



STORMSHIELD

EVENT REPORTER V. 1.2

USER CONFIGURATION MANUAL

| Date | Details |
|----------------|----------------|
| June 2014 | Creation |
| September 2014 | Update |
| November 2014 | Update |

Reference: snengde_snereporter-v1.2

FOREWORD

License

Products concerned

U30, U70, U120, U250, U450, U1100, U1500, U6000,
NG1000-A, NG5000-A,
U30S, U70S, U150S, U250S, U500S, U800S,
SN150, SN200, SN300,
SN500, SN700, SN900,
SN2000, SN3000, SN6000,
VS5, VS10, V50, V100, V200, V500 and VU.

Copyright © NETASQ 2014. All rights reserved.

Any copying, adaptation or translation of this material without prior authorization is **prohibited**.

The contents of this document relate to the developments in NETASQ'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.

NETASQ 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. NETASQ 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.

Notice



WEEE Directive

All NETASQ 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:

<http://www.netasq.com/recycling.html>



CONTENT

_Toc391901282

| | |
|---|-----------|
| 1. INTRODUCTION | 7 |
| 1.1 BASIC PRINCIPLES | 7 |
| 1.1.1 Who should read this user guide? | 7 |
| 1.1.2 Typographical conventions | 7 |
| 1.1.3 Vocabulary | 8 |
| 1.1.4 Getting help | 9 |
| 1.1.5 TECHNICAL ASSISTANCE CENTRE | 9 |
| 1.2 SOFTWARE INSTALLATION | 9 |
| 1.2.1 PRE-REQUISITES | 9 |
| 1.2.2 INSTALLING VIA YOUR PRIVATE AREA | 10 |
| 2 STORMSHIELD NETWORK EVENT REPORTER | 11 |
| 2.1 CONNECTION | 12 |
| 2.1.1 Access | 12 |
| 2.1.2 Connection | 13 |
| 2.1.3 Address book | 15 |
| 2.2 GETTING FAMILIAR WITH REPORTER | 19 |
| 2.2.1 PRESENTATION OF THE INTERFACE | 19 |
| 2.2.2 DESCRIPTION OF THE MENU BAR | 23 |
| 2.2.3 OPTIONS | 24 |
| 3 USING STORMSHIELD NETWORK EVENT REPORTER | 28 |
| 3.1 SOURCES | 28 |
| 3.1.1 Firewall | 28 |
| 3.2 GRAPHS | 29 |
| 3.2.1 Introduction | 29 |
| 3.2.2 Customizing | 29 |
| 3.3 CUSTOMIZING COLUMNS AND HEADERS | 31 |
| 3.3.1 Headers | 32 |
| 3.3.2 Columns | 33 |
| 3.3.3 Sorting by columns | 35 |
| 3.3.4 Contextual menu | 36 |
| 3.4 LOG TYPES | 36 |
| 3.4.1 "Network" logs | 36 |
| 3.4.2 "Services" logs | 38 |
| 3.4.3 "Statistics" Logs | 41 |
| 3.4.4 Miscellaneous | 44 |
| 3.5 DATA EXPORT | 45 |
| 3.5.1 Export | 45 |
| 3.5.2 Log format | 47 |



1. INTRODUCTION

1.1 BASIC PRINCIPLES

1.1.1 Who should read this user guide?

This manual is intended for network administrators or for users with the minimum knowledge of IP.

In order to configure your Stormshield Network Firewall in the most efficient manner, you must be familiar with these 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 the major TCP/IP services is also preferable:

- HTTP
- FTP
- Messagerie (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.

The better your knowledge of TCP/IP, the more efficient will be your filter rules and the greater your IP security.

1.1.2 Typographical conventions

1.1.2.1 Abbreviations

For the sake of clarity, the usual abbreviations have been kept. For example, **VPN** (*Virtual Private Network*). Other acronyms will be defined in the [glossary](#).

1.1.2.2 Display

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

| Menu **Interfaces**



1.1.2.3 Indications

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

NOTES/REMARKS

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

WARNING/RECOMMENDATION

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

TIP

This message gives 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.

1.1.2.4 Messages

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

Example: "Delete this entry?"

1.1.2.5 Examples

Example

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

1.1.2.6 Commands lines

Command lines

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

1.1.2.7 Reminders

Reminders are indicated as follows:

-  Reminder

1.1.2.8 Access to features

Access paths to features are indicated as follows:

-  Access the menu `File\Options`.

1.1.3 Vocabulary

| | |
|-----------------|--|
| Dialup | Interface on which the modem is connected. |
| Firewall | Stormshield Network UTM device /product |
| Logs | A record of user activity for the purpose of analyzing network activity. |



1.1.4 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.
- User manuals: Stormshield Network UNIFIED MANAGER, Stormshield Network REAL-TIME MONITOR and Stormshield Network EVENT REPORTER.

1.1.5 TECHNICAL ASSISTANCE CENTRE

Stormshield Network provides several means and tools for resolving technical problems on your firewall.

- A knowledge base.
- A certified distribution network. As such, you will be able to call on your distributor.
- 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".

1.2 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 "Presentation and installation of Stormshield Network products", [Ref. snengde_product-installation.pdf].*

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.

1.2.1 PRE-REQUISITES

The basic library corresponds to all the modules necessary for the other programs. 15.3 MB of hard disk space is necessary.

The minimum installation groups together:

- Stormshield Network Unified Manager: Graphical interface for the administration of Stormshield Network Firewalls
- Stormshield Network Real-Time Monitor: Real-time viewer of your Stormshield Network Firewall (2.58 MB)
- Stormshield Network Event Reporter: Log consultation and management on your firewall (140 MB)



The installation comprises all the graphic configuration tools of the Stormshield Network suite, which serve as the interface between the user and the appliance. These tools have to be installed on an administration workstation.

The Stormshield Network firewall is fully configured via a software program developed by NETASQ – Stormshield Network UNIFIED MANAGER. Using this program, you will be able to configure your firewall from a Windows workstation.

You will need the following elements in order to install this software:

- CPU with a minimum of 2GHz
- A minimum of 2 GB of RAM (Windows 7) for client software, 2 GB for server software.
- About 300MB of hard disk space as this is what the software will occupy after its installation. If possible, reserve several gigabytes of space for the database (depending on the activity of the connected firewall(s)).
- Ethernet 100 or 1000 Mbps network card

Software applications are supported on the following operating systems:

- Microsoft Windows 7 and 8,
- Microsoft Windows Server 2008 and 2012.

1.2.2 INSTALLING VIA YOUR PRIVATE 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.

1.2.2.1 Verification procedure

1.2.2.1.1 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.

-

1.2.2.1.2 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 menu **Properties** from the contextual menu that appears.
- 2** Select the **Digital signatures** tab then the name of the signor (NETASQ).
- 3** Click on **Details**: this window will indicate whether the digital signature is valid.



1.2.2.2 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.

2 STORMSHIELD NETWORK EVENT REPORTER

The EVENT REPORTER is a module of the Stormshield Network Firewall Administration Suite. This application program enables the display of log files generated by Stormshield Network Firewalls.

This data can be used to analyze your network activity, access to your computer systems, staff use of the Internet (web sites visited, email use...) in order to diagnose hacking attempts detected and blocked by the Firewall.

The data is displayed either in the form of tables, enabling a precise and detailed analysis, or in the form of graphs, thus providing a consolidated, global display of the data.

Stormshield Network EVENT REPORTER's logging functions enable displaying the events stored in each log file in one of the following ways:

- Selecting periods predefined in relation to the current date ("today", "this week", etc.) or defined manually,
- Sorting (ascending/descending) by the value in each field in which a security event has been captured
- Hierarchical classifications according to the value of one or several fields in which a security event has been captured.

WARNING

The version 1.0 of Stormshield Network EVENT REPORTER no longer supports Syslog (except the possibility to open/view a log file in Syslog UNIX, in **Tools Menu**) or any other form of database.

2.1 CONNECTION

2.1.1 Access

There are 2 ways to launch the Stormshield Network EVENT REPORTER application:

- Via the shortcut **Applications\Launch Stormshield Network EVENT REPORTER** in the menu bar on other applications in the Administration Suite.

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 appliance].

- Via the menu **Start\Programs\Stormshield Network \Administration Suite 1.0\Stormshield Network Event Reporter**.

A connection window or the main window will open:

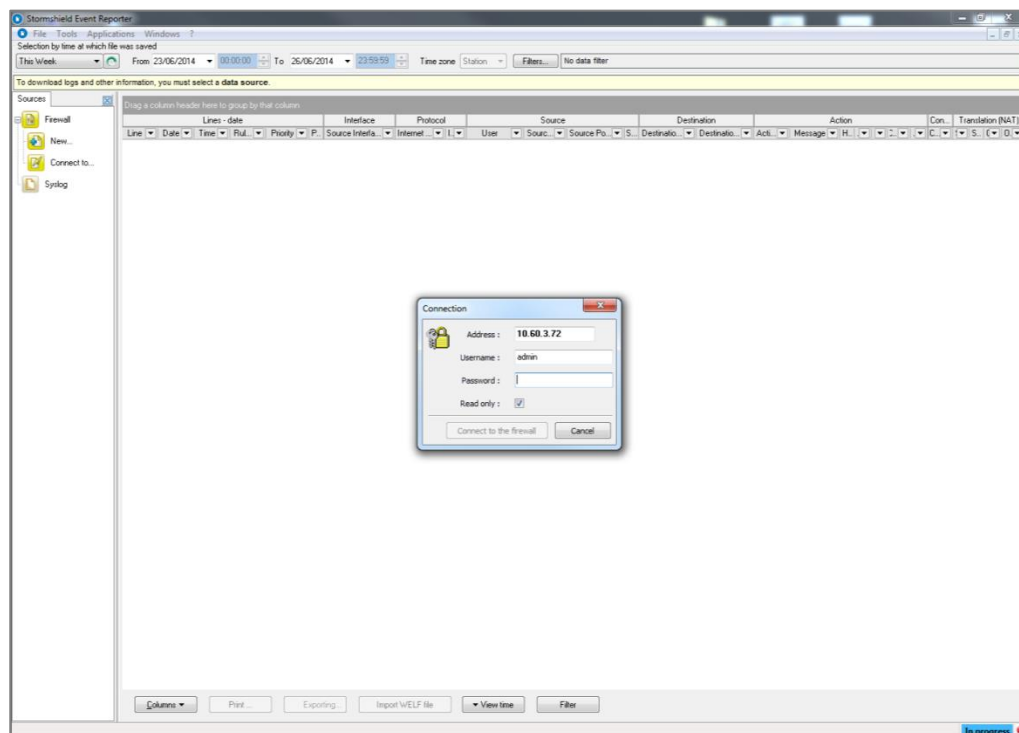


Figure 1: Connection



2.1.2 Connection

In the window “Connection”, you can select how you wish to view data:

When Stormshield Network EVENT REPORTER is executed from the “Windows” menu, Windows will check whether there is an address book. This address book, which is common to all Stormshield Network applications, may or may not be encrypted. If it is encrypted, or does not yet exist, there will be an additional step before connecting Stormshield Network EVENT REPORTER to the Firewall.

REMARK

A message appears when connecting to a firewall configured with its default password.

2.1.2.1 Direct connection to a Stormshield Network Firewall

REMARK

This connection is recommended if you have only one firewall and the amount of logs generated is fairly small.

If the address book exists and is encrypted (see the section *Part1/Chapter 2: Address Book* for more information on address book options), its password will be requested before every connection to Reporter on each registered Firewall.

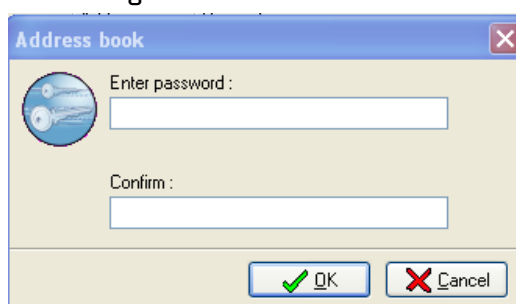


Figure 2: Address book - Password

Next, Stormshield Network EVENT REPORTER will display a log grid and a connection popup which allow you to enter connection information for a Firewall. This connection window can be accessed if the option **Connect to firewall** has been selected. (See section *Options*).

To connect to a Firewall, use the menu **Firewall** in the tab **Sources** in the menu directory and select a firewall. The following window will then open:

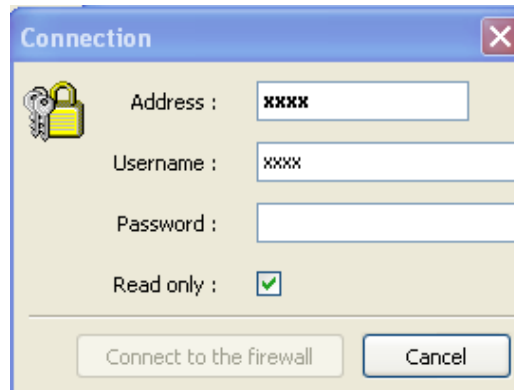


Figure 3: Connection

| | |
|------------------|--|
| Address | Stormshield Network Firewall's IP address or host name on the internal network |
| Username | User name for the configuration |
| Password | Password for the user. |
| Read only | Enables connecting to the Firewall in read-only mode. In this way, you can connect to the firewall without modification privileges using an account that ordinarily has these privileges. This allows avoiding the use of modification privileges if they are not necessary. |

REMARK

If Stormshield Network EVENT REPORTER has been launched from Stormshield Network UNIFIED MANAGER or Stormshield Network REAL-TIME MONITOR, Reporter will automatically connect to the Firewall that is connected to Manager or Monitor.

WARNING

The Stormshield Network Firewall is case-sensitive, both for the user name as well as for the password.

The option **Read Only** enables connecting to the Firewall in read-only mode. In this way, you can connect to the firewall without modification privileges using an account that ordinarily has these privileges.

TIP

You may connect to several Firewalls simultaneously by opening several windows (menu `File\Open`).

2.1.2.2 Connection via the menu Sources

REMARK

This connection mode is recommended if you have a fleet of firewalls.

If the option **Connect to firewall** has not been selected in the configuration of the service, the connection window will not appear. Instead, Stormshield Network EVENT REPORTER's main window will open.

To connect, click on the tab **Sources\Firewall**, then select the firewall(s) on which you would like reporting (see the CHAPTER Sources for more information on this connection).



2.1.3 Address book

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

The address book centralizes all passwords for access to different modules and other application in the Administration Suite.

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 **Encrypt address book**. In this case, you will be asked to enter an encryption key. For each Firewall, indicate a name (you can select any name, which does not necessarily have to correspond to the Firewall's name), IP address, password and serial number.

! WARNING

You are strongly advised to activate the encryption of the address book for obvious security reasons.

Once this information has been entered, you may save it using the **"Save"** button.

! WARNING

If you modify the "Encrypt address book" option, the address book has to be saved once more to apply the changes.

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

2.1.3.1 Adding an address

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

| | |
|--------------------|---|
| Name | The name of the firewall |
| Address | IP address of the firewall |
| User | The administrator account. |
| Password | Administrator password |
| Description | Description or comments regarding the firewall. |

2.1.3.2 Modifying the password for an address

The procedure for modifying the password for an address is as follows:

- 1** In the column "Password", double-click on the password for an address that needs to be changed. A window will open, allowing you to make the change.
- 2** Click on the **OK** button or close the address book. The following message will appear: "The address book has been modified. Save changes?"
- 3** Click on the **Yes** button to confirm changes.



2.1.3.3 Deleting an address

Pour supprimer un firewall du carnet d'adresses, suivez la procédure ci-dessous:

- 1 Select the firewall to delete.
- 2 Click on the **Delete** button. The following message will appear:
"Confirm removal of these items?"
- 3 Click on **Yes** to confirm removal.

2.1.3.4 Importing an address book

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

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

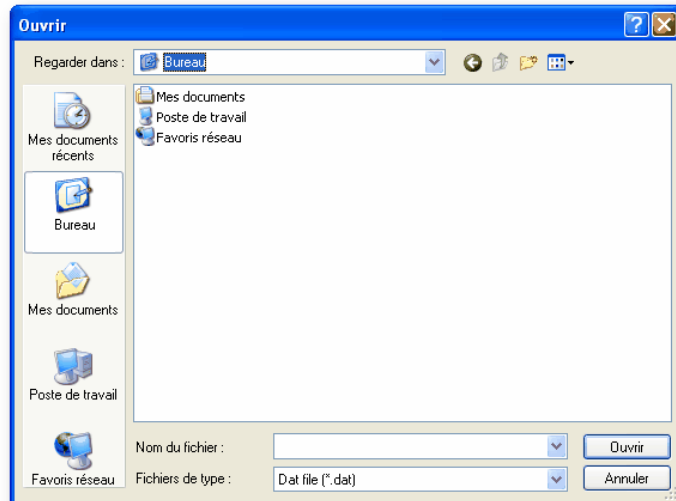


Figure 4: Importing an address book

- 2 Select the file to import.

 **REMARK**

The file to import should be in **.CSV** format.

- 3 Click on **Open**.

For obvious security reasons, the address book can be encrypted. To activate encryption, check the option **Encrypt address book**, then define the related password. This password is absolutely necessary for reading information contained in the address book. The address book is encrypted in AES, which is currently the most powerful symmetrical encryption algorithm.

2.1.3.5 Exporting an address book

All the information in the address book can be exported to be used, for example, for complementing another address book. The procedure for exporting an existing address book is as follows:

- 1 Click on the **Export** button. The following window will appear:
- 2 The following message will appear:
"Encrypt address book? (Highly recommended)"
- 3 If you click on **Yes**, you will be asked to enter the password for the address book before the save window appears:

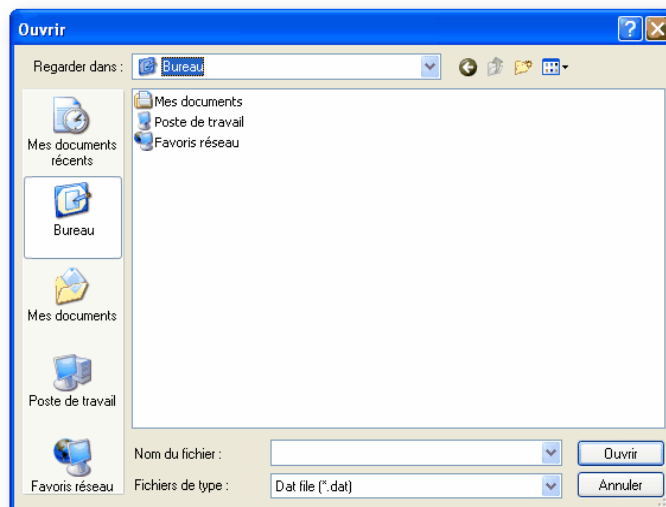


Figure 5: Exporting an address book

 **REMARK**

The file to export should be in .dat format.

- 4 Click on **Save**.

2.2 GETTING FAMILIAR WITH REPORTER

2.2.1 PRESENTATION OF THE INTERFACE

2.2.1.1 Main window

Once you are connected to the Firewall, Reporter's main window appears.

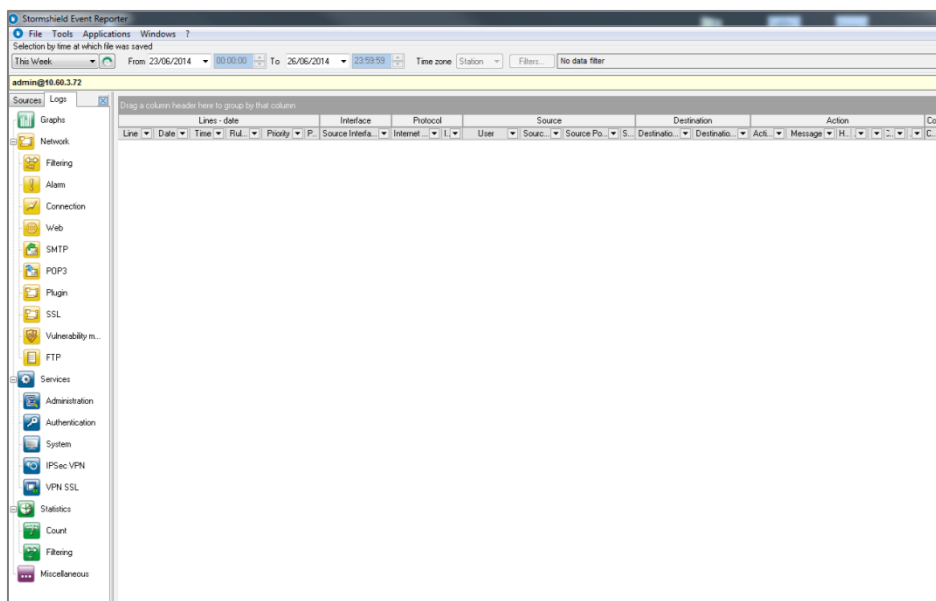


Figure 6: Main window

It comprises six parts:

- A menu bar.
- A menu directory (to the left of the screen)
- A date and filter selection bar (allowing only the analysis of data in the chosen period).
- A result display zone.
- An action bar
- A status bar.

2.2.1.2 Menu bar

The main window contains the following options:

| | |
|---------------------|--|
| File | Allows you to connect to the firewalls and to access options in the application. |
| Applications | Allows you to directly launch the two other applications that make up the Stormshield Network Administration Suite: UNIFIED MANAGER and REAL-TIME MONITOR. |
| Windows | Position of the windows and icons in the application. |
| ? (Help) | Allows access to the current help file and to find out Reporter's version. |



2.2.1.3 Menu directory

The menu directory consists of 2 tabs:

| | |
|----------------|--|
| Sources | Enables specifying the source of the viewed logs (firewall). |
| Logs | Concentrates all the operations in order to analyze data. |

2.2.1.3.1 Sources tab

The **Sources** tab enables connection to different log sources provided by Stormshield Network for the analysis of logs and events raised by the Firewall.

| | |
|-----------------|--|
| Firewall | When directly connected to the Firewall, this log retrieval method makes it possible to dispense with the use of log centralization tools. However, it does not allow centralizing the logs of several Firewalls, which is usually essential for analyzing an event that is spreading on several company sites. Furthermore, this method is only available for appliances that have a hard disk, as without it, logs cannot be saved directly on the Firewall. |
|-----------------|--|

(These three actions in the **Sources** tab are explained in [the Part 3/Chapter 1: Sources](#) in this manual).

2.2.1.3.2 Logs tab

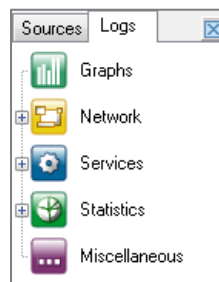







Figure 7: "Logs" tab

This tab contains five options, each distinguished by a colored icon:

| | |
|---|---|
|  Graphs | Enables you to display - in the form of on-line graphs, vector graphs or histograms - different types of Firewall data (security and system indicators, processor consumption, throughput on different interfaces, quality of service). |
|  Network | Enables you to display - in the form of tables - all types of Firewall logs, which are divided into 8 tables: Filter, alarms, connection, web, SMTP, POP3, plugin and Vulnerability Manager. |
|  Services | Enables viewing different types of information and messages (administration on the Firewall, authentication information and errors or IPSec and SSL VPN information and errors) in the form of tables. |
|  Statistics | Enables you to display - in the form of tables - different types of statistics (counters, filter rules created and address translation). |
|  Miscellaneous | Enables you to retrieve various log data. It is also possible to generate a file containing the addresses of all the Internet sites consulted. |



Selecting an entry that is already displayed will refresh data.



2.2.1.4 Date and filter selection bar

2.2.1.4.1 Selecting the date

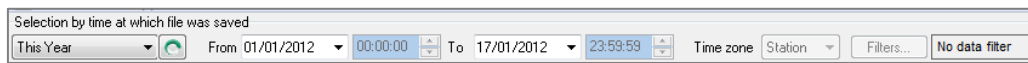


Figure 8: Selecting the date

This bar enables you to define the period over which you wish to retrieve data. You may choose from among a number of pre-defined periods:

- Manual selection
- Last hour
- Last six hours
- Today
- Yesterday
- This week
- This month
- This year
- Last week
- Last month
- Last year
- All
- Last lines

2.2.1.4.2 Filters

You can select the filters to be applied on the columns and perform multi-criteria searches using the selection button (see the section Part 3/Chapter 5: [“Filter Constructor in this manual”](#)).

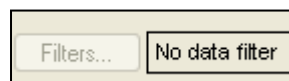


Figure 9: Filters

The selection of this option enables you to constitute data filters on each column. When you activate this option, an arrow pointing downwards (▼) appears at the far right of the columns. By selecting one of the pre-entered values or entering a value of your own choice, you automatically limit the table data to those corresponding to the filter on the selected column.

Then the arrow turns navy blue and the actual filter appears at the bottom of the table. A white cross enables you to delete all the active filters at once.

2.2.1.5 Result display zone

Data and options from the selected menus appear in this zone, in the form of graphs or tables.

NOTE

These windows will be explained in further detail in the corresponding chapters.

2.2.1.6 Status bar



Figure 10: Status bar

This bar comprises 5 information zones:

- A text zone displaying Reporter's activity in real time,
- A progress bar allowing an estimate of the duration of the operation,
- A zone displaying the application's status (whether processing is in progress or not, respectively blue or green).
- An icon displaying the status of the connection with the firewall.

2.2.1.7 Action bar

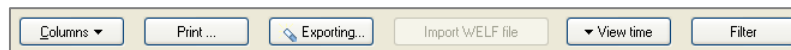


Figure 11: Action bar

2.2.1.7.1 Columns

| | |
|----------------------|--|
| Customize | The columns of the table may be moved around, removed or. This option enables you to select the columns you wish to display. A window comprising two tabs then appears, enabling you to manage column headers and the columns. To add or delete a column from the table, all you have to do is select the group of columns or column and drag it either into the table or into the tools window. |
| Reset | Enables you to restore the original column display |
| Best fit | Enables you to adapt the width of the columns to the width of the application |
| Fit to screen | Enables you to adapt the width of the columns to the width of the application |
| Show totals | Subtotaling of packet volumes (sent, received, duration) for all logs viewed. When you perform a sort (by dragging and dropping a column), a sub-total per sort may be viewed. |

2.2.1.7.2 Print

With this option, you are able to access a print preview menu.

2.2.1.7.3 Export

Displayed data may be exported for it to be used in other environments. A Wizard will assist you in this process. See [Chapter 6: Data Export](#).

2.2.1.7.4 See time

This option allows you to automatically calculate the date and time of the logs displayed in Reporter according to different time zones depending on:

- Your computer's time zone,
- The Firewall's time zone,
- GMT

Thus the date and time vary according to the option selected from those indicated above. Logs from a firewall in London (GMT) can therefore be consulted on a workstation in Paris (GMT+1).

**Example**

An "antispam update" event was detected at midnight (London time). If the user selects the option "Your computer's time zone", he will see this event at 1.00 a.m. (Paris time). However, if he selects the option "The Firewall's time zone", at midnight he will see whether the firewall has been configured as it should be in the London timezone.

2.2.2 DESCRIPTION OF THE MENU BAR

2.2.2.1 File menu

The **File** menu allows the following:

| | |
|---------------------|--|
| Open | Enables connecting directly to a Firewall via its protocol. |
| Address book | Access to the Stormshield Network Administration Suite's address book. |
| Options | General configuration of the application and log options. |
| Quit | Closes all connections and exits the application. |

2.2.2.2 Applications menu

The **Applications** menu enables connecting to other applications in the Administration Suite. Use these shortcuts instead of having to re-authenticate each time on each application.

| | |
|--|---|
| Launch Stormshield Network REAL-TIME MONITOR... | Enables opening the REAL-TIME MONITOR application from the Administration Suite. |
| Launch Stormshield Network UNIFIED MANAGER... | Enables opening the UNIFIED MANAGER application from the Administration Suite, in Global Administration mode. |

2.2.2.3 Windows menu

| | |
|------------------------|---|
| Arrange icons | Enables the organization of icons representing the Firewalls. |
| Cascade | Cascades the windows connected to Firewall. |
| Tile vertical | Enables vertically organizing windows which have not been reduced to icons. |
| Tile horizontal | Enables horizontally organizing windows which have not been reduced to icons. |

2.2.2.4 ? menu (help)

| | |
|----------------|--|
| Help | Displays a screen that accesses documentation in your secure-access area on the website. |
| License | Enables retrieving a new downloaded license from a directory. |
| About | Displays the "about" box, indicating the software version of Stormshield Network EVENT REPORTER. In the professional version, information on the REPORTER license is found here: license version, organization name, contact name, e-mail address, and unique user identification for technical support. |



2.2.3 OPTIONS

The **Options** sub-menu allows configuring the application, and logs.

➔ Go to the menu **File\Options** to configure these options.

2.2.3.1 General tab

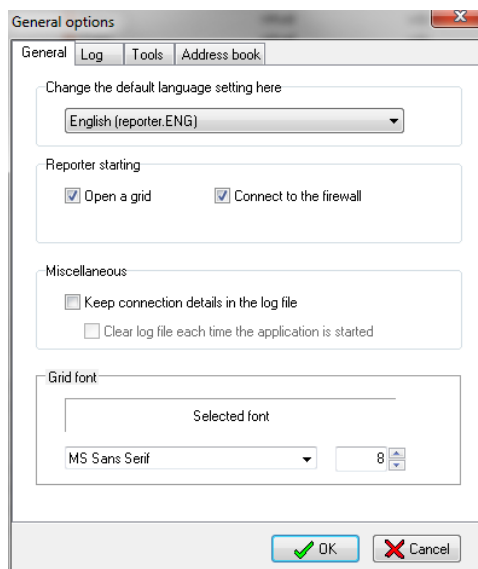


Figure 12: General options - General

2.2.3.1.1 Default language

The Stormshield Network EVENT REPORTER application is multilingual. Select the language required for the graphical interface.

2.2.3.1.2 At startup

2 options are possible:

- **Open a grid:** opens up a log grid when the application is opened.
- **Connection to the firewall:** Authorizes a direct connection to the firewall.

2.2.3.1.3 Miscellaneous

- **Keep connection logs in a file:** Enables you to generate logs concerning the application's behavior.
- **Empty the log file each time the application is started:** Enables you to have a file of limited volume and to keep active logs only for the purpose of the application in progress.

2.2.3.1.4 Grid font

This option allows you to specify the font and font size of the text which appears in the log grid.

2.2.3.2 Log tab

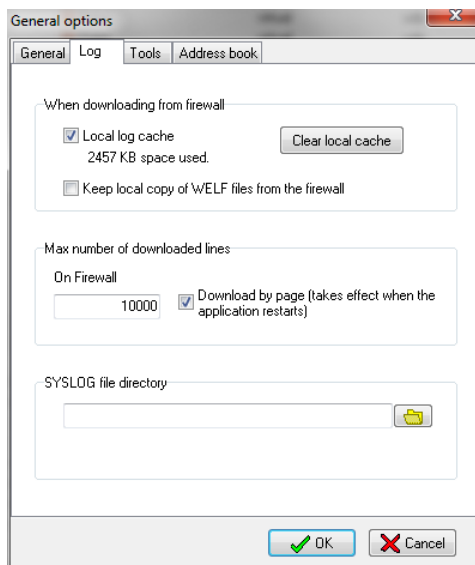


Figure 13: General options - Log

2.2.3.2.1 When downloading from firewall

- **Local log cache:** this option allows you to speed up log information searches which have already been performed. Data is no longer sent from the Firewall when this option is selected and when data has already been sent. This option is inactive when working on the current day.
- **Keep local copy of WELF files from the firewall:** Locally stores all the log files downloaded from the Firewall.

The **Clear local cache** button, as its name implies, allows you to purge the local cache of downloaded logs.

2.2.3.2.2 Maximum number of downloaded lines

This option allows you to specify the maximum number of lines downloaded for a connection to the Firewall. In order to facilitate loading and transforming logs, they can be displayed in 15,000 lines per page when you select the option **Download by page**. If the specified period contains more than the maximum number of lines, the logs will be loaded in cache, and a browsing system will enable the display of 15,000 lines per page each time (only in the case of logs directly downloaded from a Firewall).

Example

You have indicated that you wish to load a maximum of 500 log lines per page for the firewall. If the number of lines exceeds this number, the button will become Page 1/2.

REMARK

This only applies to logs that have been directly downloaded from a Firewall.

2.2.3.3 Tools tab

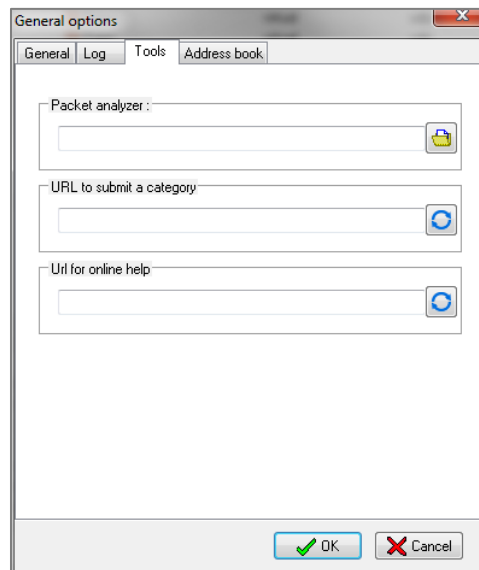


Figure 14: General options - Tools tab

2.2.3.3.1 Packet analyzer

When an alarm is raised on a Stormshield Network Firewall, the packet that set off the alarm can be viewed. You will need a packet viewer such as Wireshark or Packetyzer to do this. Specify the viewer to be used in the “Packet analyzer” field, so that Reporter can use it to display malicious packets.

2.2.3.3.2 URL to submit a category

Administrators of Stormshield Network Firewalls cannot edit listed and categorized URL groups. However, certain URLs may turn out to be wrongly categorized or are not in the list. To add URLs to the list, administrators can submit these URLs to the website [<https://mystormshield.eu/>].

There are two ways of submitting URLs: by connecting directly to the website to manually specify the URL, or when the URL appears in Reporter’s tables, by using the contextual menu of the Web grid in Reporter so that the submission will be automatic. In order to do this, the URL to be submitted has to be specified in the “URL to submit a category” field in Reporter.

2.2.3.3.3 URL for online help

The address shown here allows you to access the online help Stormshield Network.

2.2.3.4 Address book tab

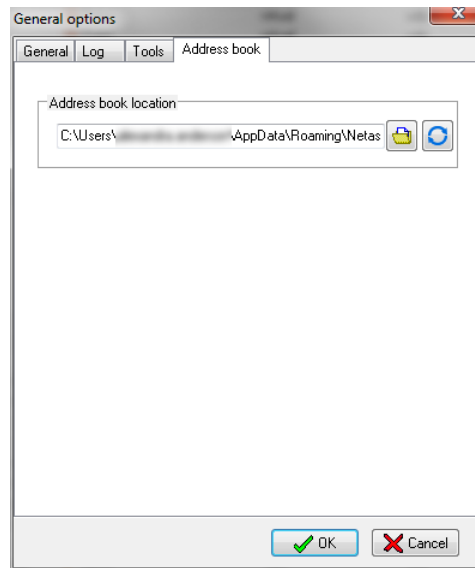


Figure 15: General options - Address book tab

- **Location of the address book:** the Stormshield Network UNIFIED MANAGER, Stormshield Network REAL-TIME MONITOR and Stormshield Network EVENT REPORTER applications use the same address book and therefore the same address book file.

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



3 USING STORMSHIELD NETWORK EVENT REPORTER

3.1 SOURCES

The **Sources** tab in the menu directory enables specifying the source of logs viewed (Firewall).

The **Sources** tab enables connection to different log sources provided by Stormshield Network for the analysis of logs and events raised by the Firewall.

3.1.1 Firewall

When directly connected to the Firewall, this log retrieval method makes it possible to dispense with the use of centralization tools. However, it does not allow centralizing the logs of several Firewalls, which is usually essential for analyzing an event that is spreading on several company sites. Furthermore, this method is only available for appliances that have a hard disk, as without it, logs cannot be saved directly on the Firewall. *(See the section [Connection](#) for more information.)*

3.1.1.1 Ways of connecting to the Firewall

A **Firewall** connection in the **Sources** tab enables performing three connection-related actions:

- **New:** By clicking on this option, the address book opens automatically on the list of registered Firewalls. This enables saving the address book of a new Firewall.
- **Connect to the Firewall:** By clicking on this option, the connection window appears and allows connections to the Firewall without the need to register it.

REMARKS

- 1) If a firewall was already connected, the following message will appear before the connection screen appears: "Confirm disconnection?".
 - 2) If you wish to remain connected while connecting to another firewall, access the menu bar and select **File\Open**. A connection window will open, allowing you to authenticate in order to access another firewall. You can be connected simultaneously to as many firewalls as you wish.
- **Firewall_{xx}:** lastly, this option provides direct access to the list of registered Firewalls, allowing quick connection to the selected Firewall.



3.2 GRAPHS

3.2.1 Introduction

Reporter is capable of analyzing the Firewall's activity. The **Graphs** menu in Reporter enables the display of Security and System events, the use of the firewall's processor, indicators of vulnerability levels supplied by Stormshield Network Vulnerability Manager, throughput on the appliance's interfaces as well as the use of each QoS rule.

3.2.2 Customizing

When you select the **Graphs** menu in the directory, the customization screen will appear at the same time as the graphs. You may close this screen at any time.



TIP

Click on the graph zone to open the window "Customize graph" again if you have closed it.

3.2.2.1 Security indicators and system events

3.2.2.1.1 Security

The security indicator is linked to the monitoring of alarm and events relating to the ASQ kernel.

The security indicator is weighted in several elements:

- **Minor alarms:** indicators of the number of minor alarms.
- **Major alarms:** indicators of the number of major alarms.
- **ASQ memory:** indicators of the amount of ASQ memory left.

The display of these indicators is based on the weighting of system events in relation to each other in order to present a coherent status of the Firewall (major alarms will have more weight than minor alarms).

3.2.2.1.2 System events

System indicators are linked to the monitoring of events relating to Ethernet interfaces supported by the Firewall processor.

System indicators concern:

- **Logs:** indicators relating to the occupation of space allocated to logs.
- **Ethernet:** indicators relating to interface connectivity.
- **CPU:** indicators relating to the load of the Firewall processor.
- **HA:** indicators relating to the high availability set-up, if this is present on the Firewall.
- **Server:** Indicators relating to some of the Firewall's critical servers

The display of these indicators is based on the weighting of system events in relation to each other in order to present a coherent status of the Firewall (major alarms will have more weight than minor alarms).



3.2.2.2 CPU load

This graph represents the processor's load.

- **User:** load attributable to processes that the user executes
- **Interruptions:** load represented by exchanges between the kernel and processes executed by the user
- **System events:** load attributable to the kernel

3.2.2.3 Vulnerability Manager

3.2.2.3.1 Vulnerabilities

Vulnerability indicators concern the following:

- Total
- Remote: refers to vulnerabilities that can be exploited remotely (via the network).
- Target server: vulnerability that affects a server application.
- Critical
- Minor
- Major
- Fixed: refers to vulnerabilities for which a fix is available.

3.2.2.3.2 Information

Information indicators concern the following:

- Total info
- Minor info
- Major info
- Monitored

3.2.2.4 Interfaces

3.2.2.4.1 List of interfaces

This section sets out the list of different interfaces (In, Out, Dmz).

3.2.2.4.2 Traffic by interface:

This section of the graphs represents the use of each interface on the Firewall. For every interface, four types of information are given:

- Incoming throughput: At a given moment.
- Maximum incoming throughput: Observed over the defined period.
- Outgoing throughput: At a **given moment**.
- Maximum outgoing throughput: Observed over the defined period.



3.2.2.5 QoS

3.2.2.5.1 List of QoS rules

This section sets out the list of different QoS (Qualities of service) defined on the firewall.

- DEFAULT
- HTTP
- DNS
- CIFS
- SSH_priq
- SSH_Ext
- Squid
- FTP

3.2.2.5.2 Traffic by QoS

- Incoming bandwidth: At a given moment.
- Maximum incoming bandwidth: Observed over the defined period.
- Outgoing bandwidth: At a given moment.
- Maximum outgoing bandwidth: Observed over the defined period.

3.2.2.6 Graphs options

3.2.2.6.1 Full precision for longs periods

When this option is checked, all the points in the period are taken into account. However, for very long periods, only certain significant points are taken in order to prevent the graph from getting too cramped.

3.2.2.6.2 Percentage of CPU up to 100%

When this option is selected, the scale at which the processor's load is plotted is dynamic. Therefore, if the processor's load is light, graphs (scale) will be adapted so that the administrator can read them. Otherwise, the maximum value of the scale will remain at 100% regardless of the maximum value obtained up until then.

3.3 CUSTOMIZING COLUMNS AND HEADERS

The names of the following columns correspond to the data that may be consulted in **Network** logs. These columns are grouped according to the type of data, under headers.

➔ To start customizing your headers and columns, open a log file in the **Logs** tab, click on the **Columns** button (in the action bar)**Customize**.



Figure 16: Button bar



3.3.1 Headers

Headers are thematic classifications of columns. Columns under the same header are placed adjacently.

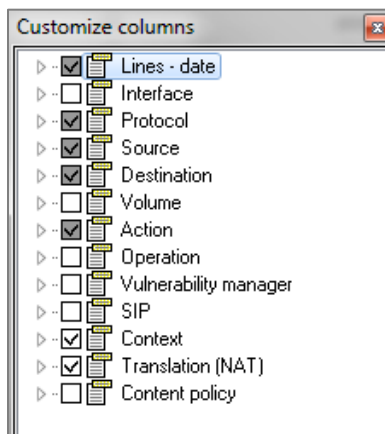


Figure 17: Customizing headers

- **Lines-date:** Information relating to the line and time of the packet's log
- **Interface:** Information relating to the interface through which the packet passed.
- **Protocol:** Information relating to the packet's protocol.
- **Source:** Information relating to the packet source.
- **Destination:** Information relating to the packet's destination
- **Volume:** Information relating to the packet's volume.
- **Action:** Information relating to the volumes of data in the packet.
- **Operation:** Information relating to the commands carried out when using protocols managed by plugins and proxies.
- **Vulnerability Manager:** Information relating to the VULNERABILITY MANAGER module.
- **SIP:** Information relating to media, caller and callee of the SIP plugin.
- **Context**
- **Translation (NAT)**
- **Content policy**

When you deselect an option that is linked to a header in the grid, the column will be deleted for that grid.

Example

For "Alarm" logs, you have deselected the header Line-date. The header and the options associated with it will be removed from the grid. The other log files will nonetheless maintain this header.

If you disconnect and reconnect to the firewall, changes to the customization will be saved.



3.3.2 Columns

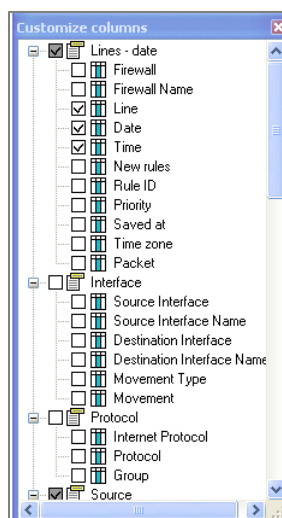


Figure 18: Customizing columns

3.3.2.1 Lines-date

- **Firewall:** Firewall's serial number
- **Firewall name:** Name of the firewall.
- **Line:** Number of the log line.
- **Date:** Date the log line was generated
- **Time:** Time the log line was generated.
- **Slot level:** Number corresponding to the classification of filter rules (local or global).
- **Rule ID:** Rule identifier.
- **Priority:** Alarm level (major or minor).
- **Saved at:** Time at which log was saved.
- **Timezone:** Firewall's timezone.
- **Packet:** Displays the packet which had raised the alarm. This feature has to be configured on Monitor in the Administration Suite.

3.3.2.2 Interface

- **Source interface:** Source interface's network adapter.
- **Source interface name:** Name of the source interface.
- **Destination interface:** Destination interface's network adapter.
- **Destination interface name:** Name of the destination interface.
- **Movement type:** Type of packet movement.
- **Movement:** Packet movement.

3.3.2.3 Protocol

- **Internet Protocol:** Internet Protocol
- **Protocol:** Base protocol.
- **Group:** Protocol group.

3.3.2.4 Source

- **Source name:** Source IP address or resolved name.
- **User:** Name of the authenticated user.



- **Source:** IP address.
- **Source port name:** Name of the source port.
- **Source port:** Source port number.

3.3.2.5 Destination

- **Destination:** Destination IP address.
- **Destination name:** Destination IP address or resolved name.
- **Destination port:** Destination port number.
- **Destination port name:** Name of the destination port.

3.3.2.6 Volume

- **Sent:** Amount of data sent.
- **Received:** Amount of data received.
- **Duration:** Connection duration

3.3.2.7 Action

- **Action:** Filter rule action: “none”, “pass”, “block”, “reset”.
- **Message:** Alarm.
- **Help:** Links to an explanation of the alarm raised.
- **Alarm ID:** Alarm’s identifier on the Firewall.
- **Repeat:** Number of times the alarm has been repeated within the duration specified in the Administration Suite.
- **Rule name:** This column contains the value specified in the “Name” field in the filter rule editor.
- **Class:** Class to which the raised alarm belongs.

3.3.2.8 Operation

- **Category:** Category to which the URL having caused the generation of logs belongs.
- **Category group:** category group containing the category to which the URL that set off the log function belongs.
- **Operation:** Protocol’s identified command.
- **Result:** Error message return code.
- **Argument:** Operation’s parameter.
- **Ads:** icon.
- **Spam level:** Spam level: 0 (message not considered spam) 1, 2 and 3 (spam) x (error when processing message) and ? (The nature of the message could not be determined).
- **Virus:** Indicates whether the e-mail contains a virus. Possible values are “safe”, “infected”, etc
- **Classification:** Generic category in which the alarm belongs (Examples: Protocol, Content_filtering, Web, Mail, FTP...)

3.3.2.9 Vulnerability Manager

- **Vuln ID:** Vulnerability identifier.
- **Family:** Family to which the vulnerability belongs.
- **Severity:** Level of the vulnerability’s criticality.
- **Solution:** “Yes” or “no”, depending on whether there is a solution suggested.
- **Exploit:** Indicates the location where a vulnerability can be exploited (2 possible options: locally or remotely).
- **Client target:** Client target.



- **Server target:** Server target.
- **Detected on:** Date on which the vulnerability was detected.

3.3.2.10 SIP

- **Media:** Indicates the type of media (control, audio, video, etc)
- **Caller:** Indicates the caller
- **Callee:** Indicates the party being called, i.e., callee

3.3.2.11 Context

- **Configuration id:** ID configuration

3.3.2.12 Translation (NAT)

- **Source address**
- **Source port**
- **Destination orig.**
- **Destination port orig.**


3.3.2.13 Content policy

- **ID Politique :** identifier of configuration policy in force.

3.3.3 Sorting by columns

Logs are displayed in a table that has certain properties which enhance data reading.

Firstly, it is possible to sort the data according to type (alphabetical, date, bytes etc.), in ascending or descending order. In order to do so, click on the header of the column selected. An arrow pointing upwards or downwards enables you to confirm that the sorting has been carried out.

A grouping system, in the form of nodes, enables you to isolate the data requested. A "drop" zone is placed above the table; it reads as follows: "Drag a column header here to group by that column". In order to group together the data of any one column, select the header of the column and drag it into this zone. The table will then change its form. The grouped column appears in the drop zone and the table displays the values resulting from this grouping, in the form of nodes. A  sign appears in front of the group values, enabling the expansion of the nodes. It is thus possible to group data together within the groups.

This feature applies to all logs files (**Network, Services and Statistics**).

Example

When you select the display of Web logs, it is possible to group data firstly according to the user and then according to the destination, in order to highlight the Internet consultations carried out by internal users.



| Classification | Action | Alarm ID | Destination Po... | |
|----------------|-------------------|----------|-------------------|------------------|
| Interface | Protocol | Source | | |
| Interface Name | Internet Protocol | User | Source Name | Source Port Name |

Figure 19: Sorting columns



The order of the table columns may be customized using the "drag and drop" mechanism. This can be done by right-clicking and keeping the mouse button depressed on the column whose order you wish to modify, then dropping it to its desired location. Two green arrows will help you to locate this new location.

Columns cannot be moved under a different header.

3.3.4 Contextual menu

In each log grid in Reporter, contextual menus (accessible by right-clicking with the mouse) enable the quick execution of specific actions. A maximum of three options are defined for the contextual menu (depending on the information on which you right-click):

- **Copy line to clipboard as WELF:** This option enables rewriting a line in the Reporter log grid to the clipboard to be used outside Reporter.
- **Submit URL to a category:** when you open the contextual menu after having selected a URL, this option allows sending the URL to the URL submission form on the website.
- **Go to xxxxxx:** when you open the contextual menu after having selected a destination, this option enables an HTTP connection attempt to this destination

3.4 LOG TYPES

Stormshield Network EVENT REPORTER allows you to view logs in the form of tables. These files comprise three menus:

- Network
- Services
- Statistics

3.4.1 "Network" logs

- **Filter:** logs generated by the filter rules. To obtain these logs, at least one of the filter rules must have the **Log** option.
- **Alarm:** alarms raised by the firewall.
- **Connection:** information on all the authorized connections having passed through the Firewall.
- **Web:** logs from visited web sites (HTTP plugin and HTTP proxy).
- **SMTP:** e-mail logs generated by the SMTP proxy. The SMTP proxy has to be activated for these logs to be available.



- **POP3:** e-mail logs generated by the POP3 proxy. The POP3 proxy has to be activated for these logs to be available.
- **SSL :** SSL: secure connection logs (HTTPS)
- **Plugins:** information regarding plugins activated on your Firewall (except the HTTP plugin).
- **FTP:** Transferred log files (FTP proxy).

(See Customizing columns and header, Part 3, CHAPTER to get a better description of the table).

NOTES

Web and plugin logs can no longer be merged, as they will become independent again. The name of the intrusion prevention profile will be displayed in the Alarms, Connection and Filter logs.

3.4.1.1 Web

Right-clicking on a destination name will display the contextual menu that allows you to:

- **Submit URL to a category:** when you open the contextual menu after having selected a URL, this option allows sending the URL to the URL submission form on the website.

This form will also enable putting a URL into a category and to submit a new URL category.

3.4.1.2 Vulnerability Manager

21 fields are used:

- **Line:** Line number in the logs.
- **Date:** Date on which recorded logs were generated.
- **Time:** Time at which recorded logs were generated.
- **Internet Protocol:** Name of the internet protocol used.
- **Protocol:** Name of the protocol used.
- **User:** Connection identifier.
- **Source name:** source address of the connection.
- **Source port name:** source port of the connection.
- **Message:** command line sent to the firewall.
- **Argument:** complementary information associated with the log line (contacted web page).
- **Vuln ID:** Vulnerability identifier
- **Family:** Family type to which the vulnerability belongs.
- **Severity:** Level of criticality of the vulnerability.
- **Solution:** Indicates with a “yes” or “no” whether a solution is offered.
- **Exploit:** The solution may be accessed locally or remotely (via the network). It allows exploitation of the vulnerability.
- **Product:** Name of the client application.
- **Service:** Name of the server application.
- **Detail:** self-explanatory
- **Client target:** Client target
- **Server target:** Server target
- **Detected:** Date on which the vulnerability was detected.



3.4.1.3 FTP

11 fields are used:

- **Line:** Line number in the logs.
- **Date:** Date on which recorded logs were generated.
- **Time:** Time at which recorded logs were generated.
- **User:** Connection identifier.
- **Source name:** source address of the connection.
- **Destination name:** destination address of the connection.
- **Destination port name:** destination address port of the connection.
- **Received:** Volume received.
- **Action:** Action to perform – “Pass”, “Block” or “Scan”.
- **Message:** command line sent to the firewall.
- **Operation:** Indicates FTP commands (LIST, RETR, QUIT...)
- **Virus:** Indicates the name of the detected virus.

3.4.2 "Services" logs

3.4.2.1 Introduction

5 services are available:

- Administration
- Authentication
- System
- IPSec VPN
- SSL VPN

3.4.2.2 Administration

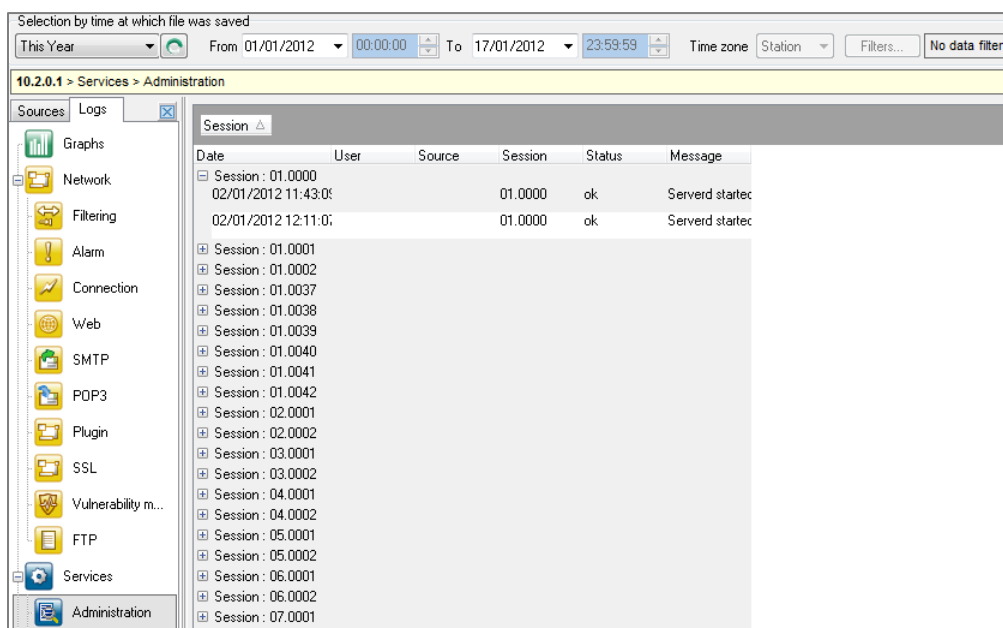


Figure 20: Administration

A history of all commands transmitted to the Firewall is given in this sub-menu.

11 fields are used:

- **Firewall:** Firewall's serial number.
- **Date:** Date on which the entry was generated
- **Time:** Time at which the entry was generated.
- **Line:** Line number in the log file.
- **Date-time:** Date and time on which the entry was generated.
- **Result:** error message.
- **User:** connection identifier,
- **Source:** connection's source address
- **Session id:** 00.0000 format. The first two digits correspond to the number times the Firewall has been reinitialized; the following 4 correspond to the number of connections on the Firewall
- **Message:** command line sent to the Firewall.
- **Timezone:** Firewall's time zone at the moment of writing the log.

3.4.2.3 Authentication



| Date | User | Source | Method | Status |
|---------------------|------|-------------|--------|-------------|
| 01/01/2012 01:24:16 | | 10.2.22.1 | SSL | ok |
| 01/01/2012 01:42:14 | | 10.2.27.1 | SSL | Auth failed |
| 01/01/2012 01:42:14 | | 10.2.27.1 | SSL | Auth failed |
| 01/01/2012 01:42:20 | | 10.2.27.1 | SSL | Auth failed |
| 01/01/2012 01:42:21 | | 10.2.27.1 | SSL | ok |
| 01/01/2012 02:17:49 | | 10.2.200.40 | PLAIN | ok |
| 01/01/2012 05:24:16 | | 10.2.22.1 | SSL | ok |
| 01/01/2012 05:45:02 | | 10.2.27.1 | SSL | ok |
| 01/01/2012 09:24:17 | | 10.2.22.1 | SSL | ok |
| 01/01/2012 09:45:57 | | 10.2.27.1 | SSL | ok |
| 01/01/2012 13:24:17 | | 10.2.22.1 | SSL | ok |
| 01/01/2012 13:46:57 | | 10.2.27.1 | SSL | ok |
| 01/01/2012 17:24:18 | | 10.2.22.1 | SSL | ok |
| 01/01/2012 17:47:51 | | 10.2.27.1 | SSL | ok |
| 01/01/2012 21:24:18 | | 10.2.22.1 | SSL | ok |
| 01/01/2012 21:49:16 | | 10.2.27.1 | SSL | Auth failed |
| 01/01/2012 21:49:16 | | 10.2.27.1 | SSL | Auth failed |
| 01/01/2012 21:49:26 | | 10.2.27.1 | SSL | Auth failed |
| 01/01/2012 21:49:49 | | 10.2.27.1 | SSL | Auth failed |

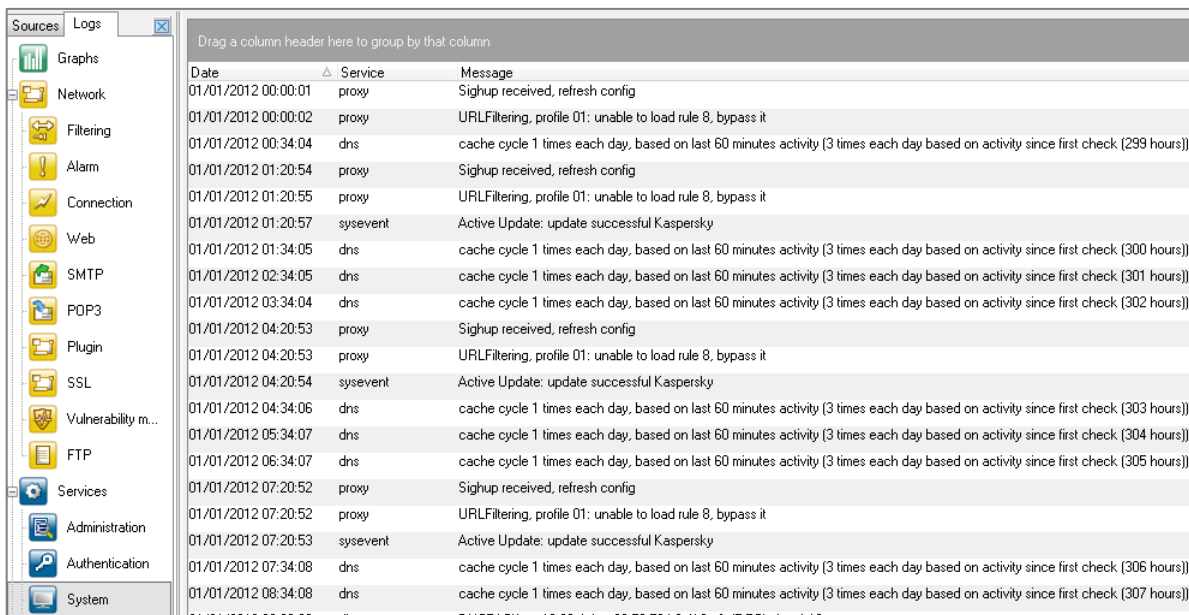
Figure 21: Authentication

This sub-menu provides a history of authentication requests.

Several fields are used:

- **Firewall:** Firewall's serial number
- **Date:** Date on which entry was generated
- **User:** user seeking authentication,
- **Source:** address requesting authentication
- **Result:** Error message.
- **Message:** return message for the request.

3.4.2.4 System




| Date | Service | Message |
|---------------------|----------|--|
| 01/01/2012 00:00:01 | proxy | Sighup received, refresh config |
| 01/01/2012 00:00:02 | proxy | URLFiltering, profile 01: unable to load rule 8, bypass it |
| 01/01/2012 00:34:04 | dns | cache cycle 1 times each day, based on last 60 minutes activity (3 times each day based on activity since first check (299 hours)) |
| 01/01/2012 01:20:54 | proxy | Sighup received, refresh config |
| 01/01/2012 01:20:55 | proxy | URLFiltering, profile 01: unable to load rule 8, bypass it |
| 01/01/2012 01:20:57 | sysevent | Active Update: update successful Kaspersky |
| 01/01/2012 01:34:05 | dns | cache cycle 1 times each day, based on last 60 minutes activity (3 times each day based on activity since first check (300 hours)) |
| 01/01/2012 02:34:05 | dns | cache cycle 1 times each day, based on last 60 minutes activity (3 times each day based on activity since first check (301 hours)) |
| 01/01/2012 03:34:04 | dns | cache cycle 1 times each day, based on last 60 minutes activity (3 times each day based on activity since first check (302 hours)) |
| 01/01/2012 04:20:53 | proxy | Sighup received, refresh config |
| 01/01/2012 04:20:53 | proxy | URLFiltering, profile 01: unable to load rule 8, bypass it |
| 01/01/2012 04:20:54 | sysevent | Active Update: update successful Kaspersky |
| 01/01/2012 04:34:06 | dns | cache cycle 1 times each day, based on last 60 minutes activity (3 times each day based on activity since first check (303 hours)) |
| 01/01/2012 05:34:07 | dns | cache cycle 1 times each day, based on last 60 minutes activity (3 times each day based on activity since first check (304 hours)) |
| 01/01/2012 06:34:07 | dns | cache cycle 1 times each day, based on last 60 minutes activity (3 times each day based on activity since first check (305 hours)) |
| 01/01/2012 07:20:52 | proxy | Sighup received, refresh config |
| 01/01/2012 07:20:52 | proxy | URLFiltering, profile 01: unable to load rule 8, bypass it |
| 01/01/2012 07:20:53 | sysevent | Active Update: update successful Kaspersky |
| 01/01/2012 07:34:08 | dns | cache cycle 1 times each day, based on last 60 minutes activity (3 times each day based on activity since first check (306 hours)) |
| 01/01/2012 08:34:08 | dns | cache cycle 1 times each day, based on last 60 minutes activity (3 times each day based on activity since first check (307 hours)) |

Figure 22: System

This sub-menu provides a history of messages linked to Firewall services.

3.4.2.5 IPSec VPN



| Date | Result | phase | Source | Destination |
|---------------------|--------|-------|-----------------|-------------|
| 01/01/2012 04:18:00 | Info | 1 | Firewall_bridge | gw |
| 01/01/2012 04:18:59 | Info | 2 | Firewall_bridge | gw |
| 01/01/2012 04:19:18 | Info | 2 | Firewall_bridge | gw |
| 01/01/2012 05:07:00 | Info | 2 | Firewall_bridge | gw |
| 01/01/2012 05:07:19 | Info | 2 | Firewall_bridge | gw |
| 01/01/2012 05:55:01 | Info | 2 | Firewall_bridge | gw |
| 01/01/2012 05:55:20 | Info | 2 | Firewall_bridge | gw |
| 01/01/2012 06:43:02 | Info | 2 | Firewall_bridge | gw |
| 01/01/2012 06:43:21 | Info | 2 | Firewall_bridge | gw |
| 01/01/2012 07:31:03 | Info | 2 | Firewall_bridge | gw |
| 01/01/2012 07:31:22 | Info | 2 | Firewall_bridge | gw |
| 01/01/2012 08:19:04 | Info | 2 | Firewall_bridge | gw |
| 01/01/2012 08:19:23 | Info | 2 | Firewall_bridge | gw |
| 01/01/2012 09:06:00 | Info | 1 | Firewall_bridge | gw |
| 01/01/2012 09:06:01 | Info | 1 | Firewall_bridge | gw |
| 01/01/2012 09:06:01 | Info | 1 | Firewall_bridge | gw |
| 01/01/2012 09:07:05 | Info | 2 | Firewall_bridge | gw |
| 01/01/2012 09:07:24 | Info | 2 | Firewall_bridge | gw |
| 01/01/2012 09:55:07 | Info | 2 | Firewall_bridge | gw |
| 01/01/2012 09:55:26 | Info | 2 | Firewall_bridge | gw |
| 01/01/2012 10:43:08 | Info | 2 | Firewall_bridge | gw |
| 01/01/2012 10:43:27 | Info | 2 | Firewall_bridge | gw |

Figure 23: IPSec VPN

This sub-menu provides a history of events concerning IPSec VPN.



Several fields are used:

- **Date:** Date on which entry was generated
- **Result:** Error message.
- **Phase:** SA negotiation phase (*Corresponds to a VPN tunnel endpoint*)
- **Source:** connection's source address
- **Destination:** connection destination address,
- **Message:** Message regarding the attempt to set up a tunnel
- **User:** user identifier (in the context of an anonymous tunnel),
- **Initiator Cookie:** "Initiator" identifier for the negotiation session in progress,
- **Receiving Cookie:** "Responder" identifier for the negotiation session in progress.
- **Spi in:** identifier for the ingoing SA.
- **Spi out:** identifier for the outgoing SA.

3.4.2.6 VPN SSL

This sub-menu provides a history of events concerning VPN SSL.

Several fields are used:

- **Date:** Date on which entry was generated
- **Result:** Result of the SSL VPN connection to the selected server
- **Port:** server connection port
- **Source:** connection's source address
- **Destination:** connection destination address
- **Message:** Message relating to the SSL VPN connection
- **User:** user identifier
- **Argument:** additional information regarding the log line (*web page contacted*)

3.4.3 "Statistics" Logs

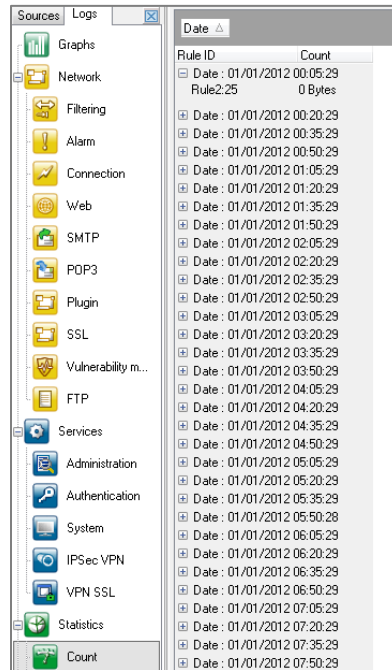
3.4.3.1 Introduction

2 types of statistical analyses are available:

- Counters,
- Filters,

3.4.3.2 Counters

This table corresponds to the number of times a rule has been activated. To display information in this zone, the **Count** option must have been activated in the filter rules.



| Rule ID | Count |
|----------------------------|---------|
| Date : 01/01/2012 00:05:29 | |
| Rule2:25 | 0 Bytes |
| Date : 01/01/2012 00:20:29 | |
| Date : 01/01/2012 00:35:29 | |
| Date : 01/01/2012 00:50:29 | |
| Date : 01/01/2012 01:05:29 | |
| Date : 01/01/2012 01:20:29 | |
| Date : 01/01/2012 01:35:29 | |
| Date : 01/01/2012 01:50:29 | |
| Date : 01/01/2012 02:05:29 | |
| Date : 01/01/2012 02:20:29 | |
| Date : 01/01/2012 02:35:29 | |
| Date : 01/01/2012 02:50:29 | |
| Date : 01/01/2012 03:05:29 | |
| Date : 01/01/2012 03:20:29 | |
| Date : 01/01/2012 03:35:29 | |
| Date : 01/01/2012 03:50:29 | |
| Date : 01/01/2012 04:05:29 | |
| Date : 01/01/2012 04:20:29 | |
| Date : 01/01/2012 04:35:29 | |
| Date : 01/01/2012 04:50:29 | |
| Date : 01/01/2012 05:05:29 | |
| Date : 01/01/2012 05:20:29 | |
| Date : 01/01/2012 05:35:29 | |
| Date : 01/01/2012 05:50:28 | |
| Date : 01/01/2012 06:05:29 | |
| Date : 01/01/2012 06:20:29 | |
| Date : 01/01/2012 06:35:29 | |
| Date : 01/01/2012 06:50:29 | |
| Date : 01/01/2012 07:05:29 | |
| Date : 01/01/2012 07:20:29 | |
| Date : 01/01/2012 07:35:29 | |
| Date : 01/01/2012 07:50:29 | |

Figure 24: Count

3 fields are available:

- **Date:** Date on which entry was generated
- **Rule ID:** Rule identifier.
- **Count:** Indicates the number of megabytes.

1.1.1.1.1. Filtering

3.4.3.2.1 3.4.3.3.1 Filter stats

- **Date:** Date on which entry was generated
- **Firewall:** Firewall's serial number or name (if known).
- **Time:** Time at which entry was generated.
- **Line:** Line number in the log file.
- **Date-Time:** Date and time on which the entry was generated.
- **Saved evaluation:** Number of rule evaluations that could not be performed because of the ASQ technology.
- **Fragmented:** Number of fragmented packets transmitted through the firewall.
- **Timezone:** Firewall's time zone at the moment of writing the log.
- **Slot:** Number of the activated policy.
- **Real host**
- **Host:** Memory allocated to a host.
- **Fragmented:** Number of fragmented packets transmitted through the firewall.
- **ICMP:** Memory allocated to ICMP.
- **Connection:** Memory allocated to connections.
- **Dynamic:** Percentage of ASQ memory being used.

3.4.3.2.2 3.4.3.3.2 Memory

- **Logged:** Number of log lines generated
- **Log overflow:** Number of log lines lost.
- **Accepted:** Number of packets matching “Pass” rules
- **Blocked:** Number of packets matching “Block” rules

3.4.3.2.3 3.4.3.3.3 Rules

- **Rule (n:nn):** Number of times that a rule has been applied to a packet. In brackets, the first number

Indicates the number of the policy and the second refers to the number of the rule in this policy.

3.4.3.2.4 3.4.3.3.4 Bytes

- **TCP:** Number of bytes from TCP packets transmitted through the firewall.
- **UDP:** Number of UDP packets transmitted through the firewall.
- **ICMP:** Number of ICMP packets transmitted through the firewall.

3.4.3.2.5 3.4.3.3.5 Packets

- **TCP:** Number of TCP packets transmitted through the firewall.
- **UDP:** Number of UDP packets transmitted through the firewall.

3.4.3.2.6 3.4.3.3.6 Connections

- **Rule ID:** Rule identifier.
- **Filtered:** -

3.4.3.2.7 3.4.3.3.7 Filtered

- **Facts:** -
- **Overflow:** Number of log lines lost.

**TIP**

If you select a line from a developed node, an explanation appears in the button bar situated below the table.



3.4.4 Miscellaneous

The **Miscellaneous** menu enables viewing several types of information.

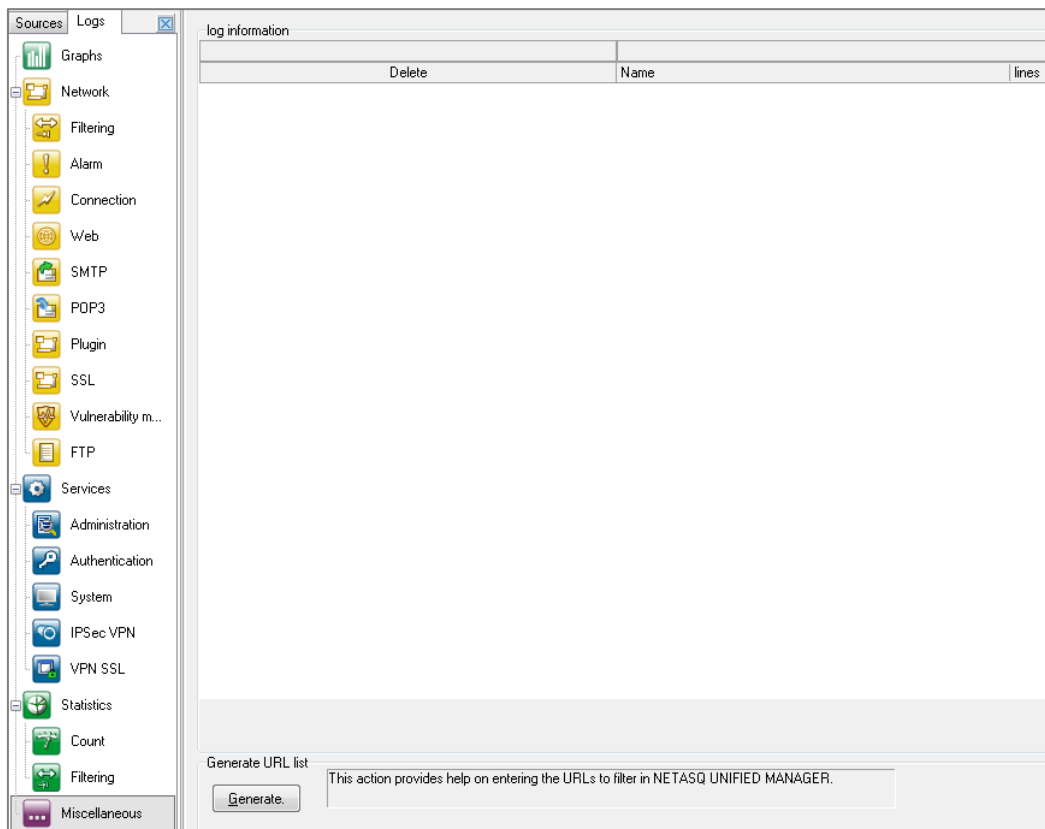


Figure 25: Miscellaneous

3.4.4.1 The "Log information" section

This section provides information on the number of log lines (on the Firewall).

To update information, click on the **"Get info"** button.

If you possess modification privileges, an additional column will appear, enabling the selection of logs to be deleted on the Firewall using the **"Clear on firewall"** button. Archived logs will then be deleted.

| | |
|---------------|--|
| Delete | The selected line will be deleted if this option is checked. |
| Name | Name given to the table. This name always begins with "Log". |
| Lines | Total number of lines for a given table. The number of lines per day is indicated in brackets. |
| Start | Date on which lines started being generated. |
| End | Date on which lines stopped being generated. |

3.4.4.2 The “Generate URLs” section

This section generates a list of web addresses visited by users in an HTML file in the case URL filtering has been activated. This list can be used to indicate to Stormshield Network UNIFIED MANAGER new URLs to filter.

Click on the “**Generate**” button to generate this HTML file. A screen will appear, allowing you to name the file and save it in a folder of your choice.

1.1.1.1. The “Firewall information” section

This section provides information about Firewall: firewall identifier (serial number), firewall name, user name, et HA : satus of High avalaibility.

3.5 DATA EXPORT

3.5.1 Export

➔ Click on the “**Export**” button in the action bar of the **Logs** tabs to export data.

A wizard will guide you in exporting your data. Data can be exported in 4 formats:

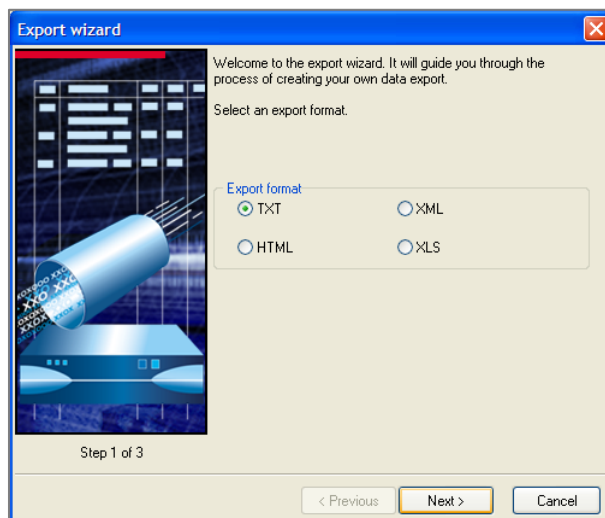


Figure 26: Export wizard - Step 1

- TXT
- XML
- HTML
- XLS

If you select the TXT format, during Step 2, the assistant will prompt you to choose a field separator as shown in the example below:

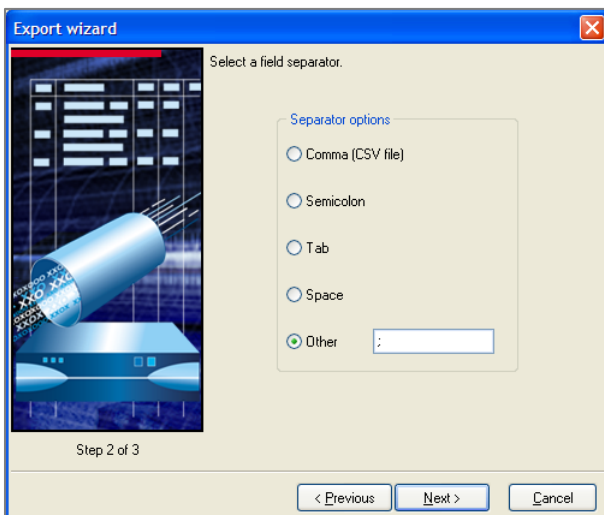


Figure 27: Export wizard - Step 2

In the last step (Step 3), the wizard will ask you to select the column headers and the columns to be exported using checkboxes.

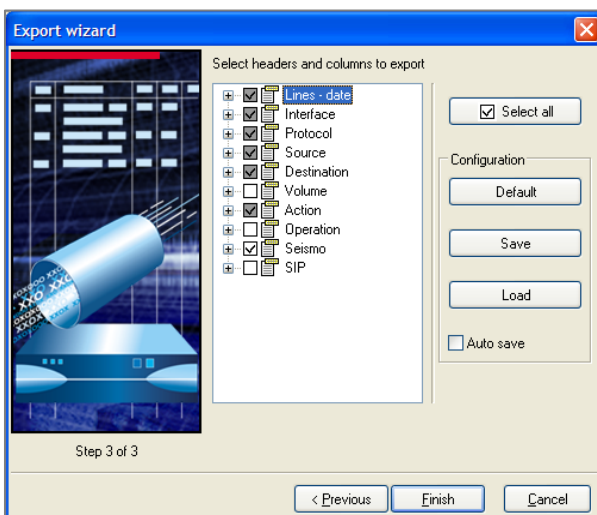


Figure 28: Export wizard - Step 3

The interface allows you to check or uncheck all the boxes, get the default selection, save/restore your column selection. Each export type has its own backup. By checking a box, you automate this operation.

When you later select the **“Finish”** button, the interface will ask you if you wish to save the generated file in a folder of your choice. This folder will be remembered for each export type.

**i** REMARK

If the Reporter connects directly to a Firewall and the number of lines to be retrieved on the Firewall exceeds 10,000, a download confirmation message will appear on the screen.

3.5.2 Log format

The logs are in WELF (WebTrends Enhanced Log Format) format.

- **Line (whole type)**: number of the Firewall log line (alphabetical type): Firewall serial number,
- **Time (Log Time, type date)**: date of the log line,
- **Pri (whole type)**: priority of the event (alarm ref.),
- **Srcif (alphabetical type)**: source interface,
- **Srcifname (alphabetical type)**: interface name,
- **Dstif (alphabetical type)**: destination interface,
- **Dstifname (alphabetical type)**: destination interface name,
- **Movement (whole type)**: direction of movement (in to in, in to out, out to out, out to in),
- **MoveTypeMS (whole type)**: direction of movement (Server to Server, Server to Client, Client to Client, Client to Server),
- **Ipproto (alphabetical type)**: Internet protocol
- **Proto (alphabetical type)**: protocol
- **Src (alphabetical type)**: source address (IPV6 ready)
- **Srcport (alphabetical type)**: source port
- **Srcportname (alphabetical type)**: source port name
- **Srcname (alphabetical type)**: name of the source
- **Dst (alphabetical type)**: destination address (IPV6 ready)
- **Dstport (alphabetical type)**: destination port
- **Dstportname (alphabetical type)**: name of destination port
- **Dstname (alphabetical type)**: destination name
- **User (luser, alphabetical type)**
- **Ruleid (whole type)**: filter rule identifier
- **Action (chain type)**: action, reserved word for interbase
- **Msg (alphabetical type)**
- **Sent (whole type)**: amount of data sent
- **Rcvd (whole type)**: amount of data received
- **Duration (real type)**: duration
- **Op (alphabetical type)**: operation
- **Result (alphabetical type)**
- **Arg (alphabetical type)**: command parameters (of a web page)



STORMSHIELD

documentation@stormshield.eu