the RAID volume or of a disk that it comprises. **Example**: Degraded, Optimal.

6.4.5 Log storage disks

The information relating to the storage medium is:

Type	Indicates the type of storage medium.
Username	Identifier of the storage medium (assigned by the firewall).
Status	Indicates whether the storage medium is recognized.
Disk space	For formatted media, this indicates the size of the partition in Gigabytes.
Formatted	Indicates whether the storage medium is formatted.

In the event of a problem with a disk, a message will be displayed in the dashboard.

7. Policies

This module shows information relating to:

- Filter and NAT policies,
- VPN policies.

7.1 Filter policy

The **Filter Policy** menu, accessible from the menu directory, in Monitor recaps the active filter policy by grouping together implicit rules, global filter rules and local filter rules.

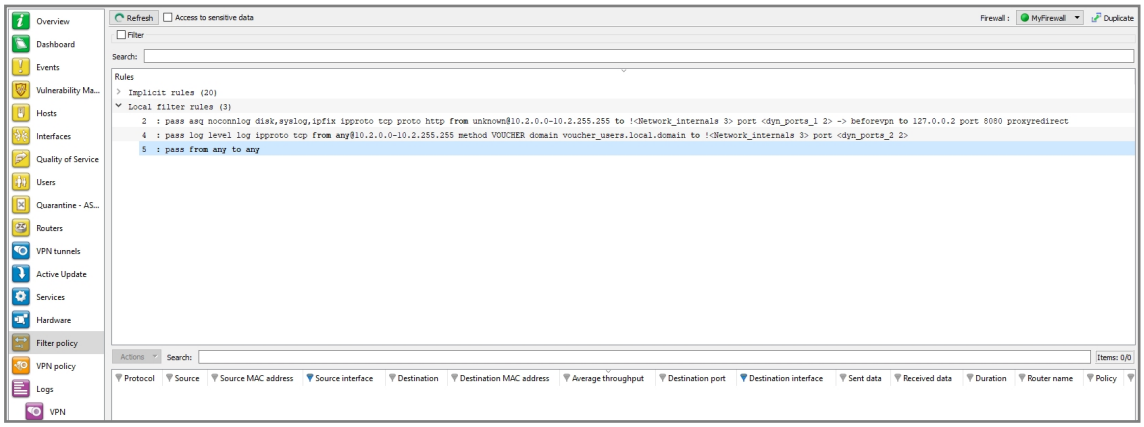


Figure 56: Filter policy

Every line is shown in the following manner:

- <identifier for the rule type > can be “0” for implicit rules, “1” for global filters and “2” for local filters.
- <identifier for the rule in the slot>: this identifier is always “0” for implicit rules.
- <filter rule>: filter rule created by Stormshield network.
- <NAT rule>: NAT rule created by Stormshield network.

7.1.1 "Connections" view

The “Connections” view sets out for each rule, all the connections allowed by the implicit, local and global filter policies.

7.2 VPN policy

Definition VPN (Virtual Private Network)
The interconnection of networks in a secure and transparent manner for participating applications and protocols – generally used to link private networks to each other through the internet.

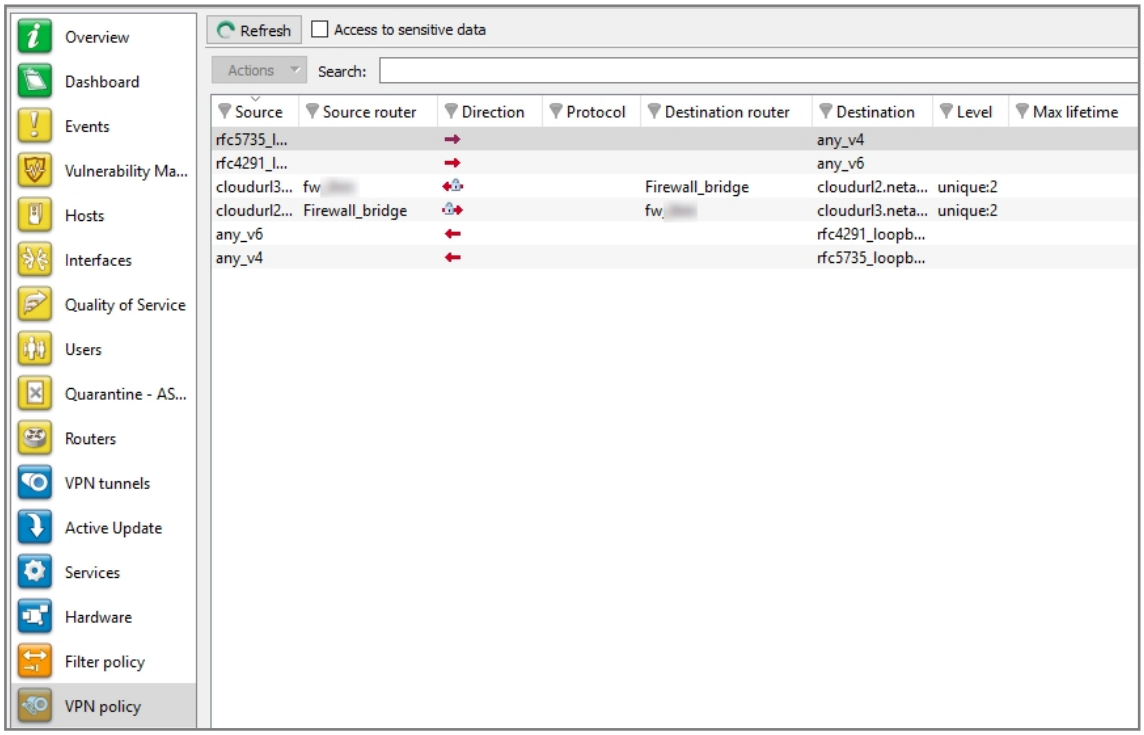


Figure 57: VPN Policy

The VPN section allows viewing the configuration of different VPN tunnel policies defined in the active VPN slot. These VPN policies do not necessarily have to be used in order to be displayed. The VPN slot only needs to be activated.

The following information is displayed in this window:

Source	Traffic endpoint. Indicates the source network.
Source router	Sending endpoint of the gateway that makes up the VPN tunnel.
Direction	Indicates the direction of the traffic represented by the following icons: •  •  •  • 
Protocol	Indicates the protocol(s) allowed to pass through the tunnel.
Destination router	Receiving endpoint of the gateway that makes up the VPN tunnel.
Destination	Traffic endpoint. Indicates the destination network.
Level	Level of security associated with the tunnel. **REMARK** This level is defined when creating the VPN tunnel according to the encryption and authentication algorithm.
Max lifetime	Maximum lifespan of the configured VPN policy.

The **Actions** button makes it possible to perform certain actions on the selected event (for further information, please refer to the section Pop-up menu on rows):

- View corresponding tunnels.

8. Logs

The **Logs** module sets out information that can be found in the firewall's logs, events relating to VPNs as well as the disk space used by logs.

8.1 Status of use

A graph represents the current size of the log file in real time (“Alarms”, “Authentication”, ”Connections”, “Filters”, “ftp”, “Monitor”, “Plugins”, “POP3”, “Vulnerability Manager”, “Administration”, “SMTP”, “System”, “IPSec VPN”, “Web”, “SSL VPN”) in relation to the size allocated on the Firewall for each log type.

DEFINITION OF LOGS

Chronological record of a computer’s activity, which makes up a journal of events that took place in programs and systems over a given period.

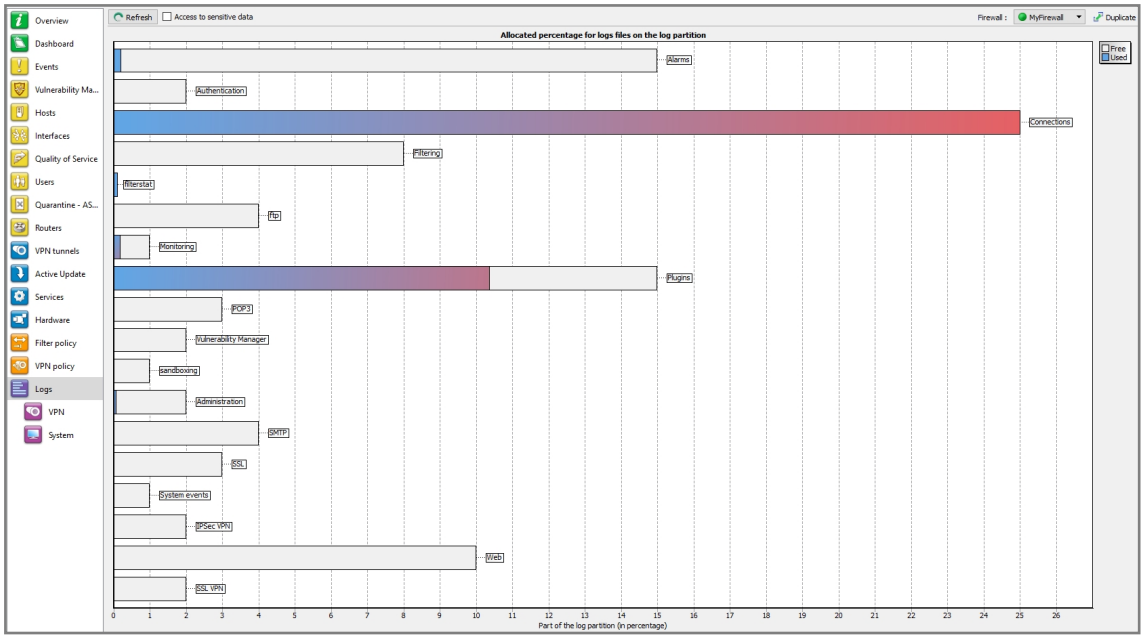


Figure 58: Logs

8.2 Log types

8.2.1 VPN

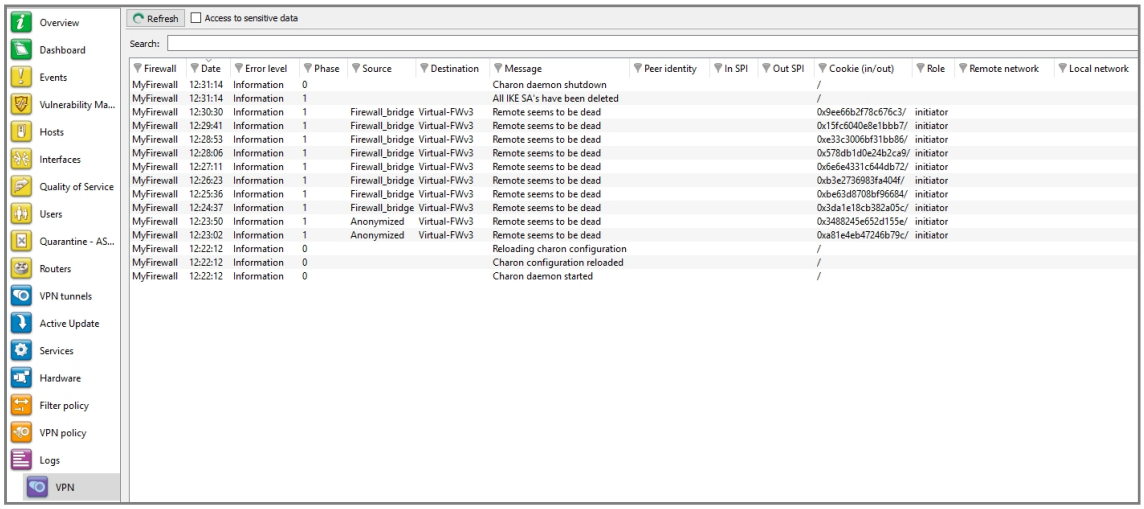


Figure 59: VPN Logs

The following data is displayed when you click on the VPN menu:

Date	Date and time the log line was generated
Error level	Error message
Phase	SA negotiation phase

Source	Connection source address (tunnel initiator).
Destination	Destination IP address or name
Message	Message informing of an attempt to set up a tunnel.
Peer identity	Identity of the peer indicated in pre-shared key configuration where “IP address” has not been specified as the identity type.
SPI in	SPI number of the negotiated incoming SA (in hexadecimal).
SPI out	SPI number of the negotiated outgoing SA.
Cookie (incoming / outgoing)	Temporary identity markers for the initiator and recipient of the negotiation.
Role	Indicates the user’s endpoint.
Remote network	IP address of the remote network on the traffic endpoint.
Local network	IP address of the local network on the traffic endpoint.

NOTE

VPN logs will now be displayed for models without hard drives.

8.2.2 System

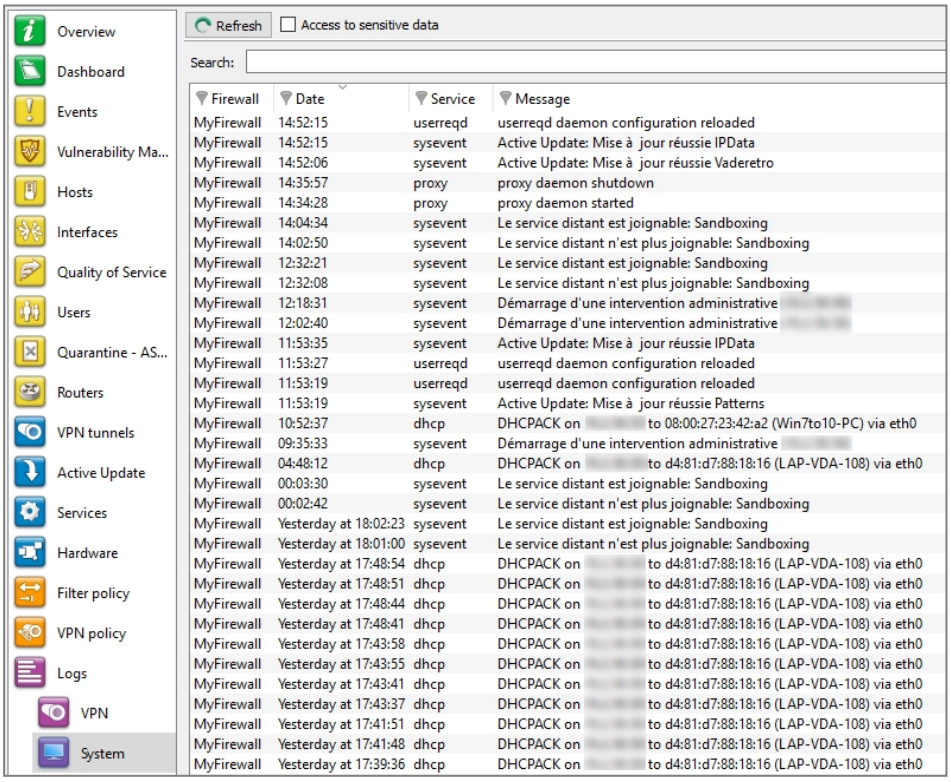


Figure 60: System Logs

The following data is displayed when you click on the System menu:

Date	Date and time entry was generated
Service	Name of the service
Message	Indicates the action applied.

NOTE

SYSTEM logs will now be displayed for models without hard drives.

9. Further reading

9.1 Session and user privileges

Name	Description	Privileges assigned
Logs (R)	Log consultation	base, log_read
Filter (R)	Filter policy consultation	base, filter_read
VPN (R)	VPN configuration consultation	base, vpn_read
Logs (W)	Privilege to modify log configuration	modify, base, log
Filter (W)	Privilege to modify filter policy configuration	modify, base, filter
VPN (W)	Privilege to modify VPN configuration	modify, base, vpn
Monitoring	Privilege to modify the configuration from Stormshield Network Real-Time Monitor	modify, base, mon_write
Content filtering	Privilege for URL filtering, Mail, SSL and antivirus management	modify, base, contentfilter
PKI	Privilege to modify PKI	modify, base, pki
Objects	Privilege to modify Object database	modify, base, object
Users	Privilege to modify Users	modify, base, user
Network	Privilege to modify network configuration (interfaces, bridges, dialups, VLANs and dynamic DNS configuration)	modify, base, network
Routing	Privilege to modify routing (default route, static routes and trusted networks)	modify, base, route
Maintenance	Privilege to perform maintenance operations (backups, restorations, updates, Firewall shutdown and reboot, antivirus update, modification of antivirus update frequency, High Availability modification and RAID-related actions in Real-Time Monitor)	modify, base, maintenance
Intrusion prevention	Privilege to modify Intrusion prevention (IPS) configuration	modify, base, asq
Vulnerability manager	Privilege to modify vulnerability management configuration (Stormshield Network Vulnerability Manager)	modify, base, pvm
Objects (global)	Privilege to access global objects	modify, base, globalobject
Filter (global)	Privilege to access the global filter policy	modify, base, globalfilter

The *base* privilege is assigned to all users systematically. This privilege allows reading the whole configuration except filtering, VPN, logs and content filtering. The *modify* privilege is assigned to users who have write privileges. The user who has logged on as admin will obtain

the *admin* privilege. This is the only privilege that allows giving other users administration privileges or removing them.

9.2 SA states

-	Undetermined
Larval	The SA is in the process of being negotiated or has not been completely negotiated.
Mature	The SA has been established and is available; the VPN tunnel has been correctly set up.
Dying	The SA will soon expire; A new SA is in the progress of being negotiated.
Dead	The SA has expired and cannot be used; The tunnel has not been set up and is therefore no longer active.
Orphan	A problem has occurred, in general this status means that the tunnel has been set up in only one direction.

10. Frequently asked questions

1) What is the meaning of the message: “Impossible to locate the machine on x.x.x.x”?

2) How can I check the IP address (es) really assigned to the Firewall?

3) What is the meaning of the message: ‘You lost the MODIFY privilege’?

4) What is the meaning of the message: ‘The operation has exceeded the allotted time’?

5) How do I know if there has been an attempted intrusion?

6) It is possible to allow protocols other than IP?

1) What is the meaning of the message “Impossible to locate the machine on x.x.x.x”?

This message means that the host on which you are connected cannot reach the Firewall by the IP address you have specified in the connection window. This may be for one of several reasons.

Check:

- That the IP address which you have specified in the connection window is that of the Firewall (that of the internal interface in advanced mode),
- That your host has indeed a different IP address from the Firewall but is on the same sub-network,
- That the connections are properly in place (use a crossover cable only if you are connecting the Firewall directly to a host or a router. Type "**arp -a**" in a DOS window under Windows to see if the PC recognizes the Stormshield Network firewall’s physical address (Ethernet). If it doesn’t, check your cables and the physical connections to your hub.
- That you have not changed the firewall’s operating mode (transparent or advanced),
- That the firewall recognizes the IP address (see “How can I check the IP address (es) really assigned to the Firewall?”).
- That the access provider for the graphical interface has not been deactivated on the Firewall.

2) How can I check the IP address (es) really assigned to the Firewall?

If you wish to check the IP address (es) or the operating mode (transparent or advanced) you need only connect to the Firewall in console mode. To do so you can either conduct an SSH session on the Firewall (if SSH is active and authorized) or connect directly to the firewall by the serial port or by connecting a screen and a keyboard to the firewall.

Once connected in console mode (with the admin login) type the command "**ifinfo**". This will give you the network adapter configuration and the present operating mode.

3) What is the meaning of the message ‘You lost the MODIFY privilege’?

Only one user can be connected to the Firewall with the MODIFY privilege. This message means that a user has already opened a session with this privilege.

In order to force this session to close, you need only connect, adding an exclamation mark before the user’s name (!admin).

WARNING

If an administrator session is open on another machine with the MODIFY right, it will be closed.

4) What is the meaning of the message 'The operation has exceeded the allotted time'?

As a security measure any connection between the firewall and the graphical interface is disconnected after a given time whether finished or not. In particular, this prevents an indefinite wait for a connection if the Firewall cannot be reached via the network.

5) How do I know if there has been an attempted intrusion?

Each attempted intrusion triggers a major or minor alarm, depending on its gravity and configuration. You are informed of these alarms in four ways:

- Firstly the LEDs on the front panel of the firewall light up (red) or flicker (yellow) to alert you.
- Then the alarms are logged in a specific file which you can consult from the graphical interface (**Stormshield Network Real-Time Monitor**),
- You can choose to receive alarm reports at a regular frequency (cf. *Receiving alarms*) via the firewall's web administration interface. This feature may be configured so that whenever an alarm is raised an e-mail is sent. When several alarms are raised in a short period, they will be sent in a collective e-mail
- **Stormshield Network Real-Time Monitor** displays alarms received in real time on the screen.

6) It is possible to allow protocols other than IP?

The Stormshield Network firewall can only analyze IP-based protocols. All protocols that the firewall does not analyze are regarded as suspicious and are blocked.

However, in transparent mode, Novell's IPX, IPv6, PPPoE, AppleTalk and NetBIOS protocols may be allowed through even though they are not analyzed.

documentation@stormshield.eu