NETASQ UNIFIED MANAGER

V. 9.0

USER CONFIGURATION MANUAL

Date	Version	Auteur	Objet
April 2010	V8.0	NETASQ	Creation
May 2010	V8.1	NETASQ	Updating
May 2012	V9.0	NETASQ	Updating

Reference : naengde_numanager-v9.0

NETASQ applies a method of continual development and as such reserves the right to modify and improve any product described in the document without prior notice.

Under no circumstances shall NETASQ be held liable for any loss of data or revenue, or any special damage or incident, resulting from or indirectly caused by the use of the product and its associated documentation.

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.

To ensure the availability of products, which may vary according to your geographical locations, contact your nearest NETASQ distributor.

Products concerned

U30, U70, U120, U250, U450, U1100, U1500, U6000,
NG1000-A and NG5000-A,
VS5, VS10, V50, V100, V200, V500, VU.

CONTENTS

FOREWORD

Copyright

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 NETASQ 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 NETASQ's website at this address:
http://www.netasq.com/recycling.html

License Agreement

Introduction

The information contained in this document may be changed at any time without prior notification. Despite the care taken in preparing this document, it may contain some errors. Please do not hesitate to contact NETASQ if you notice any.
NETASQ will not be held responsible for any error in this document or for any resulting consequence.

Acceptance of terms

By opening the product wrapping or by installing the administration software you will be agreeing to be bound by all the terms and restrictions of this License Agreement.

License

NETASQ hereby grants, and you accept, a non-exclusive, non-transferable license only to use the object code of the Product. You may not copy the software and any documentation associated with the Product, in whole or in part. You acknowledge that the source code of the Product, and the concepts and ideas incorporated by this Product, are valuable intellectual property of NETASQ. You agree not to copy the Product, nor attempt to decipher, reverse translate, de-compile, disassemble or create derivative works based on the Product or any part thereof, or develop any other product containing any of the concepts and ideas contained in the Product. You will be held liable for damages with interests therein in favor of NETASQ in any contravention of this agreement.

Limited warranty and limitation of liability

a - Hardware

NETASQ warrants its Hardware products ("Hardware") to be free of defects in materials and workmanship for a period of one year, in effect at the time the Purchaser order is accepted. This period begins with effect from the date on which the product is activated.

b - Software

NETASQ Software products ("Software") are warranted for a period of 90 days (unless otherwise stated at purchase) from the date of the product's activation to be free from defects and to operate substantially according to the manual, as it exists at the date of delivery, under the operating system versions supported by NETASQ.

NETASQ does not warrant its software products for use with operating systems not specifically identified.

c – Default

NETASQ's entire liability and your exclusive remedy shall be, at NETASQ's option, either a return of the price paid for this License or Product resulting in termination of the agreement, or repair or replacement of the Product or media that does not meet this limited warranty

d – Warranty

Except for the limited warranties set forth in the preceding paragraph, this product is provided "*as is*" without warranty of any kind, either expressed or implied. NETASQ does not warrant that the product will meet your requirements or that its operation will be uninterrupted or error free. NETASQ disclaims any implied warranties or merchantability or fitness for particular purpose, or non-infringement.

e - Recommendations

In no event will NETASQ be liable to you or any third party for any damages arising out of this agreement or the use of the product, including lost profit or savings, whether actual, indirect, incidental, or consequential, irrespective of whether NETASQ has been advised of the possibility of such damages. NETASQ's maximum liability for damages shall be limited to the license fees received by NETASQ under this license for the particular product(s) which caused the damages.

Any possible legal action relating to the alleged defectiveness of the software will come under the jurisdiction of NETASQ's headquarters, French law being the binding authority.

WARNING

1) Certain NETASQ products enable gathering and analyzing logs. This log information allows the activity of internal users to be tracked and may provide nominative information. The legislation in force in the destination country may impose the application of certain measures (namely administrative declarations, for example) when individuals are subject to such monitoring. Ensure that these possible measures have been applied before any use of the product.
2) NETASQ products may provide cryptographic mechanisms which are restricted or forbidden by the legislation in force in the destination country. Despite the control made by NETASQ before exportation, ensure that the legislation in force allows you to use these cryptographic mechanisms before using NETASQ products.
3) NETASQ disclaims all liability for any use of the product deemed illegal in the destination country.

Hypotheses derived from the Common Criteria

DEFINITION

The common criteria evaluate (on an Evaluation Assurance Level or EAL scale of 1 to 7) a product's capacity to provide security functions for which it had been designed, as well as the quality of its life cycle (development, production, delivery, putting into service, update).

They are a convergence of different security-related quality standards devised since 1980:
Orange Book – DoD
CTCPEC (Canadian Trusted Computer Product Evaluation Criteria)
ITSEC (Information Technology Security Evaluation Criteria)
TCSEC (Trusted Computer System Evaluation Criteria).

Introduction

Installing a Firewall often comes within the scope of setting up a global security policy. To ensure optimal protection of your assets, resources or information, it is not only a matter of installing a Firewall between your network and the internet. This is namely because the majority of attacks come from the inside (accidents, disgruntled employees, dismissed employee having retained internal access, etc.). However, one would also agree that installing a steel security door defeats its purpose when the walls are made of paper.

Backed by the Common Criteria, NETASQ advises taking into consideration the hypotheses of use for the Administration Suite and Firewall product stated below. These hypotheses set out the usage requirements by which to abide in order to ensure that your Firewall operates within the context of the common criteria certification.

Hypotheses on physical security measures

NETASQ UTM appliances are installed and stored in compliance with the state of the art regarding sensitive security devices: secured access to the premises, shielded twisted pair cables, labeled cables, etc.

Hypotheses on organizational security measures

A particular administrative role that of the super-administrator, has the following characteristics:

- Only the super-administrator is permitted to connect via the local console on NETASQ UTM appliances, and only when installing the Firewall or for maintenance operations, apart from actual use of the equipment.
- He is in charge of defining the profiles of other administrators,
- All access to the premises where the appliances are stored has to be under his supervision, regardless of whether the access is due to an intervention on the appliance or on other equipment. He is responsible for all interventions carried out on appliances.

User and administrator passwords have to be chosen in such a way that successful attempts at cracking them will take longer. This can be assured with the implementation of a policy regulating their creation and verification.

> **Example**
>
> Combination of letters and numbers, minimum length, addition of special characters, words which are not taken from ordinary dictionaries, etc.

Administrators have the task of directing users' awareness to these practices (*Cf. Part 13: PKI, chapter 6 User Awareness*).

For equipment in "trusted" networks which have to be protected, the control policy for traffic to be implemented should be defined in the following manner:

- **Complete**: the standard scenarios of how equipment is used have all been considered when defining the rules and their authorized limits have been defined.
- **Strict**: only the necessary uses of the equipment are authorized.
- **Correct**: rules do not contradict each other.
- **Unambiguous**: the wording of the rules provides a competent administrator with all the relevant elements for direct configuration of the appliance.

Hypotheses relating to human media

Administrators are competent non-hostile persons, possessing the necessary means to accomplish their tasks. They are trained to carry out the operations of which they are responsible. Their competence and organization mean that:

- Different administrators having the same rights will not perform administrative actions which conflict

> **Example**
>
> Incoherent modifications to the control policy for traffic.

- The use of logs and treatment of alarms are carried out within the appropriate time limits.

Hypotheses on the IT security environment

NETASQ UTM appliances and installed in accordance with the current network interconnection policy and are the only passageways between the different networks on which the control policy for traffic has to be applied. Connection peripherals (modems) are prohibited on "trusted" networks.

Besides applying security functions, NETASQ UTM appliance do not provide any network service other than routing and address translation.

> **Example**
>
> no DHCP, DNS, PKI, application proxies, etc.*

NETASQ appliances are not configured to retransmit IPX, Netbios, Appletalk, PPPoE or IPv6 traffic.

NETASQ UTM appliances do not rely on “online” external services (DNS, DHCP, RADIUS, etc.) in order to apply the control policy for traffic.

Protecting workstations: remote administration stations are secure and kept to date of all known vulnerabilities concerning operating systems and the hosted applications. They are exclusively dedicated to the administration of firewalls.

Network equipment which the firewall uses to establish VPN tunnels are subject to constraints relating to physical access, protection and control of their configuration. These constraints are equivalent to those faced by the TOE’s firewall-VPN appliances.

Protecting clients: workstations on which authorized users execute their VPN clients are subject to constraints equivalent to those on client workstations in “trusted” networks. These constraints are namely, the control of physical access, protection and command of their configuration. Trusted networks are secured and kept to date of all known vulnerabilities concerning operating systems and the hosted applications.

* These services are available on firewalls but are not part of the scope of evaluation of the common criteria.

1. INTRODUCTION

NETASQ UNIFIED MANAGER is an application that allows you to securely update your product locally or remotely.

With it, you will be able to configure the following:

- your network
- your objects
- your security poilcy
- internet access from your internal network (NAT)
- your backups

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 NETASQ 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 the 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.

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

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*). Other acronyms will be defined in the Glossary.

1.2.2. Display

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

> **Example**
>
> Menu **`Interfaces`**

1.2.3. Indications

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

NOTE/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 NETASQ 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. Reminders

Reminders are indicated as follows:

- Reminder.

1.2.8. Access to features

Access paths to features are indicated as follows:

- Access the menu **`File\Firewall.`**

1.3. VOCABULARY USED IN THE MANUAL

Appliance	Refers to the security device (firewall). The terms “appliance” and “security device” are used interchangeably.
Dialup	Interface on which the modem is connected.
UTM Fxx	Refers to the NETASQ product range. Other terms also used: NETASQ Fxx, Fxx appliance.
Firewall	NETASQ UTM device /product
Intrusion prevention	Unified Threat Management is also used in its place.
Configuration slot	(*or policy*). Configuration files which allow generating filter and NAT policies, for example.
Host	Terms used as much to refer to workstations as to users.
Logs	A record of user activity for the purpose of analyzing network activity.

1.4. GETTING HELP

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

- website: www.netasq.com. Your secure-access area allows you to access a wide range of documentation and other information.
- user manuals: NETASQ UNIFIED MANAGER, NETASQ REAL-TIME and NETASQ EVENT REPORTER.

1.5. TECHNICAL ASSISTANCE CENTRE

NETASQ 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 "Standard NETASQ support".

2. SOFTWARE INSTALLATION

This section provides you with the elements for installing the software suite that would allow you to administer your poduct.

For further information on the appliances and how to install them, please refer to the product installation guide "Presentation and installation of NETASQ products", (Ref. naengde_product-installation.pdf).

You will need the graphical interface installation file. This file can be found on the CD-ROM that comes with your firewall or on the NETASQ website (www.netasq.com). 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. PRE-REQUISITES

The NETASQ firewall is fully configured via a software program developed by NETASQ – NETASQ 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 512 MB of RAM (Windows XP) 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

NETASQ supports the execution of the software in a defined environment:

Client software applications are supported on the following 32-bit operating systems:

- Microsoft Windows Server 2003 SP2
- Microsoft Windows XP Service Pack 2 and higher,
- Microsoft Windows Vista
- Microsoft Windows Server 2008

Server software applications are supported on the following 32-bit operating systems:

- Microsoft Windows Server 2003 SP2
- Microsoft Windows XP Service Pack 2 and higher

2.2. INSTALLING VIA CD-ROM

Insert the installation CD-ROM that has been provided.

Once the CD-ROM has been inserted, the administration suite installation wizard will launch automatically and will guide you step by step.

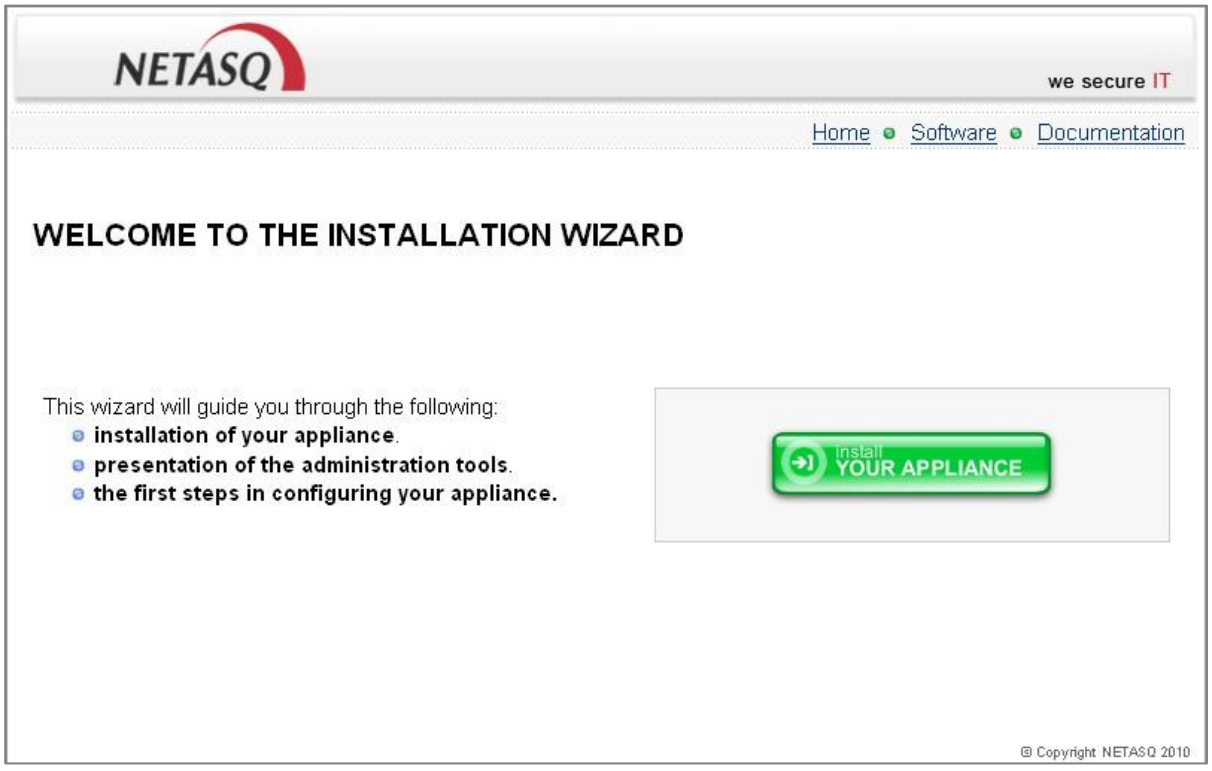

Figure 1: CD-ROM installation wizard

2.3. INSTALLING VIA YOUR PRIVATE AREA

Download the necessary files from NETASQ's 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.

2.3.1. Verification procedure

2.3.1.1. Signature verification procedure

When you download an application from your client or partner area on www.netasq.com, 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.

2.3.1.2. Manual verification

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

1. Right-click on the NETASQ 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.

2.3.2. Client and server administration suite: choice of package

Several packages may be selected:
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:

- Netasq Unified Manager: Graphical interface for the administration of NETASQ firewalls
- Netasq Real-Time Monitor: Real-time viewer of your NETASQ firewall (2.58 MB)
- Netasq Event Reporter: Log consultation and management on your firewall (140 MB)
- Netasq Updater: Help download service for alarms, system events and vulnerabilities (10.5 MB). *(Cf. Please refer to the documentation relating to this program for further information).*

Server addition group together:

- Netasq Autoreport: Automatic report creation and scheduling according to your firewall’s logs, stored in a database (165.7 MB).
- Netasq Collector: service and database for keeping your firewall’s logs (165. 7 MB)
- Netasq Syslog: service that allows retrieving logs generated by the firewalls (131.6 MB)

The minimum installation comprises all the graphic configuration tools of the NETASQ suite, which serve as the interface between the user and the appliance. These tools are installed on an administration workstation.

As for the server additions, they comprise all the communication tools used in retrieving logs from appliances that belong to you. These tools are generally installed on a dedicated host due to the amount of resources that they require.

2.3.3. 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 NETASQ's technical support.

3. GLOBAL ADMINISTRATION

In this section, the general use of the NETASQ GLOBAL ADMINISTRATION configuration graphical interface is explained.
Do note that in version 9, NETASQ UNIFIED MANAGER will no longer be supported (but it will continue to be supported in versions 8 and earlier).

NETASQ GLOBAL ADMINISTRATION is the software solution for easily and affordably managing from a single central point certain administration actions over an entire fleet of NETASQ products.

3.1. PRESENTATION

3.1.1. Description

Managing installed security assets is often a complex and time-intensive task, involving numerous operations on each product in order to maintain an optimal level of security. A security product must be updated frequently in order to handle the new IT threats that appear on a daily basis. These updates, if they are executed manually on each product, require significant human resources.

NETASQ Global Administration allows conveniently managing certain administrative functions for the whole group of NETASQ products at a lower cost, since this is done from a central unique location; these functions are:

- centralized automatic update of NETASQ firmware
- centralized automatic update of licenses
- deployment of security policies and object databases.
- centralized automatic update of licenses
- backup of system partitions
- administration tool execution
- launching NETASQ tools: NETASQ UNIFIED MANAGER, NETASQ REAL-TIME MONITOR, NETASQ EVENT REPORTER for administering, monitoring and analyzing logs on every firewall in the fleet.

NETASQ Global Administration connects automatically to the NETASQ website to download updates and appliance licenses, it can also connect completely automatically to the appliances managed to update them, which considerably reduces the time required for asset administration.

The other function supplied by NETASQ Global Administration is to provide tools for monitoring and supervision of the NETASQ equipment assets:

- status indicator of the NETASQ product or networked host (on-line, inaccessible, or switched off, current software version, license version etc.)
- system status indicator for each product
- security status indicator

The information can be displayed in tabular form or graphically in topology form, which offers the easiest method of reading the information and the most intuitive and user-friendly administration.
This section describes the various elements and functions of NETASQ Global Administration and is designed to guide the administrator in his task of configuring and using the product.

3.1.2. Access

➲ To use NETASQ Global Administration, start the application using the Windows **Start** menu, from the following path: **Start\Programs\Netasq\Administration Suite 7.0\NETASQ UNIFIED MANAGER**.

WARNING

Global Administration mode has to be indicated in the menu **Options\Preferences\General**.

3.1.3. Creating/opening a project

NETASQ Global Administration works in project mode. Thus it is possible to carry out several configurations (projects), each project corresponding to a group of NETASQ products that can be managed.

➲ When you launch NETASQ Global Administration

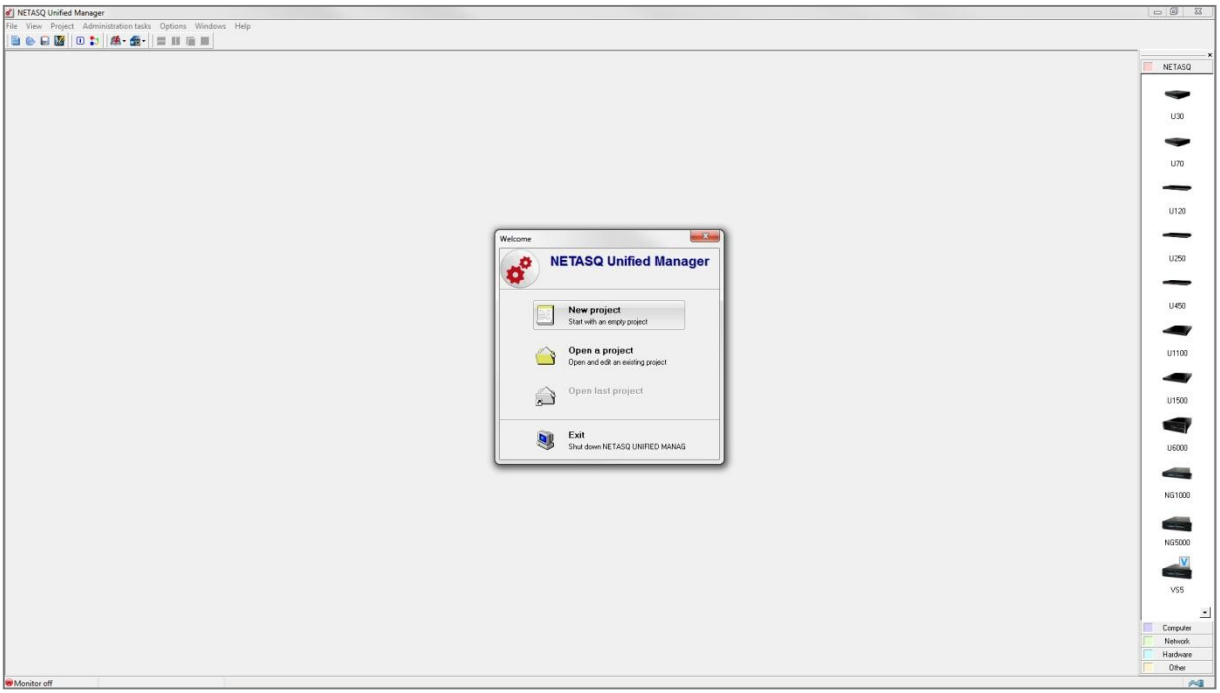

Figure 2 : ***Launching Global Administration***

Several choices are given:

- **New project**: for creating a new project or a new administration configuration
- **Open a project**: opens an existing project. A window opens allowing you to select the appropriate project file,
- **Open last project** allows you to open the last project opened or created by NETASQ Global Administration.
- **Reboot in Manager mode (temporary):** opens NETASQ UNIFIED MANAGER in Firewall Manager mode. In this case, a message will appear asking whether you wish to permanently modify the application in Firewall Manager mode.
- **Exit** immediately closes the application.

NETASQ Global Administration can only open one project at a time.
When using NETASQ Global Administration for the first time, select **New Project**.

3.2. GLOBAL ADMINISTRATION

3.2.1. User interface

3.2.1.1. Main window

The topological window is presented in the following manner when a new project is created:

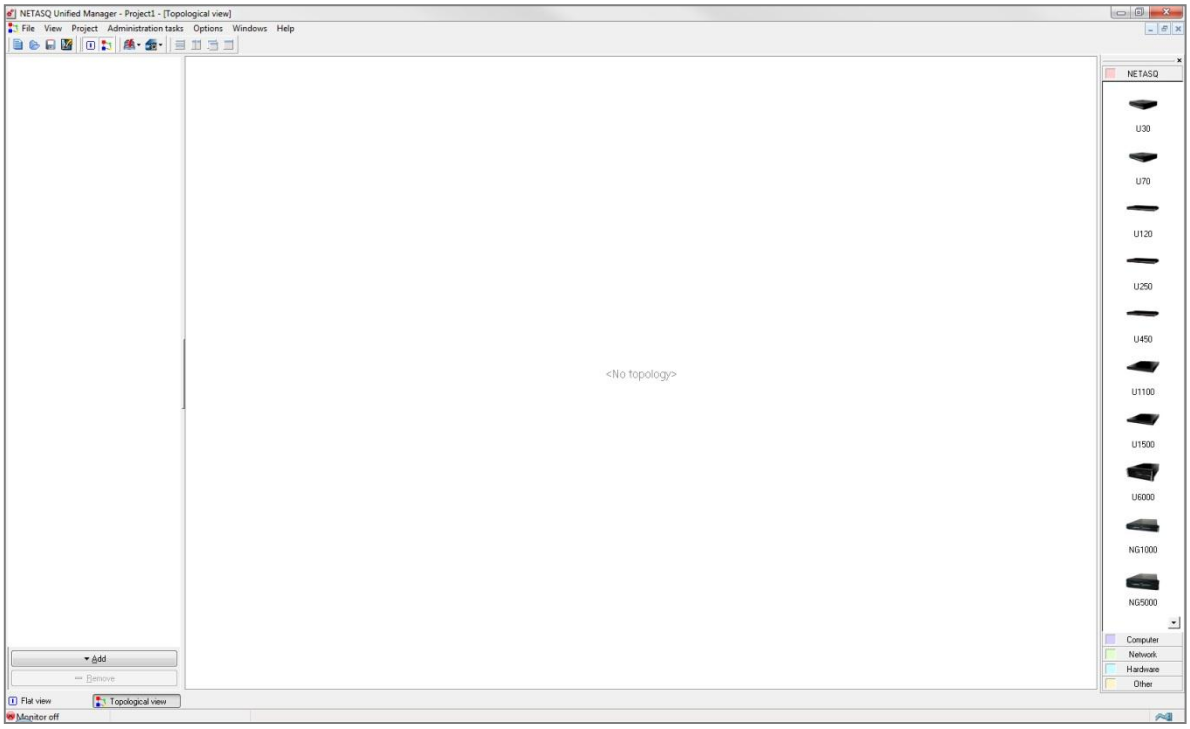

Figure 3 : ***Main window***

This window comprises several parts:

- a menu bar.
- an icon and shortcut bar.
- an object bar.
- a global view (a table listing the fwls in the project).
- a bar to change views.

3.2.1.2. Menu bar

This bar contains the following menus:

- **File**
- **View**
- **Project**
- **Administration Tasks**
- **Options**
- **Windows**
- **Help**

3.2.1.1. Icon and shortcut bar

The following bar contains the shortcuts for certain operations:

Figure 4: Icon and shortcut bar

	For creating a new project (corresponds to menu item **File\New project**)
	For opening an existing project (corresponds to the menu item **File\Open**).
	For saving the current project (corresponds to the menu item **File\Save**).
	For defining or modifying the NETASQ Global Administration preferences (corresponds to the menu item **Options\Preferences**).
	For displaying or hiding the flat view (corresponds to the **View\Flat view**).
	For displaying or hiding the topological view. (corresponds to the menu **View\Topological view**).
	Menu for accessing configuration features (Backup and Restore) in Global Administration. See "**Administration tasks**".
	Menu for accessing update, backup partition and scripting features in Global Administration (corresponds to the menu **Administration tasks**).
	For arranging the windows of the current project horizontally (corresponds to the menu **Windows\Tile horizontal**).
	For arranging the windows of the current project horizontally (corresponds to the menu **Windows\Tile vertical**).
	For cascading the windows of the current project (corresponds to the menu **Windows\Cascade**).
	For arranging the windows of the current project. (corresponds to the menu **Windows\Arrange**).

3.2.1.1. Object bar

The object bar is organized as follows:

It contains all the objects that can be used in the topological view to construct a graphic view of the network or the sub-network administered. These objects are divided into 5 categories:

- NETASQ
- Computers
- Network
- Hardware
- Other

Figure 5 : ***Object bar***

3.2.1.1.1. Category descriptions

NETASQ	This category groups together all the NETASQ equipment that can be managed by NETASQ Global Administration
Computers	This category groups two subsets together: workstations on which NETASQ Global Administration is installed and other network workstations, mobile computers, and servers).
Network	This category groups together the network connection equipment (Internet network, router, modem, hub, switch, WIFI, Intranode scanner)
Hardware	This category groups certain equipment, like non-NETASQ printers or firewalls, together.
Other	This category contains an object that allows you to add a note to the topological diagram, and an object that allows you to represent a link to another existing topology.

3.2.1.1. Switching views

The bar, located at the bottom of the NETASQ Global Administration screen, indicates the open views (topological and flat view). The view displayed is the one which is indented. To move to another open view, click on its name.

Figure 6: Switching views

Two cases are present by default: Topological View and General View. By choosing to hide one view or the other in the icon or shortcut bar, or in the **View** menu, you hide the corresponding box.

REMARK

Also note that other boxes can appear when you configure certain functionalities of NETASQ Global Administration (**`Configuration`**, **`Partition backup`**, and **`Deployment`**).

3.2.1.2. Monitor and web mode

There is a bar containing two information items underneath the change view bar. These two information items refer to the monitor status and the web mode status.

Figure 7: Monitor and web mode

The web mode status is represented by an electric socket plugged (webmode activated) or unplugged (webmode deactivated), This option determines whether or not NETASQ Global Administration can connect to the NETASQ web site to obtain information to update the Firewalls. To modify the mode status, double click on the icon representing the plug, or define the **Work offline** option in the menu **`Options\Preferences\Website access`**.

3.2.1.3. Topological view

This view is the first view displayed when a new project is created:

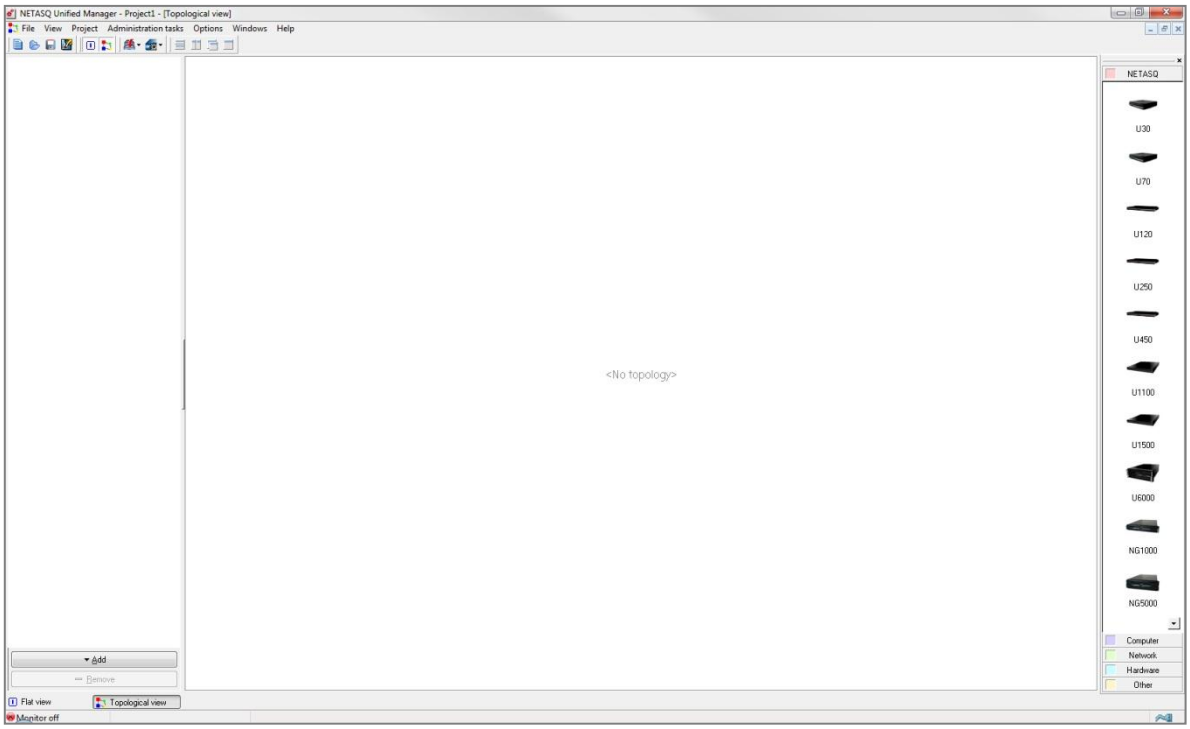

Figure 8: Topological view

More information about this view is provided in the course of the manual.

3.2.2. Menus

3.2.2.1. File

New project	For creating a new project.
Open	To open an existing project.
Save	To save modifications made to the current project.
Save as	For saving the project under a different name.
Import address book	To retrieve an existing address book in **.gap** format.
Import firewall file	For importing a **.CSV** format file containing a list of NETASQ appliances.
Export firewall file	For exporting a **.CSV** format file containing a list of NETASQ appliances.
Quit	To quit the application

3.2.2.2. View

General view	For opening or closing the general view.
Topological view	For opening or closing the topological view.
Topological main toolbar	For showing or hiding the object bar.

3.2.2.3. Project

Modify password	For modifying the password that protects the current project.
Options	For defining the current project's options

3.2.2.4. Administration tasks

Configuration	Opens the configuration's backup or restore screen.
Update Firmware	Opens the firewall update window
Update license	Opens the license update window
Backup the partition	Opens the system partition backup window.
Scripts…	Executes NETASQ scripts on targeted UTM appliances.
Deployment	Opens the menu for defining the deployment options of the security policies and/or the object bases.

3.2.2.5. Options

Preferences	For defining the NETASQ Global Administration options.

3.2.2.6. Windows

Horizontal tile	For organizing the windows of the current project in a horizontal layout.
Vertical tile	For organizing the windows of the current project in a vertical layout.
Arrange	For arranging the windows of the current project.
Cascade	For cascading the windows of the current project.

3.2.2.7. Help

Help	Displays the online help file.
Update NETASQ UNIFIED MANAGER	Displays information on installed versions.
About…	Displays a window indicating the information relating to NETASQ Global Administration.

3.2.3. Project

➲ There are several options that are specific to each project. To configure them, go to the **`Project\Options`**.

3.2.3.1. Client monitoring

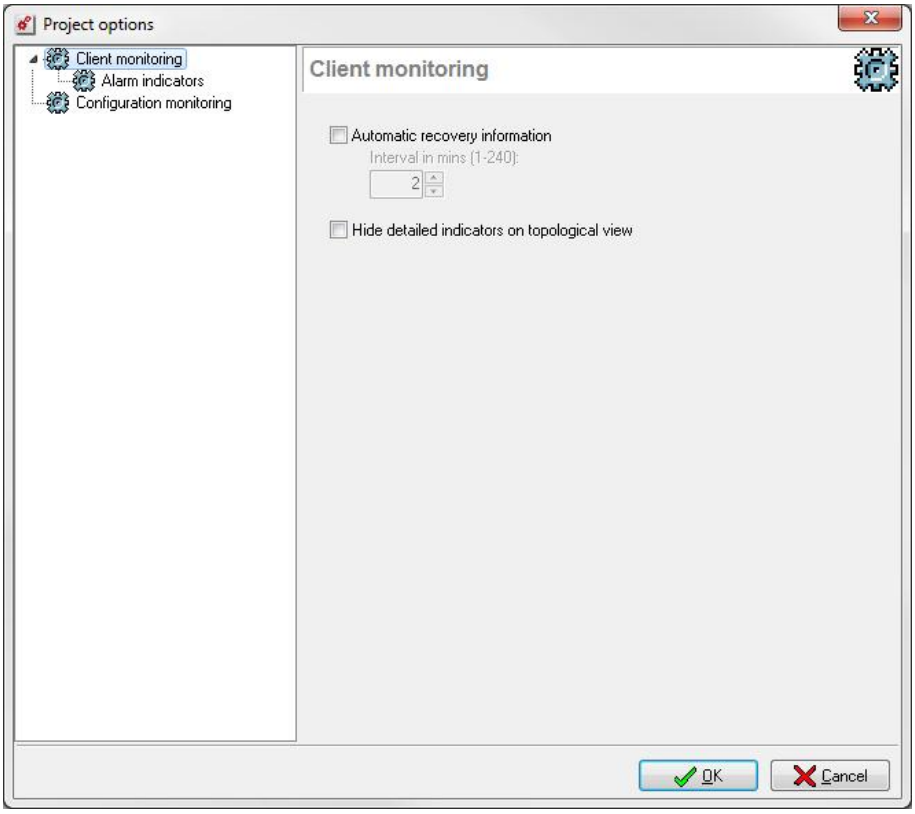

Figure 9 : ***Project options - Client monitoring***

If the option **Automatic information recovery** has not been selected, data (version, model, status, attributes…) and alarms (system and security) will not be automatically refreshed. If the box has been checked, indicate the period between each refreshment in minutes.

Detailed indicators can also be hidden (Levels of system issues, levels of security problems, alarm status) in the topological view.

3.2.3.1.1. Alarm indicators

The “Alarm indicators” screen allows you to define the display of the status of the alarms in the Topological View. The different options allow you to view the aggregation of alarm status, or the status of alarms in real time, or both of these options.

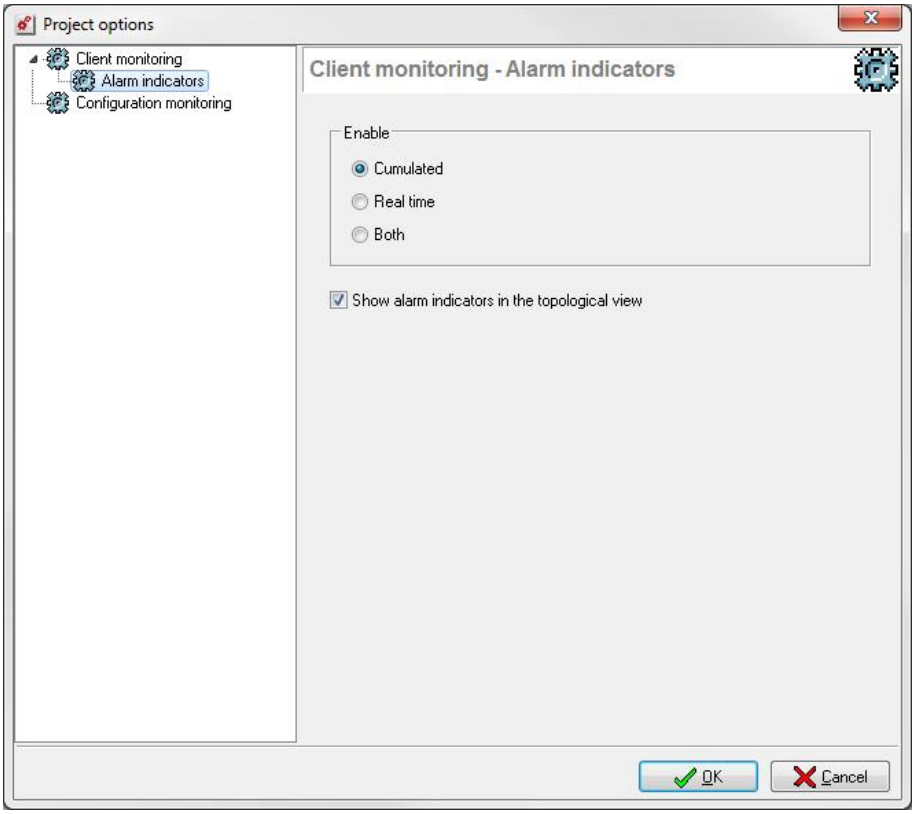

Figure 10 : ***Project options – Alarm indicators***

3.2.3.2. Configuration monitoring

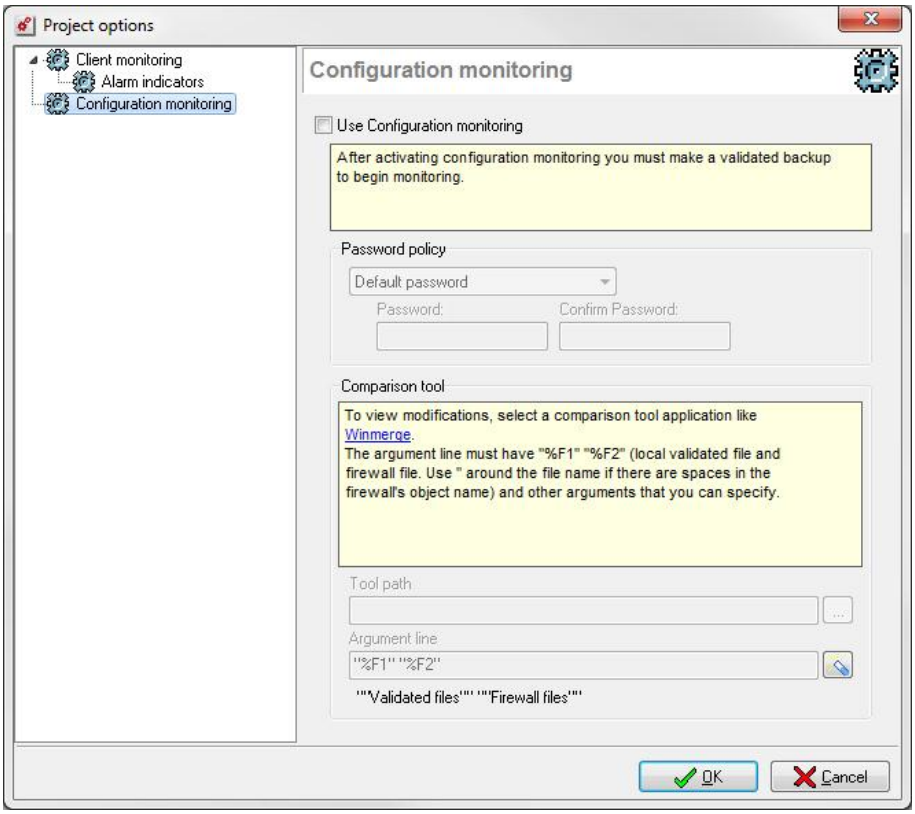

Figure 11 : ***Project options – Configuration monitoring***

The **Configuration monitoring** menu makes it possible to monitor modifications made to the configuration of appliances managed by NETASQ Global Administration (features available only for appliances in version 6.3 and upwards).

Use configuration monitoring	Option that activates configuration monitoring. The configurations of the monitored appliances have to be backed up and validated before you begin.
Password policy	By default, passwords are not needed when validating a configuration. However, passwords can be defined, either a single identical password for all managed appliances, or specific passwords for each appliance. This option enables defining the mode for managing the validation of passwords: • Default password: default management mode; • A single password for all: a single password has to be defined. It will be the same for all the managed appliances. In this case, indicate a password and confirm it. • One password per firewall: a different validation password is defined for each appliance.
Comparison tool	To view changes made to the monitored configurations, you will need to specify an external comparison tool (such as Winmerge). To do so, first specify the file comparison application by indicating the path to the program. Then select the command lines that will be used when the application is launched. By default, two arguments, "%F1" and "%F2" should be found, respectively representing local "validated" configuration files and firewall files. REMARK Quotes have to be used in command lines if the names of your firewalls contain spaces or other arguments that you can specify.
Tool path	Specify the path of the selected tool in order to access it more quickly.
Argument line	It must contain the characters specified in the shaded section on the capture.

3.2.4. Options

3.2.4.1. Behavior

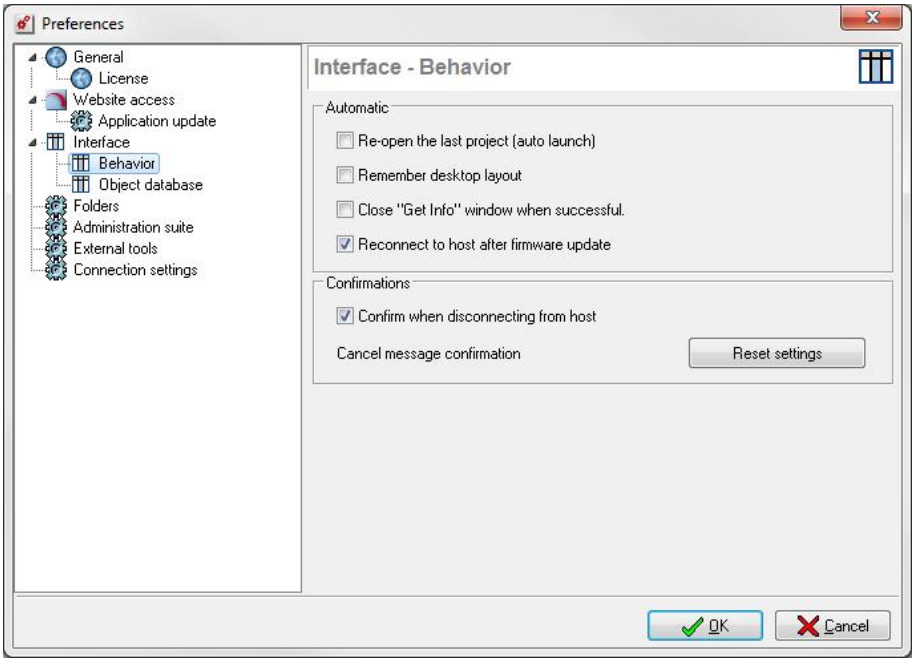

*Figure 12 : **Interface - Behavior***

Reopen last project (autolaunch)	If this option has been selected, the last edited project will automatically be opened when the NETASQ Global Administration application is launched.
Remember desktop layout	If this option has been selected, the project will open with the windows laid out in the same way as during the previous session.
Close "Get into" window when successful	Closes this window automatically.
Reconnect to host after firmware update	Automatically reopens the application after the update has been performed.
Confirm when disconnecting from host	Displays a confirmation message before disconnecting from the firewall.
Cancel message confirmation	Reverts to the default configuration.

3.2.4.1. Folders

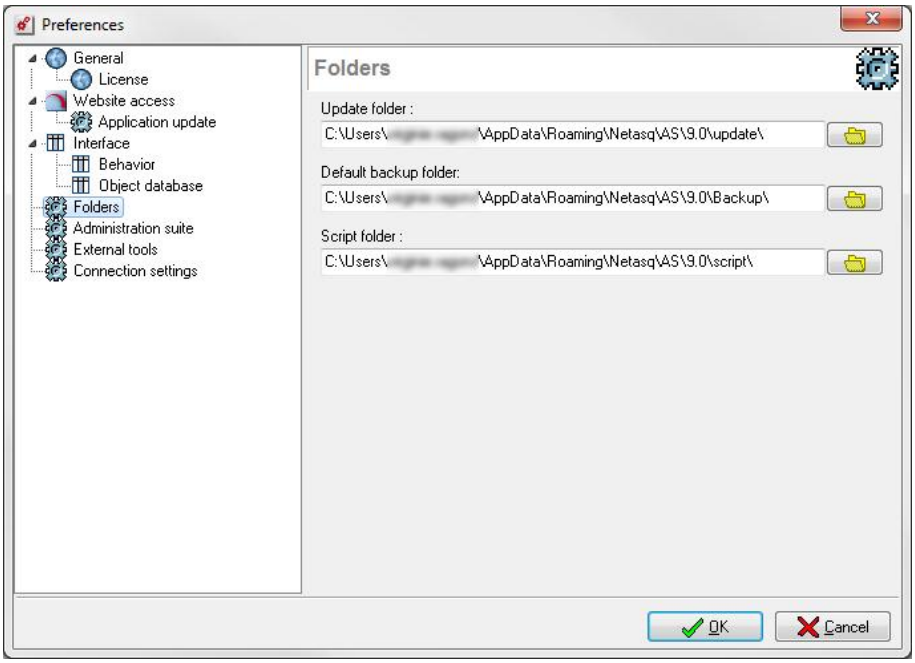

Figure 13 : ***Preferences – Folders***

Update folder	In this field, indicate the directory in which updates will be stored. When NETASQ Global Administration retrieves a firmware update on NETASQ's website, the file will be stored in this directory before being distributed and installed on the appliances. The default folder is: `%Administration Suite 7.0 installation directory \Update\`
Default backup folder	In this field, indicate the directory in which configurations backup will be stored. When NETASQ Global Administration retrieves a configurations backup, the file will be stored in this directory. By default the folder is: `%Administration Suite 7.0 installation directory \Backup\`
Script folder	In this field, indicate the folder in which scripts will be saved. By default the folder is: `%Administration Suite 7.0 installation directory \script\`

3.2.4.1. External tools

This tab enables configuring external tools such as SSH or telnet (max. 12), which may be launched for an appliance (or for any other equipment for which the "IP address", "login" and "password" fields have been entered in the information record).

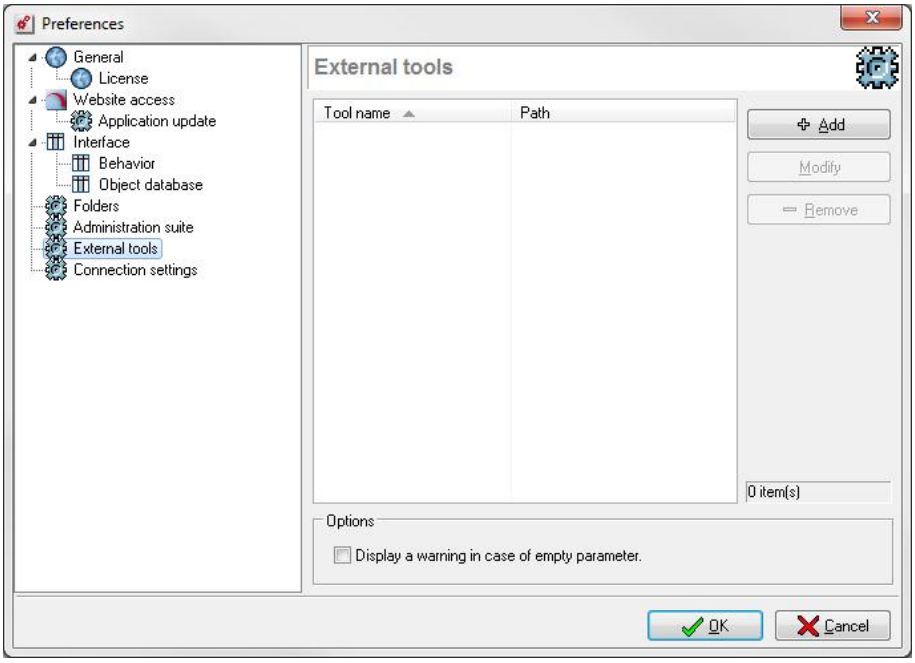

Figure 14 : Préférences - ***External tools***

To add an external tool, click on **Add**.

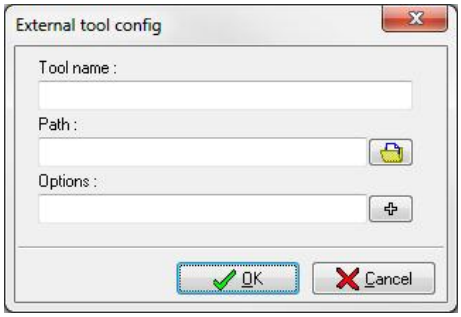

Figure 15 : ***Configuring external tools***

In the window which appears, indicate the following information:

Tool name	Indicate the name referring to the tool.
Path	By clicking on the associated button, select the external tool's executable file.
Options	You may specify an option string in this field, which will become a command line parameter when the external tool is launched. In this string, during the launch of the tool, it is possible to dynamically insert information from the object's records peculiar to this object **Example** Connection login, IP address, password, e-mail address, etc. To add dynamic information to the option string, click on the associated button and select the information in this list which appears.

Next, click on **OK**.

You may add as many tools as you wish. To easily locate a tool in the list, you may sort the list by clicking on the title of the "Tool name" column or filter the tool names by clicking on the little black arrow in the title of the "Tool name" column.

To delete an external tool from the list, select the tool and click on the **Remove** button. To modify the configuration of the launch of an external tool, select the tool and click on the **Modify** button.

At the bottom of the window, the option **Show warning if a field is empty**, if selected, allows warning the NETASQ Global Administration administrator that one of the fields which has to be in the option string is empty (the field had not been entered in the object's information records). This warning is given when the tool is launched.

Example

Using **PUTTY** to connect to an appliance in SSH command line

In the tool creation window, indicate the following information:

Name: SSH
Path: <path to putty.exe>
Options: -ssh -2 -pw $PASSWORD$ $LOGIN$@$ADDRESS$

Therefore, once the tool is launched, it will connect directly to the desired appliance and you will not need to enter either a login or password.

3.3. USING THE GLOBAL ADMINISTRATION MODE

3.3.1. General

3.3.1.1. Presentation

NETASQ Global Administration works in project mode. The projects correspond to network or sub-network administration configurations. All projects are protected by a password.

3.3.1.2. Creating a project

A project can be created by using the menu item **File\New project**, or by using the corresponding shortcut in the shortcut bar.

3.3.1.3. Opening and closing a project

You can open a project by starting NETASQ Global Administration (Creating/Opening a project), or via the menu item **File\Open**. A window opens asking you to select the project file to open. The project files have **.gap** as the extension. You can also open a file by clicking on the corresponding shortcut in the shortcut bar. Only one project may be open at a time. If you open a project when another project is in use, then the latter (the project in use) will be closed automatically. When opening a project you must enter the password that protects it.

Close a project either by exiting the application, or via the menu item **File\Quit**, or by opening another project.

3.3.1.1. Saving a project

Save a project by either using the menu item, **File\Save**, or by using the corresponding shortcut in the shortcut bar, or by using the keyboard shortcut **CTRL+S**. All modifications will be saved in the current project.

It is also possible to save a project under another name or in another location. To do this, you can use the menu item, **File\Save as**..., or you can use the corresponding shortcut in the shortcut bar.

When a project is saved for the first time, or when using the **Save as**... function, a message window will ask you to enter and confirm a password to protect the project.

3.3.1.2. Importing NETASQ UTM appliances into a project

It is possible to import a database of IPS-Firewall objects into a project. To do this you must use the menu item **File\Import firewall file**. A window appears asking you to choose a file of firewall objects. This file must be in **.csv** format.

This file can contain the following information:

- Name of the Firewall
- IP address of the Firewall.
- Name of the administration account.
- Password for the administration account.

> **WARNING**
>
> For security reasons, you are advised against filling in this field.

- Description of the Firewall.
- Last name of the contact person for the Firewall.
- First name of the contact person for the Firewall.
- Company of the Firewall's contact person.
- City where the Firewall is installed.
- The address of the place in which the Firewall is installed.
- Postal code of the city where the Firewall is installed.
- Country where the Firewall is installed.

Each line of the file must correspond to a firewall. The information must be separated by commas, or by semi-colons, or by a character of your choice

> **WARNING**
>
> This character should not be a commonly-used character to prevent the risk of it being used in the information fields. None of the fields are mandatory; therefore it is not necessary to fill in all the above information (we strongly recommended not entering the password in the CSV file, as it is an unencrypted file). The order of fields in the file is not important.

> **Example**
>
> FW_1,10.0.0.1,admin,FRANCE,jean.dupont@NETASQ.com
> FW_2,10.0.0.2,admin,ITALY
> FW_3,10.0.0.3,BELGIUM

In this example the first part of the information corresponds to that contained in the name of the firewall field, the second corresponds to the IP address of the Firewall, the third, to the name of the administration account, the fourth to the country where the Firewall is installed, and the last to the E-mail address of the contact person.

REMARKS

1) A field can be empty for certain appliances and filled in for the others (as is the case with FW_3), thus you must leave the separation characters in this case.
2) Only indicate those fields in the file for which you require information.

You will then be able to define the rules governing the import of the information. First of all, you must specify the type of separator between the information (comma, semi-colon, or particular character that you must define) and the type of delimiter for text zones.
Then you can move the columns of the preview zone using a drag & drop method so that the file information corresponds to the preview of the column layout. This layout will then be applied to the file during the import of the information.

In our preceding example you had to choose the separator **comma** and place the columns in the following order:

Name,Address,Login,Country,Email

The contents of the file will then be displayed in the "Preview" zone. If information that is present in the file does not appear, then verify that you have correctly separated the file fields using the right separator.
Importing a file allows you to add the file information in the flat view. All the Firewall information already contained in the flat view is retained after import.

3.3.1.1. Exporting firewall from a project

All appliances in the general view of a selection of some of them can be exported to a .csv or .txt file.
This file could contain the following information for each appliance:

- Name of the Firewall
- IP address of the Firewall
- Name of the administration account
- Password for the administration account

WARNING

For security reasons, you are advised against filling in this field (passwords are displayed in plaintext).

- E-mail address for the administration account
- Description of the firewall.
- Custom1
- Custom2
- Custom3
- ZipCode
- City where the Firewall is installed
- Country where the Firewall is installed.
- Company of the Firewall contact person
- Last name of the contact person for the Firewall
- First name of the contact person for the Firewall
- Postal code of the city where the Firewall is installed
- SuperviseGenerationPassword
- SuperviseFirewallValidBackup
- MonitoringOn

➲ To export information on appliances to a file, go to the menu **File\Export firewall file…**.

First select the type of separator that will be used between each field of the file. Also indicate the text delimiter.

Then choose the columns that you would like to export. To do this, click on the **Columns** button and then click on **Customize**.

In this window you will find the names of the columns that are not displayed but which can be displayed. To display a column, select the name of this column with the left mouse button, and keep the mouse button depressed. Then move the column header to where you would like to insert it in the preview, and then release the mouse button.

To hide a column, use the reverse operation: in the column header bar, select the name of the column that you want to hide, by using the left mouse button. Keep the left button depressed and move the name of the column to the "Customization" window, and then release the button.

You can change the layout of the columns displayed by using the same drag & drop method. This is all that is necessary to select one column and to move it to the location desired.
To revert to the original column layout, click on the **Columns** button, and then click on **Reset**.

Lastly, if you want to export all project appliances, then select the menu item, **All clients**. If you only want to export the previous selection then check the box **Only the selection**.

Click on the **Export** button; choose the name and the location of the file. Then the information will be inserted in the file in a particular format: one line per appliance and each field delimited by a previously selected separator.

3.3.1.1. Modifying the project password

It is possible to modify the password protecting the current project.
Select the menu item **Project\Modify password**.
Enter the old project password, and then enter and confirm the new password.

3.3.2. Managing firewalls in the flat view

3.3.2.1. Flat view

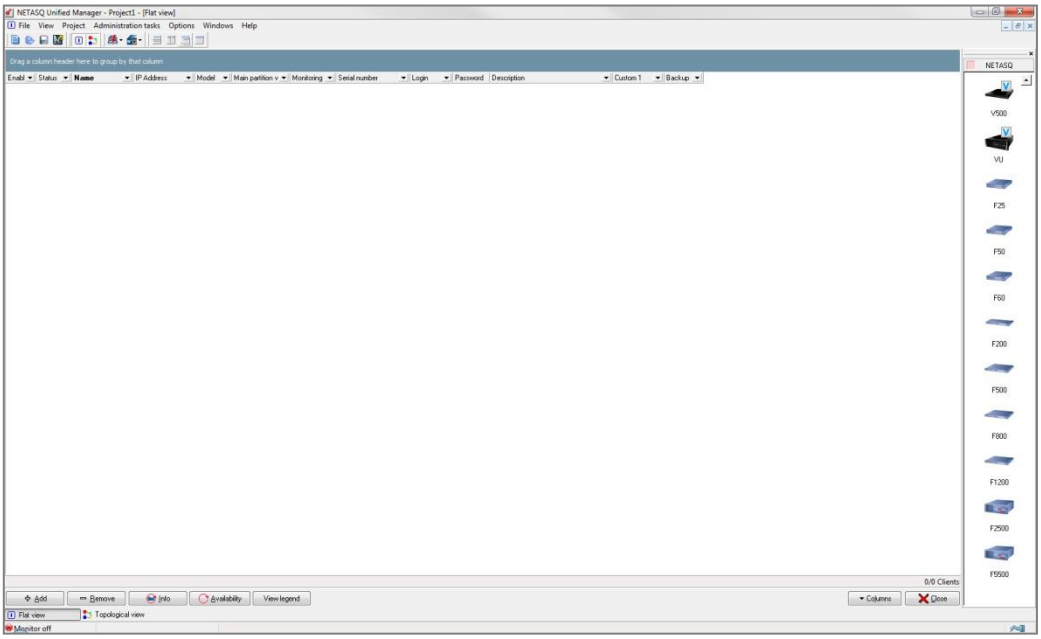

Figure 16 : Flat view

This view contains the list of all the NETASQ equipment that has been added in the project (that has been added from the flat view or from the topological view).
This list is displayed in table form showing the information concerning each one of the appliances.

At the bottom of the view there is a bar with action buttons:

Add	Allows you to add an appliance to the table
Delete	Allows you to delete an appliance from the table
Info	Allows displaying information about the firewall.
Availability	Allows checking whether the firewall is available in case it needs to be used.
Legend	Displays an information window regarding the last connection, high availability, configuration tracking and the connection.
Columns	Manages the display of the table columns.
Close	Closes the view.

3.3.2.1. Managing appliances in a table

3.3.2.1.1. Adding appliance to the table

There are three ways to add an appliance in the flat view:

- use the **Add** button located at the bottom of the view
- use the object bar to the right of the view, if it is displayed. If the bar is not displayed, then select the menu item **`Views\Topological main toolbar`** to display it. Then to add an appliance, all you have to do is choose the desired appliance model in the NETASQ category, then click with the left mouse button in the flat view. You cannot use the objects of the other categories in the flat view.
- by using the contextual menu. To do this, click with the right mouse button in the flat view. Choose the "Add" option.

In these three cases the following window opens, asking you to enter the information relating to the new firewall:

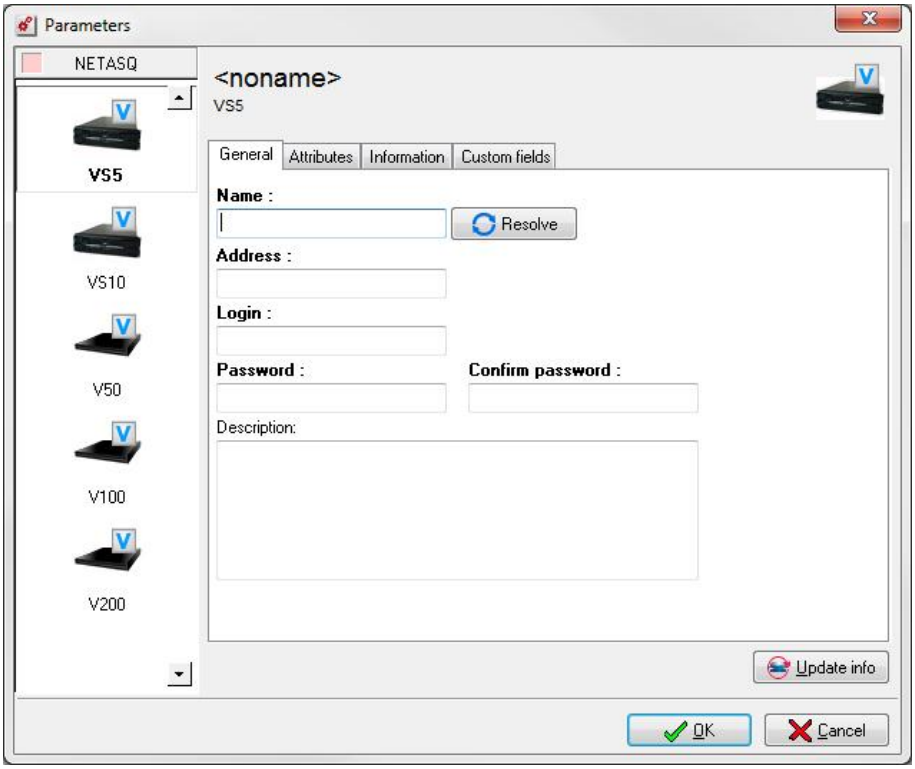

Figure 17 : ***Parameters - General***

. "General" tab

The information requested in the **General** tab is necessary to insert the appliance in NETASQ Global Administration.

Name	Enter the name selected for the appliance. This name will be used to distinguish the appliance from other equipment. The **Resolve** button will resolve IP addresses of "manual" hosts.
Address	Enter the IP address of the appliance that the host (on which NETASQ Global Administration is installed) can contact.
Login	Enter the login for the administration account on the appliance.
Password	Enter the password for the administration account on the appliance.
Confirm password	Confirm the password for the administration account.
Description	Enter comments concerning the appliance.

REMARK

Fields in bold are mandatory.

. "Attributes" tab

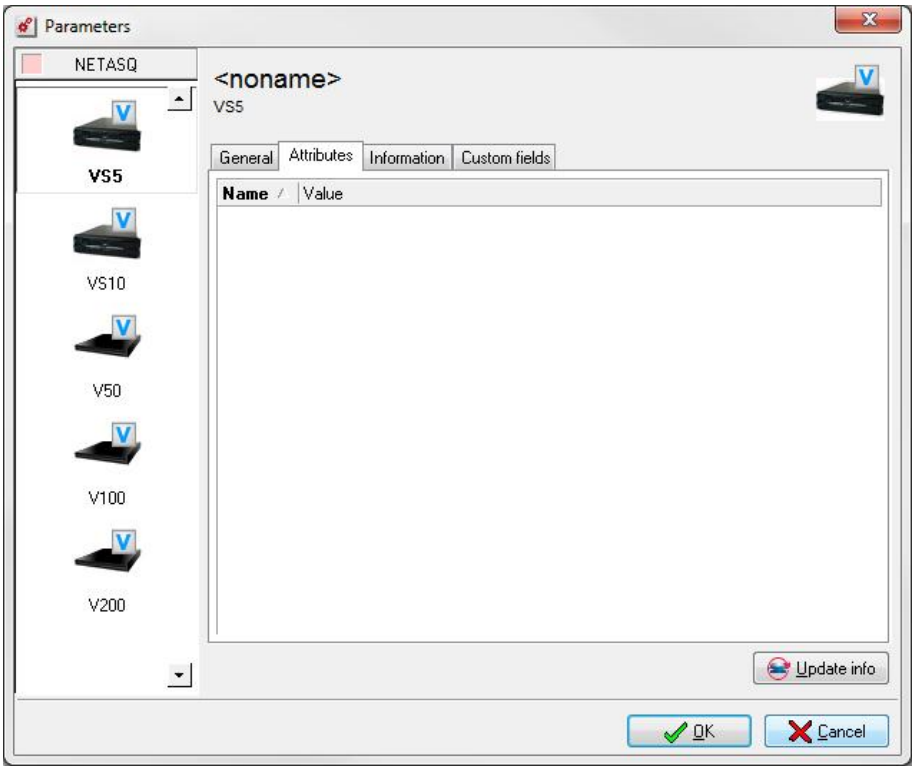

*Figure 18 : **Parameters - Attributes***

This zone does not display data until after an initial update of the appliance information. The data displayed are:

Serial number	NETASQ UTM appliance serial number.
Firmware	Version of the appliance firmware
OEM	Brand under which the product was sold
GMTDate	Firewall date in GMT format
GMTOffset	Deviation of local time from GMT
HA	High availability status
CurrentPartition	Active partition (main or backup)
Backup partition version	Version of the partition that is not active
LastSaveToOtherPartition	Last backupfrom the active partition to the other partition.
Global Admin Options	License option that allows the Firewall to be run in “service” mode. Contact your dealer or NETASQ commercial service for more information about this mode.

To refresh the data of this table, click on the **Update info** button at the bottom of the window.

. **"Information" tab**

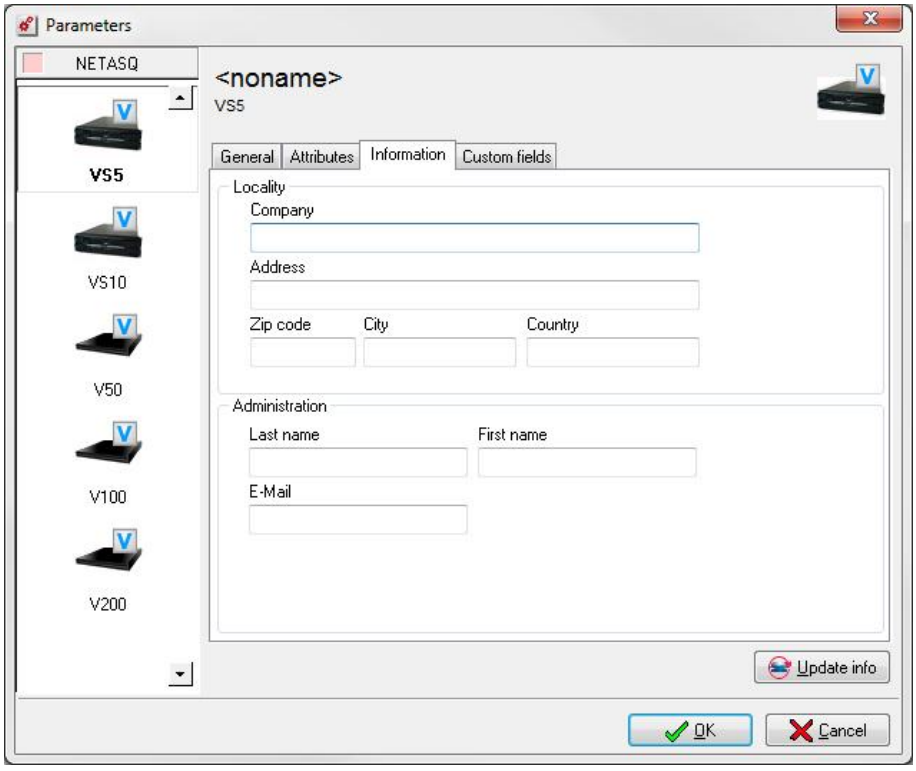

Figure 19 : ***Parameters - Information***

The information requested in this tab is optional and is used to identify the appliance.

Company	Enter the name of the company (or the subsidiary, department…) where the appliance is installed
Address	Enter the address where the appliance is installed.
Zip Code	Enter the postal code of the city where the appliance is installed.
Country	Enter the country where the appliance is installed.
City	Indicate the city in which the UTM appliance is installed.
Last name	Enter the last name of the contact person who manages the appliance locally.
First name	Enter the first name of the contact person
E-mail address	Enter the e-mail address of the contact person.

. "Customized" tab

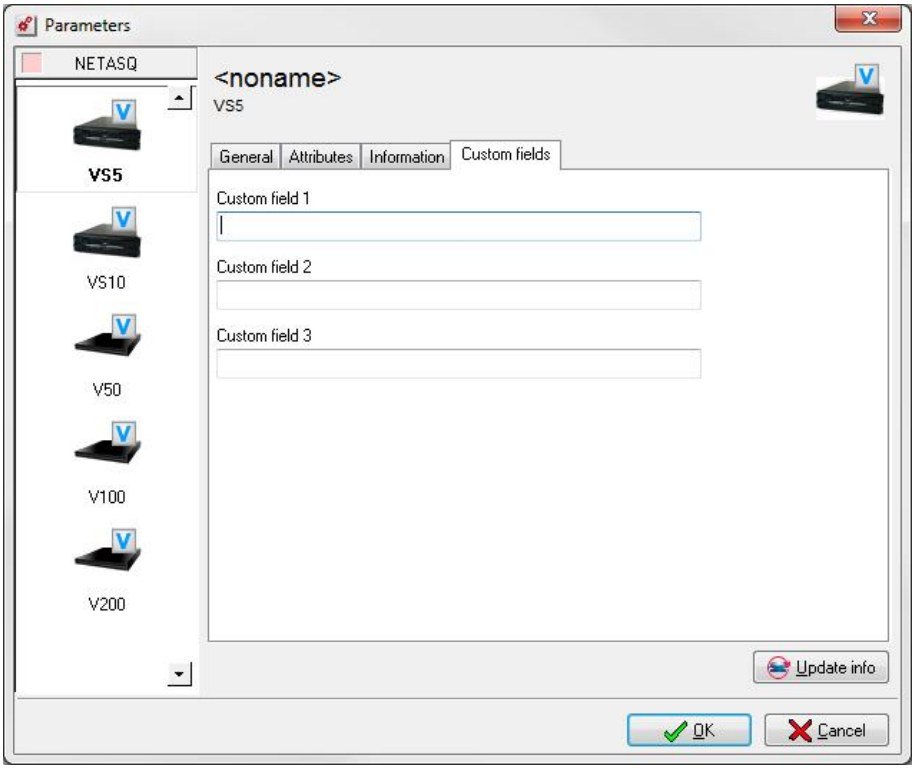

Figure 20 : ***Parameters – Custom fields***

This tab allows you to provide additional information regarding the firewall.

3.3.3. Managing firewalls using the topological view

3.3.3.1. Topological view

The first view that appears when you open a new project is the topological view.

This view, which is more intuitive than the flat view, presents project equipment in a graphic form, showing the topology of the network and sub-networks. Several topologies can be edited with the same objects.

This view can be displayed by selecting the menu item **`View\Topological view`**. If the view is already open, then just click on **Topological view** at the bottom of the screen in the view change bar, to access the view.

The view is organized as follows:

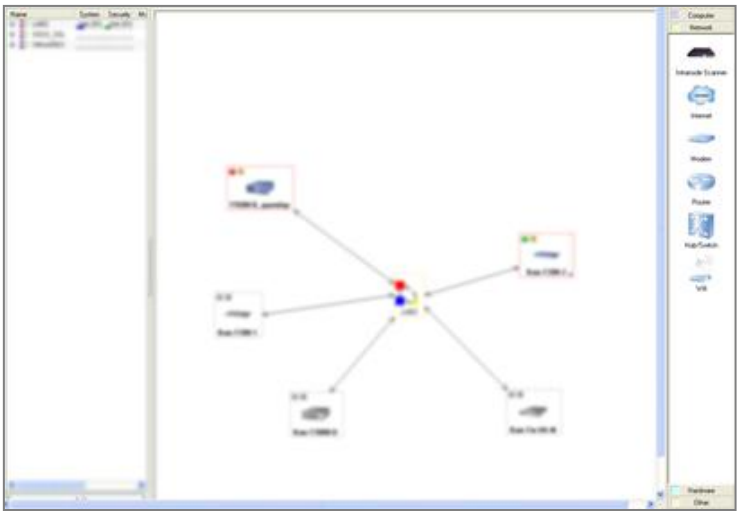

Figure 21 : ***Topological view***

The window is divided into three parts:

- a zone for classifying the topologies (left side of the screen).
- a zone to view a network's or sub-network's topology (in the center).
- the object bar (right side of the screen).

3.3.3.1. Topology classification zone

You can define the group of topologies under a tree-structure in this zone. Thus, administration of the sub-network will be facilitated by dividing the network into several topologies (each one corresponding to a sub-network).

To create the topology tree-structure that will be used in the project, create as many levels and sub-levels that you would like in order to better organize your project. The appliances belonging to each level or sub-level will be displayed in this window.

To create a new grouping at the root level of the tree structure, click on **Add** then “On the root”. A window will ask you to enter the name of the group.

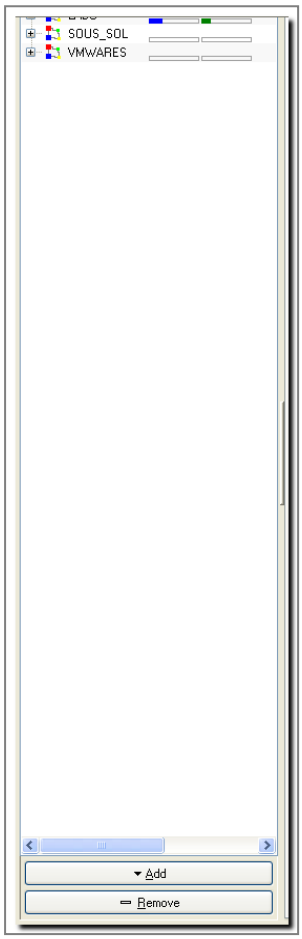

*Figure 22 : **Topology classification***

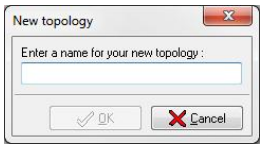

*Figure 23 : **New Topology***

The name will then appear at the root level of the hierarchy.

To create a sub-level in a group, you must select the group that you want to create the sublevel for, and click on **Add**, then on **<Name of the group>**; or click with the right mouse button and select **Add** on <Name of the group>”.
A contextual menu is available to rename or delete this level, or add a sub-level; click with the right mouse button and choose the option desired.

You can create as many groups and sub-levels as you desire.
The sub-levels in a group can be displayed or hidden. When the sub-levels are displayed, the following icon appears in front of the name of the group. Just click on this icon to hide the sub-levels of the group. When the sub-levels are hidden, then the following icon appears in front of the name of the group. Just click on this symbol to display the sub-level of the group.

3.3.3.1.1. Quick view of indicators

In addition to the different topologies and the objects present in these topologies, the classification zone of the topologies also provides a quick view of system and security indicators, as well as of the accumulated alarms present on each Firewall. A more detailed explanation of the indicators is provided later in the document.

3.3.3.2. Topology viewing zone

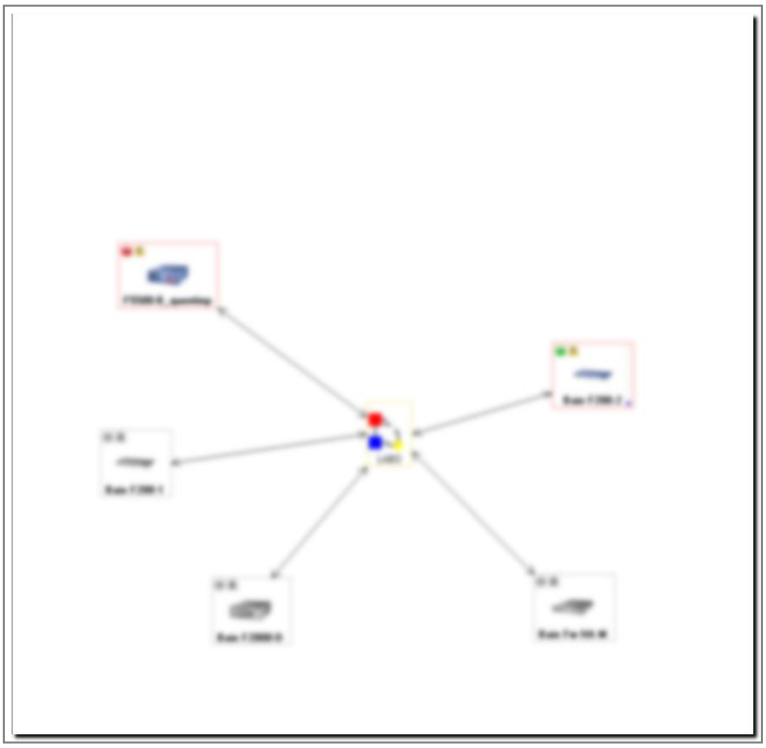

Figure 24 : ***Topology viewing zone***

Use this zone to create and manage the topology of each hierarchical element of the classification zone. To do this, select the element of the hierarchy that you would like to edit, then construct your topological view graphically. The same object can be used in several topologies but may not be used several times in the same topology.

The action bar below the topology visualization zone allows you to:

- **Check all**: this button allows you to check the status of all clients in the zone,
- **Legend:** displays a window with information on the last connection, high availability, configuration tracking and the connection.
- **Zoom +:** zooms in on the visualization zone,
- **Zoom -:** zooms out of the visualization zone.
- **Default zoom**: this button allows you to reset the zoom in the visualization zone.

3.3.3.2.1. Adding, editing and deleting objects in the view

. **Adding an object**

There are two ways to add an object in a view:

- using the object bar to the right of the view, if it is displayed. If the bar is not displayed, then select the menu item **`View\Topological Main Toolbar`** to display it. To add an object, just select the object you want in the desired category, then click with the left mouse button in the general view.
- by using the contextual menu; to do this click with the right mouse button in the visualization zone of the view. Select the object type.

WARNING

Not all objects can be added in this way.

In these two cases the following window opens, asking you to fill in the information relating to the object:

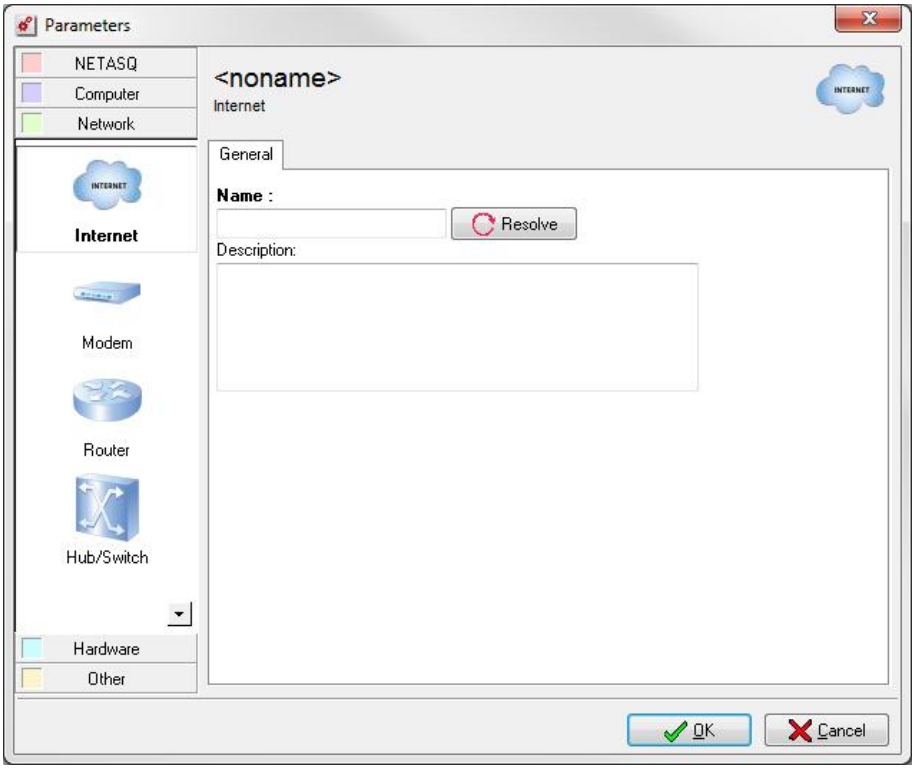

Figure 25 : Parameters – General

. **Editing an object**

To modify the properties of an object, just double click on it, or right-click on the object and choose the "Configure" option in the contextual menu that appears.

. **Deleting an object**

To delete an existing object, select the object with the left mouse button and press the **Del** button.

. **Updating object information**

To manually update the attributes of a NETASQ appliance (software version, high availability status, etc.) double click on the object representing the appliance with the left mouse button and click on the button **Update info** which is present in the new window.

3.3.3.2.1. For "NETASQ" category objects

The following window is the first one displayed:

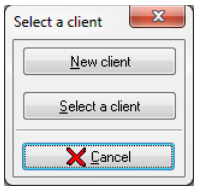

*Figure 26 : **Choosing a client***

If the appliance has already been defined in the flat view, then click on the **Select a client** button and choose the appliance desired, this appliance is then added to the visualization zone. If you want to create a new appliance, then click on the **New client** button and the following window is displayed:

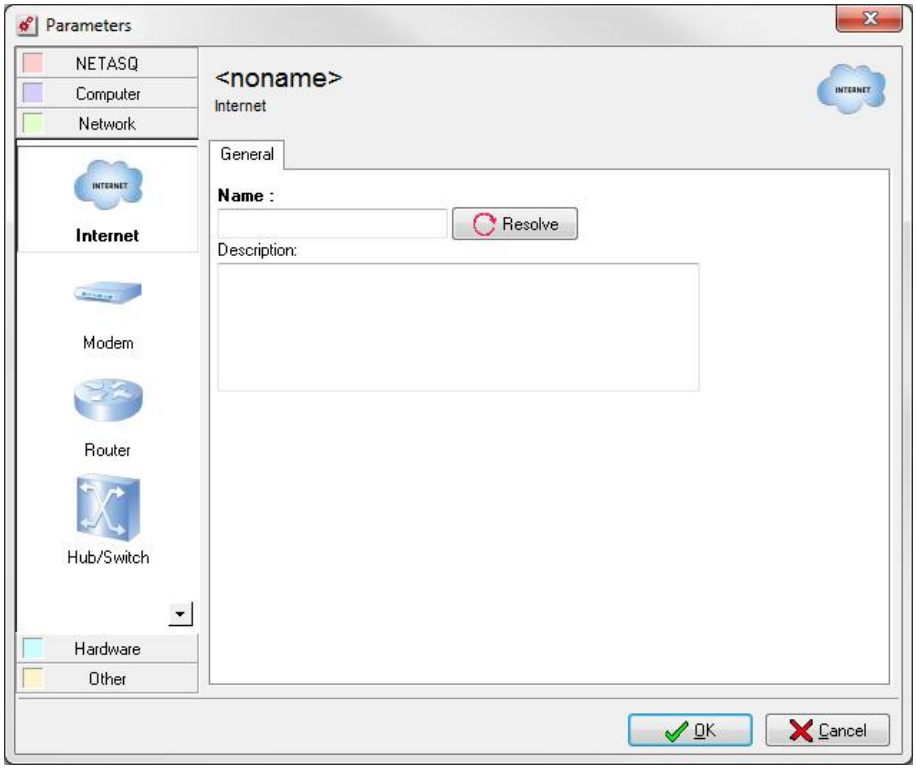

*Figure 27 : **Parameters - General***

Information will then be requested under several tabs:

. General tab

The information requested in the **General** tab is necessary to insert the appliance in NETASQ UNIFIED MANAGER.

Name	Enter the name selected for the appliance. This name will be used to distinguish the appliance from other equipment.
Address	Enter the IP address of the appliance that the host (on which NETASQ Global Administration is installed) can contact.
Login	Enter the login for the administration account on the appliance.
Password	Enter the password for the administration account on the appliance.
Confirm password	Confirm the password for the administration account.
Comments	Enter a comment as desired concerning the appliance.

Fields in bold are mandatory.

. Attributes tab

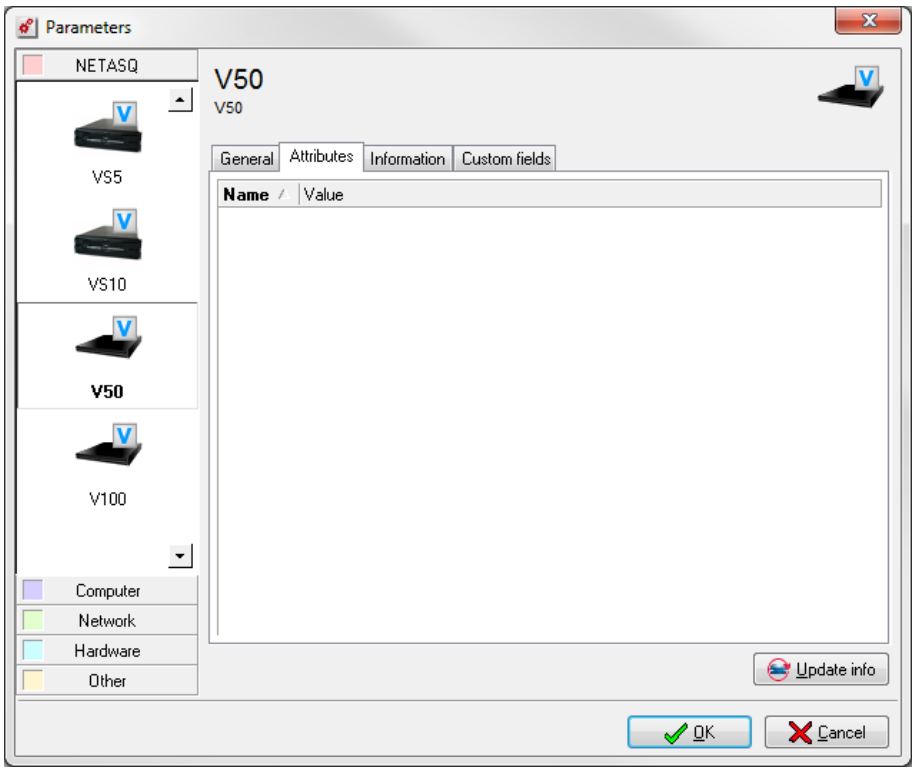

Figure 28 : Parameters - Attributes

This zone does not display data until after an initial update of the appliance information. The data then displayed are:

Serial number	Appliance serial number
Firmware	Version of the appliance firmware
OEM	Brand under which the product was sold
GMTDate	Firewall date in GMT format
GMTOffset	Deviation of local time from GMT
HA	High availability status
CurrentPartition	Active partition (main or backup)
OtherPartitionVersion	Version of the partition that is not active
LastSaveToOtherPartition	Last backup of the active partition to another partition
GlobalAdminOption	License option that allows the Firewall to be run in “service” mode. Contact your dealer or NETASQ sales department for more information about this mode.

To refresh the data of this table, click on the **Update info** button at the bottom of the window.

. **Information tab**

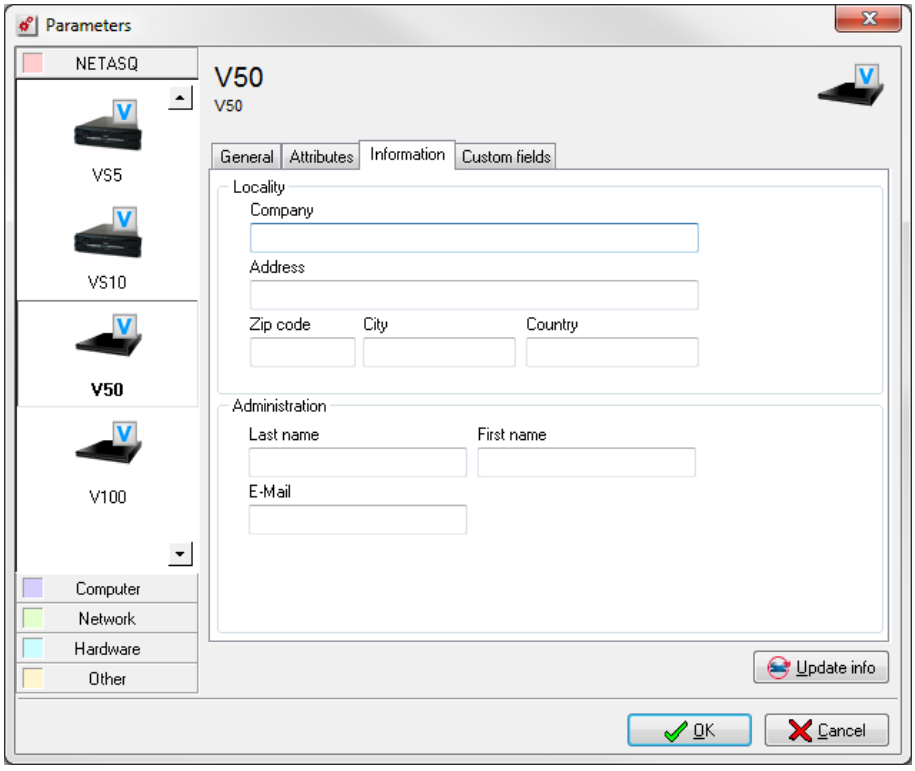

*Figure 29 : **Parameters - Information***

The information requested in this tab is optional and is used to identify the appliance.

Company	Enter the name of the company (or the subsidiary, department, etc.) where the appliance is installed
Address	Enter the address where the appliance is installed.
Zip Code	Enter the zip code of the city where the appliance is installed.
City	Enter the city in which the firewall has been installed
Country	Enter the country where the appliance is installed.
Last name	Enter the last name of the contact person who manages the appliance locally.
First name	Enter the first name of the contact person
E-mail address	Enter the e-mail address of the contact person.

You can also change the appliance model selected; to do this, just select a new model in the bar to the left of the window.

The appliance is then added in the visualization zone. A question mark is displayed in the top left corner of the object if no information regarding the appliance has been downloaded yet. This icon will disappear as soon as information will be updated.

3.3.3.2.1. For a “computer” category object

The following information will then be requested:

Name	Enter the name selected for the object. This name will be used to distinguish the object from other equipment.
Address	Enter the IP address of the object which the host (on which NETASQ Global Administration is installed) can contact.
Login	Enter the administration account login for the object.
Password	Enter the administration account password for the object.
Confirm password	Confirm the password for the administration account.
Description	Enter a comment as desired concerning the object.

Fields in bold are mandatory.
Click on **OK**. The object is then added in the preview zone.

3.3.3.2.1. For “Network” category objects

Then the following information will be requested:

Name	Enter the name selected for the object. This name will be used to distinguish the object from other equipment.
Address	Enter the IP address of the object which the host (on which NETASQ Global Administration is installed) can contact.
Login	Enter the administration account login for the object.
Password	Enter the administration account password for the object.
Confirm password	Confirm the password for the administration account.
Description	Enter a comment as desired concerning the object.

Fields in bold are mandatory.
Click on **OK**. The object is then added in the preview zone.

3.3.3.2.1. For a “Hardware” category object

Then the following information is requested:

Name	Enter the name selected for the object. This name will be used to distinguish the object from other equipment.
Address	Enter the IP address of the object which the host (on which NETASQ Global Administration is installed) can contact.
Login	Enter the administration account login for the object.
Password	Enter the administration account password for the object.
Confirm password	Confirm the password for the administration account.
Description	Enter a comment as desired concerning the object.

Fields in bold are mandatory.
Click on **OK**. The object is then added in the preview zone.

3.3.3.2.1. For “Other” category objects

This category only contains the objects “Note” and “Topology”. The “Note” object allows you to define a zone where it is possible to include text in the visualization zone. Enter the text that you would like to have displayed.

The “Topology” object allows you to define a zone, representing a different topology already defined, on the visualization zone; clicking on the object directly accesses the view of the corresponding topology. Choose the topology that will be linked when you edit this object.

For both objects, indicate the text you would like to display.
Click on **OK**. The object is then added in the preview zone.

3.3.3.2.2. Topological View contextual menu

A right click on Topological View opens the contextual menu. The features accessible from the contextual menu are different when selecting an object or when placing the pointer over empty space. Unlike in General View, here they are complementary. We will describe both menus.

. Contextual menu on a Topological View object

The Topological View contextual menu provides access to the following submenus:

Configure	Access to the firewall configuration. Reminder: Double clicking on the object also allows you to access the configuration.
Disable	Stops a firewall from being taken into account in the General View. This action allows you to block the appliance from all actions possible in NETASQ Global Administration, without having to remove the appliance.
Disable monitoring	Monitoring can now be enabled and disabled. By default, it is enabled as long as the license allows it.
Delete	Removes a firewall from the Topological View.
Manage	Opens NETASQ UNIFIED MANAGER.
Tools	Access to NETASQ configuration tools and external tools.
Direct configuration	Access to direct configuration (See 20.3.10. Direct configuration).
Maintenance	Access to NETASQ Global Administration maintenance functions.
Deployment	For deploying the configurations in NETASQ Global

Scripts…	Enables the execution of NETASQ scripts on targeted appliances.
Test availability (ping)	Availability test (tries to connect to serverd).
Check status	Manual update of the appliance status
Reset alarms	Enables resetting alarm statuses to their default values.

. Contextual menu outside a Topological View object

This Topological View contextual menu provides access to submenus for adding configurable objects in NETASQ UNIFIED MANAGER mode:

- NETASQ UTM.
- Host: NETASQ UNIFIED MANAGER workstations, servers, others.
- Network object: switch, modem, other.
- Hardware object.
- Notes.
- Topologies.

3.3.3.3. Adding, editing, and deleting a link between two objects

. Adding a link

When several objects have been created and added to the topology visualization zone, you can represent the physical links that exist between them (Ethernet connection, dial-up connection, WiFi, customized, etc.).

To do this, just use the right mouse button. Click on the first object that you would like to include in this link, with the right mouse button. Keep the button depressed and move the cursor to the object that constitutes the second extremity of the link, then release the button. A line has been drawn between the two objects and a window opens.

Enter the following information in this window:

Link label	Enter a name here to denote the link. This name will be displayed below the link, in the visualization zone.
Types	Link types: Ethernet, WIFI (radio), dial-up, or custom. Each link type has a different color in the display. Use the custom link type to define a personalized link type.
Attributes	Link attributes: high throughput (100M or Gigabyte link, for example), encryption level (none, low or high encryption)

Link color	You can define a color that has been personalized in the color palette for the "Custom" link type.
Source	The drop-down list allows you to specify whether an arrow should point to the source object (first object selected when creating the link).
Destination	The drop-down list allows you to specify whether an arrow should point to the destination object (second object selected when creating the link).

The link is then completely created and joins both objects. It is also possible to link a topology object to other objects.

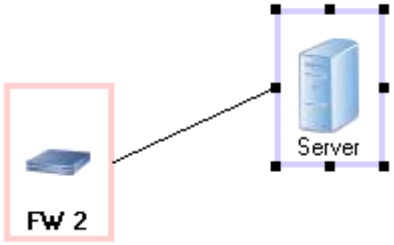

Figure 30 : Link

The link will be displayed differently depending on parameters chosen in the previous window: a different color for each link type, a thick line for a high-throughput link, a key on the link if an encryption level has been chosen.

. Modifying a link

To modify the properties of a link, double click on it with the left mouse button and the window that was described previously will open.

It is possible to modify the link appearance if you want curved lines to represent the links for layout and object presentation reasons. To do this click with the left mouse button on the place where you want a curve, then move the link, keeping the mouse button depressed. Release the button when the appearance of the link is satisfactory.

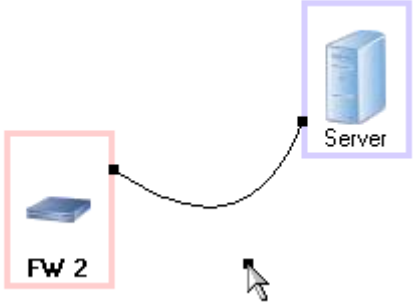

Figure 31 : Link

. **Deleting a link**

To delete a link, click on it with the left mouse button and press the **Del** button on your keyboard.

. **Moving one or several objects**

Select an object or the objects that you want to move, and then move the selection to the required location, keeping the left mouse button depressed.

3.3.4. System and security indicators

The Global Administration mode allows high-performance monitoring of system and security events for NETASQ objects in Topological View. Indeed, the Global Administration mode offers an indicators window for each NETASQ appliance. This window can be updated by the monitor in the Global Administration mode, or it can be manually updated using the "status verification" function.

These indicators are grouped in two categories: System indicators, which apply to the surveillance of events relating to the Ethernet interfaces supported by the Firewall processor, and security indicators, which apply to the surveillance of alarms and the events relating to the ASQ kernel.

3.3.4.1. Topological View indicator window

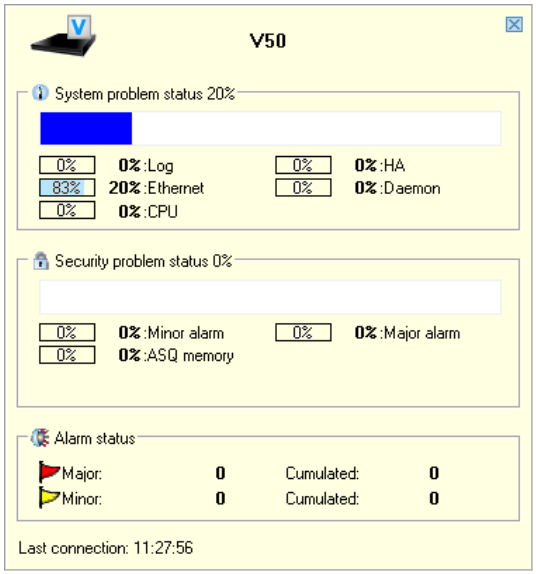

*Figure 32 : **Indicators***

The indicator window groups several information items concerning the Firewall monitored:

- The name of the Firewall.
- The level of system problems,
- The level of security problems,
- The status of the alarms,
- The last time the monitor in Global Administration mode connected to this firewall.

3.3.4.2. System indicators

The first section of the indicators window groups the system indicators. These 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 weight of system events in relation to each other in order to present a coherent status of the Firewall. Each indicator is presented in the following manner:

> [percent] percent: name of the indicator

The following example is used to explain the information presented:

> **Example**
>
> [75%] 17%: Ethernet

The first percentage listing refers to the level of Ethernet problems. For instance in this case 3 out of 4 Firewall interfaces are not connected whereas the administrator has defined them as active in NETASQ UNIFIED MANAGER. Surely there is a problem with these interfaces.

The second percentage refers to the global incidence of these problems on the Firewall. Here you will see that each of the system events is weighted with a maximum weight threshold on the Firewall's general status.

3.3.4.3. Security indicators

The second section of the indicator window groups the system indicators. These indicators concern:

- Minor alarms: indicators relating to the number of minor alarms,
- Major alarms: indicators relating to the number of major alarms,
- ASQ memory: indicators relating to the occupation rate of the ASQ memory.

The display of these indicators is based on the weight of security events in relation to each other in order to present a coherent status of the Firewall. Each indicator is presented in the following manner:

> **Example**
>
> [percent] percent: name of the indicator

See the section on system indicators for a more thorough explanation of the information presented.

. Alarm status

Alarm status is set out in the section “Security Indicators” because they are closely linked. Parameters can be set in the project options in this section.

The number of alarms (major or minor) raised between NETASQ REAL-TIME MONITOR updates and a cumulative total of alarms raised from the launch of NETASQ GLOBAL ADMINISTRATION, are presented by alarm type (major or minor).

3.3.5. Administration tasks

3.3.5.1. Presentation

The primary function of NETASQ Global Administration is to facilitate the administration of a group of NETASQ appliances using the various tools integrated in the product.

NETASQ Global Administration can connect to the NETASQ website in order to automatically download firmware updates, and appliance licenses, and it can also install them automatically on the various appliances that are being managed.

WARNING

During administrative tasks, you are advised to deactivate the NETASQ Global Administration monitor (see the Monitoring and supervision section for more details).

The "Administration tasks" menu item is the main administrative tool of NETASQ Global Administration which enables updating appliances and licenses, deploying security policies, creating scripts, etc.

Configuration	Backs up and restores the configurations of appliances.
Update firmware	Updates the firmware of appliances.
Update license	Updates the licenses of appliances.
Back up partition	Backs up main partitions on secondary partitions (backup partitions).
Scripts	Enables the execution of NETASQ scripts on targeted appliances.
Deployment	Enables the deployment of security policies and object databases.

3.3.5.2. Configuration

The Global Administration mode allows you to back up or restore the configurations of the selected appliances. These functionalities are accessible through the following menu:
`Administrative tasks\configuration\Backup` or **`Restore`**.

3.3.5.2.1. Configuration backup

A Backup wizard appears.

Step 1

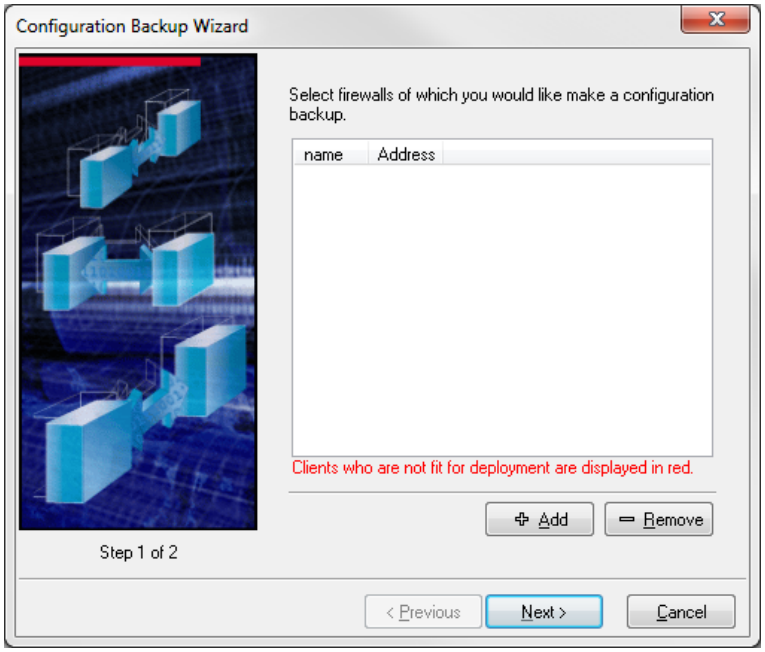

Figure 33 : ***Backup wizard - Step 1***

Select the Firewall whose configuration you want to back up.
Click on **Add**, the following window will appear:

Step 2

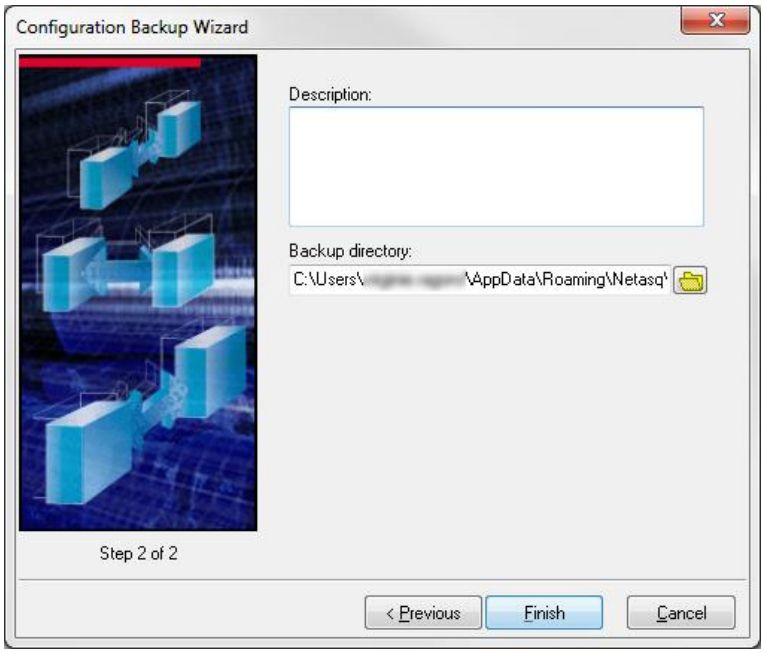

Figure 34 : Assistant de sauvegarde - Etape 2

This step allows you to add a description to the backup and to specify the backup directory where you want to store the backups. By default the backup directory is the one defined in the preferences in the Global Administration mode. Click on **Finish** to back up the configurations.

The window for managing the backups of the configurations will appear. It summarizes the parameters defined in the configuration backup assistant.

By default the first column entitled "BP" is for specifying the breakpoints in the execution of the configured task. The principle is as follows: upon specifying a breakpoint on a line, the configured task will first be started on each of the appliances located below or on this breakpoint in the table, then if all the tasks are successfully completed, NETASQ Global Administration mode will execute the tasks for the appliances which follow. To specify a breakpoint, double click on the desired line. To delete a breakpoint, double click on the breakpoint.

By default the second column displays a signal light. The color of the signal light depends on the status of the action:

	Waiting.
	Action begun
	Action cancelled or not performed
	Action successfully completed

Thereafter the table is composed of the following columns:

Name	Name chosen for the appliance
Address	IP address of the appliance
Status of the task	Status of the action (waiting, begun, completed, etc.)
Current version	Current version of the firmware of the appliance
Description	Comments relating to the backup.

. Adding configuration

Add the appliances you want to back up to the table of appliances by clicking with the right mouse button, and then choosing **Add** in the contextual menu that is displayed.

Then choose **`Firewalls`** if you want to select the appliances to back up or **`All activated firewalls`** if you want to update all the active Firewalls (those with ON status in the flat view).

To remove an appliance from the list, select it and right-click on it and select **Remove**.
The **Reset** button resets the configuration backup tasks.

WARNING

for the backup to be effective the information concerning the chosen appliances must have been updated (via the **Update info** button of the flat view).

. **Backing up configurations**

Click on the **Update all** button. The signal light then changes to orange on the appliances that are being updated and you can see the progress bar advance. All the appliances will be updated, simultaneously.

3.3.5.2.1. Restoring the configuration

To back up the configuration of one or several appliances, select the menu **`Administrative tasks\Configuration\Restore`**. There are four steps in the restoration of a configuration.

Step 1

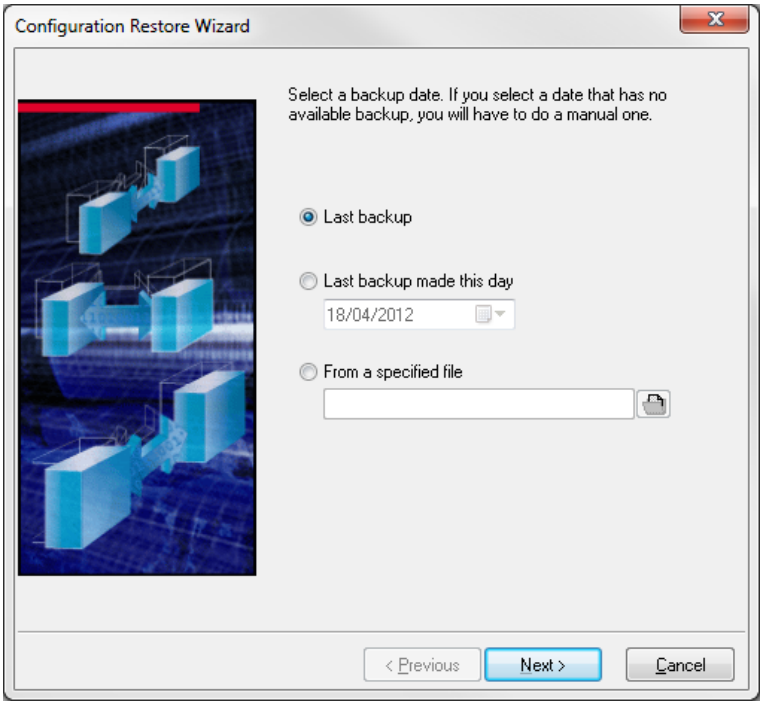

*Figure 35 : **Restoration wizard***

Steps 1 and 2 consist of defining the backup to be used for the restoration by defining the backup date and source.
Last backup: This option is for specifying the last backup located in the configuration backup directory.
Last backup made on the date indicated: This option is for specifying the last backup on the date indicated in the configuration backup directory. Use the calendar provided to define the search date.
From file: Specify the backup file that you wish to restore. If you select this parameter, the wizard will skip Step 2 (explained below).

Step 2

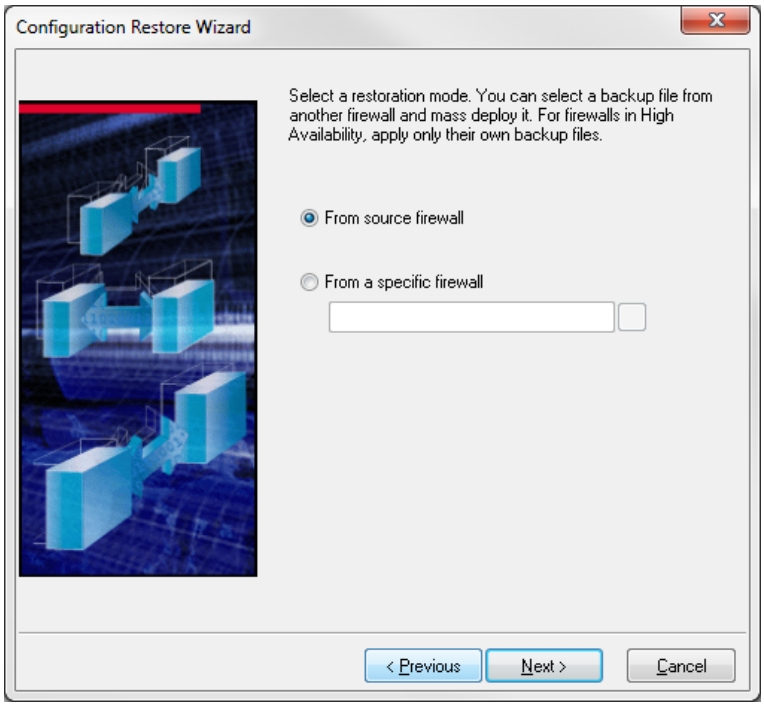

Figure 36 : ***Restoration wizard***

From source Firewall: This option is for specifying a backup located in the configuration backup directory created from the Firewall on which the restoration will be executed.
From a specific firewall: This option is for specifying a backup located in the configuration backup directory created from the selected Firewall.

Step 3

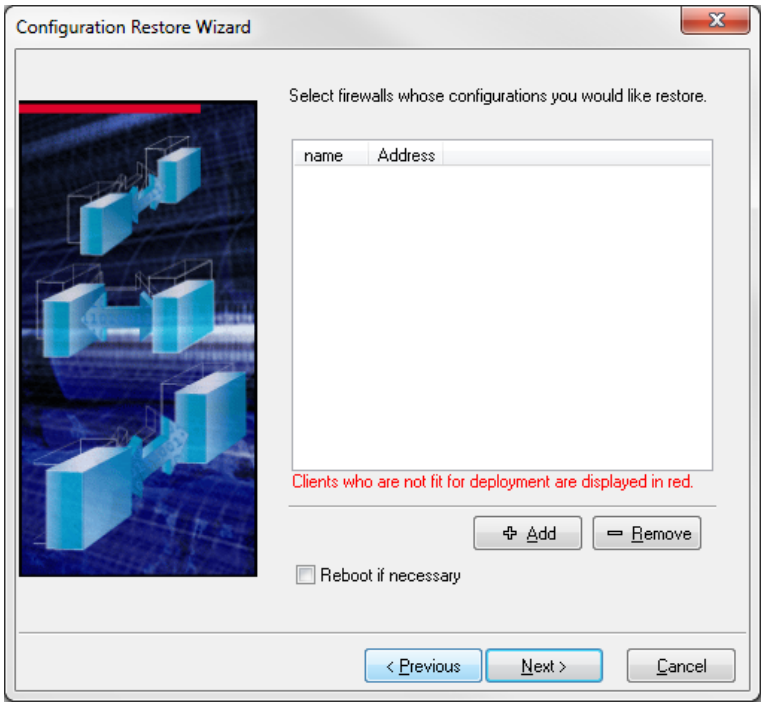

Figure 37 : Restoration wizard

Step 3 consists of defining the Firewalls on which a restoration has to be performed.
The option **Reboot if necessary** allows indicating whether the appliance will be rebooted if the need arises, to apply changes to files due to the restoration.

Etape 4

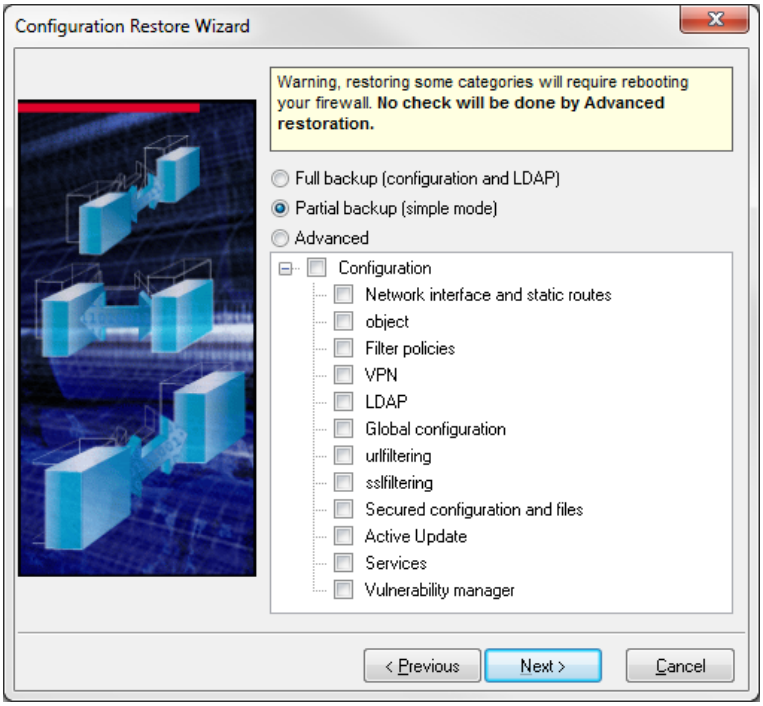

Figure 38 : Restoration wizard- Simple

In your previous selections, if you had selection either “From the original firewall” or “From a specific firewall”, the restoration wizard will allow you to select three types of restoration:

- Configuration and LDAP (Full restoration): this choice allows you to restore the appliance’s configuration and all information stored in the LDAP database (user records). This configuration restores everything without options.
- Simple (Partial restoration): this choice allows you to restore the appliance’s configuration according to the administrator’s choices. This type of partial configuration allow, for example, restoring the object database and to ease the administrator’s workload.
- Advanced (Partial restoration): this option, which is more granular than the simple mode, allows the most specific selection restoration-wise. But proceed with caution, as this type of restoration allows the restoration of incomplete configurations (IPSec VPN tunnels without their keys, for example).

The restoration options are as follows:

- Configuration: selects all the elements classified under this header.
- Interfaces and static routing: appliance's network configuration, configuration of interfaces, default gateway and static routes.
- Objects: object database, excluding users.
- NAT policies: all the address translation configuration slots.
- Filter policies: all filter configuration slots.
- Configuration and LDAP, PKI databases: configuration of the appliance's LDAP database, as well as the elements saved in the database (users) and PKI configuration.
- URL filter groups and policies: all URL filter configuration slots as well as static URL groups (created by the administrator).
- Global configuration: all global configuration slots as well as global objects.
- Secure configuration and secure files: secure configuration and encrypted files secured by secure configuration.
- Active Update: configuration of the appliances automatic update module.
- Proxies: configuration of HTTP, SMTP and POP3 proxies.
- Certificates and pre-shared keys: certificates stored in the "Certificates" menu and configured pre-shared keys.
- Intrusion prevention (ASQ): configuration of the appliance's intrusion prevention engine, ASQ
- SSL VPN module configuration: configuration of the SSL VPN module.
- PPTP tunnel configuration: configuration of the PPTP server.
- IPSec VPN tunnels: configuration of IPSec VPN tunnels only.
- Time schedule: schedule defined for slots.
- Event rules: event rules configured manually by the administrator.
- QoS: configuration of Quality of Service policies.
- Authentication: configuration of authentication.
- Indicators (system and security): indicators found in Global Administration.
- DHCP server: appliance's DHCP service.
- NTP Client: appliance's NTP service.
- DNS Proxy: appliance's DNS service.
- SNMP Agent: appliance's SNMP service.
- Logs: configuration of logs only.
- Static routing: default gateway and configured static routes.
- System events: configuration of system events.
- Dynamic routing: configuration of the dynamic routing platform.
- Antispam: Antispam module.
- Communication (syslog, notifications): appliance's communication module, notably the sending of logs to syslog servers and the sending of alarm notifications to administrators.
- Data: selects all the elements classified under this header.
- Dynamic URL groups: all dynamic URL groups, obtained via Active Update.
- Contextual signatures: ASQ signatures obtained via Active Update.

Step 5

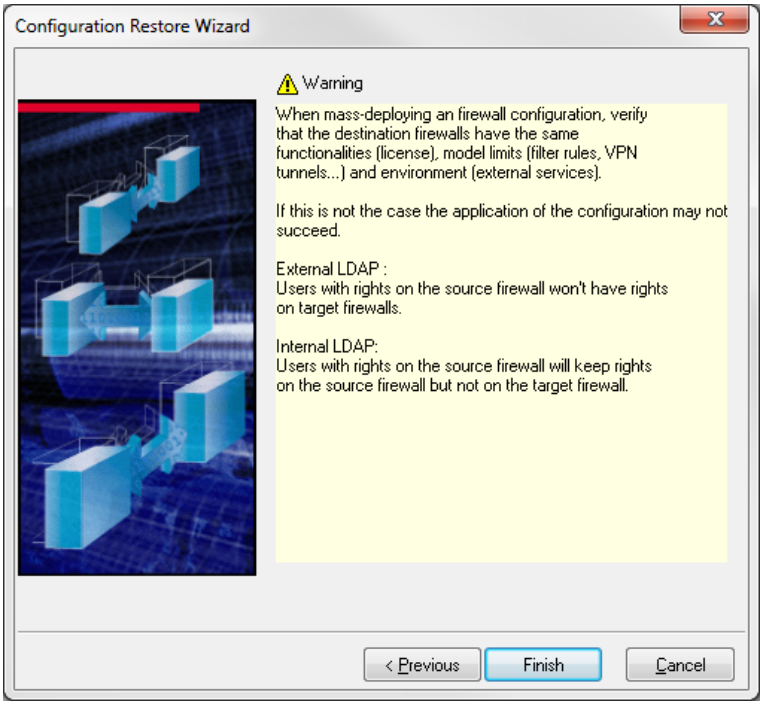

Figure 39 : ***Restoration wizard***

. **Configuration restoration manager**

When all parameters have been defined, click on **Finish** to restore the configurations. The configuration restoration window will appear. It will summarize the parameters defined in the configuration backup wizard. In this window, you will be able to modify the defined parameters.

3.3.5.1. Updating the firmware

➲ Sélectionner le menu `Tâches administratives\Mettre à jour le firmware.`

By default the first column entitled “BP” is for specifying the breakpoints in the execution of the configured task. The principle is as follows: upon specifying a breakpoint on a line, the configured task will first be started on each of the appliances located below or on this breakpoint in the table, then if all the tasks are successfully completed, the Global Administration mode will execute the tasks for the appliances which follow. To specify a breakpoint, double click on the desired line. To delete a breakpoint, double click on the breakpoint.

By default the second column displays a signal light. The color of the signal light depends on the status of the action:

	Waiting
	Action begun
	Action cancelled or not performed
	Action successfully completed

Thereafter the table is composed of the following columns:

Name	Name chosen for the appliance
Address	IP address of the appliance
Status of the task	Status of the action (waiting, begun, completed, etc.)
Current version	Current version of the firmware of the appliance
Update version	Update versions available for this appliance. You can choose the "custom" option in the drop-down list. This option allows you to choose an update file that will be stored locally on the administration machine.
Storage	Location of the update (Internet if it is on the NETASQ website, custom, if it is local)
Task progress	Progress of current task
Result	Update task result
Message	Explanatory message relating to the "Result" field

Some information displayed may not be particularly necessary for you, and by the same token, you may want to display information that is useful to you. You can hide and display certain table columns. To do this, click on the **Customize Columns** button.

3.3.5.1.1. Choosing the UTM appliances to update

Add the appliances you want to back up to the table of appliances by clicking with the right mouse button, and then choosing **Add** in the contextual menu that is displayed.

Then choose **`Firewalls`** if you want to select the appliances to back up or **`All activated firewalls`** if you want to update all the active Firewalls (those with ON status in the flat view).

To remove an appliance from the list, select it and right-click on it and select **Remove**.

WARNING

In order for updates to be carried out, information on the selected firewalls has to be updated (using the button **Update information in flat view**).

3.3.5.1.1. Updating NETASQ UTM appliances

Select the update version to install for each appliance (in the "Update version" column) then click on **Update** button. The signal light then changes to orange on the appliances that are being updated and you can see the progress bar advance. All the appliances will be updated, one after another.

WARNING

You are strongly advised to perform a partition backup after each firmware update.

3.3.5.1. Updating the license

When you select the **`Administration tasks\Update the license`** menu item the window "Licenses updating" opens.

By default the first column entitled "BP" is for specifying the breakpoints in the execution of the configured task. The principle is as follows: upon specifying a breakpoint on a line, the configured task will first be started on each of the appliances located below or on this breakpoint in the table, then if all the tasks are successfully completed, the Global Administration mode will execute the tasks for the appliances which follow. To specify a breakpoint, double click on the desired line. To delete a breakpoint, double click on the breakpoint.

By default the second column displays a signal light. The color of the signal light depends on the status of the action:

	Waiting
	Action started.
	Action aborted or not performed.
	Action successfully terminated.

Thereafter the table is composed of the following columns:

Name	Name chosen for the appliance
Address	IP address of the appliance

Status of the task	Status of the action (waiting, begun, completed, etc.)
Current version	Current version of the firmware of the appliance
License version	Current version of the license.
Task progress	Progress of current task
Result	Update task result
Message	Explanatory message relating to the “Result” field

WARNING

The version number of the license does not correspond to the version number of the firmware. These two numbering systems are totally independent.

3.3.5.1.1. Choosing the appliances for which licenses must be updated

Add the appliances you want to update to the table of appliances by clicking with the right mouse button, and then choosing **Add** in the contextual menu that is displayed.

Then choose **Firewalls** if you want to select the appliances to update or **All activated firewalls** if you want to update all the active Firewalls (those with ON status in the flat view).

To remove an appliance from the list, select it, right-click on it and select **Remove**.

WARNING

For the updates to be effective the information concerning the chosen NETASQ UTM appliances must have been updated (via the **Update info** button in the flat view).

3.3.5.1.2. Updating the licenses of the appliances

Click on **Update**. The signal light then changes to orange on the appliances that are being updated and you can see the progress bar advance. All the appliances will be updated, one after another.

3.3.5.2. Backing up the partition

This feature enables backing up a complete system remotely from the main partition (the active partition) onto the backup partition. In this way, if a problem arises on the active partition, it will be possible to boot the system using an up-to-date backup partition. You are strongly advised to perform a backup after each firmware update.

Select the **`Administration tasks\Partition backup`** menu.

By default the first column entitled "BP" is for specifying the breakpoints in the execution of the configured task. The principle is as follows: upon specifying a breakpoint on a line, the configured task will first be started on each of the appliances located below or on this breakpoint in the table, then if all the tasks are successfully completed, NETASQ Global Administration mode will execute the tasks for the appliances which follow. To specify a breakpoint, double click on the desired line. To delete a breakpoint, double click on the breakpoint.

By default the second column displays a signal light. The color of the signal light depends on the status of the action:

	Waiting.
	Action begun
	Action cancelled or not performed
	Action successfully completed

Thereafter the table is composed of the following columns:

Name	Name chosen for the appliance
Address	IP address of the appliance
Status of the task	Status of the action (waiting, begun, completed, etc.)
Current version	Current version of the firmware of the appliance
Other partition	Version of the appliance's backup partition
Task progress	Progress of current task
Result	Update task result
Message	Explanatory message relating to the "Result" field

3.3.6. Scripts

Global Administration enables the deployment and execution of formatted scripts according to the NSRPC configuration mode, which allows the full configuration of NETASQ appliances. As such, scripts provide a solution for deploying the configuration of a whole fleet of appliances for features that have not been included in Global Administration's deployment menus.

Selecting the **Administration tasks\Script** menu item opens the window "Executing scripts".

Step 1

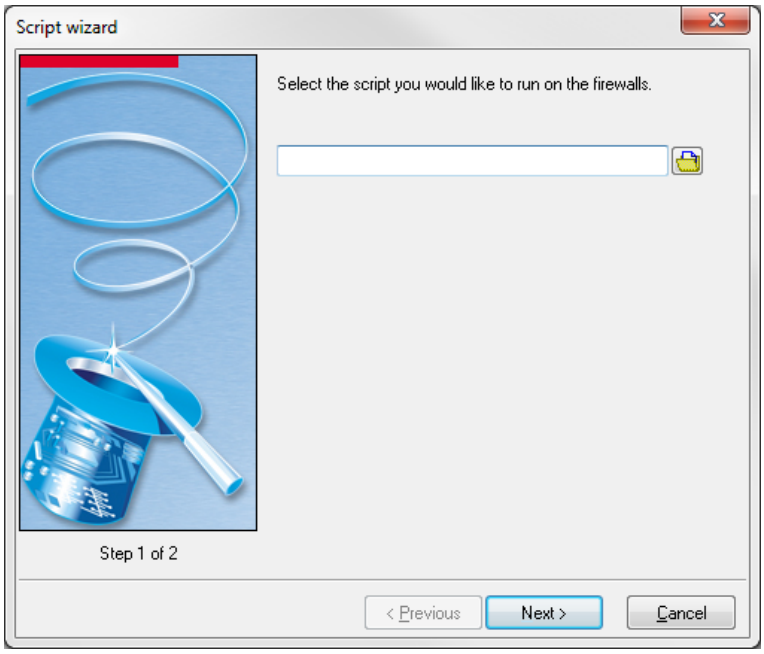

Figure 40 : ***Script wizard - Step 1***

The first step in the script deployment wizard requires the definition of a script that has to be deployed and then executed. Therefore, select the script to be executes on the firewalls and click on **Next**.

Step 2

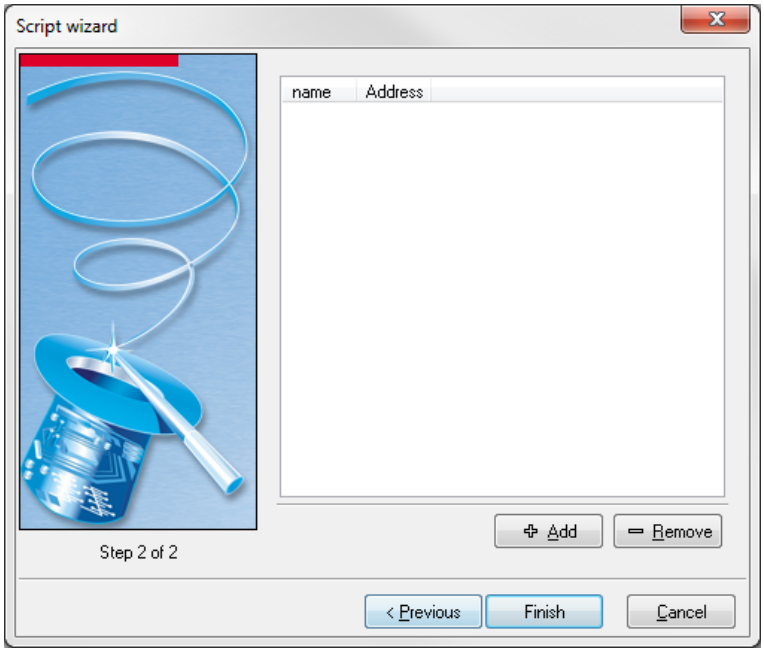

*Figure 41 : **Script wizard - Step 2***

The second step in the script deployment wizard requires the definition of the appliances that will be affected by this deployment. To do this, click on **Add** to open the window that displays the available appliances. When you click on **Finish**, the script deployment and execution window will appear:

3.3.6.1. Executing the script on firewalls

Click on **Execute**. The LED will turn to orange on appliances that are being backed up and you can track its progress with the progress bar. All the appliances will be updated, one after another.

3.3.6.2. Building a script

Scripts are formatted as NSRPC commands grouped together in a file that will be specified in the script deployment wizard. Refer to the related documentation on NETASQ's website for further information on the NSRPC configuration mode.

WARNING

All commands with negative results will disrupt the execution of the script.

NSRPC commands can be associated with macros or variables which will ease the mass deployment of defined scripts.

. Comments

Comments can be inserted between the different lines of script, and begin with the character #.

. Macros

Macros represent the variables associated with the appliance on which the script will be deployed. A macro has to be framed by the character "%" in order to be interpreted correctly, e.g. %MACRO%.

The following macros can be used in scripts:

WARNING

Macros are not case-sensitive.

- **APP_PAT:** Full path of the file, including the application "path delimiter",
- **FW_ADDRESS:** Firewall's IP address,
- **FW_COMPANY**: Company in which the firewall has been installed,
- **FW_COUNTRY**: Country in which the firewall has been installed,
- **FW_DESCRIPTION:** Firewall's "Description" field,
- **FW_LOCATION:** Location of the firewall,
- **FW_MODEL:** Firewall's model,
- **FW_NAME:** Firewall's name,
- **FW_SERIAL:** Firewall's serial number,
- **FW_VERSION:** Firewall's version name,
- **FW_ZIP_CODE**: Zip code of the area in which the firewall was installed,
- **FW_CITY:** City in which the firewall was installed,
- **FW_CUSTOM1:** Custom field number 1,
- **FW_CUSTOM2:** Custom field number 2,
- **FW_CUSTOM3:** Custom field number 3,
- **NOW:** Full date of the local format,
- **NOW_AS_DATE:** Date of the local format,
- **NOW_AS_TIME:** Time of the local format,
- **SCRIPT_PATH:** Full path of the script file, including the application "path delimiter",
- **ADMIN_LASTNAME:** Administrator's last name,
- **ADMIN_FIRSTNAME**: Administrator's first name,
- **ADMIN_EMAIL:** Administrator's e-mail address.

. Functions

Certain undefined functions in the NSRPC commands have to be used for backup and restoration operations, for example. These functions begin with the character $ and are case-sensitive:

The syntax for these functions is therefore as follows: $FUNCTION("file path"). Please note that the quotation marks following the opening bracket and preceding the closing bracket are mandatory.

The following are the functions:

- **SAVE_TO_DATA_FILE:** Saving a file without Unicode treatment,
- **SAVE_TO_TEXT_FILE:** Saving a file with Unicode treatment,
- **FROM_DATA_FILE**: Reading a file without Unicode treatment,
- **FROM_TEXT_FILE**: Reading a file with Unicode treatment.

*_DATA_FILE functions are used for *.na files while *_TEXT_FILE functions will be used for slot files, for example.

WARNING

File names must follow the restrictions imposed by Windows operating systems, ie, a file name cannot contain “/”, “:”, “*”, “?”, “ ” ”, “<”, “>” and “|”.

. **Example**

Confirmation

A few examples of script are given below:

```
# Configuration backup
CONFIG BACKUP list=all $SAVE_TO_DATA_FILE("%APP_PATH%%FW_NAME%\all.na")

# Restoration of filter rules created on 16/12/2005
CONFIG                          RESTORE                          list=filter
$FROM_DATA_FILE("%APP_PATH%16_12_2005\all.na")

# Activation of filter rule 05
CONFIG SLOT ACTIVATE type=filter config=5
```


3.3.7. Deployment

Use this menu to access each of the screens enabling the deployment of security policies and of object databases. The NETASQ Global Administration mode allows deployment of the following policies and bases:

Objects	Deployment of object configuration.
Intrusion prevention	Deployment of the ASQ kernel.
QoS	Deployment of QoS rules
Address translation (NAT)…	Deployment of translation policy configuration.
Filtering	Deployment of the filter policy configuration

Global filtering	Deployment of global filter policy configuration. It is similar to classic filtering except that global filtering has priority when filters are executed. Network packets that pass through the firewall will first apply rules established in the global filter instead of applying those in the local filters.
URL filtering	Deployment of URL filter policy configuration.

The description of NETASQ Global Administration's deployment functionalities are explained in the section Deployment.

WARNING

These features are only available for deploying configurations on Firewalls in versions 7 or 8. As a result, security policies or object bases in version 9 will not be compatible.

3.3.8. Monitoring and supervision

The NETASQ Global Administration mode also provides monitoring and supervision tools for all your appliances, allowing an overall view of the status of the equipment installed. In order to monitor and supervise your appliances, use the topological view and its topology visualization zone.

3.3.8.1. Monitor

The NETASQ Global Administration mode provides a tool which enables monitoring appliances in the background. When this tool has been activated, the following icon will be visible in the bottom left corner of the main window . The monitor enables the automatic update of information, indicators and operating statuses (represented by a signal light in the object frame) relating to the appliances. By default, the tool is activated.

WARNING

During administrative tasks, you should deactivate the monitor in NETASQ Global Administration mode.

To deactivate or reactivate it, right-click with the mouse on the icon .

3.3.8.2. Checking the operational status of appliances

3.3.8.2.1. Overall check

The topological view allows checking the operating status of all equipment in the viewing zone. To launch this tool, click on the **Check all** button. A status indicator (in the form of a colored signal light) will then appear in the top left corner of certain objects in the view (all objects for which an IP address has been defined).

This indicator may take on the following colors:

	Equipment status check in progress
	Check done – equipment in operation
	Check done – equipment not in operation or inaccessible

The NETASQ Global Administration mode will ping all equipment in the view for which an IP address has been defined.

WARNING

If certain appliances are filtered, the NETASQ Global Administration mode may consider them non-operational even if they may be operating perfectly fine. Likewise, if the equipment does not respond to ICMP commands, it will be considered non-operational. In order to use the NETASQ Global Administration mode effectively, ensure that there is no equipment filtering ICMP requests coming from the administration workstation in Global Administration mode and that the equipments are configured to respond to ICMP queries.

When the monitor in NETASQ Global Administration mode has been activated, appliance status indicators will be automatically refreshed.

3.3.8.2.2. Individual check

It is also possible to individually check the operating status of each appliance or equipment. This operation may be carried out in flat and topological views for appliances and only in topological view for other equipment.

In order to do this, select the desired equipment and right-click with the mouse. Choose the **Test availability** option in the contextual menu which is displayed and the following window will open (NETASQ Global Administration attempts to connect to servers in the case of appliance, and to ping other objects):

You will be able to view certain information:

LED – status indicator	The color of the indicator changes according to the operating status: Blue for operation in progress, green for successful operation and orange for failed operation.
Host	Name assigned to the tested equipment
Address	Address of the tested equipment
Status	Message explaining the operating status

Progress bar	Operation progress bar
Total online	Total number of equipment in operation
Total offline	Total number of non-operational or inaccessible equipment
Export	Exports the results table in .txt format

Information in the table may be sorted by clicking on the title of the column you wish to sort. It is also possible to filter lines by clicking on the little black arrow to the right of the column title on which you wish to place the filter and by choosing the filtering criterion in the drop-down list.

WARNING

If certain appliances are filtered, the NETASQ Global Administration mode may consider them non-operational even if they may be operating perfectly fine. Likewise, if the equipment does not respond to ICMP commands, it will be considered non-operational. In order to use the NETASQ Global Administration mode effectively, ensure that there is no equipment filtering ICMP requests coming from the administration workstation in Global Administration mode and that the equipments are configured to respond to ICMP queries.

3.3.8.1. Indicator display

To display a firewall's indicators, point the mouse's cursor over the indicator in the viewing zone (topological view).

The following window then appears:

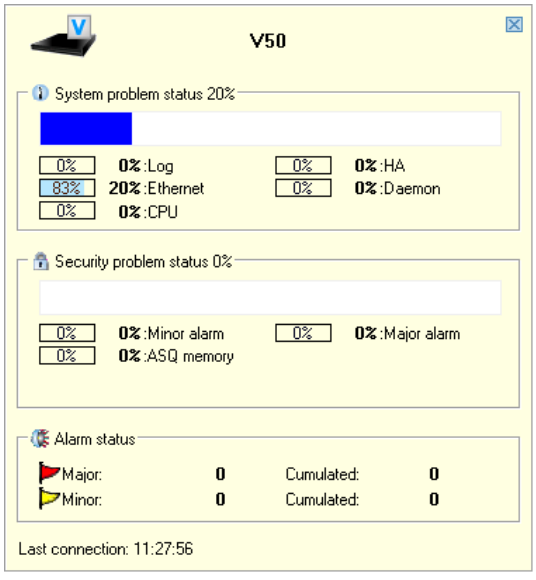

*Figure 42 : **Indicators***

The following is found in this window:

- A graphical representation of the Firewall type and the name of the Firewall concerned.
- Two gauges which represent the indicators. The System gauge represents the System indicator. The Security gauge represents the Security indicator. The higher the value of the gauge, the more critical the Firewall's situation.
- Values of the information used to calculate both indicators.

3.3.8.2. Administration Suite

Software in the NETASQ Administration Suite can be used to ease the supervision and monitoring of appliances. As such, it is possible to connect directly using one of these software components in the desired appliance.

Tools in the Administration Suite have the following functions:

NETASQ UNIFIED MANAGER	Enables the administration and definition of security policies.
NETASQ REAL-TIME MONITOR	Enables supervision in real time
NETASQ EVENT-REPORTER	Enables log analysis

3.3.8.2.1. Launching NETASQ REAL-TIME MONITOR and NETASQ EVENT REPORTER

NETASQ REAL-TIME MONITOR and NETASQ EVENT REPORTER are indispensable to the supervision and monitoring of the set of appliances. NETASQ REAL-TIME MONITOR enables supervising appliances' activities in real time (throughput, connections, authenticated users, VPN tunnels, use of system resources, alarms generated, etc.). NETASQ EVENT REPORTER enables viewing logs generated by the appliance and conducting analyses on these logs (graphical analyses, edition of filters, hierarchical groupings, etc.).

To launch NETASQ REAL-TIME MONITOR, select the Firewall that you wish to administer in flat view or topological view, then right-click with the mouse and select the **Tools\Launch NETASQ REAL-TIME MONITOR** option in the contextual menu. The link will be grayed-out if NETASQ REAL-TIME MONITOR has never been launched before.

If the path to NETASQ REAL-TIME MONITOR has not been defined for the software version of the appliance, or if the software version is unknown, then an assistant will help you choose the appropriate firewall. The NETASQ REAL-TIME MONITOR launch window then appears.

Connection to the software is automatic (no need to enter a password, IP address or login). You may then monitor the Firewall. Several NETASQ REAL-TIME MONITOR windows may be opened, connected to different Firewalls.

To launch NETASQ EVENT REPORTER, select the Firewall that you wish to administer in flat view or topological view, then right-click with the mouse and select the option **Tools\Launch NETASQ EVENT REPORTER** in the contextual menu. The link will be grayed-out if the firewall has never been launched before or if the appliance concerned is a U30, U70 or VBox Agency.

If the path to NETASQ EVENT REPORTER has not been defined for the appliance's software version or if the software version in unrecognized, an assistant will help you choose the appropriate Reporter.

Connection to the software is automatic (no need to enter a password, IP address or login). You may then monitor the Firewall. Several NETASQ EVENT REPORTER windows may be opened, connected to different Firewalls.

WARNING

NETASQ EVENT REPORTER is always inaccessible in the Global Administration mode for F50 and VBox Agency appliances. The link is therefore always grayed-out for these appliances.

3.3.9. Configuration monitoring

Modifying the configuration of a security appliance is one of the most sensitive administrative tasks. Indeed, the appliance, which has its place at the heart of the infrastructure, acts as the key to the vault that is the entire network architecture. Every modification can lead to errors that may sometimes turn out to be even more catastrophic for the stability of the network and even more so for the company's productivity. This is why the different steps involved in modifying the configuration are measured, action by action, option by option.

Version 6.3 of NETASQ appliances will be providing a tool that allows comparing configurations. With this feature, an administrator will be able to use a configuration as a reference when comparing modifications.

3.3.9.1.1. Operating principle

The Global Administration mode will establish a model for comparing configurations based on a "validated" configuration backup. This means that the configuration is constantly compared with the configuration currently running on the monitored appliance. As soon as a difference is detected between both configurations, the Global Administration mode will indicate so via the usual visual cues. Thereafter, the administrator will be informed of this modification and can view the changes using the menus in the Global Administration mode together with a file comparison software.

3.3.9.1.2. Setting up configuration monitoring

Step 1: Activating configuration monitoring

Enable configuration monitoring by selecting the option **Enable configuration monitoring**. (Cf. Configuration monitoring for more information on the available parameters in this menu).

Step 2: Setting up the Monitor

Activate the monitor in Global Administration mode to enable constant monitoring of the appliances on which configuration monitoring has been implemented. (Cf. Configuration monitoring)

Step 3: Backing up and validating a configuration

The third step in setting up configuration monitoring is the backup of a configuration that will be considered "validated". (Refer to "Configuration" under the section "Administration" in the chapter "Project" to find out how to back up a configuration.) During this backup, the option **Validate the configuration** must be checked.

When the configuration is backed up, monitoring for the backed up and validated configuration will be activated. NETASQ Global Administration will then check for changes made to this configuration and informs the administrator of the same.

3.3.9.1.3. Detecting modifications on a monitored configuration

. **Indicator of modifications made to the "validated" configuration**

As soon as a modification is made to a monitored configuration, the icon will appear in the flat or topological view.

Right-clicking on the appliance whose configuration has been modified will open the menu **`View modifications`**. Click on this menu in order to view the changes made.

. **View modifications**

The modification window displays all existing modifications between "validated" files and the files on the appliance. Three types of modifications are identified – "Differences", "Addition" and "Deletion". "Differences" indicates that there are differences in one of the files among the "validated" ones and those on the appliance. "Addition" indicates that a file which did not exist in the "validated" files has been added. "Deletion" indicates that a file that existed in the "validated" files has been deleted.

As mentioned earlier, configuration monitoring is based on a "validated" backup in order to warn the administrator of possible changes made to the configuration. By default, this means the most recent backup. In the comparison window, you will be able to select an older backup. It is even possible to restore the "validated" configuration if the administrator monitoring the configuration does not approve of the changes made. To do so, click on the button **Restore this configuration**.

. **File comparison tool**

To view details of modifications made to a given configuration file, select the line that indicates where a change has been made and click on the button ··· to the right of the selection. The configured comparison tool will then execute, displaying the differences identified in the files.

3.3.10. Quitting Global Administration mode

To exit the application in Global Administration mode, select the menu **File\Quit** or click on the button that closes the window (in the top right corner of the NETASQ Global Administration mode window).

If the project in progress has not been saved, a confirmation window will appear asking you if you wish to save your project.

3.3.11. Direct configuration

3.3.11.1. 20.310.1. Direct configuration

The "Direct Configuration" menus in Global Administration mode enable quick and direct access to the configuration of selected Firewalls (no need to reauthenticate on the selected Firewall to make the configuration menu appear).

These configuration sections (**Intrusion Prevention**, **Network**, **Objects**, **Logs**, **ASQ**, **Address Translation**, **Filter**, **Global Filter**, **QoS**, **VPN** and **URL Filtering**) are specific to the selected Firewall in Global Administration mode and in particular to the installed firmware version.

Each of the menus in "Direct Configuration" is accessed via the contextual menus in flat and topological views:

1 Select a NETASQ appliance.

2 Right click to make the contextual menu associated to this product appear.

3 Select the "Direct Configuration" section of your choice

3.3.12. Deploying configurations

3.3.12.1. Access

The cornerstone of a computer system's security is a security policy that is calculated, designed and implemented by administrators and persons in charge of data security (confidentiality, integrity and authenticity) and the system's resources.

When network elements making up the computer system operate in various versions, this weakens security policies defined on theoretical (therefore ideal) working models. Ensuring that your systems are homogeneous means better use of an efficient and powerful security policy.

Everyday, centralized management tools help administrators to locate the system's weaknesses (even flaws) and to fight their effects. The Global Administration mode takes a step further than other products by easing the deployment of homogeneous configurations on products in the NETASQ range.

Based on the principle of a client/server mode, the Global Administration mode enables deploying configurations (objects, ASQ kernel, QoS rules) or slots (filter, global filter, translation, URL filter) to all NETASQ appliances ("clients") on a network from a source Firewall (the "server").

Deployment features are accessible in two ways:

- the contextual menu enabling general and topological views,
- the menu **Administrative tasks\Deployment** in the main window.

3.3.12.1.1. Contextual menu

Right-click on a NETASQ Firewall object to view the contextual menu for flat and topological views:

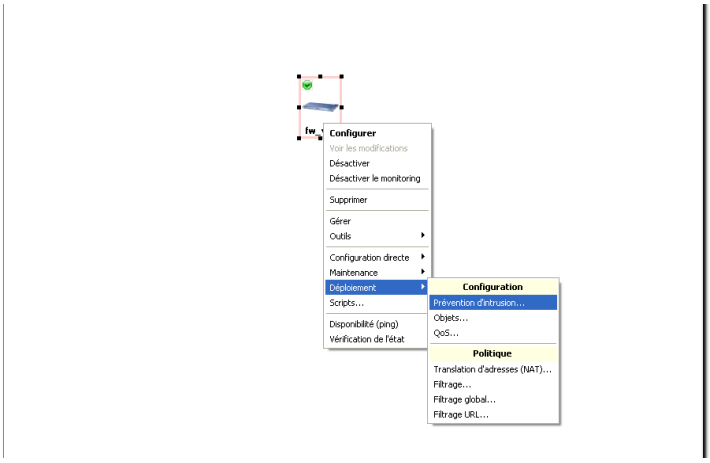

Figure 43 : ***Contextual menu***

3.3.12.1. Presentation of the deployment interfaces

These interfaces are almost the same as the configuration interface, except that the deployment options are different.

The deployment interface has 4 distinct sections.

- source firewall (the "server")
- destination firewall(s) (the "clients")
- action bar
- deployment options.

3.3.12.1.1. The source firewall

Select a firewall by clicking on **Source.**

WARNING

If there has not been any deployment from the current open project, the message “No client selected” will appear in red under the button’s icon. Otherwise, the Firewall selected in the last deployment from the current open project will be indicated by default.

When the general selection window appears, select the Firewall from which you intend to perform the deployment (its object database will be deployed to all the selected destination Firewalls) using the button in the “Source” zone.

There are 2 tabs that allow you to look for firewalls – the flat view and topological view.
Search filters can also be used on the “Name” column to find a firewall more easily.

3.3.12.1.2. “Destination" Firewalls

Firewalls selected to receive object databases from the source Firewall are presented in the form of a list in which the following is possible:

- adding a new Firewall: click on the **Add** and select the Firewall or some or all of the Firewalls in the list (hold down the **Ctrl** key and select the desired Firewalls). The selection of destination Firewalls is presented according to the general view in the **`Flat View`** tab (you can use the search filter in the “name” column) or according to the topological view model in the **`Topologies`** tab (which appears only if Firewalls have been defined in a topology).
- removing a firewall from the list of destination Firewalls: select the Firewall or some or all of the Firewalls in the list (hold down the **Ctrl** key and select the desired Firewalls) in the list of destination Firewalls and click on **Remove**.

WARNING

The selected Firewall appears in red on the list of Firewalls if its version is not suitable for the source Firewall (the configuration of a firewall cannot be deployed en version 7 to a firewall in version 6 and vice-versa).

3.3.12.1.1. Action bar

The action bar in the object configuration deployment menu consists of two buttons:

OK	Deploys object configuration.
Cancel	Cancels modifications.

When you click on **OK**, objects will continue to be deployed.

As the screen indicates, two options have to be defined before deployment of the source Firewall's object database can be continued:

Replace duplicate entries	When this option is checked, the value of the object in the source database will replace the value of the object in the destination database if an object in the destination object database bears the same name as an object in the source object database.
Merge	**WARNING** If unchecked, all objects in the destination object database which are not in the source object database will be deleted. Warning: Rules which use the deleted objects may fail to work if this option is checked.
Deploy	When you click on this button, the Global Administration mode will begin loading the object database and will ask you if you wish to edit it before sending. A screen will subsequently appear, enabling you to execute the deployment.

3.3.12.1.1. Objects categories

Categories are used in the deployment of objects.

- Select "Objects" if you wish to deploy an object database.

Source data options in the configuration deployment menu can be defined with two parameters. First of all, select a source, then select the categories that will be sent to the destination firewalls. The categories that can be configured are: **Hosts, Address ranges, Networks, Protocols, Services, Service groups, Groups.**

3.3.12.1.1. Choosing the intrusion prevention profile

The profile is used in the intrusion prevention (ASQ) module.

- Select "Intrusion prevention» if you intend to deploy the configuration of the ASQ kernel. The following window will appear:

The drop-down list will allow you to select a profile. This profile must be configured beforehand in Firewall Manager mode in the intrusion prevention menu.

- Reminder: profiles contain all the parameters defined in the **`Intrusion Prevention`** menu.

3.3.12.1.1. List of QoS elements

For this deployment, the list is limited to 253 elements. In fact, if a new source is selected, the new configurations from this source will overwrite the older configuration, which may render the filter configuration obsolete.
The list has been reduced in order to prevent the firewall capacity from being exceeded.

3.3.12.1. Deploying the object database

Copy the source object database to the destination clients	This option will activate the deployment options for the object database described below. (This option applies to the following windows: intrusion prevention, address translation (NAT), Filtering, Global filtering, URL filtering).
Replace duplicate entries	When this option is checked, the value of the object in the source database will replace the value of the object in the destination database if an object in the destination object database bears the same name as an object in the source object database. (This option applies to the following windows: intrusion prevention, address translation (NAT), Filtering, Global filtering, URL filtering).
Merge	**WARNING** If unchecked, all objects in the destination object database which are not in the source object database will be deleted. Warning: Rules which use the deleted objects may fail to work if this option is checked. (This option applies to the following windows: intrusion prevention, address translation (NAT), Filtering, Global filtering, URL filtering).

Only used objects	When this option is checked, the deployment mechanism will copy only the objects from the source database used in the deployed filter policy's rules to the destination object database.

When you click on **OK**, the filter policy will continue to be deployed, the Global Administration mode will load the source Firewall's filter slots.

3.3.12.2. Deployment windows

Upon completing the definition of a deployment (objects, ASQ, filters, etc) the Global Administration mode will display a deployment window, which recaps the Firewalls on which the configured deployment will be performed.
The title of the tab changes according to the type of deployment.

3.3.12.2.1. Data grid

In the second column of the table (by default) an indicator will be displayed. The indicator's color depends on the status of the action:

	On standby
	Action has begun.
	Action has been canceled or has not been performed
	Action successfully completed

The rest of the table consists of the following columns:

BP	Breakpoint: firewalls above this breakpoint will be updated (the firewall on the line of the breakpoint will be included in this group) before the firewalls under it. The results of operations performed on the first group have to be successful before the second group can be treated.
Name	Name chosen for the appliance
Address	Firewall's IP address
Current status	Action's status (standby, in progress, done, etc)
Current version	Firewall's firmware version

Task in progress	Progress of the task
Result	Results of the update
Message	Explicative message with regards to the “results” field.

As some of the information displayed may not necessarily be useful to you, you may wish to display only information you need. You can hide or show columns by clicking on **Customize columns**.

In this window, there are names of columns which are not displayed but can be made visible. To display a column, left-click on the column’s name and hold down the mouse button. Drag the column to where you wish to insert it in the column title bar and let go for the mouse button (“drop” the column).

To hide a column, do the opposite: using the left mouse button, select the name of the column to hide in the column title bar. Hold down the left button and drag the column to the “Customization” window before letting go.

The layout of the displayed columns can be rearranged by using the same drag and drop mechanism. All you need to do is to select a column and move it to the desired location.

To close the “Customization” window, click on the white cross found at the top right of the window.

3.3.12.2.2. Deploying configurations on destination UTM appliances

You can manage the deployment with three buttons:

Reset	Removes all the destination Firewalls from the configured deployment.
Update All	Starts deployment.
Close	Closes the deployment window. This action will cancel the deployment.

WARNING

Information on destination Firewalls have to be up to date in order to perform a deployment. If you cancel the update, there will be no deployment on the Firewall which has not been updated.

APPENDICES

Appendix A: TCP/IP Services

In this appendix, you will find the list of commonly used TCP/IP services such as: FTP, Telnet, www, SMTP, etc. This appendix is presented in the form of a list made up of four columns:

- A column containing the service name.
- A column containing the port number associated to the service.
- A column indicating the protocol used (TCP and/or UDP).
- A column containing a description of the service.

We recommend that you do not enter all of these services when defining the list of objects so as to avoid overloading your display and thus improving legibility.

Service	Port	Protocole	Description
echo	7	TCP/UDP	Echo
discard	9	TCP	Discard
systat	11	TCP/UDP	Systat
daytime	13	TCP/UDP	Daytime
qotd	17	TCP/UDP	Quote of tThe Day
chargen	19	TCP/UDP	Character generator
ftp-data	20	TCP	File Transfer (Default Data)
ftp	21	TCP	File Transfer (Control)
telnet	23	TCP	Telnet
smtp	25	TCP	Simple Mail Transfer
time	37	TCP/UDP	
rip	39	UDP	Ressource Locator Protocol
nameserver	42	TCP/UDP	Host Name Server
nicname	43	TCP	
login	49	TCP/UDP	
domain	53	TCP/UDP	Domain Name Server (DNS)
Sql-net	66	TCP/UDP	Oracle SQL Net
bootps	67	UDP	Bootstrap Protocol Server
bootpc	68	UDP	Bootstrap Protocol Client
tftp	69	TCP/UDP	Trivial File Transfer
gopher	70	TCP	Gopher
finger	79	TCP	Finger
www	80	TCP	World Wide Web
kerberos	88	TCP/UDP	Kerberos
npp	92	TCP/UDP	Network Printng Protocol
hostname	101	TCP	NIC Host Name Server
Uucp-path	117	TCP	ISO-TSAP Class 0

sqlserv	118	TCP/UDP	SQL Services
nntp	119	TCP	Network News Trasfer Protocol
ntp	123	UDP	Network Time Protocol
epmap	135	TCP/UDP	Netbios Net Service
netbios-ns	137	TCP/UDP	DCE edpoint resolution
netbios-dgm	138	UDP	Netbios Datagram Service
netbios-ssn	139	TCP	Netbios session service
Imap2	143	TCP	Interim Mail Access Protocol version 2
sql-net	150	TCP/UDP	SQL-NET
snmp	161	UDP	Simple Network Management Protocol
snmptrap	162	UDP	SNMP trap
print-srv	170	TCP	
bgp	179	TCP	Border Gateway Protocol
irc	194	TCP	Internet Relay Chat Protocol
ipx	213	UDP	IPX over IP
imap3	220	TCP / UDP	Internet Message Access Protocol 3
Idap	389	TCP	Lightweight Directory Access Protocol
netware-ip	396	TCP / UDP	Novell Netware over IP
ups	401	TCP / UDP	Uninterruptible power Supply
smtpe	420	TCP / UDP	SMPTE
https	443	TCP / UDP	Https Mcom
microsoft ds	445	TCP / UDP	
kpasswd	464	TCP / UDP	Kerberos (v5)
isakmp	500	UDP	Internet Key Exchange
exec	512	TCP / UDP	Remote process execution
biff	512	TCP / UDP	Notify user of new mail received
login	513	TCP / UDP	Remote login
who	513	TCP / UDP	Who's logged in to machines
cmd	514	TCP / UDP	Remote exec
syslog	514	TCP / UDP	
printer	515	TCP	Spooler
talk	517	UDP	
ntalk	518	UDP	
router	520	TCP / UDP	Extended File Name Server
timed	525	UDP	Timeserver
tempo	526	TCP	
courier	530	TCP	
conference	531	TCP	
uucp	540	TCP	
klogin	543	TCP	Kerberos login
kshell	544	TCP	Kerberos remote shell
remotefs	556	TCP	Remote login using Kerberos
rmonitor	560	UDP	

rmonitor	561	UDP	
whoami	565	TCP / UDP	
Idaps	636	UDP	LDAP over TLS/SSL
Kerberos-adm	749	TCP / UDP	Kerberos administration
Kerberos-iv	750	UDP	Kerberos version IV

Appendix B: Data input control

When configuring the firewall, different types of data will have to be entered:

- IP address.
- Comments.
- File name.
- Object name (host, network, service).

Each of these data types accepts a specific group of characters. These characters are filtered during parameter input.

IP address

The only characters accepted are the figures "0" to "9" and the decimal point ".". To erase a character, use the **Backspace** or **Del** keys.

Comments

You can use conventional cursor movement techniques when editing a comment (mouse or keyboard arrows).

File name

Certain characters, such as accents and spaces are not accepted in file names.

Object name

Certain characters, such as accents and spaces are not accepted in object names. When editing an object name, if an accented character is entered using the keyboard, the configuration software inserts the corresponding non-accented character. A non-accepted character is not validated and does not appear on screen.

Appendix C: ICMP Codes

Type	Code	Description	Requête Erreur
0	0	echo reply	x
3		Destination unreachable	x
	0	network unreachable	x
	1	host unreachable	x
	2	protocol unreachable	x
	3	port unreachable	x
	4	fragmentation needed but don't fragment bit set	x
	5	source route failed	x
	6	destination network unknown	x
	7	destination host unknown	x
	8	source host isolated (obsolete)	x
	9	destination network administratively prohibited	x
	10	destination host administratively prohibited	x
	11	network unreachable for TOS	x
	12	host unreachable for TOS	x
	1	communication administratively prohibited by filtering	x
	14	host precedence violation	x
	15	precedence cutoff in effect	x
4	0	source quench	x
5		redirect :	
	0	redirect for network	x
	1	redirect for host	x
	2	redirect for type of service and network	x
	3	redirect for type of service and host	x
8	0	echo request	x
9	0	routeur advertisement	x
10	0	routeur solicitation	x
11		time excedeed !	
	0	time tolive equals 0 during transit	x
	1	time to live equals 0 during reassembly	x
12		parameter problem :	
	0	IP header bad	x
	1	required option missing	x
13	0	timestamp request	x
14	0	timestamp reply	x
15	0	information request (obsolete)	x
16	0	information reply (obsolete)	x
17	0	address mask request	x
18	0	address mask reply	x

Appendix D: Configuration examples for NAT

The examples below illustrate different configurations using address translation. They use the different possibilities available according to needs and network structure in deliberately simplified cases.

- Unidirectional address translation of the internal network for internet access
- Configuration with a web server in the DMZ
- Configuration with a web server in the DMZ which must be accessible from the internal and external networks with its official address.
- Connection via modem on the Firewall's serial port for internet access.
- Port re-direction: using only one IP address to contact several servers.
- Load balancing: balancing connections over a pool of servers.

Example 1: Unidirectional translation of the internal network

The diagram below offers an example of configuring unidirectional address translation from the whole internal network to a virtual address on the external network.

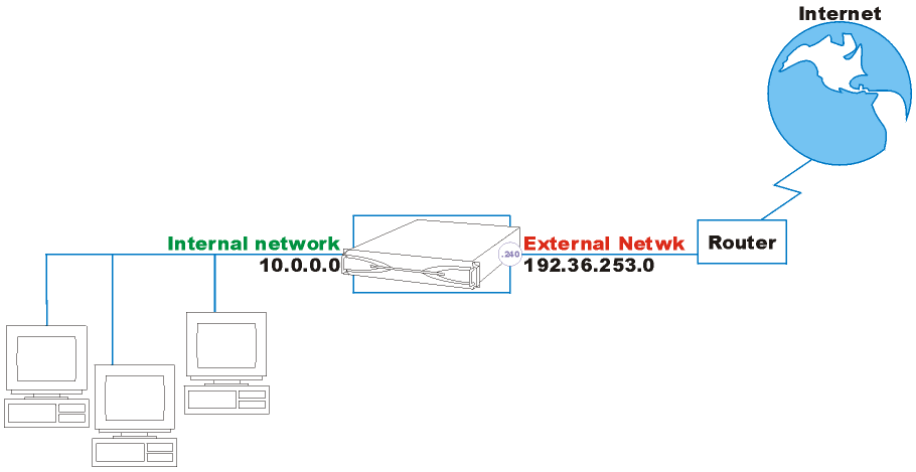

Figure 44 : ***Unidirectional translation***

Concerning the NETASQ Firewall, the corresponding configuration for address translation is:

Status	Action	Option	Source	Destination	Destination port	Translated	Description
On	Map	None	Ntwk_in	<Any>	<Any>	Firewall_out	

Typically, this configuration allows all hosts situated on the internal network to gain access to the internet. The hosts leave the network with the virtual address 192.36.253.240 and can receive responses to their requests.

It is necessary, of course, for the virtual address on the external network to be routable on the internet (official IP address).
However, internal hosts are not reachable from the outside (unidirectional); if a connection request to address 192.36.253.240 reaches the Firewall, no address translation will be carried out to a host's address on the internal network.

Moving on to advanced configuration (button ), it is worth noting that this rule translates destination ports to a range called ephemeral_fw (port 20000 to 59999). This means that not only the source address but also the source port is translated. The NETASQ Firewall uses a port available for translation in this range, which avoids conflicts if two hosts on the internal network are using the same source port.
If you wish to remove a host from the map operation (this host's IP address will not be translated), use the "no map" operation.

The following example demonstrates how to remove a host from the map operation (the IP addresses specified no longer correspond to the previous example):

Status	Action	Option	Source	Destination	Destination port	Translated	Description
On	No map	None	Client	<Any>	<Any>		
On	Map	None	Network_bridge	<Any>	<Any>	Firewall_out	

In this case, the "Client" host will not be mapped.

Example 2: Bi-directional translation

The example below illustrates a configuration which features a Web server in the DMZ:

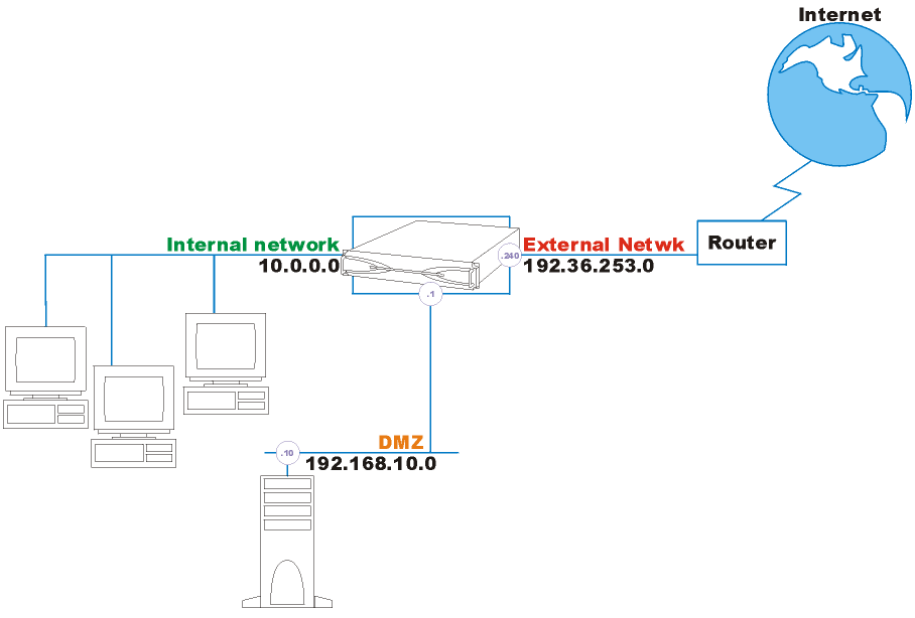

Figure 45 : ***Bi-directional translation***

The configuration for the address translation on the Firewall must be the following:

Status	Action	Option	Source	Destination	Destination port	Translated	Description
On	Bi-map	None	private_web_server1	<Any>	<Any>	Public_web_server	

With bi-directional address translation; the server is accessible from the outside. The address used externally is the virtual address, routable on the internet.

In this way, requests coming from the outside (OUT direction) with the destination address 192.36.253.10 are changed to 192.168.10.11 and routed by Firewall to the DMZ.

Example 3: Access to a web server in the DMZ

The example below illustrates a configuration with three sub-networks (internal, external and DMZ) and a web server in the DMZ. We want the web server to be accessible from the outside but also from the inside with its official (virtual) address.

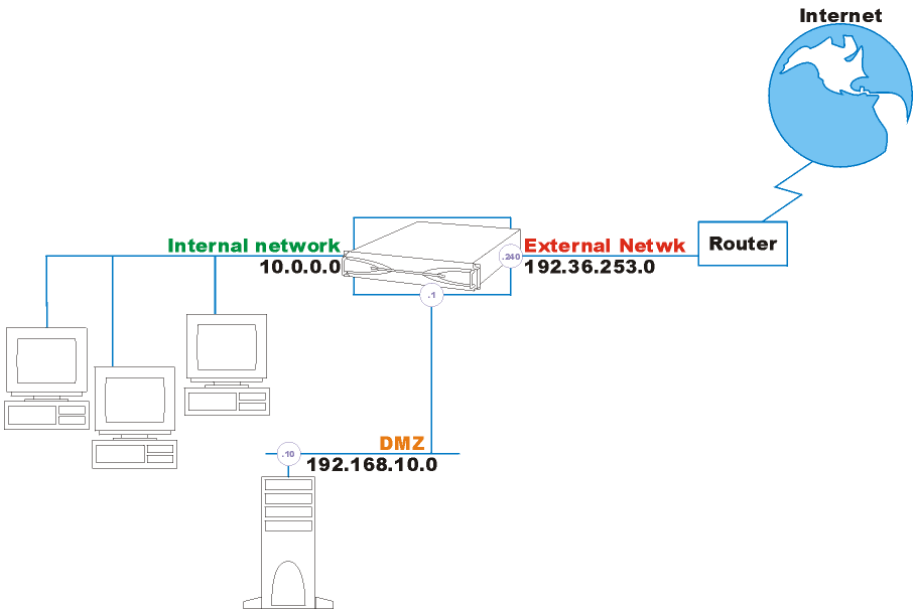

Figure 46 : ***Web server in DMZ***

If a host on the internal network wants to connect to the web server via its URL, the first thing to be carried out is DNS resolution.

In the event the DNS server is external, it will send back the virtual address of the web server as it is known on the internet (192.36.253.10). The machine therefore sends its request with this destination address. Because the targeted machine does not exist on the internal network, the request is sent to the internet and is lost or sends back an error message. The request can also be sent back by the router.

It is therefore necessary to translate this virtual address on the internal Firewall interface to the server's real address in the DMZ. We also want the server to be accessible from the external network with this virtual address.

We therefore have the same rule twice but applied to different interfaces. The interface is selected in advanced mode ( button). By default, the Firewall chooses the interfaces where the virtual IP address is located (OUT in the example).

Status	Interface	Action	Option	Source	Destination	Destination port	Translated	Translated port	Description
On	Out	Bi-map	None	Private_web_server1	<Any>	<Any>		Public_web_server	
On	in	Bi-map	None	Private_web_server1	<Any>	<Any>	Firewall_out	Public_web_server	

In this way, requests coming from the outside (OUT Interface) and from the internal network (IN Interface) with destination address 192.36.253.10 are changed to 192.168.10.11 and routed directly by the Firewall to the DMZ.

REMARKS

1) The order of rules is important here. For this case, it is essential to place the rule with the virtual IP address and the network interface (direction) belonging to the same network in first place. In our example, the virtual address belongs to the external network (OUT). It is therefore necessary to put in first place the rule having the direction of the OUT interface.

2) It is impossible to contact the server with its virtual address if the client and the server are actually on the same network. In fact, the message will reach the server but the server will respond directly to the client (since they are on the same network) with its real address. The client then receives the response with a different address from his initial request and rejects the packet.

Example 4: Internet connection via modem

In a modem connection, the addresses of internal hosts wishing to use the modem must be translated on the NETASQ Firewall's serial port or external interface.

Addresses must be translated to the address firewall_dialup. This interface has an IP address (fixed or not) negotiated with the provider during the connection request.

In this example, we want to allow internet access to the internal network via the modem installed on the appliance's serial port:

Status	Action	Option	Source	Destination	Destination port	Translated	Description
On	Map	None	Ntwk_in	<Any>	<Any>	Fwall_dialup	

If you are operating in transparent mode, you have to implement this rule (by replacing the object *Network_in* with *Network* or *Bridge*) in order to access the internet with your modem.

Example 5: Port redirection

In the event you have only one public IP address and several public servers, port re-direction allows you to re-direct traffic to these servers using the port number alone.

Business A has the public IP address 192.36.253.240. It hosts a web server and a mail server in the DMZ.

The Firewall will redirect traffic to the appropriate server using the port number targeted. If the connection request concerns port 80 (HTTP), the firewall will redirect to the web server. If the connection request is made on port 25 (SMTP), the firewall will redirect traffic to the mail server.

Status	Interface	Action	Option	Source	Destination	Destination port	Translated	Translated port
On	out	redirect	none	<Any>	Firewall_out	http	Web_Server	http
On	out	redirect	none	<Any>	Firewall_out	smtp	Mail_Server	smtp

REMARK
Traffic can be to another port on the destination host.

Example 6: Load balancing

Certain servers are physically replicated on several machines so as to respond more efficiently to the many connections reaching them.

With the NETASQ Firewall, these servers can be reachable via one IP address alone. The Firewall will re-direct connection requests made to the public IP address towards the servers.

Business A, for example, possesses a web server (www.netasq.com) which has been physically installed on several machines in the DMZ. DNS resolution sends IP address 192.36.253.10 for the site www.netasq.com.

We are going to create a host group with the servers' physical IP addresses and give a translation rule to the Firewall.

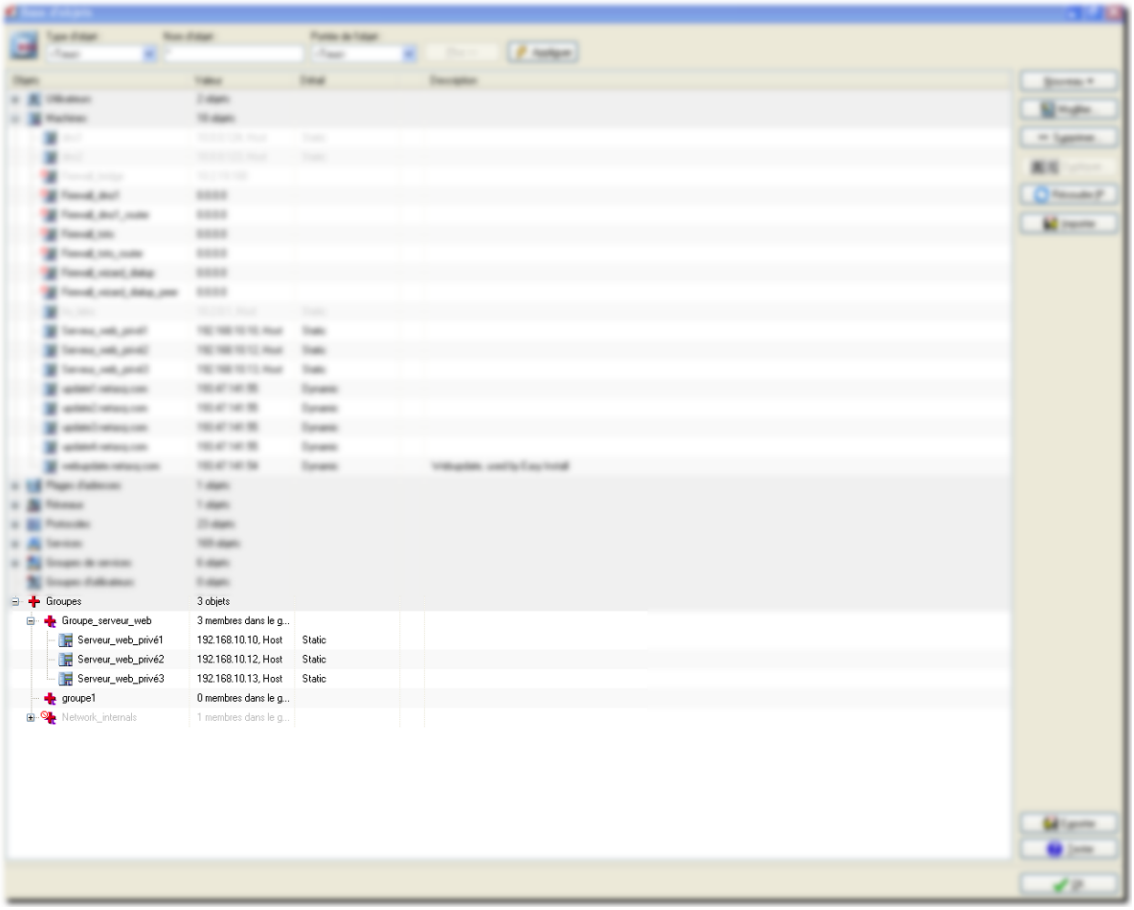

*Figure 47 : **Groups***

The traffic directed to public IP address 192.36.253.10 is distributed evenly and sequentially between the different hosts of the web server group.

Status	Action	Option	Source	Destination	Destination port	Translated	Description
On	split	None	public_web_server	<Any>	<Any>	web_server_group	

REMARK

The source ports of the source and destination hosts can be specified in advanced mode. This results in a combination of load balancing and port re-direction.

Load balancing is done evenly in this version, without taking into consideration the respective load on each host and/or the availability of these hosts.

Appendix E: Examples of filter rules

In this appendix we will show you how to configure certain basic rules such as:

- DNS access
- ICMP access
- Telnet access
- FTP access
- Access to an internal web server from the outside and from the internal network
- Internet access with or without URL filtering
- Client workstations' access to the mail server
- Configuring a mail server
- Regulating bandwidth
- Verifying filter rules
- Authentication

WARNING

Some configurations could be unnecessary if you activate the specific implicit rules.

ICMP access

In this example, we will be adding the internal network's access to ICMP, allowing namely the use of the "ping" program.
To add ICMP, just select "ICMP" from the list of services.

Figure 48 : ICMP access

You can filter ICMP codes. In this example, only ping (echo request) is allowed.

Internet access

To provide internet access to the internal network by passing through the Firewall, you only need to create a rule which allows the internal network to contact everyone using "http" and the protocol "udp_domain" for DNS resolution. These protocols are included in the "Web" service group.
This becomes:

Figure 49: Internet access

If you use URL filtering, you will indirectly pass through a web proxy located on the Firewall.
Therefore, you no longer connect directly to the web server but to the web proxy. The proxy then connects to the web server. These different phases are implicit in the filter rules.

Where the workstations are concerned, you can configure your browser so as to connect to a remote proxy server. In this case, to access the internet, the workstation no longer uses “http” on port 80 but on port 8080.
If you have implicitly overlooked this protocol at the Firewall level, your users can access the internet without passing through the URL filtering that you have set up.

To avoid this, you can redirect all requests using a specific service (8080 for example) to URL filtering:

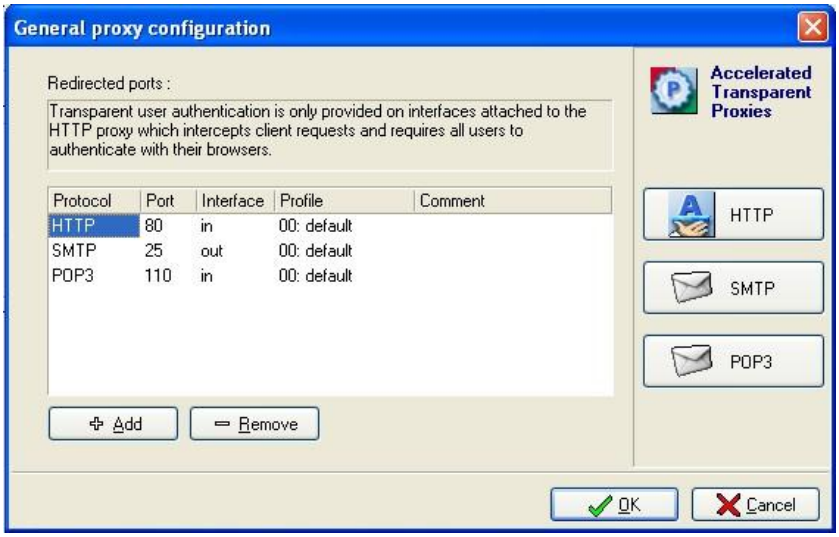

Figure 50: General proxy configuration

Access to a web server

In this example, we assume that your Web server is located in the DMZ.
It must be accessible from the external network (from the internet) and from the internal network, in other words, accessible to everyone.
Filtering configuration is therefore quite simple: the source host is "any", the destination host is "Private_web_server", the service is "http" and the action to take it "Pass":

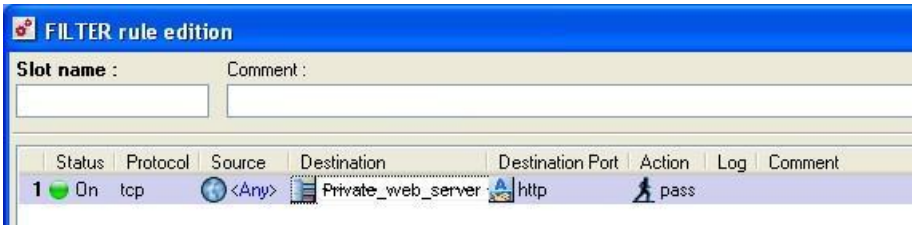

Figure 51: Editing filter rules

WARNING

If you carry out address translation for this web server, you have to configure and additional translation rule to access it from your internal network using its domain name. For more information, refer to the example on address translation dealing with this case.

DNS access

We will give the group requiring web access (Network_in) access to the DNS service in order to use domain names instead of IP addresses.

The following rule allows the internal network to access DNS servers (internal and external). This rule is also included in the WEB group of services.

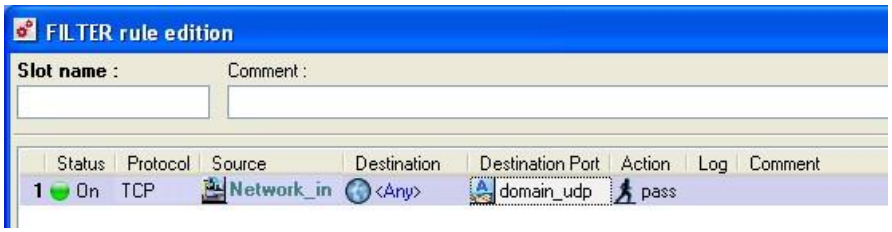

Figure 52: Editing filter rules

FTP access

FTP is a particular protocol. It uses two types of connections:

- A command connection to send and receive FTP commands
- A data connection for the transit of traffic.

In addition, FTP can be used in two different modes:

- Active FTP (in DOS, for example), in which the data transfer connection is made by the server's FTP-data port. The server initiates this connection. In active FTP, the client's private IP address is sent to the server via the command connection, so that the server can establish the second connection. If the client's private address is translated, the "Support for active FTP" option has to be checked in the address translation configuration so that the Firewall will automatically modify the address sent in the FTP commands.
- Passive FTP (with a web browser, for example), in which the source host makes both connections itself on the FTP server. However, the data transfer is not carried out on the server's FTP-data port but on an ephemeral port.

General rule

The NETASQ Firewall includes an FTP plugin which automatically generates the second connection (data connection); this allows you to define a single filter rule (the one needed to authorize the client-server connection command). The only rule you need to define is the following:

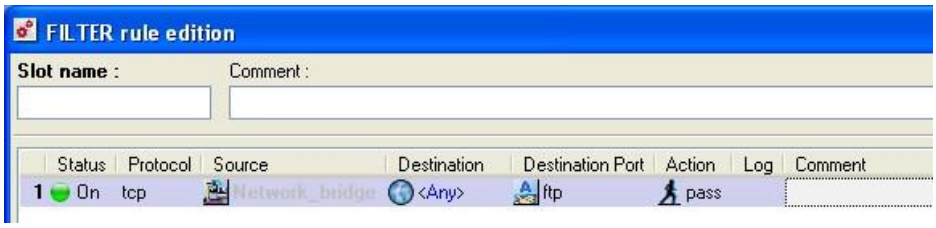

Figure 53: Editing filter rules

This rule allows an internal network machine (Network_Bridge) to access FTP servers on the Internet.

Access to a mail server in the DMZ

In order to send and receive e-mails on a client workstation, the SMTP and POP3 services must be authorized for the client workstation to the mail server.
The mail server can be hosted internally or can be external to the network (with the provider for example). It is therefore necessary, in object configuration, to declare the mail server (using its IP address).

You can then create a service group called "Mail" in which you will place the POP3 and SMTP services. This will avoid the need to place two lines with the same properties in the filter rules.
You then need to create the filter rule for the internal network (where the client workstations are placed) to the Mail server, using the "Mail" service group and the **Pass** action. This results in:

Telnet access

The telnet service allows a shell to be opened on a remote host (generally a UNIX machine).

In this example, we will authorize the "Client" host to connect to the "Private_WEB_Server1" in order to perform administrative duties.

Figure 54: Editing filter rules

Only the host “Client” will be able to conduct telnet session on the web server located in the DMZ.

IPSec connections

After setting the IPSEC VPN parameters on the Firewall, filter rules have to be implemented to authorize these protocols on the Firewall (except if implicit rules are activated for this traffic type).
The first phase of the IKE protocol is negotiated on UDP port 500 (ISAKMP). It is therefore necessary to authorize connections on this port on the Firewall interface with the tunnel is concerned.

In the case of an outgoing IPSec connection, a connection on the remote Firewall on the ISAKMP port must be accepted.

Depending on the protocols selected in VPN configuration (ESP), these protocols have to be allowed to reach the Firewall. These rules are not taken into account by the Stateful Inspection module and therefore have to be positioned in both directions of communication.
The first three rules in the following screen allow the VPN tunnel to be established between the local and remote Firewalls (these 3 rules have to be indicated on both Firewalls using VPN). For an anonymous tunnel, the “FW_peer” object has to be replaced by “ANY”.

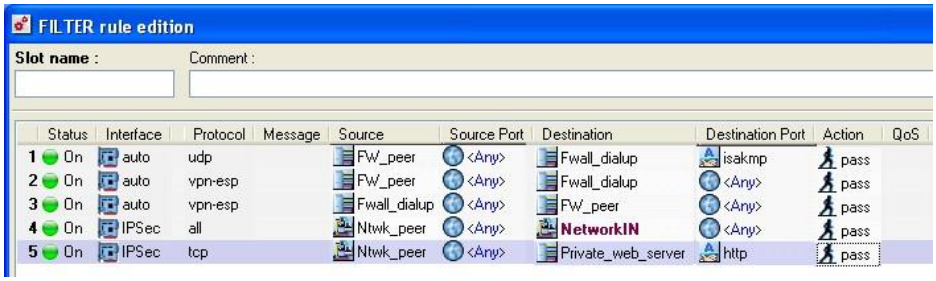

Figure 55: Editing filter rules

Once these first 3 rules are in place, the tunnel can be created.
You can then filter VPN access to the internal hosts. To filter packets reaching the Firewall through the tunnel, you have to specify the IPSec interface (in advanced mode) in order to define the filter rules. To filter packets going out from your Firewall to the VPN tunnel, you do not have to define the interface (leave the interface as “auto”) if the source and destination objects have been specified.
The last two rules indicate how to filter traffic coming from the remote network and passing through the VPN.

PPTP connections

After configuring the PPTP server on the Firewall, you will need to create the associated filter rules (except if implicit rules have been activated for this traffic type) .
You will need to add three rules:

- The first one to authorize PPTP clients to connect with PPTP (TCP port 1723) on the Firewall interface used for PPTP connections.
- Two other ones to authorize the GRE protocol (encapsulation protocol) from the client to the Firewall and in the opposite direction.

Example

Take for example a host connecting to its provider A. Generally, this provider assigns IP addresses in a particular range which is possible to locate.

Therefore we will create an object called "Provider_IP_pool" with this range of addresses. If you don't know these addresses, you can leave the object as "any".

The internet connection is considered linked to the Out interface of the Firewall and the mobile workstations reach this interface to connect with PPTP.

The filter rules, in this case, are:

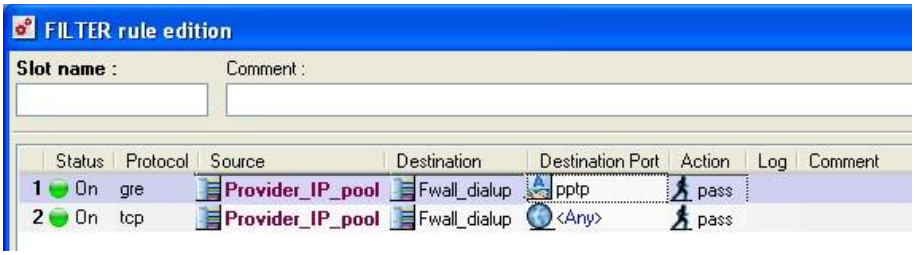

Figure 56: Editing filter rules

Bandwidth control

The NETASQ Firewall allows you to limit the available bandwidth. This is achieved by authorizing the passage of a limited number of bytes per second.

The level can be defined with precision as you can limit each of the IP protocol services, for each different machine.

Bandwidth is controlled through filtering, using the "Limit to" action. Instead of blocking packets, or allowing them to pass, they will be authorized to pass up to the defined threshold. Beyond this they will be rejected if the threshold is reached during the defined period.

The example bellow shows how to limit FTP downloads from the internal network.

Figure 57: Editing filter rules

Filter control

After having configured the simplest rules, you may begin to wonder if there isn't anything missing in order to ensure proper network operation.

It is also possible that an application server uses a specific protocol that you don't know.

If you have not defined any explicit blocking rules for these hosts or protocols, a simple solution is to temporarily place a log rule at the end of the filtering. This rule will log all elements blocked by the Firewall.

Thus, the flow that you have not explicitly authorized passes through all rules and arrives at the end of the table where it is subjected to the default rule (block). If you place a rule that logs everything just before the default rule (that is not displayed in the list of filter rules), the flow is entered into the log files that you can then view.

The log file will show, in particular, the destination port number, which is useful if you do not know it.

You can also analyze everything that has been blocked and check that these flows really should be blocked.

Access to the mail server

In order to be able to send and receive Email on a client workstation, the SMTP and POP3 services of the client workstation to the mail server must be authorized.
Of course, this is only useful if your mail server communicates with the outside. If the rules are applicable only the internal mail server, then they are useless.

The mail server sends or receives mail from different mail servers which are unidentifiable. They will be represented by the host "any".
Both rules (one for sending and one for receiving) are the following:

Figure 58: Editing filter rules

REMARK

If your mail server is just a go-between for your ISP's mail server, the exchange takes place only from port 25 (SMTP) to your server's port 25.

Authentication

Authentication may be requested for access to certain services or to certain hosts. For this, you must have already defined forms for the users who may authenticate themselves on the Firewall. For example, access to the web, for authenticated users belonging to the internal network, may be authorized by the following rule:

Figure 59: Editing filter rules

You may also grant particular access to certain authenticated users. For example, the following policy authorizes "Smith" to conduct FTP sessions (wherever he is located), authenticated users from Network_bridge can surf the web and all the users on Network_bridge, authenticated or not, have access to the mail server:

Figure 60: Editing filter rules

Authentication of users is also possible for incoming connections (coming from the internet). In this way, you can grant certain internet users access to certain services hosted on your internal network (of course, the connection information must have been given to these users beforehand). The following example shows how to grant the user group «Partner" access to a particular Web server (e.g., for an extranet).

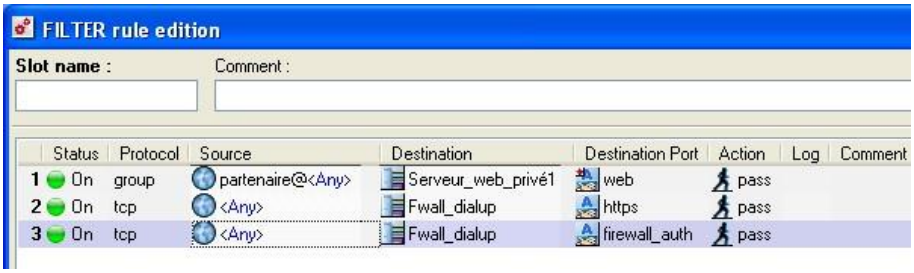

Figure 61: Editing filter rules

If you wish to authorize authentication for users situated outside the security perimeter of the Firewall, you also have to authorize the services which are necessary for authentication, the HTTPS service and NETASQ's proprietary authentication service via SRP (port 1200). Warning, the port 1200 must be open only if you are using the authentication via SRP. In other cases, only HTTPS is necessary.

Appendix F: Commands

Connecting in console mode (SSH, serial port or screen-keyboard) allows maintenance of the Firewall by a set of commands.
This appendix sets out the main commands (pay attention to case).

REMARK
To see the full list of these commands, please refer to the ***CLI console / SSH commands reference* guide, which can be found in the Document Base**.

Launching the command server

- **nsrpc user@127.0.0.1** *ou* **cli**: launches the Firewall's command server with the admin login.

REMARK
The full list of NETASQ commands is set out in the ***CLI SERVERD reference* guide, which can be found in the Document Base**.

Viewing configuration information

- **ifinfo:** displays the correspondence between the names of interfaces defined in network configuration (with NETASQ UNIFIED MANAGER) and the names used by the system.
- **ifconfig:** displays information about the Firewall's network configuration
- **sfctl -s filter:** displays the active filter rules.

You can view the contents of configuration files with an editor such as vi.
Configuration files are found in /Firewall/ConfigFiles.

Activating/Deactivating a filter policy or an option

- **enfilter xx:** activates the filter slot bearing the number xx.
- **enfilter 10:** activates slot 10 (pass_all in the default configuration, the Firewall allows all packets to pass)
- **endialup:** reconnects to a modem
- **ennetwork:** reloads a network configuration
- **engui:** reactivates NETASQ UNIFIED MANAGER's connection authorization on internal networks

Firewall activity

- **sfctl -s stat:** gives the Firewall's statistics.
- **sfctl –T:** displays "real-time" information on the Firewall's stateful engine,
- **dstat:** gives the list of active services.
- **top -u:** gives the activity of the processor and the processes and the memory used

- **tcpdump -i <interface name> <filter>**: Real time display of packets transiting by a firewall interface.
  - *<interface name>* is the name of the interface used by the system (this name can be retrieved using the ifinfo command)
  - *<filter>* filters the protocols or services displayed.

A service's filter must be preceded by the word "port". Services can be indicated by their port number or by their name (if the service is part of the current services).

Examples of filters

- tcpdump -i fxp0 not port 23 (to mask telnet traffic),
- tcpdump -i fxp0 udp OR port HTTP (only displays UDP and http traffic),
- tcpdump -i fxp0 tcp AND port 53 (to display only DNS TCP traffic),
- tcpdump –s0 –w /tmp/dump –i fxp0 (writes traffic in a file),
- tcpdump –s0 –i fxp0 ESP OR port isakmp (viewing ESP encrypted traffic or VPN negotiation phases).

VPN Commands

- **showSPD:** Displays the SPD (Security Policy Database) containing all the data regarding defined tunnels (active or inactive)
- **showSAD:** Displays the SAD (Security Association Database) containing data relating to active tunnels.

Deactivation

- **envpn 00:** deactivates the active VPN tunnel.

Activation

- **envpn xx:** activates the VPN slot bearing the number xx.

Miscellaneous

- **getversion:** displays the Firewall software version

WARNING

1) Use this command to check that the version delivered corresponds to the expected version as soon as you receive your Firewall.
2) The handling of files and the use of certain commands must be done carefully, as certain operations can adversely affect the operation of the Firewall.

Technical support and "sysinfo"

The command “sysinfo” allows viewing the full configuration of a NETASQ UTM appliance. The information that this command returns is absolutely necessary in helping you to understand the cause of your problem, and you will be asked to provide it when you contact technical support for the resolution of a case.

For information, the return of this command can be obtained from the menu **Firewall\NETASQ technical support** in NETASQ UNIFIED MANAGER. This menu allows saving the result for the purpose of sending it to technical support, for example.
An example (partial) of a sysinfo command return is shown below.

```
##############################
#   Software information     #
##############################
current date :  2006-07-18 18:42:42
Serial       :  U70XXA0Z0899020
Model        :  U70
Software     :  Netasq Firewall software version 6.2.1
Branch/Build :  EUROPE / M
Partitions      :    Active=Main  BackupVersion="6.2.1"  BackupBranch="  EUROPE  "
Date="2006-07-11 14:42:39" Boot=Main
Uptime       :  36 days 3:52, hours
##############################

##############################
#   Slot information         #
##############################
Filtering : slot_filter_01
NAT       : slot_nat
VPN       : slot_vpn
URL       :
##############################

##############################
#   Memory information       #
##############################
Stateful
--------

host                                    0 %
fragment                                0 %
ICMP                                    0 %
connection                              0 %
data tracking                           0 %

mbuf
----
1012/1056/7798 mbufs in use (current/peak/max):
        1012 mbufs allocated to data
261/272/5199 mbuf clusters in use (current/peak/max)
808 Kbytes allocated to network (6% of mb_map in use)
0 requests for memory denied
0 requests for memory delayed
0 calls to protocol drain routines
```

Appendix G: FAQ

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 stop the major alarm warning indicator on the Firewall?
6). How do I know if there has been an attempted intrusion?
7). What happens when the Firewall sets off an alarm?
8). 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 NETASQ 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 appliance by the serial port or by connecting a screen and a keyboard to the appliance.

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 graphic 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 stop the major alarm warning indicator on the Firewall?

The major alarm LED lights up as soon as a major alarm is received and it remains alight as long as no one validates the alarm display.

To stop the LED, validate the option **Switch off LEDs** in the firewall menu in NETASQ UNIFIED MANAGER.

6) 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:

- The alarms are logged in a specific file which you can consult from the graphical interface (NETASQ REAL-TIME MONITOR or NETASQ EVENT REPORTER),
- You can receive an alarm report at regular intervals (see Receiving alarms) via the NETASQ UNIFIED MANAGER application, which can 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
- Finally NETASQ REAL-TIME MONITOR displays on the screen the alarms received in real time.

7) What happens when the firewall raises an alarm?

All intrusion attempts or detected attacks are automatically thwarted. Depending on the configuration, the packet that caused the alarm to be raised will either be blocked, or the connection will be reset. Moreover, an action can be added: sending an e-mail to the administrator or quarantining the packet behind the alarm.

Quarantining involves blocking all packets originating from the host in question.

In the case of open hacking, you should closely monitor incoming connections with the NETASQ REAL-TIME MONITOR or NETASQ EVENT REPORTER or other network analysis tools.

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

The NETASQ 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.

Appendix H: Role of the DMZ

The main purpose of a DMZ (De-Militarized Zone) is to isolate from your internal network machines which have to receive connections from the outside.

Thus, you can completely isolate direct access of the external network to your internal network. Possible accesses from the outside occur only in the DMZ, which is physically separated from the internal network.

You enjoy efficient protection for the internal network as such. Hosts in the DMZ are exposed to a greater risk (as they can be contacted from outside).

You then need to carefully define the relations between the DMZ and the internal network in order to avoid compromising the level of security achieved.

Example of setting up a DMZ

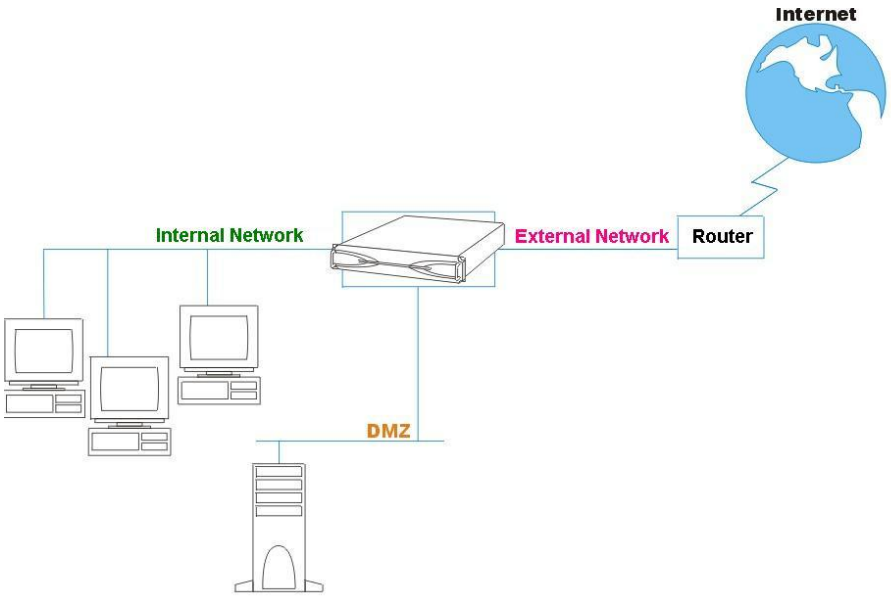

Figure 62 : Setting up a DMZ

The DMZ can be used for other purposes (e.g. separating an enterprise's branches).

Appendix I: Connecting to the SSH server

The NETASQ Firewall has an SSH server installed. Connection to this server may serve as the Firewall configuration in console mode (in command line).

Definition of Secure Shell

Secure Shell is a secure communication protocol allowing remote access to the Firewall in order to run programs. SSH bridges the security weaknesses of remote accesses such as telnet by providing the essential security services: server authentication, confidentiality of traffic (especially passwords).
SSH is based on the RSA asymmetric cryptography technique for authentication and it uses IDEA symmetrical algorithms for traffic confidentiality.

Activating the SSH server on the Firewall

The service is deactivated on the Firewall by default, so it must be activated through the **`Firewall\Security`** menu.

The admin user's private key is required for authentication at the time of connection. You must therefore save it and store it in a directory on the PC from which the SSH connection will be run.

The Firewall filtering blocks the Firewall's connection to port 22 (SSH) by default, so you must set up a filter rule to authorize this communication.

Client section configuration

WARNING

You need SSH software that supports version 2 of this protocol in order to use it with the Firewall.

The client configuration depends on the client software used.

Appendix J: Configuring other equipment

In order to achieve optimum performance on your NETASQ Global Administration, there are several operations to carry out on your NETASQ appliances and on filtering equipment on your network (the central Firewall, for instance).

Configuring NETASQ appliances

Certain manipulations have to be conducted on the NETASQ appliances managed by NETASQ Global Administration depending on the administration and supervisory operations you wish to perform.

If the NETASQ Global Administration mode accesses the appliance by its internal interface (or another protected interface)
As a rule, no operation is necessary (except to use the operation checking tool and external tools). You only need to check that implicit rules for the administration server are active.

For a firewall in version 5 or 6, connect to the appliance using the corresponding NETASQ UNIFIED MANAGER, then select the Configuration\Implicit rules menu. The "Administration server" option should be checked. If you wish to use EZAdmin from NETASQ Global Administration, ensure that the "Authentication server" option has also been checked.
For a firewall in version 4, connect to the appliance using the corresponding NETASQ UNIFIED MANAGER, then select the menu **Configuration\Filter\Edit the active slot**, and click on **Extra parameters**.

The boxes "access NETASQ UNIFIED MANAGER on internal networks" and "Access authentication service on internal networks" have to be checked.

If the NETASQ Global Administration mode accesses the appliance by its external interface (or another unprotected interface)
In this case, you have to create a specific filter rule where the appliance's security policy is concerned. Select the menu **Configuration\Filter\Edit the active slot**.

First, create a host by clicking on **Edit objects**. This host represents the NETASQ Global Administration administration host and therefore possesses the host's IP address

WARNING
In the case of address translation, please pay careful attention: if an equipment carries out address translation between the host and the appliance, the translated address has to be used.

Then create a rule indicating that "firewall_srv" type connections coming from the NETASQ Global Administration host are authorized on the appliance.

If the NETASQ Global Administration mode accesses the appliance via a VPN tunnel

If NETASQ Global Administration accesses the appliance via a VPN tunnel, do not forget to authorize TCP port 1300 to pass through the tunnel. On a NETASQ Firewall, you only need to add a rule in the filter rules, authorizing "firewall_srv" connections coming from the IPSec interface to connect to the appliance.

Next, select the menu **Configuration\VPN\IPSec tunnels\Edit the active slot**, and click on **Extra parameters**. Ensure that you have checked the option "Consider IPSec peers as internal".

Using the operation check tool

The appliances' operation check tool and status indicators use ICMP (ping command), therefore it is necessary to authorize this data flow type on the appliance in order to use this feature. All you need to do is to add a rule in the filter rules authorizing ICMP (in particular the ping command) data flows in the direction of the appliance.

Using an external tool

Using an external tool to connect to an appliance in SSH requires activating the SSH service. Select the **Firewall\Security** menu. Check the "Activate SSH access to firewall" box. If you wish to carry out an SSH connection with certificates, do not check the box "Enable password access", but rather, export the keys (certificates) into the external tool. If you wish to carry out an SSH connection using passwords, check the box "Enable password access". In this case, the **admin** login and its password will be used.

Next, create the filter rule authorizing the SSH connection on the appliance:

Configuring filtering devices

Certain equipment on your network may prevent the application from functioning properly. It is therefore important to identify all the elements which risk filtering traffic that NETASQ Global Administration needs and modifying their configuration as a result.

Rules for authorizing data flows between the NETASQ Global Administration administration host and the NETASQ website

The NETASQ Global Administration administration host and the NETASQ website communicate via HTTP (port TCP/80) and HTTPS (port TCP/443), therefore it is important that these data flows not be blocked between both extremities. Furthermore, the NETASQ Global Administration administration host has to be able to conduct DNS resolution, therefore this service has to be authorized and accessible.

Lastly, it would be preferable not to require authentication for HTTP and HTTPS data flows passing between the administration host and the NETASQ website, as this might disrupt the application's operation.

Rules for authorizing data flows between the NETASQ Global Administration administration host and NETASQ appliances

The NETASQ Global Administration administration host and NETASQ appliances use several data flow types depending on the features used:

Features	Types of traffic used
NETASQ Global Administration	Port TCP/1300
Appliance operation check and status indicators	ICMP (PING)
NETASQ REAL-TIME MONITOR, NETASQ EVENT REPORTER	Port TCP/1300
Web Administration Interface	Port TCP/443
External tool for SSH connections	Port TCP/22
Other external tools	Depends on the tool

To use a feature correctly, ensure that the necessary data flows are not filtered between the NETASQ Global Administration host and the appliances. It is therefore advisable to add filter rules authorizing these data flows.

Lastly, it would be preferable not to require authentication for necessary data flows passing between the administration host and the appliances, as this might disrupt the application's operation.

GLOSSARY

The terms found in this glossary are related to the subjects covered in this manual.

100BaseT

Also known as "Fast Ethernet," 100BaseT is Ethernet in 100 Mbps instead of the standard 10 Mbps. Like regular Ethernet, Fast Ethernet is a shared media network in which all nodes share the 100 Mbps bandwidth.

A

Active Update

The Active Update module on NETASQ firewalls enables updating antivirus and ASQ contextual signature databases as well as the list of Antispam servers and the URLs used in dynamic URL filtering.

Address book

A centralized tool for several NETASQ applications. This address book can contain all the necessary information for connecting to a list of firewalls, simplifying the administrator's access as he no longer has to remember all the different passwords this entails.

Address translation

Changing an address into another. For example, assemblers and compilers translate symbolic addresses into machine addresses. Virtual memory systems translate a virtual address into a real address (address resolution)

Advanced mode (Router)

Configuration mode in which the firewall acts as a router between its different interfaces. This involves changes in IP addresses on routers or servers when you move them to a different network (behind an interface on a different network)

AES (Advanced Encryption Standard)

A secret key cryptography method that uses keys ranging from 128 to 256 bits. AES is more powerful and secure than Triple DES, until recently the de facto standard.

Alias IP

A supplementary address associated with an interface.

Antispam

System that allows the reduction of the number of unsolicited and occasionally malicious electronic messages that flood mail systems and attempt to abuse users.

Antispyware

System that enables detecting and/or blocking the spread of spy software (which gathers personal information about the user in order to transmit it to a third party) on client workstations.

Antivirus

System that detects and/or eradicates viruses and worms.

Antivirus (*Kaspersky*)

An integrated antivirus program developed by Kaspersky Labs which detects and eradicates viruses in real time. As new viruses are discovered, the signature database has to be updated in order for the antivirus program to be effective

Appliance

Hardware that embeds the software as well as its operating system.

Asic (Application-Specific Integrated Circuit)

Specially-designed technology for a handful of specific features. These features are directly managed by the circuit instead of the software. ASICs cannot be reprogrammed.

ASQ (Active Security Qualification)

Technology which offers NETASQ Firewalls not only a very high security level but also powerful configuration help and administration tools. This intrusion prevention and detection engine integrates an IPS which detects and gets rid of any malicious activity in real time.

Asymmetrical cryptography

A type of cryptographic algorithm that uses different keys for encryption and decryption. Asymmetrical cryptography is often slower than symmetrical cryptography and is used for key exchange and digital signatures. RSA and Diffie-Hellman are examples of asymmetrical algorithms.

Authentication

The process of verifying a user's identity or origin of a transmitted message, providing the assurance that the entity (user, host, etc.) requesting access is really the entity it claims to be. Authentication can also refer to the procedure of ensuring that a transaction has not been tampered with.

Authentication header (AH)

Set of data allowing verification that contents of a packet have not been modified and also to validate the identity of a sender.

B

Backup appliance

Formerly known as a "slave", a backup appliance is used in high availability. It transparently takes over the master appliance's operations when the former breaks down, thereby ensuring the system to continue functioning with minimum inconvenience to the network's users.

Bandwidth

The transmission capacity of an electronic pathway (e.g. communications lines). It is measured in bits per second or bytes per second in a digital line and in an analog line, it is measured in Hertz (cycles per second).

Blowfish

A secret key cryptography method that uses keys ranging from 32 to 448 bits as a free replacement for DES or IDEA.

Bridge

Device connecting 2 LAN segments together, which may be of similar or dissimilar types (eg, Ethernet and Token Ring). The bridge is inserted into a network to segment it and keep traffic contained within segments to improve performance. Bridges learn from experience and build and maintain address tables of the nodes on the network. By keeping track of which station acknowledged receipt of the address, they learn which nodes belong to the segment.

Bridge or transparent mode

The transparent mode, also known as "bridge", allows keeping the same address range between interfaces. It behaves like a filtering bridge, meaning that all the network traffic passes through it. However, it is possible to subsequently filter traffic that passes through it according to your needs and to therefore protect certain portions of the network

Brute force attack

An exhaustive and determined method of testing all possible combinations, one by one, to find out a password or secret key by trial and error. This method only works when the sought after password contains very few characters.
This attack can be thwarted simply by choosing longer passwords or keys, which the intruder will take longer to find out.

Buffer

Temporary storage zone.

Buffering

Temporary storage of information for the purpose of processing it at one goes, instead of as and when it is received.

Buffer overflow

An attack which usually works by sending more data than a buffer can contain so as to make a program crash (a buffer is a temporary memory zone used by an application). The aim of this attack is to exploit the crash and overwrite part of the application's code and insert malicious code, which will be run after it has entered memory.

C

CA Certificate (or Certification)

Authority - A trusted third-party company or organization which issues digital certificates. Its role is to guarantee that the holder of the certificate is indeed who he claims to be. CAs are critical in data security and electronic commerce because they guarantee that parties exchanging information are really who they claim to be.

Certificate

(see digital certificate)

Certificate Revocation List (*CRL*)

A list of expired (revoked) certificates or of those that are no longer considered trustworthy. It is published and regularly maintained by a CA to ensure the validity of existing certificates.

Challenge/response

An authentication method for verifying the legitimacy of users logging onto the network wherein a user is prompted (the challenge) to provide some private information (the response). When a user logs on, the server uses account information to send a "challenge" number back to the user. The user enters the number into a credit-card sized token card that generates a response which is sent back to the server.

Chassis

Also called a case, it is a physical structure that serves as a support for electronic components. At least one chassis is required in every computer system in order to house circuit boards and wiring.

Context

The current status, condition or mode of a system.

Common criteria

The common criteria, an international standard, evaluate (on an Evaluation Assurance Level or EAL scale of 1 to 7) a product's capacity to provide security functions for which it had been designed, as well as the quality of its life cycle (development, production, delivery, putting into service, update).

Contextual signature

An attack signature, ie, the form that an attack takes. ASQ relies on a database of contextual signatures to detect known attacks in a short time.

CPU (Central Processing Unit)

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

Cryptography

The practice of encrypting and decrypting data.

D

Daemon

An application that runs permanently in the background on an operating system.

Datagram

An information block sent over a communication line within a network.

Data Encryption Standard (*DES*)

Cryptographic algorithm for the encryption of data. In particular, it allows encrypting data by blocks.

Data evasion

Also known as IDS evasion, it is a hacker's method of tricking an intrusion detection system by presenting to it packets formed from similar headers but which contain data different from what the client host will receive.

Denial of service (DoS) attack

An attack which floods a network with so many requests that regular traffic is slowed down or completely interrupted, preventing legitimate requests from being processed.

DHCP (Dynamic Host Configuration Protocol)

Protocol that allows a connected host to dynamically obtain its configuration (mainly its network configuration). DHCP finds its own IP address. The aim of this protocol is to simplify network administration.

Dialup

Interface on which the modem is connected.

Diffie-Hellmann key exchange algorithm

An algorithm that enables parties to exchange public keys securely in order to arrive at a shared secret key at both ends, without ever having to transmit the secret key, thereby avoiding the risk of the secret key being intercepted. It does not carry out data encryption, and can even be used over untrusted channels.

The Diffie Hellmann negotiation groups are, for example:

- Group 14 which uses a xxxx-bit key length.
- Group 15 which uses a xxxx-bit key length.
- Group 16 which uses a xxxx-bit key length.

Digital certificate

The digital equivalent of an identity card for use in a public key encryption system, these are mainly used to verify that a user sending a message is who he claims to be, and to provide the receiver of a message with a way to encrypt his reply. The X.509 format is most typically used and contains information regarding the user and the certification authority.

Digital signature

Method of verifying identities on a network based on public key encryption.

DMZ (Demilitarized Zone)

Buffer zone of an enterprise's network, situated between the local network and the internet, behind the firewall. It corresponds to an intermediary network grouping together public servers (HTTP, SMTP, FTP, etc.) and whose aim is to avoid any direct connection with the internal network in order to warn it of any external attack from the web.

DNS (Domain Name System)

Distributed database and server system which ensures the translation of domain names used by internet users into IP addresses to be used by computers, in order for messages to be sent from one site to another on the network.

Dynamic quarantine

An imposed quarantine following a specific event, eg, when a particular alarm is raised.

Dynamic routing

Routing that adapts automatically to changes that arise on a network so that packets can be transported via the best route possible.

E

Encapsulation

A method of transmitting multiple protocols within the same network. The frames of one type of protocol are carried within the frames of another.

Encryption

The process of translating raw data (known as plaintext) into a seemingly meaningless version (ciphertext) to protect the confidentiality, integrity and authenticity of the original data. A secret key is usually needed to unscramble (decrypt) the ciphertext.

Ethernet

Packet switching information network protocol, a technology that allows all hosts on a local network to connect to the same communication line.

Ethernet port

(see Ethernet).

F

Filtering router

Router which implements packet filters.

Filter policy

One of the more important aspects in the security of the resources that the firewall protects – the creation of filter rules that allow avoiding network flaws.

Filter rule

A rule created to perform several possible actions on incoming or outgoing packets. Possible actions include blocking, letting through or disregarding a packet. Rules may also be configured to generate alarms which will inform the administrator of a certain type of packet passing through.

Firewall

A basic feature in peripheral information security, a firewall can be a hardware or software that allows filtering access to and from the company network.

Firmware

Software that allows a component to run before the drivers.

FTP (File Transfer protocol)

Common internet protocol used for exchanging files between systems. Unlike other TCP/IP protocols, FTP uses two connections – one for exchanging parameters and another for the actual data.

Full duplex

Two-way communication in which sending and receiving can be simultaneous.

G

Gateway

Host which acts as an entrance or connection point between two networks (such as an internal network and the internet) which use the same protocols.

Gigabit Ethernet

An Ethernet technology that raises transmission speed to 1 Gbps (1000Mbps).

H

Half-duplex

One-way communication mode in which data can only be sent in one direction at a time.

Hash function

An algorithm that converts text of a variable length to an output of fixed size. The hash function is often used in creating digital signatures.

Header

A temporary set of information that is added to the beginning of the text in order to transfer it over the network. A header usually contains source and destination addresses as well as data that describe the contents of the message.

High availability

A solution based on a group of two identical Firewalls which monitor each other. If there is a malfunction in the Firewall software or hardware during use, the second Firewall takes over. This switch from one Firewall to the other is wholly transparent to the user.

Hot swap

The ability to pull out a device from a system and plug in a new one while the power is still on and the unit is still running, all while having the operating system recognize the change automatically.

HTTP

Protocol used for transferring hypertext documents between a web server and a web client.

HTTP Proxy

A proxy server that specializes in HTML (Web page) transactions.

Hub

A central connection point in a network that links segments of a LAN.

Hub and spoke

Any architecture that uses a central connecting point that is able to reach all nodes on the periphery ("spokes").

Hybrid mode

Mode which combines two operation modes - transparent mode (bridge principle) and advanced mode (independent interfaces). The purpose of the hybrid mode is to operate several interfaces in the same address class and others in different address classes.

Hypertext

Term used for text which contains links to other related information. Hypertext is used on the World Wide Web to link two different locations which contain information on similar subjects.

I

ICMP (Internet Control Message Protocol)

A TCP/IP protocol used to send error and control messages and for exchanging control information.

IDS (Intrusion Detection System)

Software that detects attacks on a network or computer system without blocking them.

IKE (Internet Key Exchange)

A method for establishing an SA which authenticates the encryption and authentication algorithms to be applied on the datagrams that it covers, as well as the associated keys.

Implicit filter rule

Filter rule that the firewall implicitly generates after the administrator has modified its configuration. For example, when the http proxy is activated, a set of implicit filter rules will be generated in order to allow connections between the client and the proxy as well as between the proxy and the server.

Interface

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

Internet Protocol

Protocol used for routing packets over networks. Its role is to select the best path for conveying packets through the networks.

IP Address

(IP being Internet Protocol). An IP address is expressed in four sets of numbers (from 0 to 255) separated by dots, and which identify computers on the internet

IPS (Intrusion Prevention System)

System that enables detecting and blocking intrusion attempts, from the Network level to the Application level in the OSI model.

IPSEC

A set of security protocols that provides authentication and encryption over the internet and supports secure exchanges. It is largely used for the setup of VPNs (Virtual Private Networks).

ISAKMP (Internet Security Association and Key Management Protocol)

A protocol through which trusted transactions between TCP/IP entities are established.

K

Kernel

The core of the operating system.

L

LAN (Local Area Network)

A communications network that is spread out over a limited area, usually a building or a group of buildings and uses clients and servers - the "clients" being a user's PC which makes requests and the "servers" being the machine that supplies the programs or data requested.

LDAP (Lightweight Directory Access Protocol)

A protocol or set of protocols used to access directory listings.

Leased line

A permanent telephone connection between two points, as opposed to dialup. Typically used by enterprises to connect remote offices.

Load balancing

Distribution of processing and communications activity across a computer network to available resources so that servers do not face the risk of being overwhelmed by incoming requests.

Logs

A record of user activity for the purpose of analyzing network activity.

M

MAC address (Media Access Control Address)

A hardware address that physically identifies each node of a network and is stored on a network card or similar network interface. It is used for attributing a unique address at the data link level in the OSI model.

Man-in-the-middle attack

Also known as a "replay attack", this consists of a security breach in which information is stored without the user's authorization and retransmitted, giving the receiver the impression that he is participating in an

authorized operation. As a result of this, an attacker can intercept keys and replace them with his own without the legitimate parties' knowledge that they are communicating with an attacker in the middle.

MAP

This translation type allows converting an IP address (or n IP addresses) into another (or n IP addresses) when going through the firewall, regardless of the connection source.

Modularity

Term describing a system that has been divided into smaller subsystems which interact with each other.

MSS (Maximum Segment Size)

MSS value represents the largest amount of data (in bytes) that a host or any other communication device van contains in a single unfragmented frame. To get the best yield possible, the size of the data segment and the header have to be lower than the MTU.

N

NAT (Network address Translation)

Mechanism situated on a router that allows matching internal IP addresses (which are not unique and are often unroutable) from one domain to a set of unique and routable external addresses. This helps to deal with the shortage of IPv4 addresses on the internet as the IPv6 protocol has a larger addressing capacity.

NETASQ EVENT REPORTER

Module in NETASQ's Administration Suite that allows viewing log information generated by firewalls.

NETASQ REAL-TIME MONITOR

Module in NETASQ's Administration Suite that allows viewing the firewall's activity in real time.

NETASQ VULNERABILITY MANAGER

Module that allows the network administrator to collect information in real time and to analyze it in order to weed out possible vulnerabilities that may degrade the network. Some of its functions include raising ASQ alarms and maintaining an optimal security policy.

NETASQ UNIFIED MANAGER

Module in NETASQ's Administration Suite that allows configuring firewalls.

Non-repudiation

The capacity of parties involved in a transaction to attest to the participation of the other person in the said transaction.

NTP (Network Time Protocol)

Protocol that allows synchronizing clocks on an information system using a network of packets of variable latency.

O

Object

Objects used in the configuration of filter or address translation. These may be hosts, users, address ranges, networks, service, protocols, groups, user groups and network groups.

OS detection

A method of determining the operating system and other characteristics of a remote host, using tools such as queso or nmap.

OSI

International standard defined by ISO describing a generic 7-layer model for the interconnection of heterogeneous network systems. The most commonly-used layers are the "Network" layer, which is linked to IP, the "Transport" layer, linked to TCP and UDP and the "Application" layer, which corresponds to application protocols (SMTP, HTTP, HTTPS, IMAP, Telnet, NNTP…).

P

Pack

Rfers to a unit of information transported over a network. Packets contain headers (which contain information on the packet and its data) and useful data to be transmitted to a particular destination.

Packet analyzer

When an alarm is raised on a NETASQ Firewall, the packet that caused this alarm to be raised can be viewed. To be able to do so, a packet viewing tool like “Ethereal” or “Packetyzer” is necessary. Specify the selected tool in the **Packet analyzer** field, which Reporter will use in order to display malicious packets.

Partition

A section of disk or memory that is reserved for a particular application.

PAT (Port Address Translation)

Modification of the addresses of the sender and recipient on data packets. Changes in IP address involve the PAT device's external IP address, and port numbers, instead of IP addresses, are used to identify different hosts on the internal network. PAT allows many computers to share one IP address.

Peer-to-peer

Workstation-to-workstation link enabling easy exchange of files and information through a specific software. This system does not require a central server, thus making it difficult to monitor.

Ping (Packet Internet Groper)

An internet utility used to determine whether a particular IP address is accessible (or online). It is used to test and debug a network and to troubleshoot internet connections by sending out a packet to the specified address and waiting for a response.

PKI (Public Key Infrastructure)

A system of digital certificates, Certificate Authorities and other registration authorities which verify and authenticate the validity of parties involved in an internet transaction.

Plugin

An auxiliary program that adds a specific feature or service to a larger system and works with a major software package to enhance its capacity.

Port redirection (REDIRECT)

The use of a single IP address to contact several servers.

Port scanning

A port scan is a technique that allows sending packets to an IP address with a different port each time, in the hopes of finding open ports through which malicious data can be passed and discovering flaws in the targeted system. Administrators use it to monitor hosts on their networks while hackers use it in an attempt to compromise it.

PPP (Point-to-Point Protocol)

A method of connecting a computer to the internet. It provides point-to-point connections from router to router and from host to network above synchronous and asynchronous circuits. It is the most commonly used protocol for connecting to the internet on normal telephone lines.

PPPoE (Point-to-Point Protocol Over Ethernet)

A protocol that benefits from the advantages of PPP (security through encryption, connection control, etc). Often used on internet broadband connections via ADSL and cable.

PPTP (Point-to-Point Tunneling Protocol)

A protocol used to create a virtual private network (VPN) over the Internet. The internet being an open network, PPTP is used to ensure that messages transmitted from one VPN node to another are secure.

Private IP Address

Some IP address ranges can be used freely as private addresses on an Intranet, meaning, on a local TCP/IP network. Private address ranges are

- 172.16.0.0 to 172.31.255.255
- 192.168.0.0 to 192.168.255.255
- 10.0.0.0 to 10.255.255.255

Private key

One of two necessary keys in a public or asymmetrical key system. The private key is usually kept secret by its owner.

Protocol analysis

A method of analysis and intrusion prevention that operates by comparing traffic against the standards that define the protocols.

Protocols

A set of standardized rules which defines the format and manner of a communication between two systems. Protocols are used in each layer of the OSI model.

Proxy

System whose function is to relay connections that it intercepts, or which have been addressed to it. In this way, the proxy substitutes the initiator of the connection and fully recreates a new connection to the initial destination. Proxy systems can in particular be used to carry out cache or connection filter operations.

Proxy server

(see *Proxy*).

Public key

One of two necessary keys in a public or asymmetrical key cryptography. The public key is usually made known to the public.

PVM

Software that enables using a set of UNIX workstations linked to a network much like a parallel workstation (PVM is the internal name for NETASQ Vulnerability Manager).

Q

QID

QoS queue identifier.

QoS (Quality of Service)

A guaranteed throughput level in an information system that allows transporting a given type of traffic in the right condition, ie, in terms of availability and throughput. Network resources are as such optimized and performance is guaranteed on critical applications.

R

RADIUS (Remote Authentication Dial-In User Service)

An access control protocol that uses a client-server method for centralizing authentication data. User information is forwarded to a RADIUS server, which verifies the information, then authorizes or prohibits access.

RAID (Redundant array of independent disks)

Hardware architecture that allows accelerating and securing access to data stored on hard disks and/or making such access reliable. This method is based on the multiplication of hard disks.

Replay

Anti-replay protection means a hacker will not be able to re-send data that have already been transmitted.

RFC (Request for Comments)

A series of documents which communicates information about the internet. Anyone can submit a comment, but only the Internet Engineering Task Force (IETF) decides whether the comment should become an RFC. A number is assigned to each RFC, and it does not change after it is published. Any amendments to an original RFC are given a new number.

Router

A network communication device that enables restricting domains and determining the next network node to which the packet should be sent so that it reaches its destination fastest possible.

Routing protocol

A formula used by routers to determine the appropriate path onto which data should be forwarded. With a routing protocol, a network can respond dynamically to changing conditions, otherwise all routing decisions have to be predefined.

S

SA (Security Association)

VPN tunnel endpoint.

SCSI (Small computer system interface)

standard that defines an interface between a computer and it(s) storage peripherals, known for its reliability and performance.

Security policy

An organization's rules and regulations governing the properties and implementation of a network security architecture.

Session key

A cryptographic key which is good for only one use and for a limited period. Upon the expiry of this period, the key is destroyed, so that if the key is intercepted, data will not be compromised.

Signature

A code that can be attached to a message, uniquely identifying the sender. Like a written signature, the purpose of a digital signature is to guarantee that the individual sending the message really is who he claims to be.

Single-use password

A secure authentication method which deters the misuse of passwords by issuing a different password for each new session.

Slot

Configuration files in the NETASQ UNIFIED MANAGER application, numbered from 01 to 10 and which allow generating filter and NAT policies, for example.

SMTP (Simple Mail Transfer Protocol)

TCP/IP communication protocol used for electronic mail exchange over the internet.

SMTP Proxy

A proxy server that specializes in SMTP (mail) transactions.

SNMP (Simple Network Management Protocol)

Communication protocol that allows network administrators to manage network devices and to diagnose network incidents remotely.

SSH (Secure Shell)

Software providing secure logon for Windows and UNIX clients and servers.

SSL (Secure Socket Layer)

Protocol that secures exchanges over the internet. It provides a layer of security (authentication, integrity, confidentiality) to the application protocols that it supports.

Star topology / Network

A LAN in which all terminals are connected to a central computer, hub or switch by point-to-point links. A disadvantage of this method is that all data has to pass through the central point, thus raising the risk of saturation.

Stateful Inspection

Method of filtering network connections invented by Check Point, based on keeping the connection status. Packets are authorized only if they correspond to normal connections. If a filter rule allows certain outgoing connections, it will implicitly allow incoming packets that correspond to the responses of these connections.

Static quarantine

A quarantine that the administrator sets when configuring the firewall.

Symmetrical key cryptography

A type of cryptographic algorithm in which the same key is used for encryption and decryption. The difficulty of this method lies in the transmission of the key to the legitimate user. DES, IDEA, RC2 and RC4 are examples of symmetrical key algorithms.

T

TCP (Transmission Control Protocol)

A reliable transport protocol in connected mode. The TCP session operates in three phases – establishment of the connection, the transfer of data and the end of the connection.

Throughput

The speed at which a computer processes data, or the rate of information arriving at a particular point in a network system. For a digital link, this means the number of bits transferred within a given timeframe. For an internet connection, throughput is expressed in kbps (kilobits per second).

Trace route

Mechanism that detects the path a packet took to get from one point to another.

Trojan horse

A code inserted into a seemingly benign program, which when executed, will perform fraudulent acts such as information theft.

TTL (Time-to-Live)

The period during which information has to be kept or cached.

U

UDP (User Datagram Protocol)

One of the main communication protocols used by the internet, and part of the transport layer in the TCP/IP stack.
This protocol enables a simple transmission of packets between two entities, each of which has been defined by an IP address and a port number (to differentiate users connected on the same host).

Unidirectional translation (MAP)

This translation type allows you to convert real IP addresses on your networks (internal, external or DMZ) into a virtual IP address on another network (internal, external or DMZ) when passing through the firewall.

URL filter

Service that enables limiting the consultation of certain websites. Filters can be created in categories containing prohibited URLs (eg. Porn, games, webmail sites, etc) or keywords.

URL (Uniform Resource Locator)

Character string used for reaching resources on the web. Informally, it is better known as a web address.

User enrolment

When an authentication service has been set up, every authorized user has to be defined by creating a "user" object. The larger the enterprise, the longer this task will take. NETASQ's web enrolment service makes this task easier. If the administrator has defined a PKI, "unknown" users will now request the creation of their accounts and respective certificates.

UTM (Unified Threat Management)

Concept that consists of providing the most unified solution possible to counter multiple threats to information security (viruses, worms, Trojan horses, intrusions, spyware, denials de service, etc).

V

VLAN (Virtual Local Area Network)

Network of computers which behave as if they are connected to the same network even if they may be physically located on different segments of a LAN. VLAN configuration is done by software instead of hardware, thereby making it very flexible.

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.

VPN keep alive

The artificial creation of traffic in order to remove the latency time which arises when a tunnel is being set up and also to avoid certain problems in NAT.

VPN Tunnel

Virtual link which uses an insecure infrastructure such as the internet to enable secure communications (authentication, integrity & confidentiality) between different network equipment.

W

WAN (Wireless Area Network)

Local wireless network.

Wifi (Wireless Fidelity)

Technology allowing wireless access to a network.

documentation@netasq.com