NETASQ

NETASQ UNIFIED MANAGER

NETASQ UNIFIED MANAGER

V. 8.0

USER CONFIGURATION MANUAL

Reference: ENUG0811_NUMANAGER-V8.0
Created: January 2007
Modified: November 2008

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.

Publication Information

Reference: ENUG0811_NUMANAGER-V8.0
Version 8.0
November 2008

Products concerned

U30, U70, U120, U250, U450, U1100, U1500 and U6000.

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

Licence 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 warrantly 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 – Warrantly

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.

PART 1: INTRODUCTION

CHAPTER 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.

CHAPTER 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
Decribes technical terms relating to NETASQ or networking. These terms will also be covered in te 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`.

CHAPTER 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 Uxx	Refers to the NETASQ product range. Other terms also used: NETASQ Uxx, Uxx appliance.
Firewall	NETASQ UTM device /product
Intrusion prevention	Unified Threat Management or IPS are 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.

CHAPTER 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.

CHAPTER 5. GENERAL

1.5.1. Introduction

Thank you for choosing NETASQ. Designed to protect structures of all sizes, NETASQ’s UTM appliances are pre-configured: no hardware or software installation nor UNIX knowledge is necessary, just a user-friendly configuration via a graphical interface.

The NETASQ UTM appliance allows the definition of incoming or outgoing access control rules. Its concept is simple: any incoming or outgoing transmission passing through the NETASQ Firewall is monitored, authorized or refused according to the rules, packet by packet.

The NETASQ Firewall is based on an upgraded packet filtering mechanism which brings a high level of security. All NETASQ Firewalls integrate the ASQ (Active Security Qualification) technology developed by NETASQ. This technology allows detection and blocking of hacking attempts in real time – illegal packets, denial of service attempts, anomalies in a connection, port scans, buffer overflows, etc.

In the case of an intrusion attempt, depending on the instructions given in the security policy, the NETASQ Firewall blocks the transmission, generates an alarm and stores the information linked to the packet which had set off the alarm. As such, you would be able to analyze the attack and trace its source.

With the new NETASQ SEISMO tool, it is now possible to report vulnerabilities that may affect data relating to the operating system, application services (e.g. web, mail) and applications installed on the corporate network. All relevant information is gathered and stored in order to compile profiles of network elements. A help system allows detecting the vulnerability and repairing it.

The Firewall not only allows preventing or limiting certain services and incoming connections on your network, but also allows monitoring the use of the internet by your internal users (HTTP, FTP, SMTP...). You may also monitor your users by way of an authenticator via an internal or external authentication database.

The NETASQ Firewall also manages port and address translation mechanisms. These mechanisms provide security (by masking your internal addressing), flexibility (by enabling the use of any private internal addressing range) and reduce costs (by enabling the provision of several servers on the internet with a single public IP address).

With the NETASQ IPS (Intrusion Prevention System) engine, a firewall offers all the more security. Its plugin architecture allows monitoring the major part of the traffic circulating through the Firewall even at the application layer. Its performance in terms of throughput, number of rules and number of tunnels, has been increased tenfold.

Thanks to its Windows-based user interface, it allows the rapid and simple definition of your network's security rules, performed from a local workstation running under Windows. You may also monitor your Firewall's activity in real time.

The NETASQ Firewall is also equipped with advanced log functions. In an intrusion attempt, the network administrator may access all data sent before the attack and see how it had been prepared. NETASQ EVENT REPORTER provides you with a graphical view and fine analysis oF logs generated on the Firewall.

Lastly, the NETASQ Firewall includes VPN gateway functions allowing you to establish encrypted tunnels with other VPN equipment. In this way, your communications between sites or with your mobile users (“Road Warriors”) may be secured even while using an insecure communication infrastructure like the internet.

1.5.2. Precautions of use

> **WARNING**
> Using the wrong type of lithium batteries may cause the components to explode. Please follow the indications given by the manufacturer of the lithium batteries (these are used in your fwl) on how to recycle used batteries.

> **WARNING**
> The firewall has to be installed in compliance with the state of the art corresponding to the practical terms of installation, that is to say: in a protected office or other premises with limited access. In order to guarantee the integrity of the product and to avoid compromising the security of your installation, all unauthorized access to the firewall has to be limited.

WARNING
Ensure that you place heavier equipment in the lower racks of the cabinet, and the lighter appliances in the higher racks.

WARNING
Most NETASQ appliances require a land-based connection. Ensure that your power grid has good ground conductivity, which meets NETASQ's specifications concerning the power supply of firewalls. It would be even better to protect the power supply with UPS devices.

WARNING
NETASQ appliances do not have power supply switches. In all cases, unplugging the power cable from the mains socket will disconnect the appliance from the main power supply.

WARNING
NETASQ firewalls should not be installed in locations where the temperature may exceed 35°C.

WARNING
Ensure that nothing obstructs the air vents on the product in order to guarantee maximum air circulation.

WARNING
The metal brackets on the front panel of the U6000 product are not to be used for lifting the product but only for racking the firewall or for removing it from its racks.

1.5.3. Upon receiving your firewall

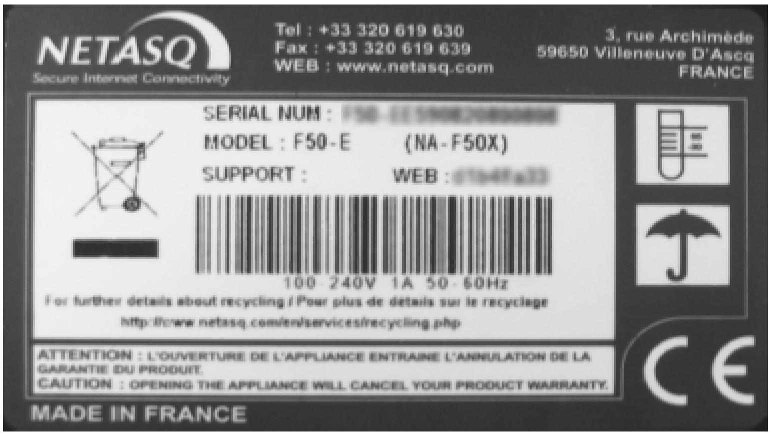
1.5.3.1. Integrity of the product

In order to guarantee the integrity of your product, NETASQ has set up several mechanisms. Check these mechanisms to confirm that your product has not been tampered with:

- **Labels**: every firewall is delivered in a cardboard box with three labels affixed, indicating information identifying the product it contains and its version. There is also a "Serial number" label affixed directly on the product. The 3rd label serves to identify the configuration of the product. Check that this information matches your order.

The 3 labels are as follows:

Serial number label: this label, pasted on the product, indicates information such as the serial number, sales platform, web activation code (which enables the activation of the client account in the NETASQ website's client area) and the barcode that contains the product's serial number.



NETASQ
Secure Internet Connectivity

Tel : +33 320 619 630
Fax : +33 320 619 639
WEB : www.netasq.com

3, rue Archimède
59650 Villeneuve D'Ascq
FRANCE

SERIAL NUM : [redacted]
MODEL : F50-E (NA-F50X)
SUPPORT : WEB : [redacted]

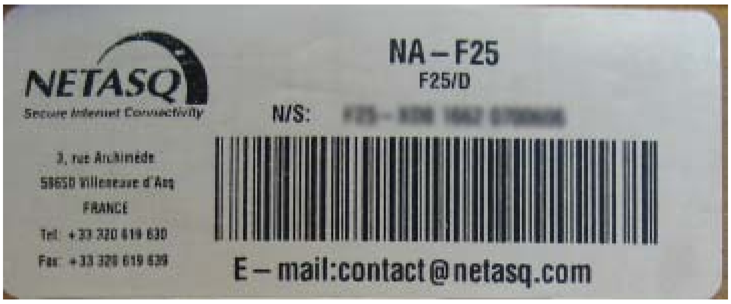
100-240V 1A 50-60Hz
For further details about recycling / Pour plus de détails sur le recyclage
http://www.netasq.com/en/services/recycling.php

ATTENTION : L'OUVERTURE DE L'APPLIANCE ENTRAINE L'ANNULATION DE LA GARANTIE DU PRODUIT.
CAUTION : OPENING THE APPLIANCE WILL CANCEL YOUR PRODUCT WARRANTY.

MADE IN FRANCE

Figure 1: Serial number label

Packaging identification label: this label, pasted on the packaging of the product, provides information relating to the sales platform, serial number of the product and the barcode containing the product's serial number.



NETASQ
Secure Internet Connectivity

NA–F25
F25/D

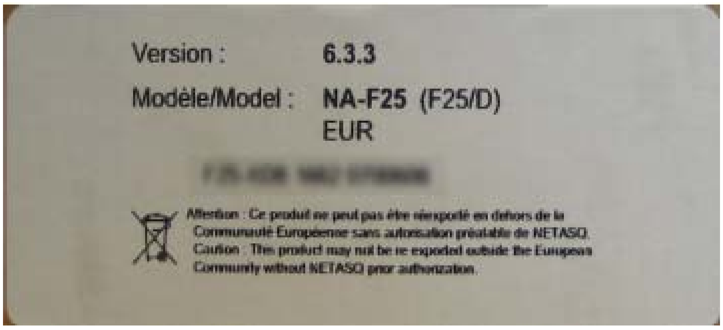
N/S: [redacted]

3, rue Archimède
59650 Villeneuve d'Ascq
FRANCE
Tel: +33 320 619 630
Fax: +33 320 619 639

E–mail:contact@netasq.com

Figure 2: Packaging identification label

Version number label: this label, pasted ion the packaging, indicates the software version installed on the firewall. The version is defined by a version number and model (which correspond to a certain export zone). This label helps to check later if the delivered version has been certified.



Version : 6.3.3
Modèle/Model : NA-F25 (F25/D)
EUR

[redacted]

Attention : Ce produit ne peut pas être réexporté en dehors de la Communauté Européenne sans autorisation préalable de NETASQ.
Caution : This product may not be re-exported outside the European Community without NETASQ prior authorization.

Figure 3: Product version label

- **Quality seal**: every firewall is delivered in a carboard box on which a NETASQ-specific quality seal is affixed. Check that there is such a seal on your product's packaging.
Except for the U6000, a "NETASQ QUALITY SEAL" label will be affixed.

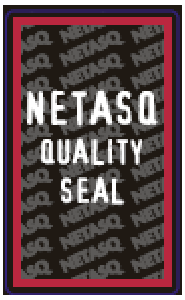
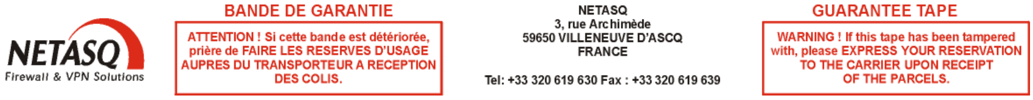


Figure 4: "Quality seal" label

For the U6000, the following label will be found:



NETASQ
Firewall & VPN Solutions

BANDE DE GARANTIE

ATTENTION ! Si cette bande est détériorée, prière de FAIRE LES RESERVES D'USAGE AUPRES DU TRANSPORTEUR A RECEPTION DES COLIS.

NETASQ
3, rue Archimède
59650 VILLENEUVE D'ASCQ
FRANCE

Tel: +33 320 619 630 Fax : +33 320 619 639

GUARANTEE TAPE

WARNING ! If this tape has been tampered with, please EXPRESS YOUR RESERVATION TO THE CARRIER UPON RECEIPT OF THE PARCELS.

Figure 5: Warranty band

If this band is missing, contact your distributor sonnest possible to find out why the packaging has been opened.

- **Firewall seal**: a seal label is pasted on all firewalls. This prevents the replacement or modification of the firewall's hardware elements. This label has the peculiarity of displaying a message (VOID) that cannot be erased once the label has been removed. There are two types of seal: on pasted by NETASQ after production and one pasted by your partner if a maintenance operation has been performed on your appliance (your partner would have explained this maintenance operation to you through an activity certificate).

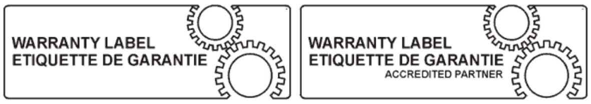


Figure 6: Firewall seal

Confirming the presence of these security mechanisms will help you ensure the integrity of the product delivered. Feel free to contact your distributor if any of these elements does not match its description.

1.5.3.2. Contents of the packaging

Keep the cardboard packaging safely in case you need it later for transporting the firewall. It has been designed to give your NETASQ firewall optimum protection (shock and temperature resistence).

Upon delivery, check that the following have been included in the packaging

- The NETASQ firewall in the model ordered
- A power cable (ref. 1076036)
- A crossover DB9F serial cable (ref. 1076033)
- An RJ 45 crossover cable (blue cable, ref. 1076034)
- An envelop containing the NETASQ software suite CD-ROM (Administration Suite)
- A sheet indicating the license agreement.
- Brackets and fastening system for racking your firewall
- The power pack for U30 and U70.

If any of the elements is missing, contact your distributor immediately.

1.5.4. Presentation of the appliances

For more information on connectors for the U Series appliances, please refer to the Technical Note “Connectors and cards: U Series (*ENTN0811_CONNECTORS-CARDS-U-SERIES*).

1.5.5. Dismantling the appliance

> ❗ **WARNING**
> Under no circumstances should you take apart a NETASQ appliance on your own.
>
> ❗ **WARNING**
> Only NETASQ and its approved maintenance agents are authorized to do so.
>
> ❗ **WARNING**
> Your warranty will be rendered null and void should you dismantle a NETASQ firewall on your own.

1.5.6. The chassis

Flexible feet have been placed under the chassis of the firewall to ensure that the NETASQ firewall is on a stable plane (on a desk or on other IT equipment).

These feet can be delivered installed on the appliance or delivered in a kit except for the U6000 model.

PART 2: INSTALLATION, PRE-CONFIGURATION, INTEGRATION

CHAPTER 1: GRAPHICAL INTERFACE

2.1.1. Introduction

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 gigabites 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

2.1.1.1. For this chapter, you will need to

Have the installation file of the graphical interface. This file is available on the CD-ROM delivered with your firewall or on the NETASQ website (www.netasq.com). The installation file exists in two languages – English and French.

Know the internal IP address of your firewall, as well as its serial number.

2.1.1.2. Purpose of this section

This section will show you the elements for the installation and general use of the configuration graphical interface (NETASQ UNIFIED MANAGER).

2.1.2.3. 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 coomunication 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.

2.1.1.4. Two modes of using NETASQ UNIFIED MANAGER

NETASQ UNIFIED MANAGER is able to operate in two different modes: Global Administration mode and Firewall Manager mode.

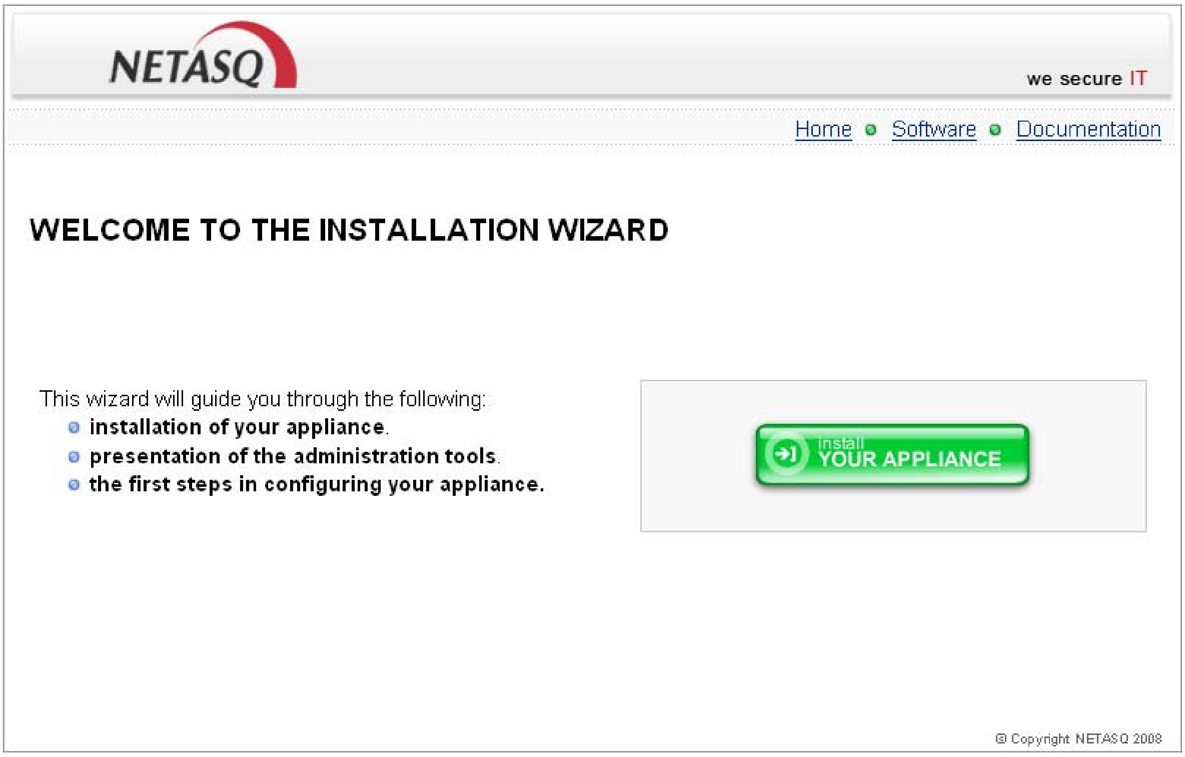
- The Firewall Manager mode allows you to configure the product.
- The Global Administration mode is the software solution for managing certain administration actions over a whole fleet of NETASQ products, easily, affordably and from a central location.

2.1.2. Installation

2.1.2.1. Installation procedure

Insert the installation CD-ROM delivered with the appliance or download the necessary files from NETASQ’s website and execute the .exe program the corresponds to the administration suite. Information regarding the installation will be displayed in the language of the version of Windows installed.

When the CD-ROM is inserted, the administration suite installation wizard will automatically launch, and will guide you through the process step by step.



WELCOME TO THE INSTALLATION WIZARD

This wizard will guide you through the following:

- installation of your appliance.
- presentation of the administration tools.
- the first steps in configuring your appliance.

Figure 7: Installation wizard in the CD-ROM

2.1.3. Verification procedure

2.1.3.1. 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?”.

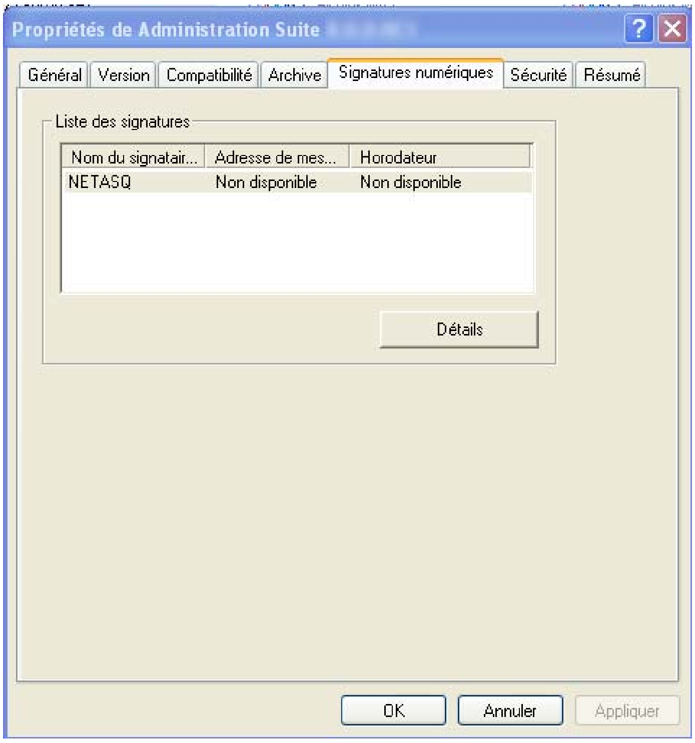
- If you choose “Open”, your web browser will check the signature automatically and inform you about the results.
- If you choose “Save” (recommended option), you will need to perform the check manually.

2.1.3.1. 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).



Nom du signatair...	Adresse de mes...	Horodateur
NETASQ	Non disponible	Non disponible

Figure 8: Digital signatures

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

2.1.4. 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.

2.1.5. Technical Assistance Center

NETASQ offers several means and tools for resolving technical problems on your firewall.

- A knowledge base.
- A certified distribution network. You can therefore call upon your distributor whenever necessary.
- Documentation: accessible on your client or partner area. You will need an account in order to access these documents.

For more information regarding technical assistance please refer to the document "NETASQ standard support".

CHAPTER 2: THE NETASQ FIREWALL

2.2.1. Introduction

2.2.1.1. For this chapter, you must have read the following chapters:

- Part 2/Chapter 1: Graphical interface

2.2.1.2. For this chapter, you will need to know

- Your firewall's IP address (if the product is still in factory configuration, the IP address will be: 10.0.0.254).

2.2.1.3. Purpose of this chapter

We advise you to read this manual carefully before installing the software. It will help you to quickly familiarize yourself with the appliance and the related tools. This first reading will already familiarize you with the NETASQ firewall.

A firewall is the central device in your network, therefore do not neglect it – install it in the best way possible, under the best conditions.

This chapter will help you in carrying out the installation of the appliance and to pre-configure it in order to integrate it into the desired network architecture.

2.2.2. Preparing for the physical installation of the appliance

2.2.2.1. Installation precautions

Premises for the installation

The appliance has to be installed in an enclosed area, or otherwise, a locked cabinet with protected physical access to the appliance. All unauthorized access to the appliance may compromise the security of your installation.

Installation recommendations

If installing the appliance in a bay, heavier equipment should be placed as low as possible in the rack or cabinet and lighter equipment above.

Ensure that the electrical power supply has been correctly grounded and correctly dosed in order to suppose the NETASQ appliance's power supply, and preferably backed up by an inverter.

REMARK
U30 and U70 appliances use a double-insulation power supply, and therefore do not require a land-based connection.

Do not install the NETASQ appliance in an environment with a surrounding temperature that may exceed 35°C.

Ensure that there is sufficient air circulation around the firewall and that nothing blocks the air vents on the product.

Warranty

Never dismantle the appliance as any unauthorized dismantling will render your warranty null and void.

2.2.2.2. Preparation before installation

Preparation of the network cables

You need to use a network cable for each firewall interface connected to your infrastructure.

Type of network cable according to network port

Type of Ethernet port	Type of cable	Connector
10/100BaseT Ethernet port	To run at 100Mbits/s: Category 5 twisted pair or higher.	RJ45
10/100/1000BaseT Ethernet port	To run at 100Mbits/s or 1000Mbits/s: Category 5 twisted pair or higher.	RJ45
1000FX Gigabit Ethernet port (fiber cable)	Optic fiber cable	LC

Type of network cable according to the connected device

Device connected to the firewall	Type of cable
Hub	Straight cable
Switch	Straight cable
Modem	Straight or crossover cable. Check the documentation on the modem to find out the type of cable to use. You can also connect the firewall to the modem (depending on the type of modem) with a serial link by using a straight serial cable.
Router	Straight or crossover cable, if the router embeds a hub.
Autre firewall	Crossover cable
PC	Crossover cable

NOTE

A crossover cable is delivered with the NETASQ firewall.

Preparation of the racking cabinet or bay

You will need to set aside a minimum space in your cabinet or racking bay in order to install the NETASQ appliance. Depending on the product, the minimum height requirements vary:

- U30, U70: 1U in height, half-19''in width
- U120, U250 and U450: 1U in height, 19'' in width
- U1100 and U1500: 1U in height, 19'' in width
- U6000: 4U in height, 19'' in width.

WARNING
Set aside a minimum vertical space between each element in the cabinet or racking bay for proper air circulation.

Preparation of internet access

Before installing the NETASQ firewall, ensure that the devices that connect to the internet (if the firewall has to be connected with the internet network) have been appropriately installed and configured.

2.2.3. Placing the appliance in a bay

All NETASQ appliances can be installed in 19-inch cabinets or bays. U1100 and U 1500 products have built-in brackets that allow the direct installation of the product. The U6000 is sold with a rail system that allows integrating it into a bay.

U120, U250 and U450 products are sold with a fastening system that has to be added to the product in order to install it. The system is available only by special order for the U30 and U70.

2.2.3.1. Installing a U30 or U70

View from the top

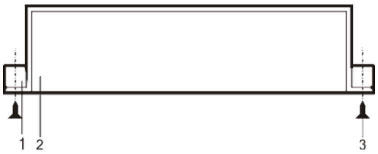


Figure 9: U30, U70: Installation in a bay – View from the top

View from the front

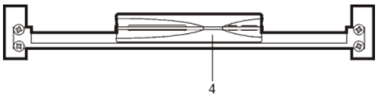


Figure 10: U30, U70: Installation in a bay - View from the front

1. Lateral bars in the bay
2. Supporting deck
3. Screws and caged nuts
4. Appliance

A system for installing the appliance in a bay can be delivered for the U30 and U70 by special order:

1 Installation of the deck in the bay. Screw the supporting deck to the lateral sides of the rack using the caged nuts.

2 Once the deck has been installed, you will be able to place on or two products (no fastening is needed) on the supporting deck.

WARNING
Ensure there is space of 1U above the product for for proper air circulation.

2.2.3.2. Installing a U120, U250 or U450

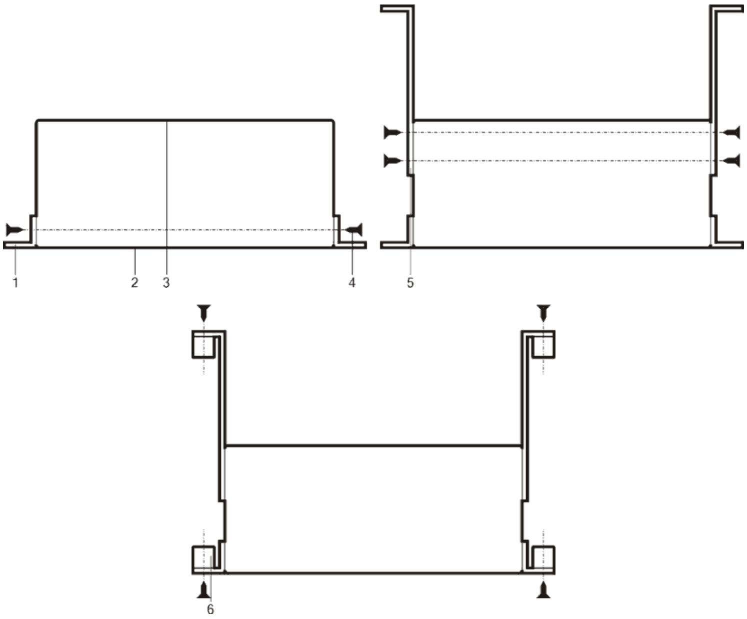


Figure 11: U120, U250, U450: Installation in a bay

1. Lateral bars in the bay
2. Front panel
3. Rear panel
4. Screws and caged nuts

The U120, U250 and U450 appliances are delivered with a set of brackets for mounting the appliance in a bay. These brackets are not shown in the diagram above.

1 Installation of the deck in the bay. Screw the lugs of the chassis to the lateral sides of the bay.

> **WARNING**
> The metal handles on the front panel of the product should not be used for lifting it, but only for setting it in or removing it from the bay.

2.2.3.3. Installing a U1100, U1500 or U6000

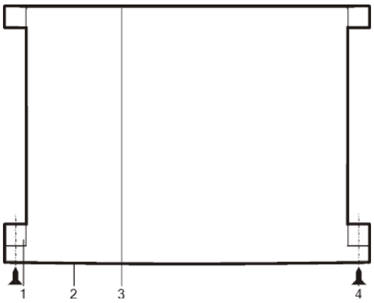


Figure 12: U1100, U1500, U6000: Installation in a bay

1. Brackets
2. Front panel
3. Rear panel
4. Screws and caged nuts
5. Supporting rail
6. Lateral bars in the bay

The U1100 and U1500 appliances are delivered with a system of brackets to be attached to the front panel of the appliance and lateral supporting rails.

1 Setup of the supporting rails. Screw the brackets to the appliance. The lugs have to be placed at the front panel of the product.

2 Setup of the supporting rails. The positioning of the supporting rails depends on the size of the bay.

3 Installation of the deck in the bay. Screw the brackets and supporting bars to the lateral sides of the bay.

2.2.4. Connections

2.2.4.1. Location

The NETASQ firewall has been designed to run continually, in an office or other premises. If you do not have a telecom closet, choose a flat and uncluttered surface, avoid places exposes to heat (sun rays, for example), humidity or dust.

2.2.4.2. Power plug

NETASQ firewalls can operate on 230V or 110V.

Insert the connector of the power cable (provided with the product) into the power socket on the rear panel of the NETASQ appliance. Next, plug in the pin of the power cable into an appropriate power supply.

The firewall will start up the moment it is plugged into the electrical network.

A redundant power supply is provided for on the U6000 firewall. We advise you to connect each of the two power cables to distinct electrical networks so that you can protect yourself from power failures on your U6000. You are furthermore advised to connect these power supplies to inverters (preferably "online)

> **WARNING**
> We recommend that you use a power supply backed up by an inverter.

2.2.4.3. Connection for administering the appliance

> **WARNING**
> The appliance is administered by default via the INTERNAL interface. This interface, depending on the model, is identified by the number "2" (U30, U70, U120, U250, U450).

2.2.4.4. Connecting to the network

Connect the firewall's different interfaces to the network interconnection elements with an RJ45 cable. The numbers of the interfaces apply to the U30, U70, U120, U250 and U450 models:

- The interface identified as "1" on the firewall corresponds to the EXTERNAL interface (called OUT by default)
- The interface identified as "2" on the firewall corresponds to the INTERNAL interface (called IN by default)
- The interfaces identified as "3, 4, 5, etc" on the firewall correspond to the DMZ interfaces (like the INTERNAL interface, these interfaces host internal networks)

The interfaces are indicated below by appliance model:

U30

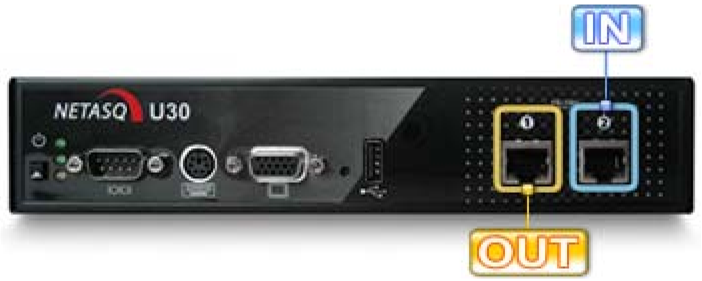


Figure 13: U30 interfaces

U70

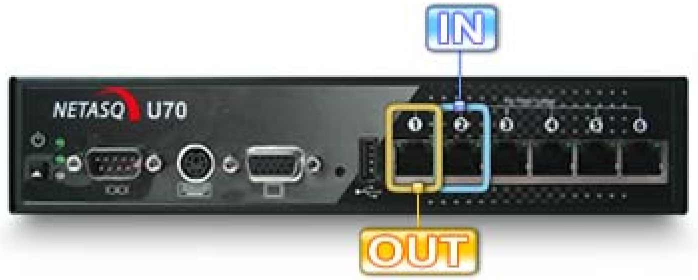


Figure 14: U70 interfaces

U120

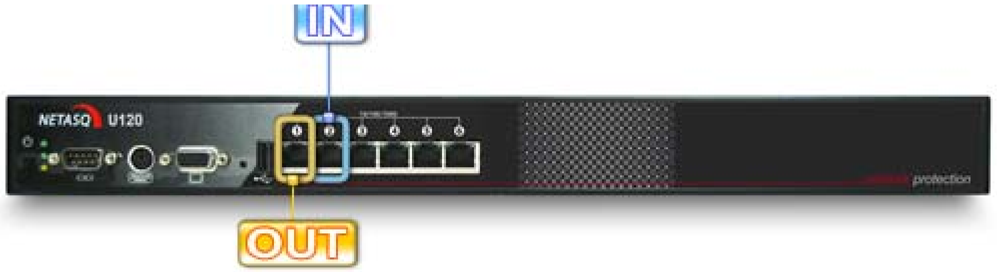


Figure 15: U120 interfaces

U250

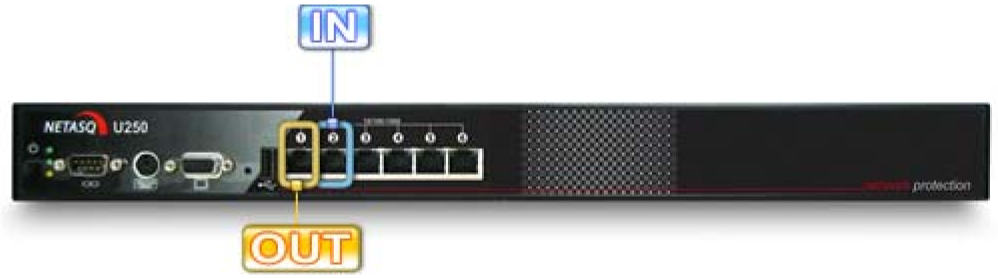


Figure 16: U250 interfaces

U450

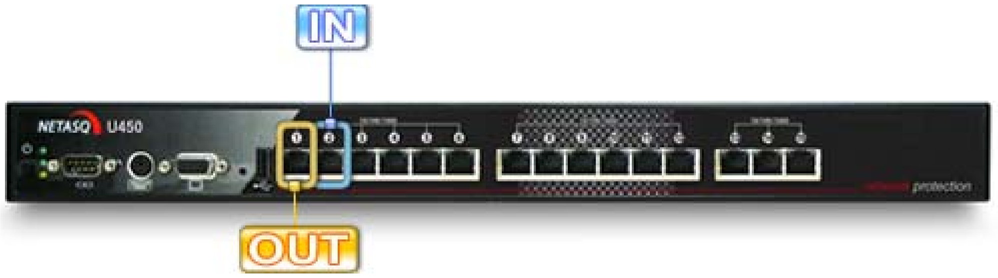


Figure 17: U450 interfaces

U1100

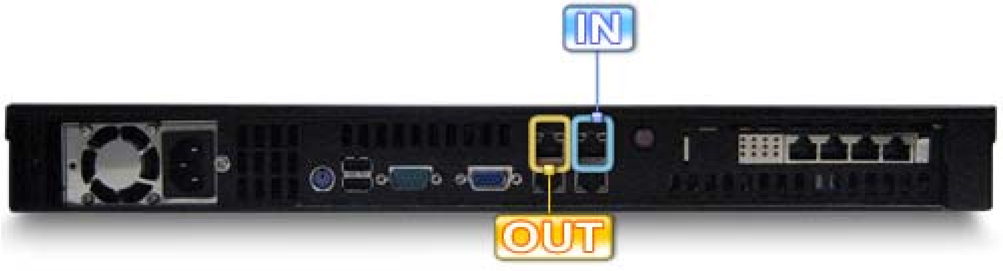


Figure 18: U1100 interfaces

U1200

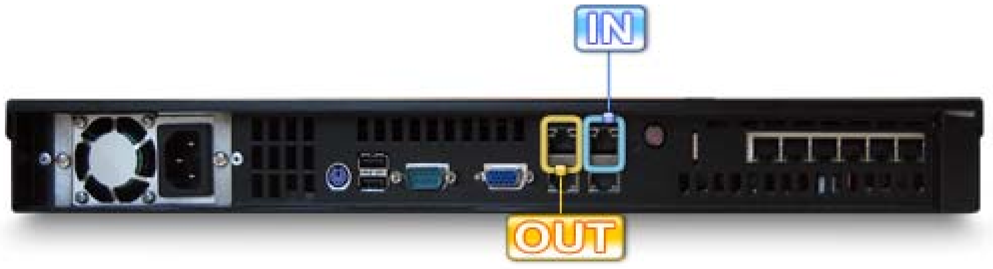


Figure 19: U1200 interfaces

U6000

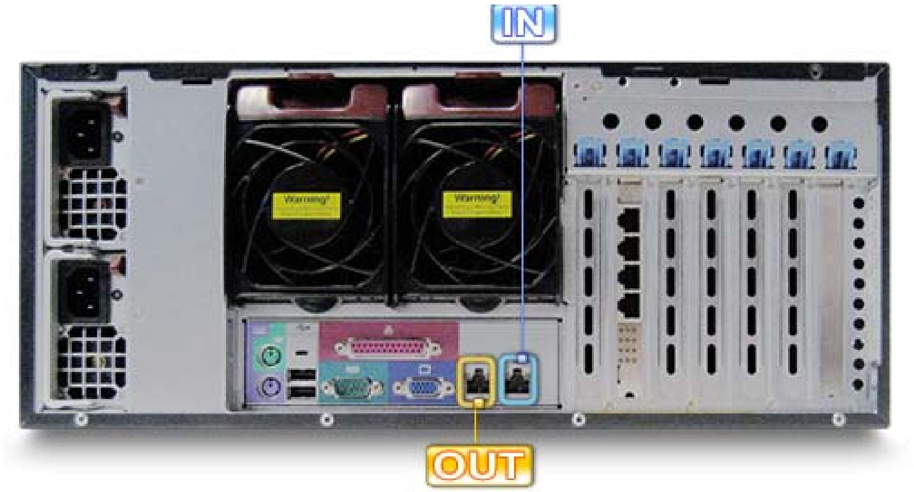


Figure 20: U6000 interfaces

Using a straight cable

A straight cable has to be used between a firewall and a hub, a switch or certain modems (depending on the type of modem, a straight or a crossover cable will be necessary).

Using a crossover cable (cable provided with the product)

A crossover cable has to be used for connecting the firewall to an active network element (router, firewall, PC, certain modems, etc).

WARNING
Certain routers have built-in hubs. In this case, you will need to use a straight cable.

WARNING
In the event there has been an error in the connection of cables, you will need to restart your product in order to connect again (this is due to the anti-spoofing protection mechanism).

NOTE
After you hear 8 consecutive beeps, you will be able to insert a USB key containing a configuration if necessary.
2 consecutive beeps indicate the end of the product's startup phase.

2.2.5. Preconfiguration

When you first receive your firewall, it will run in transparent mode and will have the IP address 10.0.0.254 with a subnetwork mask 255.0.0.0.

These parameters do not match your network configuration, but they are however necessary for the preconfiguration phase.

If you do not know what these parameters mean, we strongly advise that you read up on TCP/IP in order to understand how to configure your NETASQ firewall.

These are the intervals defined by the different classes of IP address:

Class	IP address range
A	0.0.0.0 to 127.255.255.255
B	128.0.0.0 to 191.255.255.255
C	192.0.0.0 to 223.255.255.255
D	224.0.0.0 to 239.255.255.255
E	240.0.0.0 to 247.255.255.255

Some parts of these address ranges are reserved for private networks:

Class	Reserved IP address ranges
A	10.0.0.0 to 10.255.255.255
B	172.16.0.0 to 172.31.255.255
C	192.168.0.0 to 192.168.255.255

2.2.5.1. Preconfiguring a Windows workstation

Preconfiguring from a Windows workstation is the method that we recommend, which is what we will be using for our illustrations. The workstation can either be directly linked to the firewall's internal interface, or connected to the local network, itself linked to the firewall's internal interface. For a direct connection of the workstation to the firewall, use the crossover Ethernet cable, which has been delivered with the product.

> **WARNING**
> The firewall's INTERNAL interface is labeled "2" on the appliance (on the front panel for U30, U70, U250 and U450 appliance, and on the rear panel for U1100, U1500 and U6000 appliances).

To connect to the firewall, you need to use a workstation with an IP address in the same subnetwork as the firewall. We suggest that you use the address 10.0.0.1 and the subnetwork address 255.0.0.0.

The procedure for configuring your Windows workstation is as follows:

1. Go to the Control panel on your Windows workstation,
2. Select the "Network" menu,
3. Select TCP/IP from the list of network elements, then "Properties",
4. Indicate the address information required for the network configuration of the workstation:

   - IP address: 10.0.0.250 or the IP address you have selected for your workstation,
   - Subnetwork mask: 255.0.0.0,
   - Default gateway: indicate the current address of your firewall (10.0.0.254 by default).

Or configure your workstation so that it accepts a dynamic IP address from the appliance (DHCP server):

1. Open the **Network connections** window

- Windows 2000
Start > Control panel > Network and dial-up connections

- Windows XP
Start > Control panel > Network and Internet connections

2. Right-click against "Connect to the local network" and select "Properties".
3. Select "Internet Protocol (TCP/IP)" from the list, then "Properties".
4. Select the option **Obtain an IP address automatically** and click on **OK.**
5. To confirm changes, click on **OK** again.

2.2.5.2. Registering and installing the product

Your product has an installation help web server that will show you through the different steps in the configuration.

The 1st page of the authentication portal allows you to define a password ofr your product.

Next, you will be able to:

- Configure the network to define the network architecture in which your product will be located.
- Register your product in order to obtain updates
- Perform the first updates

- Obtain the license
- Install the administration tools in order to obtain the Manager, Monitor and Reporter software suite.

2.2.5.3. Preconfiguring a firewall

You can now connect to the firewall through the NETASQ configuration graphical interface, NETASQ UNIFIED MANAGER.

After you have installed this configuration software on your client workstation, you can modify the parameters of the network interfaces on the NETASQ firewall in order to adapt it to your IP addresses and to select the operating mode (transparent or normal). (Cf. *Part 5: Network configuration*).

If you had changed the IP address of the Windows client workstation for this configuration, don’t forget to reset it to its former configuration.

2.2.5.4. Antispoofing mechanism

WARNING
If you connect to an interface then unplug the cable to connect to another interface, you will trip the firewall’s anti-spoofing security feature (it will then be impossible to connect to this appliance). When this situation arises, there are two solutions – either you change the address that you have just assigned to the administration host (this is what NETASQ recommends), or you reboot the appliance after you have changed its interface.

PART 3: GETTING FAMILIAR WITH THE "FIREWALL MANAGER" MODE

CHAPTER 1: DESCRIPTION

3.1.1. For this chapter, you must have read the following chapters

- Part 2/Chapter 1: Graphical interface.
- Part 2/Chapter 2: The NETASQ firewall.

You will find a detailed description of these points in the NETASQ UTM appliance installation manual, which can be found either on the installation CD-ROM or on NETASQ's website in the client or partner secure-access areas.

3.1.2. For this chapter, you will need to know

Your firewall's IP address (10.0.0.254 if the product has not yet been configured).

3.1.3. Purpose of this chapter

The steps described in this section will guide you in learning about your NETASQ Firewall. Once you have mastered the graphical interface, you will be in a position to continue configuring your appliance.

CHAPTER 2: EXECUTION

3.2.1. Access

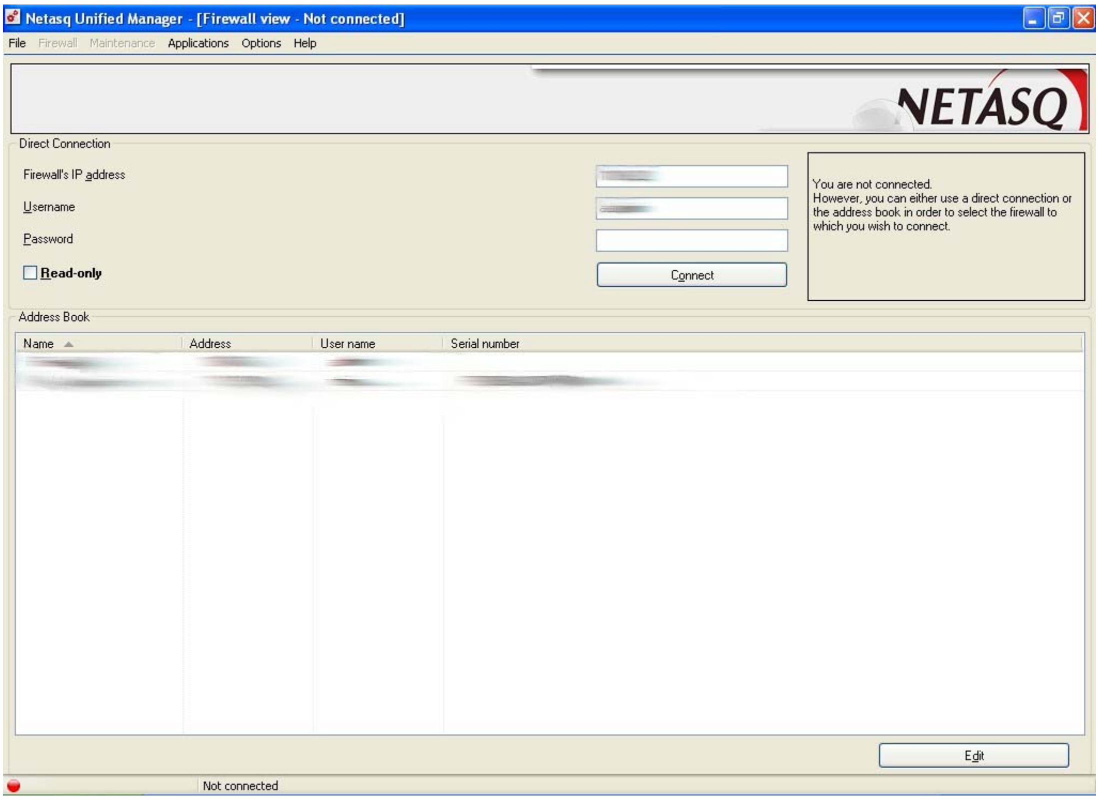
There are two ways to access the NETASQ UNIFIED MANAGER application, the configuration interface on NETASQ UTM appliances.

- Using the menu **`Applications\Launch NETASQ UNIFIED MANAGER`** in the menu bar in the applications NETASQ REAL-TIME MONITOR and NETASQ EVENT REPORTER in the Administration Suite.

- Using the menu **`Start\Programs\Netasq\Administration Suite 8.0\NETASQ UNIFIED MANAGER.`**

The main screen appears after you connect:

When you launch the NETASQ configuration interface, the application's start screen will show you the version of the software that has been installed. Thereafter, the main window of the NETASQ firewall configuration graphical interface will appear.



Direct Connection

Firewall's IP address [redacted]

Username [redacted]

Password

□ Read-only

You are not connected.
However, you can either use a direct connection or the address book in order to select the firewall to which you wish to connect.

Address Book

Name	Address	User name	Serial number
[redacted]	[redacted]	[redacted]	
[redacted]	[redacted]	[redacted]	[redacted]

Not connected

Figure 21: Accessing NETASQ UNIFIED MANAGER

From this window you can access the various NETASQ Firewall configuration sections.

As long as you are not connected to a firewall, you will be unable to access the main features of the interface. The menus to which you have access are:

- The **File** menu which allows you to access the address book in order to connect to a selected firewall. Refer to *Part 19: Miscellaneous actions* for more information.
- The **Applications** menu allows you to launch the two other applications that make up the NETASQ Administration Suite – NETASQ REAL-TIME MONITOR AND NETASQ EVENT REPORTER.
- The **Options** menu allows you to execute the general preferences for the application.
- The **Help** menu leads you to help files, allows you to update the application and to find out the version of the graphical interface.

3.2.2. Connection

Connections to the firewall as an administrator are made via software in the NETASQ administration suite: NETASQ UNIFIED MANAGER for the configuration of features, NETASQ REAL-TIME MONITOR to monitor activity and NETASQ EVENT REPORTER for compiling logs and reporting network events.

Firewalls can only be configured by product administrators. NETASQ defines an administrator as a user who possesses administration rights. Rights are assigned to users during their configuration (see *Part 4/Chapter 3: Users*).

3.2.2.1. The initial connection

WARNING
By default, NETASQ appliances can only be accessed via NETASQ UNIFIED MANAGER, meaning that ANY OTHER MEANS OF ACCESSING NETASQ UNIFIED MANAGER WILL BE BLOCKED.

> **Example**
> You cannot ping to find out whether the appliance functions.

3.2.2.2. The "admin" account, super-administrator

By default, only one user has administration rights on NETASQ products – the "admin" account (whose login is "admin"). This administrator is a super-administrator and possesses all configuration privileges as well as the special "ADMIN" privilege that only he possesses. This privilege gives him the right to perform certain operations, such as modifying a certain user's authentication method, for example. The "admin" user cannot be configured.

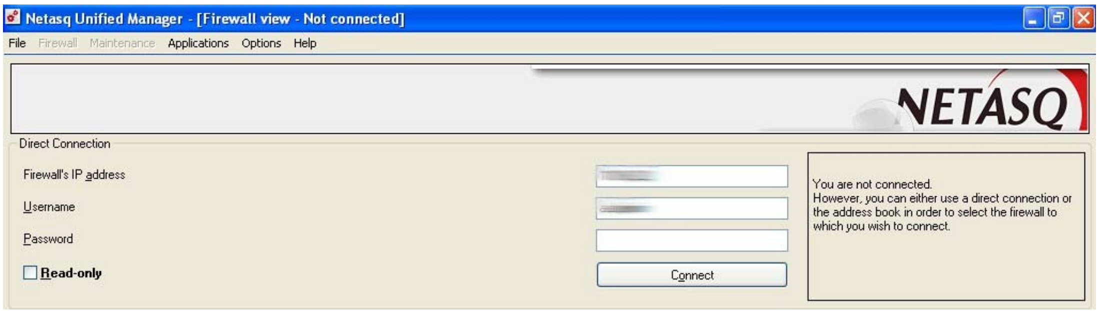
REMARK
Given the privileges that come with the "admin" account, NETASQ recommends that you use this account only for tests and maintenance.

3.2.2.3. Connection procedure

The process of connecting to a firewall is defined by a three-step procedure which varies according to the stage of the configuration.

REMARK
Step 3 only applies to the initial connection

Step 1: Sending connection information to the firewall



Direct Connection

Firewall's IP address

Username

Password

☐ Read-only

You are not connected.
However, you can either use a direct connection or the address book in order to select the firewall to which you wish to connect.

Figure 22: Connecting to NETASQ UNIFIED MANAGER

<u>In the case of an initial connection</u>

If this is your very first connection to this Firewall, the connection information is as follows:

Firewall's IP address	The IP address of the NETASQ Firewall in default configuration.
Username	"admin", only the administrator is defined in the default configuration.
Password	NO PASSWORD (empty field), a generic password is used in the default configuration.
Read only	Enables connecting in "read-only" mode. In this way, you would be able to connect to the firewall without modification privileges using an account that ordinarily would provide these privileges. Read-only mode allows the user to refrain from using modification privileges when they are not necessary.

Once you have entered the necessary connection information, click on the **Connect** button to send it to the Firewall. Then go on to the next step.

<u>In the case of other connections</u>

The following information is needed in order to connect to a firewall:

Firewall's IP address	IP address or hostname of the NETASQ Firewall on the internal network.
Username	User name for the configuration.
Password	User's password.
Read only	Enables connecting in "read-only" mode. In this way, you would be able to connect to the firewall without modification privileges using an account that ordinarily would provide these privileges. Read-only mode allows the user to refrain from using modification privileges when they are not necessary.

If you indicate a hostname in the **Firewall's IP address** field, this name has to be added to your DNS tables or in the file c:\winnt\system32drivers\etc\hosts on the administration host.

WARNING

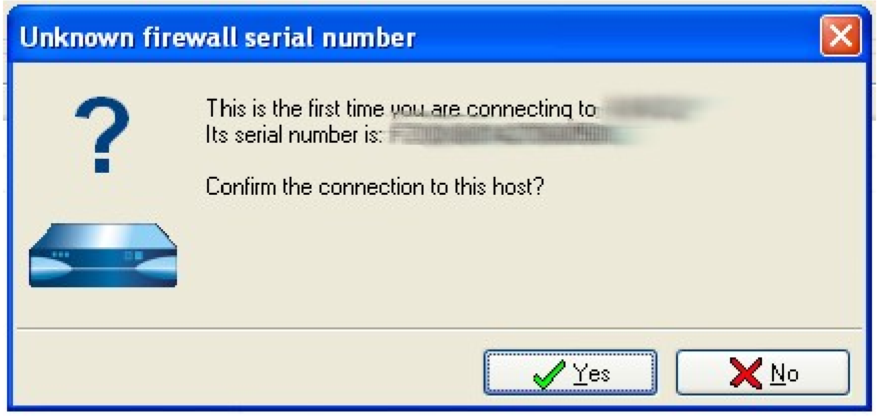
1) The NETASQ Firewall distinguishes between upper and lower case letters, both for the user name as well as for the password.
2) The password must contain at least 8 characters.

Once you have entered the necessary connection information, click on the **Connect** button to send it to the Firewall. Then go on to the next step.

Step 2: Validating the serial number of the Firewall contacted

REMARK
Step to be carried out only during the initial connection to the Firewall on a given administration workstation.

When you first connect to a firewall on an administatiobn station and the serial number of the Firewall contacted is not entered in the address book (see *Part 3/Chapter 2: Address book configuration*), NETASQ UNIFIED MANAGER will first prompt you to confirm the serial number of the Firewall contacted.



Unknown firewall serial number

This is the first time you are connecting to [redacted]
Its serial number is: [redacted]

Confirm the connection to this host?

Figure 23: Serial number unknown

The window that appears indicates the serial number that the Firewall (from which the administrator is attempting a connection) returned. If the serial number displayed is the same as the one on the label on the appliance, confirm this host's connection by clicking on **Yes**, and go on to the next step. Otherwise, the connection will be shut down.

<u>Necessity of the connection</u>

Administration sessions transmit sensitive information (e.g. administration passwords), and it would be a real disaster if such a session got hijacked. If an administrator password falls into the wrong hands, hackers may modify the appliance's security policy to their own benefit.

Every NETASQ UTM appliance is identified by a certificate, therefore confirming the serial number of the Firewall contected enables the prevention of "man-in-the-middle" attacks.

In such attacks, the hacker places himself between the administration station and the appliance, and can therefore intercept exchanges between the Firewall and the administrator. Although this type of attack is difficult to pull off, it remains an identified risk, and it would be wise to be protected from it nonetheless.

Step 3: Registering the "admin" password

REMARK
Step to be carried out only during the initial connection to the Firewall.

If this is your very first connection to the Firewall, the administration software (NETASQ UNIFIED MANAGER, NETASQ REAL-TIME MONITOR or NETASQ EVENT REPORTER) will ask you to define a password for the “admin” account.

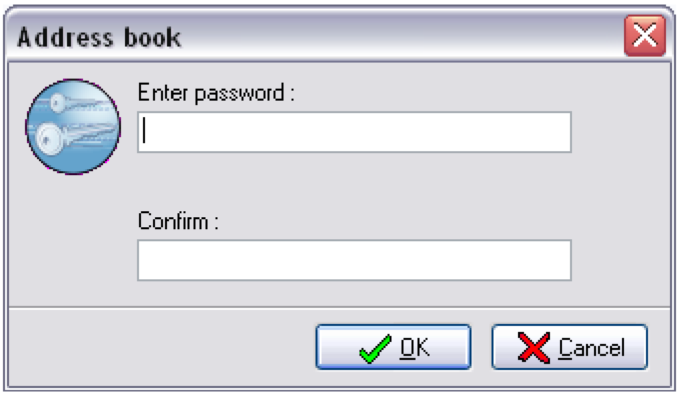


Figure 24: Password - Address book

Specify the password that will be associated with the “admin” account. Click on **OK** in order to end the connection process.

WARNING
If this message does not appear on your first connection, this means that someone else has connected to the product before you. Contact your NETASQ partner immediately.

Necessity of the connection

This step in the connection is a simple security mechanism that NETASQ has implemented in order to ensure the integrity of the Firewall up to its delivery. Consider the following:

- This step is essential for the first connection, therefore if this is your first connection and this step does not appear, this means that a third party has had access to the appliance before you and that modifications have been made to the configuration.
- The registration of the “admin” account password by the actual holder of the “admin” account ensures the full confidentiality of the particularly sensitive password.
- Connections cannot be made to the Firewall via the appliance’s administration console before the definition of a valid connection password. Before the initial connection, the “admin” connection password can only be defined via the graphical interface.

3.2.2.4. Administration restrictions

Administration privileges

Every administration command available on a firewall is associated with a consultation/modification privilege. This is seen in terms of access to certain menus in the suite of NETASQ administration software. When an administrator has a specific privilege, he has the right to perform the commands associated with this privilege. *(The list of privileges on the Firewall is indicated in Part 4: Objects*).

Multi-usage

You can have an unlimited number of sessions opened simultaneously with identical or different users. The only difficulty is that you can only have a single session with “general” modification privileges at any given moment (to avoid conflicting changes). This does not prevent other users from consulting the configuration: those with the MODIFY right will lose it temporarily if a user with the MODIFY right is already connected.

When an administrator has already connected with modification privileges; a message will inform you that modification privileges have already been assigned and you can choose whether to take over these rights or continue the session without modification rights.

> **Confirmation**
> Another user is already connected with modification rights. Do you wish to recover modification privileges (the user connected with modification rights will then be disconnected)?.

The procedure that allows identifying the user connected with modification rights is indicated in the section relating to the NETASQ REAL-TIME MONITOR.

3.2.2.5. The address book

The address book for NETASQ software is a central tool in the management of access to administration menus, as it can contain all the information necessary for connecting to a list of Firewalls, thereby simplifying the administrator’s task as he would no longer need to memorize all the different passwords.

In previous versions, the “Firewall Manager” and “Global Administration” modes referred to two separate applications, and it was therefore possible to obtain two address books – one in .dat format for Manager and the other in .gap format for Global Administration.

These two applications have been merged, so the address book can be saved in the .dat format in Manager mode (export). However, the address book used by the applications in the Administration Suite will be stored in .gap format only.

This file format is more extendable, as it contains not only firewalls, but also servers and information relating to topologies.

Importing the address book in this way into a Global Administration project means that when Manager is executed for the first time, the user will enter the password for the address book. A project containing the list of firewalls in the address book will then be created automatically. The user will also be prompted to save the project.

The address book used for NETASQ UNIFIED MANAGER, NETASQ REALTIME MONITOR and NETASQ EVENT REPORTER is located in C:\Documents and Settings\<USERNAME>\Application Data\Netasq\AS\8.0.

As for projects in G.A. mode, the address book can be stored anywhere.

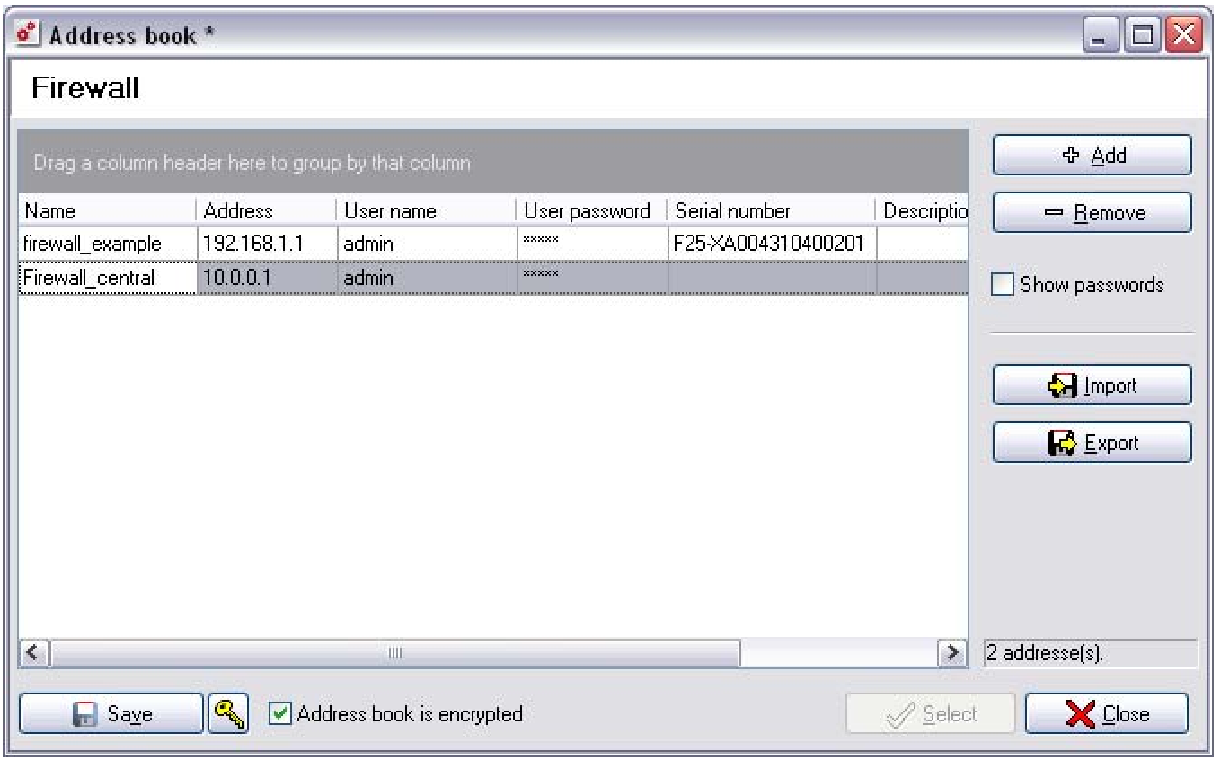
For project backup files (.gap extension) created in an ealier version, the address book will be automatically converted to the new format by backing up in the new version of NETASQ UNIFIED MANAGER (Global Administration mode).

Configuring the address book

To access the configuration of the address book:

- From the menu **`File\Address book`**…

In this address book, the Firewalls you wish to connect to can be defined. For each Firewall, indicate a name of your choice, which does not have to correspond to the Firewall's name, an IP address, a password and serial number.



Name	Address	User name	User password	Serial number	Descriptio
firewall_example	192.168.1.1	admin	*****	F25-XA004310400201	
Firewall_central	10.0.0.1	admin	*****		

□ Show passwords

2 addresse(s).

☑ Address book is encrypted

Figure 25: List of firewalls - Address book

WARNING
When defining a serial number for a firewall, this serial number will be added to the list of known serial numbers the first time you connect to this firewall using the address book. A confirmation message will not appear (step 2 of the connection process).

Show passwords

Check the option **Show passwords** to check that the passwords used for each firewall registered in the address book (the passwords will be displayed in plaintext).

Importing older address book

To retrieve an address book in an older version, you can import it in a file in **.dat** format.

Depending on the mode, the import procedure varies:

- In "Manager" mode, go to the menu **`File\Address book`** then click on **Import.**
- In "Global Administration" mode, go to the menu **`File`** then select **`Import the address book…`**

The data import file must follow the format below:

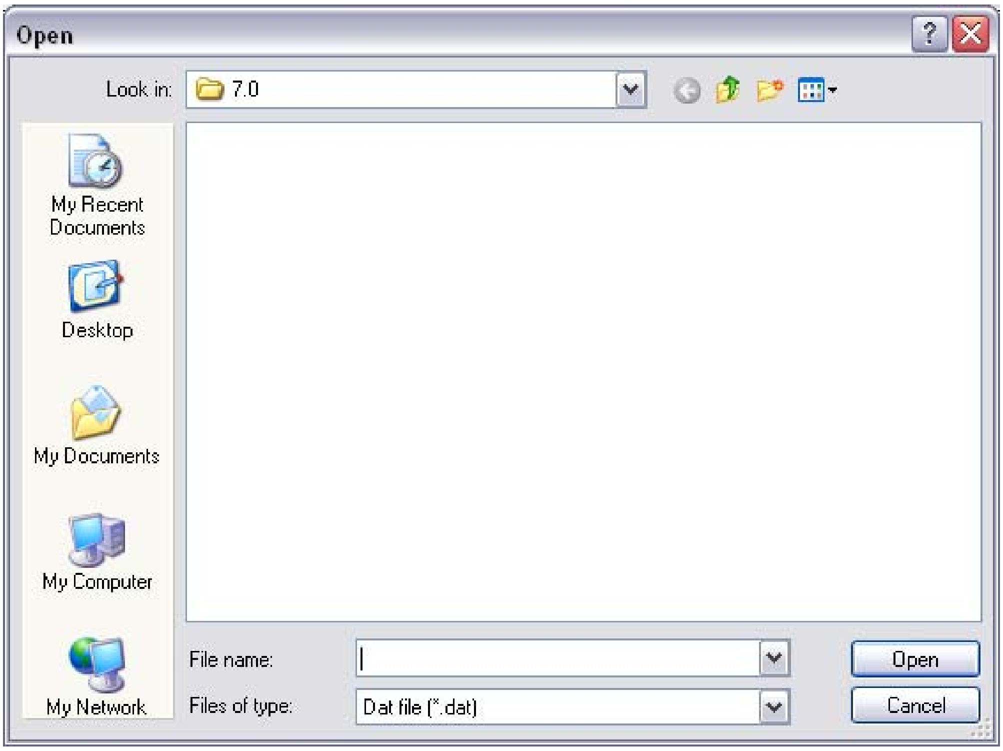
```
BOOK]
Copyright=# Firewall Address Book (c)2001 NETASQ
AddressNumber=1

[1]
Name=Firewall_Central
Comment=Head office
Type=Firewall
Address=192.168.0.1
 User=admin
Password=adminadmin
Serial=U70XXA0Z0899020
```

Or

- **Copyright**: Mandatory, with a value of "# Firewall Address Book (c)2001 NETASQ"
- **AddressNumber**: number of entries in the address book
- **[x]:** separates each line, x representing the number of the line in the address book
- **Name**: name given to the Firewall on the list in the address book
- **Comment**: comment
- **Type**: the type has to be "Firewall"
- **Address**: address for connecting to the Firewall
- **User:** administrator's login
- **Password**: administrator's password
- **Serial**: serial number of the Firewall

The following is the procedure for importing an existing address book:

1 Click on **Import from "Firewall Manager" mode**. The following window will open:



File name:

Files of type: Dat file (*.dat)

Figure 26: Importing: Selecting a file

2 Select the file to be imported.

REMARK
The file to be imported has to be in **.dat** format.

3 Click on **Open**.

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

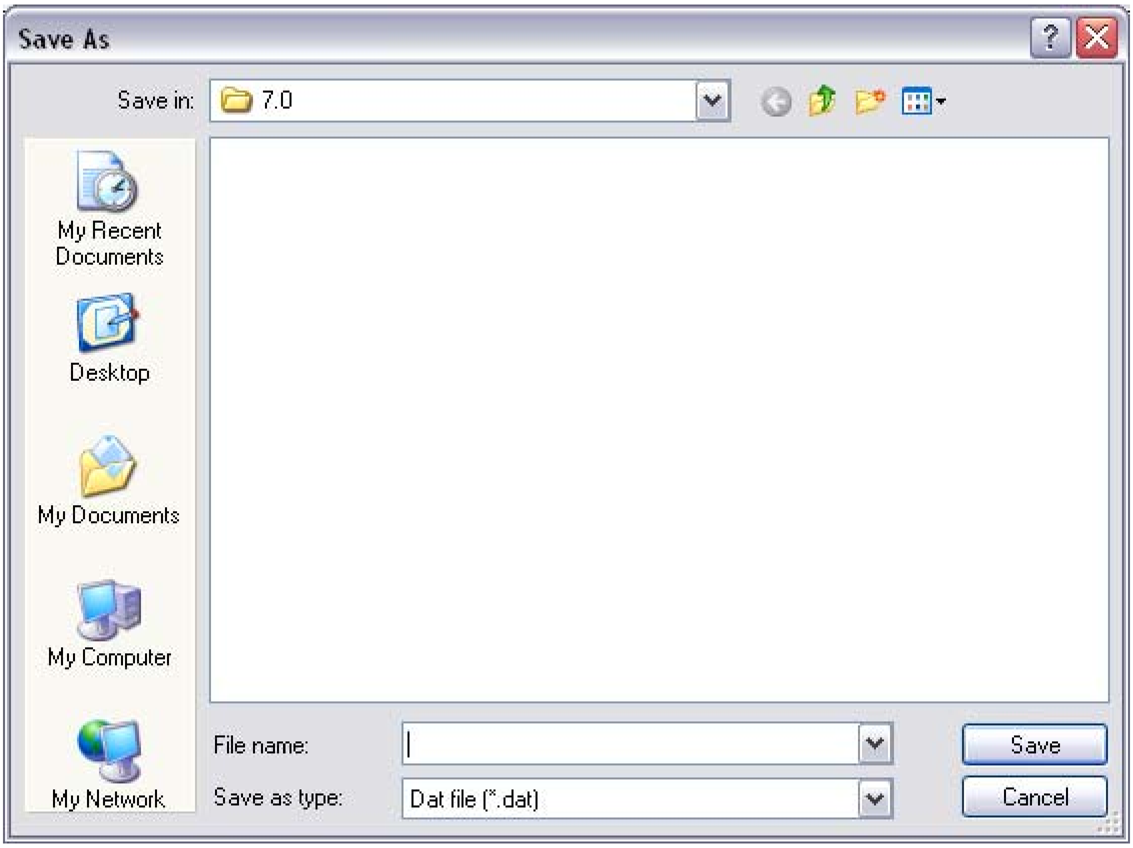
Exporting the address book

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

1 Click on **Export from "Firewall Manager" mode** in the configuration window of the address book.
2 The following message will appear:

"Encrypt the address book? (highly recommended)"

3 If you click on **Yes**, you will be asked to enter the password for the address book before the registration window opens:



File name:

Save as type: Dat file (*.dat)

Figure 27: Selecting a file to export

REMARK
The file to be exported has to be in **.dat** format.

4 Click on **Save**.

Address book is encrypted

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

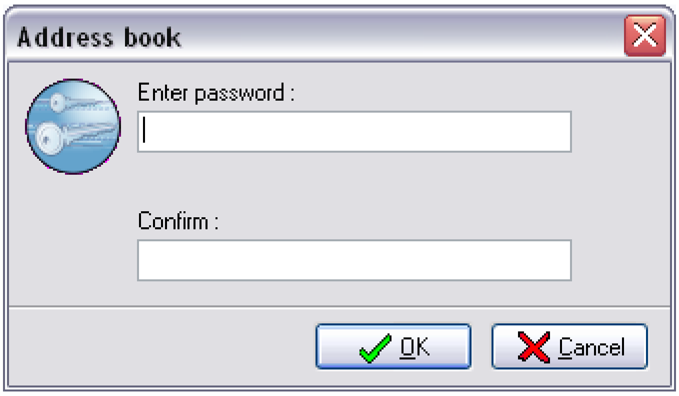


Figure 28: Password - address book

Save

Before closing the address book, new or modified data has to be saved, otherwise changes wil be lost. Click on **Save** button to save changes to the address book.

REMARKS
The **Address** and **Username** parameters entered in the connection dialog box are saved in the registry database of your administration PC.

For obvious security reasons the **Password** parameter is not saved.

Address book files on the administration host

On the administration host, address book files are located in the installation directory of the application:

- **AddrBook.dat**: this file contains the address book of the Administration Suite. If it has been encrypted, the information it contains cannot be read.

3.2.3. Disconnection

The procedure for disconnecting from a firewall is as follows:

1 Select **File\ Disconnect** from the configuration interface menu or click on the **Disconnect** button found in the menu directory.

2 You will be returned to the connection screen.

Depending on the options defined by the user, a confirmation will or will not be requested on disconnection. Canceling will return you to the main screen, with no consequences on program execution.

Disconnecting will return you to the main screen, but the LED (at bottom left) has become: ●.

3.2.4. Boot partition

3.2.4.1. Introduction

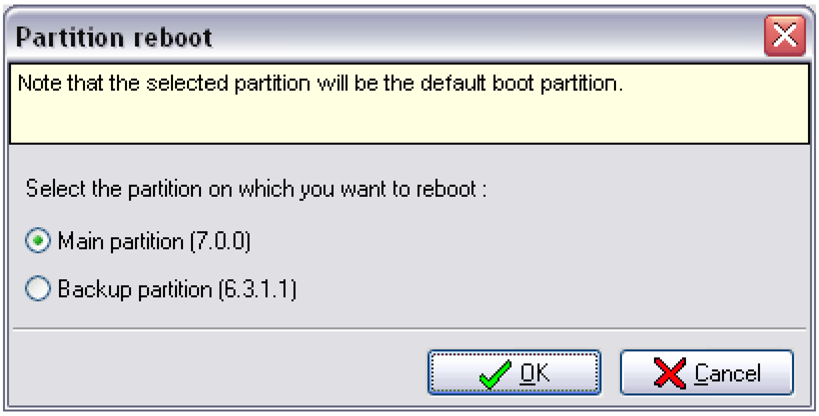
NETASQ UTM appliances allow backing up their main systems on a partition. Thus, if the main system gets corrupted, or an irreversible error is made in the configuration, the NETASQ product can be rebooted on this backup partition, which in comparison, is "clean".

There are two ways to reboot a NETASQ UTM appliance on its backup partition. The first method consists of connecting to the appliance in console mode (via serial link) and is not expanded upon in this section.

As for the second method, the menu **Maintenance\Boot partition** in "Firewall Manager" mode allows defining the UTM appliance's default boot partition. Therefore, remotely, and without connecting in console mode (via serial link), the appliance can be rebooted on its backup partition automatically and systematically.

3.2.4.2. Configuration

➲ Go to the menu **Maintenance\Boot partition.** The configuration screen on the boot partition will appear:


Partition reboot

Note that the selected partition will be the default boot partition.

Select the partition on which you want to reboot :

● Main partition (7.0.0)

○ Backup partition (6.3.1.1)

Figure 29: Rebooting on the partition

This screen indicates the two partitions detected in the appliance's hard disk and the version available on this partition. To define the appliance's default reboot partition, select one of the proposed partitions and click on **OK** to confirm the changes.

3.2.5. Quitting the application

When you close the application, a dialog box will ask you to confirm the action (depending on the options cofigured in the menu `Options\Preferences\Behavior`.)

To exit the application, go to the menu **File\Quit.** The following message will appear:

"Exit this application?"

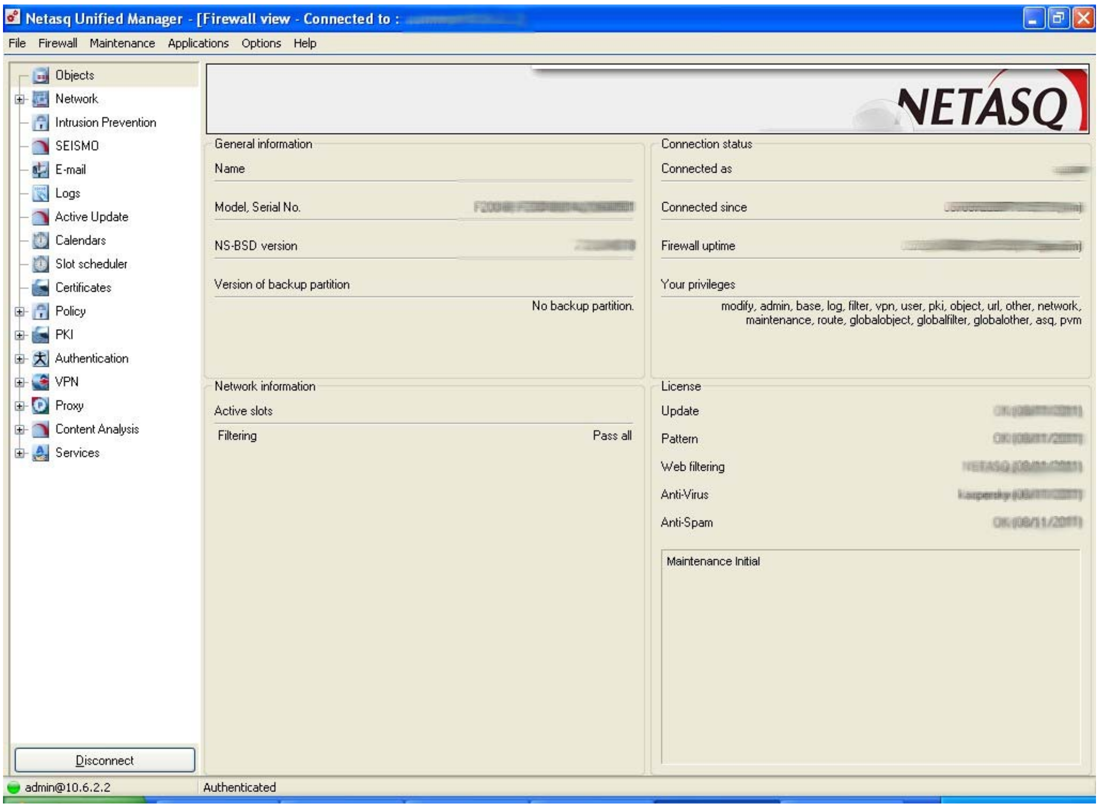
- Canceling the action will bring you back to the main screen, with no effect on the execution of the program.
- Confirming the action will exit the application.

This dialog box is also displayed when you exit the application by clicking on the ☒ at the top right corner of the window.

CHAPTER 3: PRESENTATION OF THE INTERFACE

3.3.1. Main window

Once the Firewall is connected the main window is displayed: The menus which are not accessible for the session will be disabled.



General information

Name

Model, Serial No. [redacted]

NS-BSD version [redacted]

Version of backup partition: No backup partition.

Connection status

Connected as [redacted]

Connected since [redacted]

Firewall uptime [redacted]

Your privileges: modify, admin, base, log, filter, vpn, user, pki, object, url, other, network, maintenance, route, globalobject, globalfilter, globalother, asq, pvm

Network information

Active slots

Filtering: Pass all

License

Update [redacted]

Pattern [redacted]

Web filtering [redacted]

Anti-Virus [redacted]

Anti-Spam [redacted]

Maintenance Initial

admin@10.6.2.2 Authenticated

Figure 30: Main window - NETASQ UNIFIED MANAGER

The main window consists of four separate sections:

3.3.1.1. General information

- Firewall's name
- Appliance model and serial number
- Firewall's software version (on the main partition)
- Backup partition's software version

3.3.1.2. Network Information

- Active slots (filter, translation, VPN, etc)

> **Example**
> Indicates the active filter policy.

3.3.1.3. Connection status

- The account used for the connection
- Time lapsed since connection to the Firewall, including date and time
- Duration of the Firewall's uptime, including date and time
- Privileges for the account used for the connection. *(Cf. Appendix A: Session and user privileges)*

3.3.1.4. Licenses

- Expiry date for the Update option
- Expiry date for the "Contextual Signatures" option
- Expiry date for the web filter option
- Expiry date for the Antivirus option
- Expiry date for the Antispam option

WARNING
Before any action is performed, check that the Firewall's software version indicated in the screen corresponds to the expected version. Another way of checking the product's version is explained in *Appendix H: Commands*.

3.3.2. Menu bar

The main window in "Firewall Manager" mode contains the following menu bar:

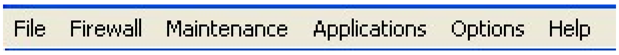


Figure 31:Menu bar

3.3.2.1. Explanation the menus

File	Disconnection from the NETASQ Firewall, edition of the Firewall's address book and quitting the application.
Firewall	License management, technical support, system configuration (date, time, language), security, high availability configuration, secure configuration, shutdown of alarm LEDs.
Maintenance	Backup, restoration, firmware update, reboot …
Applications	Quick links to the applications in the Administration Suite NETASQ REAL-TIME MONITOR and NETASQ EVENT REPORTER.
Options	Manages preferences for the application.
Aide	Access to help files, display of the "About" window indicating the graphical interface's version number, access to updates for NETASQ UNIFIED MANAGER.

3.3.3. Menu directory

The menu directory contains all the configuration menus for each feature on the Firewall. If a certain menu is grayed out, this means that the license or the user's rights do not enable this menu to be displayed or accessed.

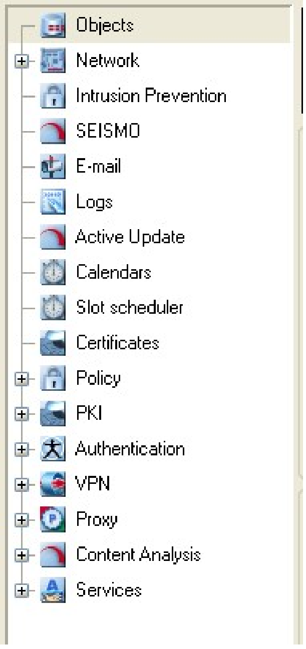


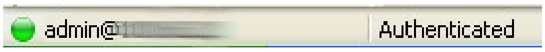
Figure 32: Menu directory

3.3.3.1. Locating the interface menus in the table of contents

Objects	Part 4: OBJECTS
Network	Part 5: NETWORK CONFIGURATION
Intrusion prevention	Part 6: INTRUSION PREVENTION (ASQ)
SEISMO	Part15: SEISMO
E-mail	Part 16: E-MAIL CONFIGURATION
Logs	Part 17: LOG MANAGMENT

Active update	Part 18: MAINTENANCE: Active Update
Calendars	Part 7/Chapter 3: Calendars
Slot scheduler	Part 7/Chapter 3: Programming slots
Certificates	Part 8: VPN
Policy	Part 7: POLICY
PKI	Part 13/Point 4: PKI
Authentication	Part 12: AUTHENTICATION
VPN	Part 8: VPN
Proxy	Part 9: PROXY CONFIGURATION
Content analysis	Part 10: CONTENT ANALYSIS
Services	Part 11: SERVICES

3.3.4. Status bar



admin@[redacted] Authenticated

Figure 33: Status bar

The status bar is at the bottom of the main window. It comprises three sections:

Status indicator (LED)	🟢 You are currently connected to NETASQ UNIFIED MANAGER. 🔴 You have been disconnected from NETASQ UNIFIED MANAGER.
User@IP	Name of connected user and Firewall's IP address
Text zone	Displays a description of the action associated with an icon, the result of an action or a description of an error which has occurred. **Example** "Authenticated"

CHAPTER 4: INTEGRATION

3.4.1. Integration

NETASQ Firewalls are very easy to integrate, as you will see from the following architecture examples.

3.4.1.1. Installing the Firewall in an existing architecture

The network which your NETASQ Firewall will protect is already connected to Internet via a router, which you do not manage. All the IP addresses on the internal network are already configured.

NETASQ Solution: insert the NETASQ Firewall between the router and the LAN, in transparent mode (same IP address on all interfaces). You need not change either the router's internal address or the IP addresses of your internal terminals.

3.4.1.2. Installing the Firewall in an architecture based on a VLAN segmentation

You can place the NETASQ Firewall at the end of an Ethernet VLAN. The Firewall can manage the filtering and routing between VLANs.

3.4.1.3. Installing the Firewall behind a modem

You would like to install a NETASQ Firewall behind an Internet access modem (ADSL, ISDN, dial-up or cable modem) but you have no router.

NETASQ Solution: The NETASQ Firewall can manage connections with ADSL (PPTP and PPPoE), ISDN, dialup and cable modems, so you no longer need a router – the Firewall replaces it without difficulty.

3.4.1.4. Migration of a server from the LAN to the DMZ

You have a server previously reserved for internal use and you want to make it available for Internet. Initially it was in your internal network and you want to move it to the DMZ in order to isolate it. This server has a private IP address which is part of the class of addresses on the internal network and it is difficult to change it, as the applications on internal PCs are configured to access the server by this address.

NETASQ Solution: The Firewall can be configured in hybrid mode. The internal network interfaces and the DMZ will have the same IP address, so the PCs connected to these two interfaces will be regarded as part of the same network. However, the traffic between the internal network and the DMZ will be filtered. You can therefore move the server to the DMZ without changing its IP address.

> **REMARK**
> The Firewall’s external interface can have an IP address which belongs to a different addressing range (public or private).

PART 4: OBJECTS

CHAPTER 1. INTRODUCTION

4.1.1. For this chapter, you will need to have completed these steps

- Part 2: Installation, pre-configuration, integration
- Part 5: Network configuration

4.1.2. For this chapter, you will need to know

- The hosts and networks to which you wish to assign particular rights
- Information regarding each user of your internal network (name, surname)
- Protocols and IP services that you will use

4.1.3. Purpose of this chapter

This chapter allows you to define the objects you will use to configure filtering and network address translation rules. At this point, you will be able to match the host name, a host group, a network, a network group with its IP address. You will also be able to match a service name with its protocol and its port number. In addition, you can create service groups if certain regulations govern a number of services, this making it easier to edit rules. You will see how to define users account for authentication. Information regarding these accounts is stored in an internal LDAP database or in an external database or with limited information on a RADIUS server or Active Directory database.

4.1.4. Accessing this chapter

➲ Go to the **`Objects`** menu in the menu directory.

To carry out any changes, you must first log in with modification rights.

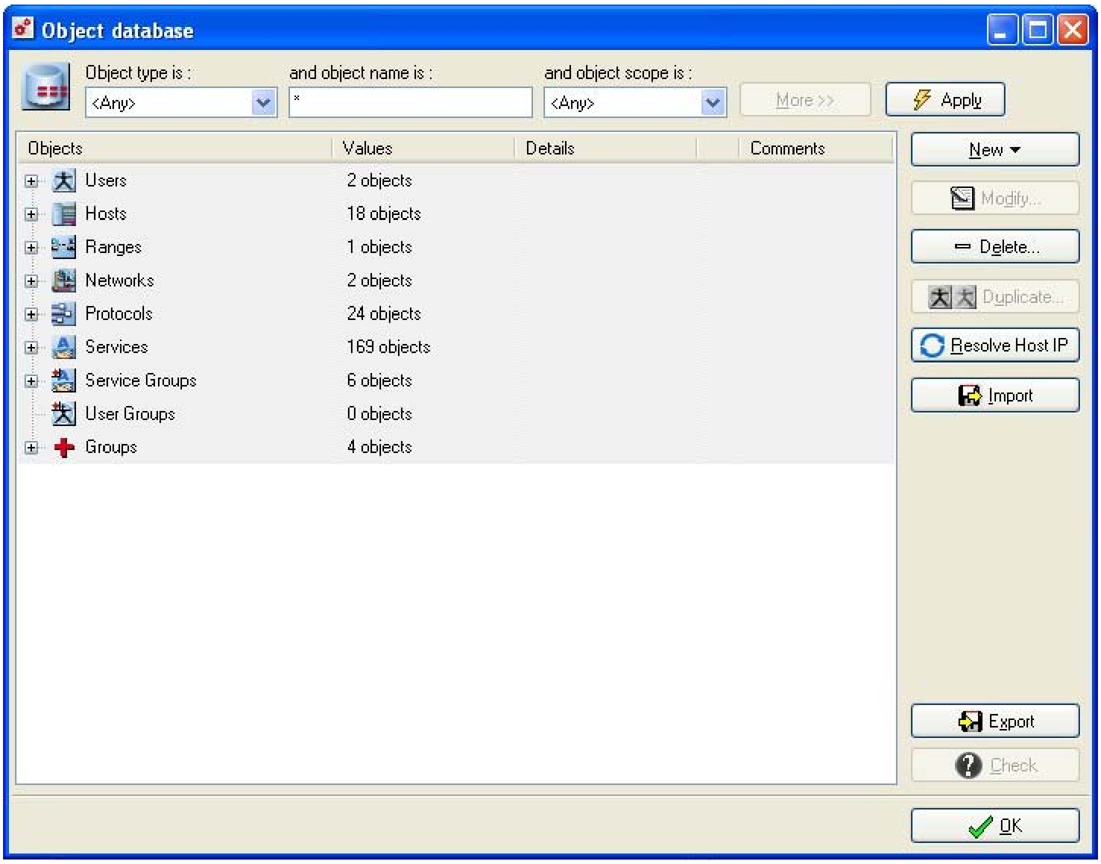
NOTE
Before carrying out any major changes to the NETASQ UTM appliance, you are advised to make a backup so that in case of any mistakes, you can return to the previous step. *(See Part 18: Backup).*

CHAPTER 2. PRESENTATION

The object database is useful in most of the configuration modules in NETASQ UNIFIED MANAGER. In general, it reappears in the other modules to allow creating, deleting or selecting hosts, users, address ranges, networks, protocols, services, object groups, etc.

Objects can be:

- Users (with logins and passwords for authentication)
- Hosts (matches an object name to an IP address)
- Address ranges
- Networks (network address and subnet mask)
- Protocols (matches a protocol name to its number)
- Services (name of service, port and protocole)
- Groups (hosts and/or networks, ranges, user groups, service groups)



Object type is : <Any>
and object name is : *
and object scope is : <Any>

Objects	Values	Details	Comments
Users	2 objects		
Hosts	18 objects		
Ranges	1 objects		
Networks	2 objects		
Protocols	24 objects		
Services	169 objects		
Service Groups	6 objects		
User Groups	0 objects		
Groups	4 objects		

Figure 34: Object database

The object definition window is divided in three parts:

- A sort and select zone in the top part of the window
- An action bar on the right side of the window
- A grid for object definition

4.2.1. Sort and select zone

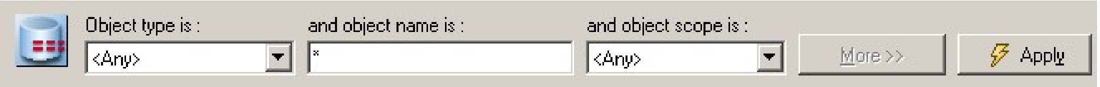


Figure 35: Sort and select zone

The sort and select zone located in the top part of the window is displayed differently according to the object type selected. When this window is opened, all objects are listed in the object definition grid but when an object is selected from the drop-down menu at the top left corner, the sort and select zone appears.

This sort and select zone enables a quick search for an object among the list of objects configured on your Firewall.

4.2.1.1. Sort and selection buttons

This zone contains several action buttons which would allow you to validate and display the results of your search.

Object type is	Selects the type of object displayed from the following: “Any”, “Users”, “Hosts”, “Ranges”, “Networks”, “Protocols”, “Services”, “Groups”, “User groups”, “Service groups”.
And object name is	Searches for objects containing the character string indicated.
And object scope is	There are 3 possible options: "All", "Local" and "Global".
More/ Less	Shows or hides the sort and select zone.
Apply	Applies the search.

4.2.1.2. Action bar

The actions enabled by the action bar are indicated in the following table:

WARNING

1) For object imports, there are no protection mechanisms to ensure the integrity of the imported configuration (the imported file may contain deliberately wrong information). The administrator is therefore responsible for validating the coherence of the whole object database before sending it to the Firewall.
2) Also, making backups of the object databse in this way is not recommended. Instead, use the available configuration backup functions (which provide cryptographic mechanisms).

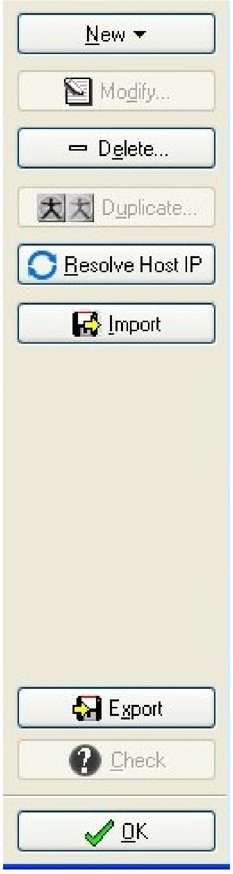
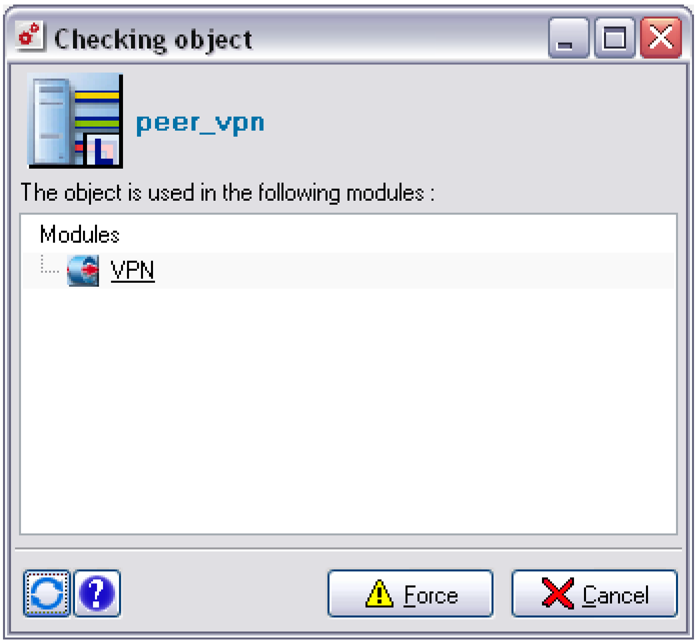


Figure 36: Action bar

New	Select the object type you wish to create and the corresponding wizard will appear.
Modify…	Modifies the selected object.
Delete…	Deletes the selected object.
Duplicate…	Duplicates the selected object
Resolve Host IP	Resolves the IP addresses of "manual" hosts.
Import	Imports a list of objects
Export	EXports a list of objects
Check	Tests the use of a selected object. (*See* *Part 4: Checking object*).
OK	Closes the object configuration window. Modifications to objects are automatically applied.

4.2.1.3. References to the object

When the **Check** button is clicked or when an object (except for user objects) is deleted from the object database, an object reference screen appears. This window indicates the different modules that use the selected object in their configurations.



Checking object

peer_vpn

The object is used in the following modules :

Modules
- VPN

Figure 37: References to the object

The object reference screen shows the name of the object and indicates in the form of links, the different modules in which the object is used. By clicking on the module listed in the reference screen, the associated configuration menu appears, making it possible to view and/or modify the configuration before deleting the object.

The object reference screen has an action bar containing four action buttons:

⟳	Refreshes the display on the object reference screen.

?	Displays the Firewall’s exact text return that indicates where the object is used in each module.
	
	Examples
	module=Filter slot=10 line=1
	module=Filter slot=10 line=2
	module=Route section=Default

✓ OK	Closes the object reference screen by accepting changes.
⚠ Forcer	The **OK** button in the object reference screen becomes **Force** when an object is being deleted. This action deletes the selected object even if it is used in the modules mentioned.
✗ Cancel	Closes the object reference screen without accepting changes.

WARNING

Changes made through the window that references the object, in the modules that use the analyzed object, cannot be cancelled by clicking on the **Cancel** button in the window.

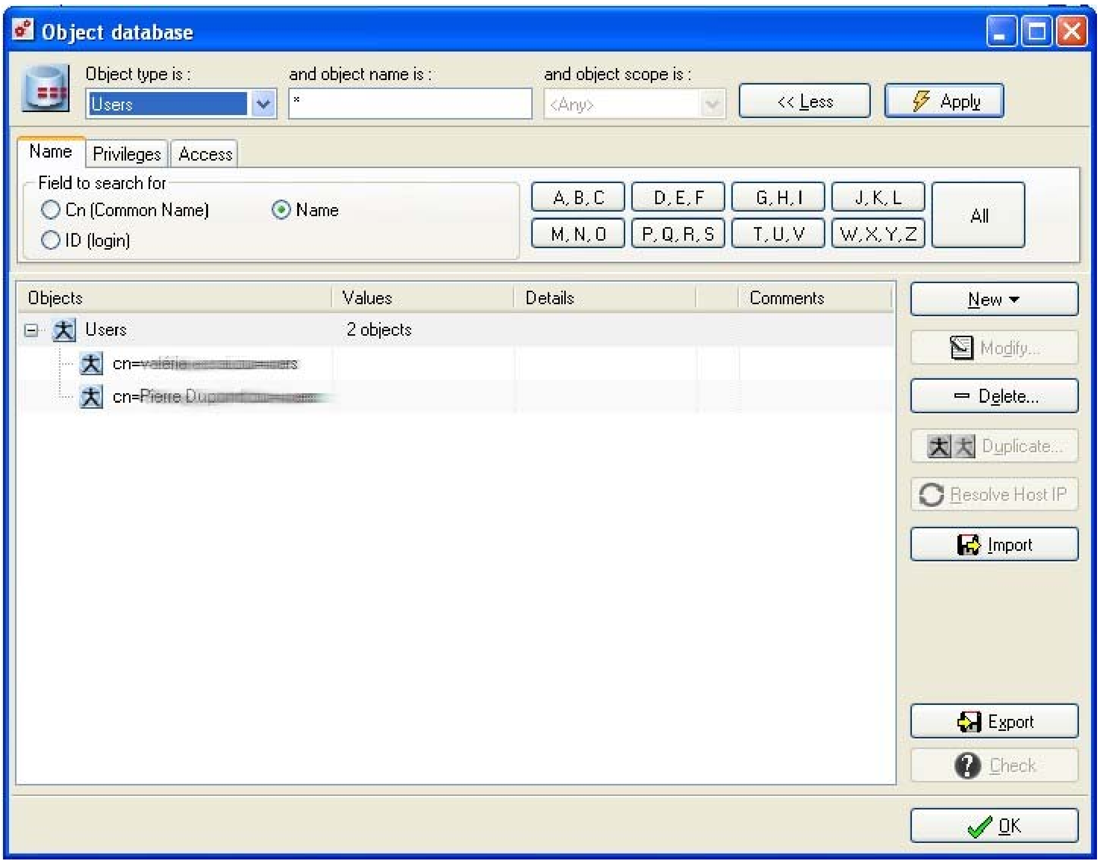
4.2.3. Remarks

Objects adopt the color of the interface they are related to. All the modifications regarding users (LDAP) are applied immediately.

If you modify an object that is used in the configuration of the UTM appliance, the changes will automatically be applied and the slots that use this object will automatically be reactivated.

> **WARNING**
> Reactivating a NAT slot may cause active connections to be lost.

CHAPTER 3. USERS



Object type is : Users
and object name is : *
and object scope is : <Any>

Field to search for
○ Cn (Common Name) ● Name
○ ID (login)

Objects	Values	Details	Comments
Users	2 objects		
cn=valérie [redacted]			
cn=Pierre Dupo [redacted]			

Figure 38: Object database - Access

User accounts have to be created in the firewall for the user authentication system. These accounts contain all the data relating to these users:

- Last name
- First name
- Connection login
- Password
- E-mail (optional)
- Telephone number (optional)
- Description (optional)

- User's authentication method
- VPN access rights and administration rights
- Pre-shared key for VPN
- PPTP password
- x509Certificats

4.3.1. Creating a user

4.3.1.1. User creation wizard

Users are created (**New\User** button) via a Wizard: This one-step wizard will ask you to enter the following information:

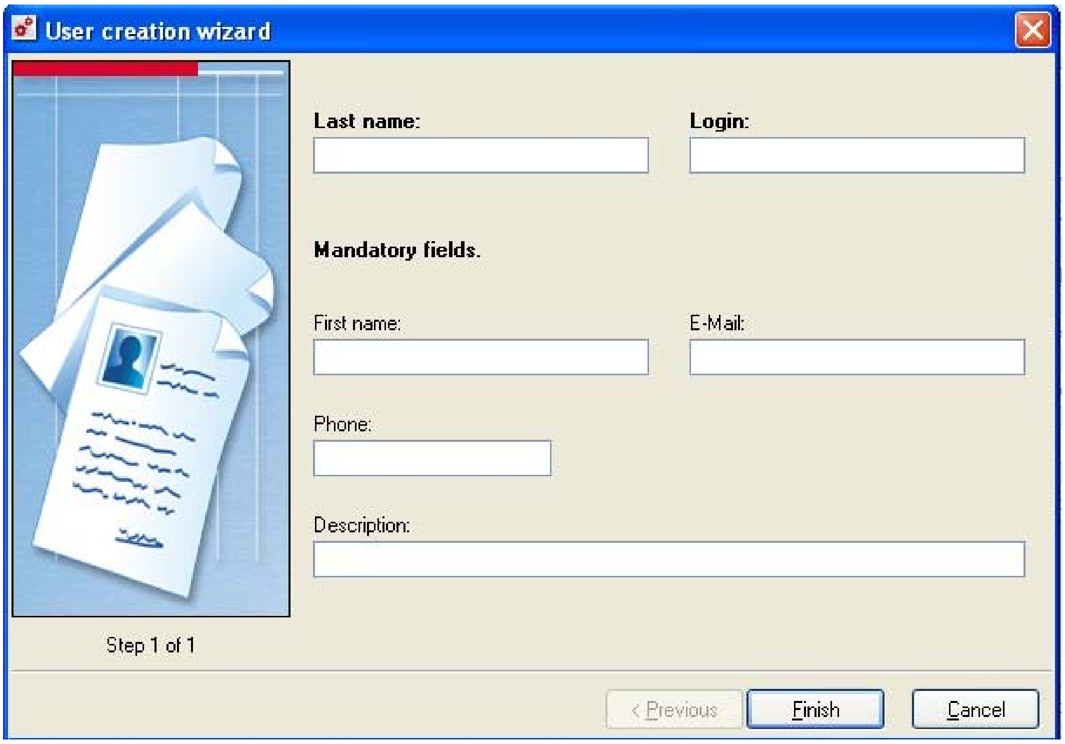


Figure 39: User creation wizard

- Mandatory fields (indicated in bold): Name and identifier (login used for user authentication).
- Optional fields: First name, e-mail address, telephone number (short string that can be modified), description (short string that can be modified).

> **WARNING**
> If you wish to generate an x509 certificate for this user you are obliged to enter his e-mail address. This information will be used in the certificate.

The e-mail address is also necessary if the user wishes to access the Firewall in VPN with an IPSEC remote client.

Once you have finished the configuration with the Wizard or when you wish to change a user's records, (select the user in the objects grid, then click on the **Modify** button); the information regarding the user configuration will be displayed in a window containing five tabs.

REMARK

All modifications concerning users are immediately applied.

4.3.1.2. User tab

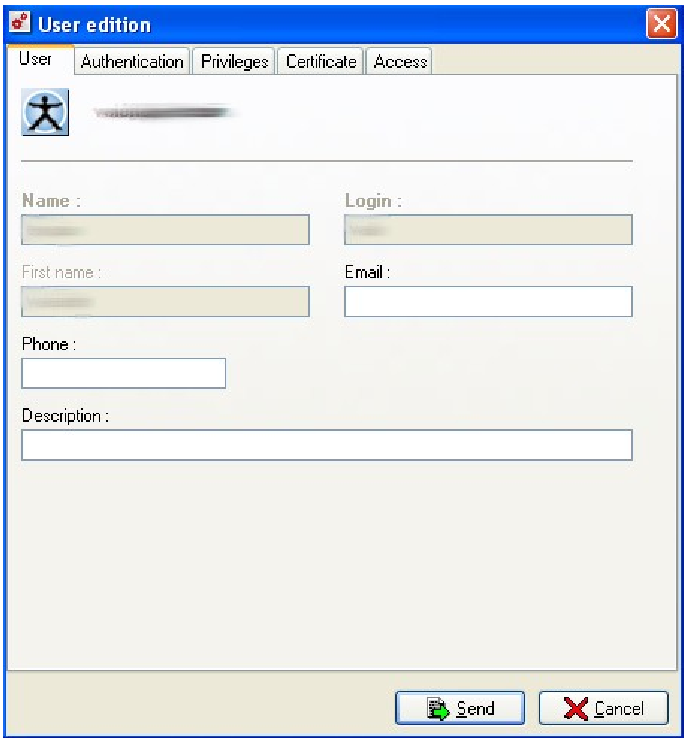
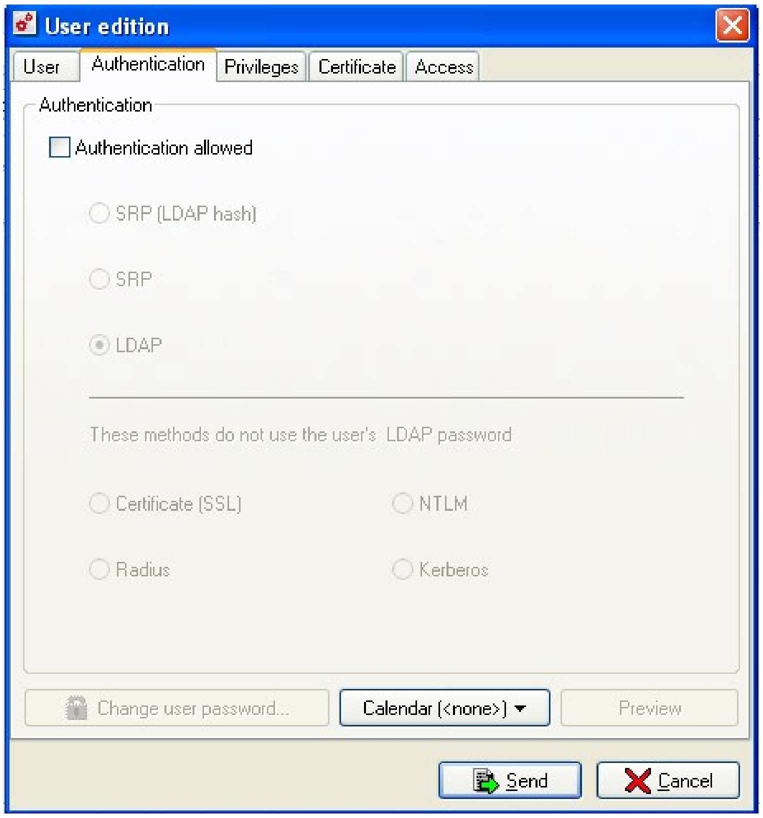


Figure 40: Editing a user – User tab

This option allows you to change the basic data on the user. Only the folliowing can be modified:

- E-mail address (optional)
- Telephone number (optional)
- Description (optional)

4.3.1.3. Authentication tab



☐ Authentication allowed

○ SRP (LDAP hash)

○ SRP

● LDAP

These methods do not use the user's LDAP password

○ Certificate (SSL) ○ NTLM

○ Radius ○ Kerberos

Figure 41: Editing a user – Authentication

This tab displays the configuration elements for authentication. Selecting the option "**Authentication allowed**" allows accessing the options in this window. This option enables determining whether the user has been allowed to authenticate on the firewall.

If so, the user will use one of the following methods:

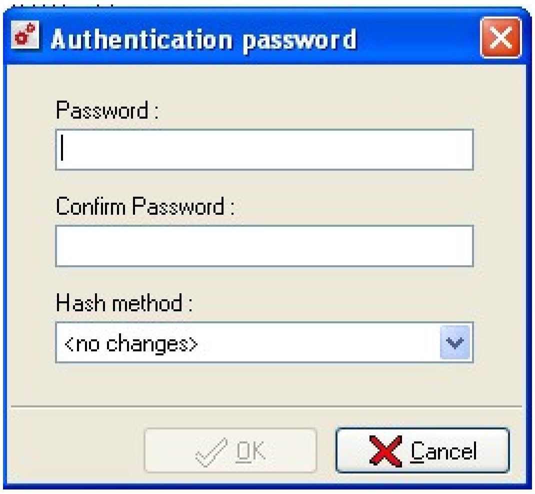
- **SRP (LDAP hash)**, a special use of the SRP method. This method requires no login fields or passwords stored in the LDAP file. The logins and passwords used are those on the LDAP base.

> **WARNING**
> This method is a bit less secure than native SRP (during access to the LDAP database, the native SRP password is more resistant to a brute force attack than the SRP Hash password. However, exchanges over the network are equally secure for both methods) but allows reusing the classic LDAP password (userpassword field).

- **SRP**, use of the native secured SRP to calculate the password. This method adds fields to the user's LDAP file, with his login and password.
- **LDAP**: the password is transmitted in SSL. (HTTPS). (This method is not recommended).

Change the user password by clicking on the **Change user password** button. This password will be used for authentication through the Firewall and if the user wishes to access the Firewall to read or change the configuration.

The following window will appear when you click on this button:



Authentication password

Password :

Confirm Password :

Hash method : <no changes>

Figure 42: Authentication password

The “hash method” field allows you to change the password’s hash method (*Cf.* *Part 12: Authentication*).

The following options are offered:

- No modification: allows you to keep the method already in use
- NONE
- MD5
- SMD5
- SHA
- SSHA
- CRYPT

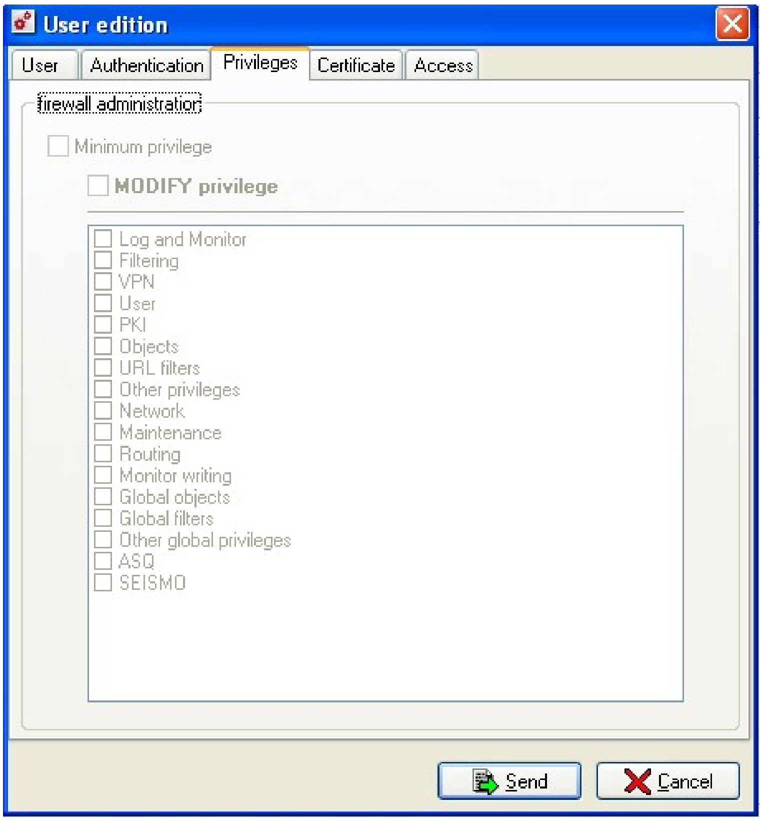
Methods without LDAP password

- **Certificate (SSL)**: uses the user’s certificate stored in the LDAP database and installed on the client workstation
- **RADIUS**: uses an authentication via a RADIUS server (*Cf. Part 12: Authentication)*
- **NTLM**: uses an authentication via an NTLM server (*Cf. Part 12: Authentication*)
- **KERBEROS**: uses an authentication via a Kerberos server (*Cf. Part 12: Authentication*)

Calendar

The button **Calendar (<None>)** enables specifying the authorized authentication periods for the user. In this calendar, if authentication is not allowed, the user cannot authenticate. (*Cf. Part 7/Chapter 3: Slot Scheduler).*

4.3.1.4. Privileges tab



firewall administration

□ Minimum privilege

□ MODIFY privilege

□ Log and Monitor
□ Filtering
□ VPN
□ User
□ PKI
□ Objects
□ URL filters
□ Other privileges
□ Network
□ Maintenance
□ Routing
□ Monitor writing
□ Global objects
□ Global filters
□ Other global privileges
□ ASQ
□ SEISMO

Figure 43: Editing a user – Privileges tab

This section enables you to specify the privileges to read and change the Firewall configuration.

REMARK
To assign privileges to a user, you must first select "Authentication allowed" in the **Authentication** tab.

List of privileges:

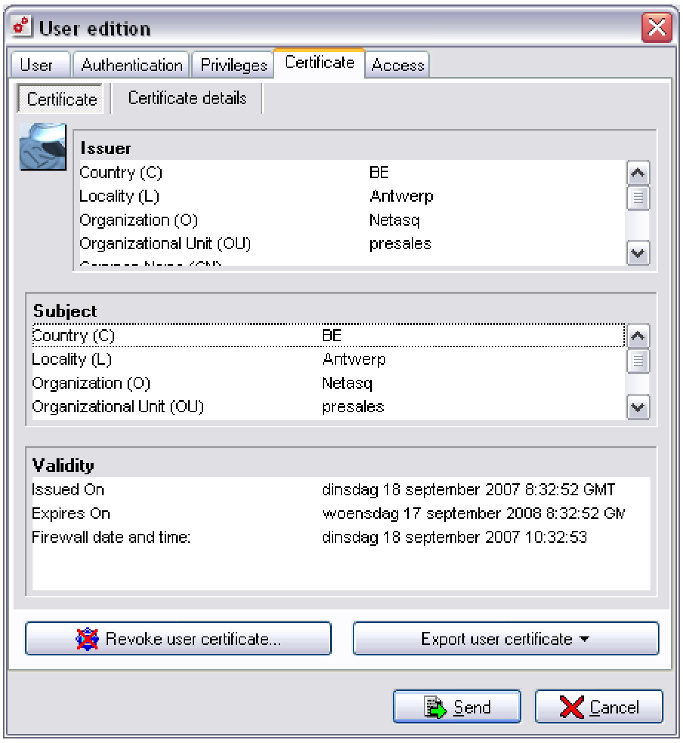
- BASE privileges, which is necessary to enable the user to connect to the Firewall (reading privileges).
- MODIFY privileges: which allows modifying the firewall's configuration.

After you have determined the reading/modification privileges, you only need to select the other privileges:

- **Log and Monitor**: log consultation privileges
- **Filtering**: consultation privileges on filter rules
- **VPN**: consultation privileges on VPN configurations
- **User**: consultation privileges on user information
- **PKI**: consultation privileges on PKI information
- **Objects**: consultation privileges on objects
- **URL filters**: consultation privileges on URL filtering
- **Other privileges**
- **Network**: modification privileges on network configuration (interfaces, bridges, dialups, VLANs and dynamic DNS configuration)

- **Maintenance**: privilege to perform maintenance operations (backups, restorations, updates, Firewall shutdown and reboot, antivirus update, modification of antivirus update frequency and RAID-related actions in the monitor)
- **Routing**: privilege to edit routing on Firewalls (default route, static routes and trusted networks)
- **Monitor writing**: privilege to perform certain operations which would require modification privileges, but without monopolizing "general" modification privileges
- **Global objects, Global filters, other global privileges**: privileges to access global configuration
- **ASQ**: privilege to consult ASQ configuration
- **SEISMO**: privilege to consult and/or modify vulnerabilities

4.3.1.5. Certificate tab



Issuer

Country (C)	BE
Locality (L)	Antwerp
Organization (O)	Netasq
Organizational Unit (OU)	presales

Subject

Country (C)	BE
Locality (L)	Antwerp
Organization (O)	Netasq
Organizational Unit (OU)	presales

Validity

Issued On	dinsdag 18 september 2007 8:32:52 GMT
Expires On	woensdag 17 september 2008 8:32:52 GM
Firewall date and time:	dinsdag 18 september 2007 10:32:53

Figure 44: Editing a user– Certificate tab

Generating a certificate

This option enables you to generate the user's x509 certificate.

This can be used in two cases – authentication via SSL and access to the Firewall in VPN with an IPSEC mobile client. It can also be used by other applications.

To create a certificate (you must first configure the internal PKI – see *Part 12: Authentication*) please refer to the following procedure.

1 Click on the button **Create a user certificate.** The following window will appear:

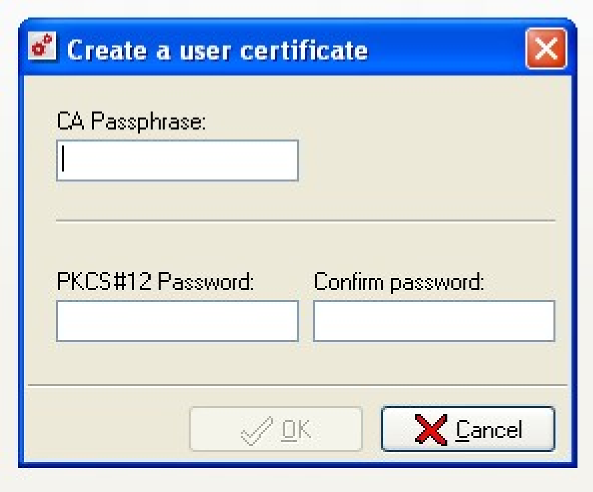
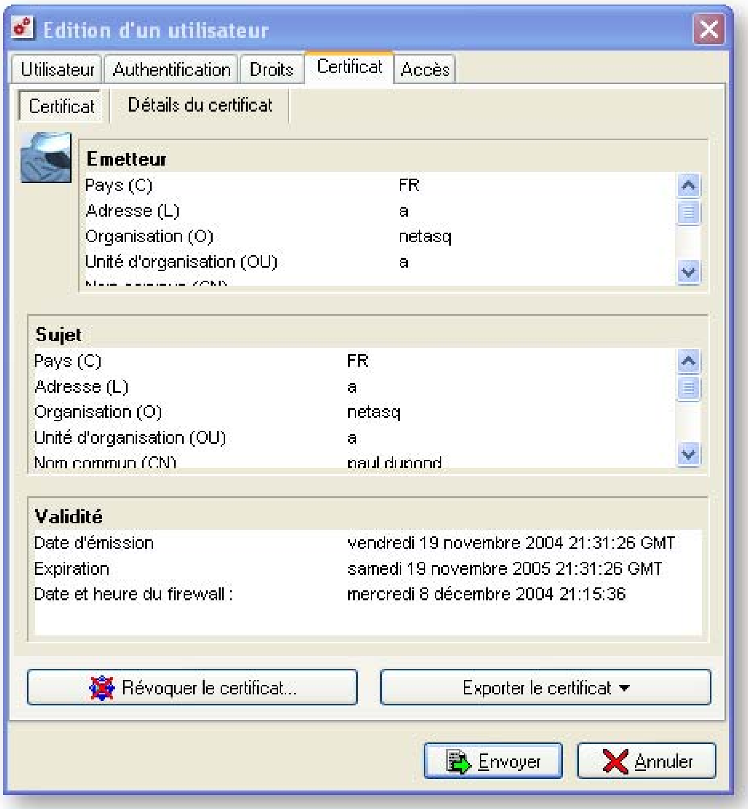


Figure 45: Creating a user certificate

2 Enter the password which you have allocated to the Firewall’s certification authority (CA).
3 Then specify the password chosen for the user’s PKC#12 container. This container can be exported to the user’s PC.

Once the user certificate is generated the contents are displayed.



Emetteur

Pays (C)	FR
Adresse (L)	a
Organisation (O)	netasq
Unité d'organisation (OU)	a

Sujet

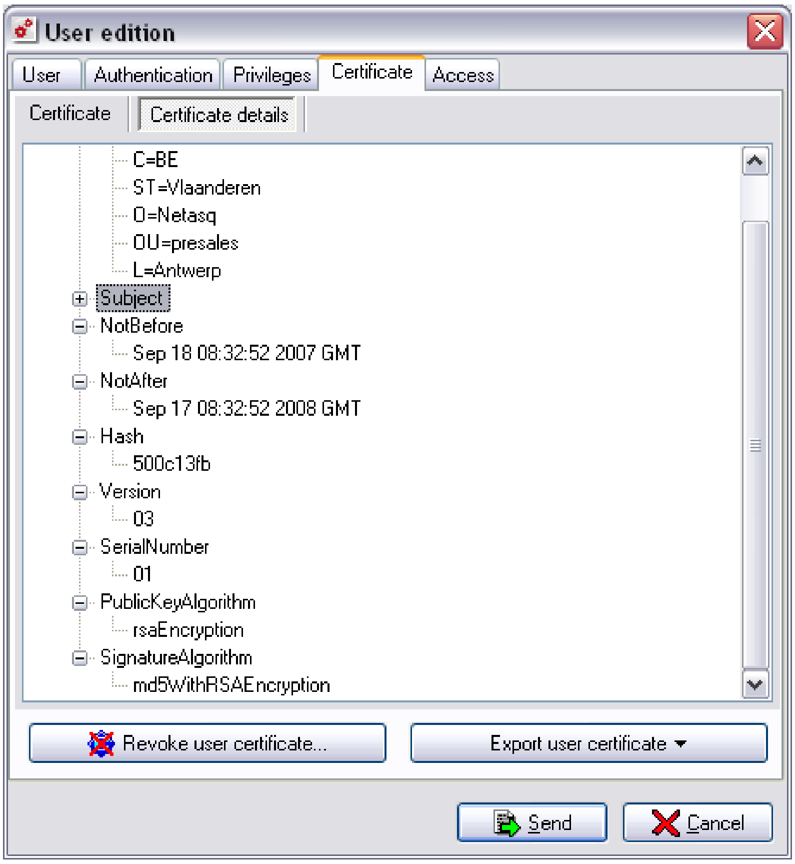
Pays (C)	FR
Adresse (L)	a
Organisation (O)	netasq
Unité d'organisation (OU)	a
Nom commun (CN)	paul dupond

Validité

Date d'émission	vendredi 19 novembre 2004 21:31:26 GMT
Expiration	samedi 19 novembre 2005 21:31:26 GMT
Date et heure du firewall :	mercredi 8 décembre 2004 21:15:36

Figure 46: Editing a user – Certificate tab

You can then visualize all the fields of the certificate (data relating to the certification authority integrated into the NETASQ Firewall, data regarding the user and the certificate’s term of validity).
You can see the contents of the certificate if you click on the **`Certificate details`** tab.



```
C=BE
ST=Vlaanderen
O=Netasq
OU=presales
L=Antwerp
Subject
NotBefore
    Sep 18 08:32:52 2007 GMT
NotAfter
    Sep 17 08:32:52 2008 GMT
Hash
    500c13fb
Version
    03
SerialNumber
    01
PublicKeyAlgorithm
    rsaEncryption
SignatureAlgorithm
    md5WithRSAEncryption
```

Figure 47: Editing a user – Details of the certificate

Revoking a certificate

A user's certificate can be revoked (cancelled) using the **Revoke the certificate…** button. In this case the user can no longer be authenticated on the Firewall (if the authentication method chosen is SSL) nor carry out VPNs (if the authentication method is based on certificates). He can no longer use the applications installed in the PKI (using the x509 certificates of the Firewall's PKI.

WARNING
You must regenerate the CRL (Certificate Revocation List) for the revocation to be effective. (See *Part 12: Authentication*). If you have other applications which use the Firewall's PKI certificates, you must redistribute this CRL to them. Certificates generated by the PKI contain a link to this CRL.

Exporting the certificate

You may save the certificate you have generated and install it on the user's PC.

It can be exported in the PKCS#12 format (recommended) or in .der format. The PKCS#12 container contains the private key and user certificate as well as the certification authority's certificate, whereas the .der format only contains the user certificate.

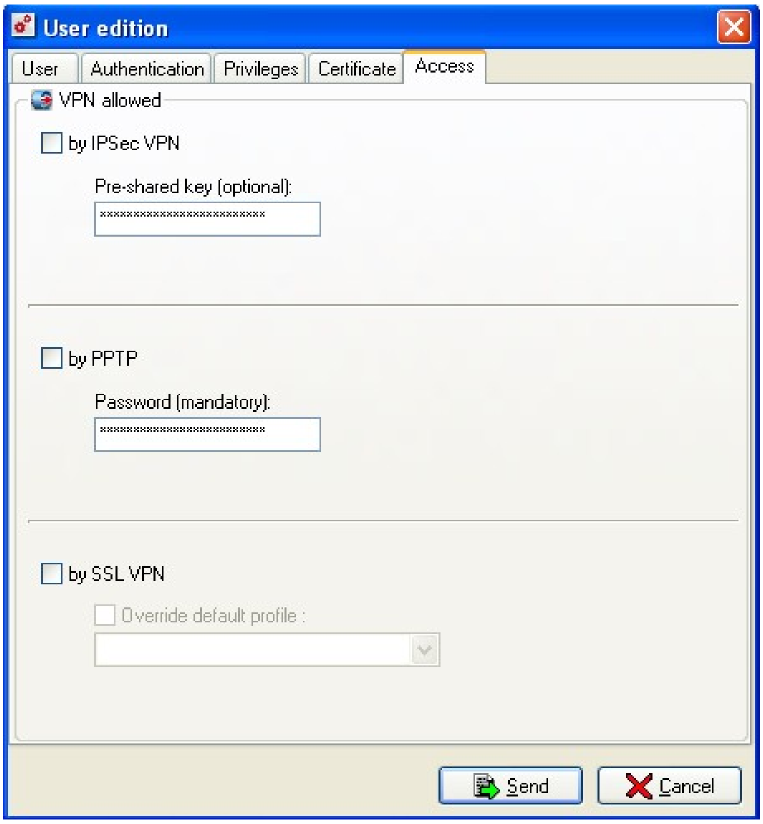
Installing a certificate in Windows

1 Copy the certificate or the PKCS#12 container locally on the user's PC.

2 Open the file. The installation of the certificate will begin.

3 You will be asked to enter the PKCS#12 container password defined during the creation of the certificate to end the installation of the certificate, which will then be added to the certificates which have already been installed on the user's PC.

4.3.1.6. VPN Access



VPN allowed

□ by IPSec VPN

Pre-shared key (optional): ************************

□ by PPTP

Password (mandatory): ************************

□ by SSL VPN

□ Override default profile :

Figure 48: Editing a user – Access

This tab allows you to define IPSec, PPTP and SSL VPN access.

IPSec VPN pre-shared key

This key will be used to create a dynamic IPSEC tunnel with a remote IPSEC client. It must be indicated on the user's mobile client configuration. (In the same way the mobile client identifier must be the user's e-mail address as specified in the internal user file on the Firewall). This field is optional and is only used in a tunnel in pre-shared key. Otherwise, the user's certificate is used (therefore no need to enter the pre-shared key). In all cases, the VPN tunnel has to be configured (at the Firewall and mobile client level) in aggressive mode, with a user@fqdn identifier (which will be the user's e-mail address for the peer).

PPTP password

The user may use this password when he wishes to connect to the Firewall in PPTP. (See .*PPTP VPN configuration*).

SSL VPN

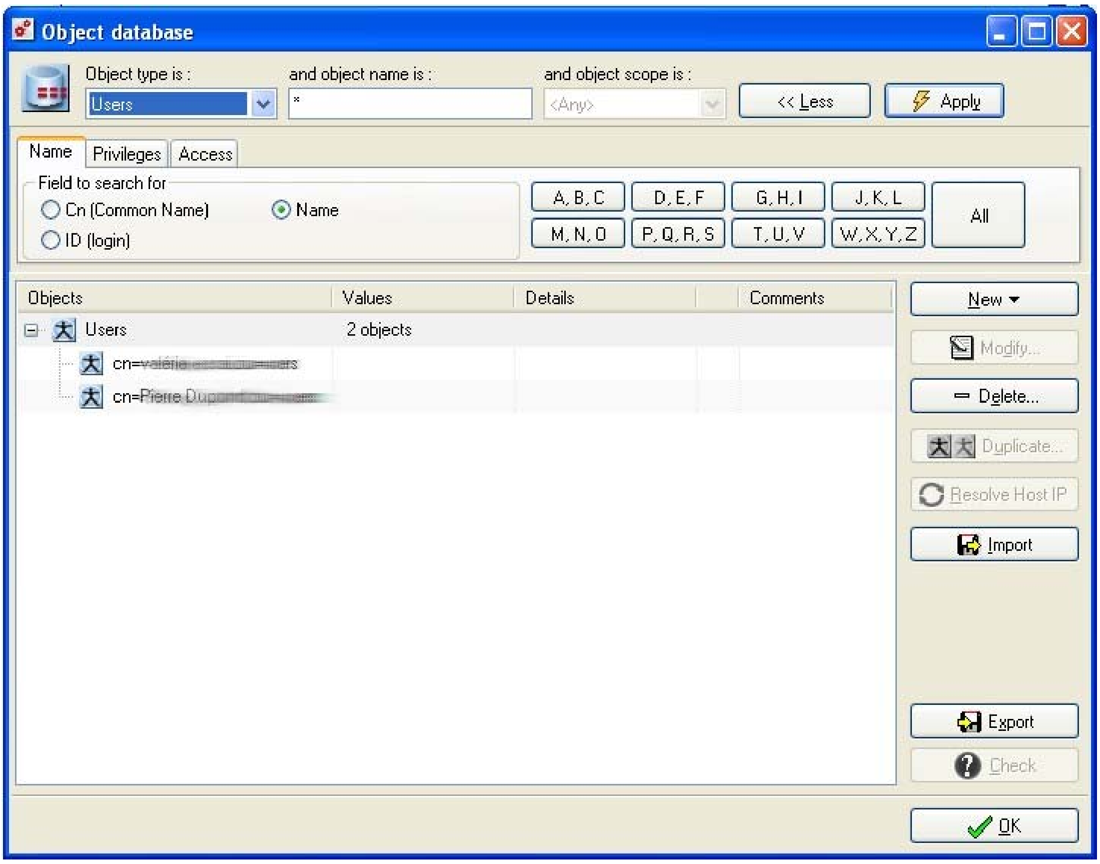
Select the **SSL VPN** option to allow the user to benefit from SSL VPN features (see. Part 8/Chapter 5: *SSL VPN configuration*). A specific profile for this user can be applied if it had been defined in the configuration of the SSL VPN module, in the menu **`VPN\SSL VPN.`**

4.3.1.7. Searching for a user

This window consists of three tabs:

- **`Name`**
- **`Privileges`**
- **`Access`**

Name tab



Object type is : Users
and object name is : *
and object scope is : <Any>

Field to search for
○ Cn (Common Name) ● Name
○ ID (login)

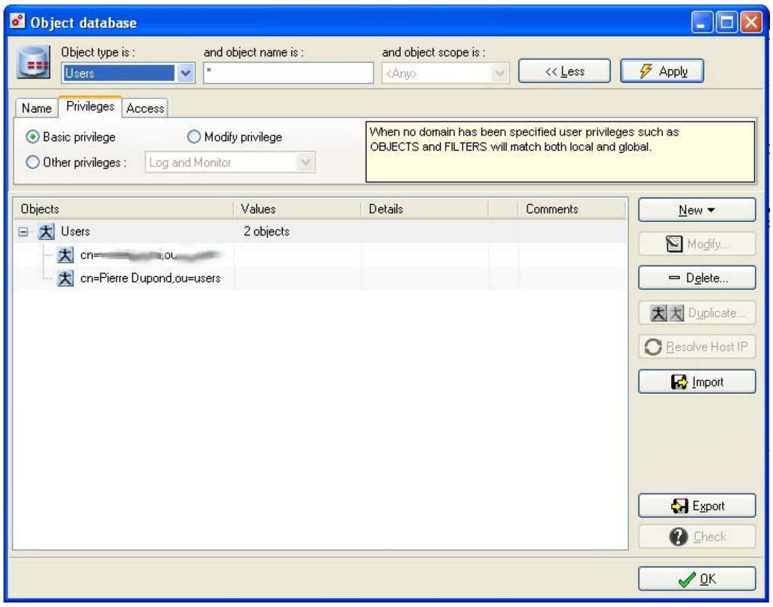
Objects	Values	Details	Comments
Users	2 objects		
cn=[redacted]			
cn=[redacted]			

Figure 49: Object database – Name tab

Users can be searched for by CN (Common Name), ID (identifier) or by username.

Letter buttons enable a refined search.

Privileges tab



Object type is : Users
and object name is : *
and object scope is : <Any>

● Basic privilege ○ Modify privilege
○ Other privileges : Log and Monitor

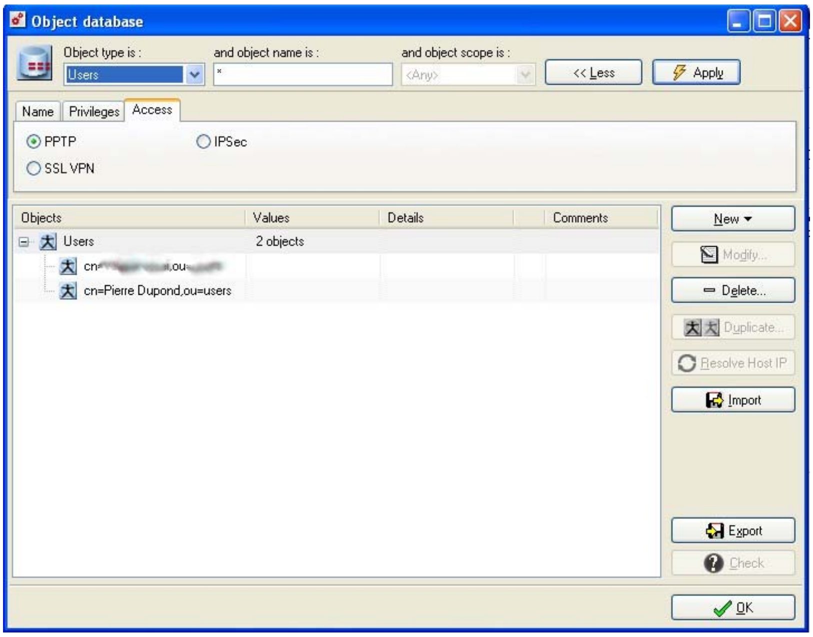
When no domain has been specified user privileges such as OBJECTS and FILTERS will match both local and global.

Objects	Values	Details	Comments
Users	2 objects		
cn=[redacted],ou[redacted]			
cn=Pierre Dupond,ou=users			

Figure 50: Object database – Privileges tab

You can search for users by the privileges that they hold.
Search strings can be refined by selecting “BASIC”, “MODIFY” or other privileges.

Access tab



Object type is : Users
and object name is : *
and object scope is : <Any>

● PPTP ○ IPSec
○ SSL VPN

Objects	Values	Details	Comments
Users	2 objects		
cn[redacted],ou[redacted]			
cn=Pierre Dupond,ou=users			

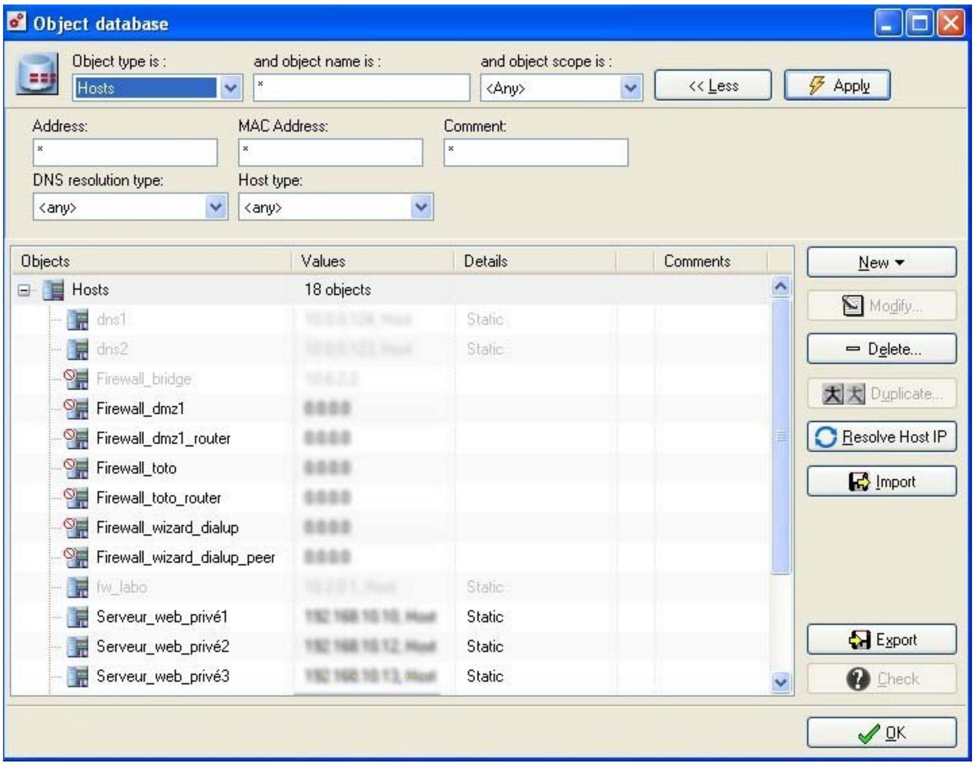
Figure 51: Object database – Access tab

User searches can be conducted and refined according to the type of access they have, ie, PPTP, SSL or IPSec VPN.

CHAPTER 4. HOSTS

This grid allows you to configure the names of hosts used in your configuration files. This allows the NETASQ Firewall to match a host name with its IP address.

In the case of high availability, a new object has been added in version 7.0: "Firewall_HA_peer".



Object type is : Hosts
and object name is : *
and object scope is : <Any>

Address: *
MAC Address: *
Comment: *
DNS resolution type: <any>
Host type: <any>

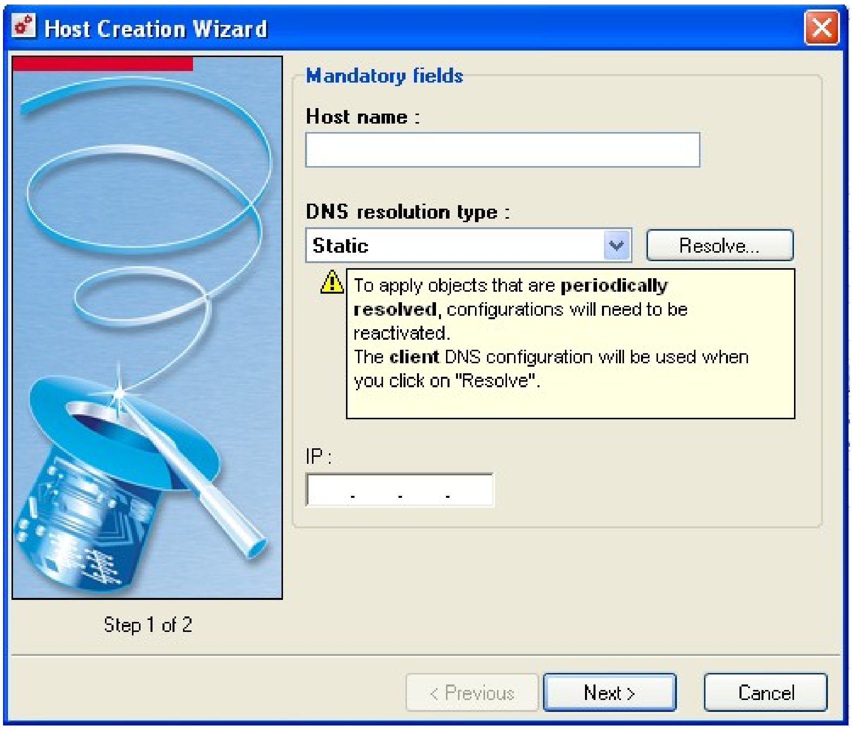
Objects	Values	Details		Comments
Hosts	18 objects			
dns1	[redacted]	Static		
dns2	[redacted]	Static		
Firewall_bridge	[redacted]			
Firewall_dmz1	[redacted]			
Firewall_dmz1_router	[redacted]			
Firewall_toto	[redacted]			
Firewall_toto_router	[redacted]			
Firewall_wizard_dialup	[redacted]			
Firewall_wizard_dialup_peer	[redacted]			
fw_labo	[redacted]	Static		
Serveur_web_privé1	[redacted]	Static		
Serveur_web_privé2	[redacted]	Static		
Serveur_web_privé3	[redacted]	Static		

Figure 52: Object database – Selecting hosts

4.4.1. Host creation wizard

Hosts can be created using a wizard (**New\Host** button), which will ask you to enter the following information:

1 **Step1**:



To apply objects that are **periodically resolved**, configurations will need to be reactivated.
The **client** DNS configuration will be used when you click on "Resolve".

Figure 53: Creating a host – Step 1

Host name: Name associated with the IP address (can be modified).

DNS Resolution type: Select the type of resolution for this object from one of the following: “Static”, “Periodic” or “Manual”.

When “Static” is selected, the address entered does not change.

When “Semi-dynamic” is selected, Manager manually performs DNS resolution to find out the address for these objects.

If “Periodic” is selected, the Firewall performs DNS resolution periodically (every 5 minutes). The features which use these objects do not manage data refreshment (the filter slot must be reactivated manually to apply changes made to objects).

IP: Host’s IP address.

Step 2:

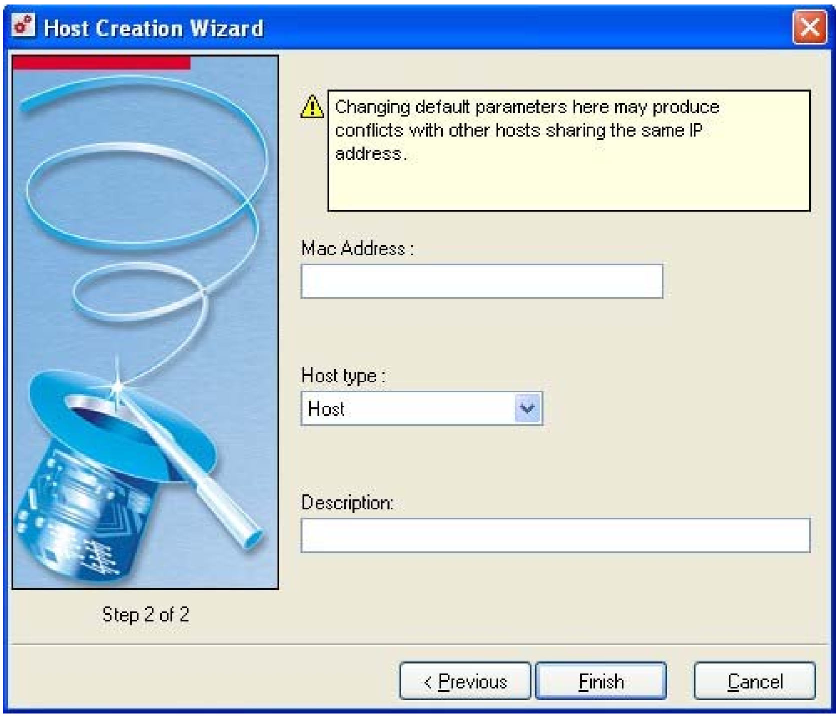

Host Creation Wizard
Changing default parameters here may produce conflicts with other hosts sharing the same IP address.
Mac Address :
Host type :
Host
Description:
Step 2 of 2
< Previous
Finish
Cancel

Figure 54: Creating a host – Step 2

MAC Address: The host's MAC address. If this value is indicated, the MAC address can be matched to an IP address to avoid usurpation of the host.
Host type: Information field allowing you to perform a search at another level. You can select from "Host", "Server" or "Router".

NOTE
"Global" or "Local" can only be entered as a host type during the creation of a host.

Description: Comments you wish to add for this object.

4.4.2. Modifying a host

Click on the **Modify** button to modify an object. If there are filter, URL filter, VPN and address translation slots associated with this object, an information window will ask if you wish to reactivate these rules, and apply the changes immediately. The slots for which the object is used are checked by default but you may unselect a slot type so as not to reactivate it.

WARNING
The VPN slot is never checked even if the object is in use. It is therefore necessary to select it manually. Reactivating a NAT slot leads to the loss of active connections.
NETASQ's DNS dynamic object resolution is not designed for modifying security policies on Firewalls, therefore given that this resolution depends on external equipment, the Firewall cannot dynamically validate modifications to the security policy. Only the administrator can bypass this mechanism (by duplicating the security policy and activating two slots alternately, for example), which has its repercussions (activating a compromised security policy).

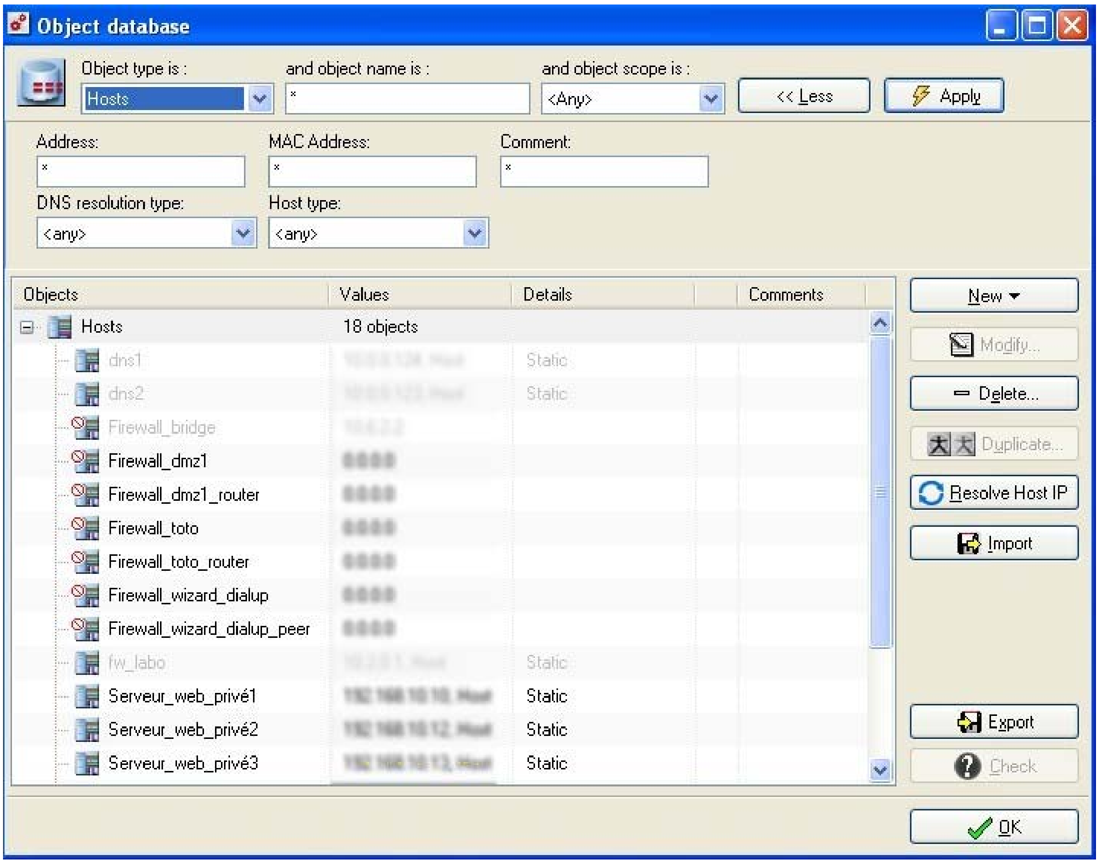
4.4.3. Deleting a host

When an object is deleted, the following message appears:

"Delete object "xxxx"?"

Some machines are pre-configured: "Firewall_in", "Firewall_out", "Firewall_dmz", "Firewall_bridge", "Firewall_vlan" correspond to the NETASQ Firewall's internal interface, external interface, DMZ, bridge and VLAN IP addresses. These can never be changed in the object configuration section.

4.4.4. Searching for a host



Object type is : Hosts
and object name is : *
and object scope is : <Any>

Address: *
MAC Address: *
Comment: *
DNS resolution type: <any>
Host type: <any>

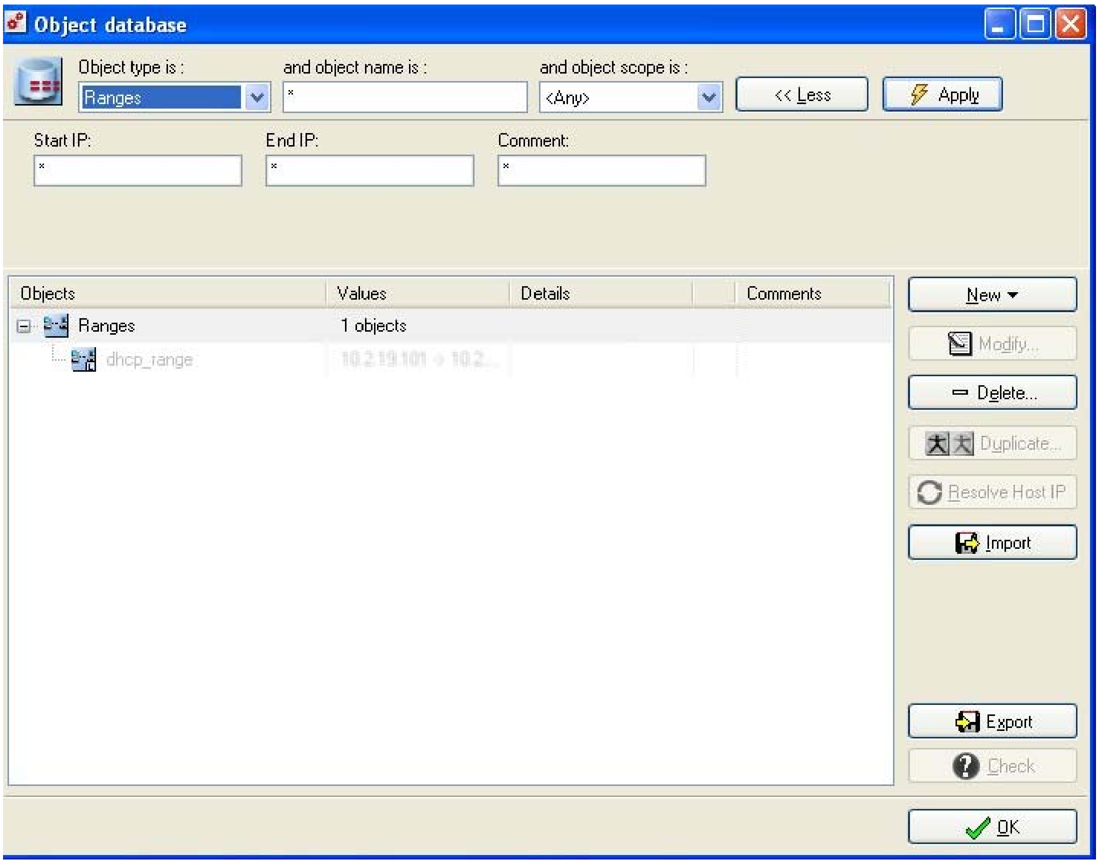
Objects	Values	Details	Comments
Hosts	18 objects		
dns1	[redacted]	Static	
dns2	[redacted]	Static	
Firewall_bridge	[redacted]		
Firewall_dmz1	[redacted]		
Firewall_dmz1_router	[redacted]		
Firewall_toto	[redacted]		
Firewall_toto_router	[redacted]		
Firewall_wizard_dialup	[redacted]		
Firewall_wizard_dialup_peer	[redacted]		
fw_labo	[redacted]	Static	
Serveur_web_privé1	[redacted]	Static	
Serveur_web_privé2	[redacted]	Static	
Serveur_web_privé3	[redacted]	Static	

Figure 55: Searching for a host

The following filters can be used to refine searches:

- Address
- MAC address
- Description
- Resolution
- Host type

CHAPTER 5. ADDRESS RANGE



Object type is : Ranges
and object name is : *
and object scope is : <Any>
Start IP: *
End IP: *
Comment: *

Objects	Values	Details	Comments
Ranges	1 objects		
dhcp_range	10.2.19.101 -> 10.2...		

Figure 56: Object database – Address ranges

This menu enables you to configure address ranges. These ranges can be used when specifying particular address pools (DHCP, PPTP, etc).

Each entry on the list is made up of an address range name, start address, end address and comments.

Click on “Modify” to make changes to the object. If you have filter, URL filter, VPN or NAT slots associated with this object, a window will open, asking if you wish to reactivate these slots and apply changes immediately. Slots for which the object has been used will be selected by default but you can unselect a slot type so that it will not be reactivated. Caution: the VPN slot is never selected even if the object is used, therefore it needs to be selected manually. Active connections will be lost when a NAT slot is reactivated.

4.5.1. Creating an address range

- To create an address range, click on **New** and select **Range**. The following window will appear:

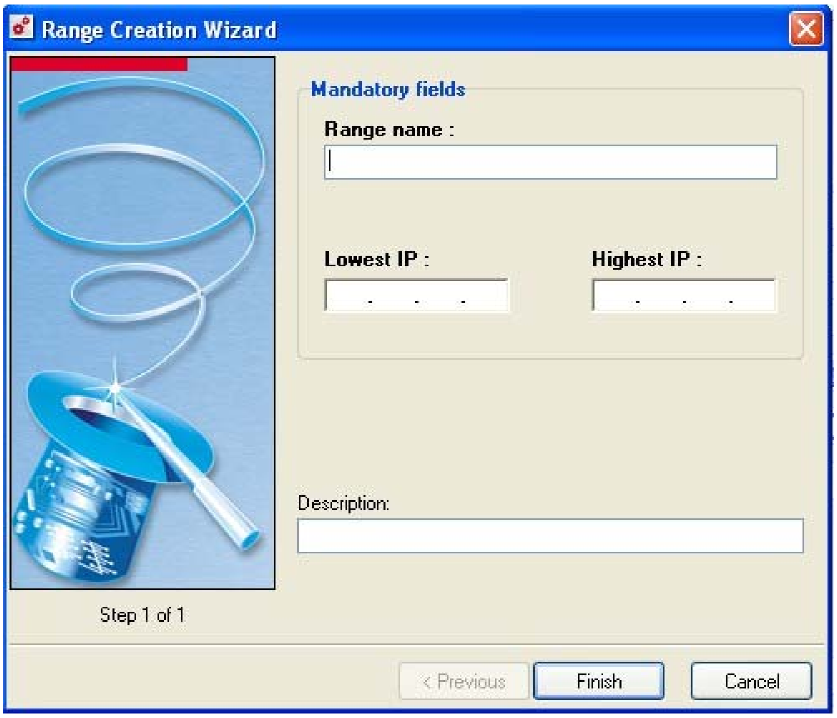
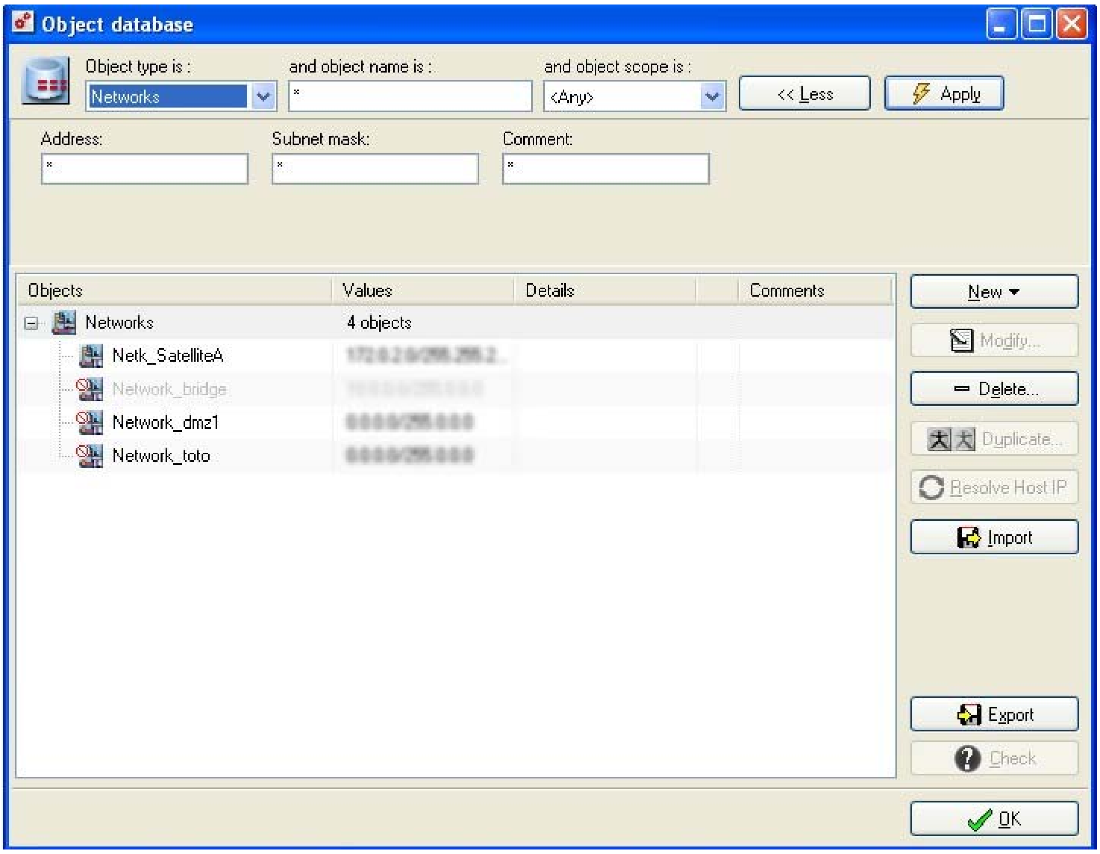


Figure 57: Creating an address range

Range name: Name that you associate with the address range (cannot be modified).
Lowest IP: Indicates the lower IP address range.
Highest IP: Indicates the higher IP range.
Description: Comments you may wish to add for this address range.

REMARK
"Global" or "Local" can only be entered as a range type during the creation of a range.

CHAPTER 6. NETWORKS



Object type is : Networks

and object name is : *

and object scope is : <Any>

Address: *

Subnet mask: *

Comment: *

Objects	Values	Details	Comments
Networks	4 objects		
Netk_SatelliteA	[redacted]		
Network_bridge	[redacted]		
Network_dmz1	[redacted]		
Network_toto	[redacted]		

Figure 58: Object database – Networks

This tab allows you to configure the network and sub-network names used in your configuration files. This allows the NETASQ Firewall to match a network name with its IP address and its network mask.

Each entry in the list consists of a network name, the IP address of the network, its network mask, details and comments on the network.

> **WARNING**
> The VPN slot is never checked even if the object is used. Thus it is necessary to manually select it. Also, the re-activation of a NAT slot leads to the loss of active connections.

Deleting a network will display a dialog box prompting you to confirm the deletion and the removal of this network from the different network groups in which it was present.

Some networks are pre-configured: "Network_in", "Network_out", "Network_dmz", correspond to the NETASQ Firewall's internal interface, external interface and DMZ IP addresses. If you use the Firewall in transparent mode, only "Network_bridge" is created. If you have created VLANs, the network "Network_vlan" will be created. These names cannot be changed.

- To create an address range, click on **New** and select **Network**. The following window will appear:

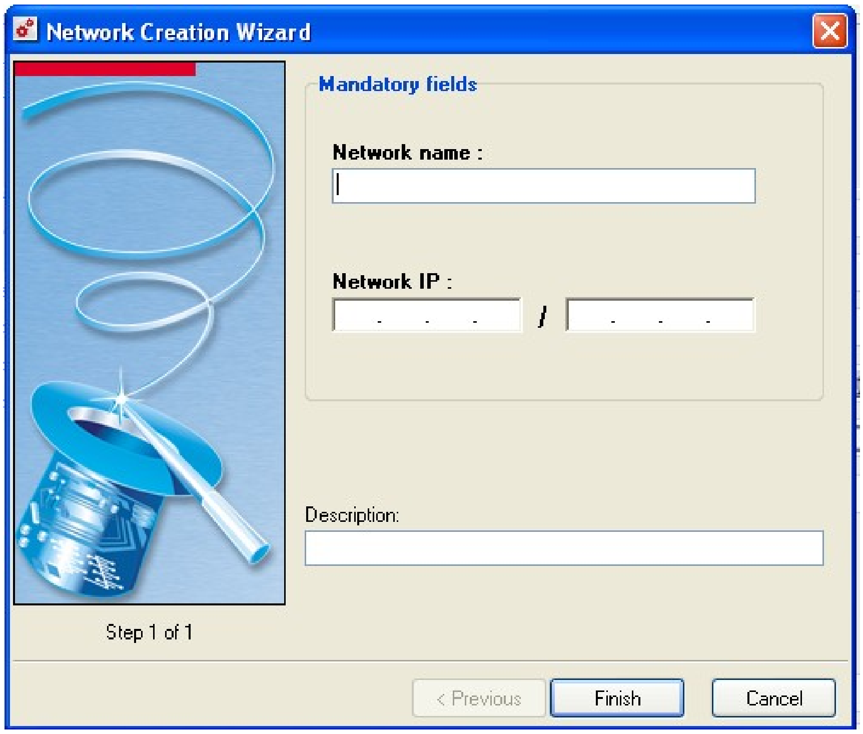
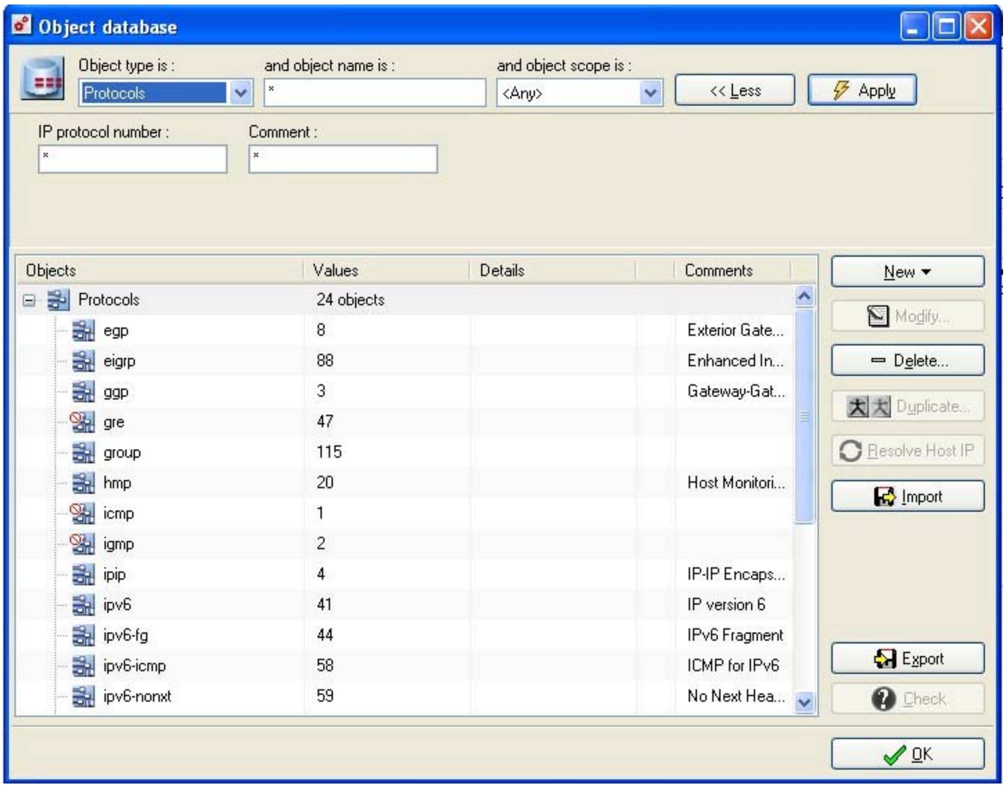


Figure 59: Creating a network

Network name (mandatory): Name that you associate with the address range (cannot be modified later).
Network IP (mandatory): Indicates the IP address of the network and of the subnet mask.
Description: Comments you may wish to add for this network.

REMARK
"Global" or "Local" can only be entered during the creation of a network.

CHAPTER 7. PROTOCOLS



Object database

Object type is : Protocols
and object name is : *
and object scope is : <Any>
IP protocol number : *
Comment : *

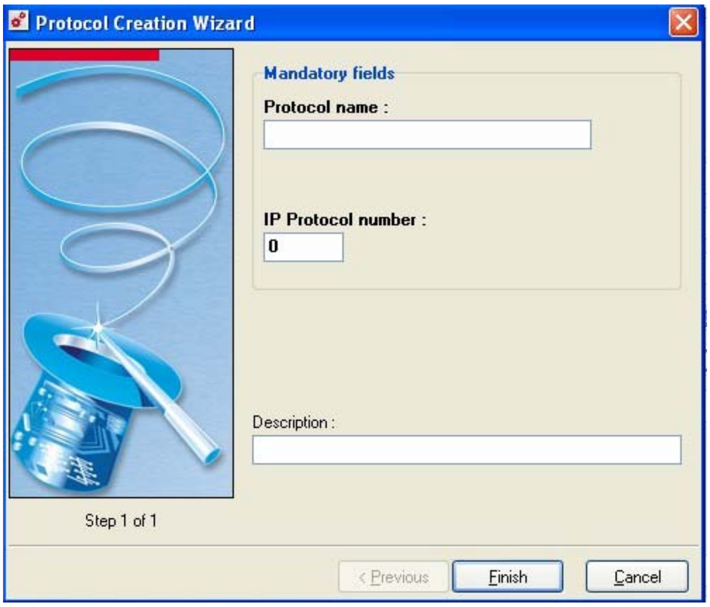
Objects	Values	Details	Comments
Protocols	24 objects		
egp	8		Exterior Gate...
eigrp	88		Enhanced In...
ggp	3		Gateway-Gat...
gre	47		
group	115		
hmp	20		Host Monitori...
icmp	1		
igmp	2		
ipip	4		IP-IP Encaps...
ipv6	41		IP version 6
ipv6-fg	44		IPv6 Fragment
ipv6-icmp	58		ICMP for IPv6
ipv6-nonxt	59		No Next Hea...

Figure 60: Object database - Protocols

This tab allows you to configure the names of IP-based protocols used in filtering configuration. This keeps Firewall informed about the correspondence between a protocol name and protocol number used by the IP layer. Any protocol that IP supports may be added and managed by the Firewall.

This allows you to use these names in filter rules and to apply security policies to these protocols.

➲ To create a protocol, click on **New** and select **Protocol**. The following window will appear:



Protocol Creation Wizard

Mandatory fields

Protocol name :

IP Protocol number : 0

Description :

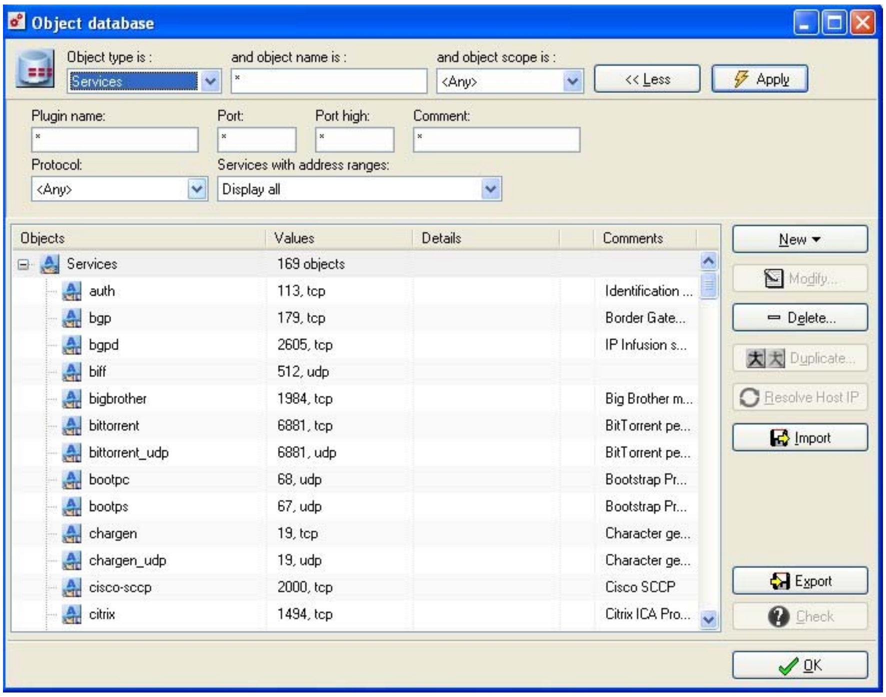
Step 1 of 1

Figure 61: Creating a protocol

Protocol name (mandatory): Name that you associate with the protocol (cannot be modified later).
IP Protocol number: Indicates the number of the protocol.
Description: Comments you may wish to add for this protocol.

REMARK
"Global" or "Local" can only be entered during the creation of a protocol.

CHAPTER 8. SERVICES



Object type is : Services
and object name is : *
and object scope is : <Any>
Plugin name: *
Port: *
Port high: *
Comment: *
Protocol: <Any>
Services with address ranges: Display all

Objects	Values	Details	Comments
Services	169 objects		
auth	113, tcp		Identification ...
bgp	179, tcp		Border Gate...
bgpd	2605, tcp		IP Infusion s...
biff	512, udp		
bigbrother	1984, tcp		Big Brother m...
bittorrent	6881, tcp		BitTorrent pe...
bittorrent_udp	6881, udp		BitTorrent pe...
bootpc	68, udp		Bootstrap Pr...
bootps	67, udp		Bootstrap Pr...
chargen	19, tcp		Character ge...
chargen_udp	19, udp		Character ge...
cisco-sccp	2000, tcp		Cisco SCCP
citrix	1494, tcp		Citrix ICA Pro...

Figure 62: Object database - Services

This screen allows you to define the names of the services used in your filter-rules. This allows the NETASQ Firewall to match the name of a service with the protocol and port number.
The “Details” column indicates the plugin associated to a service. It’s possible to activate one specific plug-in on multiple different services as well as multiple plug-ins on a single service. Moreover, a plugin is not reserved to a specific service.

Example
The HTTP plug-in is not reserved for the HTTP-service but can also be activated on other services (ports). This allows you to associate a plug-in with a port that is generally used for a specific kind of traffic but which you wish to secure by a certain plug-in and thus secure for a different kind of traffic.

When you have specified a plug-in for a service, this plug-in will not be applied unless the specific service is used in the filter-rules.

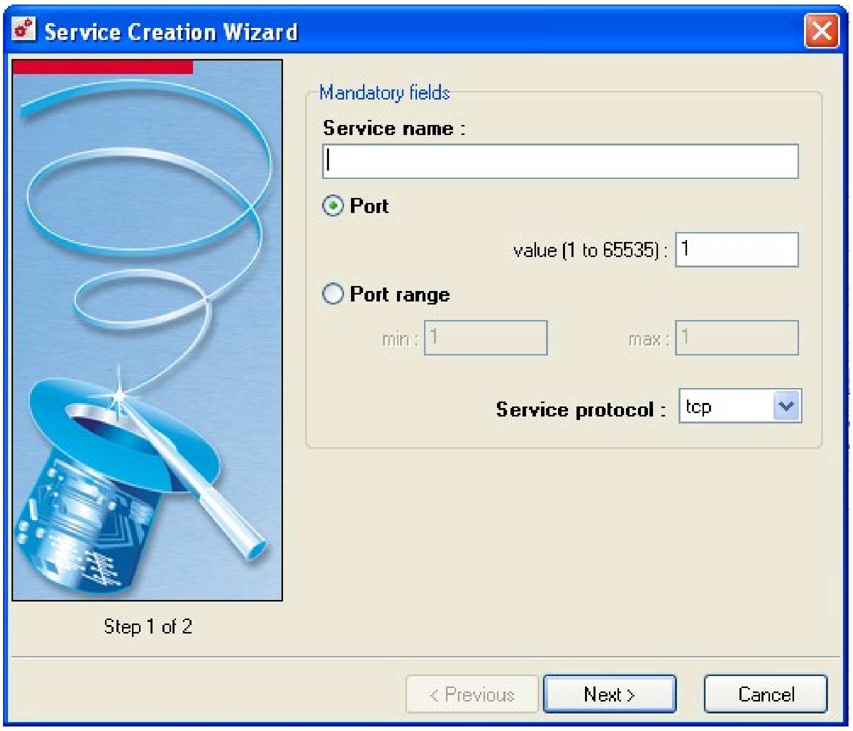
For an automatic activation of a plug-in (auto-attach), even when there’s no filter-rule directly associated with the service, refer to the section *Part 6/Chapter 9: Plugins*.

WARNING
For a maximum level of security, NETASQ recommends imposing a static plug-in rather than an automatic activation (auto-attach). Automatic activation of plug-ins should only be used on non-critical services (enabling HTTP traffic to be logged, for example).

4.8.1. Creating a service

There are 2 steps to creating a service:

Step 1

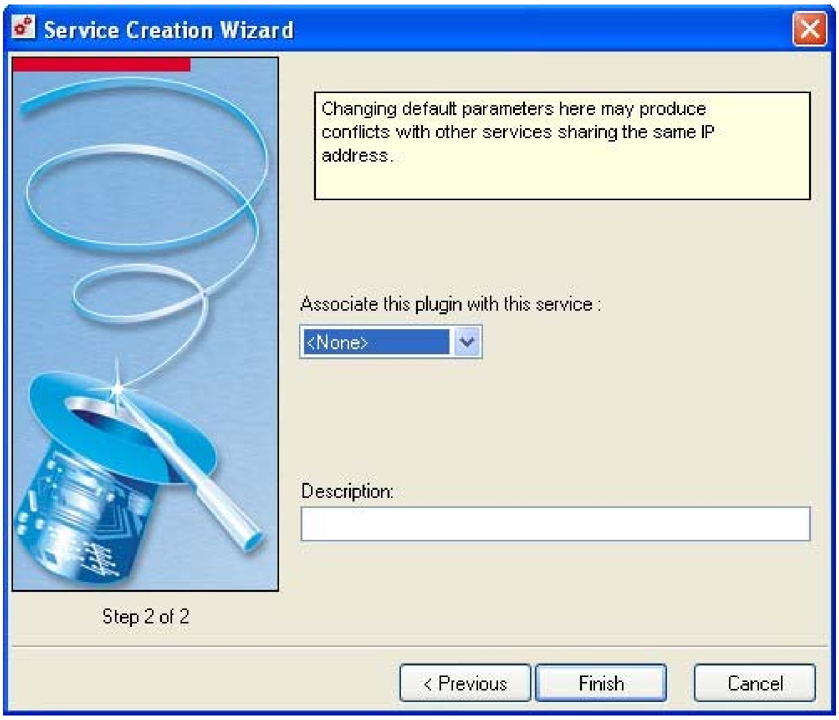


Mandatory fields
Service name :
● Port
value (1 to 65535) : 1
○ Port range
min : 1
max : 1
Service protocol : tcp

Figure 63: Creating a service - Step 1

Service name (mandatory): The name you wish to assign to the service (cannot be subsequently modified).
Port (mandatory): Number of the port associated with the service.
Port range (mandatory): Indicates a port range within the "min" and "max" fields.
Service protocol (mandatory): TCP or UDP.

2 Step 2



Service Creation Wizard

Changing default parameters here may produce conflicts with other services sharing the same IP address.

Associate this plugin with this service : <None>

Description:

Step 2 of 2

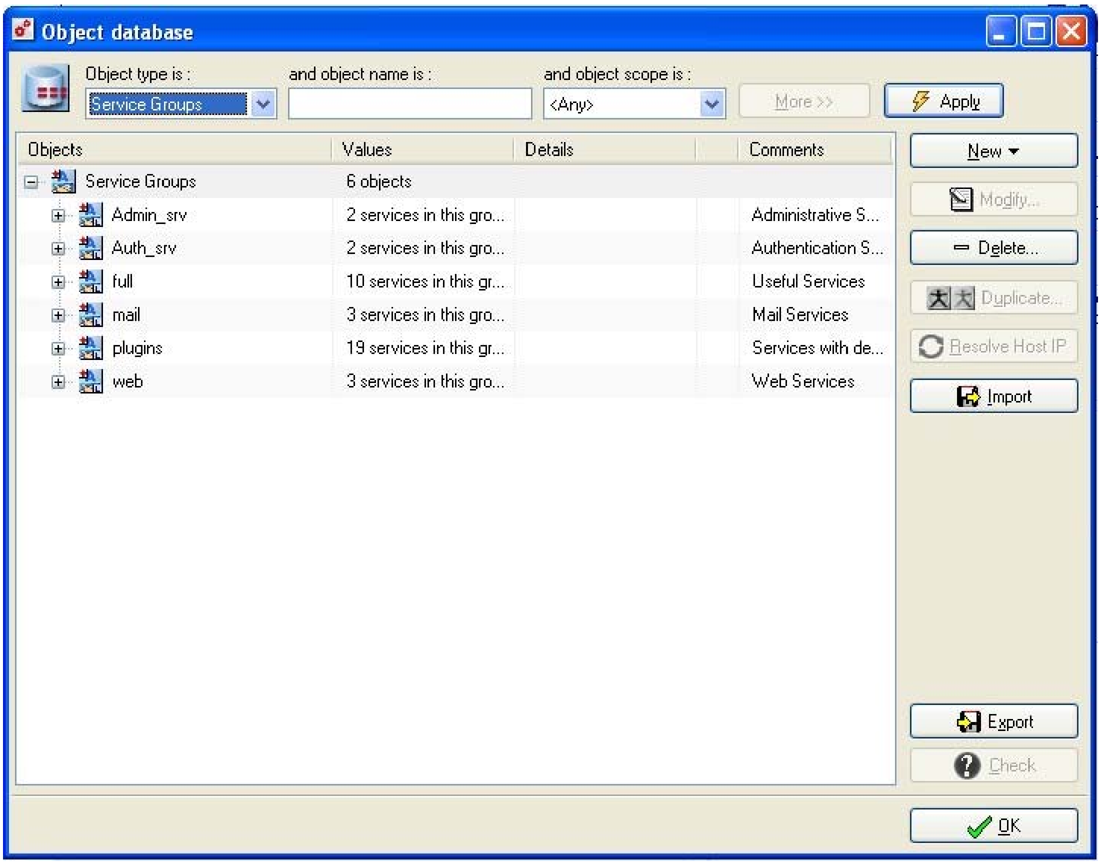
Figure 64: Creating a service - Step 2

Associate this plugin with this service: The following plugins can be matched with a service: <None>, http, FTP, EDONKEY, H323, SSL, Stream, SSH, Telnet, SMTP, POP3, IMAP4, NNTP, MySQL.
Description: Comments you may wish to add for this service.

REMARK
"Global" or "Local" can only be entered as a service during the creation of a service.

Click on the **Modify** button to modify the selected service. If you have associated filter slots, URL filtering, VPN or address translation to this object, an information window will ask you if you wish to re-activate these slots and immediately apply the changes.
This version of the NETASQ Firewall does not manage RPC (Remote Procedure Call) services, which use dynamically allocated port numbers.
Certain services cannot be modified. Moreover, a service is reserved for Firewall operations:
"Firewall_srv" (port 1300) corresponds to a service which manages communication between the NETASQ Firewall and NETASQ UNIFIED MANAGER and NETASQ REAL-TIME MONITOR. This service is also used for the **high availability** feature between two Firewalls.
You will find a list of frequently used services (DNS, HTTP, FTP...) in *Appendix B: TCP/IP Services,* as well as the relevant protocol and port number for this service

CHAPTER 9. SERVICE GROUPS



Object type is : Service Groups

and object name is :

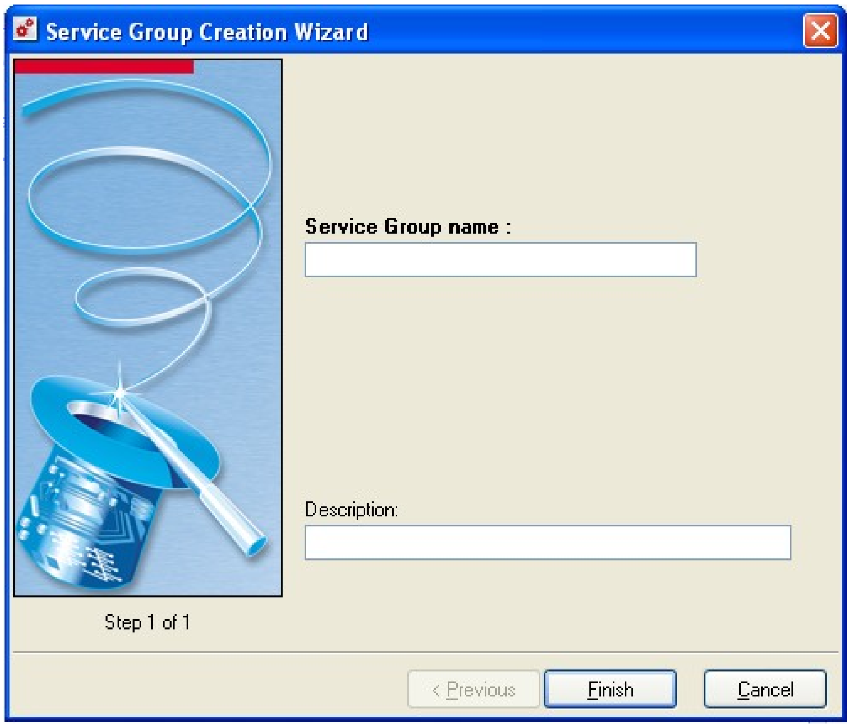
and object scope is : <Any>

Objects	Values	Details	Comments
Service Groups	6 objects		
Admin_srv	2 services in this gro...		Administrative S...
Auth_srv	2 services in this gro...		Authentication S...
full	10 services in this gr...		Useful Services
mail	3 services in this gro...		Mail Services
plugins	19 services in this gr...		Services with de...
web	3 services in this gro...		Web Services

Figure 65: Object database – Service groups

Likewise for users and network equipment, you may create service groups for services which have the same configuration properties. These service groups can then be used in the configuration as a single service. The aim of this is to simplify configuration and the understanding of your configuration by restricting the number of services to integrate.

4.9.1. Creating a service group



Service Group Creation Wizard

Service Group name :

Description:

Figure 66: Creating a service group - Step 1

Service group name (mandatory): Name that you assign to this service group.
Description: Comments you may wish to add for this service group.

4.9.2. Adding a service to a group

To add a service to a group, the procedure is as follows:

1. Select the service you wish to add from the list in object definition.
2. Right-click with your mouse.
3. Select the option **Add to** in the menu, then on **Service groups**.
4. Select the group to which this service will be added or select “**New Service group**”.

When a new group is created, the selected service will automatically be added to the group.
If you modify a group that is used in the configuration of the UTM appliance, the changes will automatically be applied and the slots that use this group will automatically be reactivated.

WARNING
Reactivating a NAT slot will cause active connections to be lost.

The Firewall contains pre-configured service groups which make configuration easier:

- Admin_srv: Firewall’s administration services (SSH and firewall_srv).
- Auth_srv: Authentication services on the Firewall (HTTPS and firewall_auth).
- Full: Contains services which allow access to web, mail, telnet and the main web-based services (news, ftp, DNS ...).

- Mail: Contains all the mail access services for clients.
- Plugins: Services with a specific plugin and the associated activated plugins.
- Web: Web access only (http and https).

CHAPTER 10. USER GROUPS

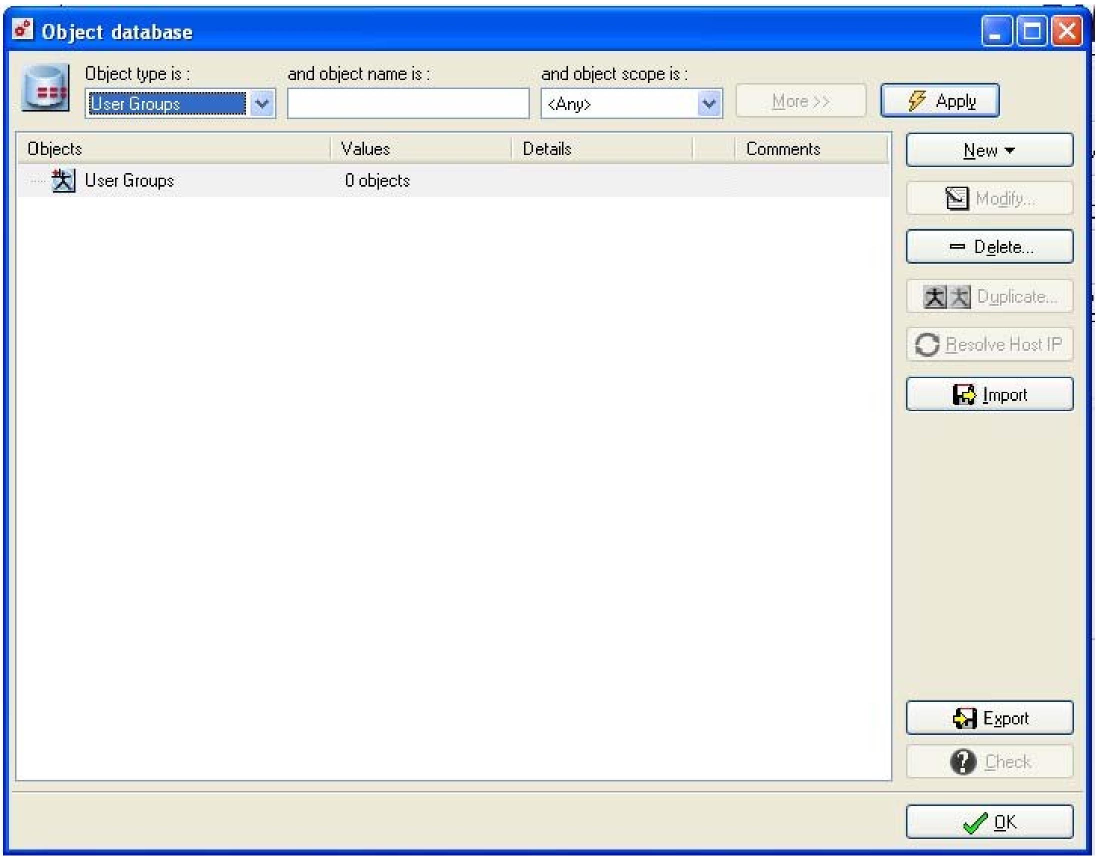


Figure 67: Object database – User groups

This window allows you to create user groups, which simplifies the editing of the filter rules: instead of defining a rule for each user you can define a single rule for all users with the same rights.

To create a new group, follow the procedure below

1 Click on the **New** button, then select **`User groups`** in the contextual menu. A group creation wizard will appear.

4.10.1. Adding a user to a group

To add a user to a user group, the procedure is as follows:

1 Select the user you wish to add from the list in object definition.

2 Right-click with your mouse.

3 Select the option **Add to** in the contextual menu then **User groups**, and select **New User Group**.

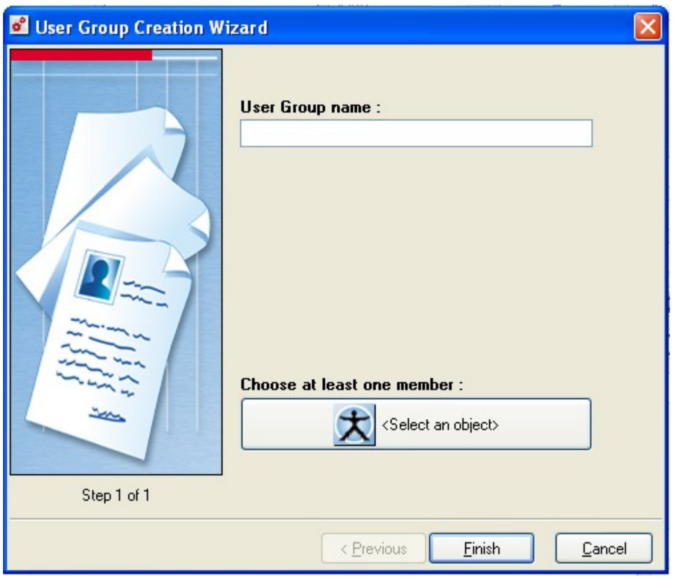
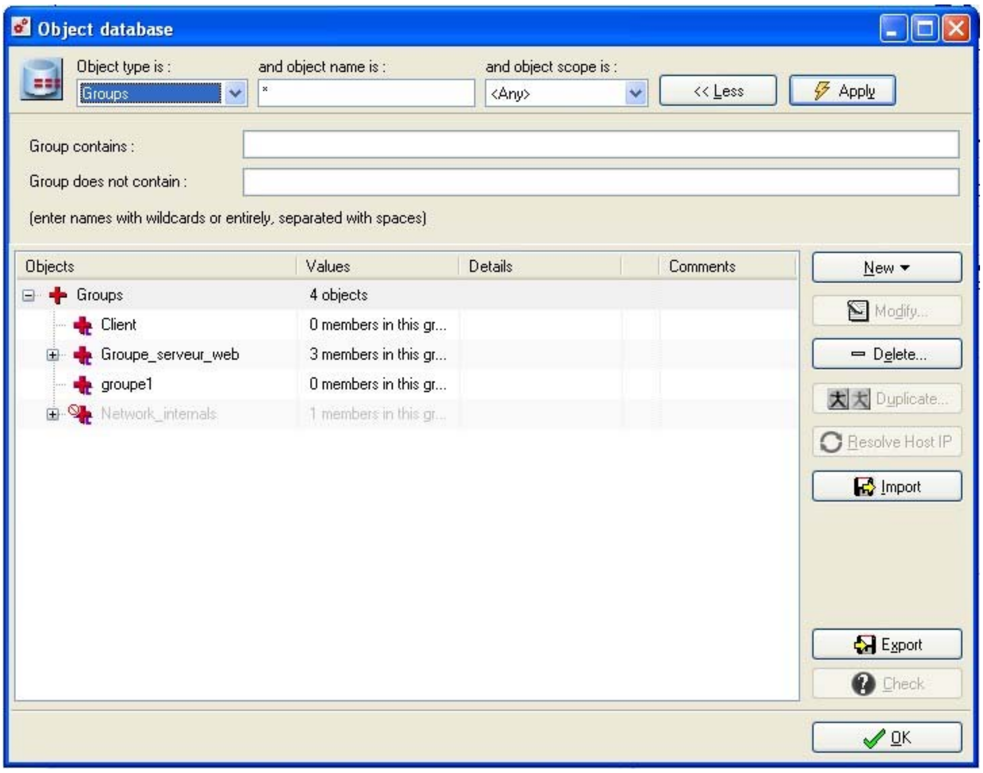


Figure 68: Creating a user group - Step 1

4 Select the group to which this user will be added.

When a new group is created, the selected user will automatically be specified in the group configuration window. If you modify a group that is used in the configuration of the UTM appliance, the changes will automatically be applied and the slots that use this group will automatically be reactivated.

CHAPTER 11. GROUPS



Object type is : Groups
and object name is : *
and object scope is : <Any>

Group contains :
Group does not contain :
(enter names with wildcards or entirely, separated with spaces)

Objects	Values	Details	Comments
Groups	4 objects		
Client	0 members in this gr...		
Groupe_serveur_web	3 members in this gr...		
groupe1	0 members in this gr...		
Network_internals	1 members in this gr...		

Figure 69: Object database - Groups

Double-click on **Groups** tab in the menu directory. The following window will appear:
This menu enables you to create "network" groups, which can contain hosts, networks, address ranges and other "network" groups.

4.11.1. Creating a group

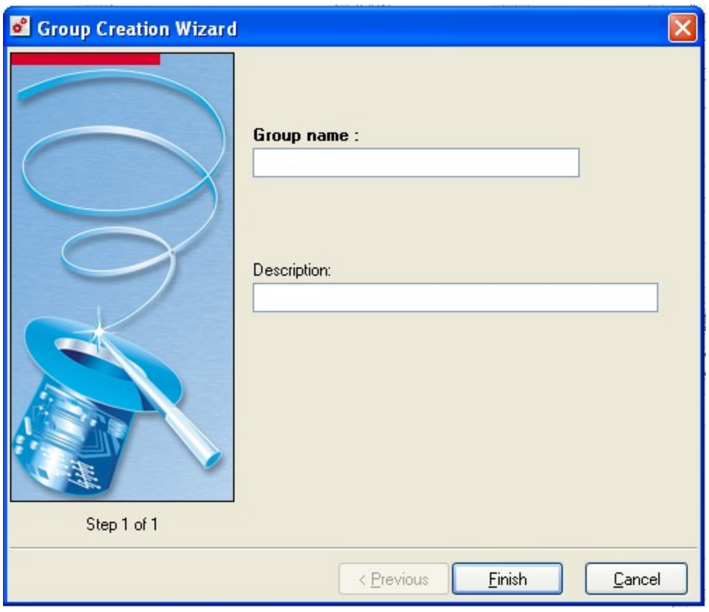


Figure 70: Creating a group - Step 1

Group name: (mandatory): Name that you assign to the group.
Description: Comments you may wish to add for this group.

4.11.2. Adding an object to a "network" group

The procedure for adding an object to a "network" group is as follows:

1. Select the object you wish to add from the list in object definition.
2. Right-click with your mouse.
3. Select the option **Add to\Groups\New group** in the contextual menu.
4. Select the group to which this object will be added.

When a new group is created, the selected object will automatically be added to the group.
If you modify a group that is used in the configuration of the UTM appliance, the changes will automatically be applied and the slots that use this group will automatically be reactivated.

CHAPTER 12. GENERAL REMARKS REGARDING OBJECTS

There are certain reserved object names:

- As a general rule, all object names beginning with "firewall_" and "network_" are prohibited.

- Protocol names GRE, ICMP, IGMP, TCP, UDP, VPN-AH, VPN-ESP are reserved.
- In the case of services, ssh, isakmp, firewall_srv, firewall_auth, ephemeral_tcp, ephemeral_udp and ephemeral_fw are reserved.

These reserved object names are marked in the different object lists by a sign next to the object name. These names cannot be modified.

There are also restrictions as to object names:

- Prohibited characters: ", <tab>, \, #, @, <space>
- Prohibited starting characters: numerals

PART 5: NETWORK CONFIGURATION

CHAPTER 1: INTRODUCTION

5.1.1. Prerequisites

5.1.1.1. For this chapter, you will need to have completed these steps

- PART 2: Installation, pre-configuration, integration

5.1.1.2. For this chapter, you will need to know

- The IP parameters to assign to the NETASQ Firewall for each interface in advanced configuration.
- The IP address to assign to the NETASQ Firewall for its connection to the network in transparent mode configuration.
- The IP address of the default router to be used.
- The static routes in case of router operation.
- Connection parameters, given by your access provider, in diaup access

5.1.1.3. Purpose of this section

This part allows you to remotely reconfigure the parameters associated to the NETASQ Firewall's network adapters, as well as the default router's IP address.

This part allows you to manage, add and delete network interface elements which represent the devices that communicate between the different networks that go through the appliance.

The following are the different types of interface that the network configuration deals with:

- **Ethernet**: these are the only interfaces that directly match a physical port located on the appliance. As such, they cannot be added or deleted in this configuration, but can only be disabled or enabled. These interfaces may have one or several network addresses, depending on whether they have a "parent" bridge.
- **Bridge**: this means a grouping of interfaces. Any interface with a valid "Bridge" parameter delegates its address management to the bridge and therefore becomes an element of this bridge. As such, bridges can be considered to have one or several addresses (static or dynamic). Besides, all the subnetworks of this bridge share the same address ranges (the bridge's address ranges).
- **VLANs**: VLANs are virtual interfaces that have their own address range (but not when they are attached to a bridge), but whose packets pass through an Ethernet interface. As a result, VLANs have a parameter that allows them to specify the Ethernet interface to which they are assigned. If the Ethernet interface is down or still disabled, the VLAN will not function either.
- **Dialups**: these interfaces are dedicated to the establishment of PPTP, PPP, PPPOE modem connections (to an access provider) or to access L2TP tunnels.

Occasionally, these elements may be linked to one another.

The Firewall can operate in three modes:

- **bridge (or transparent) mode**: it is inserted into a network and possesses an address situated on this network. In this mode, you do not need to modify your network's topology (default gateway, static routes, etc.). The Firewall therefore functions like a gateway.
- **advanced mode**: your network is separated into two, three or more parts (depending on the number of interfaces you possess) and different network addresses are assigned to each of these parts. This allows you to distinguish between the different parts of your network where addressing is concerned.
- **hybrid mode**: this mode uses a comnination of both modes mentioned earlier. Several interfaces can be defined in transparent mode.

5.1.1.4. Accessing this section

➲ Access network configuration by selecting **`Network`** in the menu directory.

You have to be connected with the "Network" right and modification privileges for modifying the configuration of interfaces and the "Route" right and modification privileges in order to modify routing configuration.

> **REMARK**
> Before performing any major modification on your NETASQ Firewall, we recommend that you perform a backup (See *Part 18: Backup*). As such, in case of any error you will be able to return to the previous configuration.

5.1.2. Presentation

This network configuration menu enables the configuration of all the Firewall's network parameters:

- the operating mode of the interfaces (bridge or advanced).
- the Firewall's IP address(es) as well as the network to which it is connected.
- remote connections on the serial port (modem).
- routing carried out by the Firewall.

You will be able to define virtual interfaces which may belong to VLANs in your network. Therefore the NETASQ Firewall may manage your architecture's VLANs. *Part 5/Chapter 2: VLAN configuration*

You may also carry out routing by interface: depending on the interface on which the Firewall receives a packet, this packet is sent toward a different gateway.
Once all these parameters have been entered, you only need to send the configuration to the Firewall using the **Send** button.

> **WARNING**
> Modifying some of these parameters requires rebooting the Firewall. While it is not necessary, it is recommended. In this case, a message will warn you before sending to the Firewall.

CHAPTER 2: INTERFACES

5.2.1. Operating mode between interfaces

The Firewall's interfaces may be configured in three ways:

- advanced mode
- transparent mode
- hybrid mode

5.2.1.1. Advanced mode

With this configuration mode, the Firewall operates like a router between its different interfaces.

This involves certain IP address changes on the routers or servers when you move them to a different network (behind a different interface of the Firewall).

The advantages of this mode are:

- possibility of address translation from one address class to another.
- only traffic passing from one interface to another passes through the Firewall (internal network to the internet, for example). This considerably lightens the Firewall's load and returns better response times.
- better distinction between the different elements belonging to each zone (internal, external and DMZ). The distinction is made by the different IP addresses for each zone. This enables a clearer view of the separations and the configuration to be applied on these elements. Furthermore, you can apply global rules on a zone with the "Network" objects.

5.2.1.2. Transparent or bridge mode

The transparent or "bridge" mode, allows the NETASQ Firewall to be installed without changing anything in your network configuration.

It simulates a filtering bridge: in other words, all the network traffic crosses it.

However, you can subsequently filter traffic across it according to your needs, and thus protect any part of your network.

There are many advantages to this mode:

- ease of integration of the product since there is no change in the configuration of client workstations (default router, static routes, etc.) and no change in IP address on your network.
- compatibility with IPX (Novell network), Netbios in Netbeui, Appletalk or IPv6.
- no address translation, therefore time-saving as far as Firewall packet treatment is concerned.

This mode is therefore recommended between the external zone and the DMZ. It allows keeping a public address range on the Firewall's external zone and on the DMZ's public servers.

5.2.1.3. Hybrid mode

The hybrid mode uses a combination of both modes mentioned earlier. This mode may only be used with NETASQ products having more than two network interfaces. You may define several interfaces in transparent mode

> **Example**
> e.g. internal zone and DMZ or external zone and DMZ) and certain interfaces in a different addressing plan. As such, you have greater flexibility when integrating the product.

5.2.1.4. Conclusion

The choice of a mode is made only where network interface configuration is concerned. The configuration of the Firewall is then the same for all modes.

Security-wise, all operating modes are equal. The same things are filtered and attack detection is identical.

5.2.2. Configuring the interfaces

5.2.2.1. Presentation of the configuration window

Interfaces are arranged in hierarchical order.

- If an interface is in a bridge, it will be repreented as a child node in relation to the bridge. Thus, a bridge may contain several interfaces.
- If a VLAN has an Ethernet interface as a physical link, it will be a child connection of this Ethernet interface unless this VLAN belongs to the bridge. In this case, it will be the direct child connection of the bridge. The hierarchy of the configuration is therefore: Bridge -> ethernet ->VLAN but never more than that.
- All dialups are at the same level, after all other interfaces.

Certain elements can be moved, either by dragging and dropping them or by performing actions suggested in the contextual menus. You can:

- "Detach" an interface from a bridge by taking it out of the bridge and dropping it off into an empty zone.
- Make the physical link of a VLAN a parent link by dropping it off on another Ethernet interface.

When an interface has no address but would probably need one (to be detached from a bridge, for example), a panel offering a choice of addresses will become available.

Every node (interface) in the hierarchy is represented by the name of the associated interface.

In addition, every interface has its own icon for quicker visual identification. This icon also allows the user to determine the operational status of the interface. If the interface has been disabled, it will be grayed out.

Ethernet interfaces have a name (e.g. “OUT”) and a number (e.g. “0”). The number is displayed ibrackets after the interface name.

There are two buttons at the bottom of the screen:

Add	Allows adding an interface to the configuration.
Remove	Allows deleting (for VLANs and dialups) and detaching (Ethernet) interfaces.

When you click on an item in the menu directory of the configuration, the configuration panel that appears will be adapted to the type of interface selected. Each configuration panel consists of a set of tabs, such as Identity and Parameters, two tabs relating to addresses and tabs that are specific to the type of interface (type of dialup, for example).

A Status tab allows the user to view a list of the modules on the appliance that use the current interface, which is very useful for getting a preview of changes to products on this interface.

➲ Interfaces on a firewall are configured via the menu **`Network\Interfaces`** in the menu directory.

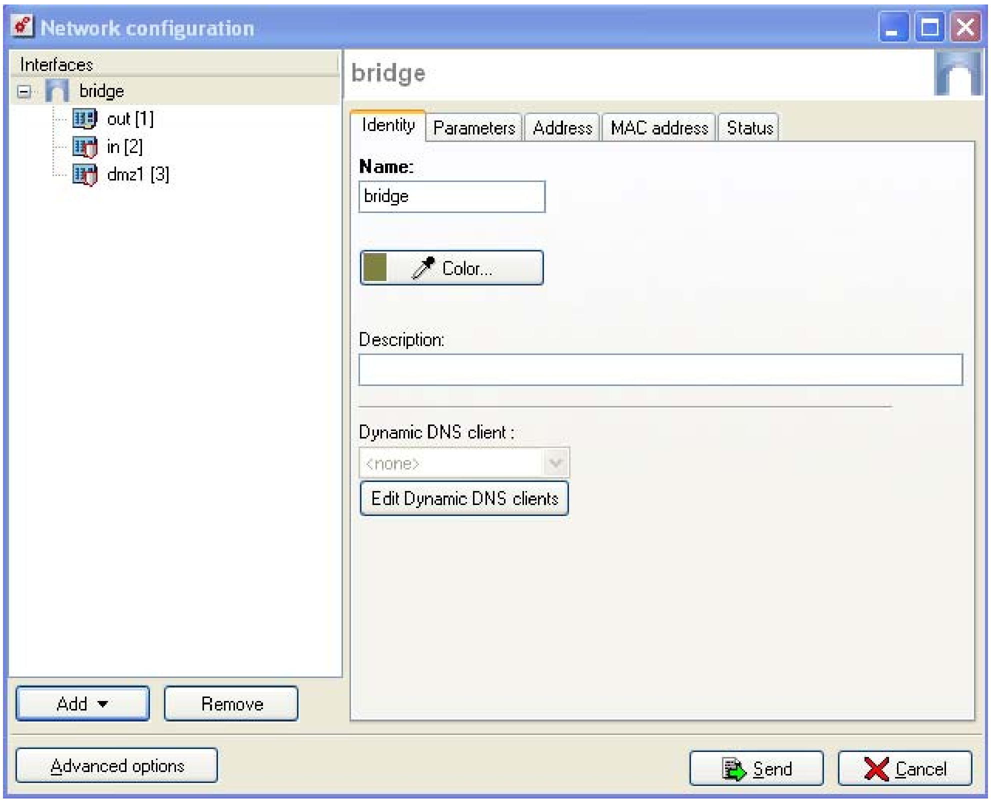
There are several ways of configuring the interfaces:

- **In transparent (bridge) mode**: the interfaces are part of the addressing range specified on the bridge,
- **In advanced mode**: each interface has a different IP address and the network connected with it is part of the same class. This allows you to configure the translation rules to access another Firewall zone.
- **In hybrid mode**: some interfaces have the same IP address and others have a separate address.

5.2.2.2. Bridge parameters

To change the bridge parameters click on the button ⊞ to the left of the **`Bridge`** menu on the left side of the window. Five tabs enable modifying the bridge's parameters.

Identity tab



Name: bridge

Description:

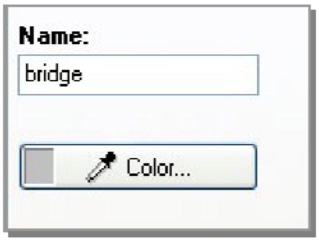
Dynamic DNS client : <none>

Figure 71: Bridge configuration - Identity

Name (mandatory)	Username of the interface. (*See. Part 5/Chapter 4: Remarks on network configuration* for prohibited names).
Color	Interface color. These colors are very useful when you are installing the filter rules, translations etc. Each object created takes on a color, depending on the zone to which the IP address belongs.
Description	Allows you to give a comment for the interface.
Dynamic DNS client	This option is used when your Firewall does not have a static IP address (e.g, your service provider, or DNS renews its IP address regularly). The assigned IP address can be matched to a domain name via a DNS service provider in order to contact this Firewall without having to know its IP address. This feature can be activated by selecting a dynamic DNS account that you would have configured earlier. The configuration of dynamic DNS clients will be explained further in the document (see *Part 5/Chapter 2: Dynamic DNS clients*).

Color definition

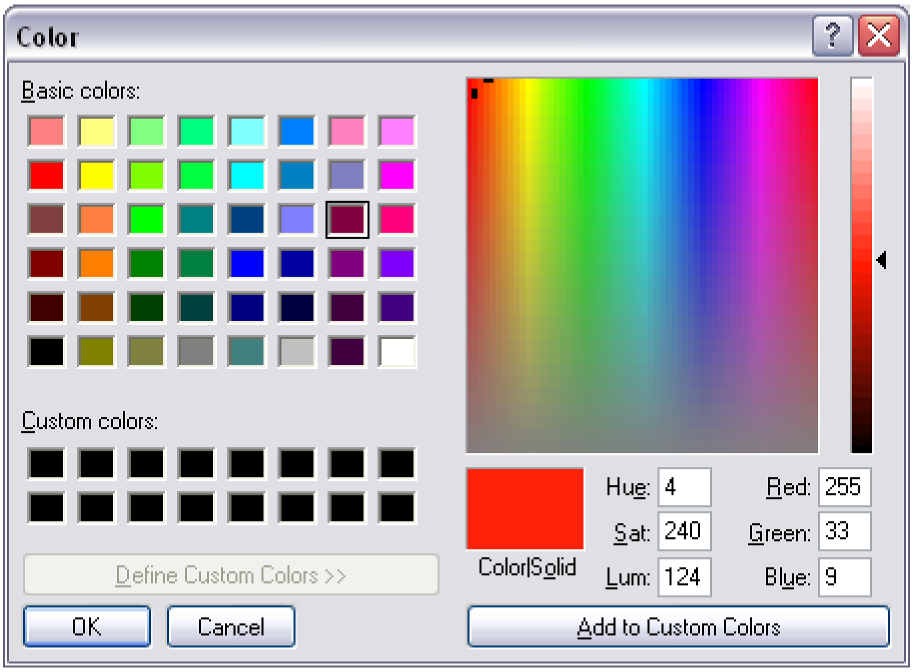
There is a specific color for each interface in the network configuration. All objects relating to an interface (computers or networks) will be in the color specified for this interface.



Name: bridge

Figure 72: Bridge color

Click on the colored rectangle indicated below the name of the interface to select a color. A window will appear, enabling you to select the color you want from among those predefined or you can specify your own (16 million colors).



Hue: 4

Sat: 240

Lum: 124

Red: 255

Green: 33

Blue: 9

Figure 73: Colors

Dynamic DNS client

The DNS service, based on exchanges between a server (maintained by a DNS service provider) and a client (integrated in NETASQ Firewalls), enables matching your Firewalls to a specific domain name. This allows you to contact these Firewalls even if you do not have a static public IP address or to use a domain name that's easy to remember instead of an IP address which is difficult to memorize.

DynDNS.org is currently the only DNS service provider that Firewalls support. Contact this provider to obtain an account which will allow you to set up this service on your Firewall.

➲ Dynamic DNS clients can be configured in the same way other interfaces are configured (bridge, interfaces in advanced mode, VLAN, Dialup) using the button **Edit Dynamic DNS clients**.

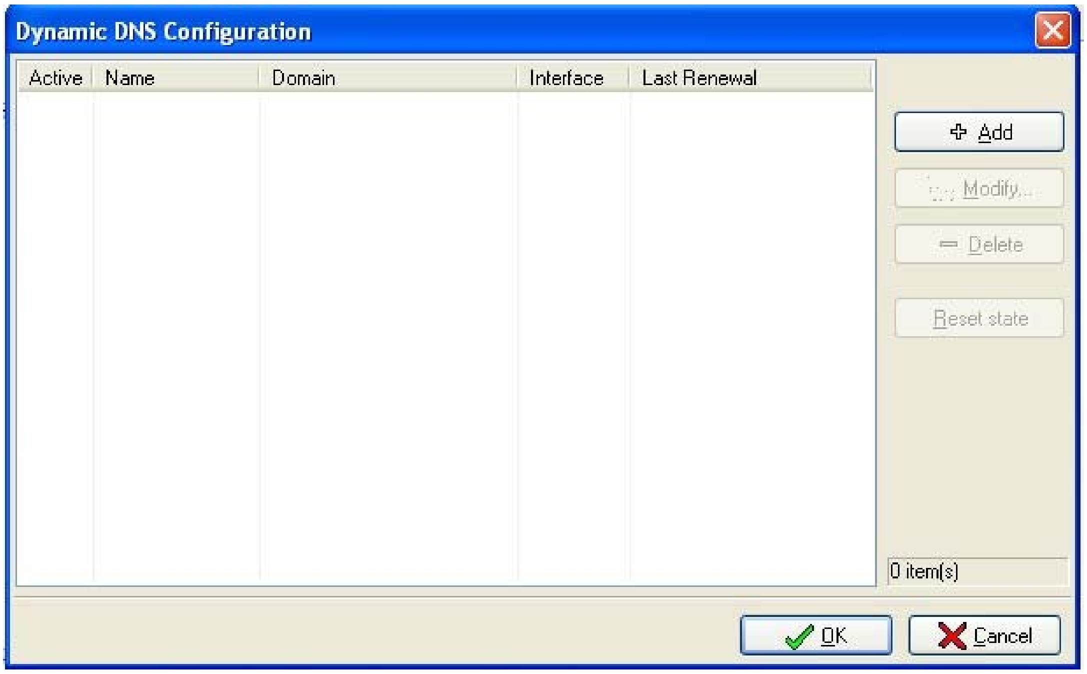


Figure 74: Dynamic DNS configuration

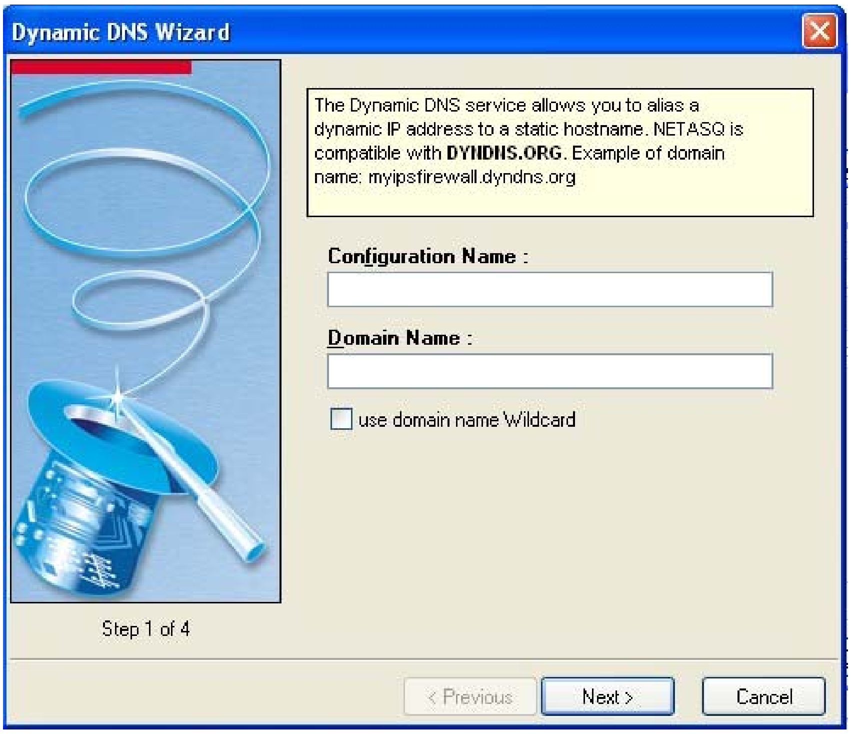
The information indicated on this window is as follows:

Active	If this option had been selected, the dynamic DNS configuration that has been created will be activated.
Name	Name associated to the dynamic DNS client configuration.
Domain	Domain name assigned to the dynamic DNS client. When the option **Use domain name wildcard** is activated, all sub-domains will be included. For example, if you specify **netasq.dyndns.org** in the “domain name” field, and the **Use domain name wildcard** option is selected, all the sub-domains (commerce.netasq.dyndns.org, lab.netasq.dyndns.org, etc) will be associated with the client.
Interface	Name of the network interface used in the link with the dynamic DNS client.
Last renewal	Date on which the DNS service was last updated.

Dynamic DNS clients are configured with a wizard.

➲ To add a new client to the list of configured dynamic DNS clients, click on the **Add** button in the dynamic DNS configuration window.

1 Step 1: General configuration



Dynamic DNS Wizard

The Dynamic DNS service allows you to alias a dynamic IP address to a static hostname. NETASQ is compatible with **DYNDNS.ORG**. Example of domain name: myipsfirewall.dyndns.org

Configuration Name :

Domain Name :

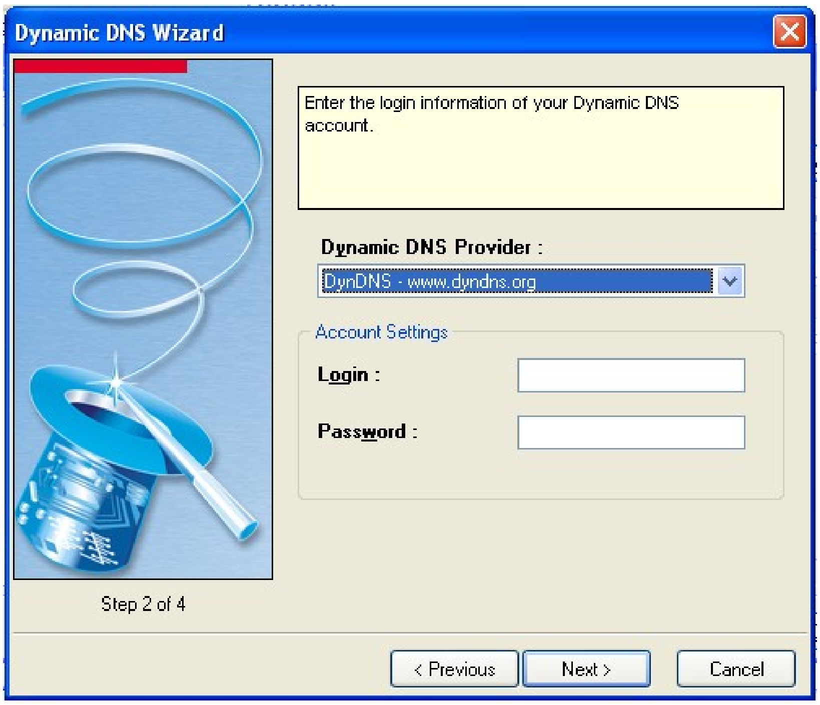
□ use domain name Wildcard

Figure 75: Dynamic DNS wizard - Step 1

Configuration name (mandatory): Name associated to the dynamic DNS client configuration. For example: *myfirewall.dyndns.org*.
Domain name: Domain name assigned to the dynamic DNS client.
Use domain name wildcard: to include all sub-domains.

2 Step 2: Provider and account settings

This window will allow you to enter the access parameters of your dynamic DNS service provider.



Dynamic DNS Wizard

Enter the login information of your Dynamic DNS account.

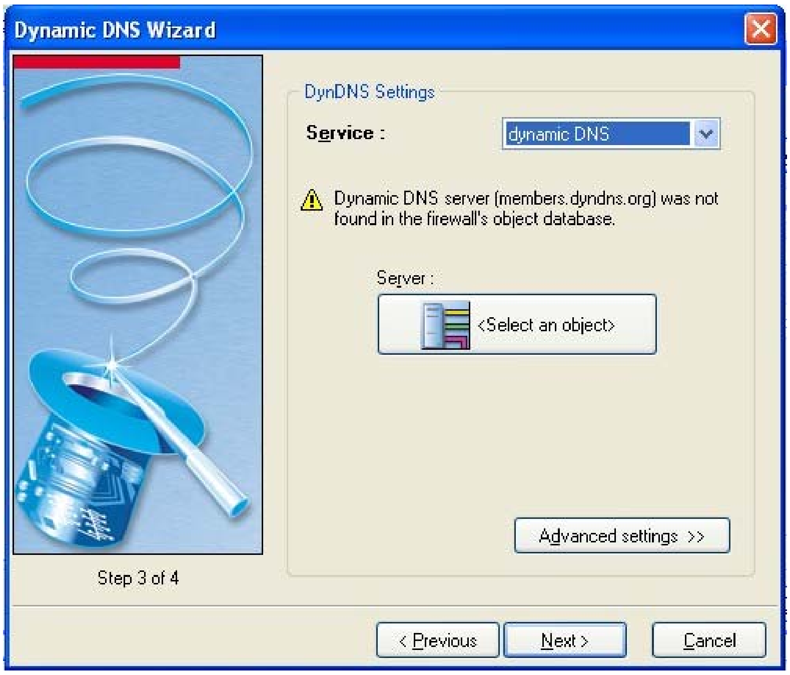
Dynamic DNS Provider : DynDNS - www.dyndns.org

Figure 76: Dynamic DNS wizard - Step 2

Dynamic DNS provider (mandatory): DNS service provider. Currently **DynDNS** is the only provider supported

Account settings: Login (mandatory) and password (mandatory) indicated by the DNS service provider for authenticating the dynamic DNS client.

3 Step 3: DynDNS settings



Dynamic DNS Wizard

DynDNS Settings

Service : dynamic DNS

Dynamic DNS server (members.dyndns.org) was not found in the firewall's object database.

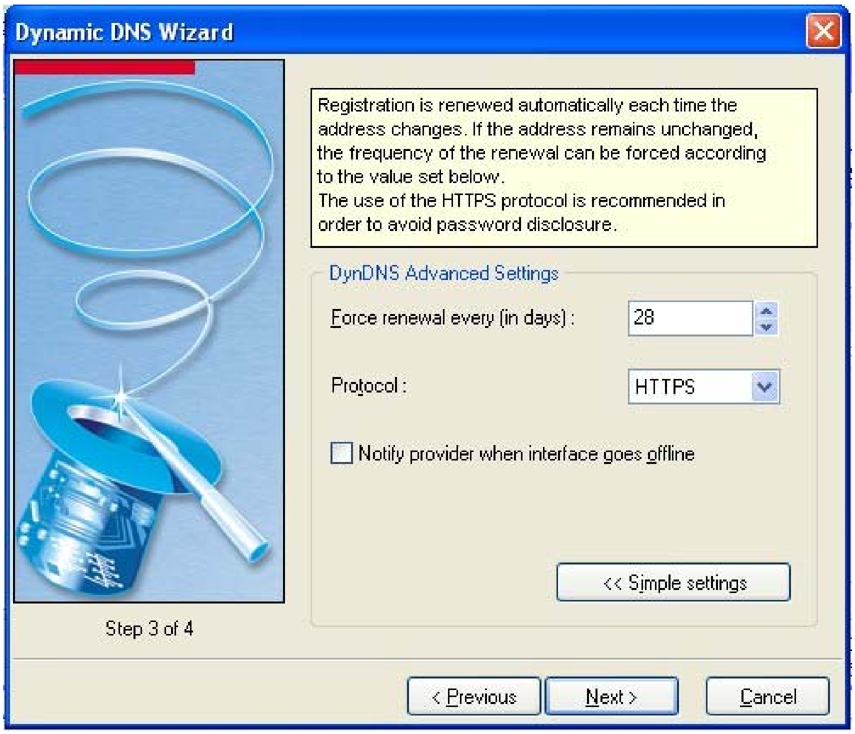
Server : <Select an object>

Figure 77: Dynamic DNS wizard - Step 3

Service: This option enables you to indicate the service that you have subscribed among the following: “Custom”, “Dynamic DNS” and “Static DNS”.

Server: DNS service provider’s server. The object to be specified in this field must be named “members.dyndns.org” in order to function with DynDNS.

In Step 3, the **Advanced settings** button will enable you to access the parameters for advanced configuration. In particular, they allow you to renew the registration of new addresses. The following window will appear when you click on the button:



Registration is renewed automatically each time the address changes. If the address remains unchanged, the frequency of the renewal can be forced according to the value set below.
The use of the HTTPS protocol is recommended in order to avoid password disclosure.

DynDNS Advanced Settings

Force renewal every (in days) : 28

Protocol : HTTPS

☐ Notify provider when interface goes offline

Figure 78: Dynamic DNS wizard - Step 3

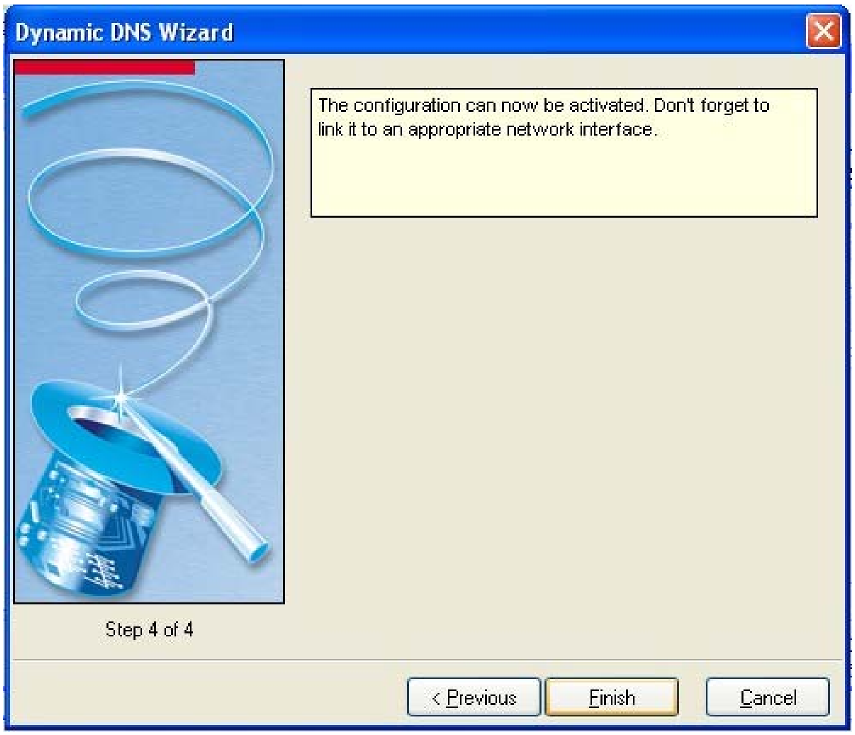
Force renewal every (in days): Renewal period of the dynamic DNS service. NETASQ has fixed this period at 28 days by default.

REMARK
Abusive renewals are penalized (by a closure of the account, for example), therefore **DynDNS** will not allow renewals made less than 26 days (after the first renewal). Also, if an account is not renewed after 35 days, it will be closed. However, the above information is subject to change as it is a **DynDNS**-established operation.

Protocol: Protocol used during the dynamic DNS service renewal phase. You can choose between HTTPS and HTTP.

Notify provider when interface goes Offline
This service, which **DynDNS** charges at a fee, enables redirecting traffic headed for your network to a specific page when your connection is inactive.

4 Step 4: Activation the configuration



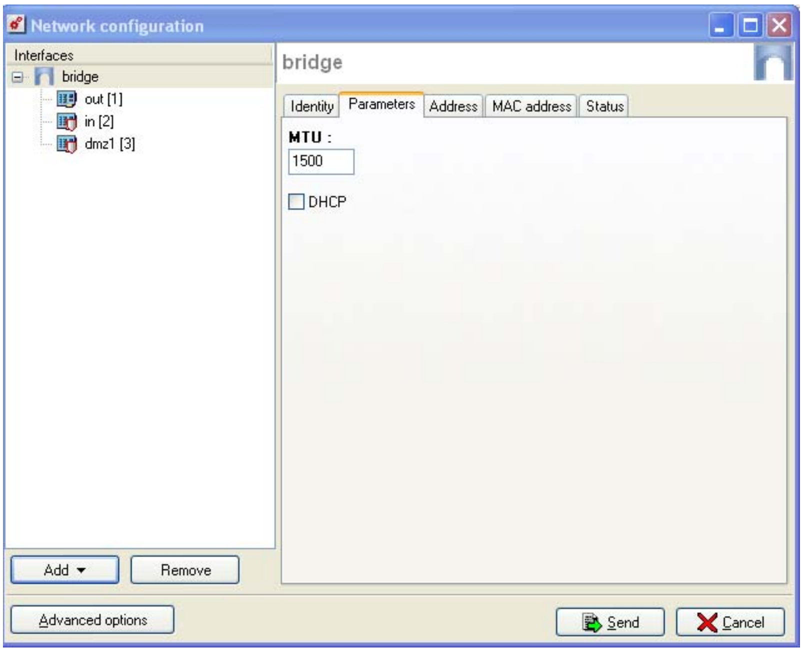
The configuration can now be activated. Don't forget to link it to an appropriate network interface.

Figure 79: Dynamic DNS wizard - Step 4

This window allows you to activate the configuration of the dynamic DNS client. To do so, click on **Finish**.

WARNING
Don’t forget to link this configuration to an appropriate network interface.

Parameters tab



MTU : 1500

□ DHCP

Figure 80: Bridge configuration – parameters

MTU	Maximum length of packets transmitted on the physical support (Ethernet).
DHCP	This field allows specifying to the Firewall that the bridge configuration (IP address and mask) is defined by DHCP. In this case, the **Address** tab becomes **DHCP**.

Address tab

This tab deals with the interface's address range. If the interface belongs to a bridge, this tab will not appear.
In this case, DHCP has not been checked, and the tab has an "Address/Mask" table, the buttons **Add/Delete** and a "Description" column.

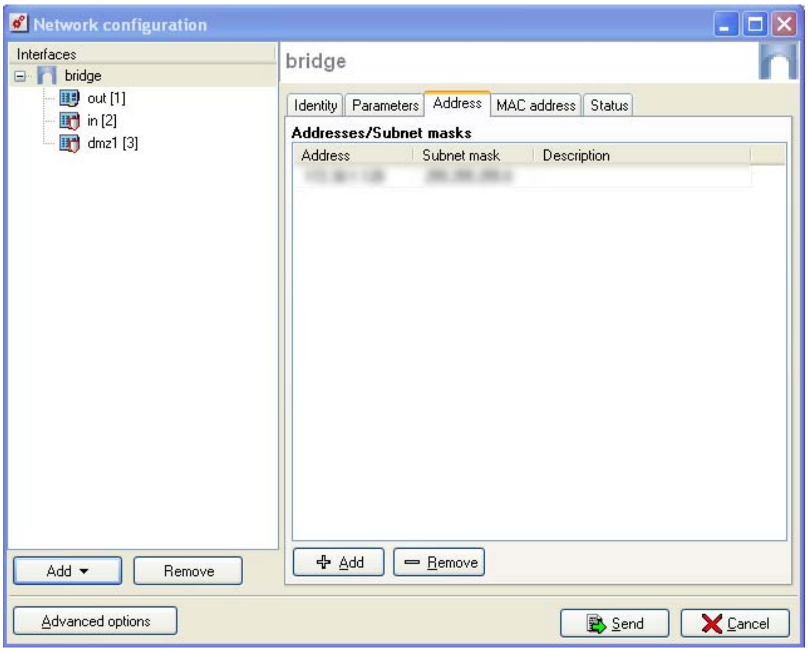


Figure 81: Bridge configuration - Address

IP Address	Bridge IP address. (All the interfaces on the bridge have the same IP address).
Subnet mask	Network mask of the sub-network to which the bridge belongs. The different interfaces which are part of the bridge have the same IP address, therefore all networks connected to the Firewall are part of the same addressing range. The network mask gives the Firewall information on the network it is on.
Description	Allows you to add a comment on the bridge addressing.

In this tab, several IP address and associated network masks may be defined for the same bridge (the need to create aliases, for example). These aliases may allow you to use the NETASQ Firewall as a central routing point. Therefore a bridge may be connected to different sub-networks having different address ranges. To add or remove them, you just need to use the action buttons under the IP address and Netmask fields.

MAC address tab

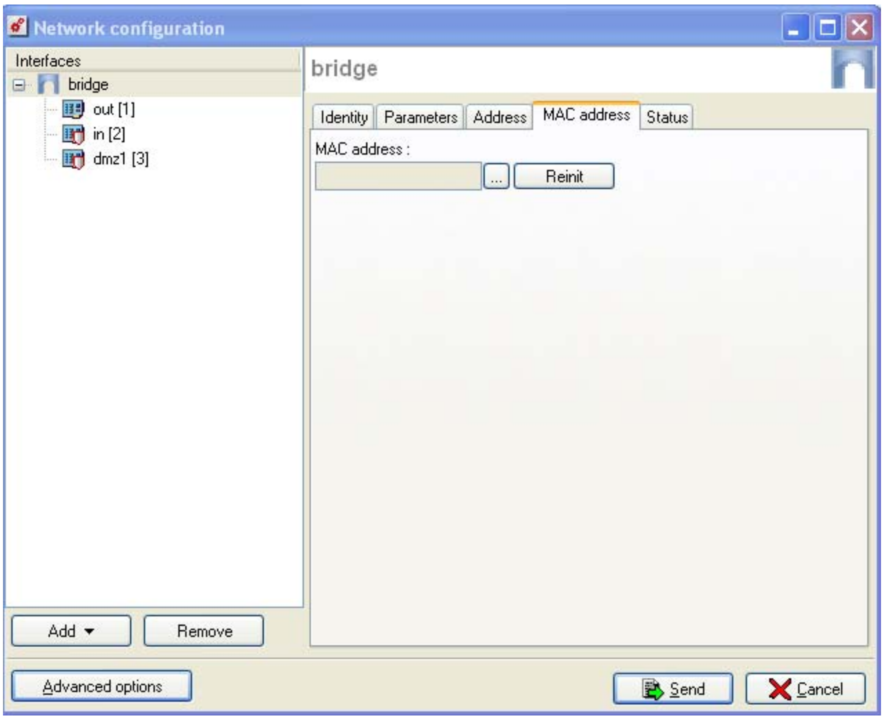


Figure 82: Bridge configuration – MAC address

WARNING
This option is not available for Firewalls in high availability.

This window allows you to specify a MAC address for an interface instead of using the address assigned by the Firewall. This allows you to better facilitate the integration of the NETASQ Firewall in transparent mode into your network (by specifying your router's MAC address instead of having to reconfigure all the workstations using this MAC address).

MAC address MAC address assigned to the bridge (all interfaces contained in the bridge therefore have the same MAC address).

To change the MAC address, click on the button ... . The window below will appear:

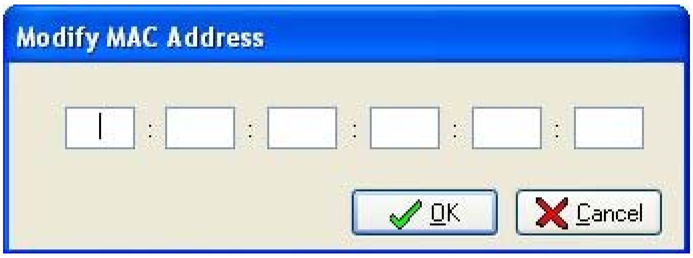


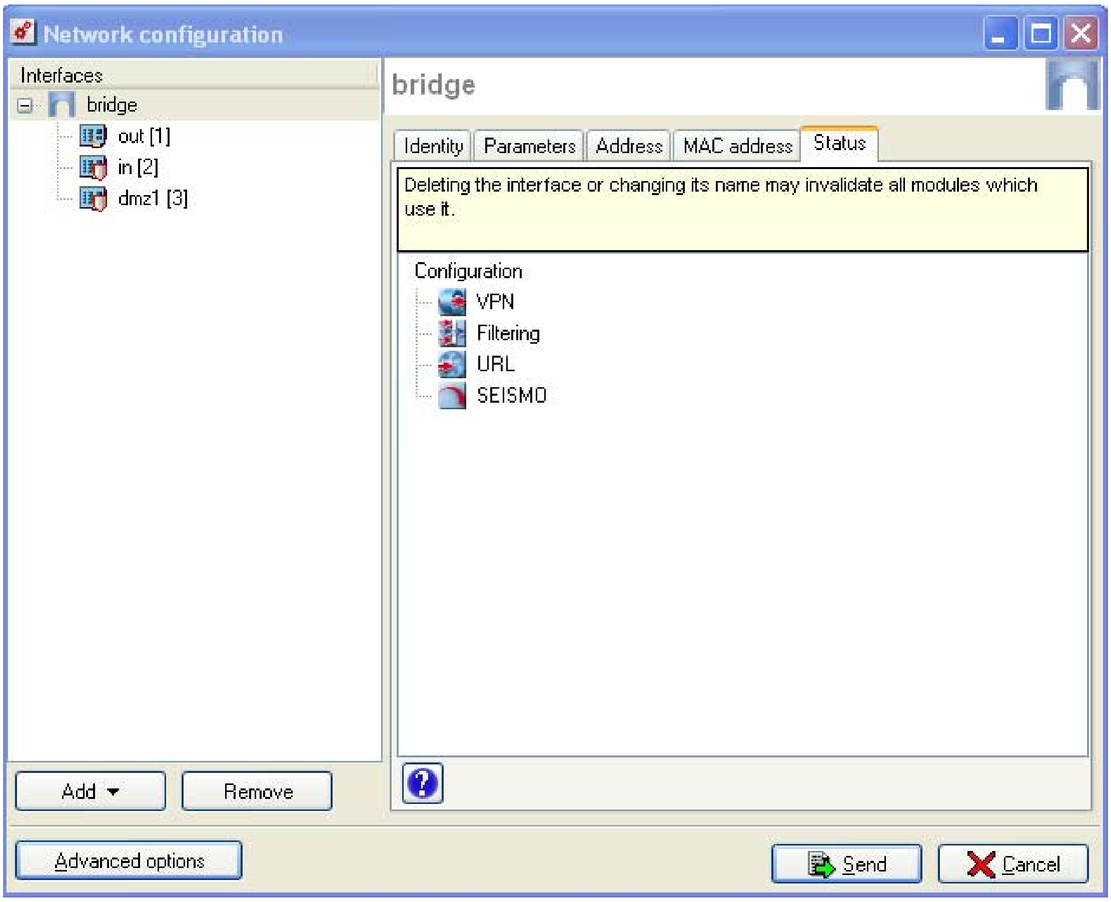
Figure 83:Modifying the MAC address

Reinit Reinitialization of the MAC address field.

NOTE
This tab will be hidden when the interface belongs to a bridge.

Status tab

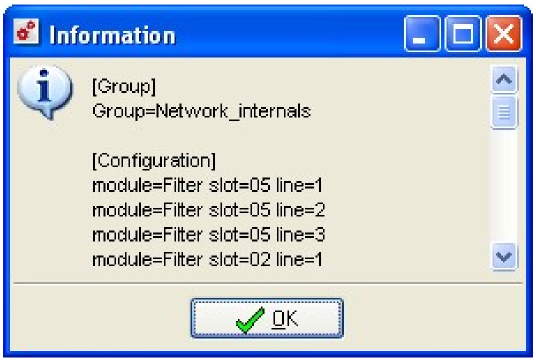
The **`Status`** tab enables viewing in real time where the interface is used and all the objects and object groups generated by the interface (Network_xx, Firewall_xx) in the configuration of the UTM appliance. This tab will prove useful whenever changes are made to this interface.



Deleting the interface or changing its name may invalidate all modules which use it.

Figure 84: Bridge configuration - Status

By clicking on the button ?, you will get a more detailed view of how the interface is used, module by module, line by line.



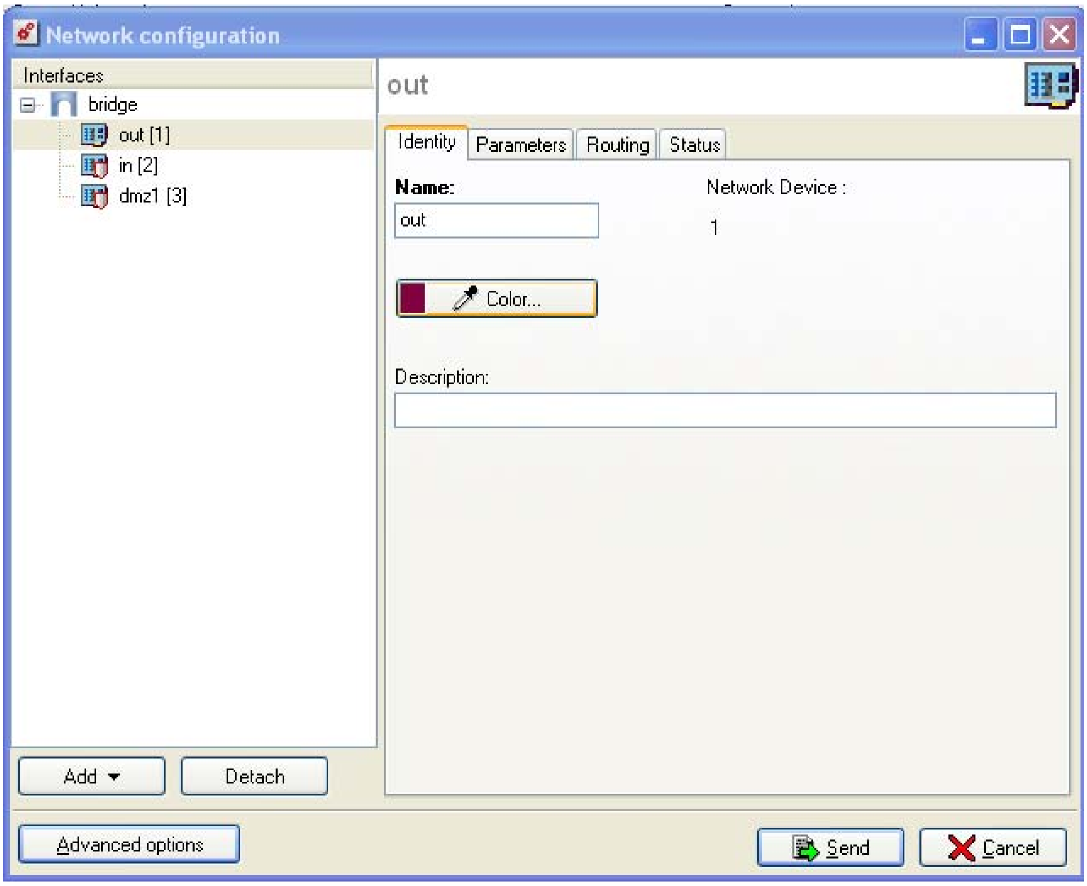
```
[Group]
Group=Network_internals

[Configuration]
module=Filter slot=05 line=1
module=Filter slot=05 line=2
module=Filter slot=05 line=3
module=Filter slot=02 line=1
```

Figure 85: Information

5.2.4.3. Bridge interface parameters

Interfaces that belong to a bridge are represented in the form of child nodes in relation to the bridge. A bridge can therefore contain several child nodes.
You can change the parameters of each interface on the bridge. To do so select an interface locatedin a bridge on the left-hand side of the window. Four tabs will then appear:

Identity tab



Name: out

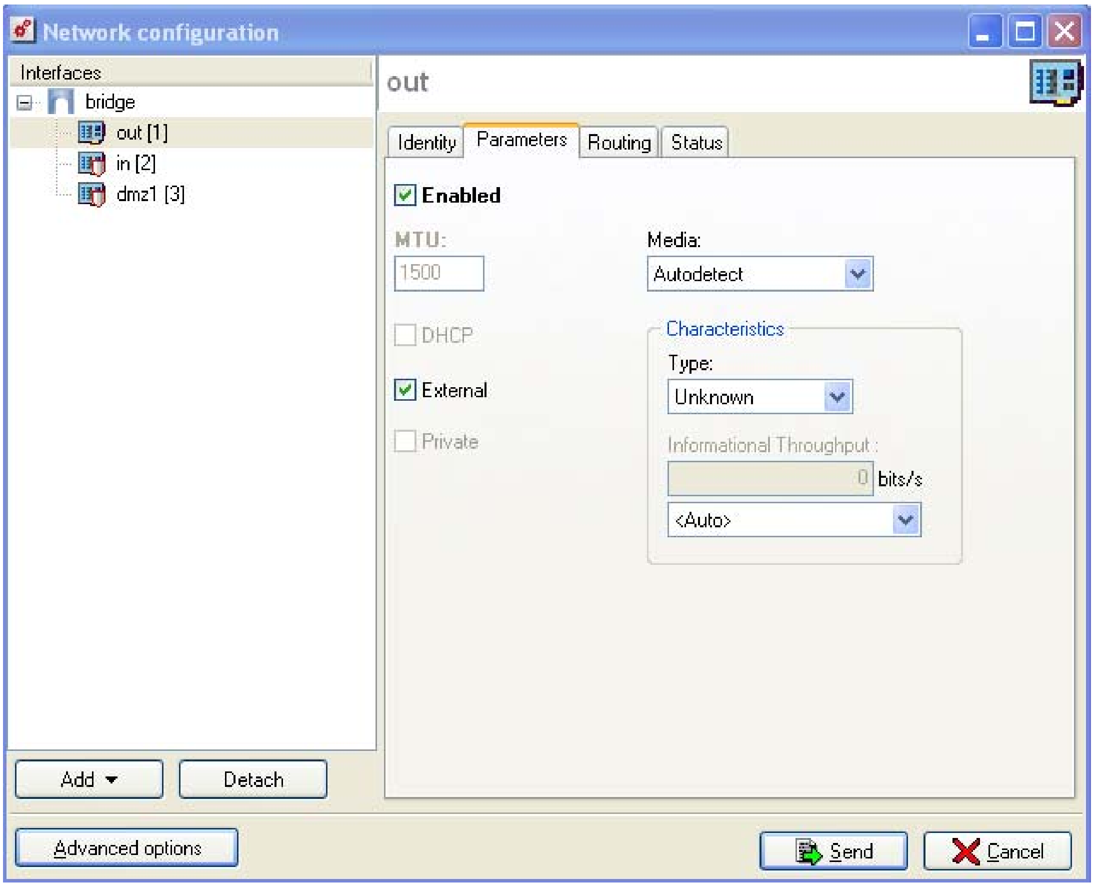
Network Device : 1

Description:

Figure 86: Configuration - Out Interface - Identity

Name (mandatory)	Name of the bridge (see *Appendix M: Prohibited names*)
Network device	Number of the network peripheral
Color	Interface color. These colors are very useful when you are installing the filter rules, translations etc. Each object created takes on a color, depending on the zone to which the IP address belongs.
Description	Allows you to add a comment for the interface.

Parameters tab



☑ Enabled

MTU: 1500

Media: Autodetect

□ DHCP

☑ External

□ Private

Type: Unknown

Informational Throughput : 0 bits/s

<Auto>

Figure 87: Configuration - Out Interface - Parameters

Enabled By checking/unchecking this option, the interface is activated/deactivated. By deactivating an interface, it becomes unusable. In terms of use, this may correspond to an interface to be used in the near or distant future, but is not active. An interface which has been deactivated because it is not in use is an example of an additional security measure against intrusions.

MTU Maximum length of packets transmitted on the physical support (Ethernet). This selection is not available for an interface on a bridge.

DHCP The interface's IP address is provided by a DHCP server (useful for internet connections via cable) (see *Part 11/Chapter 1: DHCP).* This selection is not available for an interface on a bridge (in which case, it will be grayed out).

External Check this option to indicate that this section of the network is connected to the internet. In most cases, the external interface, linked to the internet, should be in external mode. The interface's security (materialized by a shield) disappears when this option is checked.

Private This option allows indicating whether the interface is private. Addresses of "private" interfaces cannot be used as destinations for packets coming from unprotected interfaces, except if they have been translated.

NOTE
You will notice that "private" implies being on a protected interface. Therefore the options External and Private are incompatible.

Media Connection speed of internal network. By default the Firewall detects this automatically but you can enforce the use of a particular mode. The different speeds available are: "Automatic detection", "10 Mb Half duplex", "10 Mb Full duplex", "100 Mb Half duplex", "100 Mb Full duplex", "1 Gb Half duplex", "1 Gb Full duplex".

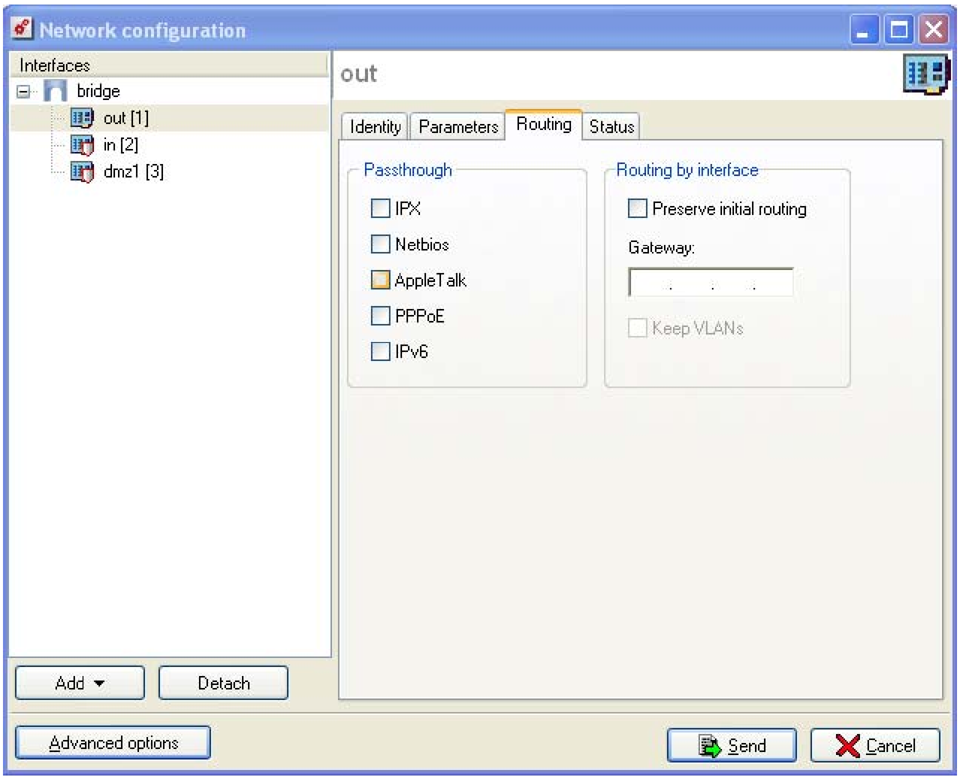
WARNING
If the Firewall is directly connected to an ADSL modem, you are advised to enforce the medium that you wish to use on the interface concerned.

Type This option defines the type of host hosted on this interface. **Host** = host computers (users) and **Unknown** = unidentified host type. The logs will show you what type of traffic is passing through the Firewall.

Informational throughput By specifying the internet link type, it is possible to define a maximum throughput. However this information is not used for regulating traffic, it merely defined the graph scale for Monitor.

Routing tab

This tab deals with routing by interface.



Passthrough
☐ IPX
☐ Netbios
☐ AppleTalk
☐ PPPoE
☐ IPv6

Routing by interface
☐ Preserve initial routing
Gateway: . . .
☐ Keep VLANs

Figure 88: Configuration - Out Interface– Routing

Passthrough Allows letting IPX (Novell network), Netbios (on NETBEUI), AppleTalk (for Macintosh), PPPoE or Ipv6 packets pass between the bridge's interfaces. No higher level analysis or filtering is carried out on these protocols (the Firewall blocks or allows it to pass).

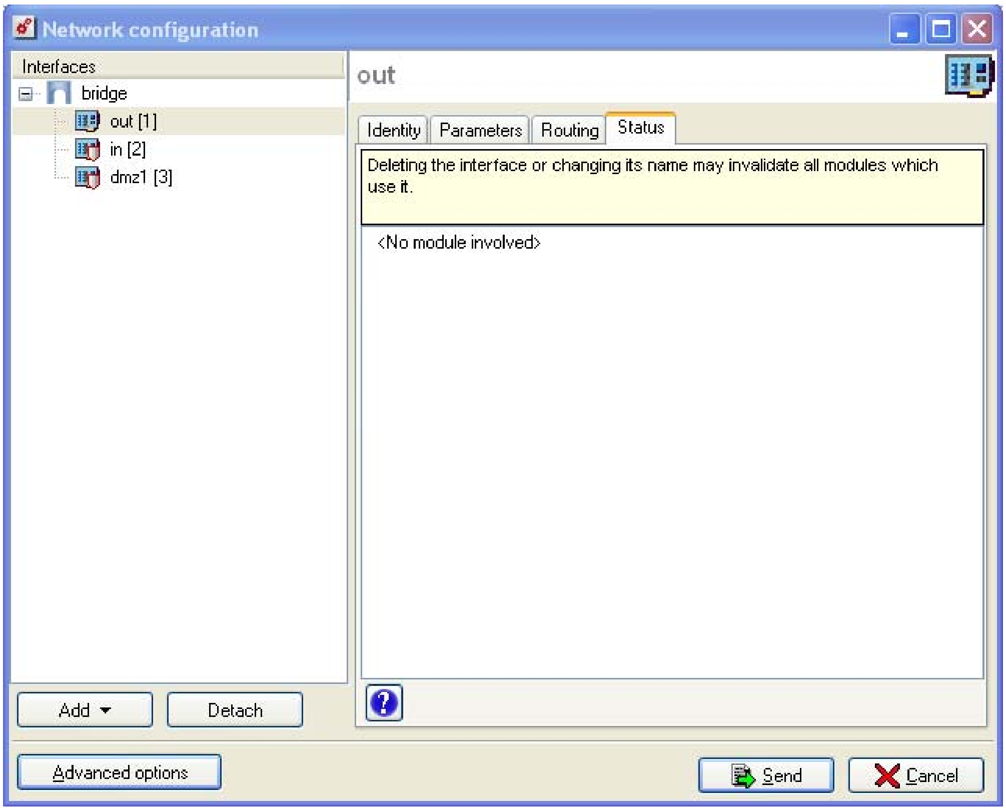
Routing As its name indicates, the **Preserve initial routing** option allows preserving the initial routing for hosts connected on this interface. As such, you may specify a default gateway for certain machines while specifying a gateway on the Firewall for hosts which do not have one. This option facilitates the Firewall's integration into an architecture comprising many different gateways.

The **Gateway** field is used for routing by interface. All packets that arrive on this interface will be routed via a gateway.

The option **Keep VLANs** enables the transmission of tagged frames without the firewall having to be the VLAN ending. The VLAN tag on these frames are kept so that the Firewall can be placed in the path of a VLAN without the Firewall interrupting this VLAN. The Firewall functions in a fully transparent manner to the VLAN.

Status tab

The **`Status`** tab enables viewing in real time where the interface is used and all the objects and object groups generated by the interface (Network_xx, Firewall_xx) in the configuration of the UTM appliance. This tab will prove useful whenever changes are made to this interface.



Deleting the interface or changing its name may invalidate all modules which use it.

<No module involved>

Figure 89: Configuration – Out interface – Status

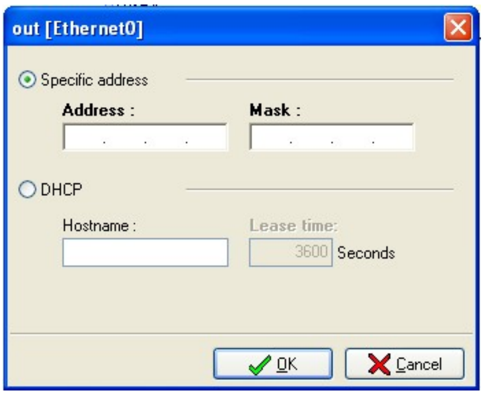
By clicking on the button ?, you will get a more detailed view of how the interface is used, module by module, line by line.

WARNING
Deleting the interface or changing its name will affect all the configurations that use it.

5.2.4.4. Interface in advanced mode

To configure an interface in a network which is not part of a bridge you need to take it out of the bridge tree with the mouse or by clicking on the right hand button when the interface is selected and by selecting **`Unlink`**. You may then configure the following interface parameters:

During detachment, the following window will appear:



out [Ethernet0]

● Specific address

Address : . . .

Mask : . . .

○ DHCP

Hostname :

Lease time: 3600 Seconds

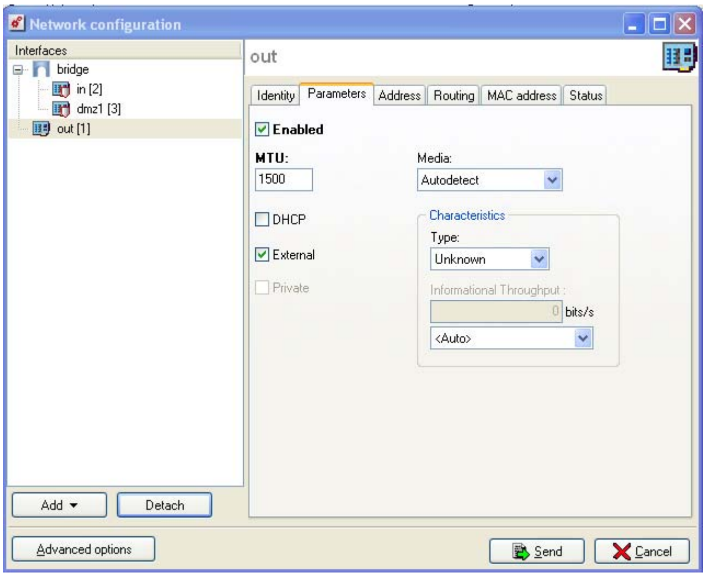
Figure 90: Out (Ethernet)

Specific address	Indicates an IP address on your interface as well as the subnet mask.
DHCP	Indicates a host name and a lease time.

Identity tab

The configuration window is the same as the one on the interface in Bridge mode.

Parameters tab



Network configuration

Interfaces
- bridge
  - in [2]
  - dmz1 [3]
- out [1]

out

☑ Enabled

MTU: 1500

Media: Autodetect

☐ DHCP

☑ External

☐ Private

Characteristics

Type: Unknown

Informational Throughput : 0 bits/s

<Auto>

Figure 91: Configuration - Parameters

Enabled	By checking/unchecking this option, the interface is activated/deactivated. By deactivating an interface, it becomes unusable. In terms of use, this may correspond to an interface to be used in the near or distant future, but is not active. An interface which has been deactivated because it is not in use is an example of an additional security measure against intrusions.
MTU	Maximum length of packets transmitted on the physical support (Ethernet). This selection is not available for an interface on a bridge.
DHCP	The interface's IP address is provided by a DHCP server (useful for internet connections via cable) (see *Partie 11/Chapitre 1: DHCP*). This selection is not available for an interface on a bridge (in which case, it will be grayed out).
External	Check this option to indicate that this section of the network is connected to the internet. In most cases, the external interface, linked to the internet, should be in external mode. The interface's security (materialized by a shield) disappears when this option is checked.
Private	This option allows indicating whether the interface is private. Addresses of "private" interfaces cannot be used as destinations for packets coming from unprotected interfaces, except if they have been translated. NOTE You will notice that "private" implies being on a protected interface. Therefore the options External and Private are incompatible.
Media	Connection speed of internal network. By default the Firewall detects this automatically but you can enforce the use of a particular mode. The different speeds available are: "Automatic detection", "10 Mb Half duplex", "10 Mb Full duplex", "100 Mb Half duplex", "100 Mb Full duplex", "1 Gb Half duplex", "1 Gb Full duplex". WARNING If the Firewall is directly connected to an ADSL modem, you are advised to enforce the medium that you wish to use on the interface concerned.
Type	This option defines the type of host hosted on this interface. **Host** = host computers (users) and **Unknown** = unidentified host type. The logs will show you what type of traffic is passing through the Firewall.
Informational throughput	By specifying the internet link type, it is possible to define a maximum throughput. However this information is not used for regulating traffic, it merely defined the graph scale for Monitor.

Address tab

NOTE

Available only if the DHCP option has not been selected.

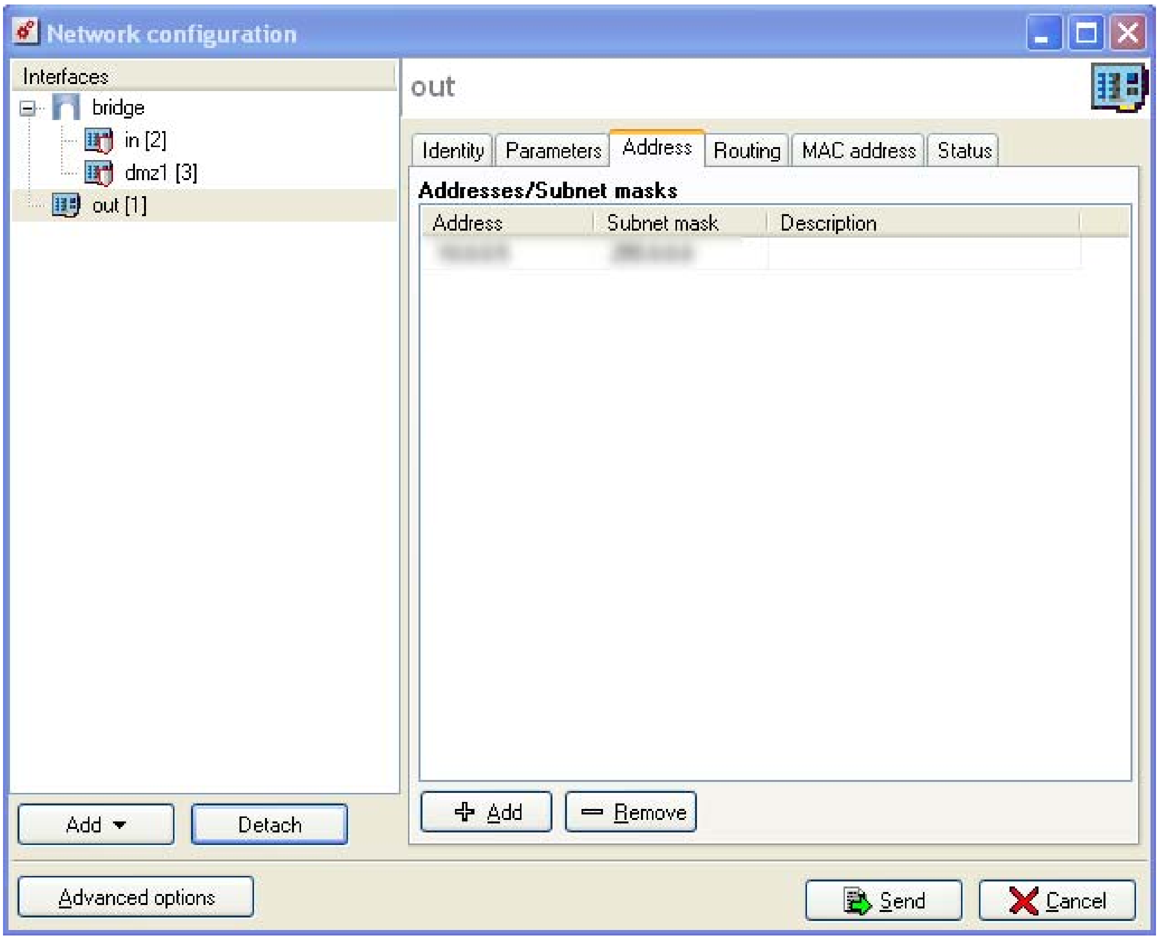
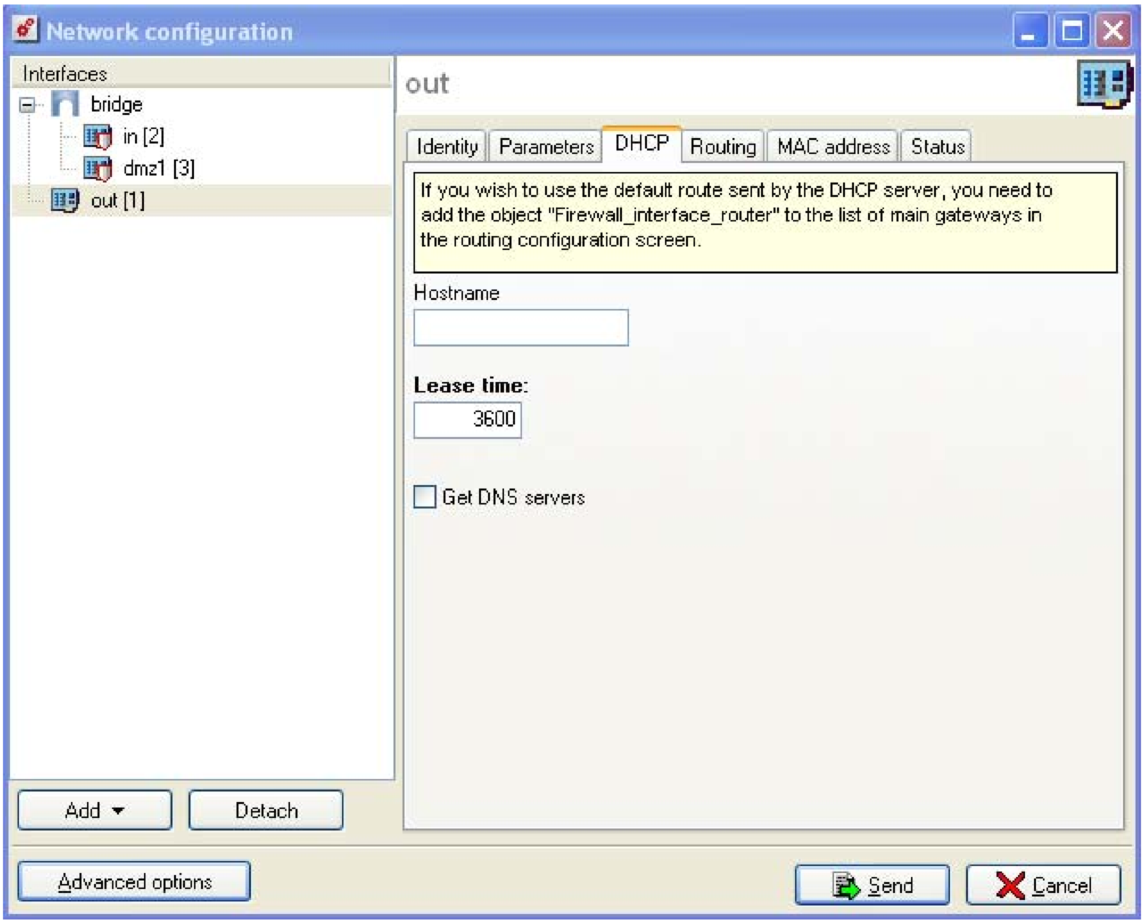


Figure 92: Configuration - Address

IP Address	IP address assigned to the interface.
Netmask	Network mask of the sub-network to which the bridge belongs. If the **DHCP** option has been selected, the **Address** tab becomes a **DHCP** tab (see Part 11/Chapter 1: *DHCP*).
Description	Enables adding a comment for the bridge address

DHCP Tab

NOTE
Available only if the DHCP option has been selected.



If you wish to use the default route sent by the DHCP server, you need to add the object "Firewall_interface_router" to the list of main gateways in the routing configuration screen.

Hostname

Lease time: 3600

□ Get DNS servers

Figure 93: Configuration - DHCP

Hostname	User name (FQDN) for the connection. This optional field does not identify the DHCP server but the Firewall. If this field has been entered and the external DHCP server has the option of automatically updating the DNS server, the DHCP server will automatically update the DNS server with the name and the IP address provided by the Firewall.
Lease time	Period during which the IP address is kept before renegotiation.

Get default route

Indicates that the interface in DHCP is connected to the Firewall's default route. If this option has been checked, the Firewall will receive its default route from the DHCP server (access provider, for example). It will then replace the default route that has already been configured.

It is still necessary to manually configure a default route in the Firewall in order to maintain the appliance's stability, particularly in obtaining its IP address from the DHCP server.

REMARK

In order to use the default route that the DHCP server sent, you will need to add the object Firewall_interface_router to the list of main gateways in the routing configuration window. For example, if the "OUT" interface has been configured in DHCP, the object that corresponds to the default route will be named "Firewall_out_router".

Get DNS servers

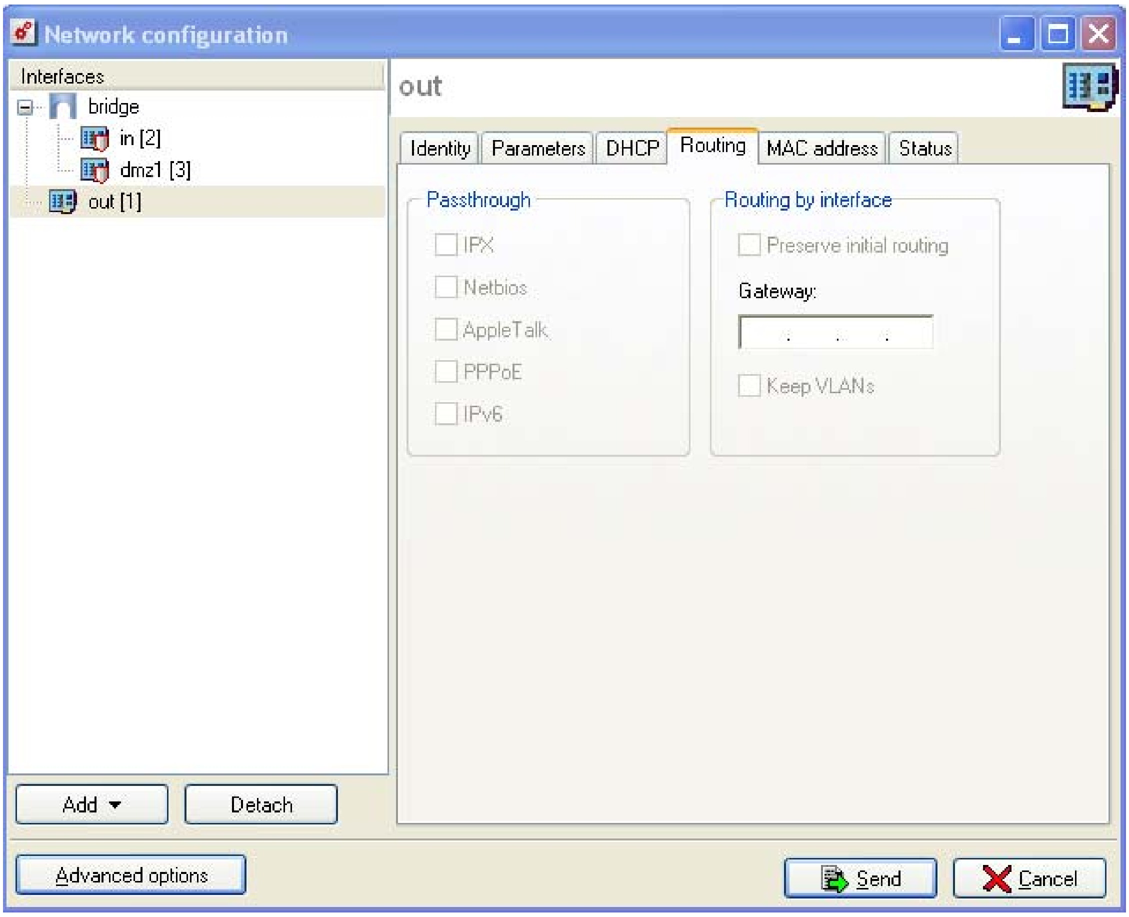
When this option is selected, the Firewall will retrieve DNS servers from the DHCP server it contacts (access provider, for example) to obtain its IP address.

Two objects will be dynamically created in the object database upon the selection of this option: Firewall_<interface name>_dns1 and Firewall_<interface name_dns2. They can then be used in the configuration of the DHCP service. So, if the Firewall provides the users on its network with a DHCP service, the users will also benefit from the DNS servers given by the access provider.

TIP

In order to use the default route that the DHCP server sent, you will need to add the object Firewall_interface_router to the list of main gateways in the menu `Routing`**,** `Advanced tab` in the NETASQ UNIFIED MANAGER menu directory. For example, if the "Out" interface has been configured in DHCP, the object that matches the default route will be called "Firewall_out_router".

Routing tab



Passthrough

☐ IPX

☐ Netbios

☐ AppleTalk

☐ PPPoE

☐ IPv6

Routing by interface

☐ Preserve initial routing

Gateway: . . .

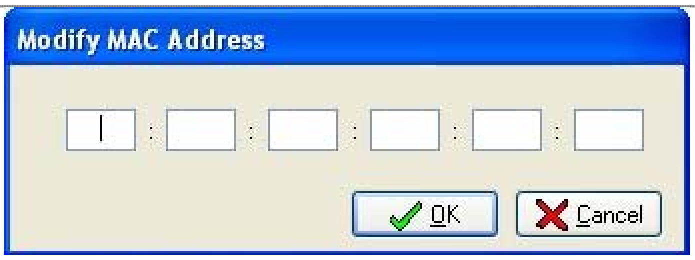
☐ Keep VLANs

Figure 94: Configuration of interfaces - Routing

Passthrough	Allows letting IPX (Novell network), Netbios (on NETBEUI), AppleTalk (for Macintosh), PPPoE or Ipv6 packets pass between the bridge's interfaces.
Routing	As its name indicates, the "preserve initial routing" option allows preserving the initial routing for hosts connected on this interface. The "gateway" field is used for routing by interface.
Keep VLANs	The option **Keep VLANs** enables the transmission of tagged frames without the firewall having to be the VLAN ending. The VLAN tag on these frames are kept so that the Firewall can be placed in the path of a VLAN without the Firewall interrupting this VLAN. The Firewall functions in a fully transparent manner to the VLAN.

MAC address tab

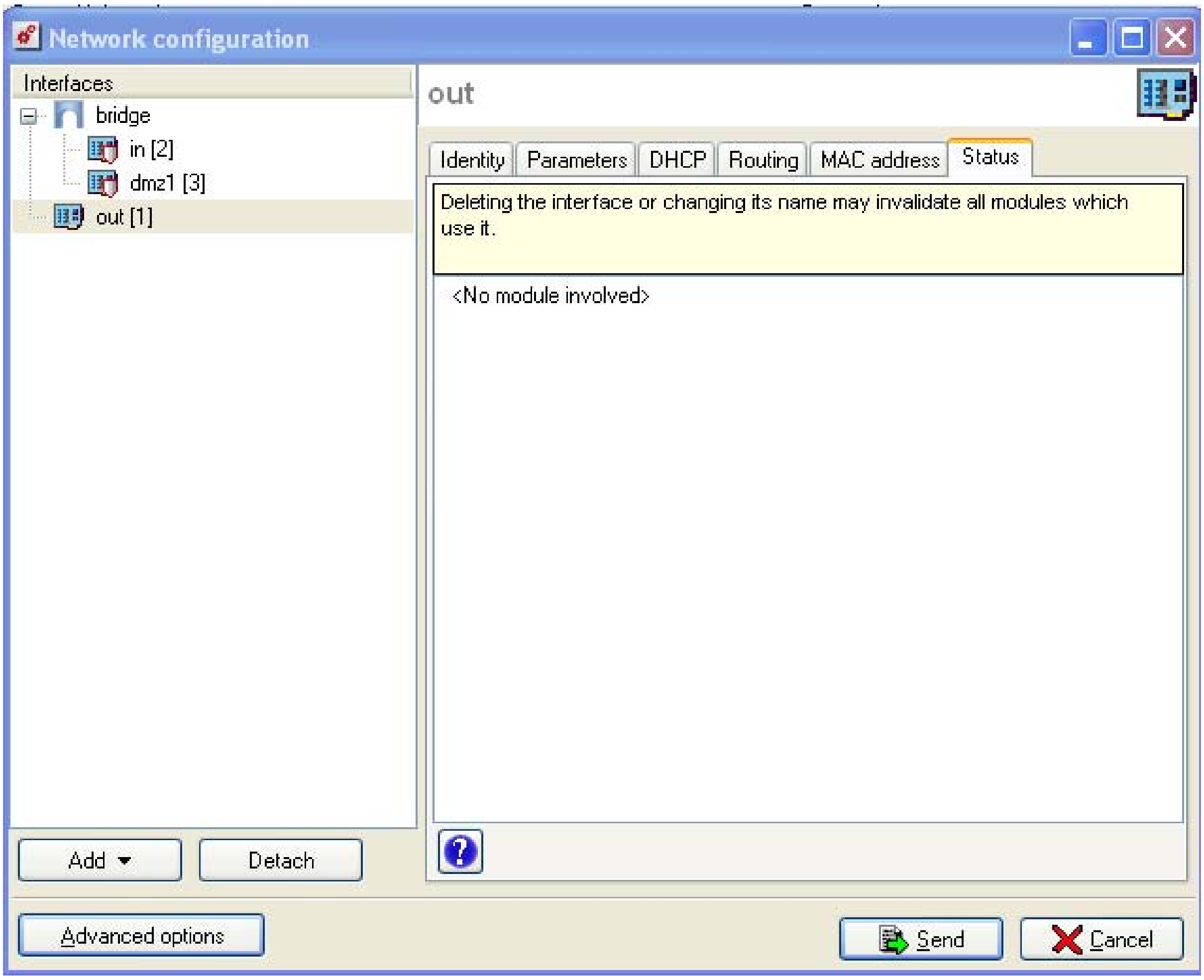
MAC address	MAC address assigned to the bridge (all interfaces contained in the bridge therefore have the same MAC address). To change the MAC address, click on the button … . The following window will appear:



Reinit	Reinitialization of the MAC address field.

Status tab

The **`Status`** tab enables viewing in real time where the interface is used and all the objects and object groups generated by the interface (Network_xx, Firewall_xx) in the configuration of the UTM appliance.



Deleting the interface or changing its name may invalidate all modules which use it.

<No module involved>

Figure 95: Configuration – Out interface – Status

By clicking on the button ?, you will get a more detailed view of how the interface is used, module by module, line by line.

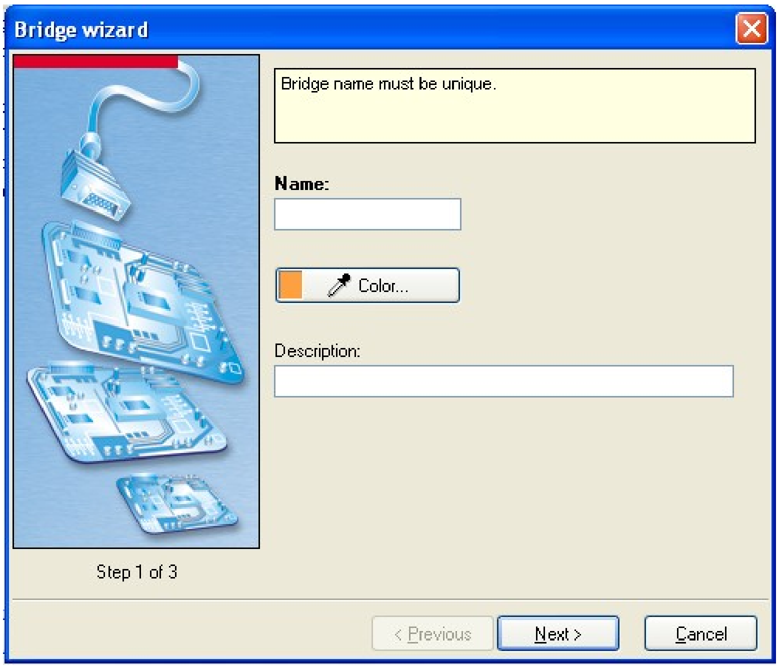
WARNING
In order to use the default route that the DHCP server sent, you will need to add the object Firewall_interface_router to the list of main gateways in the menu `Routing`, *`Advanced tab`* in the NETASQ UNIFIED MANAGER menu directory.

5.2.5. Creating a bridge

Bridges are created using a wizard that would allow you to create the interface easily.

1 Select the menu `Network\Interfaces` from the configuration interface.

2 Click on **Add** then select “Bridge" or right-click on the configuration menu directory and select "New bridge".
The window below will appear:



Bridge wizard

Bridge name must be unique.

Name:

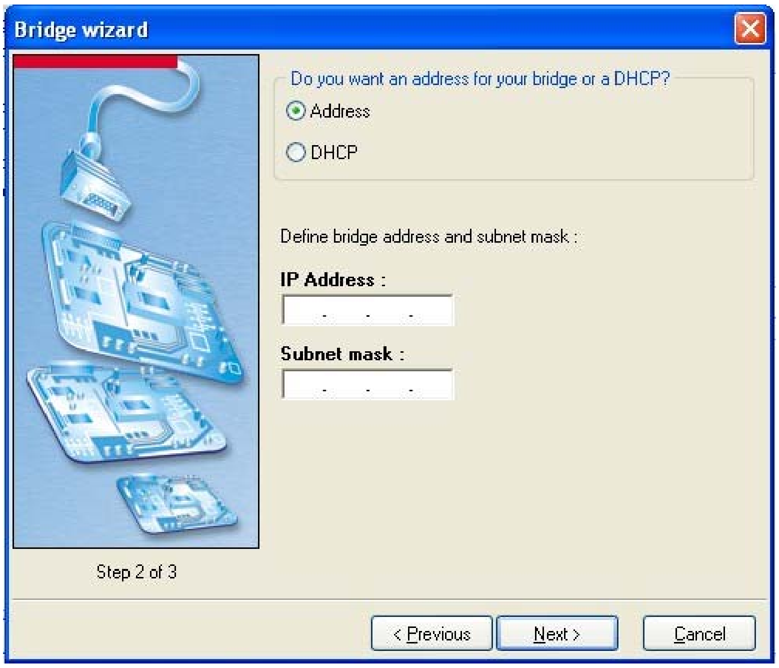
Color...

Description:

Step 1 of 3

Figure 96: Bridge wizard - Step 1

3 Enter a unique name for your bridge and define a color for it. You can also enter a description if desired. Click on **Next**. (The fields in bold are mandatory). The following window will appear:



Bridge wizard

Do you want an address for your bridge or a DHCP?

● Address

○ DHCP

Define bridge address and subnet mask :

IP Address : . . .

Subnet mask : . . .

Step 2 of 3

Figure 97: Bridge wizard - Step 2

4 If you select “Address”, indicate the bridge’s address and subnet mask. If you select “DHCP”, indicate a hostname and an allocated time (mandatory). Click on “Next”. The following window will appear:

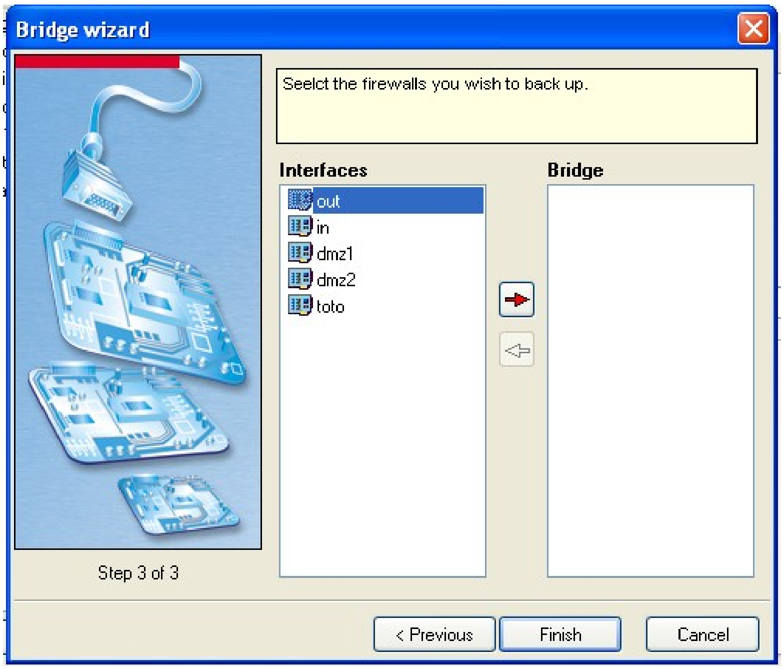


Figure 98: Bridge wizard - Step 3

5 Select the firewalls whose configurations you wish to back up. The “Interfaces” list will set out all Ethernet and VLAN interfaces already preent in the configuration. At least two interfaces will have to be selected to make a bridge, either by using arrows or by dragging and dropping between both lists. Click on **Finish** to confirm the creation of the bridge.

5.2.6. Creating a VLAN

5.2.6.1. Presentation of VLANs

A local network (LAN) is based on the principle of broadcasting. Each datum transmitted by equipment connected to the LAN is received by all the others.

With the increase in the number of terminals attached to the LAN we sometimes reach saturation points. The more terminals there are, the greater the risk of collisions.

DEFINITION
Virtual networks (VLAN: Virtual Local Area Network) enable us to establish networks based on the company's organization. They introduce the notion of virtual segmentation, which allows the construction of logical 'watertight' sub-networks within a network architecture. The VLANs, therefore, are logical groups of users or terminals (which may represent the operational organization of the company). All members of a VLAN can communicate together and form a broadcasting area.

VLANs are defined by an Ethernet frame tag (standard 802.1q). We can therefore define the broadcast areas. Exchanges within an area are automatically secured because VLANs are watertight and inter-area communications can be controlled by a Level 3 bridge such as a firewall.

NETASQ Firewalls can be placed at the end of VLANs to add or remove a VLAN tag. The Firewall carries out the filtering between the VLANS and the networks connected to the other Firewall interfaces.

The Firewall recognizes the VLANs as belonging to virtual interfaces, which enables them to be fully integrated into the company's security system.

5.2.6.2. Advantage of a VLAN

The VLAN allows the following:

- Improved performance, by limiting broadcast domains while increasing them.
- A user who moves can find the same access rights to LAN resources without the intervention of the operator.

5.2.6.3. Defining VLANs

With a NETASQ Firewall, port VLANs or VLAN IP bridges can be created.

WARNING
In order to use VLAN interfaces on the Firewall it is essential to have equipment to manage the VLANs on your network (switches).

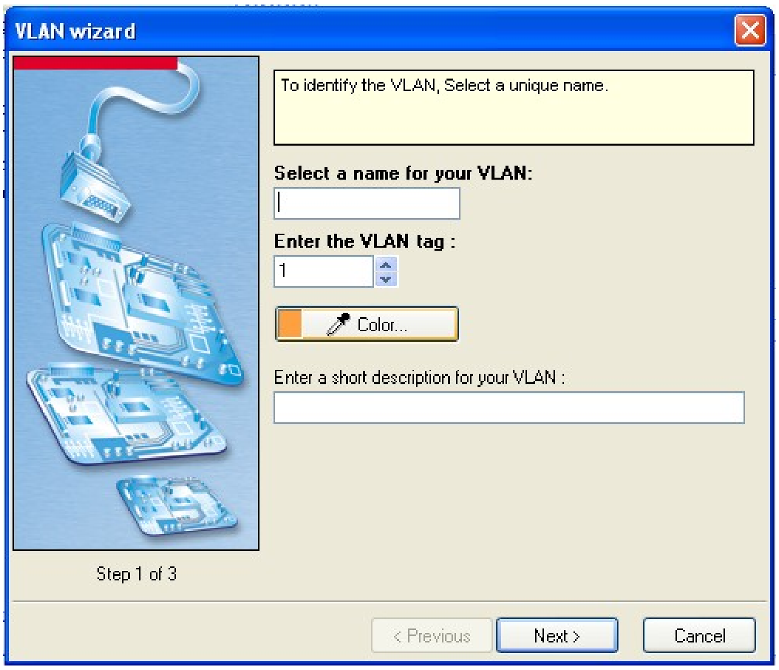
VLANs are configured through a wizard that allows you to create the interface easily.

1 Select the menu `Network\Interfaces` in the configuration interface.

2 Select the interface or bridge you wish to associate with a VLAN.

3 Click on **Add** and select `VLAN on…` or right-click and select `New VLAN` in the contextual menu.

4 The following window will appear:



VLAN wizard

To identify the VLAN, Select a unique name.

Select a name for your VLAN:

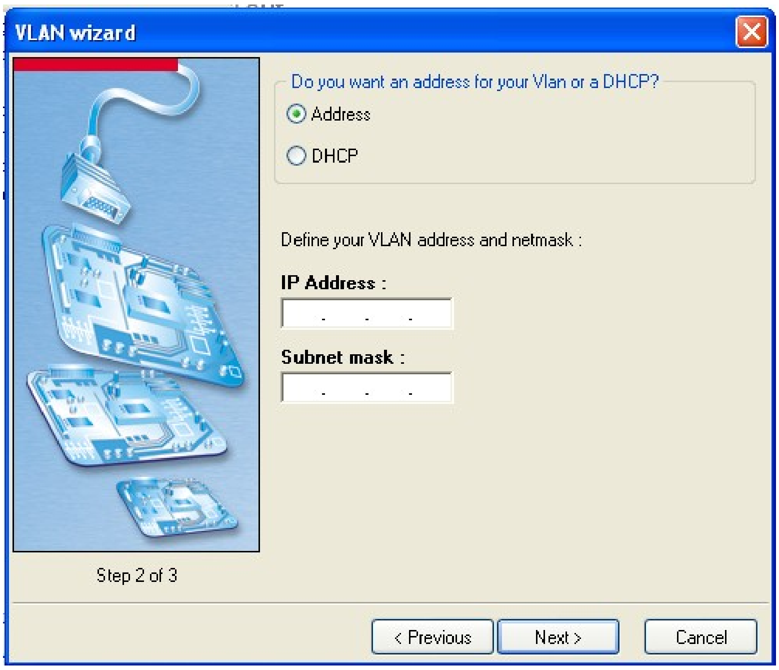
Enter the VLAN tag : 1

Enter a short description for your VLAN :

Figure 99: VLAN wizard - Step 1

1 Step 1

Enter a unique name for your VLAN, select a tag number (this number has to be unique for each VLAN that relies on the same Ethernet) and define a color for it. You can also add a description if desired. Click on **Next** (fields in bold are mandatory).



VLAN wizard

Do you want an address for your Vlan or a DHCP?

● Address

○ DHCP

Define your VLAN address and netmask :

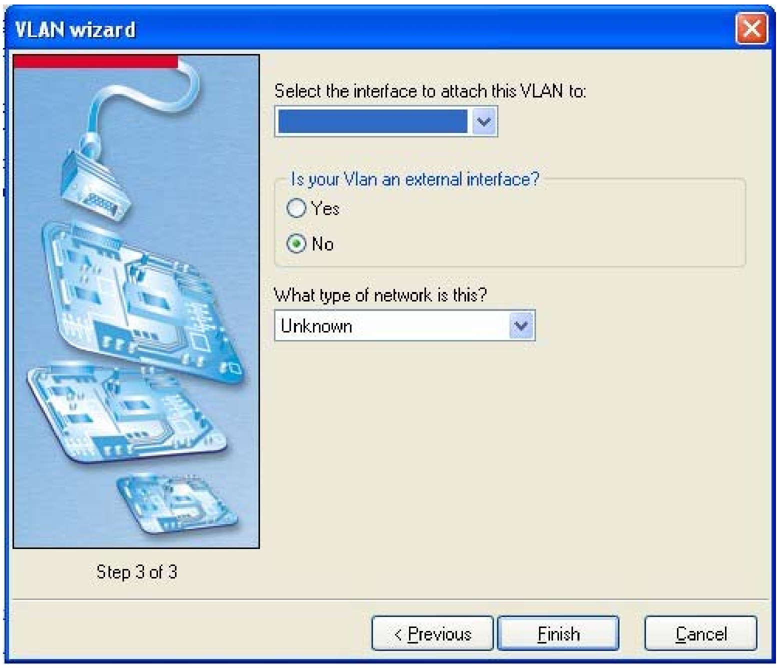
IP Address :

Subnet mask :

Figure 100: VLAN wizard - Step 2

Step 2

Check one of the following two options to give the VLAN an address (either manually or by DHCP). Click on **Next**.



VLAN wizard

Select the interface to attach this VLAN to:

Is your Vlan an external interface?

○ Yes

● No

What type of network is this?

Unknown

Figure 101: VLAN wizard - Step 3

REMARK

This second step may not be available if the VLAN had been created with a pre-determined bridge (via the interface menu directory with a bridge as the current interface).

Step 3

Select the interface on which the VLAN will be attached, then click on **Yes** or **No** to determine whether you wish to have an external interface. Lastly, define the type of host located on the network, among the options **Unknown**, **Host** and **Server**.

REMARK

When you use the **Add** button, the interface on which the VLAN is to be inserted will be shown.

Identity tab

The information to enter in the wizard is described in the tables below.

Name	Name of the VLAN (see *Appendix M: Prohibited names)*
Color	VLAN's color. These colors are very useful when you are installing the filter rules, translations etc. Each object created takes on a color, depending on the zone to which the IP address belongs.
Description	Comments relating to the VLAN.
Dynamic DNS client	This option is used when your Firewall does not have a static IP address (e.g, your service provider, or DNS renews its IP address regularly). The assigned IP address can be matched to a domain name via a DNS service provider in order to contact this

	Firewall without having to know its IP address. This feature can be activated by selecting a dynamic DNS account that you would have configured earlier. The configuration of dynamic DNS clients will be explained further in the document (see *Part 5/Chapter 2: Dynamic DNS clients*).

Parameters tab

Enabled	By checking/unchecking this option, the interface is activated/deactivated. By deactivating an interface, it becomes unusable. In terms of use, this may correspond to an interface to be used in the near or distant future, but is not active. An interface which has been deactivated because it is not in use is an example of an additional security measure against intrusions.
Tag	This field allows specifying the value associated with the VLAN in packets passing through the network. This tag identifies the VLAN and is used at the Ethernet level.
MTU	Maximum length of packets transmitted on the physical support (Ethernet). This option is not available for interfaces located in a bridge, except in the case of VLAN interfaces.
DHCP	The VLAN's IP address is provided by a DHCP server (useful for internet connections via cable) (see DHCP Configuration) This option is not available for interfaces located in a bridge.
External	Check this option to indicate that this section of the network is connected to the internet. In most cases, the external interface, linked to the internet, should be in external mode. The interface loses its security (represented by a shield) when this option is checked.
Private	This option allows indicating whether the interface is private. Addresses of "Private" interfaces cannot be used as the destination for packets coming from unprotected interfaces, unless they are translated. ℹ NOTE You will notice that "private" implies being on a protected interface. Therefore the options External and Private are incompatible.
Media	This field allows you to define the interface at the VLAN endpoint.
Type	This option defines the type of host hosted on this interface. **Host** = host computers (users), **Servers** = servers and **unknown** = unidentified host type. The logs will show you what type of traffic is passing through the Firewall (host to host, host to servers).
Maximum throughput	By specifying the internet link type, it is possible to define a maximum throughput. However this information is not used for regulating traffic, it is merely an indication.

Address tab

IP Address	VLAN interface IP address.
Netmask	Network mask of the sub-network to which the interface belongs. If the DHCP option has been selected, the `Address` tab becomes a `DHCP` tab (see *Part 11/Chapter 1: DHCP*).
Description	Enables adding a comment for the bridge address.

As usual, this tab is not available for VLANs in a bridge.

Routing tab

Passthrough Allows letting IPX (Novell network), Netbios (on NETBEUI), AppleTalk (for Macintosh), PPPoE or Ipv6 packets pass between the bridge's interfaces.

Routing As its name indicates, the **Preserve initial routing** option allows preserving the initial routing for hosts connected on this interface.

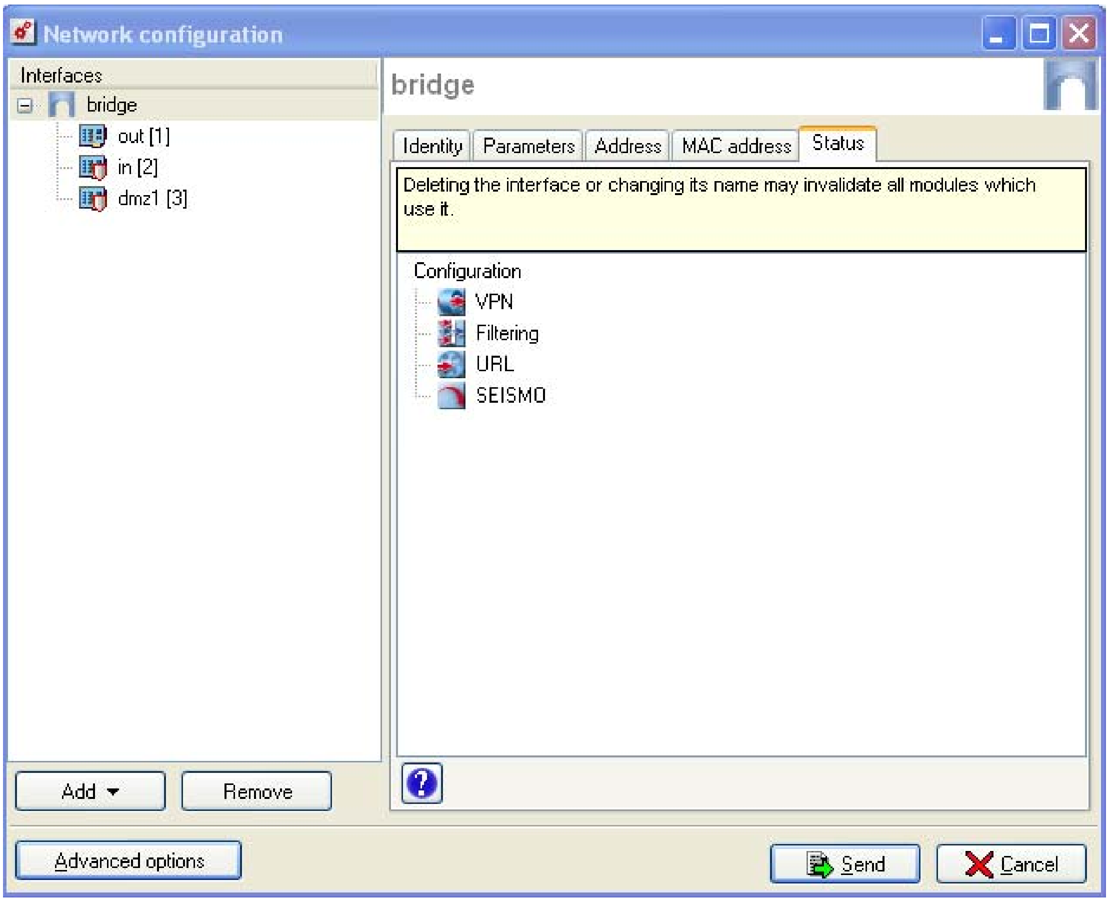
The "gateway" field is used for routing by interface.

The option **Keep VLANs** enables the transmission of tagged frames without the firewall having to be the VLAN ending. The VLAN tag on these frames are kept so that the Firewall can be placed in the path of a VLAN without the Firewall interrupting this VLAN. The Firewall functions in a fully transparent manner to the VLAN.

The NETASQ UTM appliance filters at IP level so each VLAN must have a different IP address (the Firewall maintains a look-up table between an Ethernet tag and an IP address. When a packet from a VLAN reaches the Firewall the Ethernet tag is used to find the IP address which will be used in the filter rules).

Status tab

The **`Status`** tab enables viewing where the interface is used and all the objects and object groups generated by the interface (Network_xx, Firewall_xx) in the configuration of the firewall.



Deleting the interface or changing its name may invalidate all modules which use it.

Figure 102: Iinterface configuration - Bridge – Status

By clicking on the button ?, you will get a more detailed view of how the interface is used, module by module, line by line.

5.2.6.4. VLAN in a bridge

When configuring VLANs for bridges, the same tag can be used for more than one VLAN interface associated with physical interfaces on the same bridge, making the Firewall appear transparently on the network. This method requires the use of one VLAN interface per physical interface.

Unlike the option **Keep VLANs** (which makes the Firewall fully transparent to the VLAN and which prevents the use of features which would interrupt VLAN traffic, such as proxies), this method of keeping the VLAN tag between several interfaces on the same bridge allows the use of all Firewall features.

5.2.6.5. Advanced parameters

If you wish to create a new VLAN but you have reached the maximum number of dynamic VLANs allowed, you can increase the number.

When this limit has been reached, NETASQ UNIFIED MANAGER will suggest the advanced parameters window, which will allow you to set the number of dynamic VLANs possible.

VLANs are added in blocks, but in a way that is fully transparent for the user – for example, assuming you have a U70 appliance. In this case, a maximum of 32 VLANs are allowed by default but 0 are configured. Assume also that VLANs are added in blocks of 8.

You wish to configure your first VLAN:

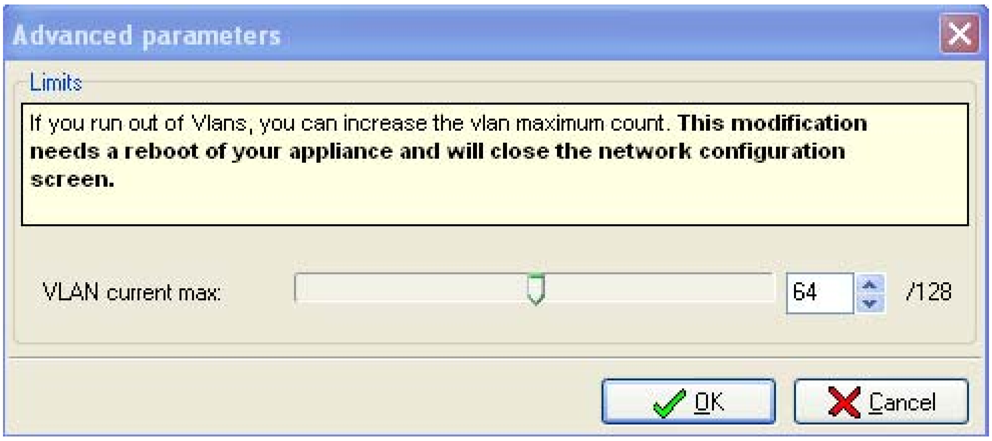
- The NETASQ UNIFIED MANAGER graphical interface will direct you to the advanced parameters window to increase the number of VLANs and informs you that you need to reboot the appliance. A block of 8 VLANs is assigned to you. You proceed to configure the 1st VLAN, but you can configure 7 more without having to reboot the appliance.
- You wish to configure a 9th VLAN, so you will need a new block. You will be informed that the firewall will reboot. Then you can configure the VLAN.

When your appliance is in factory settings, a maximum number of VLANs will be assigned according to the model. The table below indicates the maximum number of VLANs assigned:

Models	**Max no. of VLANs**
U30, U70	32
U120, U250, U450	128
U1100, U1500	256
U6000	512

In the network interfaces configuration panel, you will find the **Advanced parameters** button that will allow you to increase your maximum number of VLANs.

The following window appears when you click on this button:



Advanced parameters

Limits

If you run out of Vlans, you can increase the vlan maximum count. **This modification needs a reboot of your appliance and will close the network configuration screen.**

VLAN current max: 64 /128

Figure 103: Advanced parameters

This window allows you to choose the desired number of VLANs. You merely need to slide the scale to increase or decrease the number. If the number of VLANs indicated corresponds to a new block, the firewall will need to reboot before the VLANs can be configured (adding or deleting).

WARNING

Any modifications to the network configuration before increasing the number of dynamic VLANs will be lost since this window will be closed. A warning message will inform you.

5.2.7. Creating a dialup

5.2.7.1. Creation

Dialup interfaces are used in remote connections when your modem is directly connected to the Firewall (serial port or Out Ethernet). The Firewall accepts all modem types (ADSL, ISDN, dialup, etc).

New dialup interfaces (“dialup” and “altdialup” interfaces already exist by default) are created using a wizard. The maximum number of VLAN interfaces available on your Firewall depends on the model.

1 Select **`Network\Interfaces`** from the menu in the configuration interface.

2 Click on **`Add`** and select **`Dialup`** or right-click and select **`New dialup`** in the contextual menu. The following window will appear:

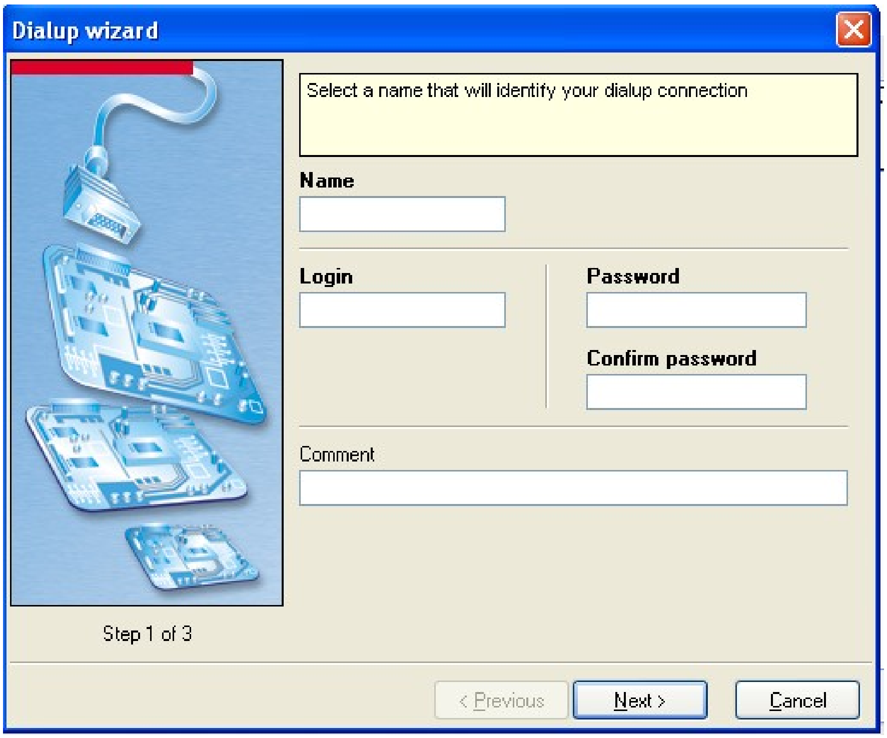
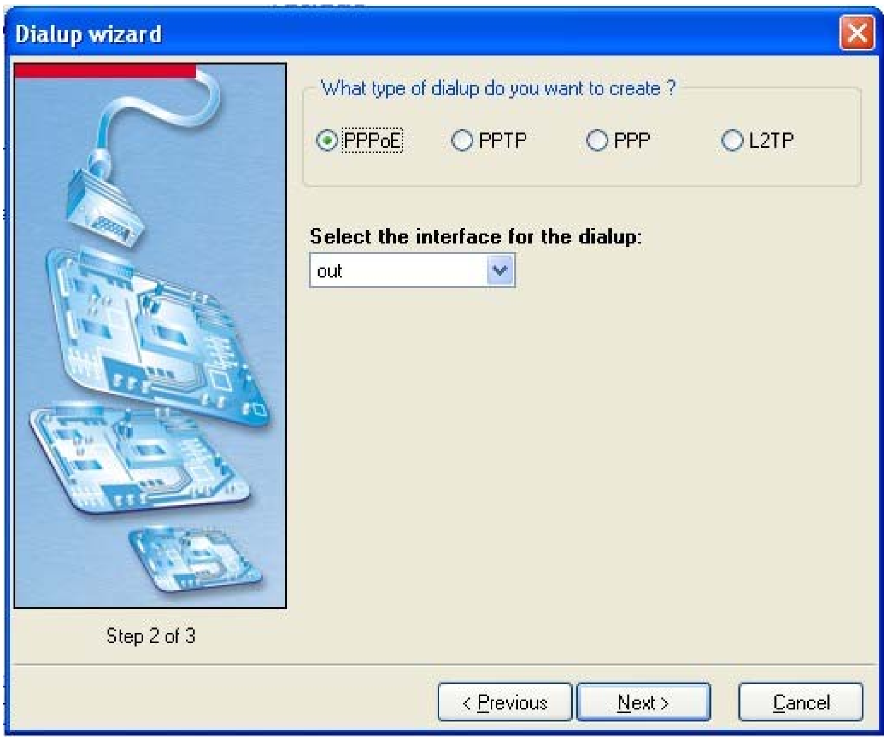


Figure 104: Dialup wizard - Step 1

4 Indicate a name (mandatory), login (mandatory), password (mandatory) and description in order to identify the dialup connection. Then click on **Next**.

5 Select the type of dialup from PPPoE, PPTP, PPP or L2TP. The configuration window will vary according to the ttype of dialup selected.

If you have selected **PPPoE**, the following window will appear:

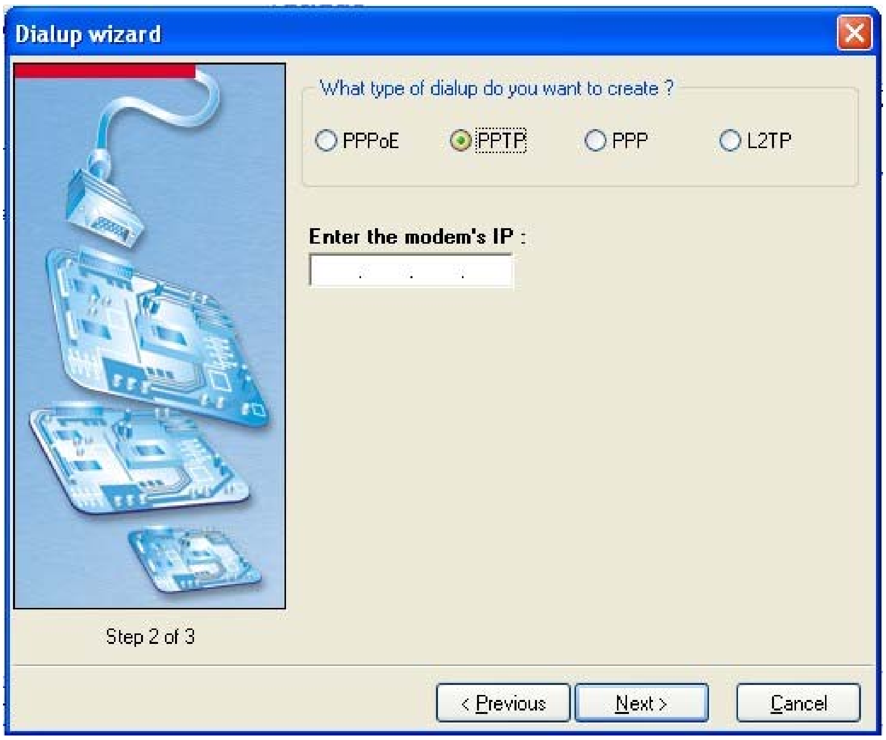


● PPPoE ○ PPTP ○ PPP ○ L2TP

Select the interface for the dialup: out

Figure 105: Dialup wizard -PPPoE - Step 2

Select the network interface used for the dialup.
If you select **PPTP**, the following window will appear:



Dialup wizard

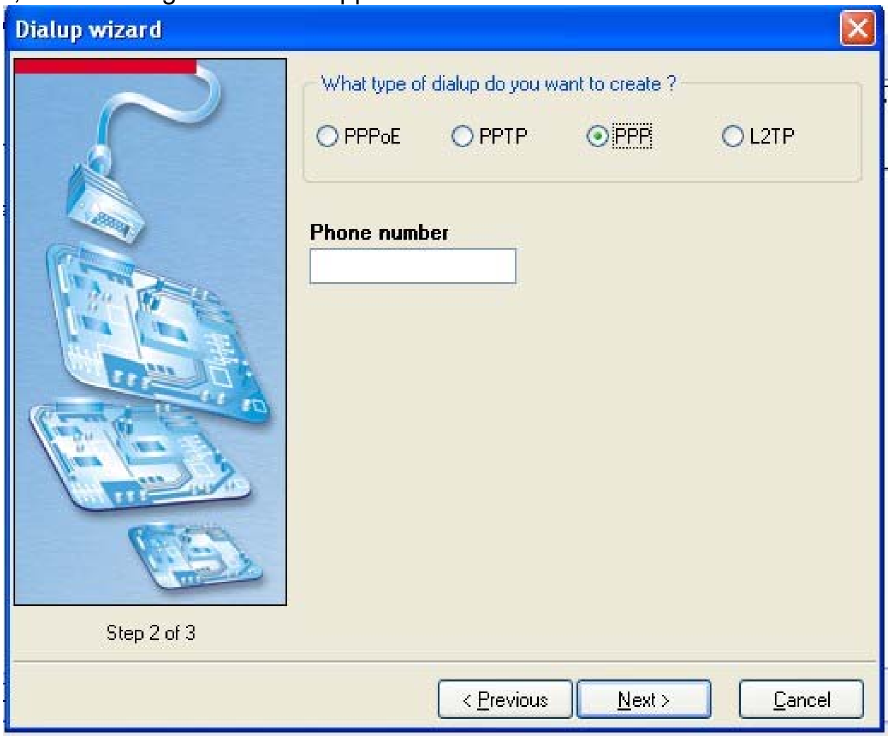
What type of dialup do you want to create ?

○ PPPoE ● PPTP ○ PPP ○ L2TP

Enter the modem's IP :

Figure 106: Dialup wizard- PPTP - Step 2

Enter the modem’s IP address.
If you select **PPP**, the following window will appear:



Dialup wizard

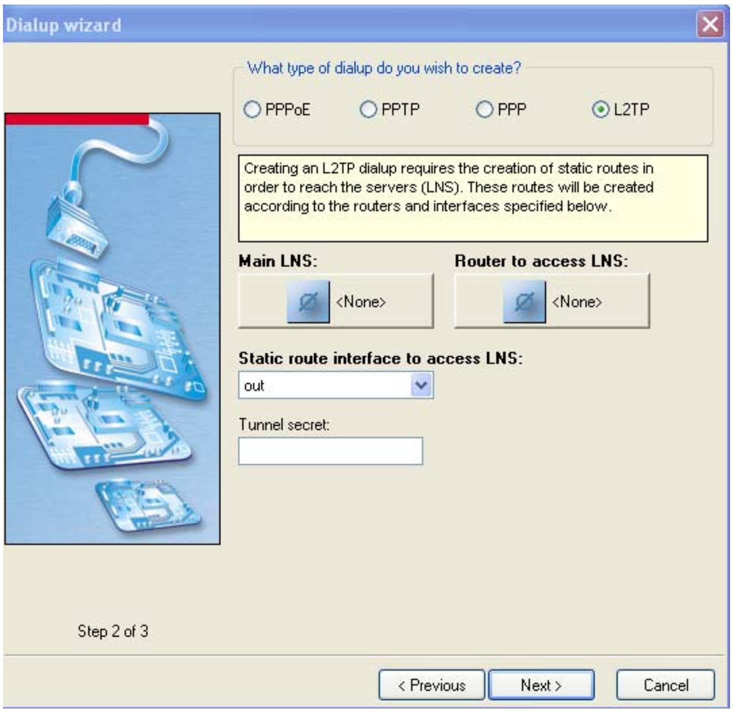
What type of dialup do you want to create ?

○ PPPoE ○ PPTP ● PPP ○ L2TP

Phone number

Figure 107: Dialup wizard - PPP - Step 2

Indicate the telephone number that will be dialed.
If you select **L2TP**, the following window will appear:



Dialup wizard

What type of dialup do you wish to create?

○ PPPoE ○ PPTP ○ PPP ● L2TP

Creating an L2TP dialup requires the creation of static routes in order to reach the servers (LNS). These routes will be created according to the routers and interfaces specified below.

Main LNS: <None>

Router to access LNS: <None>

Static route interface to access LNS: out

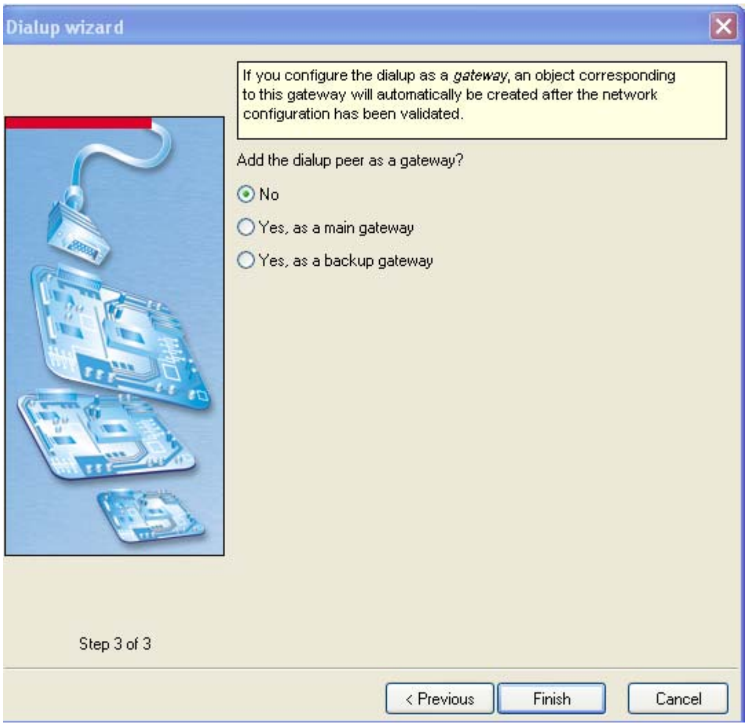
Tunnel secret:

Step 2 of 3

Figure 108: Dialup wizard - L2TP - Step 2

To create an L2TP dialup, define the main LNS the router to access the main LNS and the interface that will allow creating the static route, which will be useful when contacting the LNS server. Lastly, indicate the LNS' peer authentication (in the form of a key).

6 Once you have finished configuring Step 2, click on **Next**. The following window will appear:



Dialup wizard

If you configure the dialup as a *gateway*, an object corresponding to this gateway will automatically be created after the network configuration has been validated.

Add the dialup peer as a gateway?

● No

○ Yes, as a main gateway

○ Yes, as a backup gateway

Step 3 of 3

Figure 109: Dialup wizard - Step 3

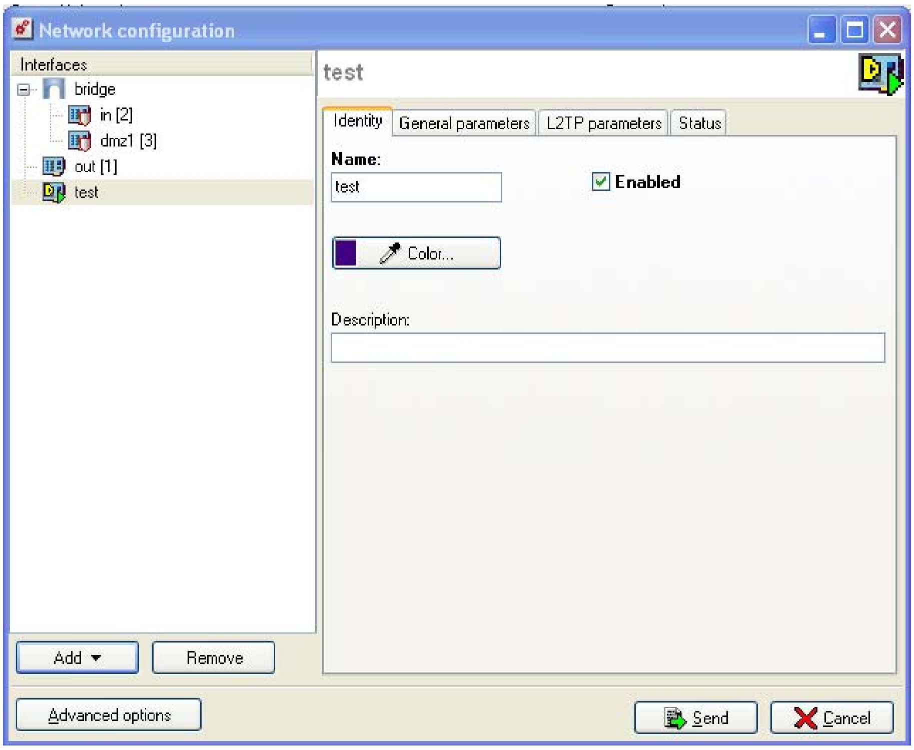
Indicate whether you wish to define the dialup as a gateway.
If so, you have 2 options – **Yes, in main gateways** or **Yes, in backup gateways**.

Click on **Finish** to confirm the creation of the dialup.

5.2.7.2. Configuration

You may then configure the interface's following parameters:

Identity tab



Name: test

☑ Enabled

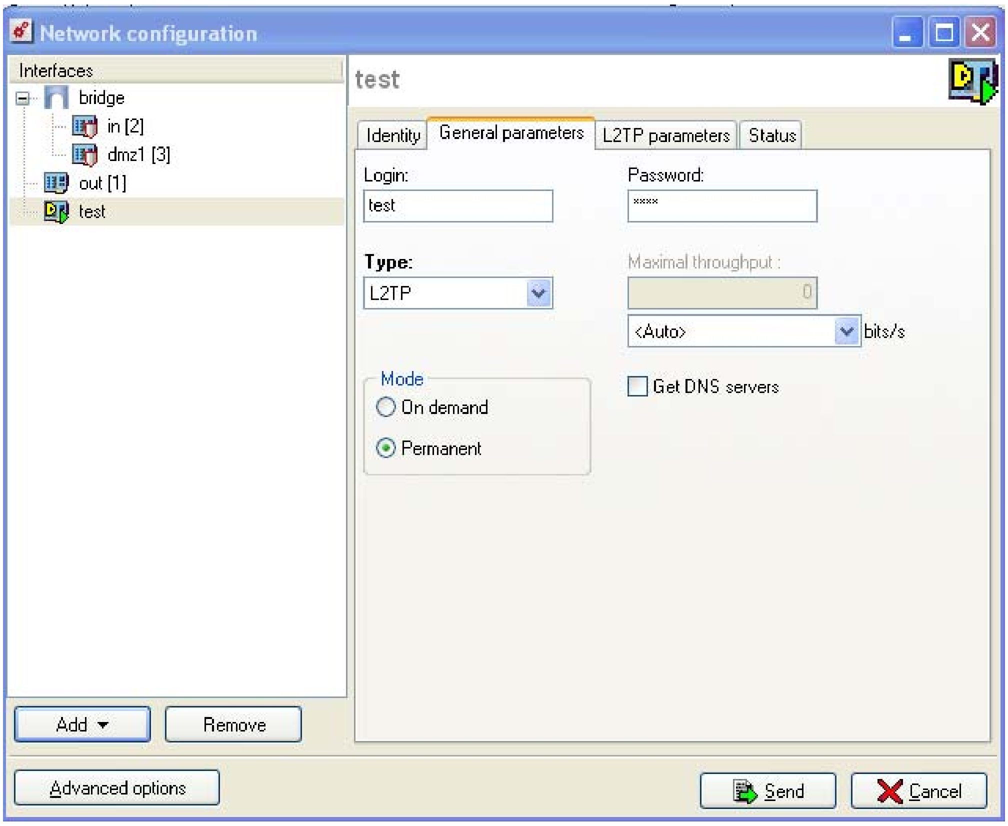
Description:

Figure 110: Configuration - Dialup - Identity

Name	Name of the remote connection (*Cf. Remarks to see which names are prohibited*).
Enabled	By checking/unchecking this option, the interface will be enabled/disabled. By deactivating an interface, it becomes unusable. In terms of use, this may correspond to an interface to be used in the near or distant future, but is not active. An interface which has been deactivated because it is not in use is an example of an additional security measure against intrusions.
Color	Color assigned to the remote connection. These colors are very useful when you are installing the filter rules, translations etc. Each object created takes on a color, depending on the zone to which the IP address belongs.
Description	Comments relating to the remote connection.
Dynamic DNS client	This option is used when your Firewall does not have a static IP address (e.g, your service provider renews its IP address regularly). The assigned IP address can be matched to a domain name via a DNS service provider in order to contact this Firewall without having to know its IP address. This feature can be activated by selecting a dynamic DNS account that you would have configured earlier. The configuration of dynamic DNS clients will be explained further in the document (see *Part 5/Chapter 2: Dynamic DNS clients*).

Two or more dialup connections may be active at the same time. This configuration has the advantage of allowing the distribution of outgoing connections. (cf *Part 5/Chapter 3: Interfaces\Routing).*

General Parameters tab



Login: test

Password: ****

Type: L2TP

Maximal throughput : 0

<Auto> bits/s

Mode

○ On demand

● Permanent

□ Get DNS servers

Figure 111: Configuration - Dialup – General parameters

Login	Login name given by the access provider.
Password	Password corresponding to the access provider's password.
Type	The remote connection type can be PPP (ISDN, dialup), PPPoE (ADSL), PPTP (ADSL) or L2TP. **REMARK** Whenever a dialup is selected, a tab of the same dialup type will be enabled for the configuration.
Maximal throughput	By specifying the internet link type, it is possible to define a maximum throughput. However this information is not used for regulating traffic, it is merely an indication.
Mode	The **On demand** mode establishes a connection to the internet only if the connection request comes from the internal network (this mode is cheaper in the case of a connection charged by duration). The **Permanent** mode keeps the internet connection permanently active.
Get DNS servers	When this option is selected, the Firewall will retrieve DNS servers from the DHCP server it contacts (access provider, for example) to obtain its IP address. Two objects will be dynamically created in the object database upon the selection of this option: Firewall_<interface name>_dns1 and Firewall_<interface name_dns2. They can then be used in the configuration of the DHCP service. So, if the Firewall

	provides the users on its network with a DHCP service, the users will also benefit from the DNS servers given by the access provider.

PPPoE Parameters tab

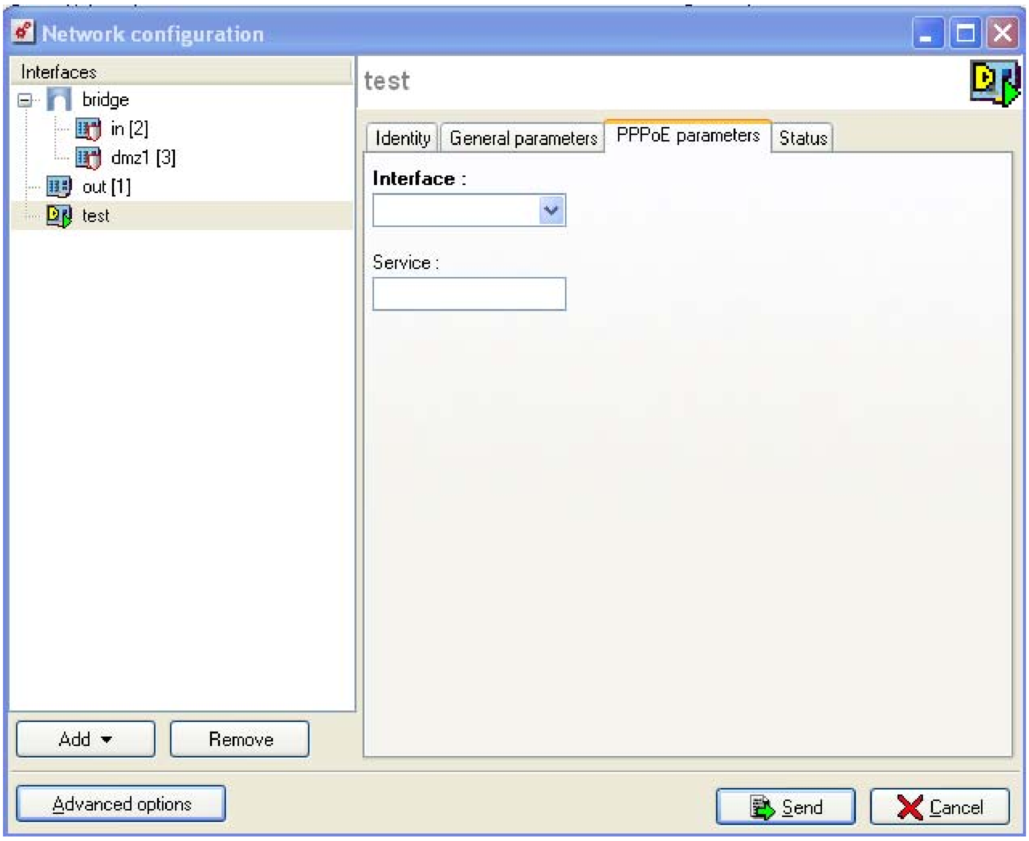
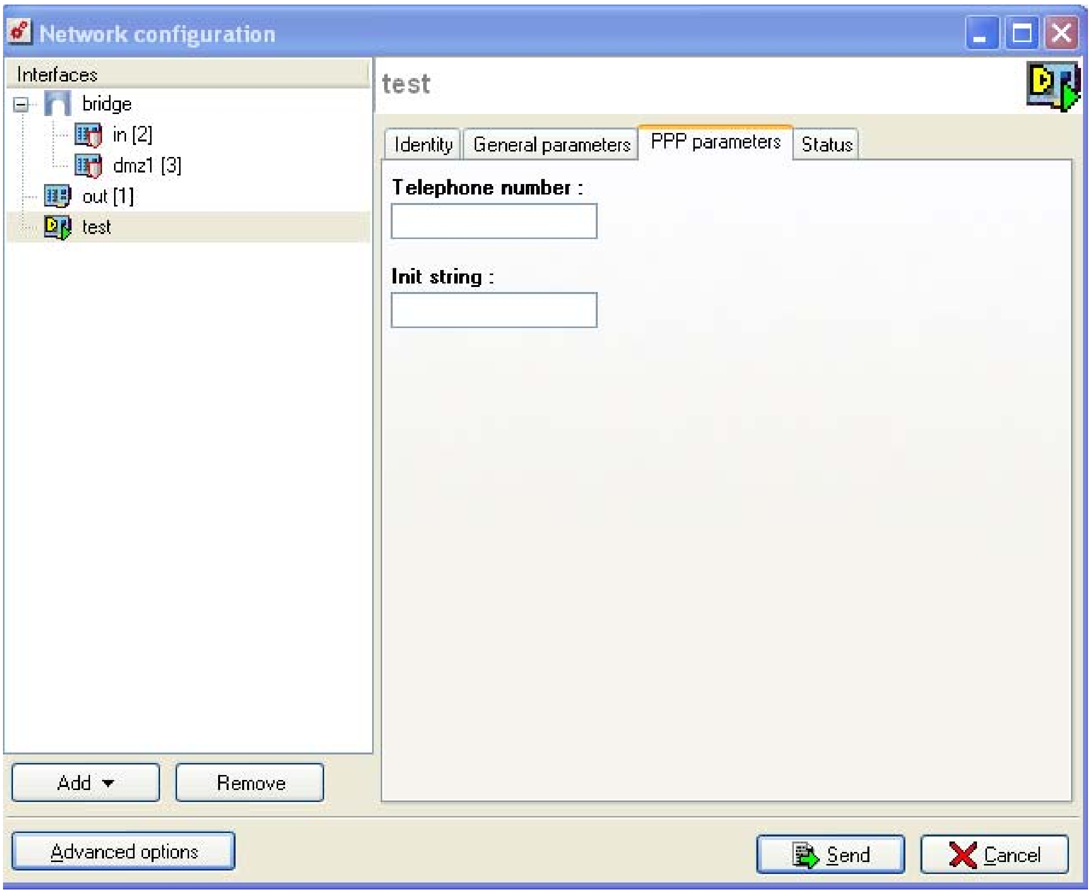


Figure 112: Configuration - Dialup – PPoE parameters

Interface	Interface on which the connection is made.
Service	Type of PPPoE service used. This option allows differentiating several ADSL modems. Leave this field empty by default.

PPP Parameters tab



Telephone number :

Init string :

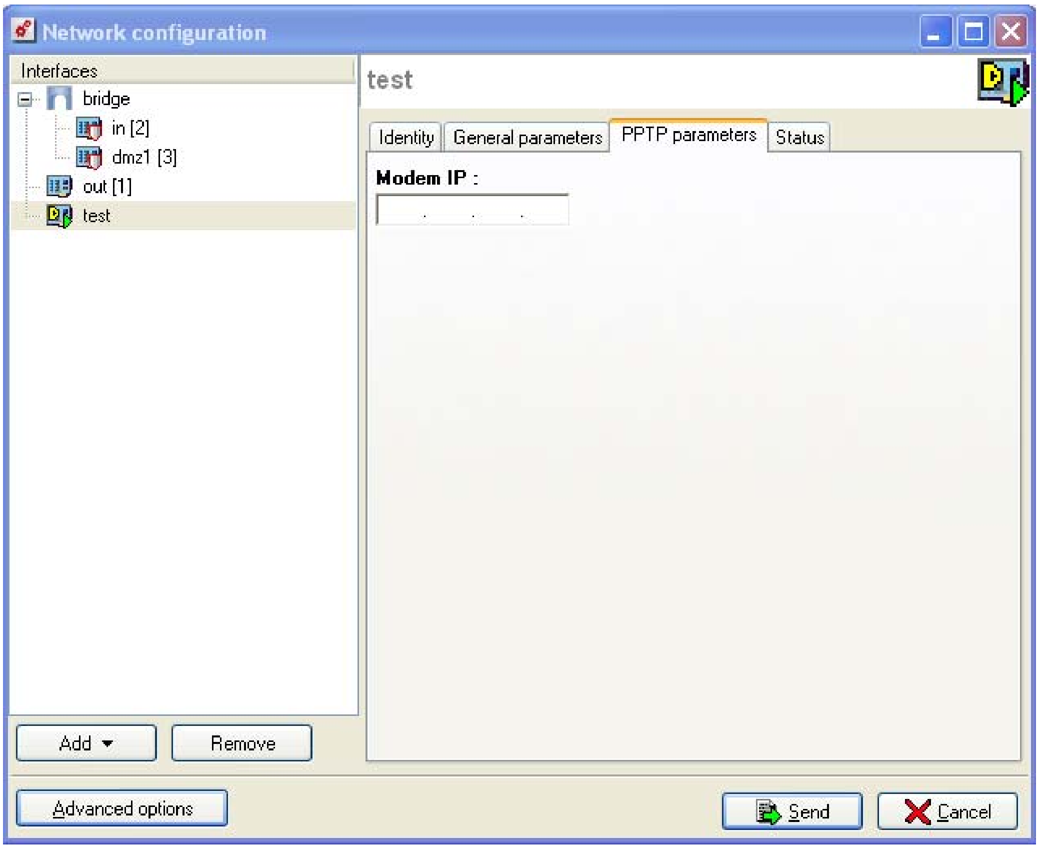
Figure 113: Configuration - Dialup - PPP parameters

NOTE
When the chosen connection type is PPP.

Telephone number (mandatory)	Access provider's telephone number
Init string (mandatory)	Character string used for initializing the connection (optional).

PPTP Parameters tab

NOTE
When the chosen connection type is PPTP.



Modem IP :

Figure 114: Configuration - Dialup - PPTP parameters

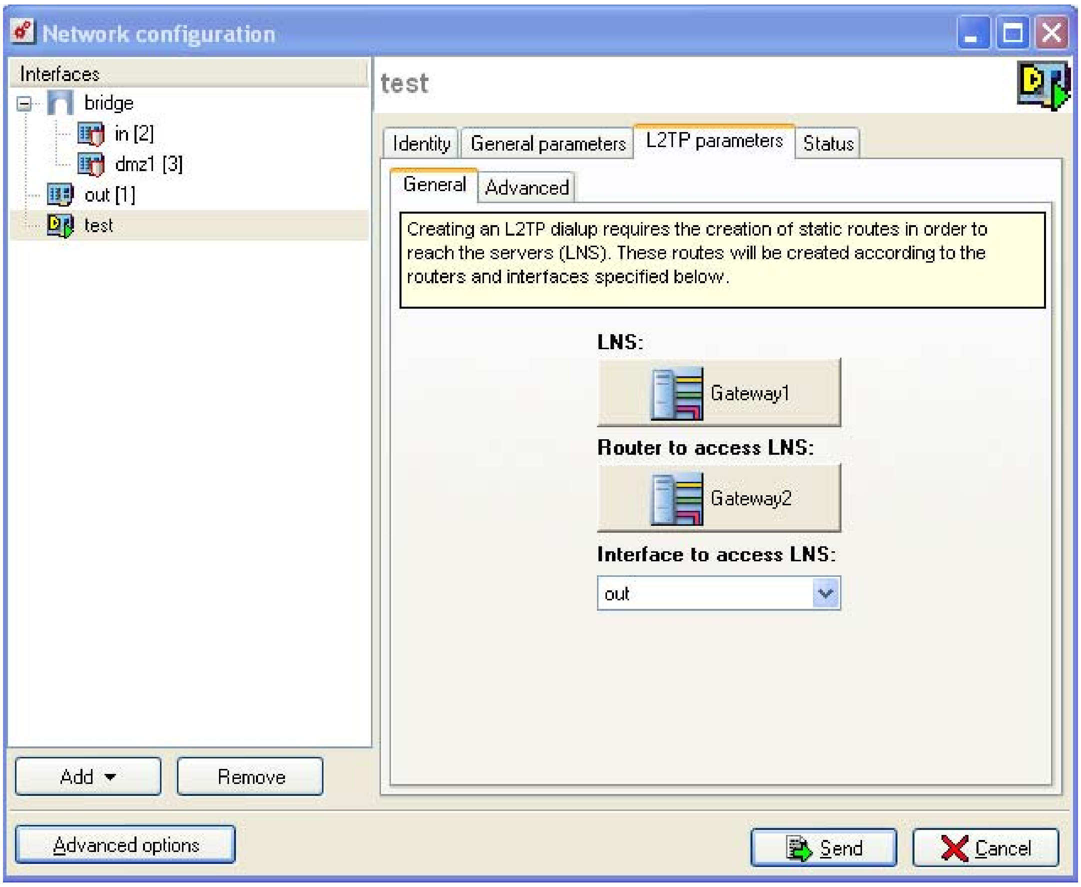
Modem IP	Internal IP address of the ADSL modem.

L2TP Parameters

NOTE
When the chosen connection type is L2TP.

The options in the **`L2TP Parameters`** tab are split into two menus, the parameters of which are explained below:

General tab

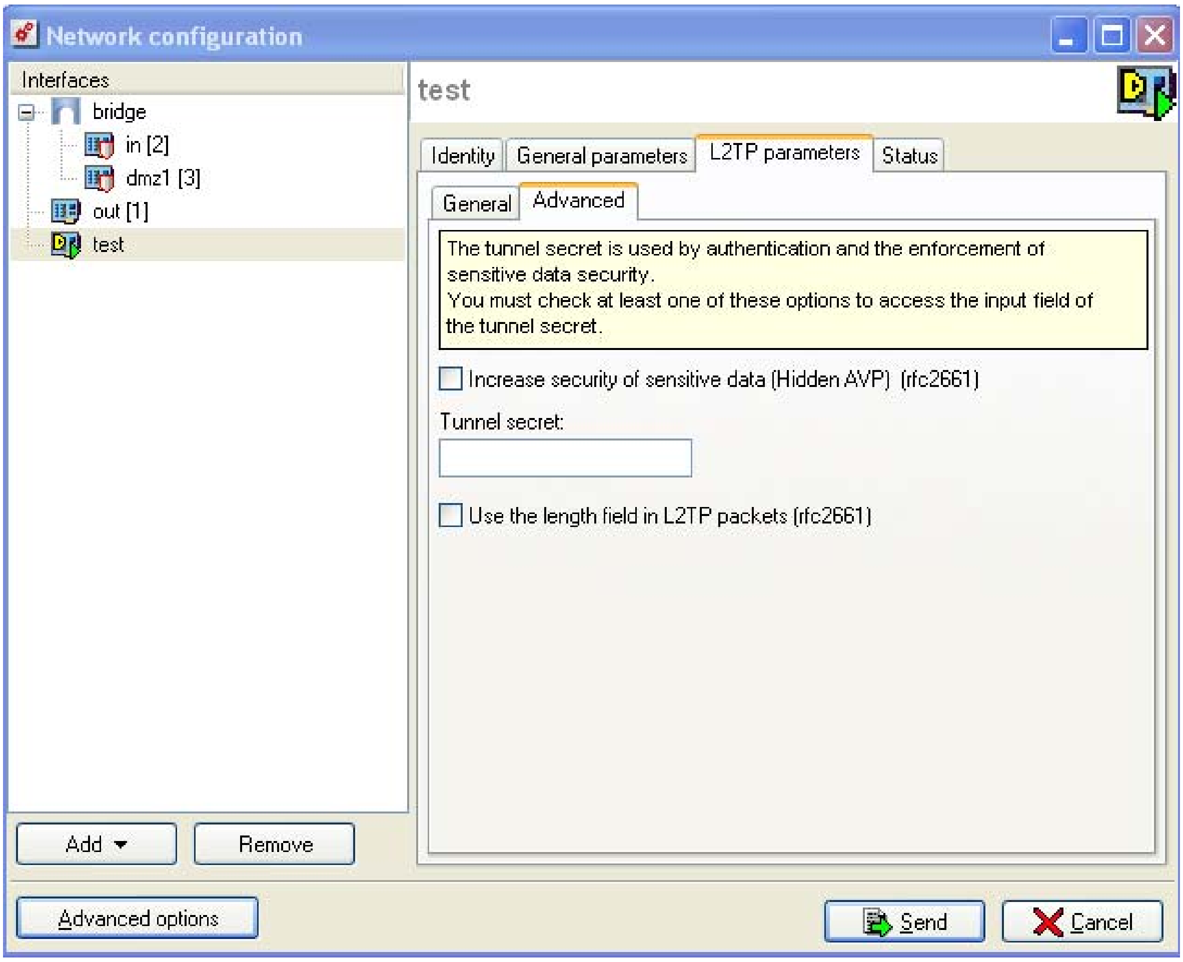


Creating an L2TP dialup requires the creation of static routes in order to reach the servers (LNS). These routes will be created according to the routers and interfaces specified below.

Figure 115: Configuration - Dialup - L2TP configuration

LNS	IP address of the remote L2TP server (LNS) used in the L2TP connection.
Router to access LNS	When creating an L2TP dialup, a static access route to the L2TP (LNS) server, defined by the access router and the interface to which it is connected, is required. This option allows defining the access router.
Interface to access LNS	Name of the interface on which the LNS is linked.

Advanced tab



The tunnel secret is used by authentication and the enforcement of sensitive data security.
You must check at least one of these options to access the input field of the tunnel secret.

□ Increase security of sensitive data (Hidden AVP) (rfc2661)

Tunnel secret:

□ Use the length field in L2TP packets (rfc2661)

Figure 116: Configuration - Dialup - L2TP configuration

Increase security of sensitive data (hidden AVP, RFC 2661)	Certain sensitive data passing through the L2TP tunnel can be protected (by masking passwords, for example) during the exchange.
Tunnel secret	This is the field used for defining the shared secret that is absolutely necessary for the options “L2TP peer authentication using pre-shared secret” and “Protection of sensitive data (Hidden AVP)”.
Use the length field in L2TP packets (RFC2661)	The RFCs on L2TP state that using this field is optional. By default this field is therefore not used but in the event it is needed (if requested by the server, for example), select this option.

5.2.7.3. Remarks on dialup configuration

- The Firewall automatically negotiates the connection and resets the connection when it is severed. In the event the connection is impossible (e.g. problem with the line), the Firewall will send an alarm message.
- The Firewall creates an object firewall_dialup representing the internet connection interface. You have to use this object in translation and filter rules.
- To authorize PPTP connections, filter rules also have to be added.

CHAPTER 3: ROUTING

5.3.1. Introduction to routing

Conveying data is a task that every network device needs to perform. As network architectures become increasingly complex, it is essential that optimum routing rules are defined. NETASQ firewalls have several features such as static routing, load balancing and even routing policies (PBR: *Policy Based Routing*).

There are several routing mechanisms for the delivery of packets.

? **STATIC ROUTING**

Based on the appliance's routing table, static routing consists of evaluating the treated IP packet with different entries in the table. If the destination address matches an entry, identified by an address (host or network), the packet will be sent to the gateway defined for this entry.

? **ROUTING BY INTERFACE**

For this type of routing, the operating system on NETASQ appliances will evaluate the transmission gateway according to the packet's source interface.

? **ROUTING POLICY**

A routing policy allows evaluating the transmission gateway according to the sender of the packet (host, network or group), its addressee (host, network or group) and the protocol used for transmitting the packet.

? **LOAD BALANCING**

Routing by load balancing allows distributing the transmission of the packet to several gateways, either according to the source host or the connections.

! **WARNING**

The different types of routing implemented in NETASQ appliances are evaluated in a specific order as shown below:

1 Static routing/dynamic routing
2 Routing policy
3 Routing by interface
4 Load balancing by connection
5 Load balancing by source
6 Routing by default

NOTE

1) A route by default is necessary once the routing policy has been defined, so that traffic that does not match the routing policy can be transmitted.
2) Routing policies can be implemented on IPSec traffic.

For further information on the topic of routing, please refer to the technical note "Types of routing v8.0".

5.3.2. Presentation of the windows and tables

The routing module consists of two parts:

- Static routing (**General** tab): (router and static routes)
- **Advanced** tab: this tab addresses more specific needs.

Both these parts operate simultaneously, with static routing having priority over all the others during the transmission of a packet over the network.

Static routing represents a set of rules that the administrator has defined as well as a default route. The **Advanced** tab can be considered an advanced form of the default route, which suggests the simultaneous use of several routes to transmit a packet, according to a configurable algorithm. The **Advanced** tab operates with a backup system.

When link high availability has been enabled and is operating correctly:

- The first batch (main routes) will contain the routes taken.
- If some of these main routes can no longer be taken (with a number of valid routes below a given limit), the second batch (backup routes) will be activated and will replace the first batch.

Every route is a "Host" object that indicates the IP address which acts as a route.

➲ Routing is configured on the firewall via the menu **Network\Routing**

5.3.2.1. General tab

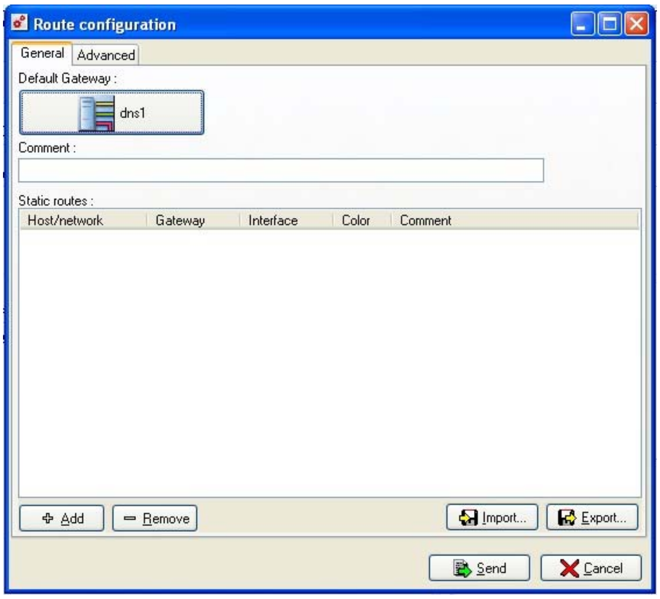


Figure 117: Route configuration - General

Presentation of the window

The window of this tab comprises three parts:

Default gateway	Default router's IP address. The NETASQ Firewall sends all packets which have to exit on the public network to this address. Often the default router is connected to the Internet. Clicking on this button will lead you to the object database and will allow you to select a host. Once it has been selected, the hostname will appear on the screen.
Comment	Comments associated to this tab (text only).
Static routes	If you have several networks "behind" a router, you can specify these different routes here. You must therefore select a network or host group then a gateway to be used to reach this network. You also have to specify the interface to which this gateway is indirectly connected. You can Add or Remove static routes with the **Add**/ **Remove** buttons.

Presentation of the table

Five fields are shown in the table:

Host /network	Double clicking on this column will open the object database in order to select a host, network or group.
Gateway	Double clicking on this column will open the object database in order to select a host (router).
Interface	A drop-down list that will allow you to select an interface among Ethernet, VLAN and dialup.
Color	Allows selection of a color for the interface.
Comments	Text zone.

The default router is generally the equipment which allows your network to access the Internet. If you do not configure the default router, the NETASQ Firewall will not be able to let through packets which have a different destination address from that directly linked to the NETASQ Firewall. You will be able to communicate between hosts on the any interface (internal, external or DMZ networks), but not with the Internet.

Command lines

```
NETWORK, INTERFACE -> GATEWAY, COLOR# COMMENTS
```

Action buttons

There are six buttons below the table:

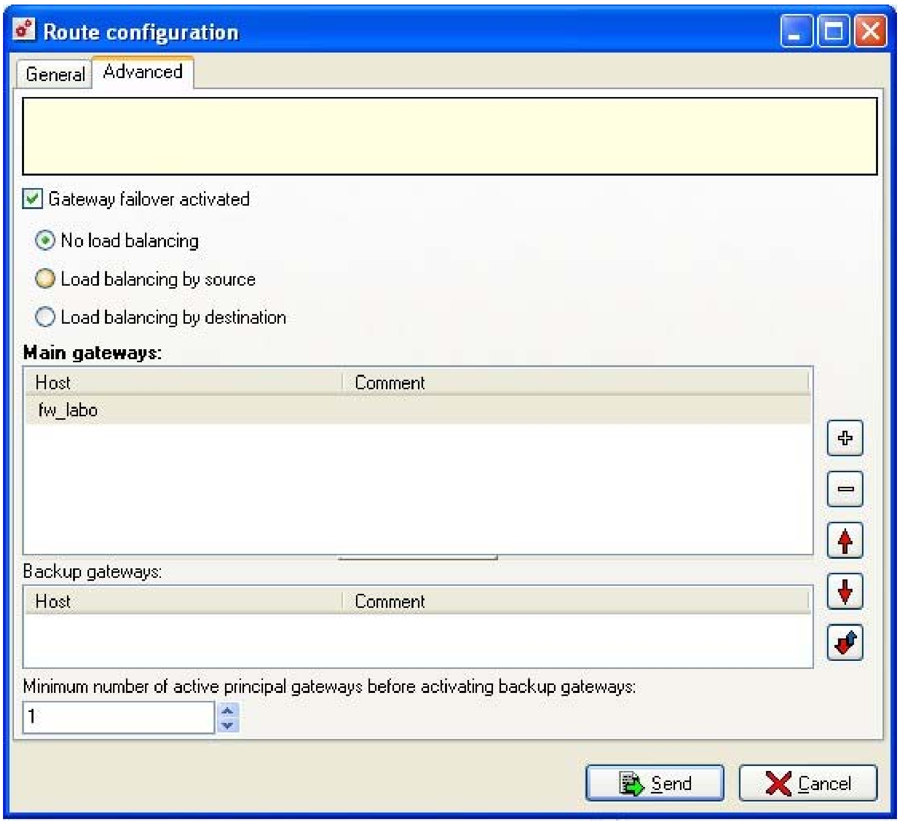
Add	Adds an “empty” static route.
Delete	Deletes a previously selected route.
Import	Imports routes. The contents of the file is in the same format as the file that the firewall receives via the command *network route show.*
Export	Exports routes. Static routes are exported in a file of the same format as imported files.
Send	Sends the configuration for static routes.

Cancel	Cancels the configuration for static routes.

REMARK
When you right-click on the table, a contextual menu that allows performing the same actions above will appear.

5.3.2.2. Advanced tab

This window allows activating the “advanced” routing mode. For default routes, this is substituted by the `General` tab.



☑ Gateway failover activated

● No load balancing

○ Load balancing by source

○ Load balancing by destination

Main gateways:

Host	Comment
fw_labo	

Backup gateways:

Host	Comment

Minimum number of active principal gateways before activating backup gateways: 1

Figure 118: Route configuration – Advanced

Load Balancing

The option **Gateway failover activated** allows activating Gatemon. When this option has been selected, it will be possible to have several routes instead of a single one (indicated in the `General` tab).

Gateway failover activated	When this option is selected, high availability of routes will be activated. There are 3 possibilities: "No load balancing", "Load balancing by source" and "Load balancing by destination". ● **No load balancing**: The first route defined in the tables "Main gateways" and "Backup gateways" is used for routing whereas the others will be ignored. Thus, if a main route is down, the backup route will take over (if there is one). ● **Load balancing by source**: All the routes defined in the table "Main gateways" will be used. Routing will be distributed according to the source of the routed traffic. If too many main routes are down, the batch of backup routes will take over. ● **Load balancing by destination**: This is almost the same as load balancing by source except that the load balancing algorithm relies not only on the source but the destination of the traffic. Traffic will then be better distributed among the various routes. In brief, depending on the host and its connections, packets may not necessary pass through the same route. **REMARK** Commands are sent in real time when the type of load balancing is selected. If there is a failure, the radio buttons will be restored.
Minimum number of active principal gateways before activing backup gateways	If high availability has been activated, the backup gateways will only be used if the number of main gateways falls below the minimum number defined in the field **Minimum number of active principal gateways before activing backup gateways**. The minimum value of this field must be set at 1.

Action buttons

To add or delete routes, click on ⊞ and ⊟ respectively. The object database will appear so that you will be able to select a host that allows routing.

⊞ **(Add)**	Adds a router. 2 options are available when you click on this button: **Add a main gateway…** or **Add a backup gateway**. When either option is selected, the object database will appear, allowing you to select a host for routing.
⊟ **(Delete)**	Deletes a router. When you click on this button, you will get the message "**Delete this element?**". Confirm by clicking on **Yes** or **No**.
⇅ **(Switch categories)**	Enables changing a main route to a backup route.
↑ **(Up)**	Moves a selected gateway up the list.
↓ **(Down)**	Moves a selected gateway down the list.

REMARK

The same actions can be obtained by right-clicking on a table.

Main and backup gateways

The tables for main gateways and backup gateways are made up of the following columns:

Host	Object that allows routing. This can be any host, dialup gateway (Firewall_<name_dialup_interface>_peer) or DHCP router (Firewall_<name_DHCP_interface>_router).
Description	Comments regarding this object.

ⓘ **REMARK**
The number of main and backup gateways that can be created is limited.

Sending the configuration

To confirm changes made in this window, click on **Send**. During this confirmation, system error messages may appear, causing micro-actions to be aborted. For this reason, when load balancing has been modified, the configuration will only be sent when routing, advanced route configuration and ASQ have been activated.

Checks are made beforehand on whether static routes are coherent – if a static route does not have a host/network/group, router or description, sending will be aborted.

If the configuration in this tab is for two main gateways or a main gateway and a backup gateway, the “Router” button in the `General` tab will be grayed out.

5.3.3. Example of a static routing configuration

5.3.3.1. Objective

This example is based on a network architecture comprising a head office and a local site (see diagram below). The NETASQ UTM appliance of the local site has been configured here to let all traffic to the head office use the line dedicated for this purpose. Traffic to the internet will use the local modem access.

5.3.3.2. Diagram

Figure 119: Static routing

5.3.3.3. Configuration

The address has to be translated and filter rules have to be created beforehand.

Configure the routing table.

5.3.4. Example of a configuration by routing policy

5.3.4.1. Objective

This example is based on a network architecture comprising a head office and a local site (see diagram below). We wish to configure the NETASQ UTM appliance of the local site to let all traffic to the head office use the line dedicated for this purpose. Traffic to the internet will use the local modem access.

5.3.4.2. Diagram

Figure 120: Network architecture

5.3.4.3. Configuration

The address has to be translated and filter rules have to be created beforehand.
2 Add a default gateway.
3 Configure the routing policy.

Example of routing by policy

Figure 121: Filter rules

The first rule indicates that all traffic from source “Network_in” to destination “remote_network” will be routed to “leasedline_router”.
As for web traffic, since it comes from the internal network, will be routed to “Internet_router”.

5.3.5. Example of a routing by interface configuration

5.3.5.1. Objective

Certain structures need to have several internet accesses with specific characteristics.

A company that hosts public servers on its network has to be able to provide an optimum quality of service for accessing these servers. In parallel, it has to give its internal users the ability to access the internet without affecting the bandwidth dedicated to public servers. Routing by interface will allow defining several internet accesses at the firewall level, which will be used according to the interface on which the connection request arrives. It will then be possible to assign an ADSL access for the internal network and a specialized link, with a guarantee of service, for access to your public servers.

5.3.5.2. Configuration

1 The address has to be translated and filter rules have to be created beforehand.
2 Configure the VLANs.
3 Configure routing by interface.

The procedure for configuring routing by interface is as follows:

1 Select the **`Interfaces`** tab in the network configuration window.

2 Select the desired interface, then the **`Routing`** tab.

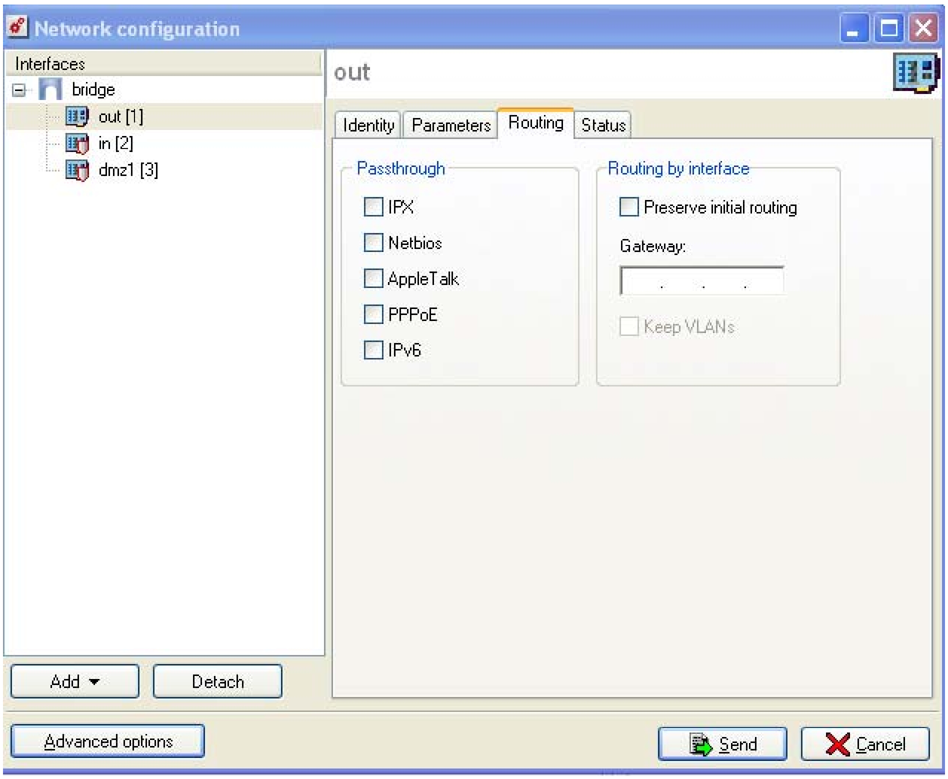


Figure 122: Configuration of the out interface - Routing

As we have indicated in the section *Part5/Chapter 1: Configuring the interfaces*, there is a "Gateway" field for each interface. This field has to contain the IP address of the default gateway (gateway for going onto the internet) used when a connection request headed for the internet is received on this interface. This field may be left empty. In this case, the default gateway used will be the one defined in the **`Routing`** tab.

5.3.5.3. Sending commands

Commands are sent in “semi-real time”. This means that changes made to an interface are reflected as commands when the configuration panel is replaced by another.

The program will then distinguish between the former status of the interface and the new, and then deduce the right commands.

5.3.6. Example of a load balancing configuration

5.3.6.1. Objective

This example is based on a network architecture comprising a head office and a local site (see diagram below). We wish to configure the NETASQ UTM appliance of the local site to let all traffic to the head office use the line dedicated for this purpose. Traffic to the internet will use the local modem access.

5.3.6.2. Diagram

Figure 123: Network architecture

5.3.6.3. Configuration

The address has to be translated and filter rules have to be created beforehand.

Configure load distribution by connection.

Configure load distribution by source.

CHAPTER 4. REMARKS ON NETWORK CONFIGURATION

REMARK
Changing the NETASQ Firewall's internal or external IP addresses may require important modifications in your configuration files so that they remain coherent. Before rebooting the NETASQ Firewall, do not hesitate to check that your data is coherent, particularly in the sections *Part 4: Objects*, *Part6/Chapter 4: Address translation* and *Part 7/Chapter 2: Filters*.

An interface should never be named "HA" or a name set out in the following way:

- "xx_peer" or "firewall_yy".
- xx being the name of an existing interface .
- yy being a character chain .

Dialup load balancing is configured in this window.
Load balancing can be performed on routers and dialups. This function is carried out by ASQ.

PART 6: INTRUSION PREVENTION (ASQ)

CHAPTER 1: INTRODUCTION

6.1.1. For this chapter, you will need to have completed these steps:

- Part 2: Installation, pre-configuration, integration

6.1.2. For this chapter, you will need to know:

- The actions to take when attacks are detected.
- Information relating to the configuration of stateful inspection.
- The ports you wish to keep an eye on.
- The application protocols you wish to analyze.

6.1.3. Purpose of this chapter

This chapter allows you to configure the ASQ kernel, the heart of a NETASQ Firewall, namely the actions to carry out when attacks are detected. Configuration of stateful, routing, probes and plug-ins add to the configuration of the Firewall before the implementation of filtering policies, translation policies, etc.

After a security event of the same alarm level is registered, the ASQ alarm functions enable performing the following actions:

- Switching on the indicator corresponding to the alarm level on the front panel of the Firewall.
- Displaying the alarm on NETASQ REAL-TIME MONITOR.
- Sending the alarm to specified users by e-mail.

6.1.4. Accessing this chapter

➲ Access the configuration dialog box using the **`Intrusion prevention`** menu in the NETASQ UNIFIED MANAGER menu directory.

You have to be connected with modification privileges in order to perform these modifications.

WARNING
Before making any significant modification to your Firewall, we recommend that you perform a backup. As such, in case of a wrong move, you will be able to return to your previous configuration

CHAPTER 2: PRESENTATION

6.2.1. Description

ASQ, an intrusion prevention and detection engine, is integrated into the whole range of NETASQ Firewall appliances. Always keeping abreast with the evolution of internet security technologies, NETASQ's Research and Development laboratories have been developing the ASQ since 1998. This intelligent engine integrates:

- An IPS (Intrusion Prevention System) which detects and gets rid of any malicious activity in real time.
- A filter engine (stateful inspection filtering) with rule optimization that allows the application of traffic control policies safely and effectively.
- An engine that detects known attacks (stateful pattern matching) using signature search optimization allowing comparisons in an appropriate context. Thus, there will be fewer false positives and unnecessary searches.

ASQ therefore intervenes on IP, fragment and global analyses, as well as on the filter policy, application protocols (via plugins) and comparisons against a database of known attacks.

This puts ASQ truly at the heart of the security that a NETASQ firewall provides.

DEFINITION
IPS (*Intrusion Prevention System*): System that enables detecting and blocking intrusion attempts, from the Network level to the Application level in the OSI model.

Nowadays, countermeasures are very complicated to implement and are specific in respect of denial of service attacks, for instance. Theoretically, most attacks aiming at creating denials of service are based on standard services or protocols on the internet. Protecting oneself would amount to cutting off normal communication lines with the internet, which in fact is the main purpose of the hosts concerned (web servers, mail servers, etc…).

Yet, something still has to be done to ensure the security of data in the enterprise. All this involves many steps: traffic has to be monitored (this being far from simple, taken for granted the amount of data which passes through), behavioral profiles have to be determined, and acceptable deviations have to be defined, beyond which one is considered the object of an attack. It is also necessary to define the attack types against which to be protected (with supporting risk analyses) as it is impossible to anticipate all of them. An intelligent and flexible protection system would be needed.

ASQ meets all these constraints, and with its traffic analysis, prevents the main attack families from taking place in real time.

6.2.1.1. Network interfaces

The link is made at two levels:

- At the Ethernet level for performing bridging functions.
- At the IP level for scanning IP traffic and higher protocols (TCP, UDP, HTTP,…).

6.2.1.2. Configuration and audit

The engine that defines the reaction (pass or block) to packets is configured by an interface between the kernel and the user programs. This FreeBSD-based interface uses the ioctl mechanism to send configuration parameters and to retrieve audit logs that ASQ generates.

Asqd

- Enables the retrieval of entries that allow the creation of audit files.
- Enables the distribution of alarm information to different modules such as serverd, snmp, etc.
- Enables the synchronization of the status of the engine with configuration files.

Serverd

- Allows providing real-time information on the ASQ status, statistics and alarms (monitoring functions).
- Allows updating ASQ configuration files.

Sfctl

- Allows configuring in administrator mode (console) which includes SSH remote access and direct access via the screen/keyboard serial port.
- Used by scripts for modifying the ASQ status (dialup load balancing routing…)
- Used during the firewall boot sequence for the initial configuration of the product before loading the various services.

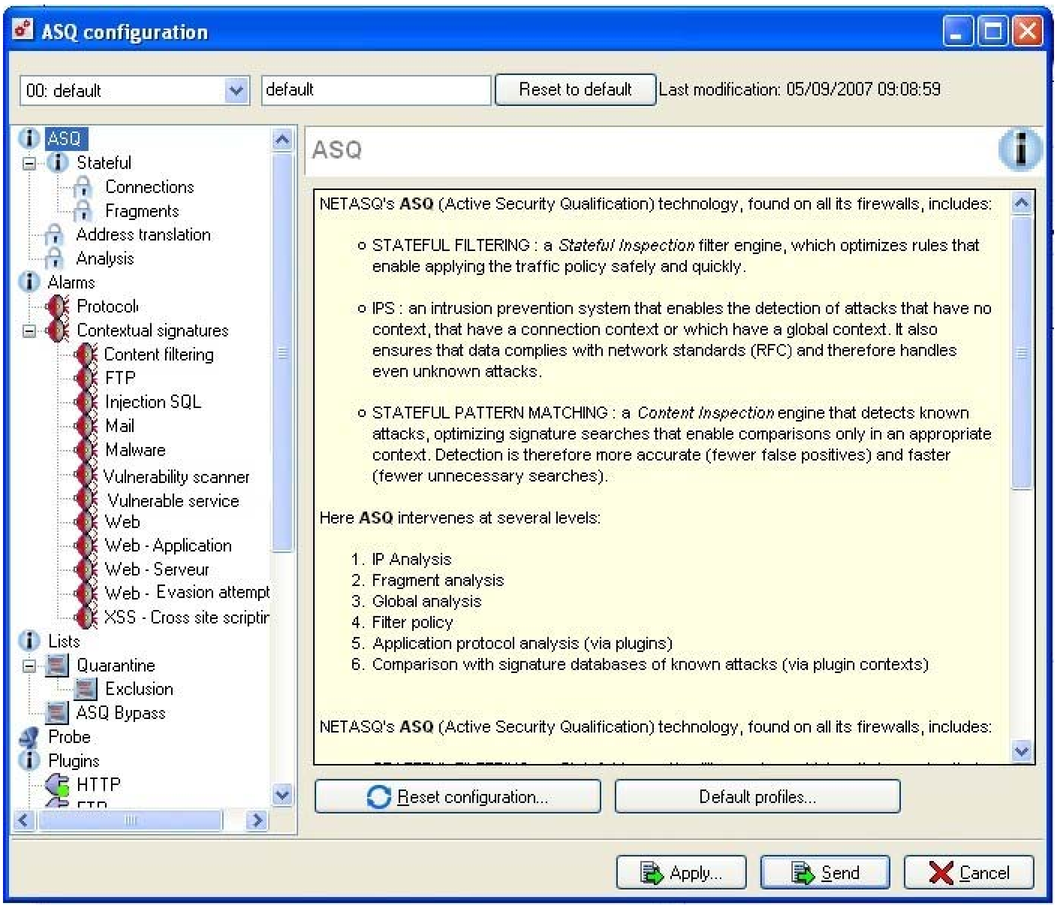
6.2.2. Configuration window

The configuration menu offers 5 ways in which ASQ can be applied:

- Configuration of the firewall's behavior with regards to traffic that passes through it.
- Configuration of alarms and signatures.
- Configuration of quarantine.
- Configuration of probes.
- Configuration of plugins.

The ASQ tab in the Configuration menu comprises two sections:

- On the left, a directory of features from the **`Intrusion Prevention`** menu
- On the right, options that can be configured.



NETASQ's **ASQ** (Active Security Qualification) technology, found on all its firewalls, includes:

- STATEFUL FILTERING : a *Stateful Inspection* filter engine, which optimizes rules that enable applying the traffic policy safely and quickly.
- IPS : an intrusion prevention system that enables the detection of attacks that have no context, that have a connection context or which have a global context. It also ensures that data complies with network standards (RFC) and therefore handles even unknown attacks.
- STATEFUL PATTERN MATCHING : a *Content Inspection* engine that detects known attacks, optimizing signature searches that enable comparisons only in an appropriate context. Detection is therefore more accurate (fewer false positives) and faster (fewer unnecessary searches).

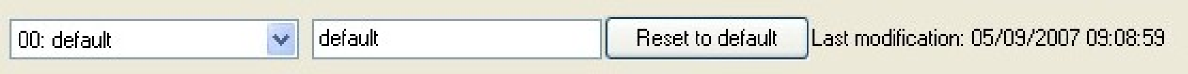
Here **ASQ** intervenes at several levels:

1. IP Analysis
2. Fragment analysis
3. Global analysis
4. Filter policy
5. Application protocol analysis (via plugins)
6. Comparison with signature databases of known attacks (via plugin contexts)

NETASQ's **ASQ** (Active Security Qualification) technology, found on all its firewalls, includes:

Figure 124: ASQ Configuration– ASQ

6.2.2.1. Multi-profile



Last modification: 05/09/2007 09:08:59

Figure 125: Multi-profile

Four ASQ profiles can now be created in order to adapt the ASQ analysis to traffic types and traffic direction. This will enable deactivating certain alarms on authorized outgoing traffic but not on incoming traffic (see *Part 7/Chapter 2: Editing a filter policy*).

The action bar at the top of the screen indicates the ASQ profile currently on display. You can name each of the profiles.

- 00: default
- 01: Profile1
- 02: Profile2
- 03: Profile3

The **Reset configuration** button enables you to redefine the parameters of ASQ profiles in their original configuration.

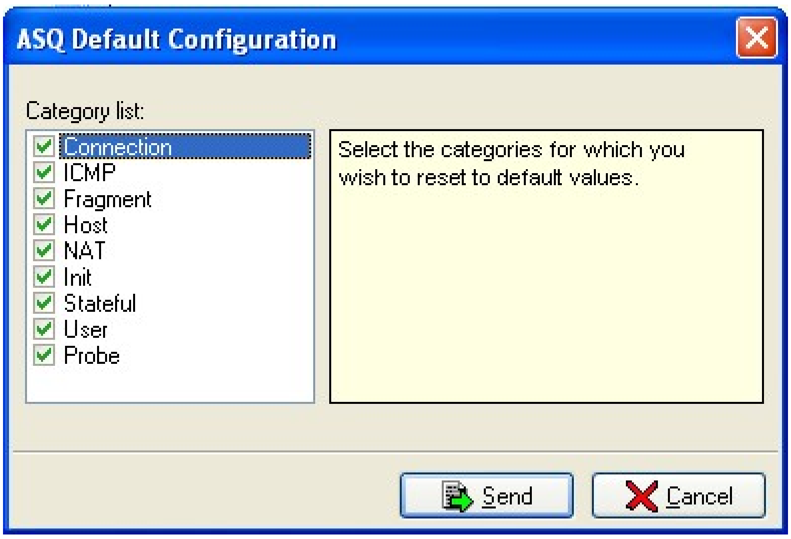
The date located next to the button indicates the date the configuration was last modified.

6.2.2.2. Applying changes

The **Apply** button located in the action bar at the bottom of the ASQ configuration window enables you to apply configured changes without having to close the window.

6.2.2.3. Default ASQ configuration

Clicking on the button **Reset configuration** will open the window below:



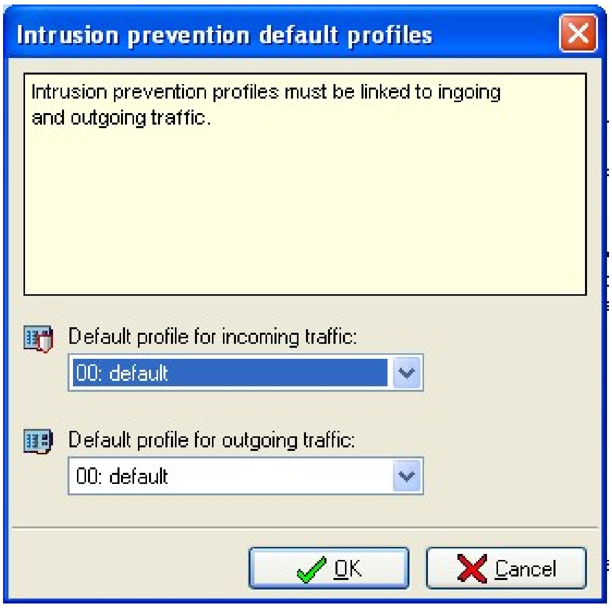
Select the categories for which you wish to reset to default values.

Figure 126: Default ASQ configuration

Here, you will be able to select and deselect one or several categories to reset. The values by default associated with the category will be restored.

6.2.2.4. Default ASQ profiles

ASQ profiles have to be linked to incoming or outgoing traffic.
The button **Default profiles** will display the following window:



Intrusion prevention profiles must be linked to ingoing and outgoing traffic.

Default profile for incoming traffic: 00: default

Default profile for outgoing traffic: 00: default

Figure 127: Default profiles - ASQ

In this window, you will be able to select a default profile for incoming and outgoing traffic.

By default, the profile 00 is assigned to incoming connections (from unprotected interfaces) whereas the profile 01 is assigned to outgoing connections (from protected interfaces).

Profiles are not migrated when you upgrade from version 6.3 to 7.0, therefore your configuration will not be modified. However, you will not benefit from this distinction between incoming and outgoing connections.

When the Defaultconfig command is executed, the configuration will be as follows:

- "IncomingProfile=00" and "OutgoingProfile=01"
- 00 is based on the "Medium" profile
- 01 is based on the "Internet" profile

CHAPTER 3: STATEFUL

This module allows datatracking on TCP connections.

The configuration parameters for the **`Stateful`** module, which analyzes packets dynamically, can be changed in the menu **`Intrusion prevention\Stateful`**.

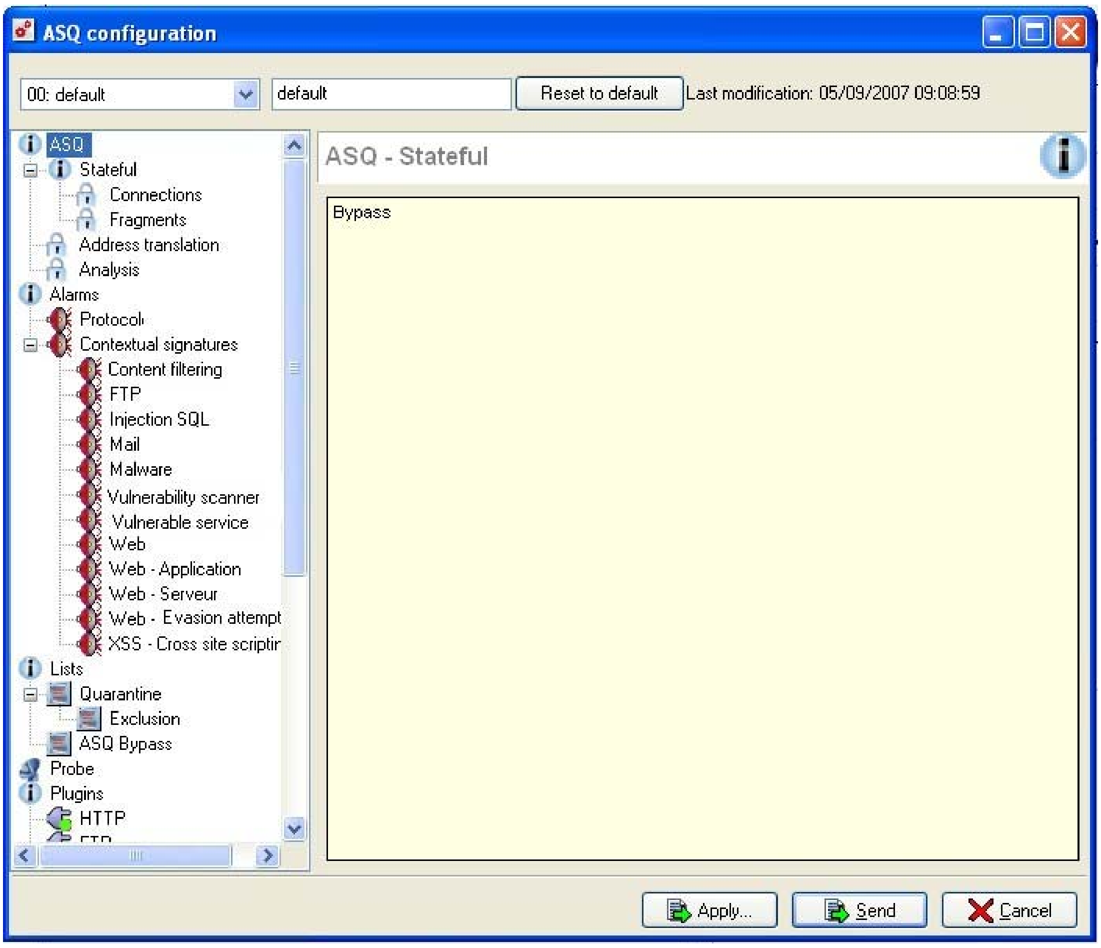


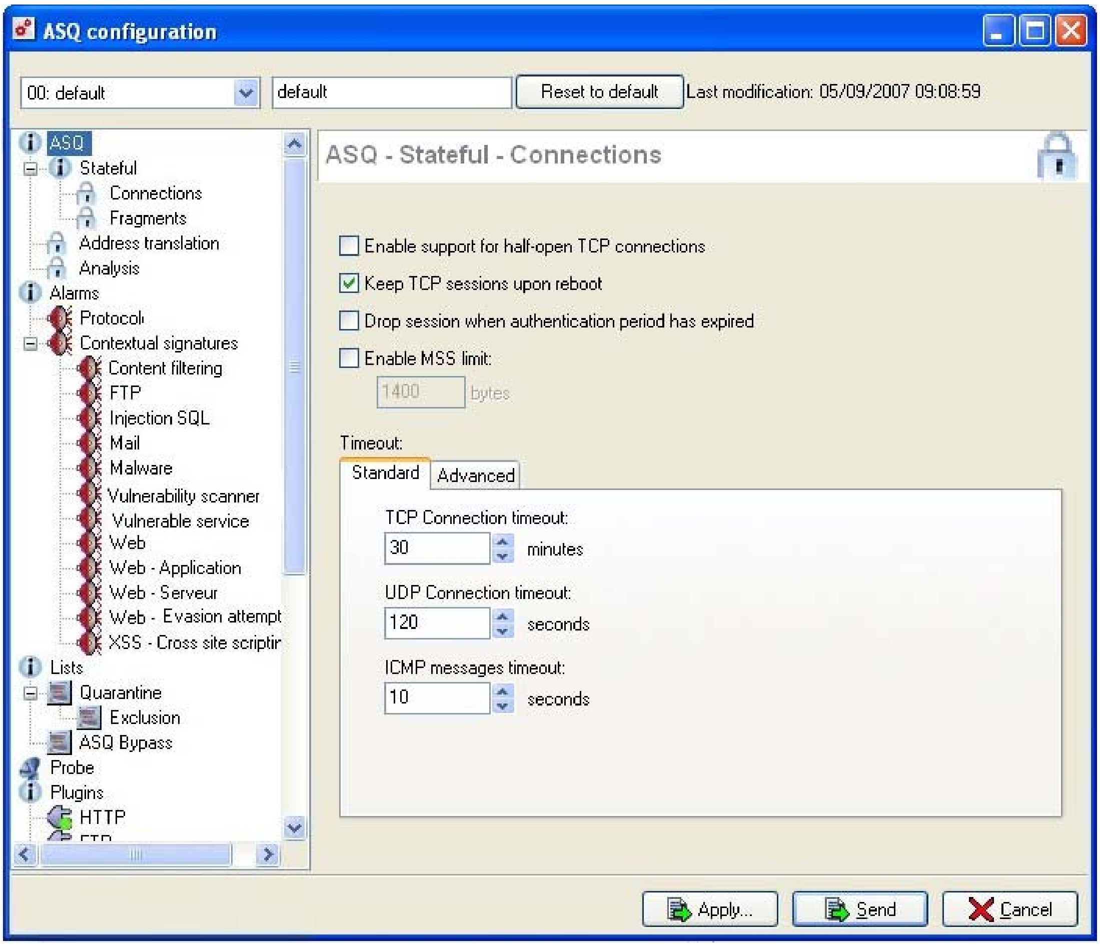
Figure 128: ASQ configuration - Stateful

This module, which is integrated into the ASQ module, preserves the state of connections and analyzes the packets to detect hacking. “Stateful” means that you need only define the “going” filter rules (rule indicating the direction of the connection); you need not specify the return rule (reply by the host contacted by the initiator of the connection).

REMARK
The firewall has to be rebooted whenever you enable or disable datatracking.

The **`Stateful`** engine configuration menu is divided into two sections: **`Connections`** and **`Fragments`**. The parameters that can be configured in these sections are explained in the following tables:

6.3.1. Connections



ASQ configuration

00: default | default | Reset to default | Last modification: 05/09/2007 09:08:59

ASQ - Stateful - Connections

☐ Enable support for half-open TCP connections

☑ Keep TCP sessions upon reboot

☐ Drop session when authentication period has expired

☐ Enable MSS limit:

1400 bytes

Timeout:

Standard | Advanced

TCP Connection timeout: 30 minutes

UDP Connection timeout: 120 seconds

ICMP messages timeout: 10 seconds

Figure 129: ASQ configuration - Connections

Enable support for half open TCP connections	A peer has shut down his connection and the other continues to transmit packets. The connection is therefore unidirectional. By default, this option is disabled.
Keep TCP sessions upon reboot	When this option has been activated, the Firewall memorizes the connection context when it reboots. Connections are therefore not interrupted. This option has to be activated so that connections are preserved during the switchover in high availability. By default, this option is disabled.
Drop session when authentication period has expired	This option enables closing active connections at the end of the authentication period. By default, this option is disabled.
Enable MSS limit	The Firewall will re-dimension TCP packets (but not UDP) to the size indicated in the “Enable MSS limit” field. This function is useful for PPPoE or VPN-type connections as the packets must not exceed a given size (otherwise they are fragmented or rejected). The recommended value is 1300 bytes.

WARNING

Using the option Enable support for half open TCP connections is not recommended. Selecting this option allows transmitting packets which jeopardize the integrity of resources protected by the

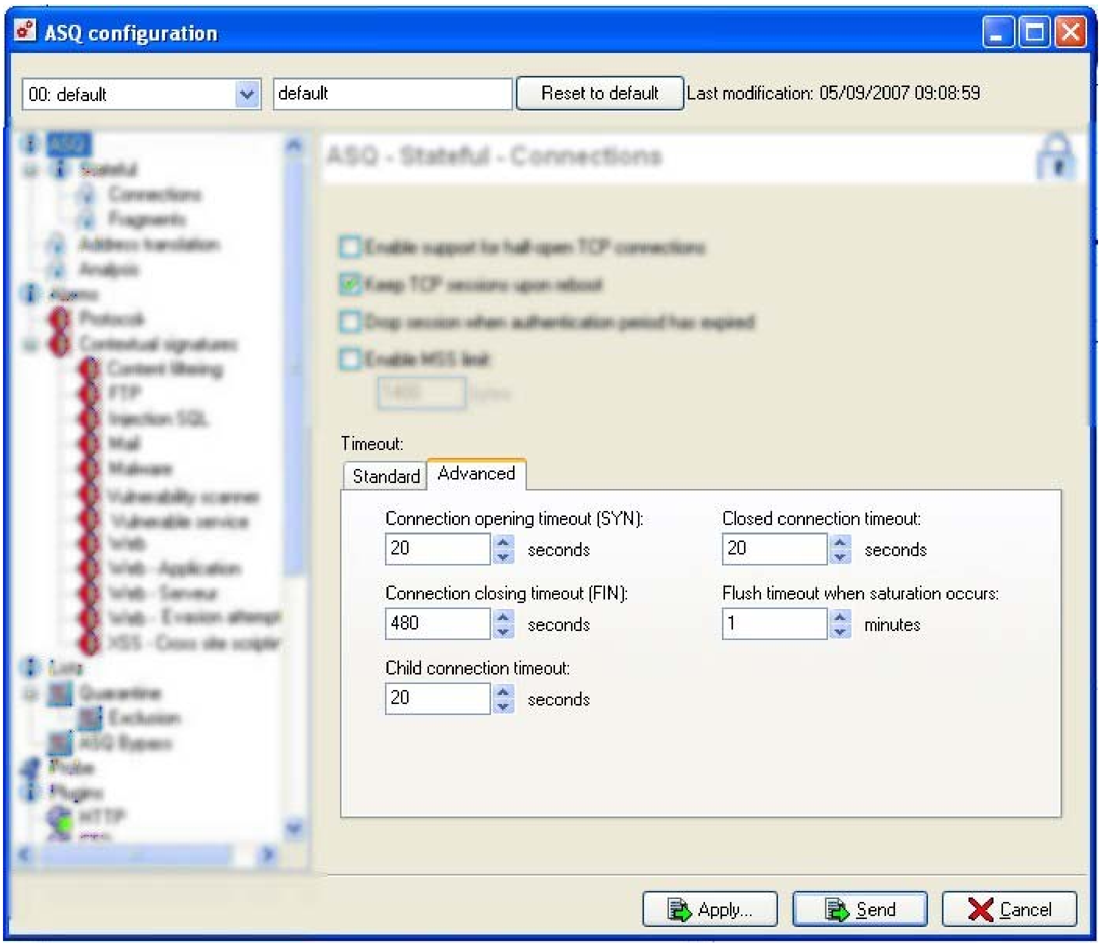
Firewall. This option is supported because of its compatibility with TCP and should only be used with full knowledge of its consequences.

6.3.1.1. Standart timeouts

Standard timeouts can be configured on the Firewall. They are explained in the table below:

TCP Connection	Amount of time after which TCP connections will be reinitialized. This may range from 10 to 100800 minutes. By default, timeout is indicated as 30 minutes.
UDP Connection	Amount of time after which UDP connections will be reinitialized. This may range from 30 to 3600 seconds. By default, timeout is indicated as 120 seconds.
ICMP Messages	Amount of time ICMP messages will be kept. This may range from 2 to 60 seconds. By default, they will be kept for 10 seconds.

6.3.1.2. Advanced timeouts



00: default | default | Last modification: 05/09/2007 09:08:59

□ Enable support for half-open TCP connections
☑ Keep TCP sessions upon reboot
□ Drop session when authentication period has expired
□ Enable MSS limit
1460 bytes

Timeout: Standard | Advanced

Connection opening timeout (SYN): 20 seconds
Closed connection timeout: 20 seconds
Connection closing timeout (FIN): 480 seconds
Flush timeout when saturation occurs: 1 minutes
Child connection timeout: 20 seconds

Figure 130: Timeout - Advanced

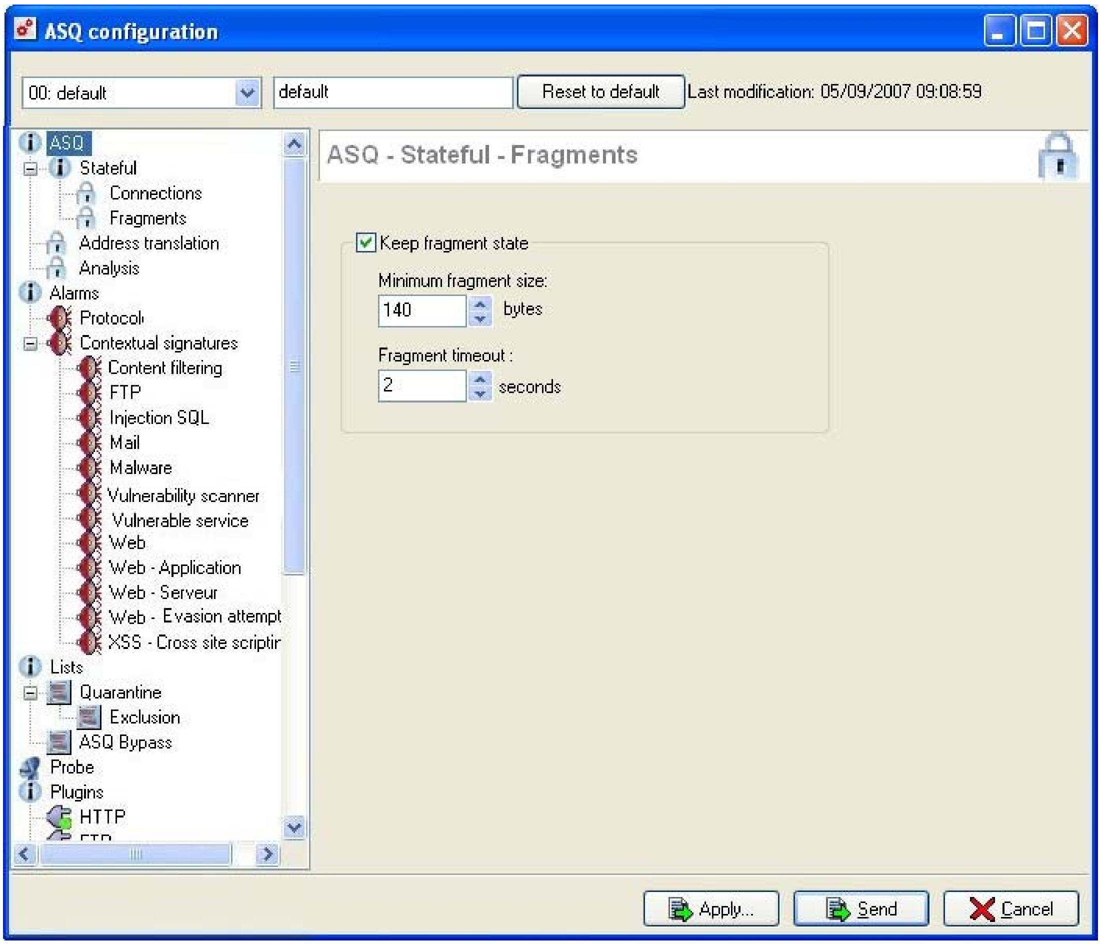
Advanced timeouts can be configured on the Firewall. They are explained in the table below:

Connection opening (SYN)	Maximum amount of time allowed for opening a TCP connection (SYN, SYN-ACK, ACK). This may range from 10 to 60 seconds. By default, the time indicated is 20 seconds.
Connection	Maximum amount of time allowed for closing a TCP connection (FIN, FIN-ACK, FIN,

closing (FIN)	FIN-ACK). This may range from 10 to 3600 seconds. By default, the time indicated is 480 seconds.
Closed connection	Connections using the same source and destination addresses and ports as in previous connections cannot be established during this **Closed connection** timeout. This may range from 10 to 60 seconds. By default, the time indicated is 20 seconds.
Child connection	Amount of time during which an attempt to establish a child connection will be tolerated. This may range from 10 to 60 seconds. By default, the time indicated is 20 seconds.
Flush when saturated	When the ASQ connection table is full and a new connection is attempted, ASQ attempts to delete certain connections from its table (basically connections in the progress of being established) in order to make way for a place. It will try again during the period defined by this option. This flush may range from 1 to 2880 minutes (by default: 1).

6.3.2. Fragments

The size of packet fragments is now higher. Refer to the table below for more information on fragment size.



ASQ configuration

00: default

default

Last modification: 05/09/2007 09:08:59

ASQ - Stateful - Fragments

☑ Keep fragment state

Minimum fragment size: 140 bytes

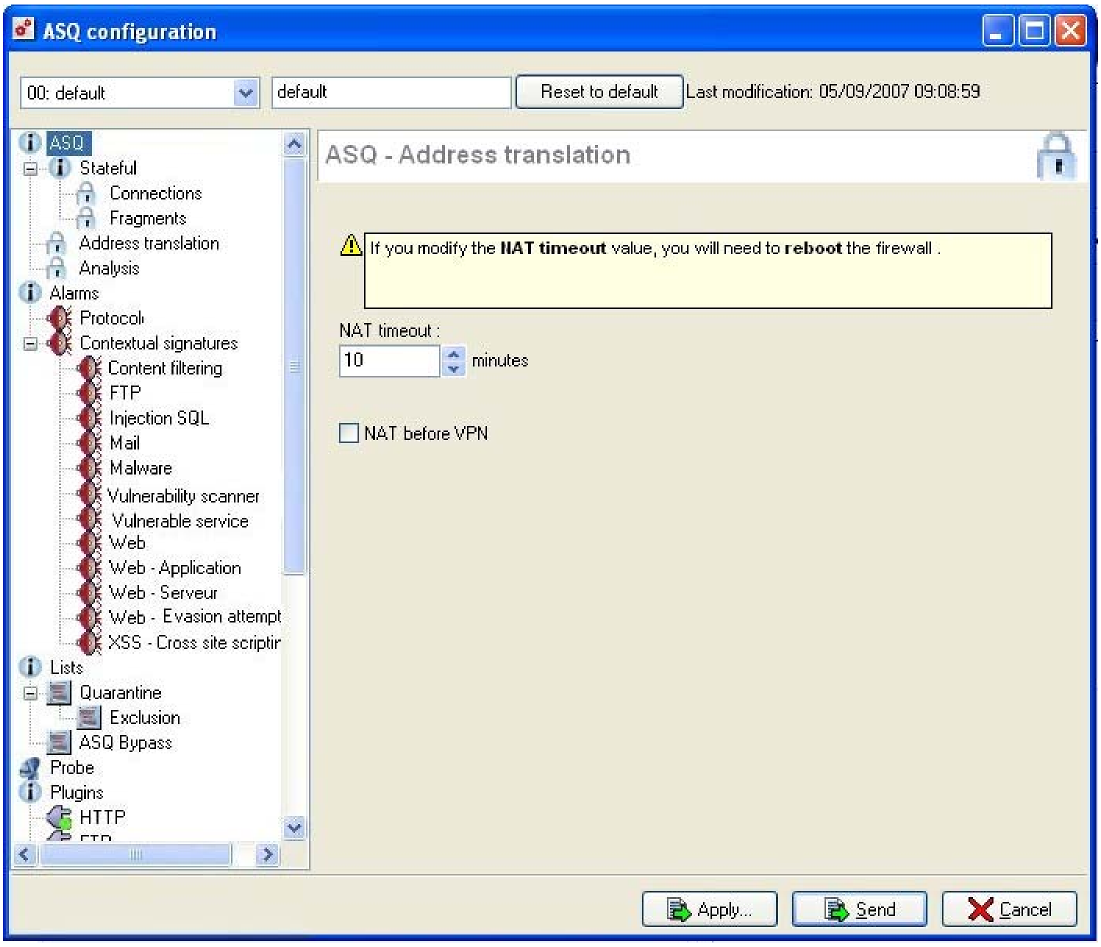
Fragment timeout : 2 seconds

Figure 131: ASQ configuration - Fragments

Keep fragment	If this option has been selected, the Firewall analyzes fragmented IP packets in

state	order to determine possible IP packet fragmentation attacks. If this option has not been activated, the Firewall will not allow fragmented packets to pass through.
Minimum fragment size	Minimum fragment size. At least 140 bytes, maximum 32757 bytes (by default: 140).
Fragment timeout	Amount of time to keep fragments passing through the Firewall. Any number between 2 and 30 seconds (by default: 2).

CHAPTER 4: NAT (ADDRESS TRANSLATION)



00: default | default | Last modification: 05/09/2007 09:08:59

ASQ - Address translation

If you modify the **NAT timeout** value, you will need to **reboot** the firewall .

NAT timeout : 10 minutes

□ NAT before VPN

Figure 132: ASQ configuration – Address translation

A section in ASQ configuration is reserved for address translation analysis on the Firewall. In fact, ASQ influences the way in which NAT is handled.

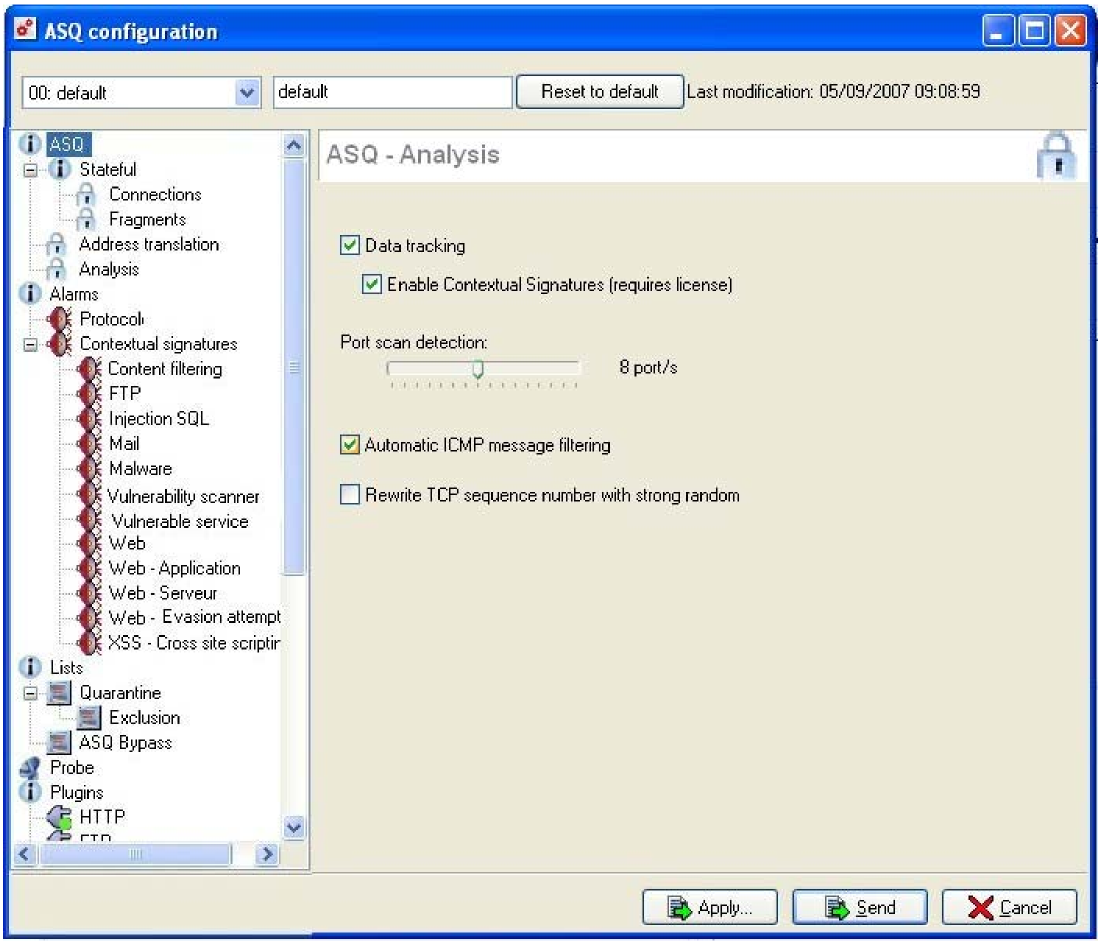
NAT timeout	Time after which connections involving network address translation are reset. This can be between 10 and 10080 minutes (by default: 10). **WARNING** The Firewall will reboot if the NAT timeout is modified.
NAT before VPN	Occasionally, NAT and VPN features may be incompatible. IPSEC VPN uses a hash function to authenticate the different packets of a VPN connection. This hash function is based on information contained in the packet header. However, NAT features modify this header, so the header and VPN hash no longer

correspond and the remote VPN peer will reject the associated packet.
To avoid the occurrence of this incompatibility, select the option **NAT before VPN** so that NAT operations can be applied before the calculation of the VPN hash.

CHAPTER 5: ANALYSIS

The traffic analysis window sets out the parameters concerning plugins. These parameters have a heavy influence on the security that the firewall offers.

➲ The configuration parameters in the **Analysis** module can be modified in the menu **`Intrusion prevention\Analysis`** in the ASQ menu directory.



00: default | default | Reset to default | Last modification: 05/09/2007 09:08:59

ASQ - Analysis

☑ Data tracking

☑ Enable Contextual Signatures (requires license)

Port scan detection: 8 port/s

☑ Automatic ICMP message filtering

□ Rewrite TCP sequence number with strong random

Figure 133: ASQ configuration - Analysis

Data tracking The firewall analyzes the coherence of data contained in packets and in their headers as well as the coherence of several fragmented packets (to prevent data-evasion attacks).

- Disabling this option prevents ASQ from using plugins.
- If the option is enabled (as it is by default), it may be possible to enable pattern matching (enabled by default).

WARNING
Activating or deactivating Data Tracking will make the Firewall reboot.

Enable contextual This option enables activating analyses based on contextual signatures.

signatures	
Port scan detection	If this option is selected the Firewall can detect port scans, including stealth scans (based on host responses to FIN packets and not to SYN packets. In most cases these scans are not logged by the scanned hosts because no SYN packet has been received). It is possible to determine the number of ports which may be scanned before the alarm was triggered. The sensitivity of the port scan detection can vary between 1 and 16 ports per second (by default: 8).
Automatic ICMP message filtering	This option allows ICMP messages to pass if they are coherent in a TCP, UDP or ICMP connection (intelligent filtering of ICMP packets). (enabled by default).
Rewrite TCP sequence number with strong random	In order to offset systems generating packets with weakly random sequence numbers, it is possible to activate this option. The Firewall will "rewrite" packets using a more unpredictable sequence number. (disabled by default).

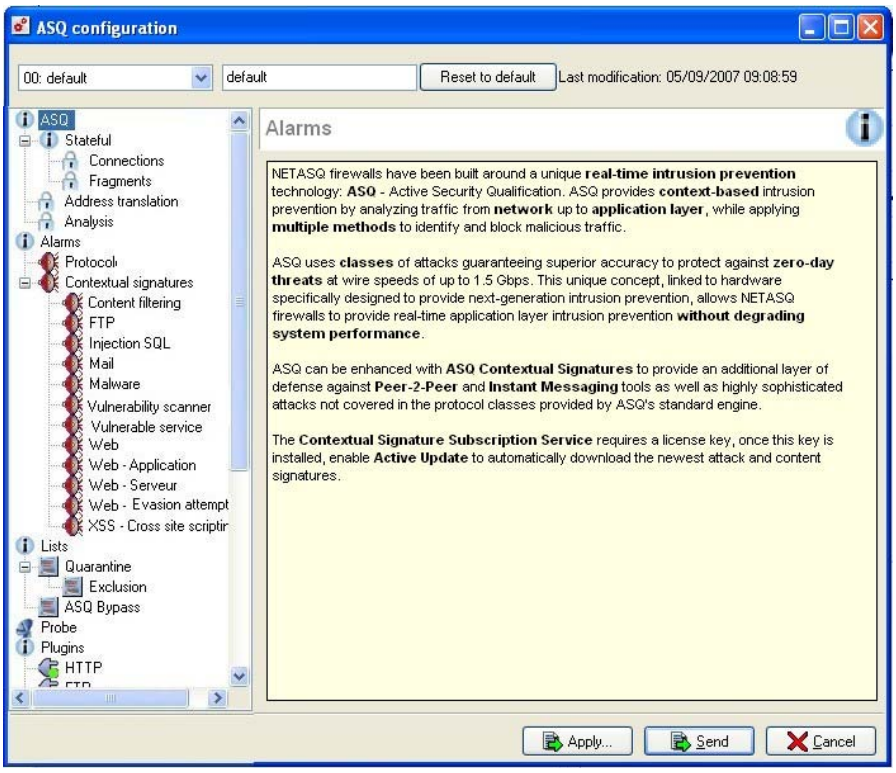
CHAPTER 6: ALARMS

ASQ (***Active Security Qualification***) is a unique real-time intrusion prevention technology that provides context-based intrusion prevention by analyzing traffic from network up to application layer, while applying multiple methods to identify and block malicious traffic.

ASQ uses classes of attacks, guaranteeing superior accuracy to protect against zero-day threats. This preventive measure is conducted in real time without degrading system performance.

The firewall's behavior can be finely configured according to each alarm that is likely to arise when traffic containing malicious elements is detected.

➲ Configuration parameters in the **Alarms** module can be modified in the `Alarms` menu in the ASQ configuration menu directory.



00: default

default

Last modification: 05/09/2007 09:08:59

NETASQ firewalls have been built around a unique **real-time intrusion prevention** technology: **ASQ** - Active Security Qualification. ASQ provides **context-based** intrusion prevention by analyzing traffic from **network** up to **application layer**, while applying **multiple methods** to identify and block malicious traffic.

ASQ uses **classes** of attacks guaranteeing superior accuracy to protect against **zero-day threats** at wire speeds of up to 1.5 Gbps. This unique concept, linked to hardware specifically designed to provide next-generation intrusion prevention, allows NETASQ firewalls to provide real-time application layer intrusion prevention **without degrading system performance**.

ASQ can be enhanced with **ASQ Contextual Signatures** to provide an additional layer of defense against **Peer-2-Peer** and **Instant Messaging** tools as well as highly sophisticated attacks not covered in the protocol classes provided by ASQ's standard engine.

The **Contextual Signature Subscription Service** requires a license key, once this key is installed, enable **Active Update** to automatically download the newest attack and content signatures.

Figure 134: ASQ configuration - Alarms

For each attack that the NETASQ firewall manages, the administrator who has modification rights can define whether to transmit or destroy the offending packet(s), and if necessary, to generate a security event bearing an alarm level, which will be automatically saved in the **Alarm** log file.

The list in this window groups together all the attacks and attack families that the firewall manages.

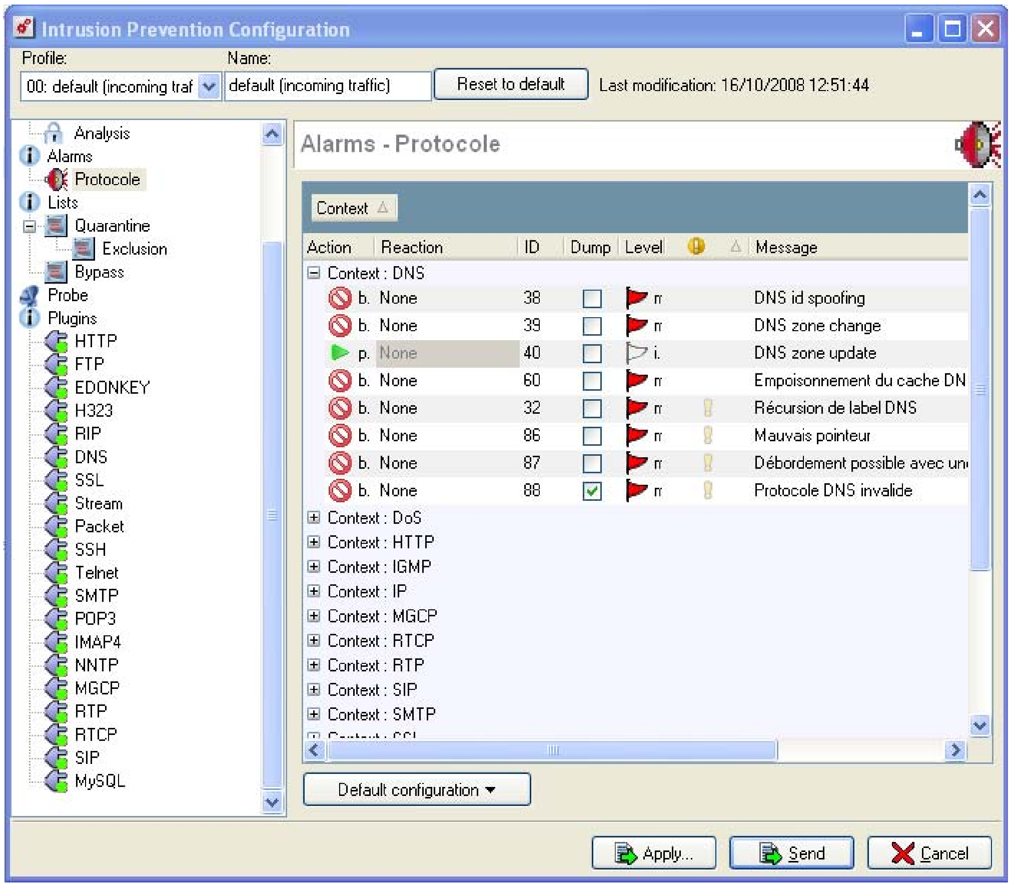
Alarms are divided into two categories:

- **Protocol** alarms: associated with ASQ's protocol analyses
- **Contextual signatures** alarms: associated with contextual signature analyses. This is a list of alarms that were raised when ASQ detects a particular sequence in the network traffic. These signatures are classified in categories, which the firewall retrieves and updates in order to counter more recent threats.

NOTE
The contextual signature analysis module requires an additional licence which comes with a charge

6.6.1. Protocol alarms

Protocol alarms have almost the same properties as contextual signatures (except for **Details** and **New**).



Profile: 00: default (incoming traf
Name: default (incoming traffic)
Last modification: 16/10/2008 12:51:44

Action	Reaction	ID	Dump	Level		Message
⊟ Context : DNS						
b.	None	38	□	m		DNS id spoofing
b.	None	39	□	m		DNS zone change
p.	None	40	□	i.		DNS zone update
b.	None	60	□	m		Empoisonnement du cache DN
b.	None	32	□	m		Récursion de label DNS
b.	None	86	□	m		Mauvais pointeur
b.	None	87	□	m		Débordement possible avec un
b.	None	88	☑	m		Protocole DNS invalide
⊞ Context : DoS						
⊞ Context : HTTP						
⊞ Context : IGMP						
⊞ Context : IP						
⊞ Context : MGCP						
⊞ Context : RTCP						
⊞ Context : RTP						
⊞ Context : SIP						
⊞ Context : SMTP						

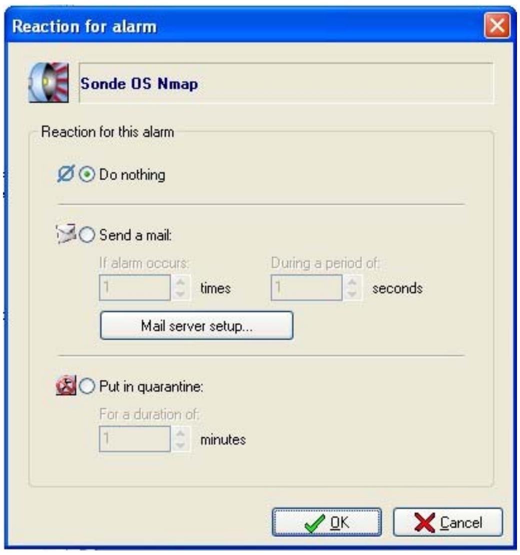
Figure 135: ASQ configuration – Protocol

There are six columns in the table:

Context Alarms are grouped in the following categories: DNS, DOS, FTP, HTTP, ICMP, IGMP, IP, Miscellaneous, SMTP, Scan, TCP, UDP, MGCP and SSL.

Action When an alarm is generated, the packet which set off the alarm undergoes the associated action. The action may be "block" or "pass". If the action is displayed in gray, this means that this action may not be modified.

Reaction Other than the action to take on the alarm, a reaction to the generation of an alarm can be defined from the following: **Send an e-mail**, **Quarantine the host** or **Do nothing**.



Reaction for alarm

Sonde OS Nmap

Reaction for this alarm

● Do nothing

○ Send a mail:

If alarm occurs: 1 times During a period of: 1 seconds

○ Put in quarantine:

For a duration of: 1 minutes

Figure 136: Reaction for alarm

1) **Send an e-mail:** when the mail service has been activated (see Part16/Chapter 1: *Mail server configuration*) mail sending can be defined when two factors justify it: the number of times the alarm has been raised and the period in which this takes place

2) **Quarantine**: quarantining enables blocking all traffic coming from the host responsible for raising the alarm. Dynamic quarantining is assigned a duration (in minutes) and is affected when the Firewall is rebooted (the list of quarantined hosts will be reset during the reboot). This can last from 1 to 7200 minutes (by default: 1).

ID Indicates the ID of the alarm considered sensitive.

Dump This option enables saving the packet responsible for raising the alarm. The size of the information saved depends on your Firewall's model. This packet can then be viewed with the NETASQ REAL-TIME MONITOR (*Refer to the NETASQ REAL-TIME MONITOR manual*).

Level Three levels of alarms are available – ignore, minor and major.

⚠ Informs with an indicator whether the alarm will pose a security problem if it is set to "Pass". If so, the help panel will display a warning.

This option is valid only for protocol alarms. The icon will be grayed out if the action is "Block".

For further information, please refer to the explanation in *Part 6/CHAPTER 9: plugin Pass_detach*

Message This corresponds to the alarm name. Additional information on the alarm is available in the NETASQ UNIFIED MANAGER via links in this column.

When you right-click on a line, a contextual menu will appear, offering the following options: **Select All**, **Select None**, **Invert the selection**, **Tag**.

6.6.1.1. Protection profiles

The **Default configuration** button allows you to redefine alarm configuration according to 4 available protection profiles:

- Low
- Medium
- High
- Internet

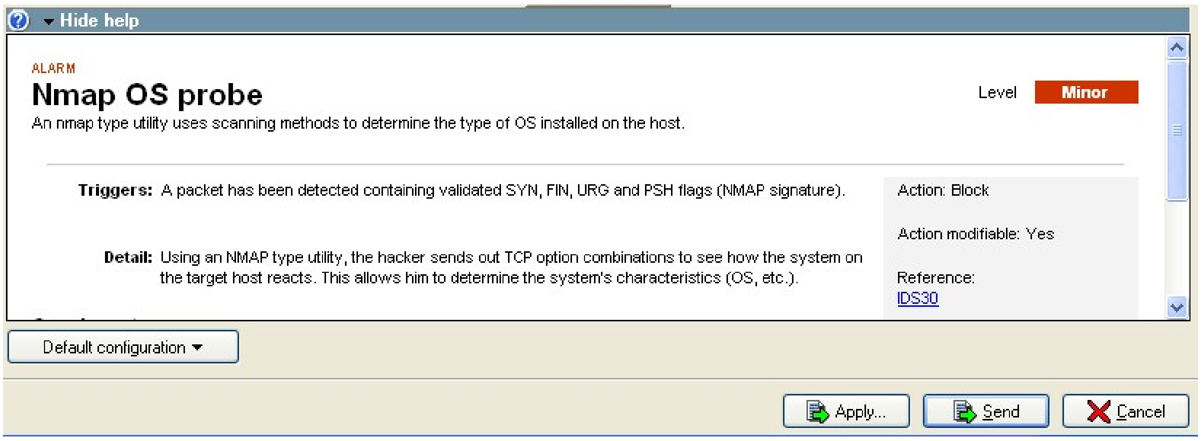
WARNING
When a security profile is applied, it will erase all the values that could have been customized for each alarm.

6.6.1.2. Online help

Each protocol alarm is explained in an individual page in the NETASQ UNIFIED MANAGER application. The procedure is as follows for viewing online help associated with a protocol alarm:

1 Select the protocol alarm for which you need an explanation.

2 Click on the **Show help** option to display the help file corresponding to the selected protocol alarm. A help screen like the one below will appear:



ALARM

Nmap OS probe

An nmap type utility uses scanning methods to determine the type of OS installed on the host.

Level: Minor

Triggers: A packet has been detected containing validated SYN, FIN, URG and PSH flags (NMAP signature).

Detail: Using an NMAP type utility, the hacker sends out TCP option combinations to see how the system on the target host reacts. This allows him to determine the system's characteristics (OS, etc.).

Action: Block

Action modifiable: Yes

Reference: IDS30

Figure 137: Help - Alarms

6.6.2. Contextual signatures

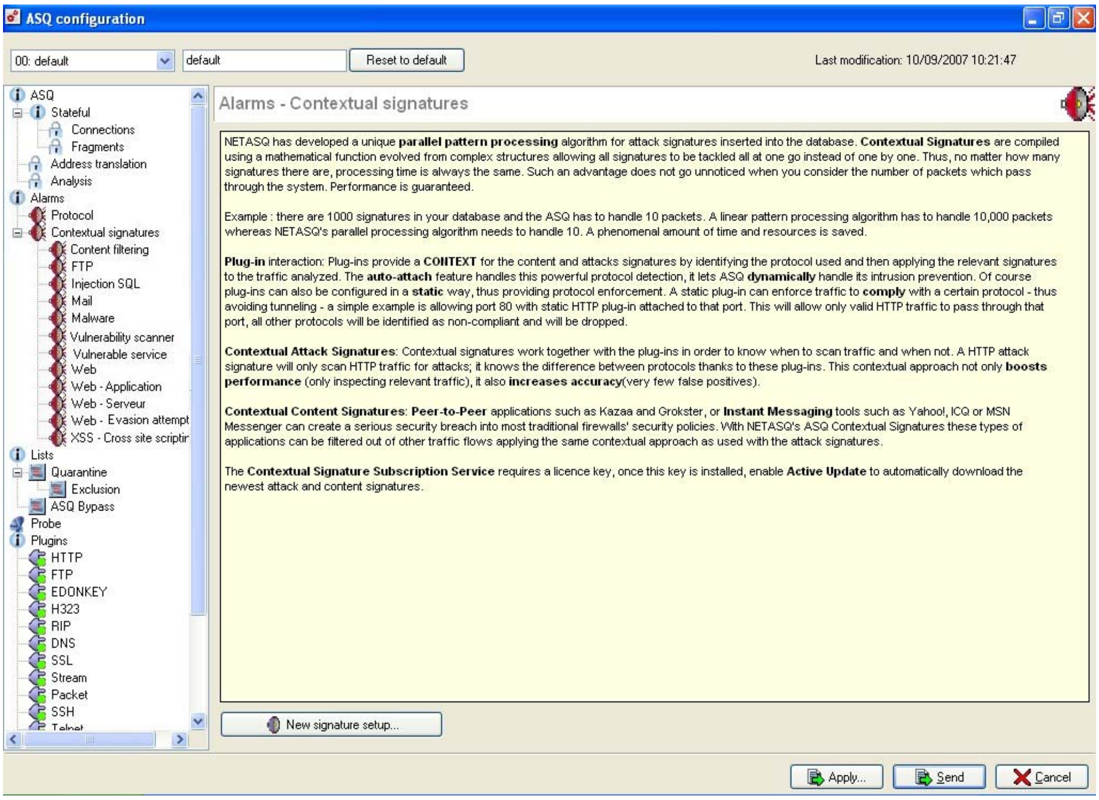
6.6.2.1. Presentation

Attacks which aim to exploit local client or server implementation errors are blocked by the contextual signature-based intrusion prevention and detection module so that additional defense can be provided against attacks, whether they are standard or more sophisticated attacks, which are not covered by the engine's protocol analyses, as well as Peer-to-Peer (Kasaa, Gnutella), instant messengers (Yahoo, MSN, AOL Messenger). This database which complements other analyses, enables refining the global traffic analysis that the NETASQ Firewall perfoms by removing the disadvantages present in the usual pattern-matching systems (eg IDS), mainly, false positives. Furthermore, the ability to save the context makes the NETASQ system even more efficient.

NOTE

Regular updates are available for ASQ contextual signatures, new applications, new attacks or even existing signatures via the *Maintenance* menu in NETASQ UNIFIED MANAGER.

The analysis of ASQ plugins enable the definition of a context for activating contextual signatures. As such, only contextual signatures that correspond to a type of traffic that the plugins detect will be used during the analysis.



NETASQ has developed a unique **parallel pattern processing** algorithm for attack signatures inserted into the database. **Contextual Signatures** are compiled using a mathematical function evolved from complex structures allowing all signatures to be tackled all at one go instead of one by one. Thus, no matter how many signatures there are, processing time is always the same. Such an advantage does not go unnoticed when you consider the number of packets which pass through the system. Performance is guaranteed.

Example : there are 1000 signatures in your database and the ASQ has to handle 10 packets. A linear pattern processing algorithm has to handle 10,000 packets whereas NETASQ's parallel processing algorithm needs to handle 10. A phenomenal amount of time and resources is saved.

Plug-in interaction: Plug-ins provide a **CONTEXT** for the content and attacks signatures by identifying the protocol used and then applying the relevant signatures to the traffic analyzed. The **auto-attach** feature handles this powerful protocol detection, it lets ASQ **dynamically** handle its intrusion prevention. Of course plug-ins can also be configured in a **static** way, thus providing protocol enforcement. A static plug-in can enforce traffic to **comply** with a certain protocol - thus avoiding tunneling - a simple example is allowing port 80 with static HTTP plug-in attached to that port. This will allow only valid HTTP traffic to pass through that port, all other protocols will be identified as non-compliant and will be dropped.

Contextual Attack Signatures: Contextual signatures work together with the plug-ins in order to know when to scan traffic and when not. A HTTP attack signature will only scan HTTP traffic for attacks; it knows the difference between protocols thanks to these plug-ins. This contextual approach not only **boosts performance** (only inspecting relevant traffic), it also **increases accuracy**(very few false positives).

Contextual Content Signatures: **Peer-to-Peer** applications such as Kazaa and Grokster, or **Instant Messaging** tools such as Yahoo!, ICQ or MSN Messenger can create a serious security breach into most traditional firewalls' security policies. With NETASQ's ASQ Contextual Signatures these types of applications can be filtered out of other traffic flows applying the same contextual approach as used with the attack signatures.

The **Contextual Signature Subscription Service** requires a licence key, once this key is installed, enable **Active Update** to automatically download the newest attack and content signatures.

Figure 138: ASQ configuration – Contextual signatures

6.6.2.2. Interface

ASQ's contextual signatures are categorized in the NETASQ UNIFIED MANAGER graphical interface according to the functions they perform, the attacks they prevent or the type of traffic they monitor. The categories of contextual signatures are as follows:

- Context filters
- FTP
- SQL Injection
- Mail
- Malware
- Vulnerability scanner
- SEISMO: integrating SEISMO signatures improves performance. The watch is mutualized between the attacks and vulnerabilities.

- Vulnerable services
- Web
- Web-Application
- Web-Server
- Web-Evasion attempt
- XSS- Cross site scripting

The contextual signature grid consists of seven columns:

Context	Alarms are grouped by context, therefore signatures apply only in a certain context, enabling the reduction of the number of false positives, thus obtaining better performance.
Action	When an alarm is generated, the packet which set off the alarm undergoes the associated action. The action may be “block” or “pass”. If the action is displayed in gray, this means that this action may not be modified.
Reaction	Other than the action to take on the alarm, a reaction to the generation of an alarm can be defined from the following: **Send an e-mail**, **Quarantine the host** or **Do nothing**. 1) **Send an e-mail:** when the mail service has been activated (see *Mail server configuration*) mail sending can be defined when two factors justify it: the number of times the alarm has been raised and the period in which this takes place. 2) **Quarantine**: quarantining enables blocking all traffic coming from the host responsible for raising the alarm. Dynamic quarantining is assigned a duration (in minutes) and is affected when the Firewall is rebooted (the list of quarantined hosts will be reset during the reboot).
Details	This option enables saving the packet responsible for raising the alarm. The size of the information saved depends on your Firewall’s model. If this option is enabled, a binary data buffer containing the suspect packet will be matched with the raised alarm. This packet can then be viewed in NETASQ REAL-TIME MONITOR or NETASQ EVENT REPORTER. (*Refer to the NETASQ REAL-TIME MONITOR and NETASQ EVENT REPORTER manuals*). This packet can be read with a tool like Wireshark or Packetyzer so that the contents can detailed.
Level	Three levels of alarms are available – ignore, minor and major.
New	This parameter indicates that the contextual signature is new in the list of contextual signatures downloaded from NETASQ’s website. The signature will remain **New** until the administrator unchecks it. Possible options: "Unchecked", "Checked", "Not checked in all profiles", "Checked in all profiles".
Message	This corresponds to the alarm name. Additional information on the alarm is available in the NETASQ UNIFIED MANAGER via links in this column. New unchecked messages will be displayed in bold.

6.6.2.3. Protection profiles

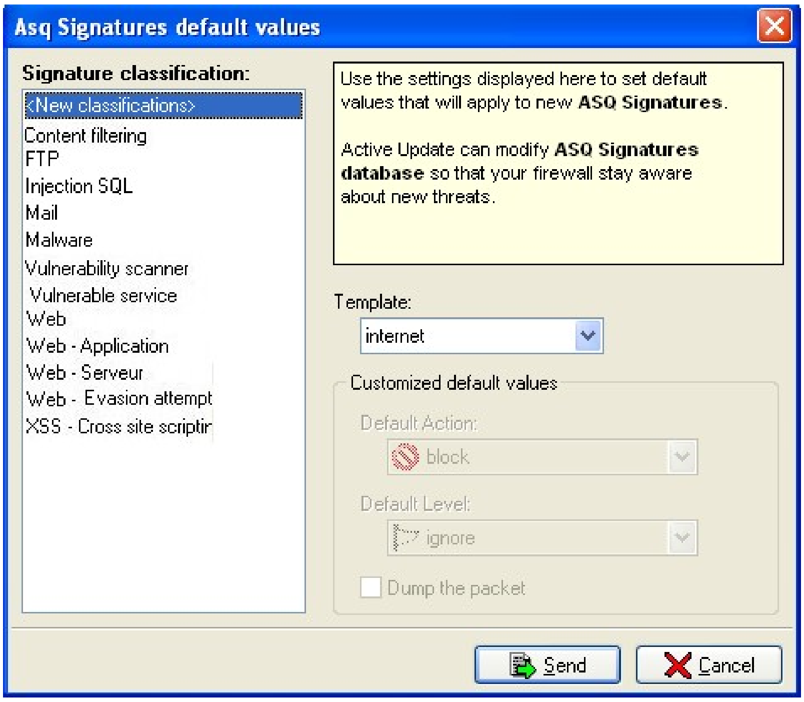
The **Default configuration** button allows you to redefine alarm configuration according to 4 available protection profiles:

- Low
- Medium
- High
- Internet: this profile is particularly adaption to the prevention of threats from the internet.

6.6.2.4. New signatures

The correct configuration of contextual signatures, especially in terms of actions (generation of alarms, blocking of malicious traffic, etc), guarantees the relevance of the Firewall's action on traffic monitored by these signatures and the security of the resources that the Firewall protects. For this purpose, NETASQ regularly updates these contextual signatures, but the task of managing the actions taken by these signatures is tedious for the administrator as he must regularly check for new signatures and configure their actions.

The option **New signatures** in the **`Contextual signatures`** sub-menu allows "preconfiguring" the behavior of future contextual signatures that will be downloaded from the contextual signature database during the update process. Preconfiguration is done according to category. All signatures belonging to a category will be configured with the parameters defined by the administrator.



Asq Signatures default values

Signature classification:

- <New classifications>
- Content filtering
- FTP
- Injection SQL
- Mail
- Malware
- Vulnerability scanner
- Vulnerable service
- Web
- Web - Application
- Web - Serveur
- Web - Evasion attempt
- XSS - Cross site scriptir

Use the settings displayed here to set default values that will apply to new **ASQ Signatures**.

Active Update can modify **ASQ Signatures database** so that your firewall stay aware about new threats.

Template: internet

Customized default values

Default Action: block

Default Level: ignore

□ Dump the packet

Figure 139: Default values of ASQ signatures

The table below lists the options in the **New signatures** menu:

Signature classification	The behavior of future signatures is preconfigured by category. The list in the "Signature classification" field sets out all the categories to be configured. 'New classifications" refers to categories of contextual signatures that do not exist yet.
Template	In the same way as for signatures that have already been downloaded, templates or protection profiles (low, medium, high, internet and custom) can be applied to future signatures. For the custom template, the administrator must define the default actions associated with these new contextual signatures.
Customized Default values	These options, which are only available during the creation of a custom template, enable the definition of default actions (default action: block or pass, default level: major, minor or ignore and delete the packet) associated with the new signatures in

	the selected classification.

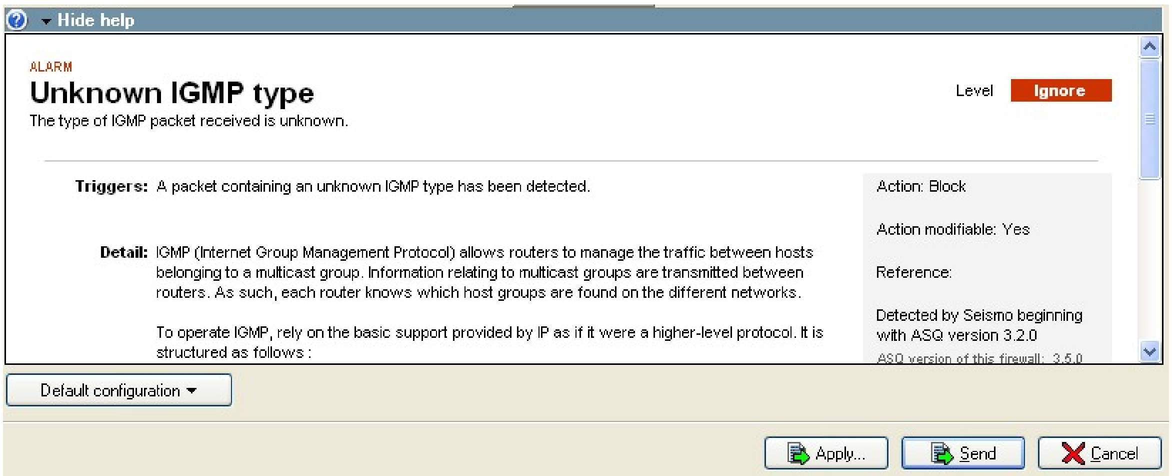
✪ New signatures are inserted into this database regularly by the firewall (Cf. Part18/Chapter 1: Active Update).

6.6.2.5. Online help

Each protocol alarm is explained in an individual page in the NETASQ UNIFIED MANAGER application. The procedure is as follows for viewing online help associated with a protocol alarm:

1 Select the protocol alarm for which you need an explanation.

2 Click on the **Show help** option to display the help file corresponding to the selected protocol alarm.



ALARM

Unknown IGMP type

The type of IGMP packet received is unknown.

Level Ignore

Triggers: A packet containing an unknown IGMP type has been detected.

Detail: IGMP (Internet Group Management Protocol) allows routers to manage the traffic between hosts belonging to a multicast group. Information relating to multicast groups are transmitted between routers. As such, each router knows which host groups are found on the different networks.

To operate IGMP, rely on the basic support provided by IP as if it were a higher-level protocol. It is structured as follows :

Action: Block

Action modifiable: Yes

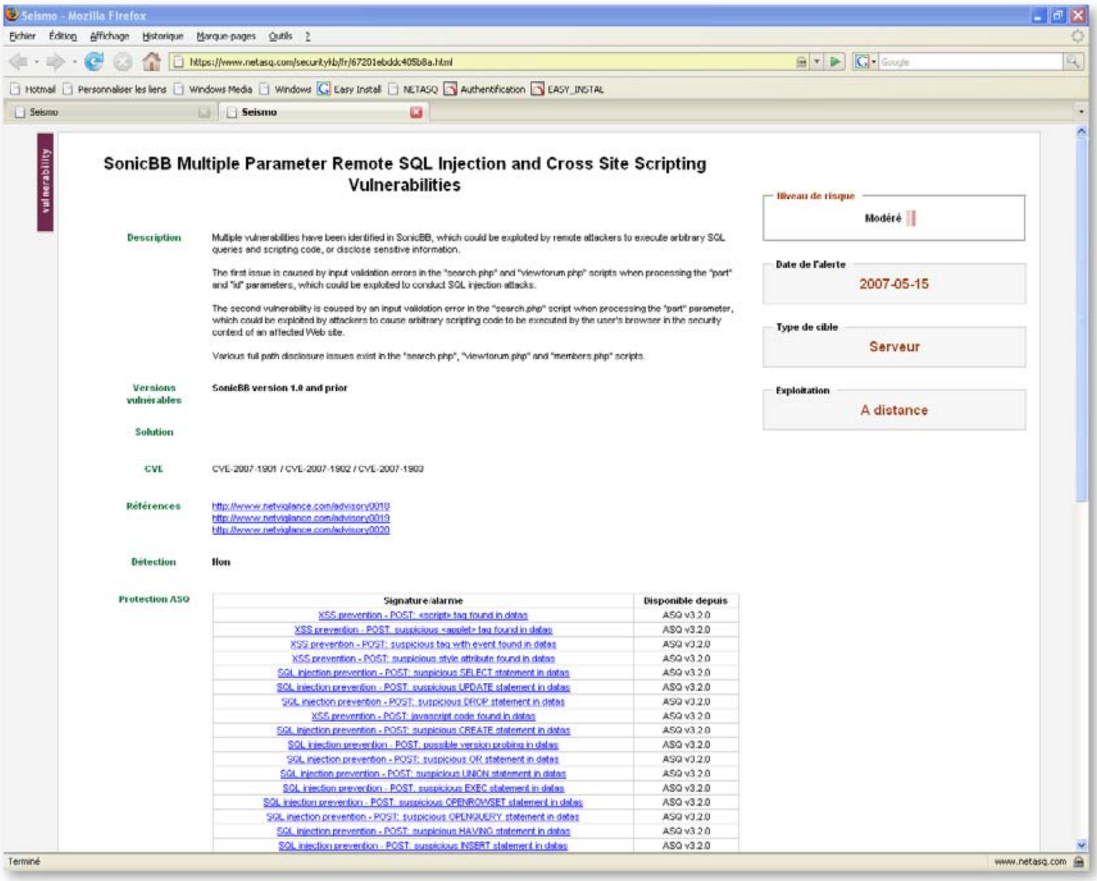
Reference:

Detected by Seismo beginning with ASQ version 3.2.0

ASQ version of this firewall: 3.5.0

Figure 140: Help - Alarms

The help displayed may contain hypertext links that will allow you to display HTML pages that include additional explanations.


Seismo - Mozilla Firefox
Fichier Édition Affichage Historique Marque-pages Outils ?
https://www.netasq.com/securitykb/fr/67201ebddc405b8a.html
Google
Hotmail Personnaliser les liens Windows Media Windows Easy Install NETASQ Authentification EASY_INSTAL
Seismo
Seismo
vulnerability
Terminé
www.netasq.com

SonicBB Multiple Parameter Remote SQL Injection and Cross Site Scripting Vulnerabilities

Niveau de risque: Modéré

Date de l'alerte: 2007-05-15

Type de cible: Serveur

Exploitation: A distance

Description: Multiple vulnerabilities have been identified in SonicBB, which could be exploited by remote attackers to execute arbitrary SQL queries and scripting code, or disclose sensitive information.

The first issue is caused by input validation errors in the "search.php" and "viewforum.php" scripts when processing the "part" and "id" parameters, which could be exploited to conduct SQL injection attacks.

The second vulnerability is caused by an input validation error in the "search.php" script when processing the "part" parameter, which could be exploited by attackers to cause arbitrary scripting code to be executed by the user's browser in the security context of an affected Web site.

Various full path disclosure issues exist in the "search.php", "viewforum.php" and "members.php" scripts.

Versions vulnérables: SonicBB version 1.0 and prior

Solution:

CVE: CVE-2007-1901 / CVE-2007-1902 / CVE-2007-1903

Références:
http://www.netvigilance.com/advisory0018
http://www.netvigilance.com/advisory0019
http://www.netvigilance.com/advisory0020

Détection: Non

Protection ASQ:

Signature/alarme	Disponible depuis
XSS prevention - POST: <script> tag found in datas	ASQ v3.2.0
XSS prevention - POST: suspicious <applet> tag found in datas	ASQ v3.2.0
XSS prevention - POST: suspicious tag with event found in datas	ASQ v3.2.0
XSS prevention - POST: suspicious style attribute found in datas	ASQ v3.2.0
SQL injection prevention - POST: suspicious SELECT statement in datas	ASQ v3.2.0
SQL injection prevention - POST: suspicious UPDATE statement in datas	ASQ v3.2.0
SQL injection prevention - POST: suspicious DROP statement in datas	ASQ v3.2.0
XSS prevention - POST: javascript code found in datas	ASQ v3.2.0
SQL injection prevention - POST: suspicious CREATE statement in datas	ASQ v3.2.0
SQL injection prevention - POST: possible version probing in datas	ASQ v3.2.0
SQL injection prevention - POST: suspicious OR statement in datas	ASQ v3.2.0
SQL injection prevention - POST: suspicious UNION statement in datas	ASQ v3.2.0
SQL injection prevention - POST: suspicious EXEC statement in datas	ASQ v3.2.0
SQL injection prevention - POST: suspicious OPENROWSET statement in datas	ASQ v3.2.0
SQL injection prevention - POST: suspicious OPENQUERY statement in datas	ASQ v3.2.0
SQL injection prevention - POST: suspicious HAVING statement in datas	ASQ v3.2.0
SQL injection prevention - POST: suspicious INSERT statement in datas	ASQ v3.2.0

Figure 141: Hypertext lines

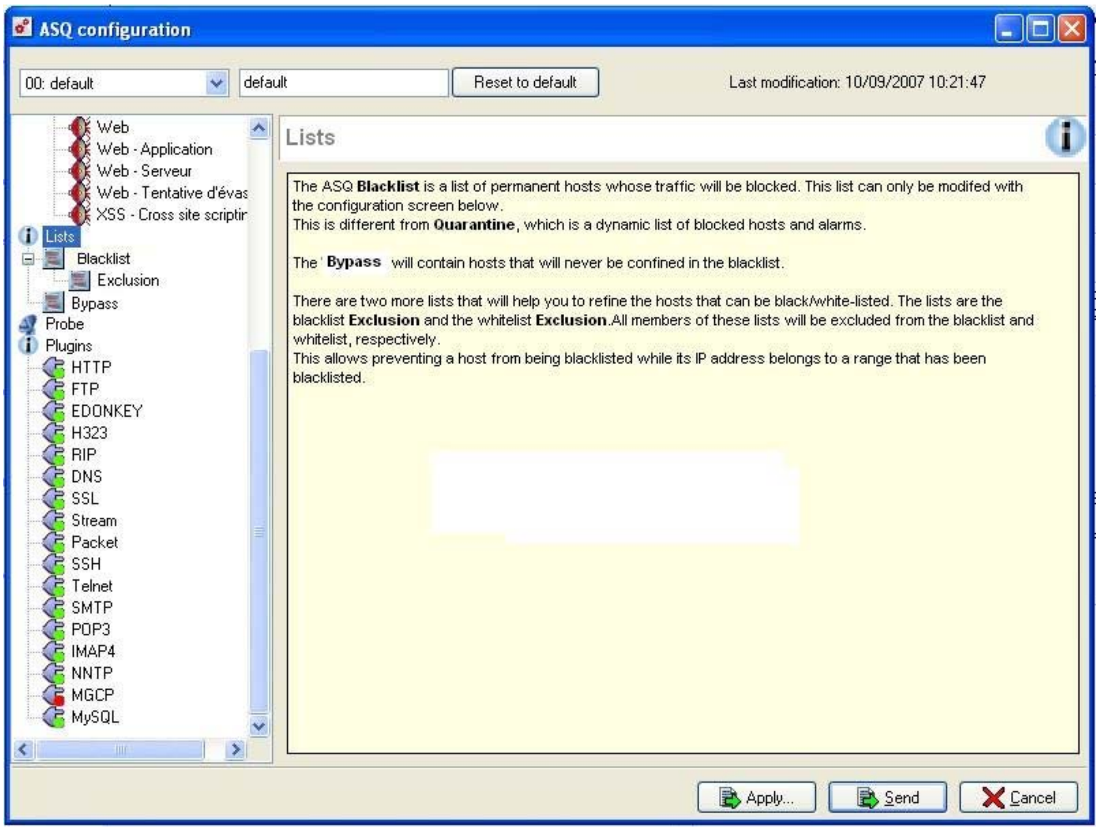
CHAPTER 7: LISTS

The ASQ blacklist, which operates differently from a quarantine, displays hosts whose traffic is permanently blocked. This list can only be modified in the ASQ configuration window.

In quarantine, a list shows hosts that have been temporarily blocked. These hosts are blocked whenever alarms are raised for traffic that corresponds to the "Quarantine" action.

The whitelist contains hosts that will never be placed on the blacklist, and which will not be analyzed by ASQ. This list should contain only hosts that do not comply with the standards that ASQ analyzes but for which the administrator has decided to let through unconditionally. This list allows incoming and outgoing traffic, and hosts found on this list will be accessible from users outside the network.

Blacklists contain a sub-menu **Exclusion**, that allows excluding, for example, a host from a host group so that it will not be blocked. Also, hosts found on this list cannot be placed in quarantine. This list has to contain trusted hosts that are unlikely to be quarantined automatically (alarms will be raised in response).



The ASQ **Blacklist** is a list of permanent hosts whose traffic will be blocked. This list can only be modifed with the configuration screen below.
This is different from **Quarantine**, which is a dynamic list of blocked hosts and alarms.

The **Bypass** will contain hosts that will never be confined in the blacklist.

There are two more lists that will help you to refine the hosts that can be black/white-listed. The lists are the blacklist **Exclusion** and the whitelist **Exclusion**.All members of these lists will be excluded from the blacklist and whitelist, respectively.
This allows preventing a host from being blacklisted while its IP address belongs to a range that has been blacklisted.

Figure 142: ASQ configuration - Lists

This ASQ configuration menu consists of two parts: **Blacklist** and **Bypass**.

6.7.1. Blacklist

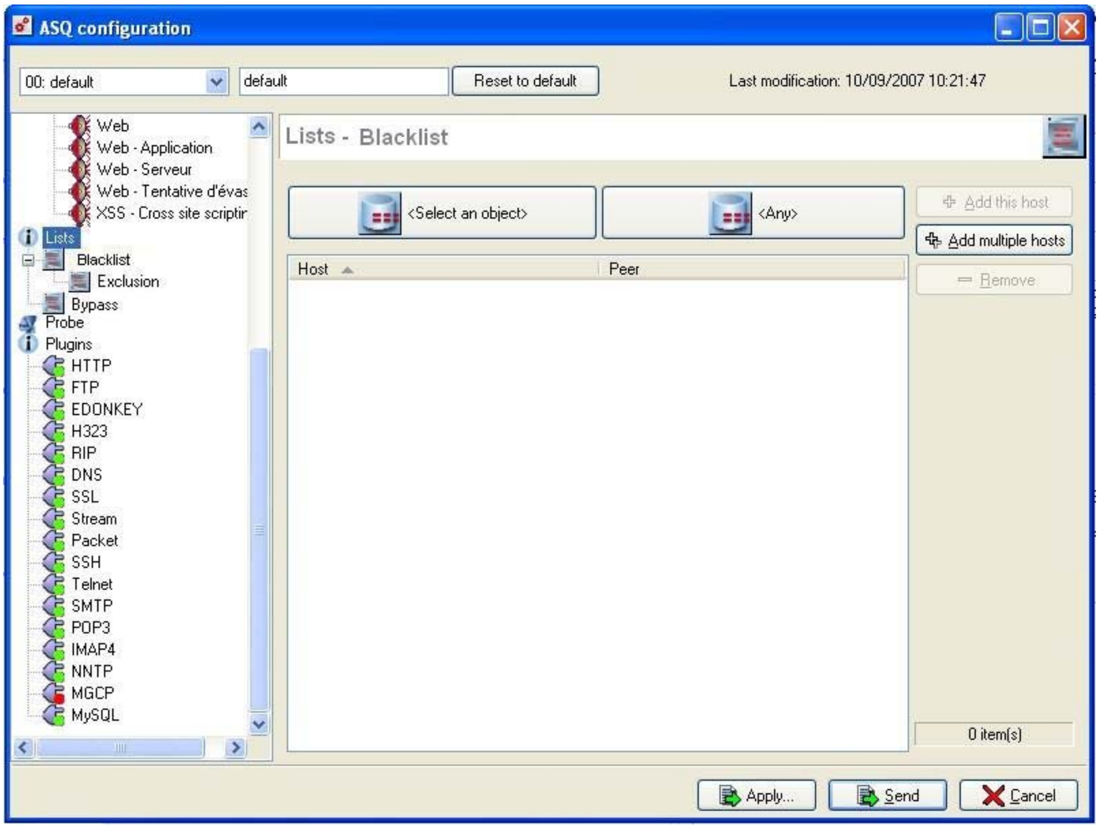


Figure 143: ASQ configuration – Blacklist

This menu allows configuring static quarantine (this is different from dynamic quarantine mentioned above – see Part 6/Chapter 6: *Protocol alarms*). All traffic coming from or going towards a particular host, or traffic between two hosts, can be prohibited using this quarantine.

The quarantine configuration menu is presented in the form of a grid displaying the hosts currently in quarantine and their peer (if necessary).

To add an entry to this grid, the procedure is as follows:

1 Select the host you wish to place in static quarantine using the **Select an object** button.

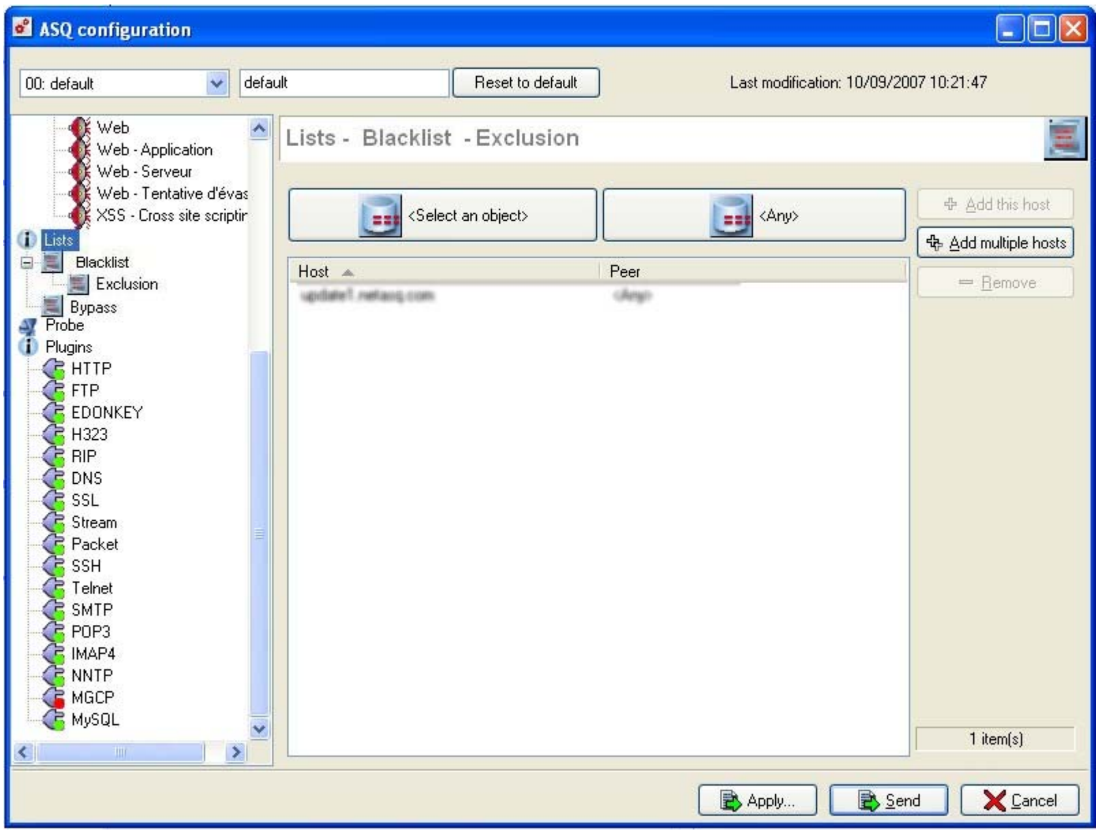
2 Select the peer host to be placed in quarantine (all traffic in both directions between these hosts, will be prohibited). If you wish to prohibit all traffic to (or from) any other host, leave the "Host" field empty,

3 Add the entry by clicking on the **Add this host** button.

The **Remove** button allows you to delete the selected entry.

The **Add several hosts** button enables you to select several hosts at the same time to place in quarantine. This button will then add an entry which prohibits traffic between this host and all other hosts.

6.7.1.1. Exclusion



ASQ configuration

00: default | default | Reset to default | Last modification: 10/09/2007 10:21:47

Lists - Blacklist - Exclusion

Host	Peer
update1.netasq.com	<Any>

1 item(s)

Figure 144: ASQ configuration - Exclusion

This menu enables excluding a host from a group which has been placed in static quarantine.

The quarantine exclusion configuration menu is presented in the form of a grid displaying hosts and their peer (if necessary) currently excluded from quarantine.

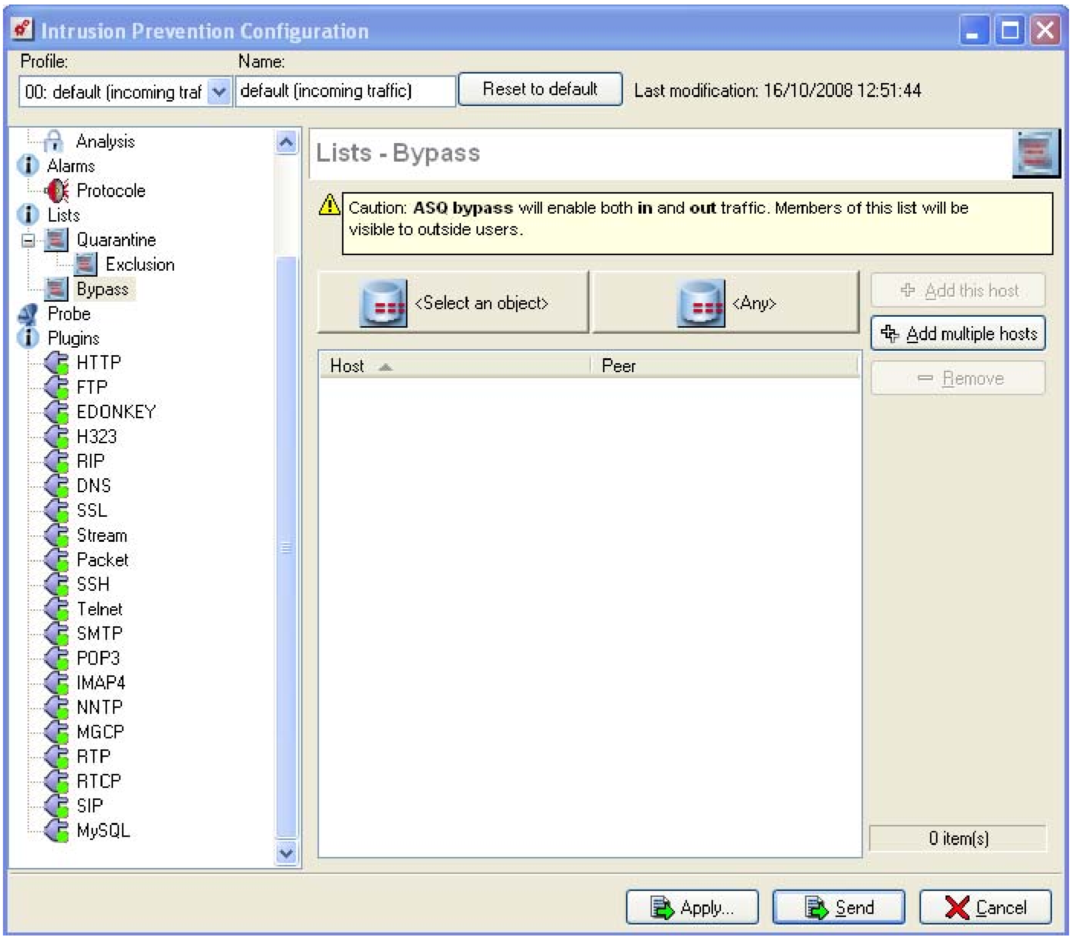
To add an entry to this grid, the procedure is as follows:

1 Select the host you wish to exclude from static quarantine using the **Select an object** button.

2 Select the peer host to exclude from quarantine (all traffic in both directions between these hosts, will not be prohibited). If you wish to not prohibit traffic to (or from) any other host, leave the "Host" field empty.

3 Add the entry by clicking on the **Add this host** button.

6.7.2. Bypass



Profile: 00: default (incoming traf

Name: default (incoming traffic)

Last modification: 16/10/2008 12:51:44

Caution: **ASQ bypass** will enable both **in** and **out** traffic. Members of this list will be visible to outside users.

0 item(s)

Figure 145: ASQ configuration - Bypass

This menu allows configuring a host whiteliset. Also known as "Bypass", this list enables defining traffic which does not have to be analyzed by ASQ.

WARNING

Security for resources and infrastructures protected by the Firewall will be considerably diminished if a white list is configured for hosts, as this means that analyses and filter policies WILL NOT be applied to traffic affected by the white list (in both directions).

The ASQ bypass configuration menu is presented in the form of a grid displaying the hosts currently in ASQ bypass and their peer (if necessary).

To add an entry to this grid, the procedure is as follows:

1 Select the host you wish to place in ASQ bypass using the **Select an object.**

2 Select the peer host to be placed in ASQ bypass (all traffic in both directions between these hosts, will not be analyzed by ASQ). If you wish to bypass the ASQ analysis for traffic to (or from) any other host, leave the "Host" field empty.

3 Add the entry by clicking on the **Add this host** button.

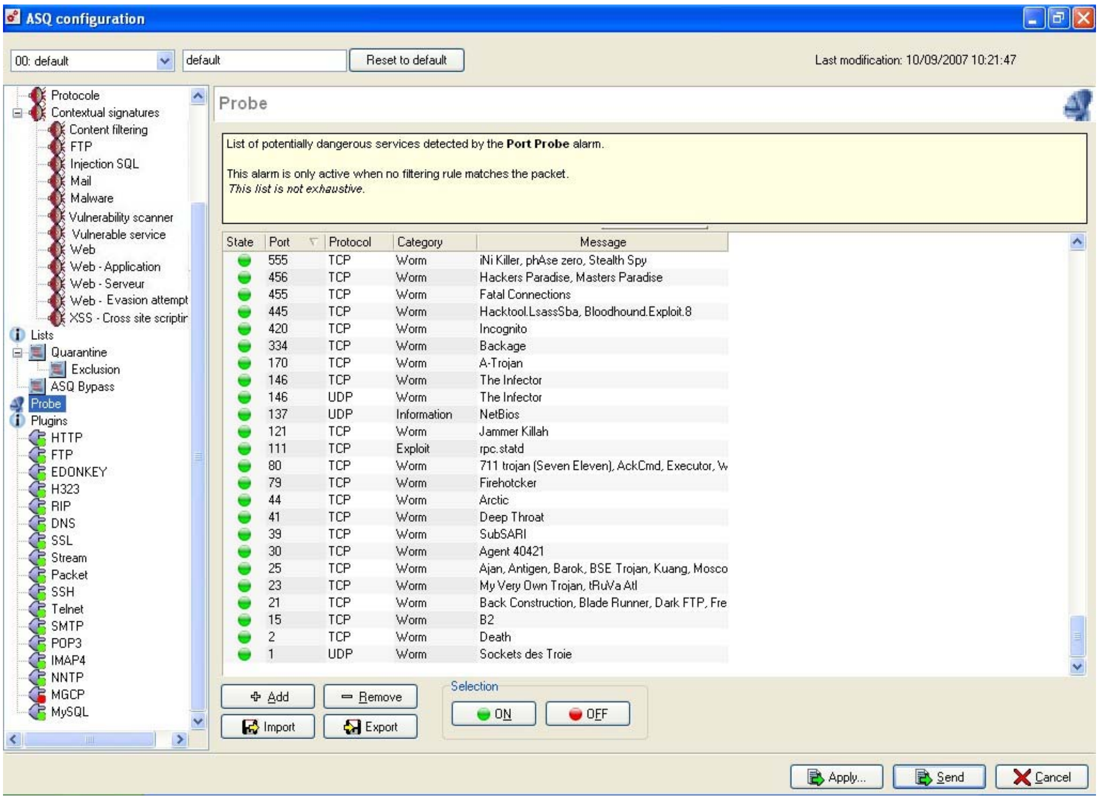
6.7.2.1. Priority in blacklists, whitelists and filtering

A packet (regardless of direction) will be systematically refused if it corresponds to an entry on the quarantine list, notwithstanding the ASQ bypass configuration and filter policy.

Once the quarantine list has been verified, packets which do not appear (on the quarantine list) will be systematically authorized if they correspond to an ASQ bypass entry, notwithstanding the filter policy, without passing through ASQ analyses (protocol and contextual signature analyses).

CHAPTER 8: PROBES

This window comprises a list of potentially-dangerous services that the Port probe alamr has detected. This alarm is activated if no filter rule has treated the packet.



Last modification: 10/09/2007 10:21:47

List of potentially dangerous services detected by the **Port Probe** alarm.

This alarm is only active when no filtering rule matches the packet.
This list is not exhaustive.

State	Port	Protocol	Category	Message
●	555	TCP	Worm	iNi Killer, phAse zero, Stealth Spy
●	456	TCP	Worm	Hackers Paradise, Masters Paradise
●	455	TCP	Worm	Fatal Connections
●	445	TCP	Worm	Hacktool.LsassSba, Bloodhound.Exploit.8
●	420	TCP	Worm	Incognito
●	334	TCP	Worm	Backage
●	170	TCP	Worm	A-Trojan
●	146	TCP	Worm	The Infector
●	146	UDP	Worm	The Infector
●	137	UDP	Information	NetBios
●	121	TCP	Worm	Jammer Killah
●	111	TCP	Exploit	rpc.statd
●	80	TCP	Worm	711 trojan (Seven Eleven), AckCmd, Executor, W
●	79	TCP	Worm	Firehotcker
●	44	TCP	Worm	Arctic
●	41	TCP	Worm	Deep Throat
●	39	TCP	Worm	SubSARI
●	30	TCP	Worm	Agent 40421
●	25	TCP	Worm	Ajan, Antigen, Barok, BSE Trojan, Kuang, Mosco
●	23	TCP	Worm	My Very Own Trojan, tRuVa Atl
●	21	TCP	Worm	Back Construction, Blade Runner, Dark FTP, Fre
●	15	TCP	Worm	B2
●	2	TCP	Worm	Death
●	1	UDP	Worm	Sockets des Troie

Figure 146: ASQ configuration - Probes

This window sets out a list of potentially dangerous services frequently used by Trojan horses or worms. When one of these services is used, a “port probe” alarm will be raised if and only if no filter rules are associated with the packet in question.

Action buttons at the bottom of the window enable you to modify this list according to the ports you wish to supervise.

The grid comprises five sections:

State	To deactivate, without deleting this port probe.
Port	The number of the port to supervise. This number must be between 1 and 65535.
Protocol	The protocol transporting malicious packets. (TCP or UDP).

Category	Several categories are available (misc, information, exploit, worm, p2p, relaying).
Message	Comments regarding this probe. E.g., the title of the port probe.

The buttons under the screen allow you to:

Add	Adds a service. An additional line will appear in the table. In the “Status” column, enable or disable this service. In the “Port” column, select the port number. In the “Protocol” column, seclect TCP or UDP. In the “Category” column, select from the following: Miscellaneous, Information, Exploit, Worm, P2P, Relay. In the “Message” column, enter a description.
Remove	Deletes the selected line directly.
Import	Imports the list. The import may contain a comment (a “#” symbol has to be inserted at the beginning of the comment). The position of the values has to comply with the order in the example above.
Export	Exports this list. The file will be generated in **.txt** format. Every line represented corresponds to a probe, followed by its properties, separated by a tab This list can be exported by clicking on the **Export** button. The file will be generated in **.txt** format. Every line represented corresponds to a probe followed by its properties, separated by a tab **Exemple** 1 1 UDP Worm Sockets des Troie]

The user can modify each of these properties. However, there cannot be two probes on the same port and same protocol.

> **Example**
> A probe on port 25/TCP and another on port 25/UDP can co-exist. However, two or more ports on port
> denied.

CHAPTER 9: PLUGINS

6.9.1. Presentation

The optimized protocol plugin architecture is what distinguishes the new version of the ASQ. These plugins carry out a thorough analysis of data which passes through in packets, namely by verifying their coherence in relation to the headers and peer protocols.

Plugins check for RFC compliance partially or fully in order to detect all attacks and excesses (Buffer overflow on URL, Invalid UTF-8 encoding…).

Plugins can be matched to traffic either:

- Manually via the object *Services* or the default port configured for the plugin.
- Automatically, by application protocol detection.

The list of plugins is as follows:

- HTTP
- FTP
- EDONKEY
- H323
- RIP
- DNS
- SSL
- Stream
- Packet
- SSH
- Telnet
- SMTP
- POP3
- IMAP4
- NNTP
- MGCP
- RTP
- RTCP
- SIP
- MySQL

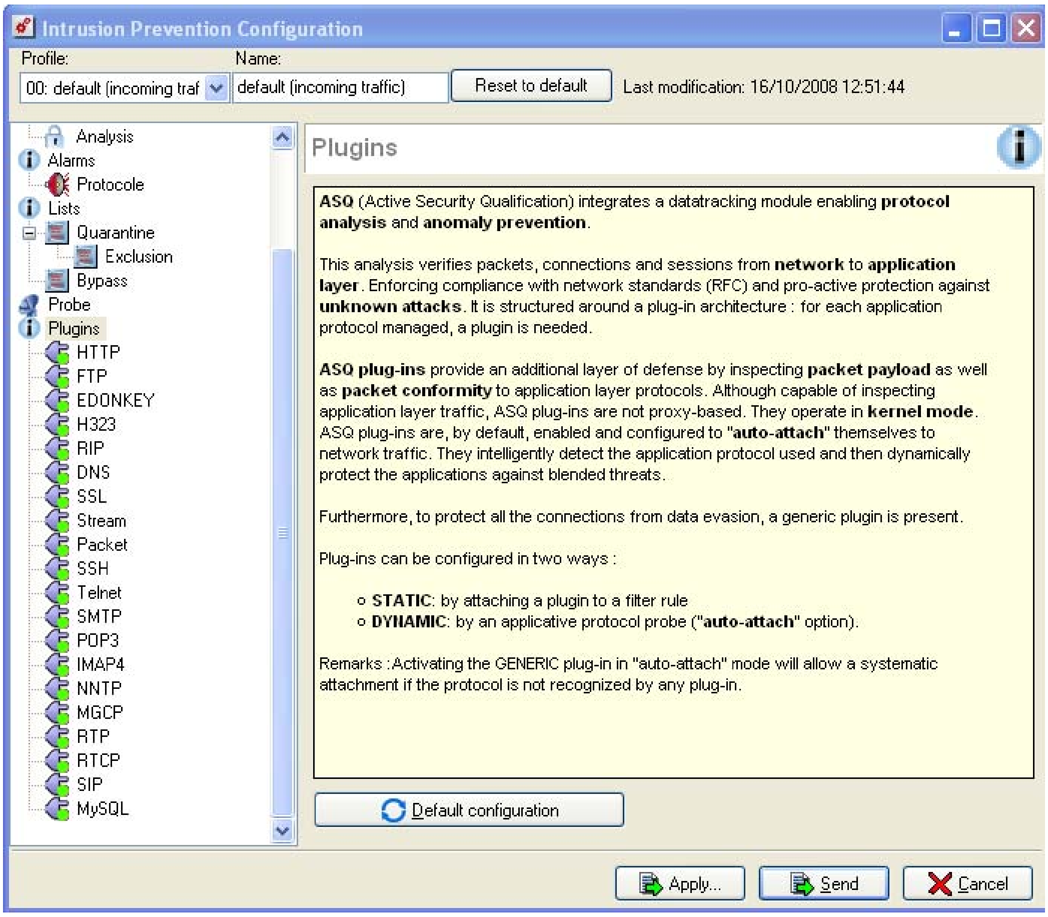
6.9.2. Attaching plugins

These plugins are attached to their standard port.

> **Example**
> http on port 80/tcp

As an option, the plugin can detect the protocol and attach itself automatically to the connection. This allows, for example, capturing HTTP sessions regardless of port in an open filter policy. A plugin can also be configured to block any traffic that appears on a non-standard port, such as HTTP traffic on a port other than port 80. Plugins can be configured to attach themselves to all connections that use a given network port, e.g. the DNS plugin will be attached to UDP port 53. Plugins can also be attached from rules in the filter policy.

➲ The configuration parameters in the Analyze module can be modified in the **`Plugins`** tab of the **`Intrusion Prevention`** menu in the menu directory.



Profile: 00: default (incoming traf

Name: default (incoming traffic)

Last modification: 16/10/2008 12:51:44

Plugins

ASQ (Active Security Qualification) integrates a datatracking module enabling **protocol analysis** and **anomaly prevention**.

This analysis verifies packets, connections and sessions from **network** to **application layer**. Enforcing compliance with network standards (RFC) and pro-active protection against **unknown attacks**. It is structured around a plug-in architecture : for each application protocol managed, a plugin is needed.

ASQ plug-ins provide an additional layer of defense by inspecting **packet payload** as well as **packet conformity** to application layer protocols. Although capable of inspecting application layer traffic, ASQ plug-ins are not proxy-based. They operate in **kernel mode**. ASQ plug-ins are, by default, enabled and configured to "**auto-attach**" themselves to network traffic. They intelligently detect the application protocol used and then dynamically protect the applications against blended threats.

Furthermore, to protect all the connections from data evasion, a generic plugin is present.

Plug-ins can be configured in two ways :

- **STATIC**: by attaching a plugin to a filter rule
- **DYNAMIC**: by an applicative protocol probe ("**auto-attach**" option).

Remarks :Activating the GENERIC plug-in in "auto-attach" mode will allow a systematic attachment if the protocol is not recognized by any plug-in.

Figure 147: ASQ configuration - Plugins

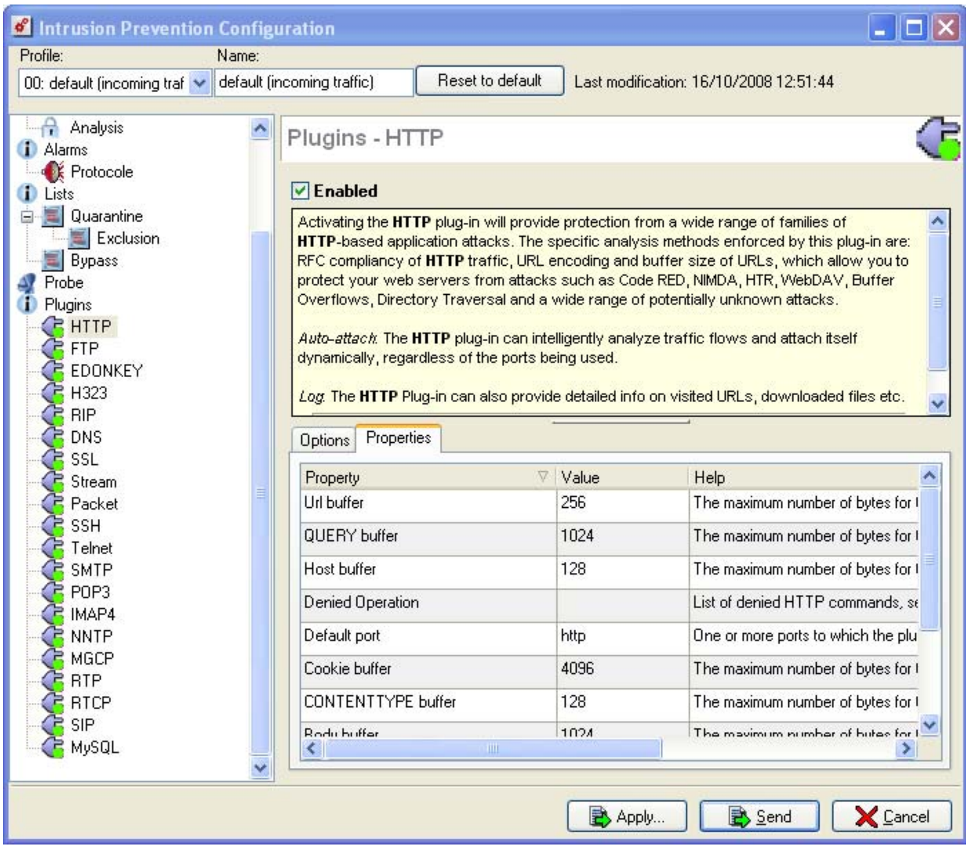
Features available for the current plugins are set out in the following table:

Enabled	Activates or deactivates the plugin
Auto-attach	If the plugin has been activated, it is automatically used to search for a corresponding packet in the filter rules. This option is not available for DNS, RIP, H323, RTP and RTCP plugins.
Close connection when attaching the plugin	When the plugin is automatically activated for a type of traffic, the connection that caused the automatic activation will be closed. Packets will then be blocked. For example, all HTTP traffic can be blocked, regardless of the port concerned. The plugins DNS, RIP and H323, RTP and RTCP do not have this option.
Log	Activates or deactivates the generation of logs regarding the plugin.
Verifying extended traffic	This option, when selected, allows certain potentially-dangerous types of traffic to be analyzed. By default, this option is checked, therefore the HTTP plugin prevents the traffic from passing through as it has not received enough data in order to be sure that the traffic is safe.
Shoutcast support	Supports Shout Cast (HTTP only)
Webdav	Supports Webdav (HTTP only)
RFC 775	Supports directory navigation features in FTP. (FTP only).
SSL Authentication	Activates SSL authentication support for FTP. (FTP only).
No authentication validation	This option allows you to enable or disable the authentication sequence on an FTP server.

6.9.3. HTTP plugin

This plugin allows preventing large families of HTTP-based application attacks. The various analyses that this plugin performs (in particular RFC compliance checks), validation of encoding in URLs or checks on URL size or requests, allow you to block attacks such as Code RED, Code Blue, NIMDA, HTR, WebDav, Buffer Overflow or even Directory Traversal…

Managing buffer overflows is fundamental at NETASQ, which is why defining the maximum sizes allowed for HTTP buffers is particularly detailed.



Profile: 00: default (incoming traf

Name: default (incoming traffic)

Last modification: 16/10/2008 12:51:44

Plugins - HTTP

☑ Enabled

Activating the **HTTP** plug-in will provide protection from a wide range of families of **HTTP**-based application attacks. The specific analysis methods enforced by this plug-in are: RFC compliancy of **HTTP** traffic, URL encoding and buffer size of URLs, which allow you to protect your web servers from attacks such as Code RED, NIMDA, HTR, WebDAV, Buffer Overflows, Directory Traversal and a wide range of potentially unknown attacks.

Auto-attach: The **HTTP** plug-in can intelligently analyze traffic flows and attach itself dynamically, regardless of the ports being used.

Log: The **HTTP** Plug-in can also provide detailed info on visited URLs, downloaded files etc.

Property	Value	Help
Url buffer	256	The maximum number of bytes for l
QUERY buffer	1024	The maximum number of bytes for l
Host buffer	128	The maximum number of bytes for l
Denied Operation		List of denied HTTP commands, se
Default port	http	One or more ports to which the plu
Cookie buffer	4096	The maximum number of bytes for l
CONTENTTYPE buffer	128	The maximum number of bytes for l
Body buffer	1024	The maximum number of bytes for l

Figure 148: ASQ configuration - HTTP

6.9.3.1. Options

Enabled	Enables or disables the plugin.
Auto-attach	If the plugin has been enabled, it will automatically be used for detecting matching packets in the filter rules. This option is not available for the DNS, RIP, H323, RTP and RTCP plugins.
Close connection when attaching the plugin	When the plugin is enabled automatically on a type of traffic, the connection that caused the automatic activation of the traffic will be shut down. Packets will then be blocked. For example, all HTTP traffic can be blocked, regardless of the port concerned. DNS, RIP, H323, RTP and RTCP plugins do not have this option.
Logs	Enables or disables the generation of logs concerning the plugin.
Block until data is reconstructed	If this option has been selected, potentially dangerous traffic can be scanned. By default, it is selected. Thus, the HTTP plugin prevents the traffic from passing as long as it has not received enough data to be sure that the traffic is legitimate.
Shout Cast support	Support for Shout Cast. (HTTP only).
Webdav support	Support for WebDav. (HTTP only).

6.9.3.2. Detection of excessively long URLs

The recent popularity of multimedia sites has given rise to longer URLs. As a result, the alarm "Buffer overflow in the URL" is mistakenly raised with increasing frequency. URLs that are too long can now be detected with more precision with the help of 3 buffers:

- URL buffer.
- QUERY buffer.
- Argument buffer.

6.9.3.3. Detection of double encoding and invalid encoding

URLs are increasingly inserted into parameters (especially advertisements), making double redirections more frequent, thus creating a growing number of false positives. Moreover, the detection of double encoding attacks via signatures is not 100% effective.

When an encoded % character is detected, raising an alarm is no longer a viable solution. In fact, due to the high number of false positives, this alarm will be disabled. The attempt to evade the analysis can now be countered without setting off false positives.

When the encoding is invalid but decoding is possible, the invalid charactercan now be decoded (in the case of characters that are not supposed to be encoded).

Detection is automatic and allows more precision in detecting encoding.

Please refer to *Appendix T: List of alarms relating to protocols*.

6.9.3.4. "Properties" tab

Authorized operations	List of authorized HTTP commands (in CSV format) separated by commas. The maximum length is 128 characters.
Prohibited operations	List of prohibited HTTP commands (in CSV format) separated by commas. The maximum length is 128 characters.
Default port	One or several ports that the plugin will link.
URL Buffer	This buffer affects the whole URL. The syntax is as follows: http://<URLBuffer>?<Querybuffer>. Maximum number of bytes for the URL including formatting attributes. The default value is 256.
BODY Buffer	Maximum number of bytes for the BODY field including formatting attributes.
COOKIE Buffer	Maximum number of bytes for the COOKIE field including formatting attributes. (Min: 128; Max: 4096).
HOST Buffer	Maximum number of bytes for the HOST field including formatting attributes. (Min: 128; Max: 4096).
CONTENTTYPE Buffer	Maximum number of bytes for the CONTENTTYPE field including formatting attributes. (Min: 128; Max: 4096).
AUTHORIZATION Buffer	Maximum number of bytes for the AUTHORIZATION field including formatting attributes. (Min: 128; Max: 4096).
QUERY buffer	Includes a set of arguments which are separated by an ampersand (&). Maximum number of bytes for the QUERY part of the URL. (Min: 128; Max: 4096). The default value is 1024.

Argument buffer	The syntax is as follows: "token=value"&. Maximum number of bytes for a parameter in the URL. (Min: 128; Max: 4096). The default value is 512.

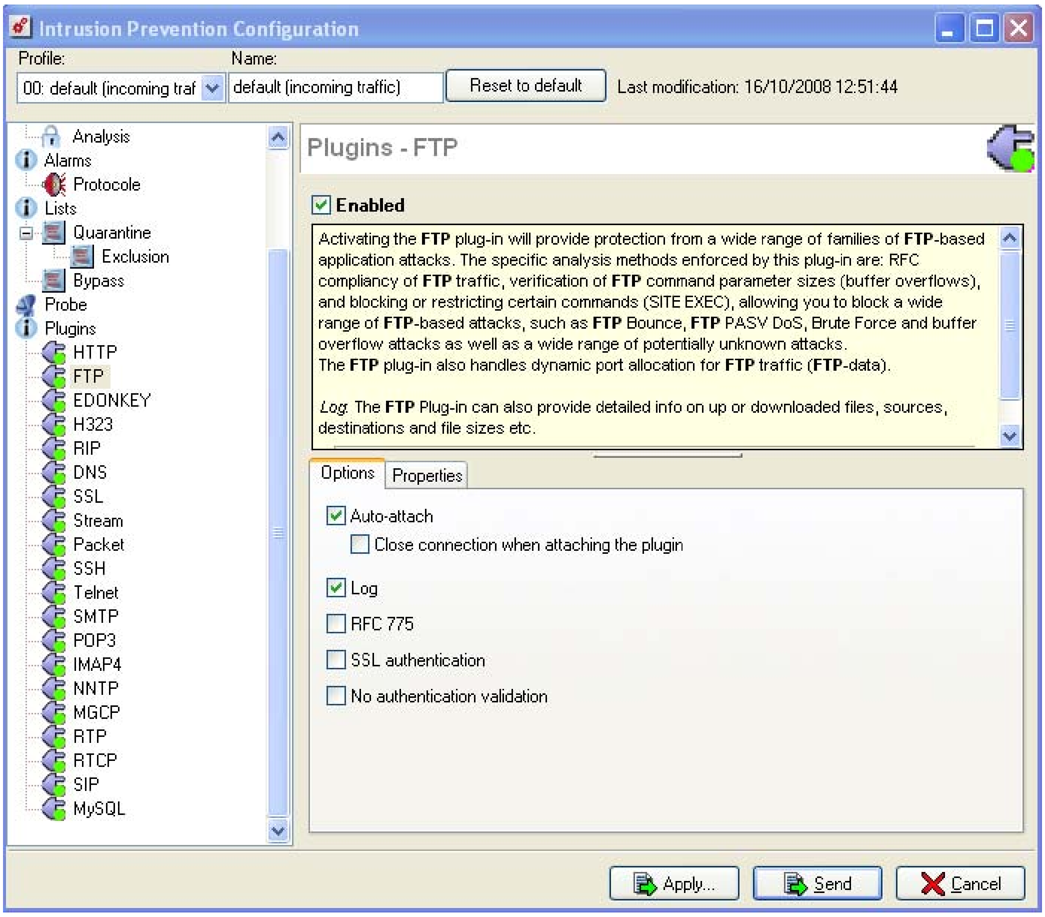
6.9.4. FTP Plugin

The FTP plugin supports the main RFC [RFC959] as well as many extensions.

Enabling this plugin allows the prevention of large families of FTP-based application attacks. This plugin performs various analyses such as the RFC compliance analysis, checks on FTP command parameter size or restrictions on the protocol (SITE EXEC for example). These analyses therefore allow stopping attacks such as FTP Bounce, FTP PASV DoS, Buffer overflow, etc. This plugin is indispensable when allowing FTP traffic to pass through the firewall and to dynamically manage FTP data connections.

6.9.4.1. Options

Status	Enables or disables the plugin.
Automatic activation	If the plugin has been enabled, it will automatically be used for detecting matching packets in the filter rules. This option is not available for the DNS, RIP, H323, RTP and RTCP plugins.
Close connection when attaching the plugin	When the plugin is enabled automatically on a type of traffic, the connection that caused the automatic activation of the traffic will be shut down. Packets will then be blocked. For example, all HTTP traffic can be blocked, regardless of the port concerned. DNS, RIP, H323, RTP and RTCP plugins do not have this option.
Logs	Enables or disables the generation of logs concerning the plugin.
RFC 775	Supports directory navigation features in FTP. (FTP only).
SSL Authentication	Activates SSL authentication support for FTP. (FTP only).
No authentication validation	This option allows you to enable or disable the authentication sequence on an FTP server.



☑ Enabled

Activating the **FTP** plug-in will provide protection from a wide range of families of **FTP**-based application attacks. The specific analysis methods enforced by this plug-in are: RFC compliancy of **FTP** traffic, verification of **FTP** command parameter sizes (buffer overflows), and blocking or restricting certain commands (SITE EXEC), allowing you to block a wide range of **FTP**-based attacks, such as **FTP** Bounce, **FTP** PASV DoS, Brute Force and buffer overflow attacks as well as a wide range of potentially unknown attacks.
The **FTP** plug-in also handles dynamic port allocation for **FTP** traffic (**FTP**-data).

Log: The **FTP** Plug-in can also provide detailed info on up or downloaded files, sources, destinations and file sizes etc.

☑ Auto-attach
□ Close connection when attaching the plugin
☑ Log
□ RFC 775
□ SSL authentication
□ No authentication validation

Figure 149: ASQ configuration - FTP

6.9.4.2. Properties

The following is a table of the FTP buffers that can be managed:

Default port	One or several ports that the plugin will link.
LINE buffer	Maximum number of bytes for an FTP line including formatting attributes. (Min: 128; Max: 2048).
PASS buffer	Maximum number of bytes for the FTP password including formatting attributes. (Min: 128; Max: 2048).
PATH buffer	Maximum number of bytes for the FTP path including formatting attributes. (Min: 128; Max: 2048).
SITE buffer	Maximum number of bytes for the FTP SiteString including formatting attributes. (Min: 128; Max: 2048).
USER buffer	Maximum number of bytes for the FTP username line including formatting attributes. (Min: 128; Max: 2048).
AllowOp	List of authorized FTP commands (in CSV format), separated by commas. Maximum length of 128 characters.
DenyOp	List of prohibited FTP commands (in CSV format), separated by commas. Maximum length of 128 characters.

6.9.5. EDONKEY plugin

Activating this plugin allows you to support the protocol for this software. Thanks to this plugin, you will be able to retrieve very comprehensive logs on files that have been exchanged (e.g. file names).

The plugin supports the dynamic attachment to connections and will therefore be able to log the protocol on non-standard ports.

6.9.5.1. Options

Enabled	Activates or deactivates the plugin
Auto-attach	If the plugin has been activated, it is automatically used to search for a corresponding packet in the filter rules. This option is not available for DNS, RIP, H323, RTP and RTCP plugins.
Log	Activates or deactivates the generation of logs regarding the plugin.

6.9.5.2. Properties

Default port	One or several ports that the plugin will link.

6.9.6. H323 plugin

Activating this plugin allows you to check whether H323 packets received conform to the standards in force for this protocol. This plugin is indispensable for allowing H323 traffic through the firewall and to dynamically manage data connections on the H323 protocol.

Default port	One or several ports that the plugin will link.

6.9.7. RIP plugin

Activating this plugin allows you to check whether RIP packets received conform to the RFCs in force for this protocol.

Default port	One or several ports that the plugin will link.

6.9.8. DNS plugin buffers

Activating this plugin allows you to prevent large families of DNS-based application attacks.

The different analyses that this plugin performs, in particular the restriction of zone transfers or RFC compliance, allow you to block attacks such as DNS ID spoofing, DNS cache poisoning or even DNS zone change and DNS zone Update.

The various DNS buffers that are supported are indicated in the following table:

Default port	One or several ports that the plugin will link.
NAME buffer	Maximum number of bytes for the NAME field in a DNS query. (Min: 128; Max: 2048).

6.9.9. SSL plugin buffer

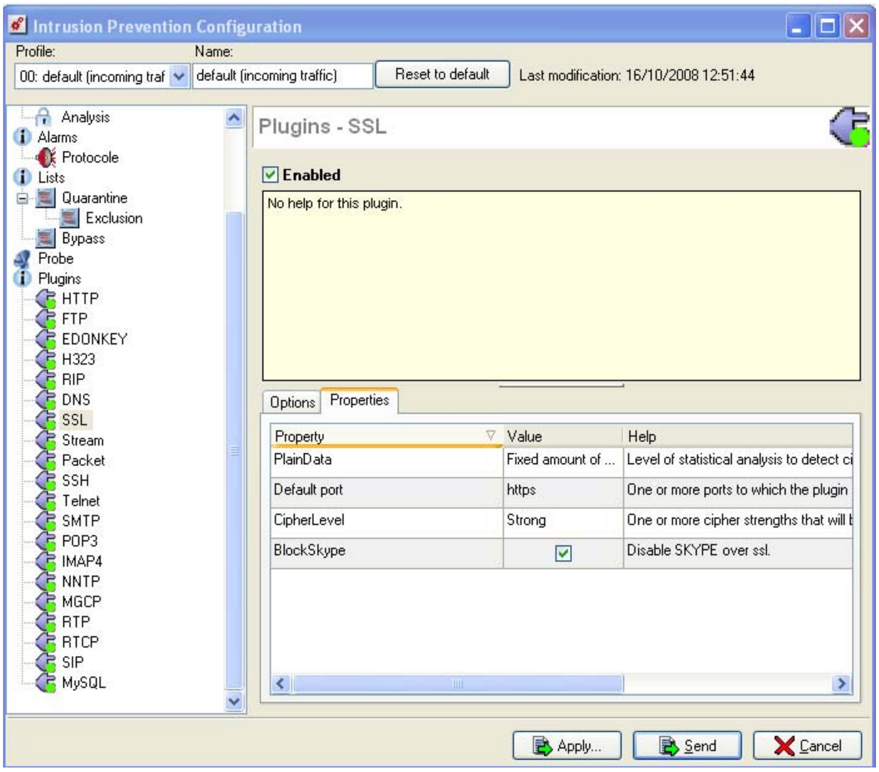
The objective of the SSL plugin is to confirm that the SSL protocol has been correctly played out through the firewall. Certain options allow reinforcing this protocol's security. For example, negotiations of cryptographical algorithms that are deemed weak can be prohibited, or software applications that use SSL to bypass filter policies can be detected (SKYPE, HTTPS proxy, etc).

6.9.9.1. Options

Enabled	Activates or deactivates the plugin
Auto-attach	If the plugin has been activated, it is automatically used to search for a corresponding packet in the filter rules. This option is not available for DNS, RIP, H323, RTP and RTCP plugins.
Close connection when attaching the plugin	When the plugin is automatically activated for a type of traffic, the connection that caused the automatic activation will be closed. Packets will then be blocked. For example, all HTTP traffic can be blocked, regardless of the port concerned. The plugins DNS, RIP and H323, RTP and RTCP do not have this option.

6.9.9.2. Properties

The various SSL buffers that are supported are indicated in the following table:



Profile: 00: default (incoming traf
Name: default (incoming traffic)
Reset to default
Last modification: 16/10/2008 12:51:44

Plugins - SSL

☑ Enabled

No help for this plugin.

Property	Value	Help
PlainData	Fixed amount of ...	Level of statistical analysis to detect ci
Default port	https	One or more ports to which the plugin
CipherLevel	Strong	One or more cipher strengths that will b
BlockSkype	☑	Disable SKYPE over ssl.

Figure 150: ASQ configuration - SSL

Default port	One or several ports that the plugin will link.
Encryption level	One or more encryption strengths that the plugin will accept. Possible values are "Unkonw encryption" (1), "NO encryption" (2), "Weak encryption (RC4-40, DES-40, etc.)" (4), Normal encryption (DES, RC4-64, etc.)" (8), "Strong encryption (AES-128, etc.)" (16). Strong AES encryption is selcted by default (encryption level 16).
Plaindata	Level of statistical analyses in order to detect encrypted data. Possible options are "No data analysis", "All data will be analyzed", "The fixed amount of data will be analyzed". After an SSL negotiation, communications with Google talk and Hopster will be blocked.
Block Skype	The Skype application uses port 443 and a protocol that resembles a SSL valid. However, several concurrent applications may block the use of Skype. This option when selected, allows the user to block Skype traffic without blocking all SSL traffic.

6.9.10. Particularity of the "Stream" and "Packet" plugins

These plugins allow verifying data which has no link to any particular protocol. Once this option has been activated, it is used by the Firewall only if no other plugin is activated during the analysis of the packet is question. This option is checked by default to provide you maximum security. However, the downside is that Firewall performance is reduced because of it. You may deactivate this option to guarantee better performance but your data security will be compromised. The **Stream** plugin is associated to TCP while the **Packet** plugin to UDP.

6.9.10.1. Stream plugin

Options

Enabled	Activates or deactivates the plugin
Auto-attach	If the plugin has been activated, it is automatically used to search for a corresponding packet in the filter rules. This option is not available for DNS, RIP, H323, RTP and RTCP plugins.
Close connection when attaching the plugin	When the plugin is automatically activated for a type of traffic, the connection that caused the automatic activation will be closed. Packets will then be blocked. For example, all HTTP traffic can be blocked, regardless of the port concerned. The plugins DNS, RIP and H323, RTP and RTCP do not have this option.

Properties

Default port	One or several ports that the plugin will link.

6.9.10.2. Packet plugin

Options

Enabled	Activates or deactivates the plugin
Auto-attach	If the plugin has been activated, it is automatically used to search for a corresponding packet in the filter rules. This option is not available for DNS, RIP, H323, RTP and RTCP plugins.
Close connection when attaching the plugin	When the plugin is automatically activated for a type of traffic, the connection that caused the automatic activation will be closed. Packets will then be blocked. For example, all HTTP traffic can be blocked, regardless of the port concerned. The plugins DNS, RIP and H323, RTP and RTCP do not have this option.

Properties

Default port	One or several ports that the plugin will link.

6.9.11. SSH plugin

The aim of the SSH plugin is to detect connections between two hosts that use the secure SSH protocol. Detection is based on the client's and server's banner. The plugin does not analyze the contents of the SSH traffic and is used by SEISMO to detect the version of the client and/or of the SSH server used in order to report possible vulnerabilities.

6.9.11.1. Options

Enabled	Activates or deactivates the plugin
Auto-attach	If the plugin has been activated, it is automatically used to search for a corresponding packet in the filter rules. This option is not available for DNS, RIP, H323, RTP and RTCP plugins.
Close connection when attaching the plugin	When the plugin is automatically activated for a type of traffic, the connection that caused the automatic activation will be closed. Packets will then be blocked. For example, all HTTP traffic can be blocked, regardless of the port concerned. The plugins DNS, RIP and H323, RTP and RTCP do not have this option.

6.9.11.2. Properties

Default port	One or several ports that the plugin will link.

6.9.12. Telnet plugin

The TELNET plugin detects connetions between two hosts that use the TELNET protocol. This is done by analyzing the common prefix for all TELNET commands. The plugin does not perform security scans on the contents of the TELNET traffic.

6.9.12.1. Options

Enabled	Activates or deactivates the plugin
Auto-attach	If the plugin has been activated, it is automatically used to search for a corresponding packet in the filter rules. This option is not available for DNS, RIP, H323, RTP and RTCP plugins.
Close connection when attaching the plugin	When the plugin is automatically activated for a type of traffic, the connection that caused the automatic activation will be closed. Packets will then be blocked. For example, all HTTP traffic can be blocked, regardless of the port concerned. The plugins DNS, RIP and H323, RTP and RTCP do not have this option.

6.9.12.2. Properties

Default port	One or several ports that the plugin will link.

6.9.13. SMTP plugin

The SMTP plugin detects connections between a client and mail server or between two mail servers that use SMTP. This is done by searching for a 220 type of response from the server (SMTP server banner). The plugin does not analyze SMTP traffic and is used by SEISMO to detect the version of the client and/or of the mail server used in order to report possible vulnerabilities.

6.9.13.1. Options

Enabled	Activates or deactivates the plugin
Auto-attach	If the plugin has been activated, it is automatically used to search for a corresponding packet in the filter rules. This option is not available for DNS, RIP, H323, RTP and RTCP plugins.
Close connection when attaching the plugin	When the plugin is automatically activated for a type of traffic, the connection that caused the automatic activation will be closed. Packets will then be blocked. For example, all HTTP traffic can be blocked, regardless of the port concerned. The plugins DNS, RIP and H323, RTP and RTCP do not have this option.

6.9.13.2. Properties

Default port	One or several ports that the plugin will link.

6.9.14. POP3 plugin

The POP3 plugin detects connections between a client and mail server that use POP3. This is done by relying on the first packet of the server that has to contain a line beginning with “+OK”. The plugin does not analyze POP3 traffic and is used by SEISMO to detect the version of the mail server used by analyzing the server’s banner in order to report possible vulnerabilities.

6.9.14.1. Options

Enabled	Activates or deactivates the plugin
Auto-attach	If the plugin has been activated, it is automatically used to search for a corresponding packet in the filter rules. This option is not available for DNS, RIP, H323, RTP and RTCP plugins.
Close connection when attaching the plugin	When the plugin is automatically activated for a type of traffic, the connection that caused the automatic activation will be closed. Packets will then be blocked. For example, all HTTP traffic can be blocked, regardless of the port concerned. The plugins DNS, RIP and H323, RTP and RTCP do not have this option.

6.9.14.1. Properties

Default port	One or several ports that the plugin will link.

6.9.15. IMAP4 plugin

The IMAP4 plugin detects connections between a client and mail server that use IMAP4. This is done by relying on the first packet of the server that has to contain a line beginning with "+OK". The plugin does not analyze IMAP4 traffic and is used by SEISMO to detect the version of the mail server used by analyzing the server's banner in order to report possible vulnerabilities.

6.9.15.1. Options

Enabled	Activates or deactivates the plugin
Auto-attach	If the plugin has been activated, it is automatically used to search for a corresponding packet in the filter rules. This option is not available for DNS, RIP, H323, RTP and RTCP plugins.
Close connection when attaching the plugin	When the plugin is automatically activated for a type of traffic, the connection that caused the automatic activation will be closed. Packets will then be blocked. For example, all HTTP traffic can be blocked, regardless of the port concerned. The plugins DNS, RIP and H323, RTP and RTCP do not have this option.

6.9.15.2. Properties

Default port	One or several ports that the plugin will link.

6.9.16. NNTP plugin

The NNTP plugin detects connections between two hosts that use the NNTP news protocol. This is done based on the banner of the news server. The plugin does not scan the contents of the NNTP traffic and is used by SEISMO to detect the version of the news server used by analyzing the server's banner in order to report possible vulnerabilities.

6.9.16.1. Options

Enabled	Activates or deactivates the plugin
Auto-attach	If the plugin has been activated, it is automatically used to search for a corresponding packet in the filter rules. This option is not available for DNS, RIP, H323, RTP and RTCP plugins.
Close connection when attaching the	When the plugin is automatically activated for a type of traffic, the connection that caused the automatic activation will be closed. Packets will then be blocked. For

plugin	example, all HTTP traffic can be blocked, regardless of the port concerned. The plugins DNS, RIP and H323, RTP and RTCP do not have this option.

6.9.16.2. Properties

Default port	One or several ports that the plugin will link.

6.9.17. MGCP plugin

The MGCP plugin performs protocol analyses and dynamically authorizes secondary connections. Connections are scanned line by line – the line has to be complete before the scan can be launched. For each line containing a header, a check will be performed according to the status of the automaton.

- For requests and responses:

    - Check of the version of MGCP and of the command (for requests) or of the command's return code (for responses), confirmation of the identifier of the transaction, the name of the caller, protection from attacks (encoding, format, buffer overflow, etc), validation of MGCP parameters for requests.

    - Analysis and validation of data presented in the SDP (encoding, buffer overflow, RFC compliance, presence and order of mandatory fields, line format, etc).

- For responses (in addition to the earlier checks): general coherence of the response in relation to the request.

6.9.17.1. Options

Enabled	Activates or deactivates the plugin
Auto-attach	If the plugin has been activated, it is automatically used to search for a corresponding packet in the filter rules. This option is not available for DNS, RIP, H323, RTP and RTCP plugins.
Close connection when attaching the plugin	When the plugin is automatically activated for a type of traffic, the connection that caused the automatic activation will be closed. Packets will then be blocked. For example, all HTTP traffic can be blocked, regardless of the port concerned. The plugins DNS, RIP and H323, RTP and RTCP do not have this option.

6.9.17.2. Properties

Default port	One or several ports that the plugin will link.

6.9.18. RTP plugin

The RTP plugin validates Voice over IP connections that use the RTP transmission protocol. The plugin does not dynamically detect RTP. It can be attached by a filter rule or by another Voice over IP plugin (MGCP, SIN) on a child connection. The RTP plugin validates the compliance of RTP packet headers with RFC 3550. The use of certain RTP codecs can be prohibited.

In the event the plugin is attached to a child connection by the SIP or MGCP plugin, the audit feature will include a session group identifier that will enable locating all the connections by conversation, by name of caller and by type of medium used (audio, video, application, data, control, etc).

AllowCodec	A list of allowed RTP codecs, separated by coma. Maximum lengh is 128 chars.

6.9.19. RTCP plugin

The RTCP plugin validates Voice over IP connections that use the RTCP control protocol. The plugin does not dynamically detect RTCP. It can be attached by a filter rule or by another Voice over IP plugin (MGCP, SIP) on a child connection. The RTCP plugin validates the compliance of headers in RTCP packets with RFC 3550, 3611 and 2032. A UDP packet may contain several RTCP packets (composed packets). The use of certain RTCP commands can be prohibited.

In the event the plugin is attached to a child connection by the SIP or MGCP plugin, the audit feature will include a session group identifier that will enable locating all the connections by conversation, by name of caller and by type of medium used (audio, video, application, data, control, etc).

Prohibited operations	A list of denied RTCP operations, separated by comma. Maximum length is 128 chars.
Authorized operations	A list of allowed RTCP operations, separated by comma. Maximum length is 128 chars.

6.9.20. SIP plugin

SIP (*Session Initiation Protocol*) is a protocol that is used for multimedia telecommunications such as internet telephony (VoIP) or host-to-host communication.

In a host-to-host exchange, once the communication has been established, two channels (A to B and B to A) will be used for transporting data. For each channel the SIP plugin of the ASQ engine will create two connections – one for transporting RTP data and the other will be to carry information regarding RTCP.

The SIP plugin supports the main RFC 3261 as well as the following extension that can be enabled or disabled as necessary:

- RFC3262: PRACK
- RFC3265: SUBSCRIBE, NOTIFY
- RFC2976: INFO
- RFC3311: UPDATE
- RFC3428: MESSAGE
- RFC3515: REFER
- RFC3903: PUBLISH

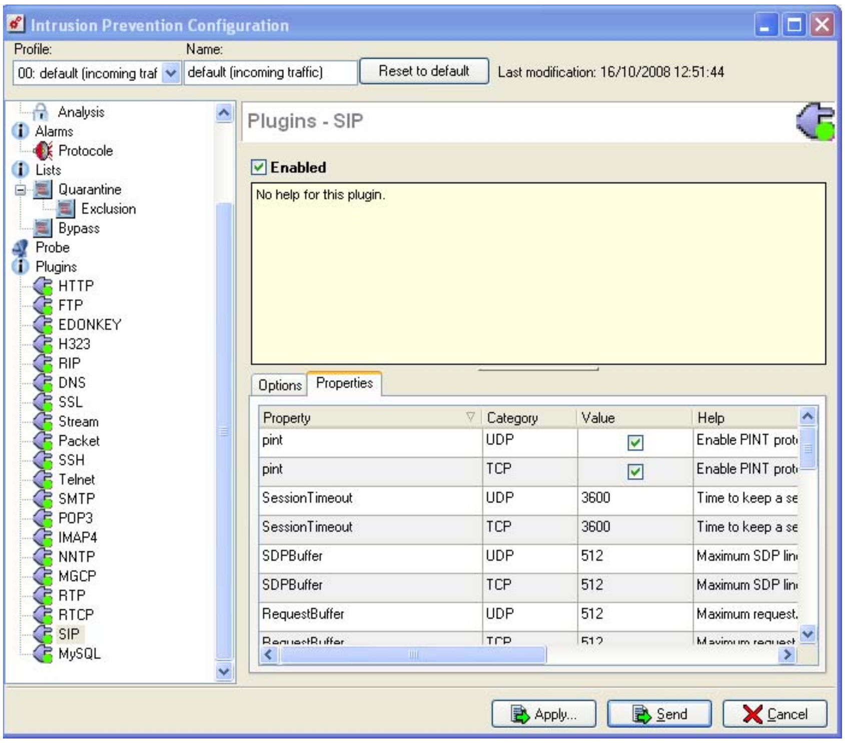
The SIP plugin performs protocol analyses and dynamically authorizes secondary connections. Connections are scanned line by line – the line has to be complete before the scan can be launched. For each line containing a header, a check will be performed according to the status of the automaton.

- For requests and responses:

    - Check of the version of SIP and of the operation, validation of the URL that has to be encoded in UTF-8.
    - Line-by-line analysis of the header: validation of the header fields and the extraction of information (e.g. name of the caller and callee), protection from attacks (encoding, buffer overflow, presence and order of mandatory fields, line format, etc).
    - Analysis and validation of data presented in the SDP (encoding, buffer overflow, RFC compliance, presence and order of mandatory fields, line format, etc).

- For responses (in addition to the earlier checks): general coherence of the response in relation to the request.

The audit feature includes a session group identifier that will enable locating all the connections by conversation, by name of caller and callee and by type of medium used (audio, video, application, data, control, etc).



Profile: 00: default (incoming traf

Name: default (incoming traffic)

Reset to default

Last modification: 16/10/2008 12:51:44

☑ **Enabled**

No help for this plugin.

Property	Category	Value	Help
pint	UDP	☑	Enable PINT prot
pint	TCP	☑	Enable PINT prot
SessionTimeout	UDP	3600	Time to keep a se
SessionTimeout	TCP	3600	Time to keep a se
SDPBuffer	UDP	512	Maximum SDP lin
SDPBuffer	TCP	512	Maximum SDP lin
RequestBuffer	UDP	512	Maximum request.
RequestBuffer	TCP	512	Maximum request

Figure 151: ASQ configuration - SIP

For more information regarding alarms relating to the SIP plugin, please refer to Appendix T: List of alarms relating to protocols.

6.9.20.1. Options

The SIP_UDP and SIP_TCP plugins are grouped together in this window, which will allow disabling the use of this protocol via UDP and/or TCP.

The options in the `Options` tab are common to both plugins, meaning that if you select for example the option “Auto-attach”, both plugins will be enabled.

Enabled	Activates or deactivates the plugin
Auto-attach	If the plugin has been activated, it is automatically used to search for a corresponding packet in the filter rules. This option is not available for DNS, RIP, H323, RTP and RTCP plugins.
Close connection when attaching the plugin	When the plugin is automatically activated for a type of traffic, the connection that caused the automatic activation will be closed. Packets will then be blocked. For example, all HTTP traffic can be blocked, regardless of the port concerned. The plugins DNS, RIP and H323, RTP and RTCP do not have this option.
Log	Activates or deactivates the generation of logs regarding the plugin.

6.9.20.2. Properties

The various SIP buffers that can be supported are indicated in the table below:

Properties	Category	Value	Help
Pint	UDP	Check	Enable PINT protocol support
pint	TCP	Check	Enable PINT protocol support
SessionTimeout	UDP	3600	Time to keep a session when there is no activity in its media.
Session Timeout	TCP	3600	Time to keep a session when there is no activity in its media.
SDPBuffer	UDP	512	Maximum SDP line size for buffer overflow protection.
SDPBuffer	TCP	512	Maximum SDP line size for buffer overflow protection.
RequestBuffer	UDP	512	Maximum request/response size for buffer overflow protection.
RequestBuffer	TCP	512	Maximum request/response size for buffer overflow protection.
RFC3903	UDP	Check	Enable RFC3903 extensions: PUBLISH.
RFC3903	TCP	Check	Enable RFC3903 extensions: PUBLISH.
RFC3515	UDP	Check	Enable RFC3515 extensions: REFER.
RFC3515	TCP	Check	Enable RFC3515 extensions: REFER.
RFC3428	UDP	Check	Enable RFC3428 extensions: MESSAGE.
RFC3428	TCP	Check	Enable RFC3428 extensions: MESSAGE.
RFC3311	UDP	Check	Enable RFC3311 extensions: UPDATE.
RFC3311	TCP	Check	Enable RFC3311 extensions: UPDATE.
RFC3265	UDP	Check	Enable RFC3265 extensions: SUBSCRIBE, NOTIFY.
RFC3265	TCP	Check	Enable RFC3265 extensions: SUBSCRIBE, NOTIFY.
RFC3262	UDP	Check	Enable RFC3262 extensions: PRACK.
RFC3262	TCP	Check	Enable RFC3262 extensions: PRACK.
RFC2976	UDP	Check	Enable RFC2976 extensions: INFO.

RFC2976	TCP	Check	Enable RFC2976 extensions: INFO.
Default port	UDP	sip_udp	One or several ports that the plugin will link up.
Default port	TCP	sip	One or several ports that the plugin will link up.
Prohibited operations	UDP		List of protocol commands that must be refused.
Prohibited operations	TCP		List of protocol commands that must be refused.
Authorized operations	UDP		Additional protocol commands that must be accepted.
Authorized operations	TCP		Additional protocol commands that must be accepted.
Messenger	UDP	Check	Enable support for Windows Messenger.
Messenger	TCP	Check	Enable support for Windows Messenger.
HeaderBuffer	UDP	512	Maximum header size for buffer overflow protection.
HeaderBuffer	TCP	512	Maximum header size for buffer overflow protection.

The lines have been duplicated due to the large number of parameters which are similar for both plugins, which thereby allows the configuration of either plugin. A column named “Category” has been added (unlike for other plugins) to differentiate the SIP_TCP plugin from the SIP_UDP plugin.

6.9.21. MySQL plugin

The MySQL plugin detects connections to a MySQL database server. This is done by relying on the first packet that contains the version of the server. The plugin does not analyze the contents of MySQL traffic and is used by SEISMO to detect the version of the MySQL server used in order to report possible vulnerabilities.

6.9.21.1. Options

Enabled	Activates or deactivates the plugin
Auto-attach	If the plugin has been activated, it is automatically used to search for a corresponding packet in the filter rules. This option is not available for DNS, RIP, H323, RTP and RTCP plugins.
Close connection when attaching the plugin	When the plugin is automatically activated for a type of traffic, the connection that caused the automatic activation will be closed. Packets will then be blocked. For example, all HTTP traffic can be blocked, regardless of the port concerned. The plugins DNS, RIP and H323, RTP and RTCP do not have this option.

6.9.21.2. Properties

Default port	One or several ports that the plugin will link.

6.9.22. The Pass_detach plugin

This plugin allows switching to IDS mode.
ASQ now allows operating in intrusion detection mode. In other words, instead of blocking suspicious traffic, it will only raise an alarm.

To operate in this mode, you need to change the management mode for protocol alarms by indicating “Pass” as the action to perform when such traffic is detected. This may affect the security of the network; alarms are indicated with the icon ❗.

For a “sensitive” alarm, if you change its action and set it to “Pass”, the suspicious traffic will not be blocked and the alarm will be raised. As for the ASQ engine, it will detect the sensitive alarm that meets the criteria associated with the “Pass” action and will detach the affected plugin. This means that the analysis is disabled on the affected plugin only for a connection in progress.

> ❗ **WARNING**
> If a plugin has been detached, it means that it has been disabled. Disabling a plugin carries risks for subsequent treatments as the plugin will no longer be applied for a given connection.
>
> E.g.: You wish to allow packets that contain an “Invalid HTTP protocol” attack to pass through. In this case, you will modify the behavior of this sensitive alarm by setting its action to “Pass”.
> If ASQ detects a packet that contains this attack, the alarm will be raised, the packet will pass through and the HTTP plugin will be detached for the current connection.
>
> Except that, if there is another packet in the same connection that contains an “Invalid %u encoding chair in URL” attack for example, since the plugin has been detached, your network will no longer be protected from this attack.

To see the list of alarms on which the “pass_detach” action is possible, please refer to Appendix S: List of sensitive alarms.

6.9.23. Default configuration

The default configuration for plugins can be retrieved by clickin on the **Default Configuration** button. In this case, all customized data will be overwritten.

PART 7: POLICY

CHAPTER 1: ADDRESS TRANSLATION (NAT)

7.1.1. Introduction

7.1.1.1 For this chapter, you will need to have completed these steps

- Part 2: Installation, pre-configuration, integration.
- Part 5: Network configuration.
- Part 4: Objects

7.1.1.2. For this chapter, you will need to know

- The hosts whose IP address you wish to translate.

7.1.1.3. Purpose of this chapter

This chapter allows you to define the objects whose addresses you wish to translate.

7.1.1.4. Accessing this chapter

➲ Access the dialog box through the **`Policy\NAT`** menu from the menu directory in the graphical interface.

You have to be connected with modification privileges in order to carry out these modifications.

Before performing any major modification on your NETASQ Firewall, we recommend that you perform a backup. As such, in case of any error you will be able to return to the previous configuration. For more information on backups, please refer to the Chapter Maintenance.

7.1.1.5. Introduction to this chapter

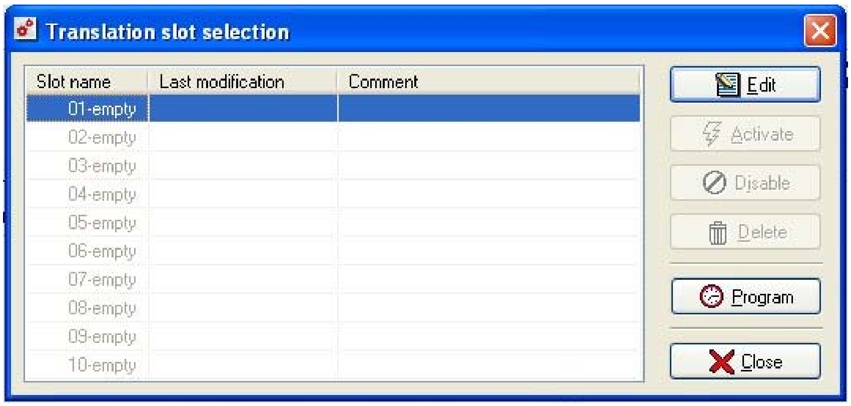
The tables for address translation are stored on the NETASQ firewall in slots (configuration files numbered from 01 to 10).

Each slot can be programmed for a precise time in the week, overriding the configuration of a previously active slot.

7.1.2. Presentation

DEFINITION: NETWORK ADDRESS TRANSLATION (NAT)
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. The rules that make up an address translation policy allow modifying certain traffic elements, therefore map, bimap and port redirection can be created.

➲ When you select the menu **`Policy\NAT`**, a dialog box appears, allowing you to handle the slots associated with address translation.



Slot name	Last modification	Comment
01-empty		
02-empty		
03-empty		
04-empty		
05-empty		
06-empty		
07-empty		
08-empty		
09-empty		
10-empty		

Figure 152: Selecting a NAT policy

It consists of two sections:

Left	List of slots
Right	Actions on selected slot

7.1.2.1. List of policies

The list of slots is found in this part of the dialog box. There are 10, numbered from 01 to 10.

Each policy has a name, a date/time of activity and the date of the last change carried out on this policy. The activation of these policies can be programmed using the slot scheduler (See Part 7/Chapter 3: Slot Scheduler).

A small green arrow to the right of its name indicates the active policy. A policy is "active" when the parameters it contains are in use. There can be no more than one active policy at a time because the parameters of the last active policy overwrite those of the previously active policy.

If you change a policy, you must reactivate it for the changes to be registered. A policy that has been modified but not reactivated is signaled by the icon ❗ instead of the usual green arrow.

It is possible for no policy to be active, implying that no address translation is active.

Each policy does not necessarily have to contain parameters.

A policy for which no configuration file exists on the NETASQ firewall appears under the name "empty" in the list.

A policy is selected when you simply click on its name with the mouse. Once you have selected it, you can edit or activate it.

7.1.2.2. Actions on selected policy

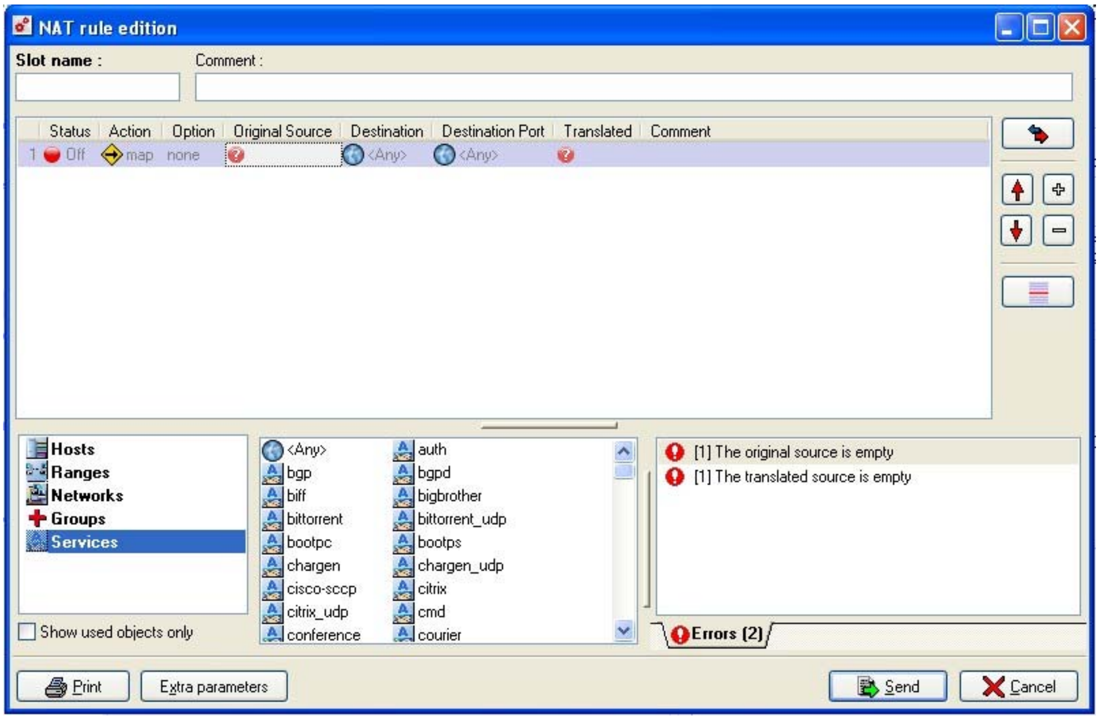
Once a policy has been selected, you can carry out various actions:

Edit	Modifies address translation rules associated to this slot.
Activate	Immediately activates a slot: the parameters stored in this slot suppress the parameters previously in use. When an active slot is selected, this buttons becomes **Disable**.
Disable	Deactivates the currently active slot. No address translation is therefore carried out.
Delete	Deletes the slot and all its information.
Program	Specifies the time and day(s) on which the file will automatically be activated.
Close	Returns to the main screen.

7.1.3. Editing an address translation policy

Refer to the following procedure to edit a translation policy:

1. Select a policy from the list of translation policies.
2. Click on the **Edit** button in the dialog box containing the list of translation policies.



NAT rule edition

Slot name :

Comment :

	Status	Action	Option	Original Source	Destination	Destination Port	Translated	Comment
1	Off	map	none	?	<Any>	<Any>	?	

[1] The original source is empty

[1] The translated source is empty

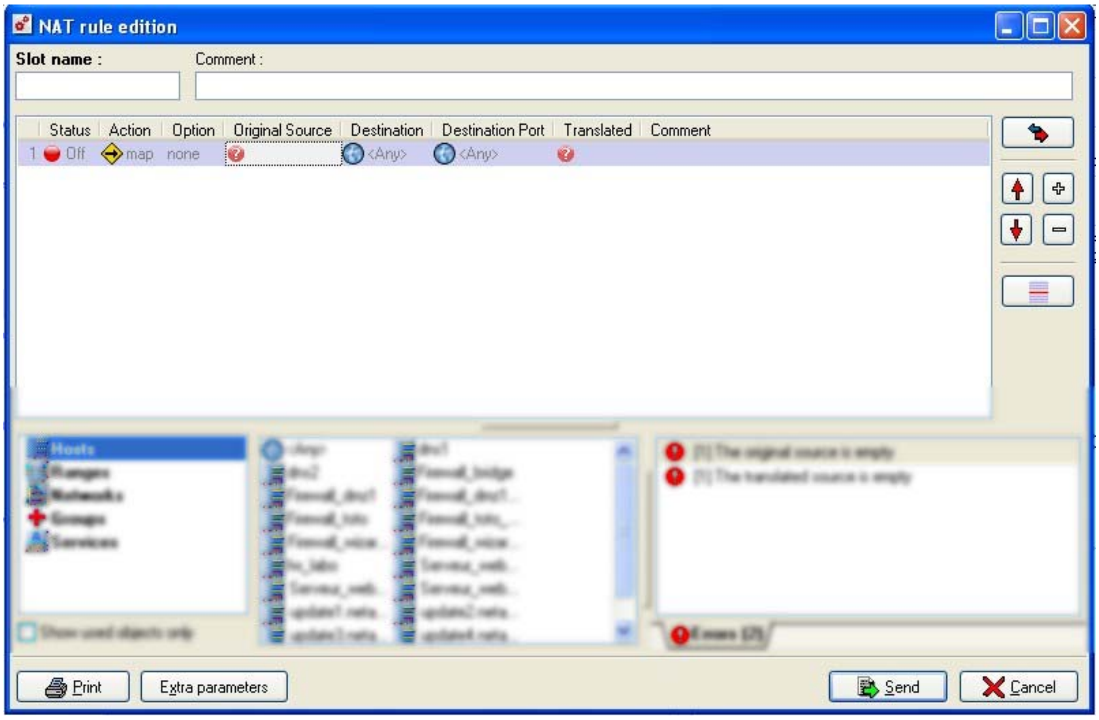
Figure 153: Editing translation rules

The translation policy edition window appears, displaying several sections:

- A table section consisting of translation rules.

- A drag & drop menu
- A rule compliance analyzer.
- A section with the possible actions to perform.

7.1.3.1. Translation rules



NAT rule edition

Slot name :

Comment :

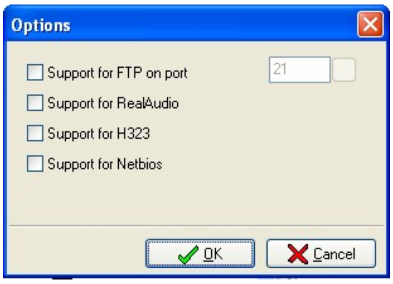
	Status	Action	Option	Original Source	Destination	Destination Port	Translated	Comment
1	Off	map	none		<Any>	<Any>		

[1] The original source is empty

[1] The translated source is empty

Figure 154: Editing translation rules

ID	Number of the rule. This field cannot be edited and indicates the location of the rule in the policy. The order of the rules is important.
Status	🟢 (On) The rule is used by the NETASQ firewall. 🔴 (Off) The rule has been deactivated. Double-click on this field to enable or disable the rule. The line will be grayed out when the rule is Off to indicate its inactivity.
Action	Defines the translation that you wish to carry out. The translation may be Map, Map bidirectionnel, Redirection, Split or No ma and is performed on all the firewall's interfaces. The selected action will determine the role of the other columns in the table.
Option	When address translation rules are used, only the IP addersses contained in the IP header of packets will be modified. However, certain protocols will reference the IP addresses in the data source layer. This window's options allow modifying the addresses found in FTP, Real/Audio, H323 and Netbios so that the packets can be correctly translated. The options allow adding four particular types of service:



Options

☐ Support for FTP on port 21

☐ Support for RealAudio

☐ Support for H323

☐ Support for Netbios

Figure 155: Options

- **Support for FTP on port**: allows supporting FTP in active mode (when the server initiates the data connection).
- **Support for RealAudio**: this will display the source addresses in the data fields of TCP/IP packets,
- **Support for H323**: allows partially managing H323 (voice/video over IP). In this case, the source address will be replaced. Note that NAT on this protocol will not be supported if gatekeepers are used (Cf. *Glossary*).
- **Support for Netbios**: allows supporter for approvals between Windows servers.

These services therefore require special attention during address translation.

Original	Untranslated IP address. Double-clicking on this zone enables selecting the associated object. The object selector only displays objects available for this field.
Destination	Destination of the traffic requiring translation. Double-clicking on this zone enables selecting the associated object. The object selector only displays objects available for this field.
Destination port	Destination port of the traffic requiring translation. Double-clicking on this zone enables selecting the associated object. The object selector only displays objects available for this field.
Translated	Translated IP address (modified by the Firewall). Double-clicking on this zone allows you to select the associated object. The object selector only displays objects available for this field.
Description	Comments which you can associate with this address translation rule.

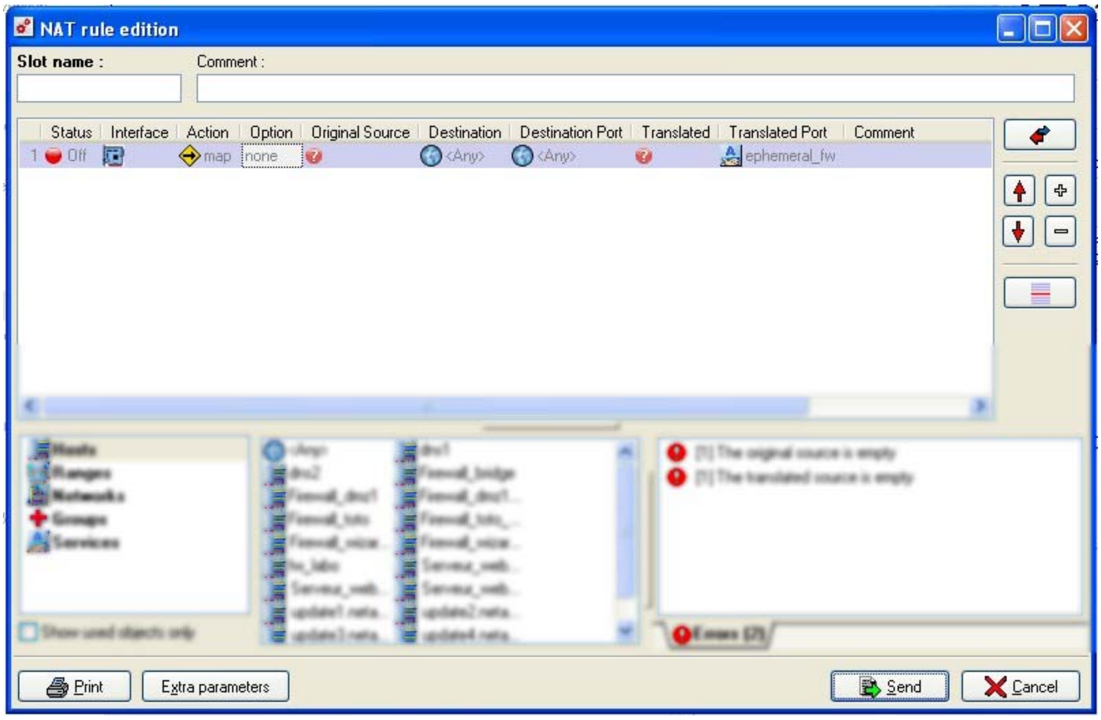
> **Example**
> It can be indicated that all traffic from "Original" to the destaintion port on the "Destination" host will be redirected to the “Translated” host.

WARNING

When the icon representing a question mark in a red circle appears in a field, this means that the field is mandatory for the translation rule.
Activate these options only if you are sure that you wish to use these services. They slow down packet treatment and may cause conflicts.

7.1.3.2. Advanced mode

Advanced mode allows you to access the interface and translated port columns. To be in advanced mode, click on .



NAT rule edition

Slot name :

Comment :

	Status	Interface	Action	Option	Original Source	Destination	Destination Port	Translated	Translated Port	Comment
1	Off		map	none		<Any>	<Any>		ephemeral_fw	

[1] The original source is empty

[1] The translated source is empty

Figure 156: Editing translation rules

Interface Interface to which the translation rule applies, presented in a drop-down list. The Firewall selects it automatically by default, according to the operation and source and destination IP addresses. It is possible to modify it to apply the rule to another interface.

Translated port Port to which translation is carried out. Mainly used to specify a port range to which unidirectional address translation or port redirection (to redirect a connection requested on port XX to port YY) is done. Double-clicking on this zone enables selecting the associated object. The object selector only displays objects available for this field.

7.1.3.3. Action

This zone in the dialog box contains a grid allowing you to define the address translations to apply. The different options are:

Unidirectional translation (map)

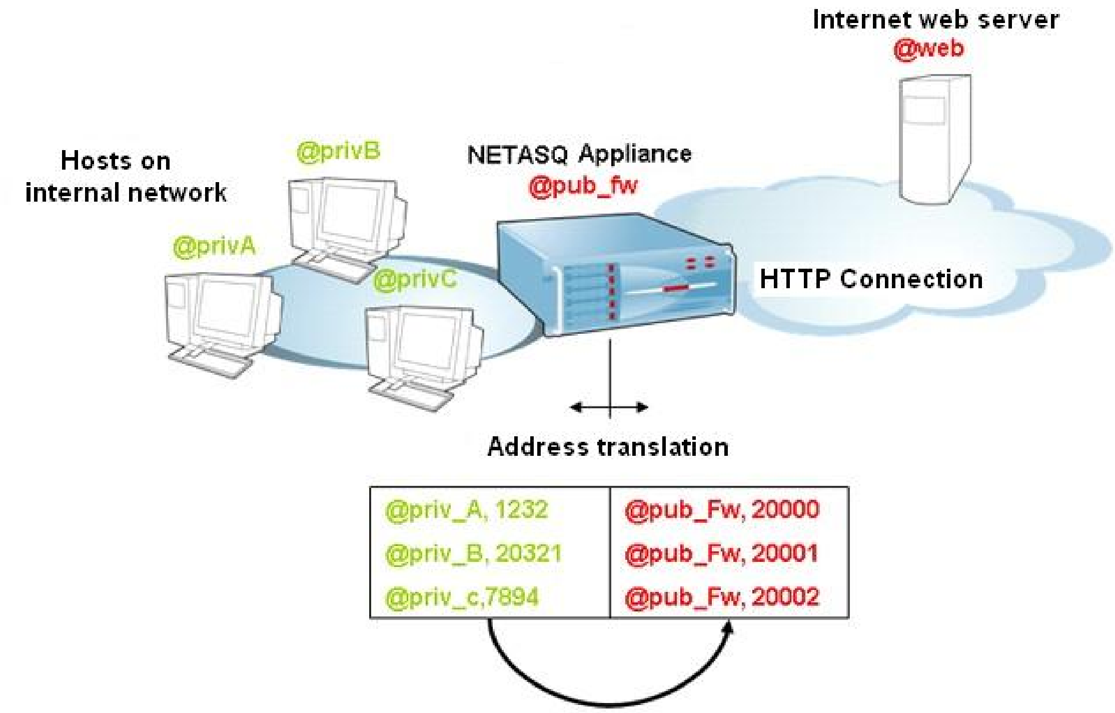
Unidirectional translation of addresses allows you to convert the real IP addresses of your network (internal, external or DMZ) to a virtual IP address on another network (internal, external or DMZ) while going through

Firewall. The source address is changed to a destination address only if the connection comes from the source host (unidirectional).

Unidirectional translation is generally used to mask IP addresses exiting the NETASQ firewall.

It is necessary to specify the translated port range in advanced mode to prevent port conflicts.

The **map** action supports address ranges. Once the ports from the first address are all used, port from the second address will be used.



@priv_A, 1232	@pub_Fw, 20000
@priv_B, 20321	@pub_Fw, 20001
@priv_c,7894	@pub_Fw, 20002

Figure 157: Unidirectional translation

Definition of the rule

Indicate the host's or network's real IP address (private) at the source and the virtual IP address you want to assign at the destination.

No map

It is possible to remove a host in a translated network from a map translation operation.
The address of this host will therefore not be translated through the Firewall.

Definition of the rule

The source must be the host which does not have to be translated. Select the **no map** option and do not indicate anything in the **Translated** column.

This rule must be followed by a map rule.

WARNING

For a no map rule, you have to specify the Firewall interface on which the operation will be applied (this interface is the same for the associated map operation).

You may consult the Examples of Address Translations in Appendix E: Configuration examples for NAT to better understand these choices.

Bi-directional translation (bi-directional map)

Bi-directional address translation allows you to convert an IP address (or N IP addresses) to another (or N IP addresses) while going through Firewall, whatever the origin of the connection.

WARNING
For an N-to-N bi-map rule, original and translated address ranges, networks or host groups have to be of the same size.

Bi-directional translation is generally used to allow access to a server from the outside with a public IP address that is not the same as the host's real address

The "bi-map" action supports address ranges. Source and translated addresses are used in the following order: the "smallest" address in the source field is translated to the "smallest" address in the translated field.

Definition of the rule

The source IP address corresponds to the physical address of the host and the translated IP address corresponds to the virtual address used.

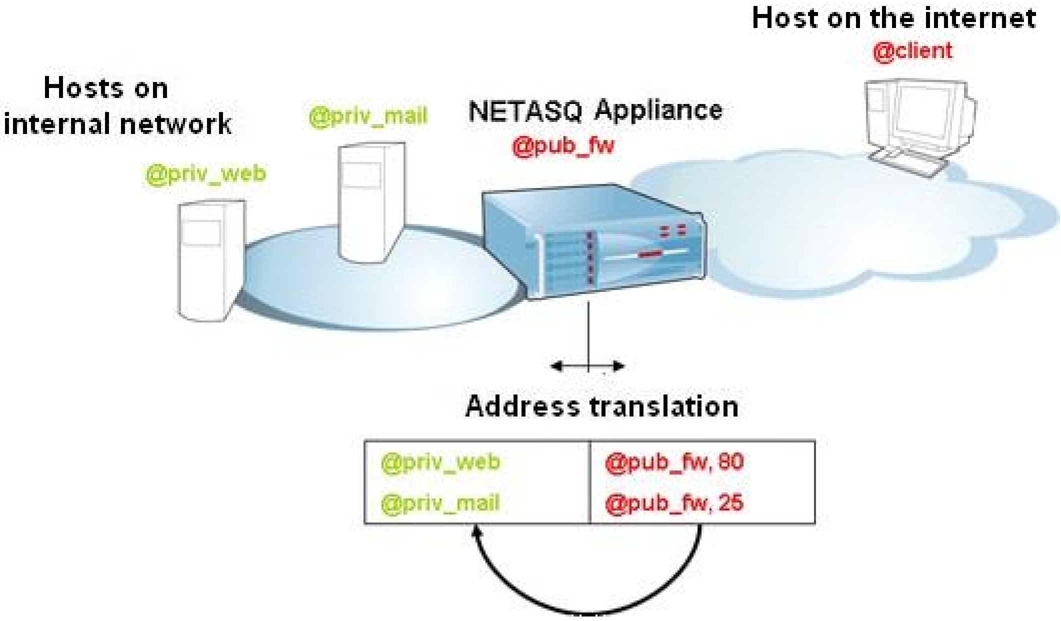


Figure 158: Bi-directional translation

Port redirection (redirect)

Port re-direction allows redirecting packets from one or several sources towards one or several IP addresses with an identical port to another IP address/port number.

This allows traffic to be redirected to the host concerned, based on one public IP address alone, taking into account the port's number.

The port numbers are accessible in advanced mode.

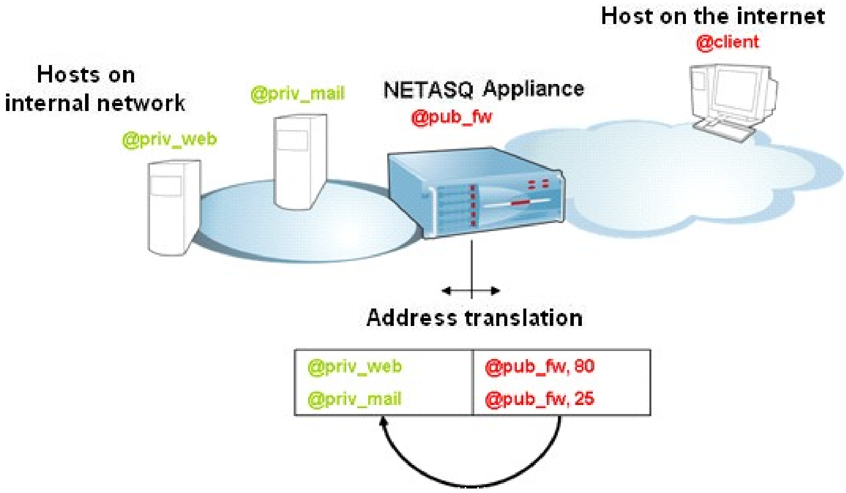


Figure 159: Port redirection

Definition of the rule

The public IP address used corresponds to the source address and the redirection address to the translated address.

Load balancing(split)

Load balancing redirects traffic intended for one IP address to several hosts (host groups). It is possible to specify the ports of the address to be redirected in advanced mode.
In this version, the balancing is carried out evenly, without checking host accessibility.

Definition of the rule

The pool of IP addresses used (host group) corresponds to the destination, the source being the IP address to be contacted

You may consult the Examples of Address Translations in *Appendix E: Configuration examples for NAT* to better understand these choices.

7.1.3.4. Possible actions

Slot name	Name given to the configuration file.
Description	Comments associated to the translation policy
Advanced mode ⇆	Displays advanced configuration parameters for address translation
Insert a rule +	Inserts a new row after the selected row.
Deleted selected line −	Deletes the selected row.
Move rule up the list ↑	Places the selected row before the row directly above it.
Move rule down ↓	Places the selected row after the row directly below it.
Insert a separator ≡ .	This option enables inserting a separator above the selected row in order to add a comment when editing address translation. To define a separator, only a comment and colour need to be be specified for this separator.
Print	Opens the print dialog box allowing you to print your translation rules.
Advanced parameters	By clicking on this button, you may keep active TCP connections when activating the policy.
Send	Sends the configuration file to the NETASQ firewall and programs it at the specified activation time.
Cancel	Cancels changes made since the last send to the NETASQ firewall and returns to the slot list.

A row is selected when one of its elements has been selected (in reverse video).

In addition to these actions you can use standard copy/paste functions for each section of the table:

- With the mouse (click right button).
- With keys **CTRL-C** to copy, **CTRL-V** to paste.
- With keys **CTRL-Insert** to copy, **Shift-Insert** to paste.

7.1.3.5. Contextual menu

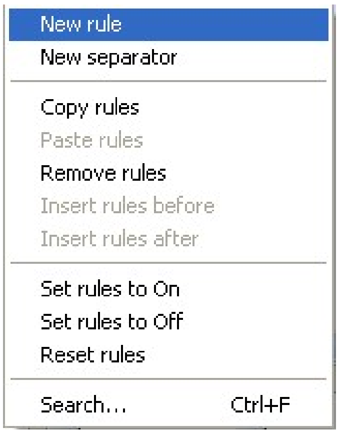


Figure 160: Contextual menu

The contextual menu can be activated by a right click on a row selected within the grid. The different actions proposed are short cuts to the equivalent buttons on the tool-bar.

7.1.3.6. Drag & Drop Menu

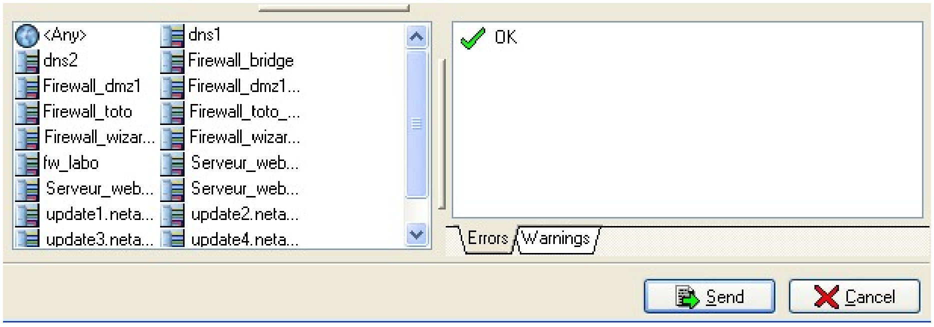


Figure 161: Drag & Drop

As its name indicates, the **Drag & Drop** menu allows positioning objects configured in translation rules in the previous chapter by dragging and dropping. The drag and drop function requires:

1 Selecting an object.
2 Holding the mouse button down.
3 Moving the object to the rule grid.
4 Dropping off the object there.

NOTE
Only the fields Original, Destination, Destination port and Translated are allowed in drag & drop operations since they require the object database.

Grid display

The display of data contained in the grid can be defined according to the administrator's preferences from the following options: large icons, small icons, details or lists.

Display options

There are two available options for displaying data from the drag & drop menu grid.

Hide unused objects

Dummy objects are created by the Firewall by default and are used when associated services are activated.

> **Example**
> Firewall_pptpXX, Firewall_dialupXX, Firewall_ipsec…

These objects make reading difficult and are therefore hidden by default.

7.1.3.7. Rule compliance analyser

The Firewall's translation policy is one of the most important elements for the security of the resources that the Firewall protects. Although this policy is constantly changing to adapt to new services, new threats and new user demands, it has to remain perfectly coherent so that loopholes do not appear in the protection provided by the Firewall.
The art of creating an effective translation policy is in avoiding the creation of rules that inhibit other rules. When a translation policy is voluminous, the administrator's task becomes even more crucial as the risk increases. Furthermore, during the advanced configuration of very specific translation rules, the multiplicity of options may give rise to a the creation of a wrong rule that does not meet the administrator's needs.
A rule compliance analyzer is now present in the translation rule edition window to warn the administrator whenever a rule contradicts another or when there is an error on a rule.
This analyzer, which is divided into two tabs, groups all the errors during the creation of rules in the **Errors** tab and coherence errors in the **Warning** tab.

CHAPTER 2: FILTERS

7.2.1. Introduction

7.2.1.1 For this chapter, you will need to have completed these steps

- Part 2: Installation, pre-configuration, integration.
- Part 5: Network configuration.
- Part 4: Objects.
- Part 7: Address translation policies.

7.2.1.2. For this chapter, you will need to know

The security policy you wish to introduce.

7.2.1.3. Purpose of this chapter

This chapter explains how to define filter rules. It is the “heart” of your policy.
This is where you define who can use what, when and how.
You may limit the inside-to-outside and/or DMZ exchanges as well as the outside-to-inside and/or DMZ exchanges.
You can also define your user’s authentication rules: which hosts or services need authentication.

7.2.1.4. Introduction to this chapter

ASQ technology includes a dynamic packet filter engine (stateful inspection) with rule optimization, enabling the quick and safe application of the filter policy. The implementation of filter functions is based on the comparison of each received IP packet’s attributes with the criteria of each rule in the active filter slot. Filtering affects all packets with no exceptions made. The criteria for filter rules are:

- the incoming interface for IP packets covered by the rule
- the source host(s) of traffic covered by the rule.
- the IP protocol(s), TCP/UDP services and types of ICMP messages from traffic covered by the rule.
- the destination host(s) of traffic covered by the rule.
- the user or user group authorized by the rule

The attributes of the IP packets compared with the first four criteria above are taken from Ethernet, IP, ICMP, UDP or TCP frame headers. As for the user or user group authorized by the rule, from the moment a user identifies himself and authenticates successfully from a given host, the Firewall will take note of it and will attribute this user’s login name to all IP packets using this host’s address as its source IP address. As a result, rules which specify user authentication, even without specifying the restrictions placed on authorized users, can only apply to IP packets transmitted from a host on which a user has already authenticated beforehand. Each filter rule can specify a check action and a log action. There are four possible values for a check action:

- **None**: the packet is analyzed by the rules that follow (this option only specifies a log action)..
- **Pass**: the packet is accepted and the rules that follow do not analyze it.
- **Block**: the packet is destroyed without raising any alarms.
- **Reset**: the packet is destroyed and a TCP RST signal (in the case of TCP) or ICMP unreachable signal (in the case of UDP) will be sent to the sender.

If no filter rule applies to the packet, or if the only rules that do apply do not specify any check action, the packet will be destroyed without raising any alarm.

It is important to note that for a set of IP packets linked to the same exchange at the transport level (TCP connection, UDP or ICMP pseudo-connection), strictly speaking, the Firewall only compares the first packet in the exchange with the current filter slot’s rules. Before any rule from the current filter slot is applied, the moment an IP packet is received, it will be compared to currently established connections/pseudo-connections. If the packet’s attributes and parameters correspond to the criteria and status of one of these connections/pseudo-connections, the packet is authorized to pass through without analysis by the filter rules. Notably, this mechanism enables managing bi-directional exchanges (in particular TCP connections) without the need to define a filter rule for both directions on the Firewall.

The Firewall generates implicit filter rules in connection with the configuration of other security functions. These rules correspond to: remote administration of the Firewall, user authentication and VPN establishment. Moreover, dynamic filter rules are also generated for protocols which require child connections.

There is always an active filter policy when the Firewall is running

Filter tables are stored on the NETASQ firewall in policies (configuration files numbered from 01 to 10). Each slot can be scheduled to run at a precise hour of the day or week, replacing the previously active slot parameters

The concept is simple: when the NETASQ firewall receives a packet (since filter rules are only applied at the entrance of the interface, the Firewall will trust itself for traffic it generates, such as RADIUS, LDAP, Kerberos, etc), it is passed through the list of filter rules. If a match is found, the action associated to this filter is applied or the packet is automatically deleted. Once a rule can be applied to a packet, the packet will no longer be compared against the following rules unless no filter action has been specified.

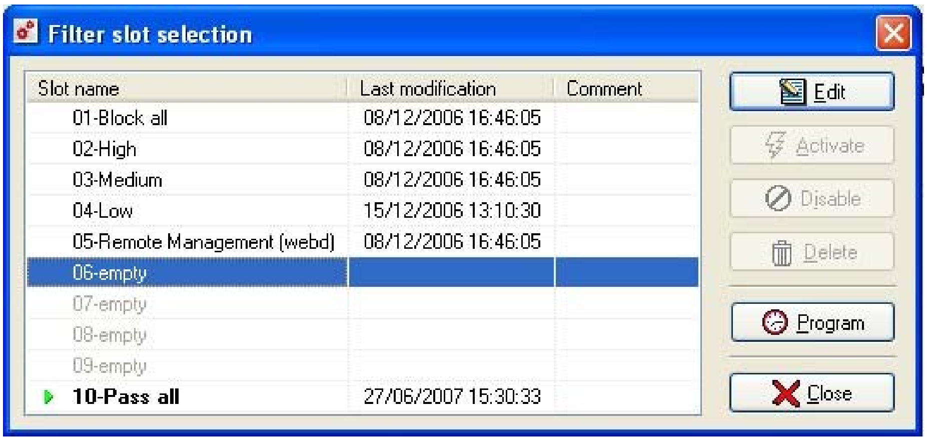
The order of the filter rules is crucial. Maintaining consistency in the order is the main difficulty in good Firewall configuration. (See. *Appendix F: Examples of filter rules*).

7.2.1.5. Accessing this chapter

➲ This dialog box can be accessed using the **Policy\Filter** menu from the menu directory in the graphical interface.

7.2.2. Presentation

DEFINITION FILTERING
Using a set of rules that determine whether certain network traffic will be accepted or blocked according to the defined criteria. (*Cf.* 7.2.4.1. Filter rules)



Filter slot selection

Slot name	Last modification	Comment
01-Block all	08/12/2006 16:46:05	
02-High	08/12/2006 16:46:05	
03-Medium	08/12/2006 16:46:05	
04-Low	15/12/2006 13:10:30	
05-Remote Management (webd)	08/12/2006 16:46:05	
06-empty		
07-empty		
08-empty		
09-empty		
▶ **10-Pass all**	27/06/2007 15:30:33	

Figure 162: Selecting a filter policy

When you select the menu **Policy\Filter**, a dialog box will appear, allowing you to handle the slots associated with address translation.

It consists of two sections:

Left	List of policies.
Right	Actions that can be performed on the selected policy.

7.2.2.1. List of slots

The list of slots (or policies) is found in this part of the dialog box. There are 10, numbered from 01 to 10. Each policy has a name, a date/time of activity and the date of the last change carried out on this policy. The activation of these policies can be programmed using the slot scheduler (See Part 7/Chapter 3: Slot Scheduler).
A small green arrow to the right of its name indicates the active policy. A policy is "active" when the parameters it contains are in use. There can be no more than one active policy at a time because the parameters of the last active policy overwrite those of the previously active policy.
If you change a policy, you must reactivate it for the changes to be registered. A policy that has been modified but not reactivated is signaled by the icon ❗ instead of the usual green arrow.

It is possible for no policy to be active, implying that no address translation is active.
Each policy does not necessarily have to contain parameters.
A policy for which no configuration file exists on the NETASQ firewall appears under the name "empty" in the list.
A policy is selected when you simply click on its name with the mouse. Once you have selected it, you can edit or activate it.

7.2.2.2. Actions on selected policy

Once a policy has been selected, you can carry out various actions:

Edit	Modifies address translation rules associated to this slot.
Activate	Immediately activates a slot: the parameters stored in this slot suppress the parameters previously in use.
Delete	Deletes the slot and all its information. The active slot will be replaced with a an empty slot.
Program	Specifies the time and day(s) on which the file will automatically be activated.
Close	Returns to the main screen.

Right-clicking on a policy will open a contextual menu. The contents of a slot can be exported or imported in a .txt file.

Slots can be copied and pasted. When this is done, the configuration window will open and will already contain the data from the copied slot. (The clipboard is not used for such copy and paste operations).

❗ **WARNING**
A pre-configured slot, named "Pass_all", allows all IP traffic to pass through. It is useful for test phases. Using it in any other scope may prove risky for the security of your sensitive resources.

7.2.3. General remarks on filters

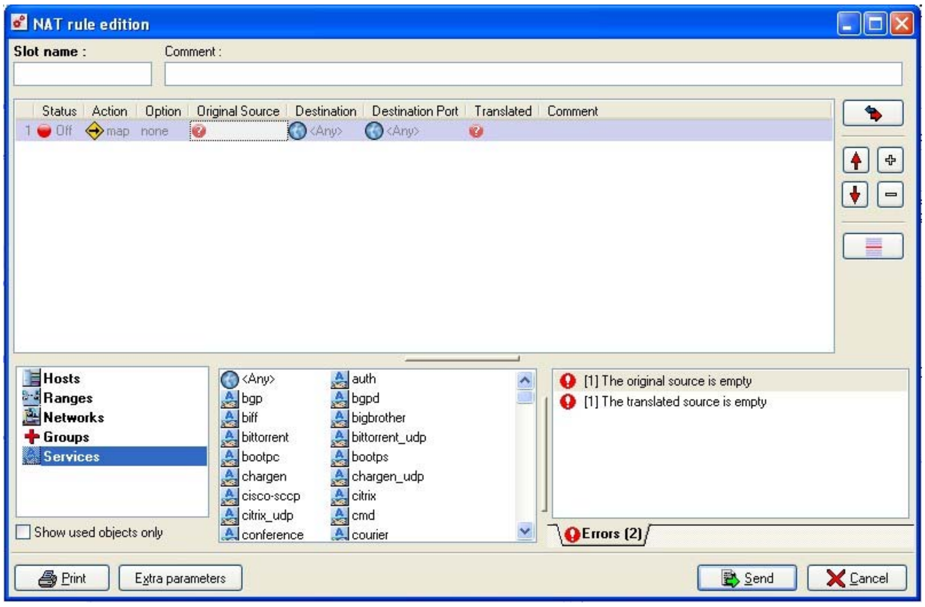
When you use address translation, do not create any filter rules for virtual IP addresses, always used the real object name.

7.2.4. Editing a filter policy

To edit a filter policy, follow the procedure below:

1 Select a policy from the list of filter policies.

2 Click on **Edit** in the dialog box containing the list of filter policies.



	Status	Action	Option	Original Source	Destination	Destination Port	Translated	Comment
1	Off	map	none		<Any>	<Any>		

<Any>, auth, bgp, bgpd, biff, bigbrother, bittorrent, bittorrent_udp, bootpc, bootps, chargen, chargen_udp, cisco-sccp, citrix, citrix_udp, cmd, conference, courier

[1] The original source is empty
[1] The translated source is empty

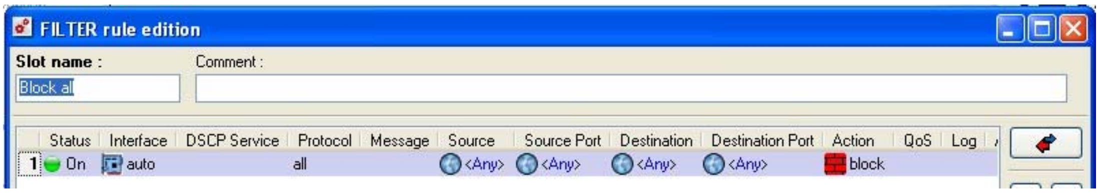
Figure 163: Editing translation rules

The filter policy edition window appears, displaying several sections:

- A table consisting of filter rules.
- A **drag & drop** menu.
- A panel of objects.
- A rule compliance analyzer.
- A section with the possible actions to perform.

Text elements can be located depending on what the administrator types. Whenever the administrator enters text, a panel will appear under the table, containing the text in the search string. Elements in the table that contain this text string will be highlighted.

7.2.4.1. Filter rules



FILTER rule edition

Slot name : Block al

Comment :

	Status	Interface	DSCP Service	Protocol	Message	Source	Source Port	Destination	Destination Port	Action	QoS	Log
1	On	auto		all		<Any>	<Any>	<Any>	<Any>	block		

Figure 164: Editing filter rules

This tab contains a grid allowing you to define the filter rules to apply. Make sure that you arrange your filter rules in order to achieve a coherent result. The Firewall runs the rules in the order in which they appear on screen and stops as soon as it finds a rule that applies to the flow attempting to pass through. It is therefore advisable that you define the rules from **most detailed to most general**.

In simple mode, the following information will appear:

ID	Number of the rule in the policy. There are as many numbers as there are rules in a policy.
Status	🟢 (On) The rule is used by the NETASQ firewall. 🔴 (Off) The rule has been deactivated. Double-click on this field to enable or disable the rule. The line will be grayed out when the rule is Off to indicate its inactivity.
Protocol	Protocol to which the filter rule applies
Source	Source object used as selection criterion for this rule. Double-clicking on this zone enables selecting the associated object. The object selector only displays objects available for this field.
Destination	Destination object used as selection criterion for this rule. Double-clicking on this zone enables selecting the associated object. The object selector only displays objects available for this field..
Destination port	Service or service group used as selection criterion for this rule. Double-clicking on this zone enables selecting the associated object. The object selector only displays objects available for this field.
Action	Action applied to the packet to fill in the selection criteria for this filter rule.
Log	Log type generated.
Description	Comments you wish you enter to associate to this rule.

In the **Status** column, a green indicator means that during the activation of the slot, this rule will be applied. A red indicator means that the rule will not be applied. This enables defining rules which will be used later or temporarily deactivating certain rules to carry out tests.

WARNING
Rules are inactive by default (red indicator).

To the left of the object names (source and destination), there is a type icon indicating the type of the object (machine or network). A small "+" symbol appears next to object groups.

If a rule is not or no longer valid, it is automatically switched to "Off" and an icon with an exclamation mark appears in the column with the problem.

7.2.4.2. Possible slot actions

Slot name	Name given to the configuration file.
Comment	Comments associated to the filter slot
Normal/ Advanced mode	Displays advanced configuration parameters for filters. Additional columns will appear in advanced mode. The grid is in normal mode by default.
Insert a rule	Inserts a new row after the selected row.
Delete selected rules	Deletes the selected row.
Move rule up the list	Places the selected row before the row directly above it.
Move rule down	Places the selected row after the row directly below it.
Insert a separator	This option enables inserting a separator above the selected row in order to add a comment when editing address translation. To define a separator, only a comment and colour need to be be specified in the configuration window. Once the separator has been inserted, a small button will appear. Click on this button in order to deploy rules. If the rules within a separator do not appear, the number of rules will be indicated next to the seprator's label.
Print	Opens the print dialog box allowing you to print your translation rules.

NOTES

1) A row is selected when one of its elements has been selected (in reverse video).
2) Certain buttons are grayed out if they are likely to be irrelevant (for example, the Normal/Advanced mode button is grayed out for URL filters)

7.2.4.3. Contextual menu

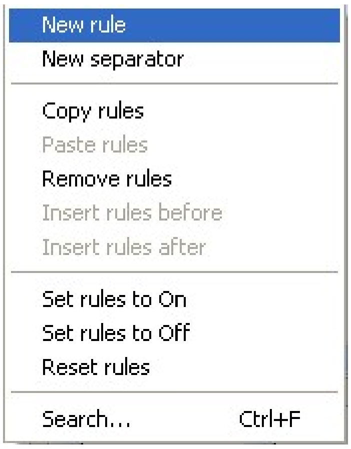


Figure 165: Contextual menu

The contextual menu can be activated by a right click on a row selected within the grid. The different actions proposed are short cuts to the equivalent buttons on the tool-bar.

Furthermore, you can use the standard cut and paste functions:

- **CTRL-c** to copy, **CTRL-v** to paste
- **CTRL-D** to delete a row
- **Ins** to insert a row after the current row
- **Maj+Ins** to insert a row before the current row

You may delete a row by directly pressing on **Del** on the keyboard.

You may move a rule with “+” and “-“ on the keyboard.

7.2.4.4. Objects panel

There are two parts to the objects panel:

- The object categories
- The objects belonging to the category of the selected object (selected by dragging and dropping). The list of objects therefore adapts to the chosen category.

Each list contains the object <Any> which represents all objects.

7.2.4.5. Drag & Drop Menu

As the name ‘Drag & drop” indicates, this menu allows positioning objects configured in translation rules in the previous chapter by dragging and dropping. It allows copying an object from one cell to another or to receive objects from the objects panel. The drag and drop function comprises:

1. Selecting an object.
2. Holding the mouse button down.
3. Moving the object to the rule grid.
4. Dropping off the object there.

When the administrator performs a drag and drop operation, the columns that contain the selected object are highlighted. Once the operation is complete, the highlighting will be removed.

The object selection menu to the right of the drag & drop menu enables selecting the object type to be displayed in the grid.

Grid display

The display of data contained in the grid can be defined according to the administrator’s preferences from the following options: large icons, small icons, details or lists.

Display options

A display option for data from the Drag & Drop menu is available.

Hide unused objects

This option enables displaying only objects that are currently used in the translation rules.

7.2.4.6. Rule compliance analyser

The Firewall's translation policy is one of the most important elements for the security of the resources that the Firewall protects. Although this policy is constantly changing to adapt to new services, new threats and new user demands, it has to remain perfectly coherent so that loopholes do not appear in the protection provided by the Firewall.

The art of creating an effective translation policy is in avoiding the creation of rules that inhibit other rules. When a translation policy is voluminous, the administrator's task becomes even more crucial as the risk increases. Furthermore, during the advanced configuration of very specific translation rules, the multiplicity of options may give rise to a the creation of a wrong rule that does not meet the administrator's needs.

A rule compliance analyzer is now present in the translation rule edition window to warn the administrator whenever a rule contradicts another or when there is an error on a rule.

This analyzer, which is divided into two tabs, groups all the errors during the creation of rules in the **`Errors`** tab and coherence errors in the **`Warning`** tab.

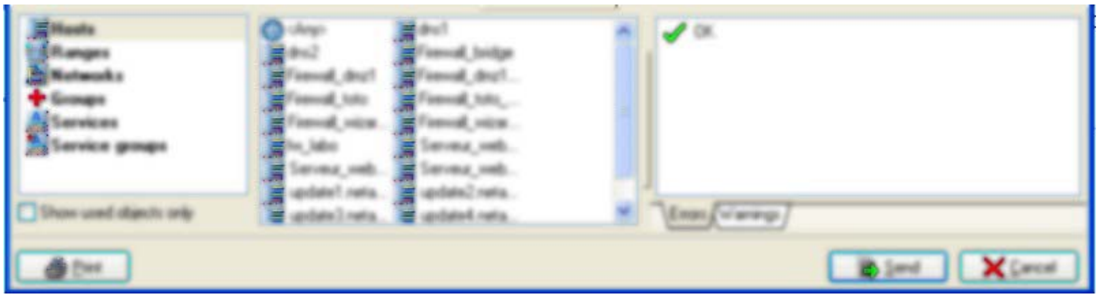


Figure 166: Warnings

The number of errors or warnings calculated in the rule configuration appears next to the titles of both tabs. Once this number is higher than 0, the title will appear in bold.

When there are errors or warnings, rows will appear in these tabs allowing comments to be indicated concerning the problem or the rule that triggered the error or warning.

When no errors or warnings are encountered, the message "No problems encountered" will remain displayed.

The calculating module operates as a background task and will not affect the administrator's tasks.

7.2.5. Creating filter rules

This section details the creation of your filter rules. The order in which these rules are created is important as the Firewall moves through the rules from the top down and stops as soon as it finds a rule corresponding to the IP packet (unless it is only running an option). Authentication rules have to be configured in this section. These rules will limit access for some users for certain services or certain hosts.

7.2.5.1. Activating and deactivating rules

● **On**: The rule is used for filtering.
● **Off**: The rule is not used for filtering

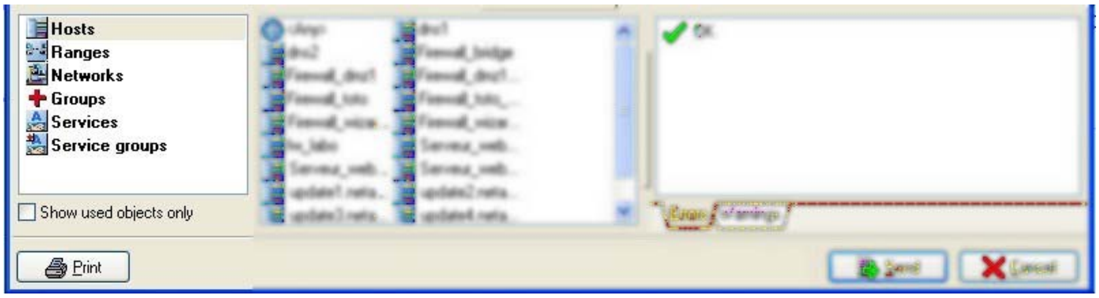


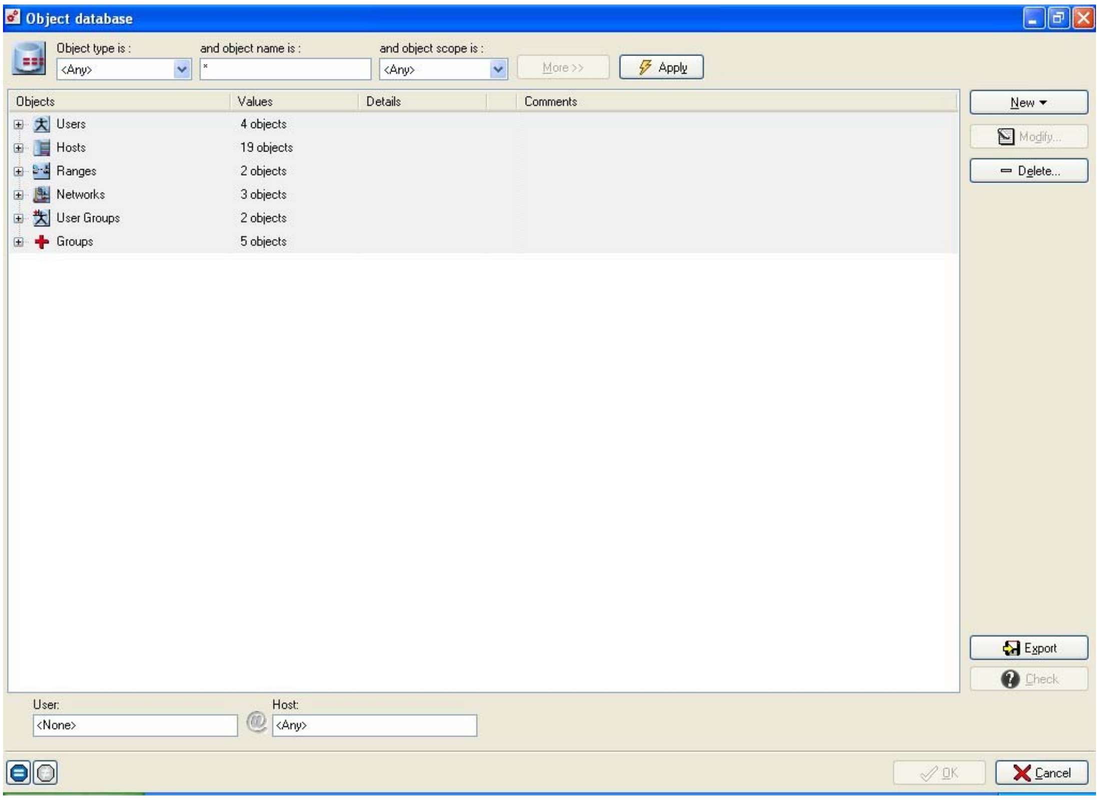
Figure 167: Enabling/Disabling rules

Filter rule activation and deactivation facilitates the development of your filters. NETASQ firewall does not take deactivated rules into account when the slot is activated.

7.2.5.2. Source object and destination object

The “Source” object corresponds to the source of the treated packet. This could be a host, network, group or range.

As for the "Destination" object, it corresponds to the destination of the treated packet.



Object type is : <Any>
and object name is : *
and object scope is : <Any>

Objects	Values	Details	Comments
Users	4 objects		
Hosts	19 objects		
Ranges	2 objects		
Networks	3 objects		
User Groups	2 objects		
Groups	5 objects		

User: <None>
Host: <Any>

Figure 168: Object database

By double-clicking on this zone, you can select the objects concerned by the rule you wish to define, thanks to the object selection dialog box.

Choice of the source

Each source of a rule is defined like this: **<User>@<IP>**.

In order to define a source, you have to choose the <User> part and the <IP> part. The <User> part could be a user or a user group defined in the Firewall. The <IP> part could be a host, a host group, a network or network group defined in the Firewall's objects.

Different scenarios:

- **<Any>@<Any>**: the rule is applied to any host but the user has to authenticate
- **<No Auth>@<Any>**: the rule is applied to any host without authentication
- **<No auth>@Object**: the rule is applied to the "Object" (this object could be a host, a host group, a network or a network group) without authentication
- **<Any>@Object**: the rule is applied to the "Object" and the user has to authenticate,
- **User@<Any>**: the rule is applied to any host but the user has to be authenticated under the "User" login.
- **User@Object**: the rule is applied to the "Object" and the user has to be authenticated under the "User" login.

If a source has a <User> part different from <No auth>, then authentication is required.

Choice of a destination

The destination is always a host, host group or network.

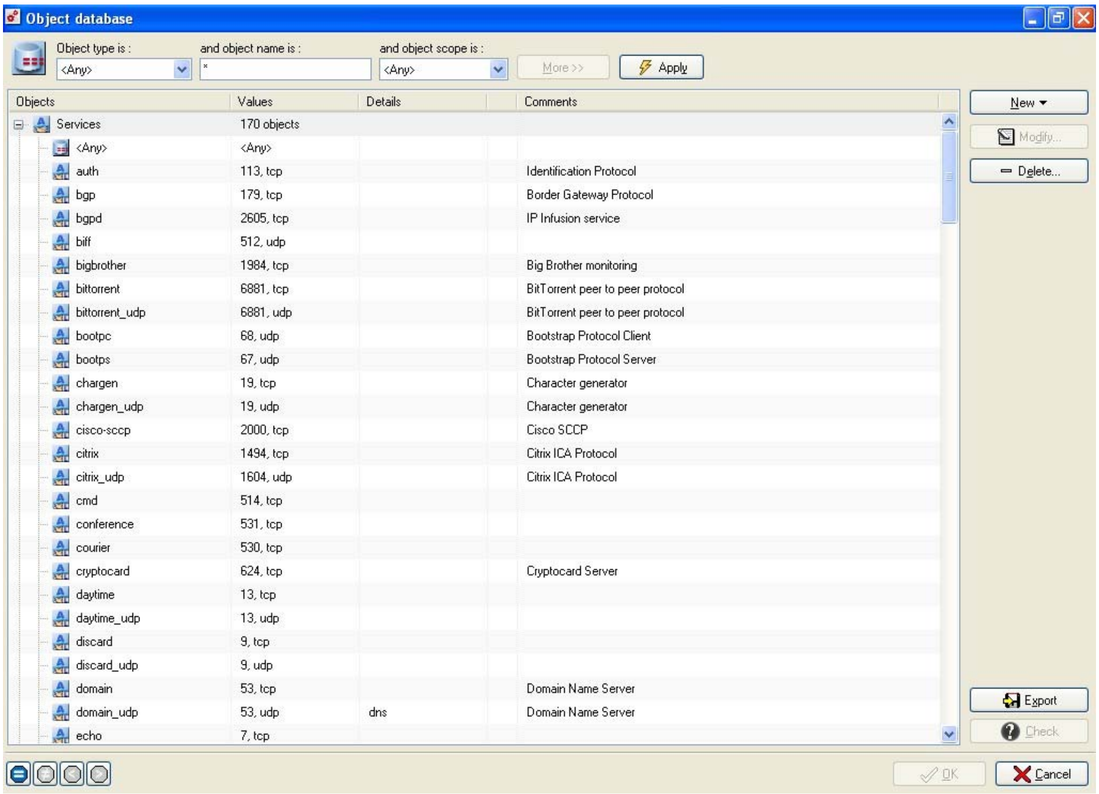
> **NOTE**
> The object **<Any>** corresponds to ALL possible IP addresses. It is important to note that the object **<Any>** is an object entirely on its own. It is not a "joker" that replaces other objects.
> *Part 4: objects*.
> These objects are those defined during *Part 4: objects*.
>
> The empty field under the tabs allows you to do a quick search in the list (with the first letter of the object for example).

Operator	= Means that the object affected by the filter rule is the object selected. ≠ Means that the object affected by the filter rule is anything but the object selected.
OK	Validates the selection.
Cancel	Cancels the selection and returns to the previous window.

> **WARNING**
> The source object is always the initiator of communication.

If you use address translation, always use the **Real** object as Source (not the translated object) as the NETASQ firewall applies rules on real addresses.

7.2.4.5. Destination port



Object type is : <Any>
and object name is : *
and object scope is : <Any>

Objects	Values	Details	Comments
Services	170 objects		
<Any>	<Any>		
auth	113, tcp		Identification Protocol
bgp	179, tcp		Border Gateway Protocol
bgpd	2605, tcp		IP Infusion service
biff	512, udp		
bigbrother	1984, tcp		Big Brother monitoring
bittorrent	6881, tcp		BitTorrent peer to peer protocol
bittorrent_udp	6881, udp		BitTorrent peer to peer protocol
bootpc	68, udp		Bootstrap Protocol Client
bootps	67, udp		Bootstrap Protocol Server
chargen	19, tcp		Character generator
chargen_udp	19, udp		Character generator
cisco-sccp	2000, tcp		Cisco SCCP
citrix	1494, tcp		Citrix ICA Protocol
citrix_udp	1604, udp		Citrix ICA Protocol
cmd	514, tcp		
conference	531, tcp		
courier	530, tcp		
cryptocard	624, tcp		Cryptocard Server
daytime	13, tcp		
daytime_udp	13, udp		
discard	9, tcp		
discard_udp	9, udp		
domain	53, tcp		Domain Name Server
domain_udp	53, udp	dns	Domain Name Server
echo	7, tcp		

Figure 169: Object database

By double-clicking this zone, you can choose the service or service group concerned by the filter rule, thanks to the following dialog box

You can select a service or service group. These services are those defined during *Part 4: objects*.

At the bottom of this window, the following buttons are displayed:

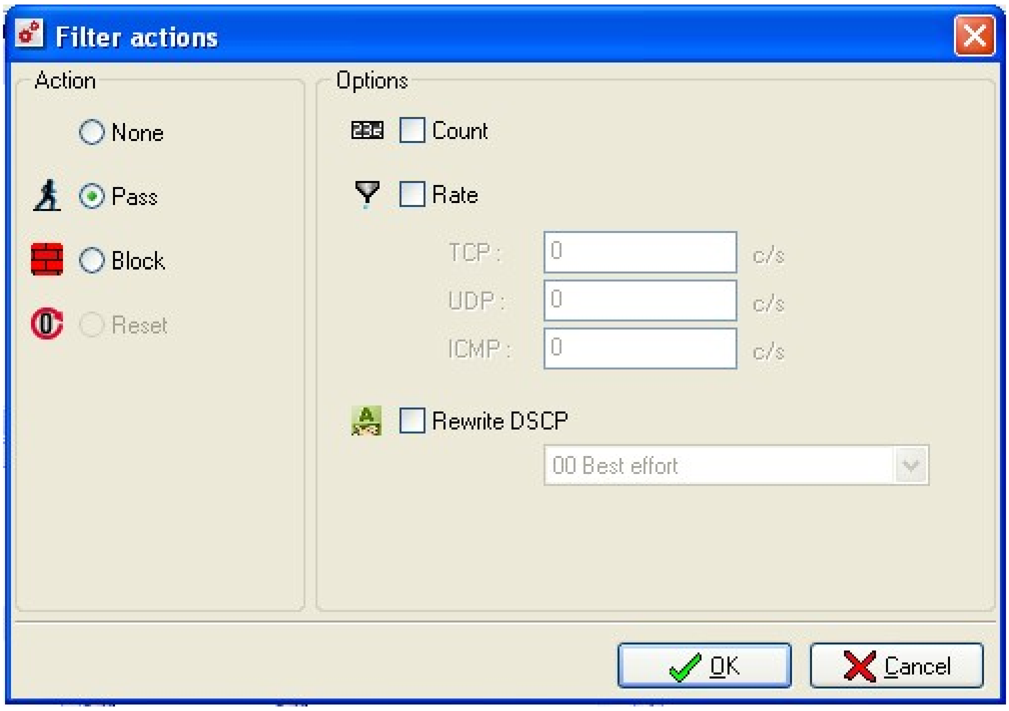
Operation	= Means that the service affected by the filter rule is the service selected. ≠ Means that the service affected by the filter rule is anything but the service selected. < Means that all services concerned are those whose port numbers are lower than or equal to the port number of the service selected. > Means that all concerned services are those whose port number is greater than or equal to the selected service's port number.
OK	Validates the selection.
Cancel	Cancels the selection and returns to the previous window.

By default, the service corresponds to the destination host’s destination port. The source ports are generated automatically by the "Stateful" module.

In certain cases, you may need to specify the source ports. In this case, simply click on ⇆ located under the rule grid. An additional column is displayed next to the "Source objects" column called "Source port". By double-clicking in this column, you can select the service to be used on the source host.

7.2.4.6. Action

Double-clicking on an action in the “Action” column opens the following window:



Action

○ None
● Pass
○ Block
○ Reset

Options

□ Count
□ Rate
TCP : 0 c/s
UDP : 0 c/s
ICMP : 0 c/s
□ Rewrite DSCP
00 Best effort

Figure 170: Filter actions

By double-clicking in this zone, you can select the action associated with the filter rule by means of the following dialog box:

The left section of the screen contains all possible actions that you can define:

None	The NETASQ firewall does nothing. This is useful if you simply want to make use of the options, with no associated action.
Pass	The NETASQ firewall allows the packet corresponding to this filter rule to pass. The packet stops moving down the list of rules.
Block	The NETASQ firewall silently blocks the packet corresponding to this filter rule: the packet is deleted without the sender being informed. The packet stops moving down the list of rules.
Reset	The NETASQ firewall explicitly blocks the packet corresponding to this filter rule: the NETASQ firewall sends A TCP-IP response to the sender of the packet. The packet no longer moves down the list of rules. This option is only available for certain services.

You can add the following complementary options to the **Pass** action:

Count	The NETASQ firewall counts the number of packets corresponding to this filter rule and generates a report (in the counter statistics). The packet continues to move down the list of rules. You may thus obtain volume information on the desired traffic.

Rate The NETASQ firewall may limit the maximum number of connections accepted per second for a filter rule. For the protocol corresponding to the rule (TCP, UDP, ICMP), define the number desired.

WARNING
The restriction only applies to the corresponding rule

> **Example**
> If you create an HTTP rule, only a TCP restriction will be taken into account. This option also allows you to prevent a denial of service which hackers may attempt: you may limit the number of requests addressed to your servers.

REMARK
If the option is assigned to a rule containing an object group, the restriction applies to the whole group (total number of connections).

Rewrite DSCP Tags the field as DSCP in order to define traffic differentiation. The menu offers two ways of defining DSCP fields: according to standards (defining classes are the subject of an RFC) or manually (this option is not compatible with equipment based only on the standard qualification).

This information can be processed by Quality of Service (QoS) equipment. This option can be associated with the DSCP Service or QoS field in the advanced filter configuration of NETASQ firewalls. Examples of usage are indicated in the section "DSCP and QoS" below.

Certain actions or options are available only after the protocol or service in the filter rule has been selected. You may consult the examples of filter rules in *Appendix F: Examples of filter rules* to better understand these choices.

7.2.4.7. Logs

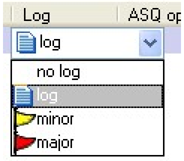


Figure 171: Logging

Clicking in this zone allows you to define the log policy for the chosen rule.

No log No log action is assigned to the rule.

Log As soon as this filter rule is applied to a connection, a log is added to the log files, in the filtering section.

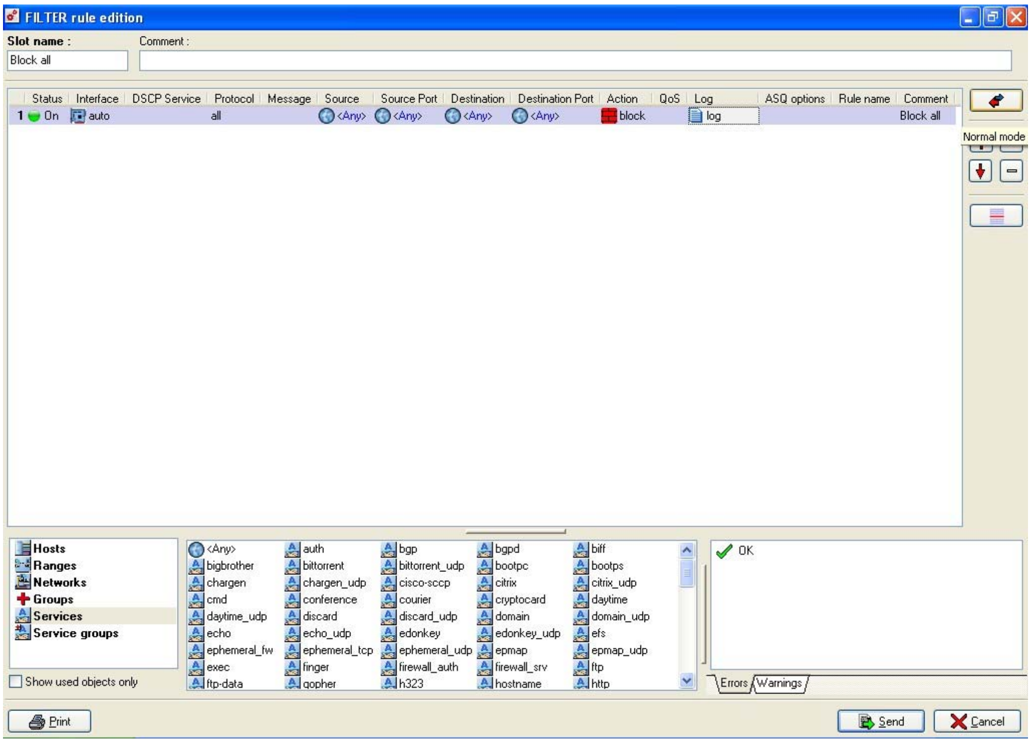
Minor As soon as this filter rule is applied to a connection, a minor alarm is generated. This alarm is transferred to the logs (alarm section), sent to the real-time monitor and may be sent by e-mail (see Chapter VIII Log Management).

Major As soon as this filter rule is applied to a connection, a major alarm is generated. This alarm is transferred to the logs (alarm section), sent to the real-time monitor and may be sent by e-mail (see Chapter VIII Log Management).

7.2.4.8. Description

This field allows the user to enter a brief description of the rule.

7.2.4.9. Advanced configuration



FILTER rule edition

Slot name : Block all

Comment :

	Status	Interface	DSCP Service	Protocol	Message	Source	Source Port	Destination	Destination Port	Action	QoS	Log	ASQ options	Rule name	Comment
1	On	auto		all		<Any>	<Any>	<Any>	<Any>	block		log			Block all

☐ Show used objects only

✓ OK

Figure 172: Editing filter rules – Advanced mode

By clicking on , some new columns appear. It allows you to configure other fields related to your filter rules:

Interface Allows you to choose on which interface you want to apply the rule. By default, the Firewall automatically selects the interface according to the IP address of the source host.

DSCP Service DSCP, or Differentiated Services Code Point, as its name implies, enables determining, through a pre-established code, whether a type of traffic belongs to a certain service. Used in the context of Quality of Service, this DSCP service allows the administrator to apply QoS rules according to the service differentiation he has defined.

In filter rules, when the administrator specifies a DSCP service, he chooses to only assign the rule to traffic with the same DSCP. This field can be associated with the QoS field in the advanced configuration of filter rules. Examples of usage are indicated in the section “DSCP and QoS” below.

Message You can choose the ICMP messages you want to filter.

Source Port This column allows you to specify the port used by the source host, if it is of a particular value. By default, the Stateful module memorizes the source port used, which will be the only authorized for return packets.

Routing This column is useful when specifying a particular router that will allow directing the traffic matching the rule to the defined router. It also allows specifying the

	host used for routing, as such making the routing configuration finer. NOTE When treating the packet, the ASQ engine will assess rules in the order in which they have been defined in the table. For example, if you wish to route the HTTP traffic to a particular router and to restrict HTTP access to a certain group of users, the users' filter rule will have to be specified before the routing rule.
QoS	The QoS field enables defining the Quality of Service policy associated with the traffic. Instructions on the full configuration and use of NETASQ's QoS are indicated in *Part 7/Chapter 5: QoS*.
ASQ options	There are three options in the "ASQ options" field: - **Profil No.:** ASQ profile to apply to the traffic. (Cf. *Part 6: ASQ Intrusion Prevention*). - **Do not attach plugins**: to enable the automatic attachment of plugins for this filter rule. - **No contextual signatures**: to disable contextual signature analysis for this filter rule.
Rule name	Enables indicating a name for the selected filter rule. This option is useful when sorting in NETASQ EVENT REPORTER.

WARNING
These options require proper knowledge of Firewall filtering. They should only be used with full knowledge of the consequences.

It is inadvisable to use the ICMP message filtering option without proper knowledge on how to operate it. The **Auto ICMP** option (in the **`Analysis`** tab of the **`Intrusion Prevention\ASQ`** menu) already performs ICMP filtering according to the connection context.

7.2.4.10. DSCP and QoS

The NETASQ UTM appliance is an integral part of the Quality of Service policy that has to be implemented within a company. In fact, most of the strategic traffic in this Quality of Service will pass through the Firewall.

Therefore the administrator of a NETASQ Firewall has to be able to configure all the services expected of a Quality of Service equipment. There are three options for this:

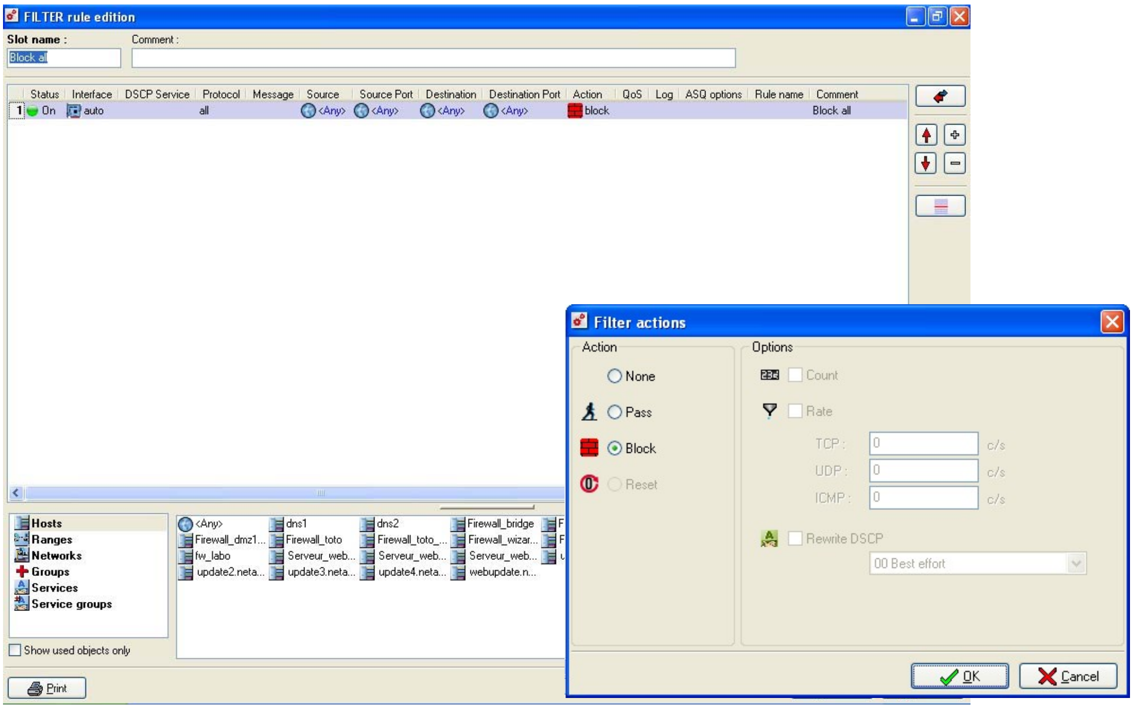
- **DSCP Service field**: located in the section for advanced filter configuration, it allows differentiating traffic that will be processed by the Firewall's filter.
- **Rewrite DSCP field**: located in the configuration menu of the action associated with a filter rule. This option merely enables the modification of the DSCP field.
- **QoS field**: located in the section for advanced filter configuration, this option allows applying QoS rules on defined traffic.

The combination of these three options enables the full configuration of a QoS policy at the Firewall level.

Example 1: Rewrite DSCP
One useful action to begin with is the rewriting of the DSCP field. For example, when certain types of traffic are not differentiated on the internet, the administrator sets up a QoS policy on the local

network, which he wishes to apply on traffic originating from the internet. In this case, a DSCP field rewriting mechanism has to be set up to tag traffic (not differentiated up to then) which has to be assigned by the QoS policy.

The configuration of the filter policy is therefore as follows:



FILTER rule edition

Slot name : Block all

Comment :

	Status	Interface	DSCP Service	Protocol	Message	Source	Source Port	Destination	Destination Port	Action	QoS	Log	ASQ options	Rule name	Comment
1	On	auto		all		<Any>	<Any>	<Any>	<Any>	block					Block all

Filter actions

Action: ○ None ○ Pass ● Block ○ Reset

Options: □ Count □ Rate TCP : 0 c/s UDP : 0 c/s ICMP : 0 c/s □ Rewrite DSCP 00 Best effort

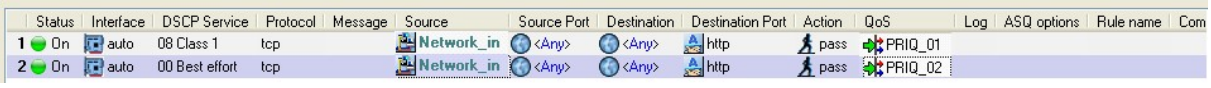
Figure 173: Editing filter rules

All undifferentiated traffic towards the web server have had their DSCP fields rewritten.

Example 2: Applying a QoS policy on differentiated traffic

The other main use for QoS options explained above is the application of a QoS policy on differentiated traffic. When a firewall receives differentiated traffic from the "DSCP Service" field, it can then apply the associated QoS rule defined by the administrator.

The following shows an example of configuring the filter policy:



	Status	Interface	DSCP Service	Protocol	Message	Source	Source Port	Destination	Destination Port	Action	QoS	Log	ASQ options	Rule name	Com
1	On	auto	08 Class 1	tcp		Network_in	<Any>	<Any>	http	pass	PRIO_01				
2	On	auto	00 Best effort	tcp		Network_in	<Any>	<Any>	http	pass	PRIO_02				

Figure 174: QoS policy

Here, two types of traffic which are practically identical (traffic originating from the local network towards the web) are treated differently because of the DSCP field.

CHAPTER 3: PROGRAMMING SLOTS

7.3.1. Slot Scheduler

Filter and encryption slots are subject to hourly scheduling. Administrators who have F+M or V+M rights use a grid which resembles an interactive table for each slot type. The horizontal scale represents the hours of the day, while the vertical scale symbolizes the days of the week. Slots can be assigned to time slots by selecting a previously-defined slot and by highlighting the corresponding time slots with the mouse.

There must always be an active filter slot at any given time. When an administrator starts with a new grid to define or modify the filter scheduling, the first slot that the administrator selects will automatically be assigned to every hour of every day in the week.

You can configure a slot so that it activates only during “office hours”, programming it to block all traffic the rest of the time.

To program the activation of a slot you have two possibilities:

- By the **`Slot Scheduler`** menu in the NETASQ UNIFIED MANAGER menu directory.
- By the **Program** button present in all slot grids.

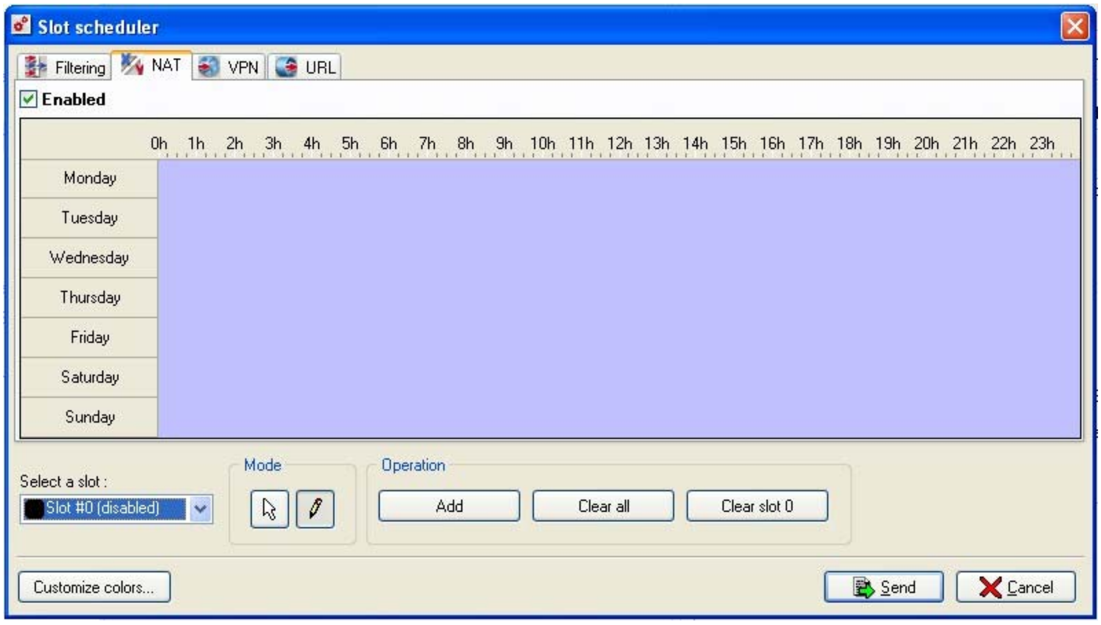


Figure 175: Slot scheduler - NAT

The slot scheduling window comprises three parts:

- Slot type selection tabs
- A timetable.
- Action buttons

Slots type selection tabs

Four slot types are available:

- **Filter**: Programs filter slots.
- **NAT**: Programs address translation slots.
- **VPN**: Programs VPN tunnel slots.
- **URL**: Programs URL filter slots.

Every one of these tabs will display an interface that allows adding, deleting or modifying a weekly slot scheduler per band and by using the mouse. The user can then define a time slot for a given policy.

Activating.Deactiving the slot scheduler

The slot scheduler can now be enabled or disabled using the checkbox **Enable** (located under the tabs). This is particularly useful if you intend to test your filter policies.

The timetable

This zone is structured like an “interactive” table. The horizontal scale represents the hours, and the vertical scale represents the days of the week. With the action buttons, you will be able to program the activation of these slots by selecting a time range with the mouse.

You will note that at all times, at least one filter slot has to be programmed. Therefore when you program the first filter slot, it is programmed for every hour, everyday.

Action buttons

Current slot	Selects a slot to be programmed.
↖	Selects a zone on the grid
✎	Modifies a zone on the grid
Add	Adds a schedule to a slot. The following window will appear:

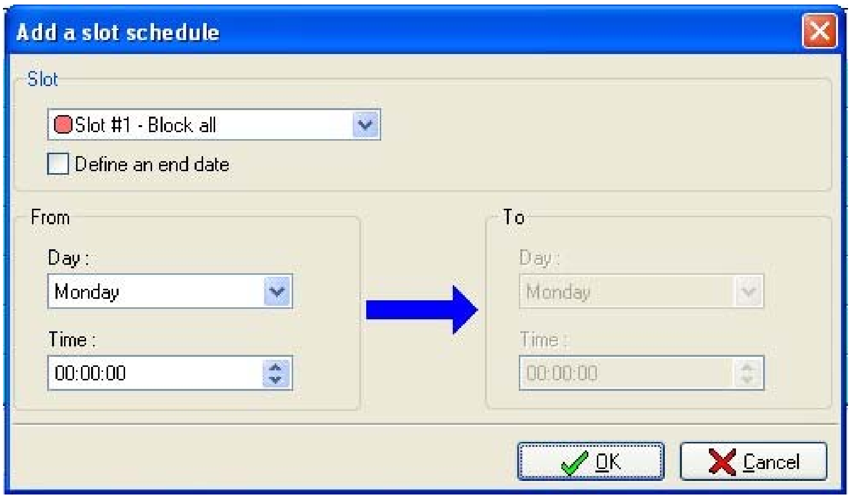


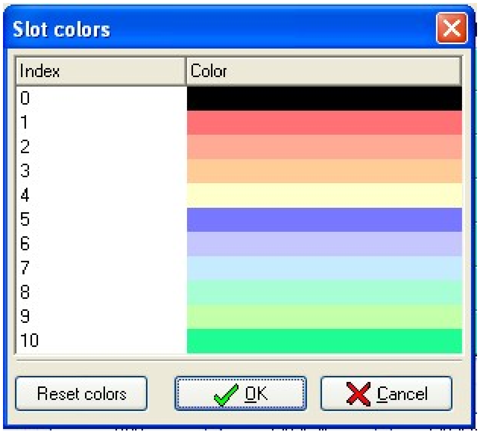
Figure 176: Adding a slot scheduler

After a slot has been selected, check the option **Define an end date** to determine an activation period (Date and time).

Clear All Deletes all the zones on the grid.

Clear a slot Deletes all the zones concerning a slot.

Colors Configures the colors associated to each slot. When you click on the button, the window below appears:



Slot colors

Index	Color
0	⬛
1	🟥
2	🟥
3	🟧
4	🟨
5	🟦
6	🟪
7	🟦
8	🟩
9	🟩
10	🟩

Figure 177: Slot colors

Send Clicking on this button will send the slot schedule to the configuration server and activate it.

7.3.2. Calendars

Calendars are used in various modules, especially user authentication.

Each user is associated to a calendar which allows him to authenticate with the Firewall when the filter policy established by the administrator requires it. This calendar may be specific to the user or several users. It defines the zones where the user has to authenticate and the zones to which the user has no access. Once the calendars have been defined, they may be selected when user authentication is configured. Access to the configuration of this calendar is via the `Calendars` menu in the NETASQ UNIFIED MANAGER menu directory. The following window appears:

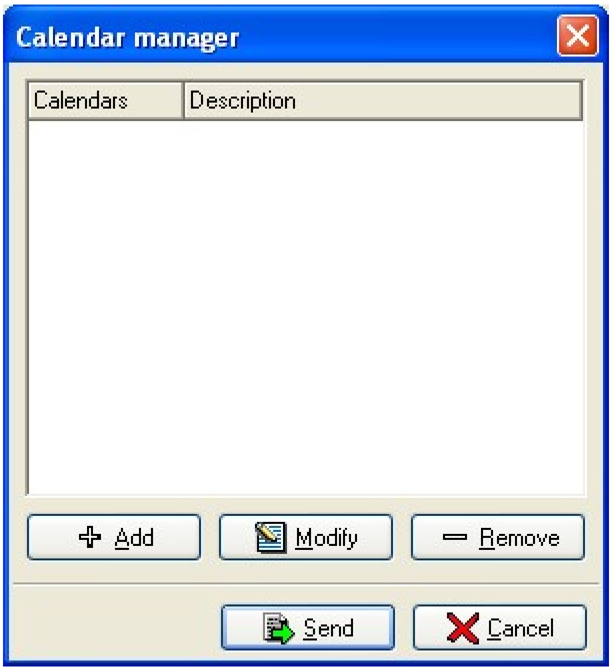


Figure 178: Calendar manager

The calendar selection window comprises three sections:

- A grid containing configured calendars,
- Action buttons allowing calendars to be added, modified or deleted,
- At the bottom of the window, buttons to confirm or cancel modifications made.

When you wish to add or modify a calendar, you have several ways of doing so:

➲ By selecting **Objects** in the NETASQ UNIFIED MANAGER menu directory, then double-clicking on a user. The window "Edit a user" will then appear. In the **`Authentication`** tab, select **`Calendar`** then **`Create a calendar`**.

➲ By selecting the **`Authentication\Captive portal`** menu in the NETASQ UNIFIED MANAGER menu director. In the menus **`Internal interfaces`** and **`External interfaces`**, select **Advanced**. Click on **`Calendar`** then select **`Create a calendar`**.

➲ By clicking on **Add** or **Modify** in the **`Calendars`** menu.

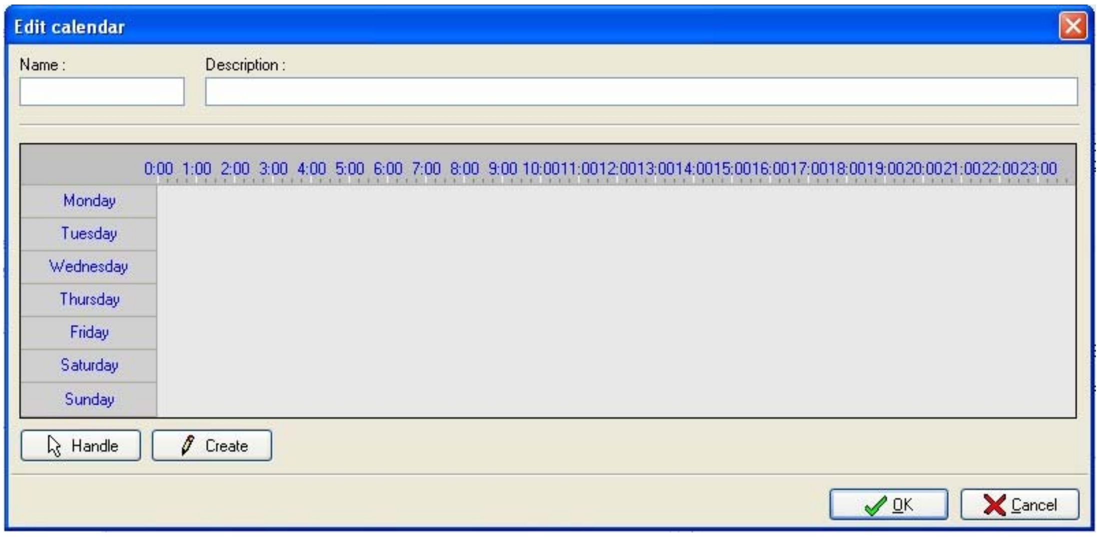


Figure 179: Editing the calendar

The calendar configuration window comprises three sections:

- The "Name" field: Name given to the calendar and "Description". The description of a calendar can be edited in the table, unlike the name.
- A timetable spanning a week.
- Action buttons that allow you to create time slots and to use them subsequently.

> **REMARK**
> Only a limited number of calendars can be created.

The timetable

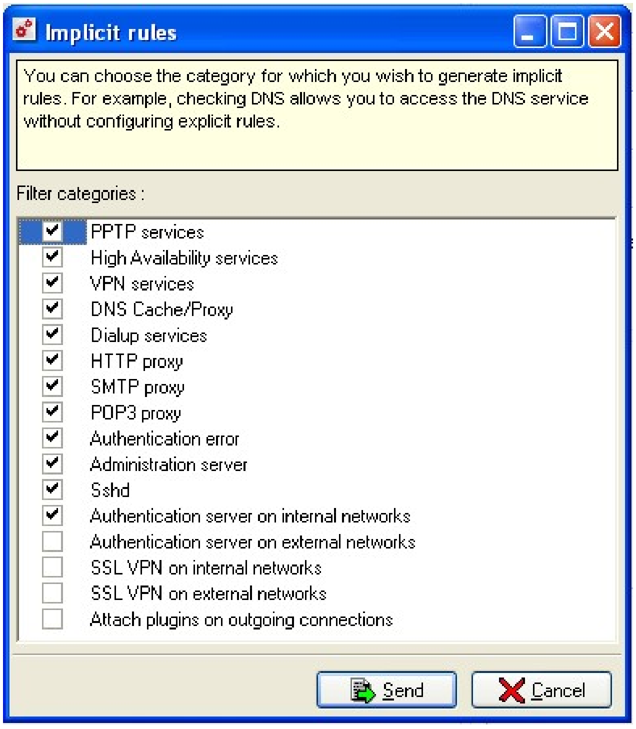
This zone is structured like an “interactive” table. The horizontal scale represents the hours, and the vertical scale represents the days of the week. With the action buttons, you will be able to program the time slots during which authentication is allowed by selecting a time range with the mouse. By clicking on these column and row “titles”, you will invert the current selection in the column or row in question. By clicking in the left upper corner of the table, you will invert the whole selection.

CHAPTER 4: IMPLICIT RULES

Implicit rules represent filter rules that are generated according to several parameters. They cannot be modified like filter rules.

➲ Go to the implicit rules via the **`Policy`** menu

The implicit rule configuration window appears:



Implicit rules

You can choose the category for which you wish to generate implicit rules. For example, checking DNS allows you to access the DNS service without configuring explicit rules.

Filter categories :

☑ PPTP services
☑ High Availability services
☑ VPN services
☑ DNS Cache/Proxy
☑ Dialup services
☑ HTTP proxy
☑ SMTP proxy
☑ POP3 proxy
☑ Authentication error
☑ Administration server
☑ Sshd
☑ Authentication server on internal networks
□ Authentication server on external networks
□ SSL VPN on internal networks
□ SSL VPN on external networks
□ Attach plugins on outgoing connections

Figure 180: Implicit rules

From this window, you will be able to automatically generate certain rules linked to the use of the Firewall's services. If you check a service, the Firewall will automatically create rules for the use of this service.

- **PPTP services**: for PPTP-secured tunnels.
- **High availability services**: for high availability.
- **VPN services**: for VPN tunnels.
- **DNS/Proxy cache**: for the DNS cache.
- **Dialup services**: for remote connections.
- **HTTP Proxy**: for the HTTP proxy.
- **SMTP Proxy**: for the SMTP proxy.
- **POP3 Proxy**: for the POP3 proxy.
- **Authentication error**
- **Administration server**: authorizes access with the graphical interface from a host located on the internal networks. This option creates an implicit rule at the Firewall level. If this option has been unselected, it would be necessary to create an explicit rule in the filter rules in order to authorize the connection to the Firewall via NETASQ UNIFIED MANAGER (service Firewall_srv, port 1300),.
- **Sshd**: allows access to the firewall in SSH in order to connect in command line.
- **Authentication server on internal networks**: allows access to the authentication service for internal network users. This service uses port 443 (https).
- **Authentication server on external networks**: allows access to the authentication service for external network users. This service uses port 443 (https).
- **SSL VPN on internal networks**: allows access to SSL VPN for internal network users ("protected" Ethernet and VLAN interfaces)
- **SSL VPN on external networks**: allows access to SSL VPN for external network users ("unprotected" Ethernet and VLAN interfaces and dialup interfaces).
- **Attach plugins on outgoing connections**: if this option is checked, the plugin corresponding to an outgoing connection will be automatically attached.

REMARK

When updating from version 6.3, the **SSL VPN on internal networks** and **SSL VPN on external networks** implicit ruled wil be deleted. Only the implicit rule for the authentication server will remain.

WARNING

If the user unselects the category "Administration server" that generates implicit rules allowing access to the firewall's administration server, a warning message will appear before the final validation.

CHAPTER 5: QUALITY OF SERVICE (QOS)

7.5.1. Presentation

7.5.1.1. What is Quality of Service (QoS)?

DEFINITION

Three factors have contributed to the development of Quality of Service on IP networks:

- As an increasing number of modern workstations now contains multimedia software, including video and audio codecs, a certain level of confidence is required for video performance (speed).

- The increasingly widespread development of IP multicast.

- The development of high-performance video and audio software programs that enable videoconferencing, for example.

Since such real-time applications cannot function fluidly on the internet given the latency times and packet losses often encountered on IP networks, it has become absolutely necessary to develop Quality of Service.

Quality of Service, which has a high level of abstraction, refers to the ability to provide a network service according to parameters defined in a Service Level Agreement (SLA). The “quality” of the service is therefore gauged by its availability, latency rate, fluctuations, throughput and rate of lost packets.

Where network resources are concerned, the “Quality of service” refers to a network element’s ability to provide traffic prioritization services and bandwidth and latency time control.

7.5.1.2. QoS on NETASQ Firewalls

ASQ’s **Stateful QoS** module enables efficient bandwidth management. A QoS policy can be associated with each filter rule when you select a packet ordering algorithm.

Two algorithms are currently available: **PRIQ** (Priority Queuing) and **CBQ** (Class-Based Queuing).

- **PRIQ** makes it possible to prioritize packets that are associated with a filter rule so that they will always be processed before the rest of the traffic;
- **CBQ** enables the treatment of packets according to bandwidth class. You can select an ordering class for each filter rule and associate a bandwidth guarantee and limit to it.

When using **CBQ** and **PRIQ** simultaneously, **PRIQ** traffic will be given priority over **CBQ** traffic.

7.5.2. Configuration

7.5.2.1. QoS configuration menu

➲ QoS can be configured using the `Policy\Quality of Service` menu in the NETASQ UNIFIED MANAGER menu directory, or when editing the filter policy by clicking on the **QoS** column in a filter rule. The window “QoS parameters of the filter rule” will appear.

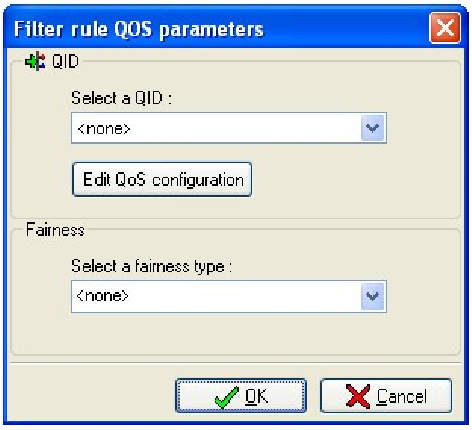


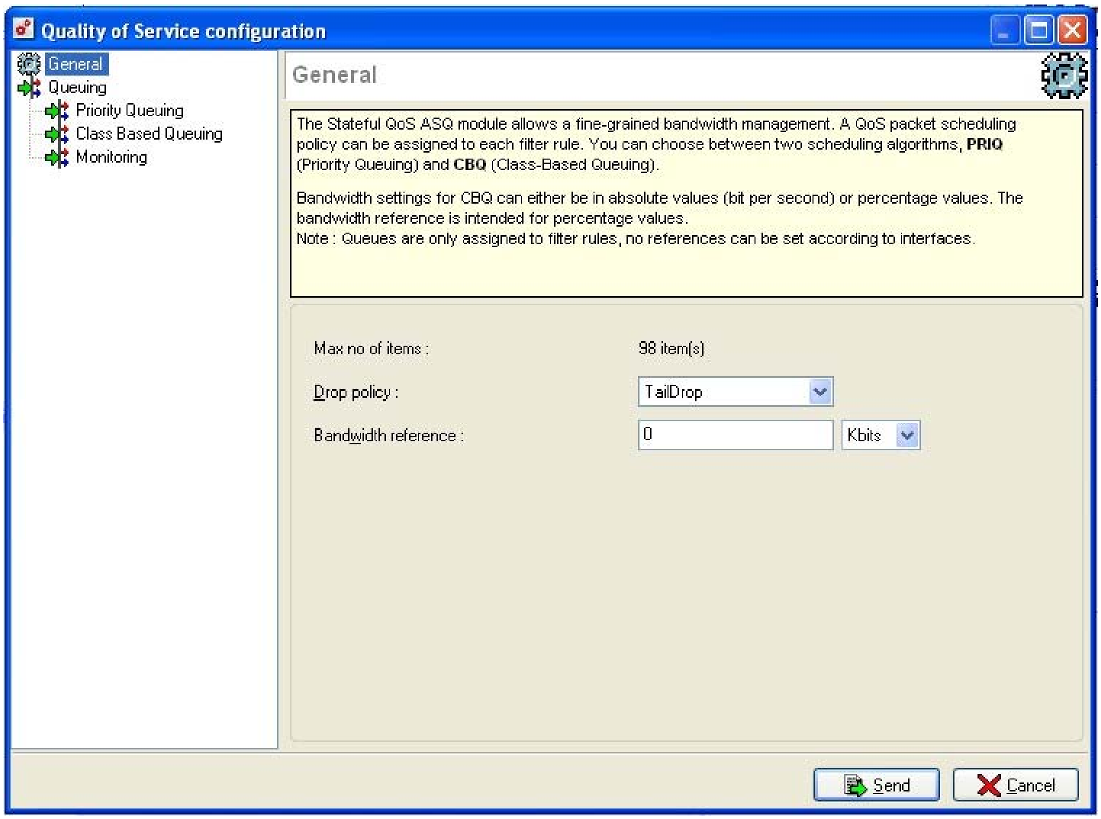
Figure 181: QoS parameters for the filter rule

Click on **Configure QoS.**

The QoS configuration menu comprises 2 parts:

- On the left, a directory of the various **QoS** features,
- On the right, the configurable options.

7.5.2.2. General



The Stateful QoS ASQ module allows a fine-grained bandwidth management. A QoS packet scheduling policy can be assigned to each filter rule. You can choose between two scheduling algorithms, **PRIQ** (Priority Queuing) and **CBQ** (Class-Based Queuing).

Bandwidth settings for CBQ can either be in absolute values (bit per second) or percentage values. The bandwidth reference is intended for percentage values.
Note : Queues are only assigned to filter rules, no references can be set according to interfaces.

Max no of items : 98 item(s)

Drop policy : TailDrop

Bandwidth reference : 0 Kbits

Figure 182: Configuring quality of service: General

The general configuration options are set out in the following table:

Max no. of elements	NETASQ UNIFIED MANAGER gives this number for information only, depending on the Firewall model (20 for U30 and U70 appliances, 100 for U120, U250 and U450, 200 for U1100 and U1500, 255 for U6000), indicating the number of queues that can be created.
Drop policy	This option enables the definition of the congestion management algorithm that will be used when the Firewall is no longer able to manage all the traffic it receives.
Bandwidth reference	The reference value in Kbits/s or Mbits/s enables indicating a reference which will be the basis of bandwidth limitations in percentage for queue configuration.

Drop policy

An important element of Quality of Service is the resolution of a major issue – the high rate of packet loss over the internet. When a packet is lost before it reaches its destination, the resources involved in its transmission will be wasted. In certain cases, this can even lead to severe congestion which may completely paralyze the systems.

At present, stability and real time for videoconferencing applications have not yet become a necessity, but proper control of congestion situations and good management of data queues are essential to the “Quality of Service”.

NETASQ Firewalls employ two algorithms for congestion management – **TailDrop** and **BLUE**. However, NETASQ recommends the use of BLUE.

<u>TailDrop</u>

The operating principle of this very basic algorithm is to delete packets that arrive on the queue when it is full.

<u>Blue</u>

This highly-powerful algorithm (whose performance far exceeds that of other algorithms) uses the history of lost packets and the rate of use for network interfaces to manage congestion.

The main principle of this algorithm is to define a unique probability (P) which will then be used to tag (via the traffic congestion option ECN) or drop packets from the data queue. The rate of queued packets getting lost increases this probability (P).

> **Example**
> In Buffer Overflows, the data queue continuously loses packets from the queue, and the probability (P) increases, thereby artificially increasing the number of tagged packets (by ECN) or the number of dropped packets. On the other hand, when the rate of use of the network interface is low or at zero, the probability (P) will then decrease.

This method results in the stabilization of network traffic, the reduction of the actual number of lost packets, maximized performance for each network interface and shortened packet latency time.

✪ These criteria are fundamental in a Service Level Agreement.

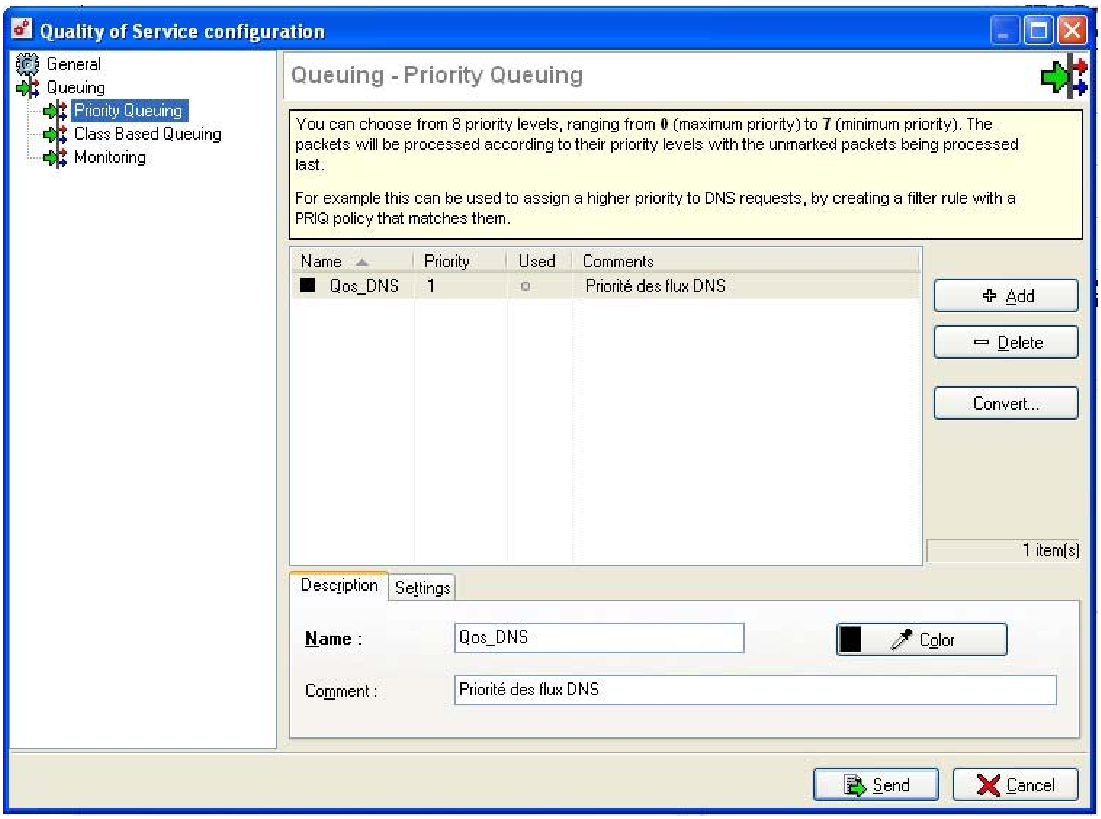
7.5.2.3. Queuing

The QoS module embedded in ASQ is associated with the filter module in order to provide Quality of Service functions. When a packet arrives on an interface, it will first be treated by a filter rule, then ASQ will assign the packet to the right queue according to the configuration of the filter rule's QoS field. Three types of queues are available on Firewalls, two of which are directly associated to the QoS algorithms mentioned above – PRIQ (Priority Queuing) and CBQ (Class-Based Queuing). The third enables traffic monitoring.

Priority Queuing

There are 8 priority levels and packets are treated according to the configured priorities.

High priority can be assigned to DNS queries by creating a filter rile and associating it with PRIQ.



You can choose from 8 priority levels, ranging from 0 (maximum priority) to 7 (minimum priority). The packets will be processed according to their priority levels with the unmarked packets being processed last.

For example this can be used to assign a higher priority to DNS requests, by creating a filter rule with a PRIQ policy that matches them.

Name	Priority	Used	Comments
■ Qos_DNS	1	○	Priorité des flux DNS

Name : Qos_DNS

Comment : Priorité des flux DNS

Figure 183: Configuring QoS – Priority queuing

Priority queuing gives certain packets priority during their treatment. This means that packets associated with a **PRIQ** filter rule will be treated before other packets.

The scale of priorities ranges from 0 to 7. Priority 0 corresponds to traffic with the highest priority among **PRIQ** queues. Priority 7 corresponds to traffic with the lowest priority among **PRIQ** queues. **CBQ** queues and traffic without QoS rules are associated with a “virtual” Priority 8 (cannot be configured) – these traffic flows will be treated after all **PRIQ** queues notwithstanding other rules.

Configuration options for PRIQ queues are as follows:

Add	The table in the **Priority Queuing** menu displays the configured queues. Add new queues with the **Add** button.
Delete	The table in the **Priority Queuing** menu displays the configured queues. Delete a selected queue using the **Delete** button.
Convert	The queue name and its comments are kept during the conversion of a **PRIQ** queue to another queue type.
xx element(s)	Global number indicating the number of **PRIQ** QoS rules that have been created. If the total number of QoS rules (**PRIQ**, **CBQ** and **Monitoring**) exceeds the Firewall’s maximum capacity as indicated in the **`General`** menu, a message will appear at the bottom left of the screen to inform the user that the maximum number of QoS rules has been exceeded.

Description tab

Name	Name of the queue to configure.
Comments	Associated comments.
Color	Color that will distinguish the queue.

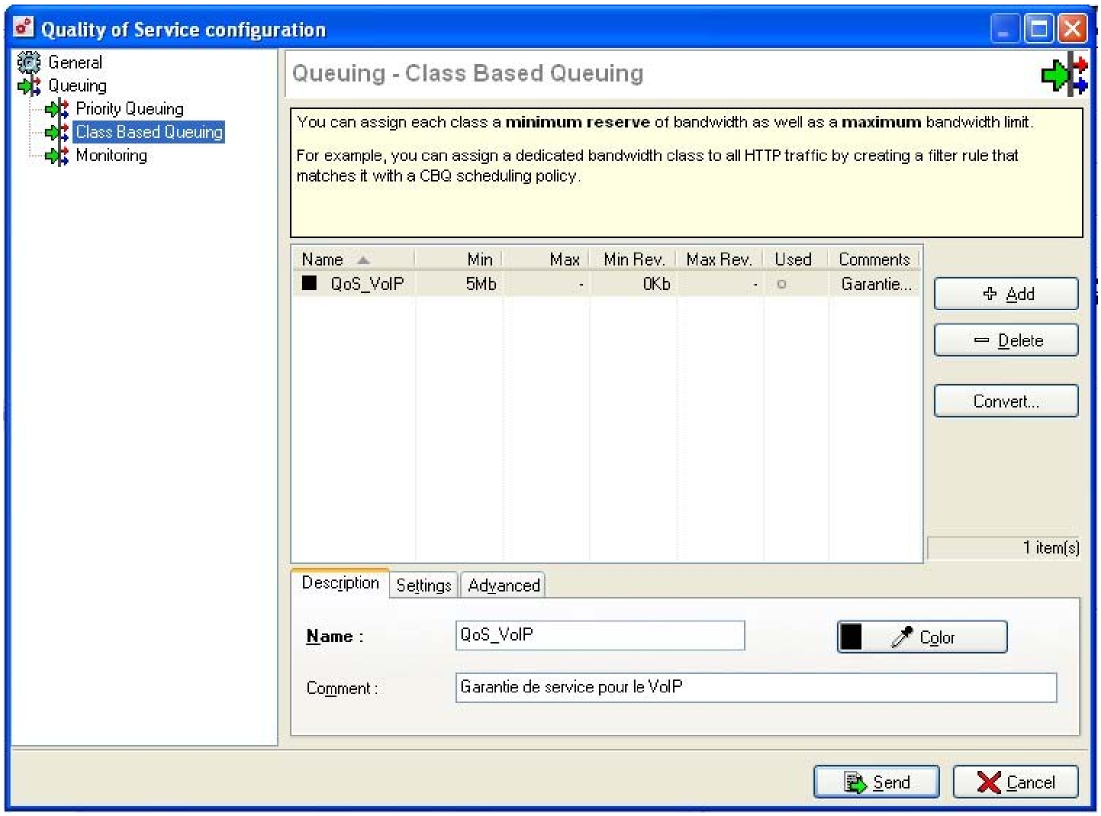
Configuration tab

Priority	Priority of the configured queue.

The table in the Priority Queuing menu displays all the configured queues. When these QoS rules are actually used in the definition of filter rules, a button ● appears in the list. Double-clicking on the button displays the list of filter rules in which this queue is used.

Class-Based Queuing

A sequencing class can be selected for each filter rule and a bandwidth guarantee and limit can be attributed to it.
For example; you can associate a sequencing class with HTTP traffic by assigning CBQ to the corresponding filter rule.



You can assign each class a **minimum reserve** of bandwidth as well as a **maximum** bandwidth limit.

For example, you can assign a dedicated bandwidth class to all HTTP traffic by creating a filter rule that matches it with a CBQ scheduling policy.

Name	Min	Max	Min Rev.	Max Rev.	Used	Comments
■ QoS_VoIP	5Mb	-	0Kb	-	○	Garantie...

1 item(s)

Name : QoS_VoIP

Comment : Garantie de service pour le VoIP

Figure 184: Configuring QoS – Class-based queuing - Description

Class-based queuing determines the way in which traffic affected by QoS rules will be managed on the network. Bandwidth reservation mechanisms for this queue type guarantee a minimum service while bandwidth limitation mechanisms enable the preservation of bandwidth when dealing with applications that consume a large amount of resources.

The different configuration options for CBQ are the same as for PRIQ.

Configuration tab

Maximum bandwidth allowed	This option acts as a limitation and prohibits exceeding the bandwidth for traffic affected by queues. It can be configured in Kbits/s, Mbits/s or as a percentage of the reference value, which is shared among all traffic affected by the QoS rule. Thus, if HTTP and FTP traffic is associated with a queue that has a maximum authorized bandwidth of 512Kbits/s, the combined bandwidth for HTTP + FTP traffic must not exceed 512Kbits/s.
Minimum bandwidth guaranteed	This option acts as a gurantee of service, and enables guaranteeing a certain throughput and maximum transfer time. It can be configured in Kbits/s, Mbits/s or as a percentage of the reference value, which is shared among all traffic affected by the QoS rule. Thus, if HTTP and FTP traffic is associated with a queue that has a minimum authorized bandwidth of 10Kbits/s, the combined bandwidth for HTTP + FTP traffic will be no less than 10Kbits/s. However, there is no restriction on the HTTP bandwidth being 9Kbits/s and the FTP bandwidth being only 1Kbits/s.
No limit on bandwidth	With this option, the maximum authorized throughput. In this case, the bandwidth value of the link affected by the QoS rule determines the maximum amount available.

The **Configuration** tab enables the definition of bandwidth reservation and limitation parameters for this queue. These parameters can be asymmetrically configured, meaning that parameters for reservation and limitation will be different depending on the direction of traffic.

By default, the **Configuration** tab defines bandwidth reservation and limitation values for both directions, but when the parameters are indicated in the **Advanced** tab (see below), the **Configuration** tab defines the parameters for traffic going in the direction of the filter rule definition, i.e., “Source” to “Destination”.

The table in the **Class-based Queuing** menu displays all the configured queues. When these QoS rules are actually used in the definition of filter rules, a button ● appears in the list. Double-clicking on the button displays the list of filter rules in which this queue is used.

Advanced tab

The **Advanced** tab enables the definition of bandwidth reservation and limitation parameters for traffic going in the opposite direction of the filter rule, ie, “Destination” to “Source”.

Maximum bandwidth allowed	This option acts as a limitation and prohibits exceeding the bandwidth for traffic affected by queues. It can be configured in Kbits/s, Mbits/s or as a percentage of the reference value, which is shared among all traffic affected by the QoS rule. Thus, if HTTP and FTP traffic is associated with a queue that has a maximum authorized bandwidth of 512Kbits/s, the combined bandwidth for HTTP + FTP traffic must not exceed 512Kbits/s.
Minimum bandwidth guaranteed	This option acts as a gurantee of service, and enables guaranteeing a certain throughput and maximum transfer time. It can be configured in Kbits/s, Mbits/s or

	as a percentage of the reference value, which is shared among all traffic affected by the QoS rule. Thus, if HTTP and FTP traffic is associated with a queue that has a minimum authorized bandwidth of 10Kbits/s, the combined bandwidth for HTTP + FTP traffic will be no less than 10Kbits/s. However, there is no restriction on the HTTP bandwidth being 9Kbits/s and the FTP bandwidth being only 1Kbits/s.
No limit on bandwidth	With this option, the maximum authorized throughput. In this case, the bandwidth value of the link affected by the QoS rule determines the maximum amount available.

The table in the **`Class-based Queuing`** menu displays all the configured queues. When these QoS rules are actually used in the definition of filter rules, a button ● appears in the list. Double-clicking on the button displays the list of filter rules in which this queue is used.

Monitoring

Monitoring queues do not affect the treatment of traffic affected by QoS rules. Throughput and bandwidth information can be saved and viewed in the **`Graph`** section of NETASQ REAL-TIME MONITOR.

Configuration options for Monitoring queues are as follows:

Add	The table in the **Monitoring** menu displays the configured queues. Add new queues with the **Add** button.
Delete	The table in the **Monitoring** menu displays the configured queues. Delete a selected queue using the **Delete** button.
Convert	The queue name and its comments are kept during the conversion of a **Monitoring** queue to another queue type.
xx element(s)	Global number indicating the number of **Monitoring** QoS rules that have been created. If the total number of QoS rules (**PRIQ**, **CBQ** and **Monitoring**) exceeds the Firewall's maximum capacity as indicated in the **`General`** menu, a message will appear at the bottom left of the screen to inform the user that the maximum number of QoS rules has been exceeded.

<u>Description tab</u>

Name	Name of the queue to configure.
Comments	Associated comments.
Color	Color that will distinguish the queue.

7.5.3. Using QoS

7.5.3.1. Activating a QoS queue

QoS rules which will be used in the treatment of particular traffic are defined during the configuration of filter policies. The QoS field can only be accessed if the advanced mode is activated in the definition of filter rules.

The procedure for activating a QoS queue is as follows:

1 Select the configuration menu **`Policy\Filters.`**

2 Edit the filter slot containing rules that have to be configured with QoS options.
3 Select **Advanced** mode.
4 Double-click on the **QoS** field in the rule to be modified, and the following window appears:

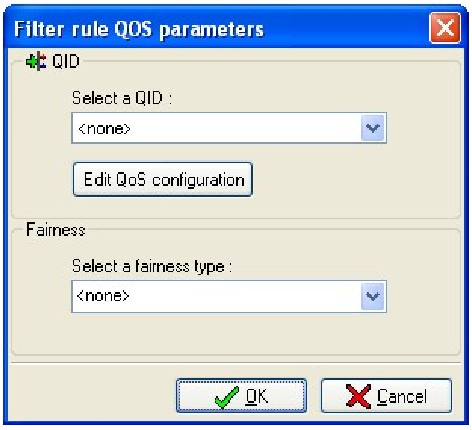


Figure 185: QoS parameters for the filter rule

5 Select a configured queue (or configure it first).
6 Select the level of fairness (if necessary – see below).
7 Click on **OK**, send the configured slot and activate the filter policy.

Fairness

> **WARNING**
> The “Fairness” option complicates the management of QoS, which has already been covered in this document. Make sure that you have fully understood the earlier aspects of configuring QoS before activating this option.

To each QoS queue, the “Fairness” option adds a packet weighting system that is peculiar to each queue. In this way, it is possible to modify the treatment mode of packets belonging to the same queue.

According to this mode, packets belonging to the same queue are treated:

- In order of arrival, on a FIFO (First In First Out) basis if NO fairness option has been specified.
- In a fair manner (equal) between each user’s packets on the queue if the fairness option has been set to **USER**;

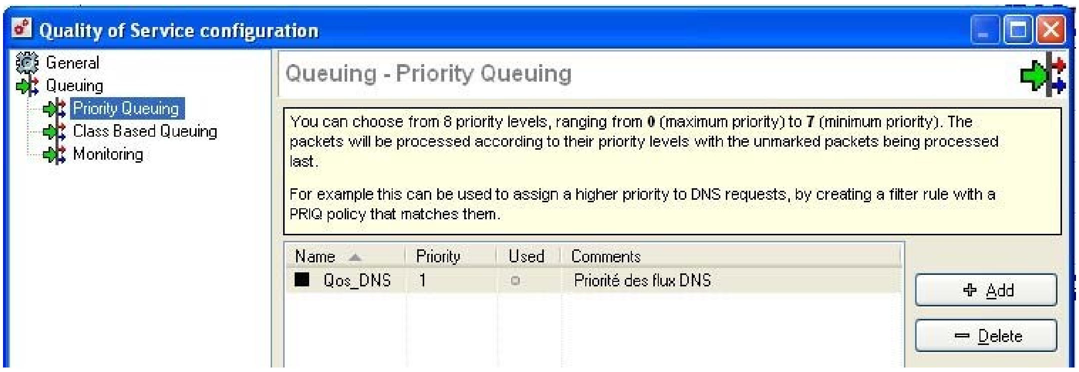
- In a fair manner (equal) between each host's packets on the queue if the fairness option has been set to **HOST**;
- In a fair manner (equal) between each connection's packets on the queue if the fairness option has been set to **CONNECTION**.

7.5.3.2. Examples of application and recommendations of use

Example 1: Prioritizing DNS traffic
DNS queries, based on UDP, lose a large number of packets due to the definition of UDP – which does not provide mechanisms for managing transmission errors – and the overwhelming presence of TCP traffic that drowns out UDP traffic in the mass of TCP packets.

To preserve such traffic, and in particular DNS traffic, the creation of a PRIQ QoS rule is recommended. This rule will help to diminish frequent packet loss, as well as latency that may occur on this type of traffic, which requires high responsiveness (this is the precise reason for DNS queries being done on UDP).

Defining the QoS rule for DNS



Queuing - Priority Queuing

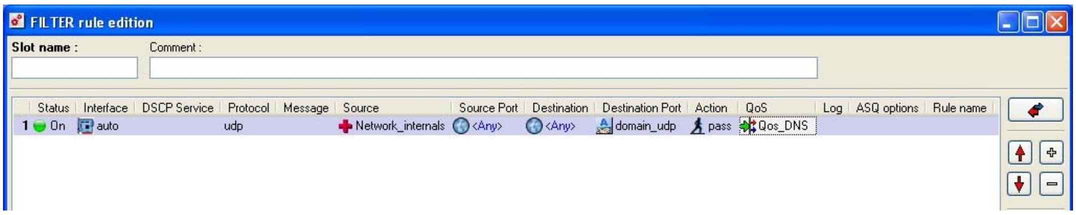
You can choose from 8 priority levels, ranging from **0** (maximum priority) to **7** (minimum priority). The packets will be processed according to their priority levels with the unmarked packets being processed last.

For example this can be used to assign a higher priority to DNS requests, by creating a filter rule with a PRIQ policy that matches them.

Name	Priority	Used	Comments
■ Qos_DNS	1	○	Priorité des flux DNS

Figure 186: Configuring QoS – Priority queuing

Using the QoS rule in the filter policy



Slot name :
Comment :

	Status	Interface	DSCP Service	Protocol	Message	Source	Source Port	Destination	Destination Port	Action	QoS	Log	ASQ options	Rule name
1	On	auto		udp		Network_internals	<Any>	<Any>	domain_udp	pass	Qos_DNS			

Figure 187: QoS in the filter policy

Effects on the traffic

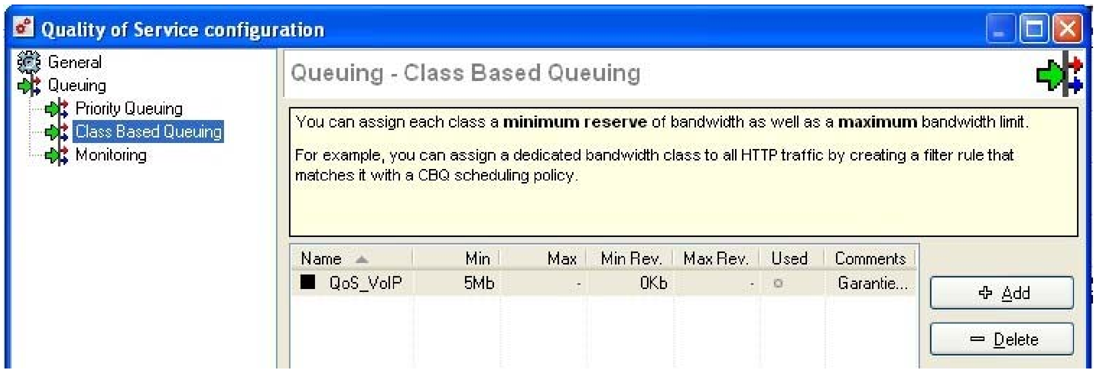
- Decreases the number of lost packets .
- Reduces latency .

Example 2: Limitation of http traffic

HTTP traffic consumes more bandwidth from the internet link and local network than any other type of internet traffic. Heavy use of the internet may cause congestion of network traffic and decrease in overall performance, making it bothersome to use the network.

Fortunately, the situation can be remedied. We recommended **limiting HTTP traffic using a CBQ QoS rule that defines the maximum throughput allowed**. This rule will allow preserving the network's bandwidth and reducing the impact of using the internet on the network's overall performance.

Defining the QoS rul for HTTP



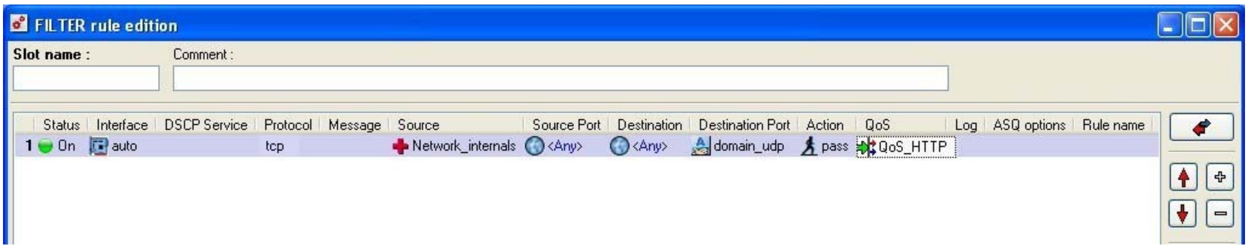
You can assign each class a **minimum reserve** of bandwidth as well as a **maximum** bandwidth limit.

For example, you can assign a dedicated bandwidth class to all HTTP traffic by creating a filter rule that matches it with a CBQ scheduling policy.

Name	Min	Max	Min Rev.	Max Rev.	Used	Comments
■ QoS_VoIP	5Mb	-	0Kb	-	○	Garantie...

Figure 188: QoS for HTTP

Using the QoS rule in the filter policy



Slot name :

Comment :

	Status	Interface	DSCP Service	Protocol	Message	Source	Source Port	Destination	Destination Port	Action	QoS	Log	ASQ options	Rule name
1	On	auto		tcp		Network_internals	<Any>	<Any>	domain_udp	pass	QoS_HTTP			

Figure 189: QoS rule in the fitler policy

Effects on traffic

- Lowers the risk of network congestion
- Reduces the impact of traffic on the network's overall performance.

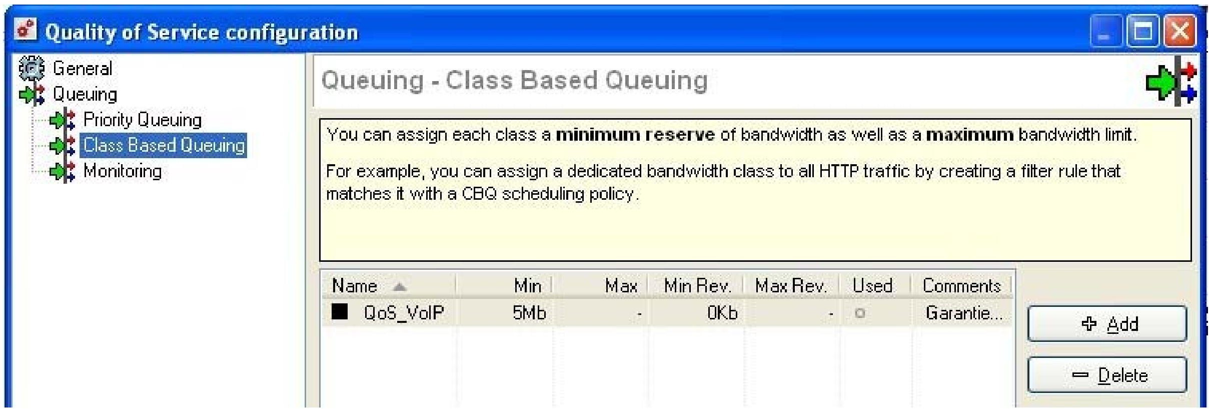
Example 3: Guarantee of a minimum service

Some applications (e.g. VoIP) require a level of service with the guarantee of compliance. Failure to comply would result in the suspension of the service (e.g. VoIP conversations can no longer be held).

Other applications and their impact on the network's general performance may disrupt the progress of obtaining the required service level.

To ensure the maintenance of the required service level, we recommend that you create a CBQ QoQ rule that defines a minimum guaranteed throughput. It will guarantee a service level for specified traffic irrespective of the impact of other traffic on the network's overall performance and without defining the bandwidth limitation for the other types of traffic.

Definiting the QoS rule for VoIP



Queuing - Class Based Queuing

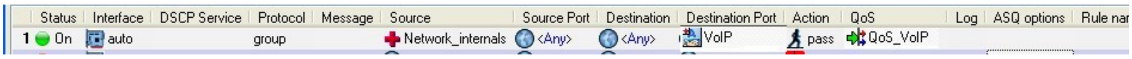
You can assign each class a **minimum reserve** of bandwidth as well as a **maximum** bandwidth limit.

For example, you can assign a dedicated bandwidth class to all HTTP traffic by creating a filter rule that matches it with a CBQ scheduling policy.

Name	Min	Max	Min Rev.	Max Rev.	Used	Comments
■ QoS_VoIP	5Mb	-	0Kb	-	○	Garantie...

Figure 190: QoS rule for VoIP

Using the Qos rule in the filter policy



	Status	Interface	DSCP Service	Protocol	Message	Source	Source Port	Destination	Destination Port	Action	QoS	Log	ASQ options	Rule nar
1	● On	auto		group		Network_internals	<Any>	<Any>	VoIP	pass	QoS_VoIP			

Figure 191: QoS in the filter policy

Effects on the traffic

- Guarantees a level of service for a specified traffic type.
- Introduces a maximum data trasfer time for the service.

PART 8: VPN

CHAPTER 1. PRESENTATION

8.1.1. What is a VPN?

DEFINITION

VPNs, for Virtual Private Networks, enable the safe transmission of sensitive data through an insecure medium, which the internet happens to be most of the time. Encryption and authentication mechanisms ensure this safe transmission throughout the entire communication between what is known as “VPN peers”.

8.1.2. Embedded VPN technologies on the Firewall

NETASQ Firewalls use three technologies to provide its VPN features, each corresponding to a specific method of using VPN:

- **IPSec Tunnels**: a standard protocol, IPSec enables the creation of VPN tunnels between a firewall and another firewall or between a firewall and mobile workstations on which VPN clients would be installed.
- **PPTP**: a Microsoft proprietary protocol, this allows creating VPN tunnels between the Firewall and mobile workstations on which a built-in PPTP client runs.
- **VPN SSL**: with this technology, it is possible to create VPN tunnels between the Firewall and mobile workstations or even the firewall and internal workstations (for example, to secure web servers or e-mail communications).. However, unlike the two technologies mentioned previously, SSL allows creating VPN tunnels without the need to install a VPN client on the mobile workstation.

8.1.2.1. Layout of the VPN section

To help you better understand VPN features and their associated technologies, the section on VPN has been separated into four parts (although the section on IPSec is the most important), each of which contain an introduction to the associated technology, its configuration on the Firewall and lastly, configuration examples.

CHAPTER 2: PRE-SHARED KEYS

8.2.1. Introduction

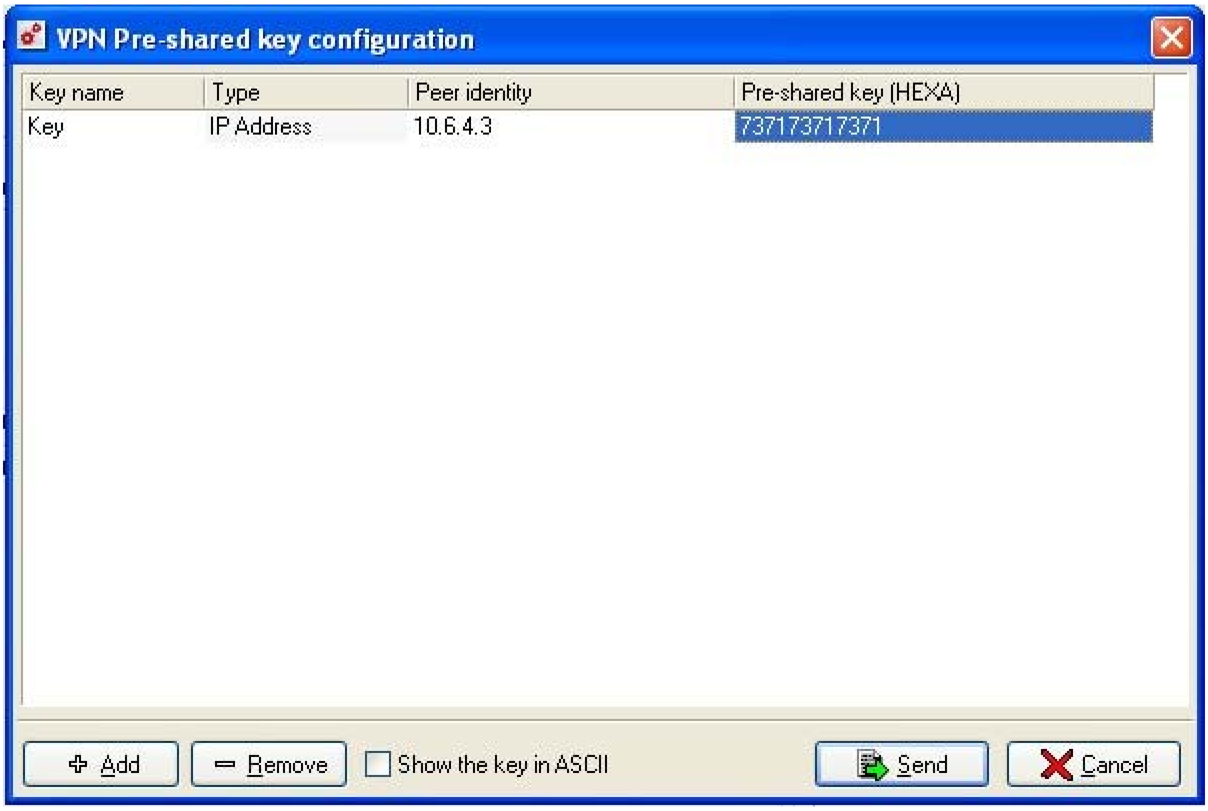
The configuration of pre-shared keys enables defining the secret exchanged earlier between both peers of the VPN tunnel. Each pre-shared key is defined according to a remote VPN peer and is MANDATORY for dynamic IPSec VPN tunnels using pre-shared keys.

> **REMARK**
> Pre-shared keys for mobile clients can also be indicated directly in user LDAP forms (see the section Object configuration > users). (*Cf.* *Part 4/Chapter 3: Objects\Users*). In this case, each user will have his own pre-shared key to authenticate with the Firewall when accessing remotely via VPN.

8.2.2. Presentation of the interface

Pre-shared keys have to be configured.

➲ This can be done using either the **`VPN\Pre-shared keys`** menu or the **`PSK Configuration`** button in the general IPSec VPN configuration menu.



VPN Pre-shared key configuration

Key name	Type	Peer identity	Pre-shared key (HEXA)
Key	IP Address	10.6.4.3	737173717371

Figure 192: Configuring pre-shared keys

Key name	Unique name in the form of a character string that you assign to the key. Valid for internal firewall use and for the management of the user's keys.
Type	Remote host's identifier type. The different possibilities are:

	◦ **Inambiguous domain name**: host's domain name (e.g.: firewall.netasq.com) ◦ **user@Fqdn** (e-mail): host's name on a domain. ◦ **IP address**: the remote host is identified by its IP address No link is created with any domain, the identifier just has to be the same on the remote host.
Peer identity	Remote host's identifier according to the type selected beforehand.
Pre-shared key (HEXA)	The value of the key in hexadecimal by default.

An unlimited number of pre-shared keys can be created.

However, when a pre-shared key belonging to an IPSec VPN tunnel is deleted, this tunnel will no longer function.

> **WARNING**
> In main mode, the IP address is the only identity available for this tunnel.

The keys are not related to any host (except with an IP address type identity) and can be used by several users concurrently.

*Several hosts may share the same IP address (behind a NAT for example). C*f.* *Part 8/Chapter 3: Application of the feature*.

CHAPTER 3: IPSEC TUNNELS

8.3.1. Introduction

8.3.1.1. Main characteristics of IPSec

> **DEFINITION**
> The term "IPSEC" (IP Security) refers to a set of security mechanisms designed to guarantee high quality security for IP traffic (IPv4, IPv6), based on cryptography and without interoperability issues. Services that IPSEC proposes range from access monitoring, to integrity in unconnected mode, authentication of data sources, protection against replay, confidentiality in encryption and on traffic flows. These services are available in IP or in other protocols in higher layers. As such, IPSEC is independent of technologies in the data link layer (ATM, Frame Relay, Ethernet, etc).

IPSec VPN allows establishing a secure tunnel (peer authentication, encryption and/or verification of data integrity) between two hosts, between a host and a network, or between two networks by using security associations (SAs) and the IPSec security policy (SPD) via the kernel.

A modified version of FAST_IPSec supplies the IPSec VPN module, corresponding to the native FreeBSD IPSec module (http://www.freebsd.org). It provides in particular good support of cryptographic hardware modules

The VPN module has to provide the following features from its configuration file.

- Setup of security policies which indicate the traffic types that can or should be encrypted.
- Encryption and/or authentication of the incoming traffic concerned.
- Decryption and/or authentication of the incoming traffic concerned.
- Request for negotiation from the Security association when necessary via the ISAKMP protocol.

IPSEC uses two protocols to ensure traffic security: "Authentication Header" (AH) and "Encapsulating Security Payload" (ESP). These protocols have also been designed to be independent of any algorithm. This modularity enables the selection of different algorithm types without affecting the implementation.

> **Example**
> Different user communities can select (or even create) different algorithm types if necessary.

Each of the protocols mentioned above support two modes of use: transport mode and tunnel mode. In transport mode, IPSec protects the

IPSec protects the contents of the IP packet. In tunnel mode, the IP packet will be completely encapsulated in a new packet.

Based on cryptography, a certain number of communication parameters have to be negotiated beforehand during the exchange of information. This context (encryption algorithms, keys, selected mechanisms…) is brought together within an SA (Security Association). The SA concept is part and parcel of IPSEC.

As the native IPSEC does not support address translation, IPSEC does not allow establishing a VPN tunnel if at least one of the tunnel endpoints has a translated address. (See *Part 8/Chapter 3: Support for the NAT-T feature*).

8.3.1.2. Two protocols for traffic security

Authentication Header (AH)

The Authentication Header (AH) was designed to ensure integrity in unconnected mode, authentication of data sources and an optional anti-replay service. The principle of AH is to add an additional field to the standard IP datagram. This enables the peer to verify the authenticity of data contained in the datagram upon its reception.

Encapsulating Security Payload (ESP)

The ESP (Encapsulating Security Payload) protocol was designed to ensure data confidentiality, but it is also capable of providing integrity services in unconnected mode, as well as data source authentication services and an optional anti-replay service. ESP's principle is to decrypt (and where necessary, to ensure the integrity of) data – including the IP header of the source packet if in tunnel mode.

WARNING
The NETASQ firewall supports only the ESP protocol in tunnel mode.

8.3.1.3. Usage modes

For each IPSEC security mechanism, there are two modes – transport and tunnel modes.

In transport mode, only data originating from the higher-level protocol and transported by the IP datagram are protected. This mode can only be used on terminal equipment.

In tunnel mode, the IP header is also protected (authentication, integrity and/or confidentiality), and the whole packet is encapsulated in a new IP packet (therefore, with a new IP header). This new header is used for transporting the packet up to the end of the tunnel, where the original header will be reestablished.

Tunnel mode can be used either on terminal equipment or at the security gateway level. This mode enables providing higher protection against traffic analysis.

The following examples show the differences between both usage modes in the case of ESP.

WARNING
The NETASQ firewall only supports the ESP protocol in tunnel mode.

ESP "transport mode"

End-to-end protection (source and destination addresses not modified).

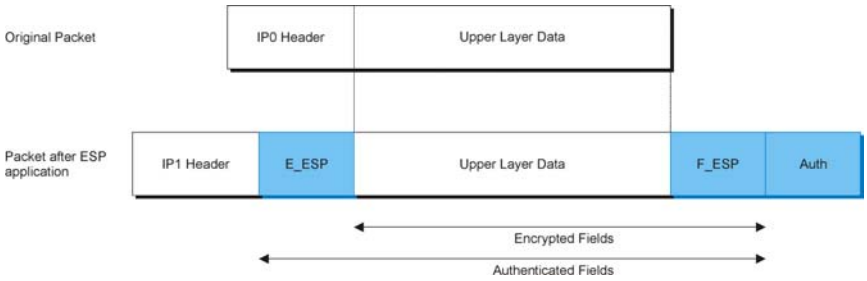


Figure 193: ESP transport mode

ESP "tunnel mode"

Used for protecting traffic between two intervening elements.

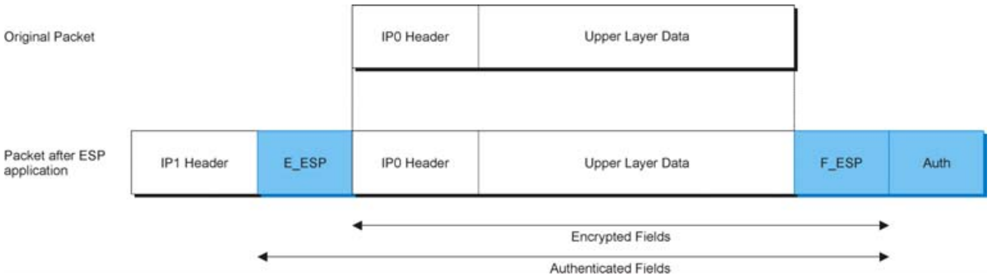


Figure 194: ESP tunnel mode

8.3.1.4. NETASQ’s choice

As indicated above, a NETASQ firewall’s encryption functions only implement the IPSEC ESP protocol to provide authentication and encryption services for datagrams exchanged with VPN peers (which may be another Firewall) possessing corresponding features.

Moreover, NETASQ firewalls make use of the ESP protocol only in tunnel mode. This means that encryption functions cannot be used from end to end but only on a section of the network which supports the traffic physically defined by the VPN peers, typically the untrusted network. On this section, the IP datagrams to protect are fully encrypted, signed and encapsulated in ESP datagrams whose source and destination IP addresses are those of the VPN peers. Thus attackers who eavesdrop on an untrusted network cannot access the IP addresses of real hosts at the endpoints of the data flow. VPN peers are called “tunnel endpoints”, as opposed to real hosts at the endpoints of the data flow, which are located “behind” the VPN peers from the standpoint of an untrusted network, and which are called “traffic extremities”.

The fact that the ESP protocol is favored in tunnel mode is based on two observations.

Schematically, the transport mode can be associated with a “host to host” usage, meaning end-to-end traffic, from a single host to another single host, whereas the tunnel mode is used rather in a “network to network” context, which is to say a host group to another host group. This latter configuration corresponds more to the architecture type encountered when using a firewall, since Firewalls are generally used for protecting networks, therefore NETASQ favors the tunnel mode.

It can also be conceived to a certain extent that the transport mode is in reality a way of using the tunnel mode (tunnel and traffic endpoints are confused). However, this case is not supported on a NETASQ firewall.

Given that NETASQ has opted to implement only the tunnel mode on its Firewalls, developments on **AH (Authentication Header)** have been interrupted. In fact, in tunnel mode, only three types of “sensitive” information would need authentication: source and destination addresses and the security index (SPI: Security Policy Identifier) of the associated SA (Security Association). Now, for the VPN policy to function, these information types are indispensable. Modifying one of these parameters will cause the peer to irreparable reject the packet, therefore using AH in the context of the tunnel mode becomes unnecessary in comparison with ESP.

8.3.1.5. Different phases

In ESP (AH as well, but only ESP matters to us in the context of the Firewall), each datagram exchanged between two given VPN peers is linked to a simplex or unidirectional connection (depending on the point of view, it is either incoming or outgoing) and implements security services, called IPSEC SA (Security Association). An IPSEC SA specifies the encryption and authentication algorithms to be applied on the datagrams it covers, as well as the associated secret keys.

Widespread use and deployment of IPSEC requires a standard SA management protocol on the internet, extensible and automated. The automated key management protocol chosen for IPSEC is IKE by default. IKE is organized around 2 negotiation phases.

Phase 1 of the IKE protocol aims to establish an encrypted and authenticated communication channel between both VPN peers. This “channel” is called ISAKMP SA (different from IPSEC SA). Two negotiation modes are possible – main mode and aggressive mode.

Phase 2 of the IKE protocol negotiates parameters of future IPSec SAs (one incoming and one outgoing) securely (through an ISAKMP SA communication channel negotiated in the first phase).

Phase 1 of the IKE protocol

Phase 1 of the **IKE** protocol works towards three objectives:

- Negotiation of ISAKMP SA parameters (one incoming and one outgoing),
- Elaboration of secret keys for authentication, encryption and derivation of the ISAKMP SA.
- Mutual authentication of VPN peers.

In a NETASQ firewall, SA establishment functions accept ISAKMP SA negotiations only with VPN peers for which a tunnel has been defined in the current encryption slot, on the network interface specified for this tunnel.

The following diagram represents the negotiation stages in main mode using an x509 certificate.

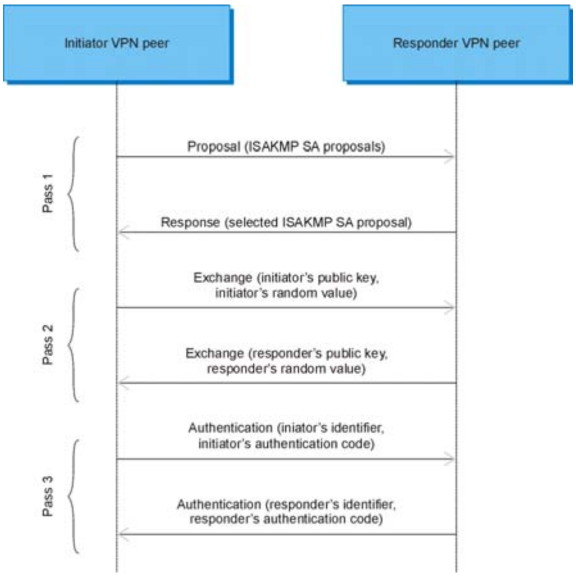

Initiator VPN peer
Responder VPN peer
Pass 1
Proposal (ISAKMP SA proposals)
Response (selected ISAKMP SA proposal)
Pass 2
Exchange (initiator's public key, initiator's random value)
Exchange (responder's public key, responder's random value)
Pass 3
Authentication (iniator's identifier, initiator's authentication code)
Authentication (responder's identifier, responder's authentication code)

Figure 195: Negotiation in main mode

Pass 1 corresponds to the negotiation of the ISAKMP SA. Each encryption rule possesses a list of ISAKMP SA proposals which are quintuples of the form (SA lifetime, authentication algorithm, authentication key size, encryption algorithm, encryption key size).

Pass 2 enables elaborating a shared secret, from which the ISAKMP SA's authentication secret key and encryption secret key are derived, which services negotiated in Pass 1 can use.

Pass 3, protected by authentication and encryption services, enable the mutual authentication of VPN peers. The authentication code for each VPN peer is generated from the pre-shared key, from the shared secret, random values and the VPN peer's identifier.

The Firewall supports other negotiation modes and authentication methods – aggressive or main modes and authentication by ^re-shared keys or by X509 certificates.

Aggressive mode

The aggressive mode takes place in three stages:

1 **Stage 1**
This stage combines the proposal, initiator key exchange and sending of the initiator's identification

2 **Stage 2**
This stage combines the response, responder key exchange and authentication of the responder.

3 **Stage 3**
For the initiator, this stage consists of sending his authentication code.

Phase 2 of the IKE protocol

Establishing a pair of IPSEC SAs between two VPN peers requires a parameter negotiation phase and key establishment in order to ensure that both tunnel endpoints apply the encryption rule associated to the IPSEC SA coherently. Negotiation of IPSEC SAs is based on Phase 2 (quick mode) of the IKE protocol. To keep things simple, the stages of this negotiation can be represented by the following sequence diagram.

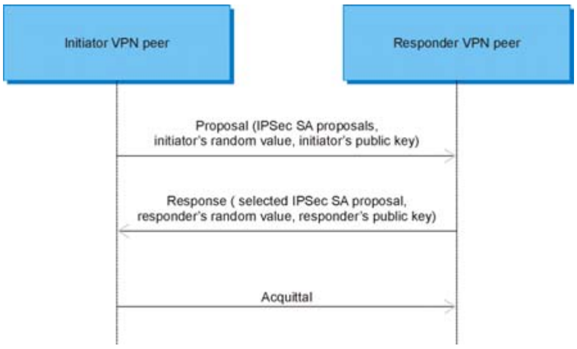

Initiator VPN peer
Responder VPN peer
Proposal (IPSec SA proposals, initiator's random value, initiator's public key)
Response (selected IPSec SA proposal, responder's random value, responder's public key)
Acquittal

Figure 196: Negotiation - Phase 2

All exchanges are encrypted and authenticated by services which the ISAKMP SA provides, negotiated and established between VPN peers before establishing the IPSEC SAs associated to the encryption rules.

Each encryption rule possesses a list of IPSEC SA proposals which are quintuples of the same form as for ISAKMP SA negotiation.

During the second stage of Phase 2 of the IKE protocol, the responder has to choose and recopy into his response one of the proposals submitted to him, otherwise the initiator will reject the negotiation. As a responder, the NETASQ firewall applies the following rules to select the response:

- The response selected is the first to correspond to the negotiation strategy specified at the tunnel level,
- The negotiation strategy may be “Exact”, “Strict”. "Claim" or "Obey". In an exact strategy, a proposal from the initiator will correspond to a local proposal if the local proposal is equal to it. In a strict strategy, a proposal from the initiator will correspond to a local proposal if the initiator’s proposal is equal to or greater than the local proposal. For a “Claim” strategy, a proposal from the initiator will correspond to a local proposal if it is equal to or more than it. However, if the lifetime is shorter, it is possible to impose a customized lifetime via a specific message). As for the “Obeyt” strategy, the peer’s first proposal will be accepted.

A proposal from the initiator is equal to or greater than a local proposal if conditions in the table below are met:

Attributes in initiator’s proposal	Relationship	Attributes in local proposal
Lifetime	≤	Lifetime
Authentication algorithm	=	Authentication algorithm
Authentication key size	≥	Authentication key size
Encryption algorithm	=	Encryption algorithm
Encryption key size	≥	Encryption key size
Perfect Forward Secrecy	≥	Perfect Forward Secrecy

In a strict strategy, attributes from an SA may turn out to be different from those in local proposals associated to the encryption rule which uses the SA.

After a successful negotiation, the authentication and encryption keys are elaborated from public keys (Diffie-Hellman shared key), random vales and other parameters exchanged during Phase 2, as well as a derived secret key elaborated during Phase 1 unless the PFS has been enabled. In this case, a shared secret will be generated via Diffie Hellman.

8.3.1.6. X509 certificates

The NETASQ firewall solution supports and uses two authentication methods: pre-shared keys and X509 certificates. Both methods have the same security level but they are managed differently. This distinction is expanded upon in the section on configuring VPN policies (refer to “Creating a VPN tunnel”).

This section focuses on the authentication of VPN peers by certificate.

It does not aim to provide a full or exhaustive explanation of public key infrastructures, but to explain ISAKMP configuration by certificates in a NETASQ firewall.

Generating certificates

A NETASQ firewall contains an internal public key infrastructure which enables creating certificates for users in your information system, but it can also integrate files generated by a private external PKI

> **Examples**
> openSSL, iPlanet CMS, Baltimore, etc) or an official external PKI (e.g. Thawte, Verisign, etc

The procedure to follow in order to generate external certificates takes place according to the formalities described in the editors' manuals for the private PKI solution or on the websites of official CAs.

The steps for generating a local certificate and the configuration of a firewall are as follows:

- Generation of a pair of keys (also called bi-key).
- Importation of the private key into the Firewall.
- Sending of certificate requests (accompanied by the public key) to the CA.
- Retrieval of the certificate from the CA after its validation.
- Importation of the certificate into the Firewall
- Retrieval and importation of the certificate from the CA
- Retrieval and importation of peer certificates

Therefore, to configure the Firewall, it is necessary to import different files (three categories of certificates, private keys and revocation list). Each file contains one of the elements cited below:

Private key

From the pair of keys generated by the PKI, the Firewall must possess the private and public copy. The Firewall does not generate the pair of keys itself; the PKI does it.

The private key allows the information sent to be signed.

The administrator generates this key at the same time as the public key with a view to generating the certificate for the local Firewall.

Local Firewall certificate

It is generated for the local Firewall. The public key which it contains allows authentication with peer Firewalls.

The administrator for the local Firewall generates these certificates.

Peer certificates

These certificates are generated by remote Firewalls. The public key which it contains allows the authentication of peer Firewalls.

The administrator of remote Firewalls provides these certificates.

CA certificates

They are generated by the **CA**. The public key that they contain allow verifying the validity of certificates from remote Firewalls (peer certificates) and those of the local Firewall.

These certificates are most often retrievable, whether in the private PKI application or on the site of the official CA.

Revocation list

Each certificate may be cancelled (revoked) when the person in charge (administrators, heads of services or company heads, whichever the case may be) decides that a certain certificate does not protect anymore or jeopardizes the security of the company's transactions. In fact, certificates are capable of creating shortfalls in security in different scenarios, such as the loss or theft of the private key, the departure of the Firewall administrator or possession by persons who are no longer allowed to access the system... PKIs allow the revocation of certificates, the generation, exportation and publication of lists containing revoked certificates. This list must be updated manually and periodically in the Firewall, otherwise certain persons or resources would be able to retain accesses to which they are no longer entitled.

Formats recognized by NETASQ Firewalls

- **PEM** (Privacy Enhanced Mail). It allows encoding X509 certificates in 64 base,
- **DER**, binary format.
- **PKCS#12**.

For example, a PEM-type certificate may look like this:

```
-----BEGIN CERTIFICATE-----
MIIDdzCCAuCgAwIBAgIBBzANBgkqhkiG9w0BAQQFADCBpDELMAkGA1UEBhMCQ0gxCzAJBgNVBAgTAkdFMQ8wDQYD
VQQHEwZHZW5ldmExHTAbBgNVBAoTFFVuaXZlcnNpdHkgb2YgR2VuZXZhMSQwIgYDVQQLExtVTklHRSBDZXJ0aWZpY
2F0ZSBBdXRob3JpdHkxETAPBgNVBAMTCFVuaUdlIENBMR8wHQYJKoZIhvcNAQkBFhB1bmlnZWNhQHVuaWdlLmNoMB
4XDTk5MTAwNDE2MjI1N1oXDTAwMTAwMzE2MjI1N1owgbExCzAJBgNVBAYTAkNIMQswCQYDVQQIEwJHRTEPMA0GA1
UEBxMGR2VuZXZhMR0wGwYDVQQKExRVbml2ZXJzaXR5IG9mIEdlbmV2YTEeMBwGA1UECxMVRGl2aXNpb24gSW5mb
3JtYXRpcXVlMRowGAYDVQQDExFBbGFpbiBIdWdlbnRvYmxlcjEpMCcGCSqGSIb3DQEJARYaQWxhaW4uSHVnZW50b2J
sZXJAdW5pZ2UuY2gwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBALIL5oX/FR9ioQHM0aXxfDELkhPKkw8jc6I7BtSY
Jk4sfqvQYqvOMt1uugQGkyIuGhP2djLj6Ju4+KyKKQVvDJIu/R1zFX1kkqOPt/A2pCLkisuH7nDsMbWbep0hDTVNELoKVoVIA
azwWMFlno2JuHJgUcs5hWskg/azqI4d9zy5AgMBAAGjgakwgaYwJQYDVR0RBB4wHIEaQWxhaW4uSHVnZW50b2JsZXJAd
W5pZ2UuY2gwDAYDVR0T200BAUwAwIBADBcBglghkgBhvhCAQ0ETxZNVU5JR0VDQSBjbGllbnQgY2VydGlmaWNhdGUsI
HNlZSBodHRwOi8vdW5pZ2VjYS51bmlnZS5jaCBmb3IgbW9yZSBpbmZvcm1hdGlvbnMwEQYJYIZIAYb4QgEBBAQDAgSwM
A0GCSqGSIb3DQEBBAUAA4GBACQ9Eo67A3UUa6QBBNJYbGhC7zSjXiWySvj6k4az2UqTOCT9mCNnmPR5I3Kxr1GpWT
oH68LvA30inskP9rkZAksPyaZzjT7aL//phV3ViJfreGbVs5tiT/cmigwFLeUWFRvNyT9VUPUov9hGVbCc9x+v05uY7t3UMeZejj8
zHHM+
-----END CERTIFICATE-----
```

The markers "-----BEGIN CERTIFICATE-----" and "-----END CERTIFICATE-----" frame the block of lines (the number of which is variable), each being 64 characters-long [A-Za-z0-9/+].

It is a format which is often transmitted by e-mail because this format is resistant to deformations brought about by mail software.

The PEM file is a text file which contains this type of information.

Likewise, a CRL file type contains chains of coded characters in 64 base framed by markers like "-----BEGIN X509 CRL-----" and "-----END X509 CRL-----".

As for the private key file, it contains chains of coded characters in 64 base framed by markers like "-----BEGIN RSA PRIVATE KEY-----" and "-----END RSA PRIVATE KEY-----".

8.3.2. Support for the NAT-T feature

The incompatibilities between NAT (Network Address Translation) and IPSec VPN tunnels are capable of causing problems that hinder the setup of IPSec VPN tunnels via NAT devices.

NAT-T allows supporting VPN traffic that passes through an address translation router. The number of NAT devices does not restrict this NETASQ feature.

8.3.2.1. Known incompatibilities between NAT and IPSec

These incompatibilities come under three categories:

- Intrinsic NAT issues – these incompatibilities arise directly from the address translation features, and will therefore be present on all NAT devices.
- Flaws in the NAT implementation – these incompatibilities are not intrinsic to NAT but are present in many implementations.
- Proprietary solutions – these incompatibilities are present on NAT devices that provide features enabling the use of IPSec via NAT.

Intrinsic NAT issues

<u>Incompatibility between IPSec AH and NAT</u>

Since the AH header incorporates the source and destination IP addresses in the message integrity check, NAT devices that modify address fields would invalidate the message integrity check. As IPSec ESP does not include source and destination IP addresses in the optional check of the message's encrypted integrity, this problem does not arise in the case of ESP.

<u>Incompatibility between checksums and NAT</u>

TCP and UDP checksums are calculated based on the headers in source and destination IP addresses. Therefore when checksums are calculated and checked upon receipt, they will be invalidated when processed by a NAT device.

As such, only IPSec Encapsulating Security Payload (ESP) can pass through NAT devices if TCP/UDP are not involved, or if the checksums are not calculated, or also if tunnel mode is used.

Incompatibility between IKE address identifiers and NAT

When IP addresses are used as identifiers in Phase 1 of the IKE (Internet Key Exchange) protocol, the modification of source and destination IP address by NAT will result in an error between the identifiers and the addresses in the IP headers.

In order to avoid using IP addresses as Phase 1 identifiers, UserIDs and FQDNs can be used instead.

Incompatibilities between IKE's fixed source port and NAT

When multiple hosts behind a NAT device negotiate ISAKMP SAs with the same peer, a mechanism is needed to enable the NAT device to demultiplex incoming IKE packets coming from the peer. Typically, this is done by translating the source IKE UDP port of the initiator's outgoing packets, so peers must be able to accept IKE traffic from ports other than port 500 and must respond on this port. It is also important to monitor this mechanism to avoid unpredictable behavior during key negotiation. If the "floating" source port is not used as the destination port for key negotiation, NAT will not be able to send renegotiated packets to the right destination.

Incompatibilities between the selection of IPSec SPIs (Service Provider Interfaces) and NAT

As ESP traffic is encrypted, it is opaque to NAT, so NAT is forced to use the elements in the IP headers and IPSec to demultiplex incoming IPSec traffic. For this purpose, the combination of the destination IP address, security protocol (AH/ESP) and the IPSec SPI is typically used.

However, as incoming and outgoing SPIs are chosen independently, there is no way for NAT to determine which incoming SPI corresponds to which destination host simply by inspecting the outgoing traffic. Therefore, when two hosts behind the NAT device simultaneously attempt to create IPSec SAs with the same destination, NAT may deliver the incoming IPSec packets to the wrong destination.

Incompatibilities between embedded IP addresses and NAT

As the payload integrity is protected, all IP addresses included in the IPSec packets cannot be translated by NAT devices. This makes the application-layer gateways (implemented with NAT) ineffective. Protocols which use embedded IP addresses include FTP, IRC, SNMP, LDAP, H323, SIP, SCTP (optional) and many sets. To counter this problem, the application-layer gateway has to be installed on a host or security gateway that can handle application traffic before IPSec encapsulation and after IPSec decapsulation.

Implicit directionality of NAT

An initial outgoing packet is needed to pass through a NAT device, for the purpose of creating an incoming mapping table. The protocol's directionality prohibits the unsolicited establishment of IPSec SAs to hosts located behind a NAT device.

Flaws in the NAT implementation

Inability to handle non UDP/TCP traffic

Certain NAT implementations delete non-UDP/TCP traffic or just simply translate addresses when a single host is located behind the NAT device. Such implementations will therefore be unable to accept traffic from AH or ESP protocols.

NAT mapping timeouts

NAT devices do not have uniform methods of managing how long UDP sessions should remain idle. Therefore, even when IKE packets are correctly translated, the translation state may be removed prematurely.

Inability to handle outgoing fragments

Most NAT devices are able to properly fragment outgoing IP packets in the event the size of the IP packets exceeds the MTU of the outgoing interface. However, it is difficult to correctly translate outgoing packets which are already fragmented, and most NAT devices do not correctly handle such traffic. When two hosts generate fragmented packets to the same destination, the fragment identifiers may overlap. Since the destination host relies on the fragmentation identifier and fragment offset for reassembly, this will result in data corruption.

Inability to handle incoming fragments

In the same manner as for outgoing fragments, to fragment IP addresses and headers, it may be necessary to perform a full assembly of fragments that do not arrive in the right order prior to completing the translation.

Proprietary solutions

ISAKMP header inspection

Some implementations attempt to use **IKE** cookies to demultiplex incoming IKE traffic. Like source port demultiplexing, **IKE** cookie demultiplexing goes through the same key renegotiation issues, since Phase 1 key renegotiation does not typically use the same cookies as in earlier traffic.

Special treatment of port 500

Since some IKE implementations are unable to handle UDP source ports other than port 500, some NATs do not translate packets with a UDP source port of 500. This means that these nat devices are limited to one IPsec client per destination gateway, unless they inspect details of the ISAKMP header to examine cookies, which creates the problem noted above.

8.3.2.2. Deployment of NAT-Traversal

In Phase 1 of IKE, NAT-Traversal support is detected and NAT is detected on the path between IKE peers.

NAT-Traversal uses several methods to allow IPSec through NAT: port floating to work around proprietary solutions, ESP encapsulation in UDP to enable differentiating IPSec peers and their traffic, and periodic sending of keepalive packets to keep the NAT session.

Detecting NAT-Traversal support

Whether a host supports NAT-Traversal is determined by an exchange of Vendor_ID payloads. NAT-T Vendor_ID payloads must be sent during the first packet exchange in Phase 1 (and both peers must receive them) in order to continue using NAT-T. A payload will be sent for each version of NAT-T supported, containing an MD5 hash of RFC 3947, with a value of 4a131c81070358455c5728f20e95452f.

Detecting NAT

NAT-T does not only detect the presence of NAT between IKE peers, but also detects the direction of the NAT. Locating the NAT device is important as keepalive packets have to be initiated by the peer behind the NAT.

In order to detect NAT between two peers, it is necessary to check whether the IP address or port changes during the transmission (this implies that the recipients must be able to handle IKE packets with a source port other than the usual port 500).

Peers send a hash of the ports and IP addresses to their counterparts. When each peer recalculates the hash (based on the IP addresses they receive), and it corresponds to the hash sent by its counterpart, then that means that NAT is not operating between them. If the hashes do not match, that means that the address or port has been translated, therefore NAT-Traversal has to be performed so that IPSec packets can pass through.

Hashes are sent as a series of NAT-D (NAT Discovery) payloads included in the third and fourth packet in main mode and in the second and third packet in aggressive mode.

The example below illustrates a NAT-D payload exchange in main mode:

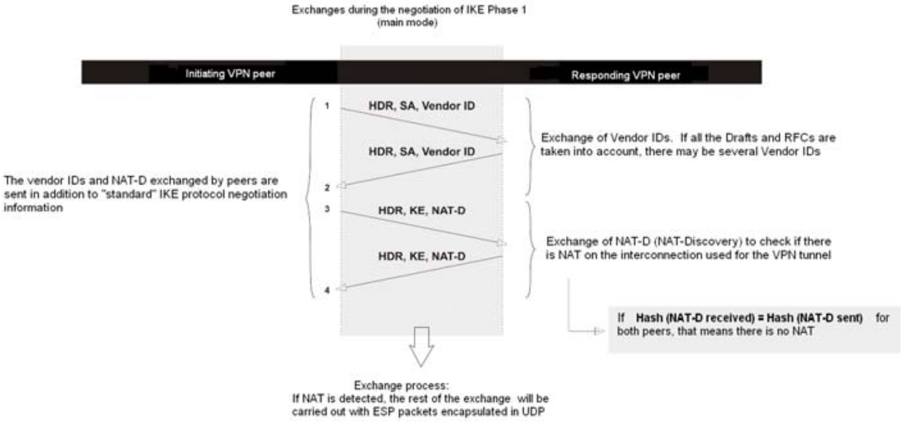
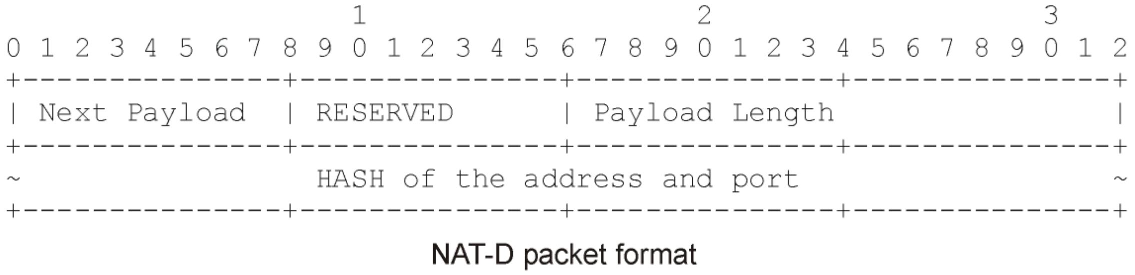

Exchanges during the negotiation of IKE Phase 1
(main mode)
Initiating VPN peer
Responding VPN peer
1
HDR, SA, Vendor ID
HDR, SA, Vendor ID
2
3
HDR, KE, NAT-D
HDR, KE, NAT-D
4
The vendor IDs and NAT-D exchanged by peers are sent in addition to "standard" IKE protocol negotiation information
Exchange of Vendor IDs. If all the Drafts and RFCs are taken into account, there may be several Vendor IDs
Exchange of NAT-D (NAT-Discovery) to check if there is NAT on the interconnection used for the VPN tunnel
If Hash (NAT-D received) = Hash (NAT-D sent) for both peers, that means there is no NAT
Exchange process:
If NAT is detected, the rest of the exchange will be carried out with ESP packets encapsulated in UDP

Figure 197: NAT-D payloads in main mode

The format of a NAT-D payload is as follows:



```
                            1                   2                   3
        0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2
        +---------------+---------------+---------------+---------------+
        | Next Payload  | RESERVED      | Payload Length                |
        +---------------+---------------+---------------+---------------+
        ~                 HASH of the address and port                  ~
        +---------------+---------------+---------------+---------------+
```

NAT-D packet format

Figure 198: NAT-D payload

The payload type for the NAT-D (NAT Discovery) payload is 20.

The hash is calculated accordingly: HASH = HASH(CKY-I | CKY-R | IP | Port).

This calculation uses the HASH algorithm negotiated earlier (hashes are sent in the third and fourth packets, while the SAs that negotiate the encryption and authentication algorithms are sent in the first and second packets). The first NAT-D payload contains the remote tunnel endpoint's IP address and the port (ie, the destination address of UDP packets). The NAT-D payloads that follow contain the IP addresses and ports of different possible local tunnel endpoints (ie, all the possible sources of UDP packets).

If there is no NAT between the peers, the first NAT-D payload that a host receives has to correspond to one of the local payloads (ie, the local NAT-D payload that this host sends to its peer), and another of the NAT-D payloads has to correspond to the peer's IP address and port. If the first check fails (ie, the first NAT-D payload does not correspond to any IP address and local port), this means that there is dynamic translation between the peers and that this tunnel endpoint has to start sending keepalive packets because this endpoint is located behind a NAT device).

CKY-I and CKY-R are respectively the initiator's and responder's cookies. They are added to the hash in order to protect the IP addresses and ports from attacks.

Changing to a new port

Interactions between IPSec and intelligent NAT often cause problem. Some NAT devices would not change the IKE source port (500) even if there are several clients behind the NAT device. They may also use IKE cookies to demultiplex traffic instead of using the source port. Both cases are problematic for NAT transparency, which in turn creates problems for IKE in the detection of NAT in devices through which the traffic passes. The best approach is to simply move the IKE traffic to a port other than port 500 soonest possible to prevent such occurrences with intelligent NAT.

Take the most common example, in which the initiator is located behind a NAT device. Once NAT has been detected, the initiator must quickly change his port to UDP port 4500 to minimize the possibility of interaction issues between IPSec and intelligent NAT.

When the responder receives this packet, the different payloads will be decrypted and handled as usual. If this step is carried out successfully, the responder will have to update his local table so that the rest of the packets (including notifications) going to the peer will use the new port and possibly even the new IP address obtained from the packet received. In general, the port will be different, and therefore NAT will map UDP(500, 500) to UDP(x, 500) and UDP(4500, 4500) to UDP(y, 4500). Rarely will the IP address be different from the previous IP address. The responder will send all the IKE packets that follow to its peer using UDP(4500, y).

Likewise, if the responder has to renegotiate the Phase 1 SA, the negotiation will use UDP(4500, y). If a negotiation begins on port 4500, nothing needs to be changed in the rest of the exchange.

Here is an example of a Phase 1 exchange using NAT-T in main mode with a port change:

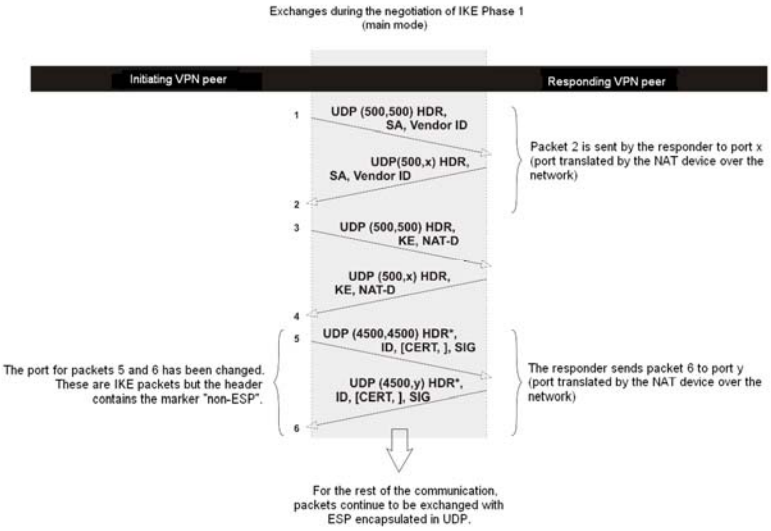

Exchanges during the negotiation of IKE Phase 1
(main mode)
Initiating VPN peer
Responding VPN peer
1
UDP (500,500) HDR,
SA, Vendor ID
UDP(500,x) HDR,
SA, Vendor ID
2
Packet 2 is sent by the responder to port x (port translated by the NAT device over the network)
3
UDP (500,500) HDR,
KE, NAT-D
UDP (500,x) HDR,
KE, NAT-D
4
5
UDP (4500,4500) HDR*,
ID, [CERT,], SIG
UDP (4500,y) HDR*,
ID, [CERT,], SIG
6
The port for packets 5 and 6 has been changed. These are IKE packets but the header contains the marker "non-ESP".
The responder sends packet 6 to port y (port translated by the NAT device over the network)
For the rest of the communication, packets continue to be exchanged with ESP encapsulated in UDP.

Figure 199: NAT traversal – Main mode

Encapsulating ESP traffic in UDP

Because of the “incompatibilities between the selection of IPSec SPIs and NAT” (explanations earlier in the document), it is absolutely necessary to implement a mechanism that enables distinguishing different types of VPN traffic. Encapsulating ESP traffic in a more “classic” protocol such as UDP enables the creation of a certain agreement between different types of VPN traffic represented by their SPIs and an element in the UDP header that NAT devices are able to handle, in this case, ports.

Thus, as soon as the VPN negotiation is over, all the ESP traffic will be encapsulated in the UDP as shown in the different diagrams below:

Several ports besides 4500 can now be used, enabling several clients from the same network to connect.

<u>Encapsulation of ESP traffic in transport mode</u>

Packet before encapsulation in ESP and UDP.

```
-----------------------------
|orig IP hdr  |      |      |
|(any options)| TCP  | Data |
-----------------------------
```

Figure 200: Before ESP encapsulation in transport mode

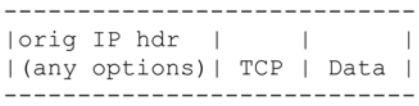
Packet after encapsulation in ESP and UDP

```
-----------------------------------------------------------
|orig IP hdr  | UDP | ESP |     |      |   ESP   | ESP|
|(any options)| Hdr | Hdr | TCP | Data | Trailer |Auth|
-----------------------------------------------------------
                          |<---- chiffré ------->|
                    |<-------- authentifié ----->|
```

Figure 201: After encapsulation in transport mode

Encapsulation of ESP traffic in tunnel mode

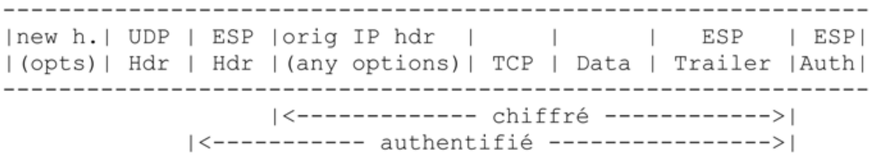
Packet before encapsulation in ESP and UDP



```
----------------------------
|orig IP hdr  |      |      |
|(any options)| TCP  | Data |
----------------------------
```

Figure 202: Before ncapsulation in tunnel mode

Packet after encapsulation in ESP and UDP.



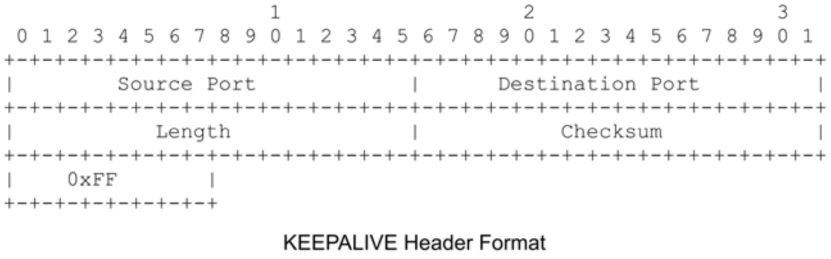
```
-------------------------------------------------------------
|new h.| UDP | ESP |orig IP hdr  |     |      |   ESP   | ESP|
|(opts)| Hdr | Hdr |(any options)| TCP | Data | Trailer |Auth|
-------------------------------------------------------------
                   |<------------- chiffré ------------>|
             |<----------- authentifié ---------------->|
```

Figure 203: After encapsulation in tunnel mode

Keeping the NAT pseudo-session

An IPSec VPN tunnel's stability is guaranteed if the NAT session is maintained through the periodic sending of keepalive packets between both VPN peers. When the session is maintained, the port chosen for the translation remains the same. The responder can thus initiate a tunnel negotiation at the end of the lifetime on the translated port.

The UDP packet is composed as follows:



```
                     1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|        Source Port            |       Destination Port        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|           Length              |           Checksum            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|    0xFF       |
+-+-+-+-+-+-+-+-+
```

KEEPALIVE Header Format

Figure 204: Keepalive

The UDP header above corresponds to a standard header defined by RFC 768, containing:

- Source and destination ports. These fields have to be exactly the same as those used for encapsulating ESP traffic in UDP,
- The UDP checksum has to be set to 0
- The initiator of the VPN connection (the only peer who is supposed to send keepalive packets, even though in practice, some solutions allow the responder to send them) has to define this packet's payload in hexadecimal 0xFF.

8.3.2.3. Configuring NAT-T on the NETASQ UTM appliance

This feature is activated transparently on NETASQ Firewalls. If the VPN peer supports NAT-T, it will then be implemented if the need arises. If the VPN peer does not support it, then the feature will not be set up.

8.3.2.4. Application of the feature

NETASQ's NAT-T feature now supports architectures in which several mobile VPN clients are used behind a single IP address.
This feature is particularly useful when several VPN clients are used to contact a central site from the same internet connection (e.g. in a hotel).

8.3.3. Configuration

A VPN configuration policy allows defining VPN tunnels.

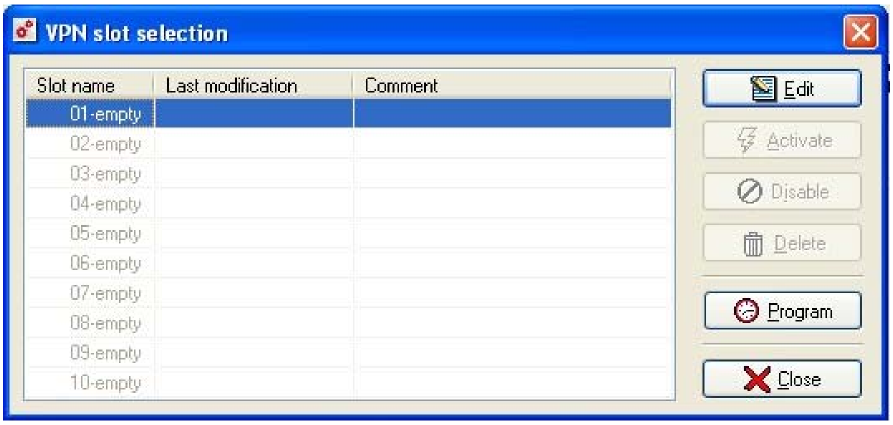
8.3.3.1. IPSec VPN on NETASQ Firewalls

➲ IPSec VPN tunnels can be configured through the menu **`VPN\IPSec Tunnels`** in the menu directory. These tunnels are configured in three steps as follows:

1 Select a VPN policy slot
2 Perform the first steps of the configuration using the wizard
3 Complete the configuration of the VPN in the IPSec VPN tunnels configuration menu.

8.3.3.2. Selecting a VPN policy slot

➲ When you select the menu **`VPN\ IPSec Tunnels`** a dialog box appears, allowing you to use the configuration files associated with IPSEC VPN configurations.



Slot name	Last modification	Comment
01-empty		
02-empty		
03-empty		
04-empty		
05-empty		
06-empty		
07-empty		
08-empty		
09-empty		
10-empty		

Figure 205: Selecting a VPN slot

It is split into two parts:

- **Left**: List of configuration files.
- **Right**: Actions on the selected file.

> **NOTE**
> This window works in the same way as those in NAT and Filters.

List of configuration files

In this part of the dialog box, you will find the list of the configuration files. There are 10 of them , numbered from 01 to 10.

Each configuration file has a name, a date/time of activity and the date of the last change carried out on this slot.

The activation includes the time and day(s) the file is activated. Days are indicated by the day's number in the week (Monday = 1). (*See Part 7/Chapter 3: Slot Scheduler*).

A small green arrow to the right of its name indicates the active configuration file.

A configuration file is "active" when the parameters it contains are in use. There can be no more than one active configuration file because the parameters of the last active configuration file overwrite those of the previously active configuration file.

If you change a configuration file, you must reactivate it for the changes to be applied. A slot that has been modified but not reactivated is signaled by the icon ❗ instead of the usual green arrow.

It is possible for no configuration file to be active, implying that no VPN tunnel is active.

Each configuration file does not necessarily have to contain parameters.

A configuration file slot for which no configuration file exists on the NETASQ Firewall appears under the name "empty" in the list.

A configuration file is selected when you simply click on its name with the mouse. Once you have selected it, you can edit or activate it.

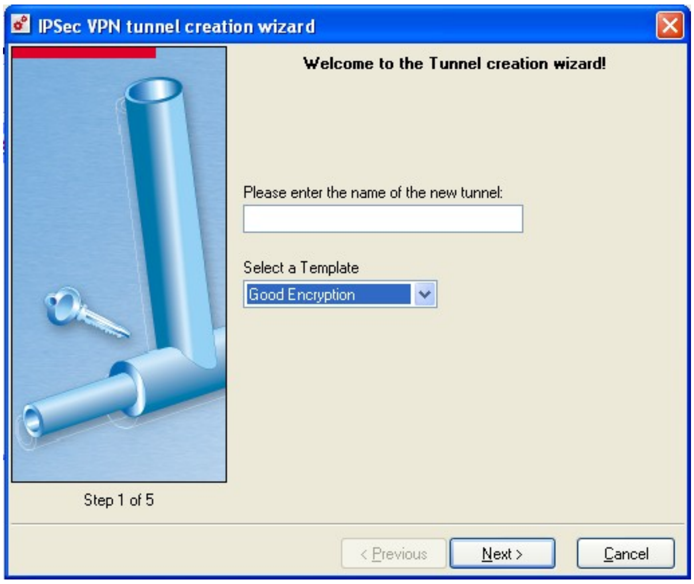
Actions on the selected configuration file

> **NOTE**
> These action buttons work in the same way as those in NAT and Filters.

8.3.3.3. IPSec VPN tunnel configuration wizard

When the selected policy slot is empty, a wizard will aid in configuring the IPSec VPN tunnel in five steps.

1 Step 1: Welcome



IPSec VPN tunnel creation wizard

Welcome to the Tunnel creation wizard!

Please enter the name of the new tunnel:

Select a Template: Good Encryption

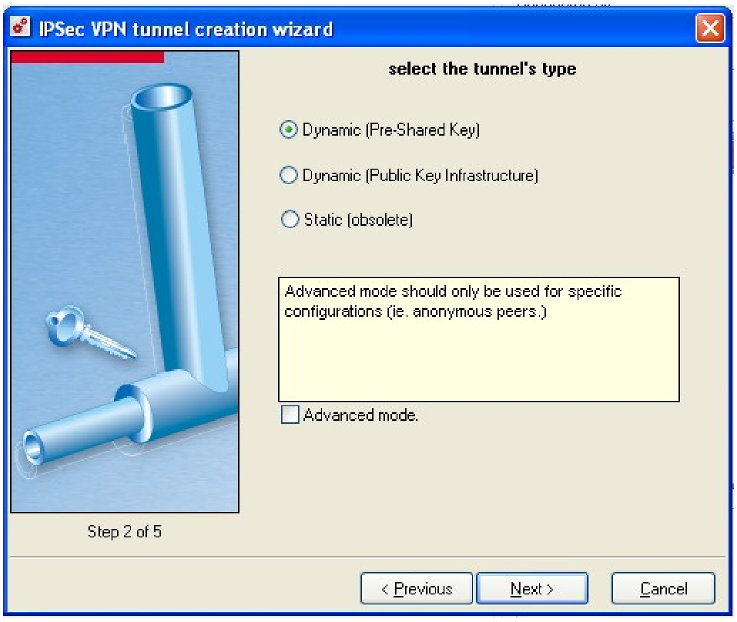
Step 1 of 5

Figure 206: Creating IPSec tunnels- Step 1

Step 1 allows defining the name assigned to the VPN policy and the protection model to be applied. A “Strong encryption (slow)” type of model will allow the implementation of IPSec VPN tunnels that are more secure but slower (stronger encryption and authentication algorithms) than those in a "Fast encryption (weak)" type of model. The “Bypass” model serves to handle IPSec exclusions, meaning the exclusion of any host or network for which encryption is not desired, communicating with another host or remote network.

The protection model defines the encryption and authentication algorithms that can be modified in the configuration suite. We therefore recommend that you leave this option to its default value (ie, “Good encryption") then to modify it when necessary.

2 Step 2: Choosing the tunnel type



IPSec VPN tunnel creation wizard

select the tunnel's type

● Dynamic (Pre-Shared Key)

○ Dynamic (Public Key Infrastructure)

○ Static (obsolete)

Advanced mode should only be used for specific configurations (ie. anonymous peers.)

□ Advanced mode.

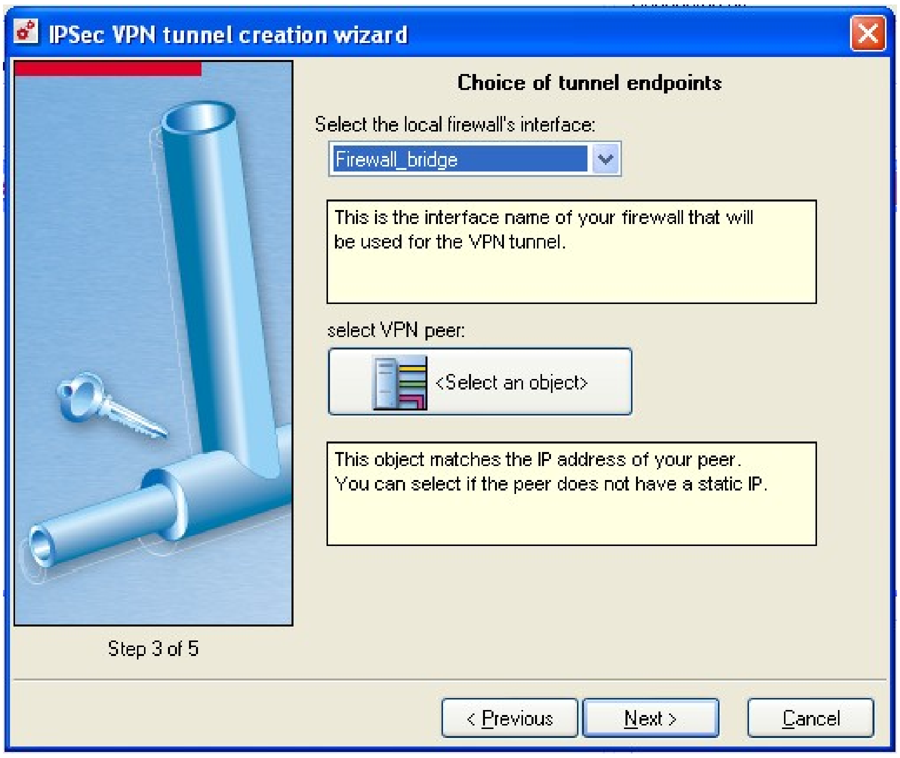
Step 2 of 5

Figure 207: Creating IPSec tunnels - Step 2

Step 2 involves defining the type of tunnel configured. Three options are available. Two of the tunnel types are based on the dynamic negotiation of VPN tunnel parameters (encryption key) through IKE, only their authentication modes differ (pre-shared keys or certificates). Note that the “Static” mode is obsolete and is only suggested for interoperability with existing configurations.

The “advanced mode” option allows using “any” for both peers. This type of configuration requires in-depth knowledge of how IPSec VPN tunnels operate on NETASQ firewalls.

3 Step 3: Choosing tunnel endpoints



Choice of tunnel endpoints

Select the local firewall's interface: Firewall_bridge

This is the interface name of your firewall that will be used for the VPN tunnel.

select VPN peer: <Select an object>

This object matches the IP address of your peer. You can select if the peer does not have a static IP.

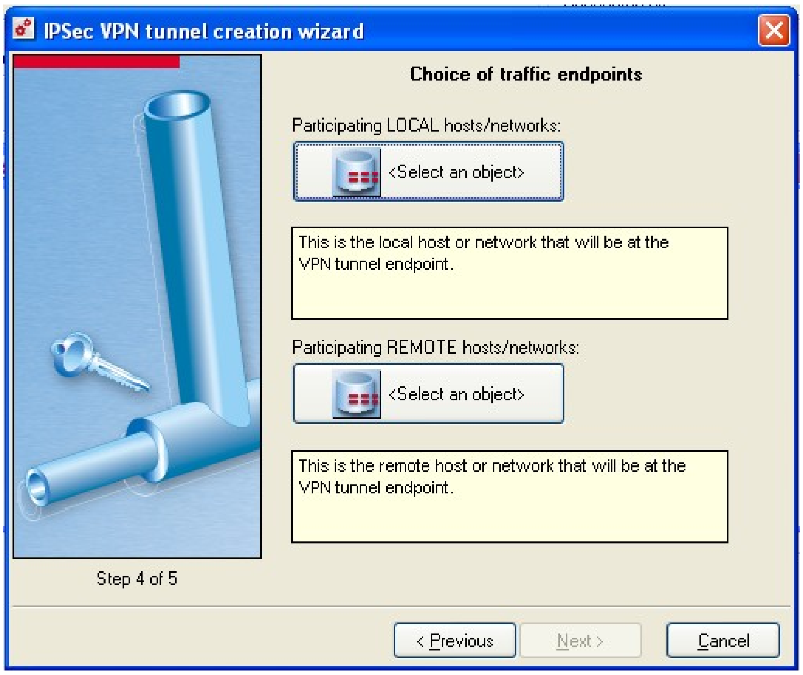
Figure 208: Creating IPSec tunnels- Step 3

In this step, you are required to define the tunnel endpoints, which are the hosts between which the tunnelis being created and for which communication is encrypted.

The local interface refers to the interface that will be the endpoint on your firewall. For example, "Firewall_out", the external interface of the firewall or "Firewall_dialup" if the VPN connections reach the firewall via a modem configured in the dialup section.

The remote interface refers to the VPN peer that will be your firewall’s counterpart. For example, your VPN peer’s known public IP address. For nomad VPN tunnels (for which the IP address is unknown) the object <any> will be used. However, for full information on this type of tunnel, refer to the configuration examples.

4 Step 4: Choosing traffic endpoints



Choice of traffic endpoints

Participating LOCAL hosts/networks:

<Select an object>

This is the local host or network that will be at the VPN tunnel endpoint.

Participating REMOTE hosts/networks:

<Select an object>

This is the remote host or network that will be at the VPN tunnel endpoint.

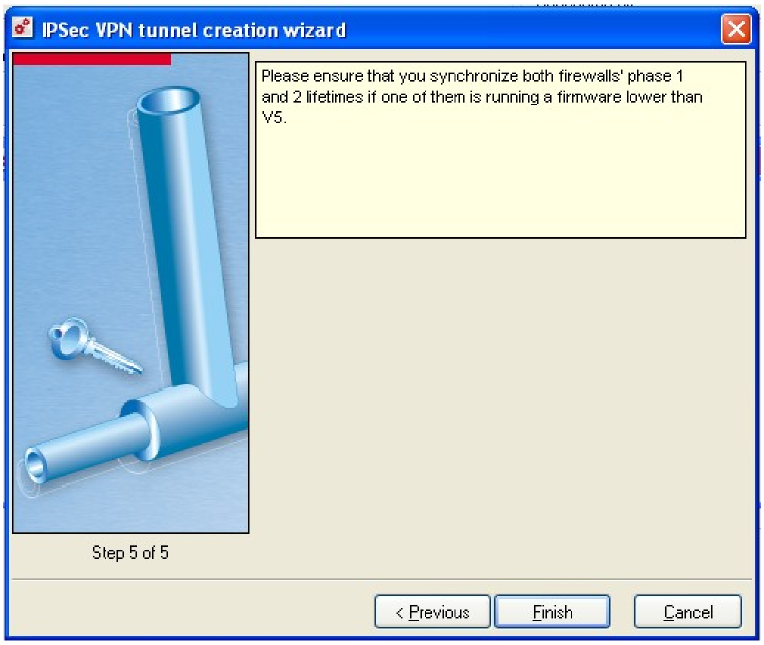
Figure 209: Creating IPSec tunnels- Step 4

Here, you are required to define traffic endpoints, which refer to the real peers that will communicate through the IPSec VPN tunnel.

The local host refers to the host on your local network that seek to communicate through the VPN tunnel. For example "Network_in", your internal network or "Network_bridge" if your internal interfaces have been defined in bridge.

The remote host refers to a host on your VPN peer's network. For example, the network IP address. For nomad VPN tunnels (for which the IP address is unknown) the object <any> will be used. However, for full information on this type of tunnel, refer to the configuration examples.

5 Step 5



Please ensure that you synchronize both firewalls' phase 1 and 2 lifetimes if one of them is running a firmware lower than V5.

Figure 210: Creating IPSec tunnels - Step 5

Step 5 will inform you that the lifetimes between Phase 1 and 2 have to be compatible for a version lower than version 5.0. Otherwise, these lifetimes can be completely independent.

> **WARNING**
> The default lifetime values between version 5 and version 6 have changed. This means that the tunnel will not operate with a firewall in version 6 or higher when connecting with a firewall in version 5 if using the wizard.

Example of a bypass configuration

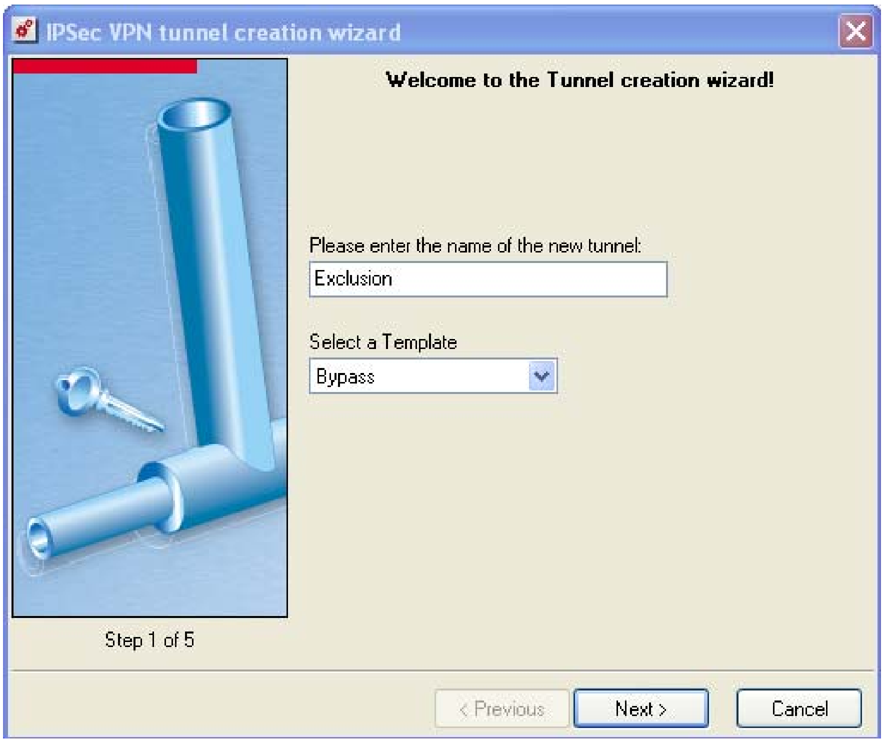
To remove a host (or a network) from the encryption process, use the “Bypass” operation (also called “No encryption”).

The order in which tunnels are configured is important – the unencrypted tunnel needs to be configured first.

> **WARNING**
> For a "bypass" tunnel, you need to specify the local host or network that will be used as the source and which will be excluded from encryption, followed by the remote entity or network that will be the destination.

The example below illustrates how to remove a host from the encryption process.

1 Step 1: Welcome to the tunnel creation wizard



Welcome to the Tunnel creation wizard!

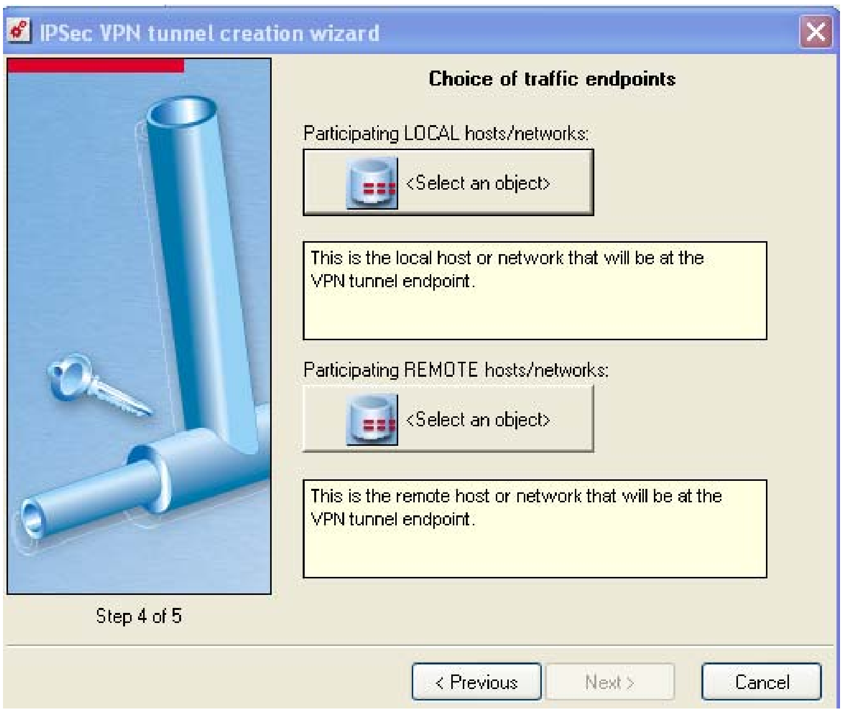
Please enter the name of the new tunnel: Exclusion

Select a Template: Bypass

Figure 211: IPSec configuration - Step 1

Name the IPSec tunnel then select the “Bypass” model.

2 Step 2: Selecting the traffic endpoints



Choice of traffic endpoints

Participating LOCAL hosts/networks: <Select an object>

This is the local host or network that will be at the VPN tunnel endpoint.

Participating REMOTE hosts/networks: <Select an object>

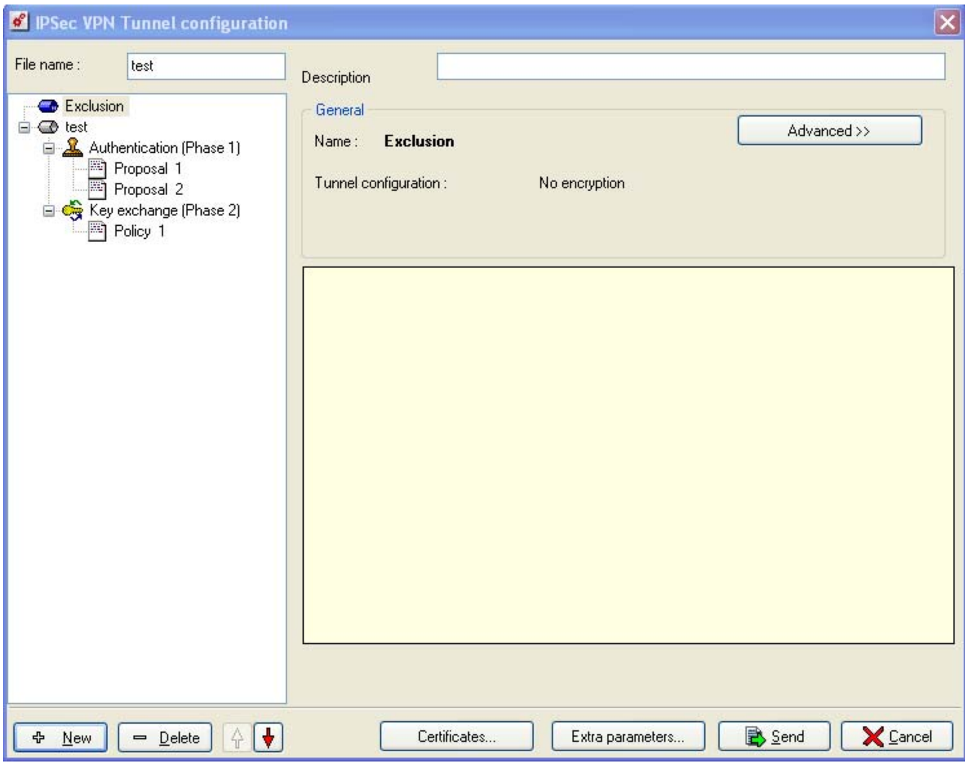
This is the remote host or network that will be at the VPN tunnel endpoint.

Figure 212: IPSec tunnel - Step 4

Here, indicate the local host or network that will be used as the source, followed by the remote entity or network that will be the destination.

3 Step 3: Order of the tunnels

Use the arrows at the bottom of the window to arrange the tunnels in order. The unencrypted tunnels have to come first.



File name : test

Description

Name : **Exclusion**

Tunnel configuration : No encryption

Figure 213: IPSec tunnel – Ordering

VPN tunnel configuration menu

When the wizard configuration is confirmed, the IPSec VPN tunnel configuration menu will appear. This menu groups together all the necessary options for creating and managing the parameters on a VPN policy.

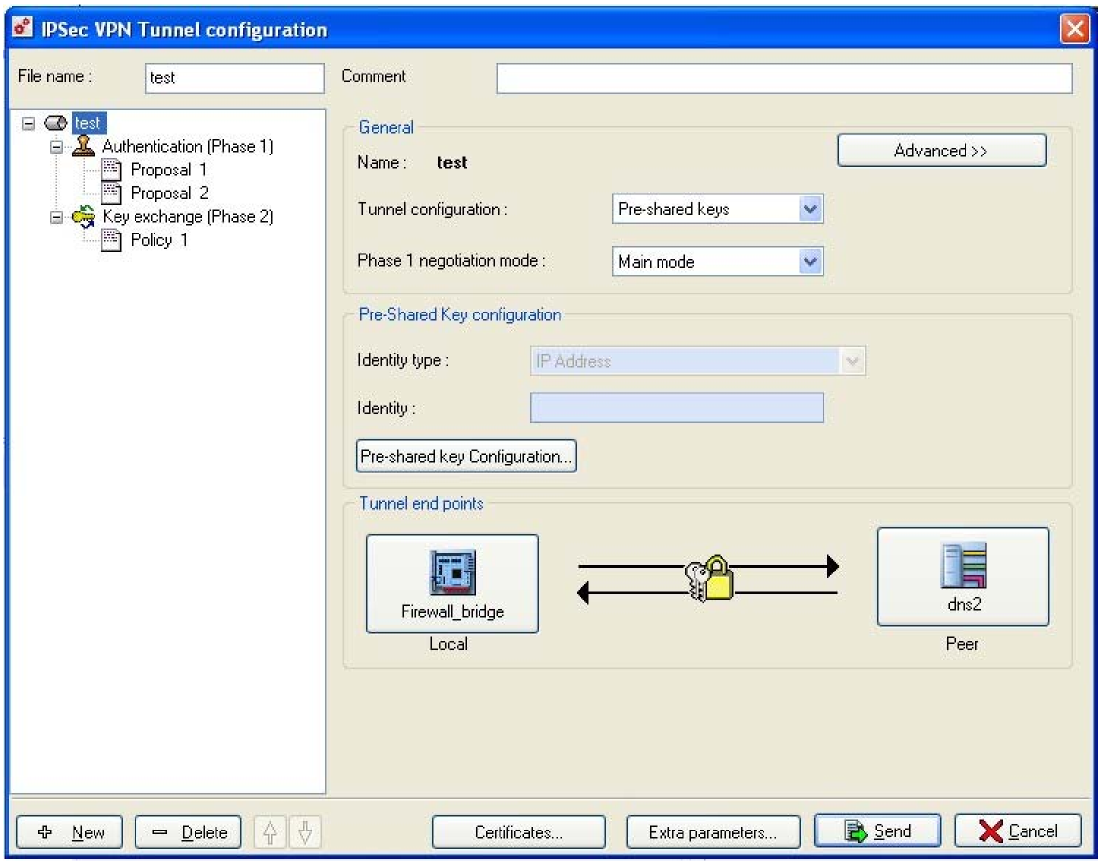
If you select a slot that is not empty, the VPN tunnel configuration menu will automatically appear, without having to go through all the steps in the wizard. To start the wizard from the beginning, select an empty slot or delete the selected slot. Or you can also select “New tunnel”.

Contextual menu

The following options will be given when you right-click on one of the tunnels in the directory:

Add	Adds a new IPSec VPN tunnel.
Duplicate	Duplicates the selected IPSec VPN tunnel.
Delete	Deletes the selected IPSec VPN tunnel.
Rename	Renames the selected IPSec VPN tunnel.

Group/deploy all	Expands/collapses the IPSec tunnels in the menu directory.



IPSec VPN Tunnel configuration

File name : test

Comment :

General

Name : **test**

Tunnel configuration : Pre-shared keys

Phase 1 negotiation mode : Main mode

Pre-Shared Key configuration

Identity type : IP Address

Identity :

Tunnel end points

Firewall_bridge — Local

dns2 — Peer

Figure 214: Configuring IPSec VPN tunnels

Refer to the relevant section corresponding to the tunnel type chosen (static or dynamic) to understand the different fields and parameters.

WARNING

When a VPN configuration slot is modified (new tunnel added, or existing tunnel deleted or modified), only the tunnels affected by the modification will be reloaded when the modified slot is reactivated.

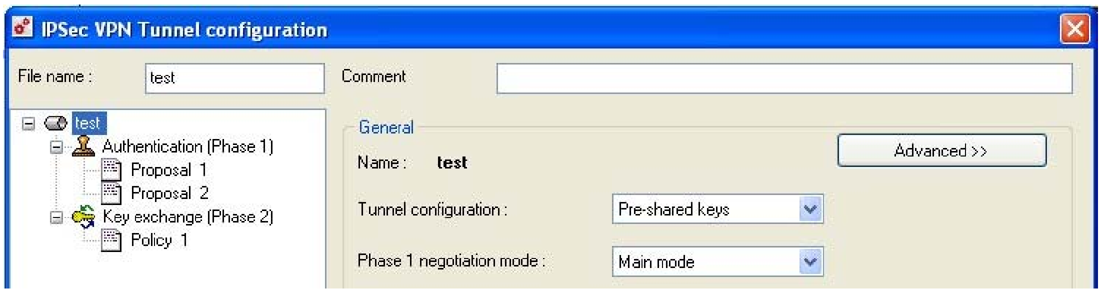
8.3.3.4. IPSec VPN tunnel configuration menu

An IPSec VPN tunnel policy is defined by a name (entered in the configuration wizard). This name is indicated at the top of the IPSec VPN tunnel configuration menu. Comments can also be added.

General parameters of the IPSec VPN tunnel

Every IPSec VPN tunnel in an IPSec VPN tunnel policy is also defined by its name. By default, this name is the same as the one in the IPSec VPN policy. Click on the name of the tunnel in the menu directory of configured tunnels in order to access all the general parameters for this tunnel.

General



IPSec VPN Tunnel configuration

File name : test

Comment

test
Authentication (Phase 1)
Proposal 1
Proposal 2
Key exchange (Phase 2)
Policy 1

General

Name : test

Advanced >>

Tunnel configuration : Pre-shared keys

Phase 1 negotiation mode : Main mode

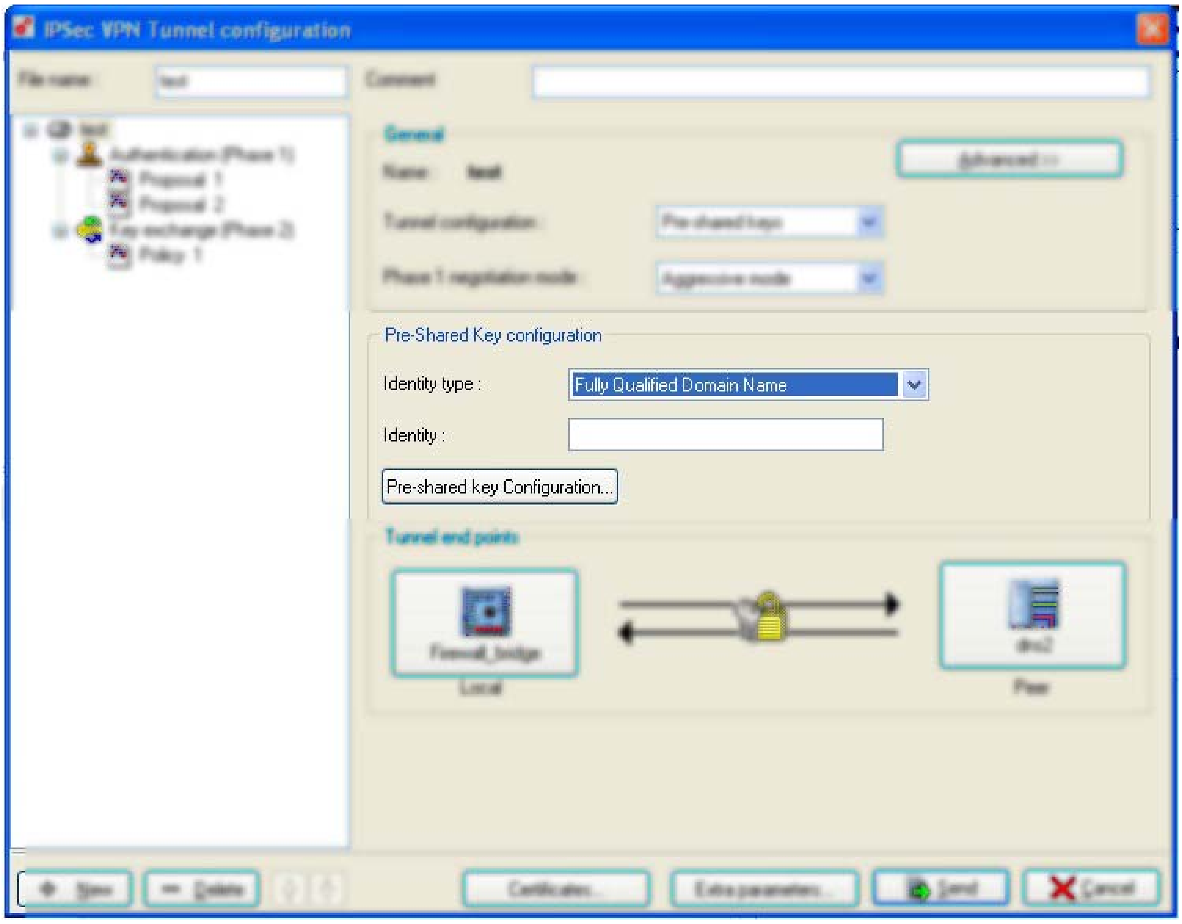
Figure 215: Configuring IPSec VPN tunnels - General

Name	The name of the tunnel that you had entered when creating the tunnel. You can modify this name by right-clicking on the name of the tunnel in the menu directory of configured tunnels.
Tunnel configuration	As in Step 2, this option defines the type of IPSec VPN tunnel configured.
Phase 1 Negotiation mode:	**Main mode**: Phase 1 takes place in 6 exchanges. The remote host can only be identified by its IP address with pre-shared key authentication. In PKI mode, the identifier is the certificate. Main mode guarantees anonymity. **Aggressive mode**: Phase 1 takes place in 3 exchanges between the Firewall and the remote host. The remote host can be identified by an IP address, FQDN or e-mail address but not by a pre-shared key certificate. Aggressive mode does not guarantee anonymity. **WARNING** The use of the aggressive mode + pre-shared keys (especially for VPN tunnels to mobile workstations) may be less safe than other modes in the IPSec protocol. NETASQ recommends using the main mode and especially main mode + certificates for tunnels to mobile workstations. In fact, the Firewall's internal PKI is capable of providing the certificates needed for such use. **REMARK** This parameter cannot be configured for static IPSec VPN tunnels.
Advanced configuration	This button shows the advanced configuration options.

Configuring pre-shared keys

Configuring pre-shared keys allows you to define the secret previously exchanged between both peers of the VPN tunnel. Every pre-shared key is defined according to a remote VPN peer and is MANDATORY for dynamic IPSec VPN tunnels.

When the type of IPSec VPN tunnel selected is dynamic and by pre-shared keys, a specific configuration section appears. This section enables defining the local identity of your Firewall, the identity of the VPN peer and the key shared by both peers.



IPSec VPN Tunnel configuration
Pre-Shared Key configuration
Pre-shared key Configuration...

Identity type : Fully Qualified Domain Name

Identity :

Figure 216: Configuring pre-shared keys

Identity type The type of identity allows defining how your Firewall will be identified. There are three types of identity on NETASQ Firewalls: public IP address, domain name (FQDN: Full Qualified Domain Name) or e-mail address (user@fqdn). In main mode, “IP address” is selcted automatically as the type of identity.

Identity The identity field allows defining your Firewall’s local identity, e.g. firewall@netasq.com for an “e-mail address” identity type.

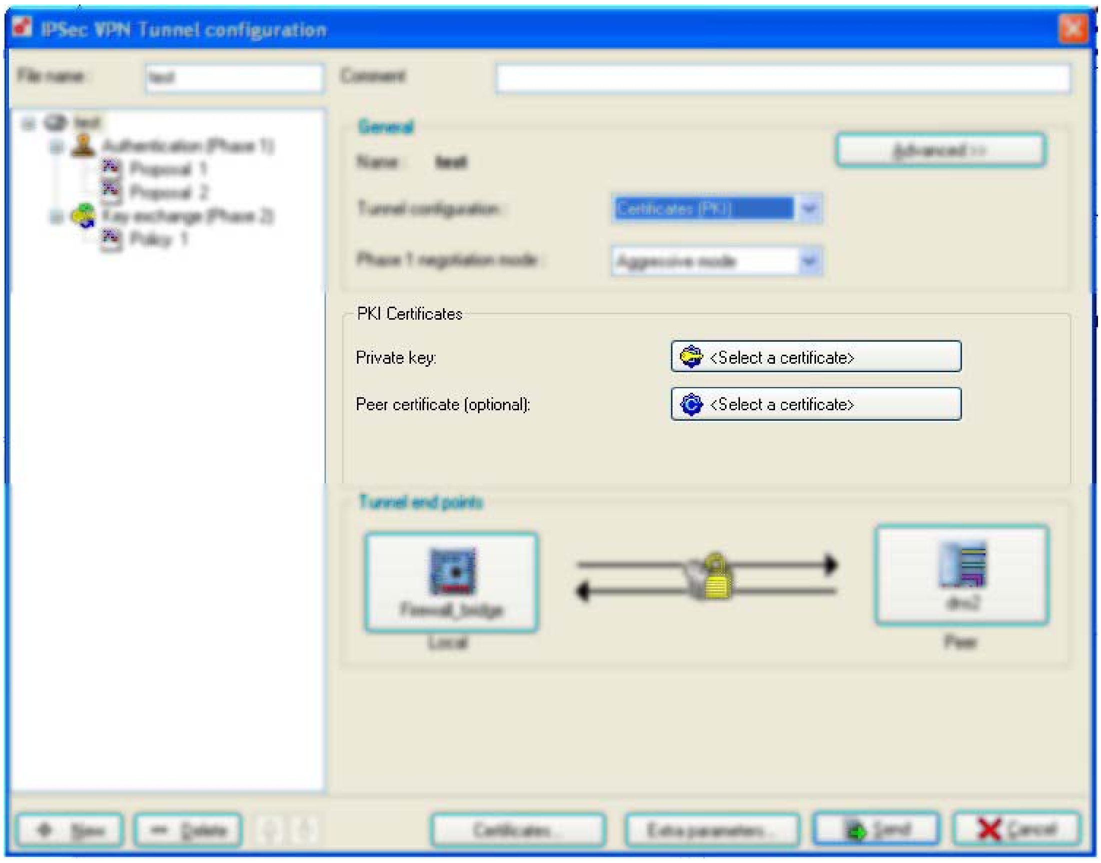
For an “IP address” identity type, the “identity” field does not need to be entered as it is automatically defined by the object that had been selected as the local tunnel endpoint.

Pre-shared key Configuration This button shows the options for the configuration of pre-shared keys (identity of the remote peer, keys shared by both VPN peers and a single key for both VPN peers).

PKI Certificates

When the type of IPSec VPN tunnel selected is dynamic and by certificates (PKI), a specific configuration section appears. This section enables defining the local identity of your Firewall (in the form of a certificate) and the identity of the VPN peer (in the form of a certificate).

Certificates used in the configuration of an IPSec VPN tunnel with certificate authentication are configured in a certificate configuration menu.



File name: test

Comment:

Name: test

Tunnel configuration: Certificates (PKI)

Phase 1 negotiation mode: Aggressive mode

Private key: <Select a certificate>

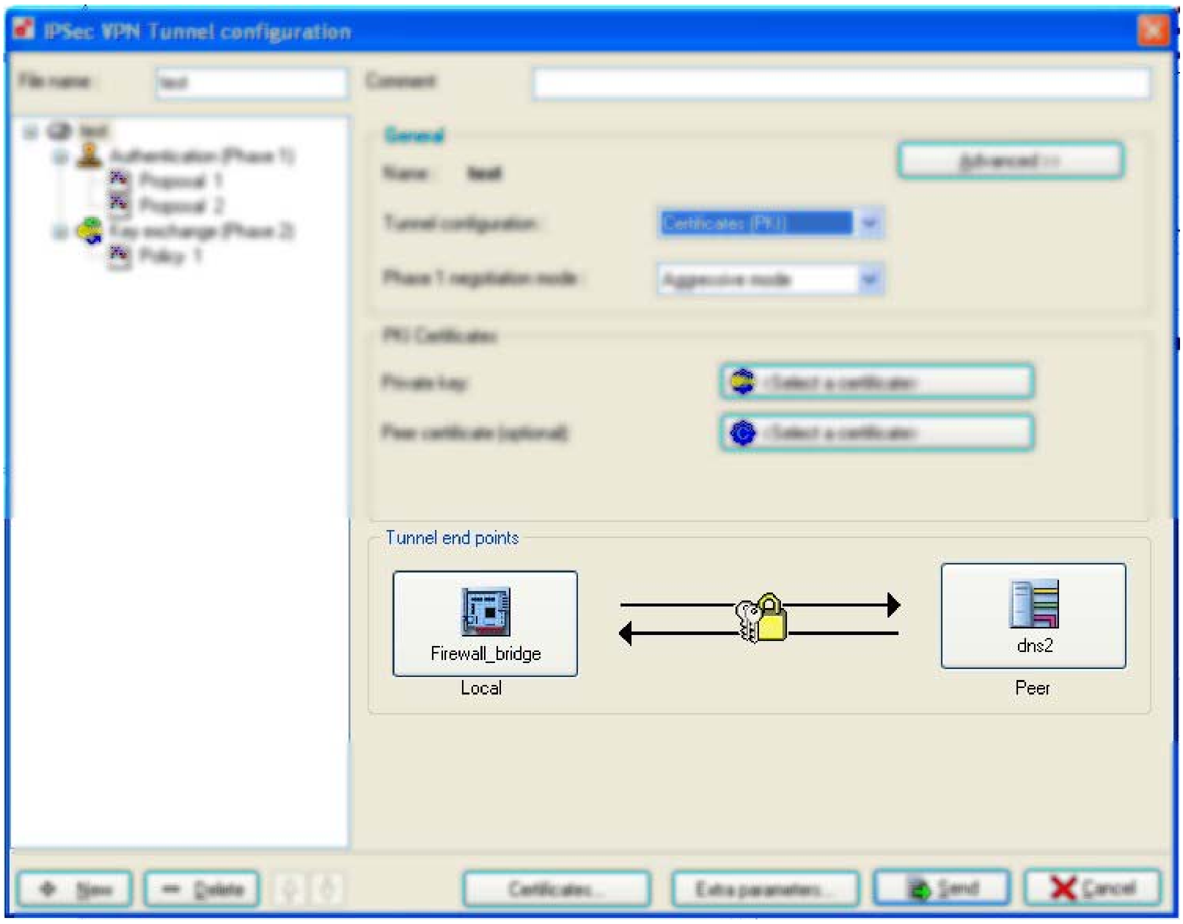
Peer certificate (optional): <Select a certificate>

Figure 217: PKI Certificates

Private key	Configuration of the local Firewall's certificate (a window will open showing the list of local certificates available). The private key enables the implementation of electronic signature, decryption and authentication algorithms for third parties.
Peer certificate (optional)	Optional configuration of the remote Firewall's certificate (a window will open showing the list of remote certificates available). **WARNING** If a certificate has been defined for the peer, during the authentication phase, the IPSec module will only check if the peer's certificate is the same as the one selected, but the validity of the certificate (expiry, revocation, authority's signature) will NOT be checked. Thus the CA's revocation of the certificate will have no effect. You are therefore advised against specifying a certificate for the peer, unless there are specific needs.

Tunnel endpoints

This section of the menu shows a recap of the tunnel endpoints configured in the configuration wizard. These tunnel endpoints can then be modified by clicking on the objects that represent the tunnel's local and peer's remote endpoints.



File name: test

Comment:

General

Name: test

Tunnel configuration: Certificates (PKI)

Phase 1 negotiation mode: Aggressive mode

PKI Certificates

Private key: <Select a certificate>

Peer certificate (optional): <Select a certificate>

Tunnel end points

Local: Firewall_bridge

Peer: dns2

Figure 218: Tunnel endpoint

Local	The interface that the IPSec VPN tunnel affects on the local Firewall.
Peer	Public IP address of the remote VPN peer. Reminder: if this IP address is unknown, the object “any” has to be used. Refer to the examples of advanced IPSec VPN tunnel configuration for further information on h ow to use the object “any”.

8.3.3.5. Advanced configuration

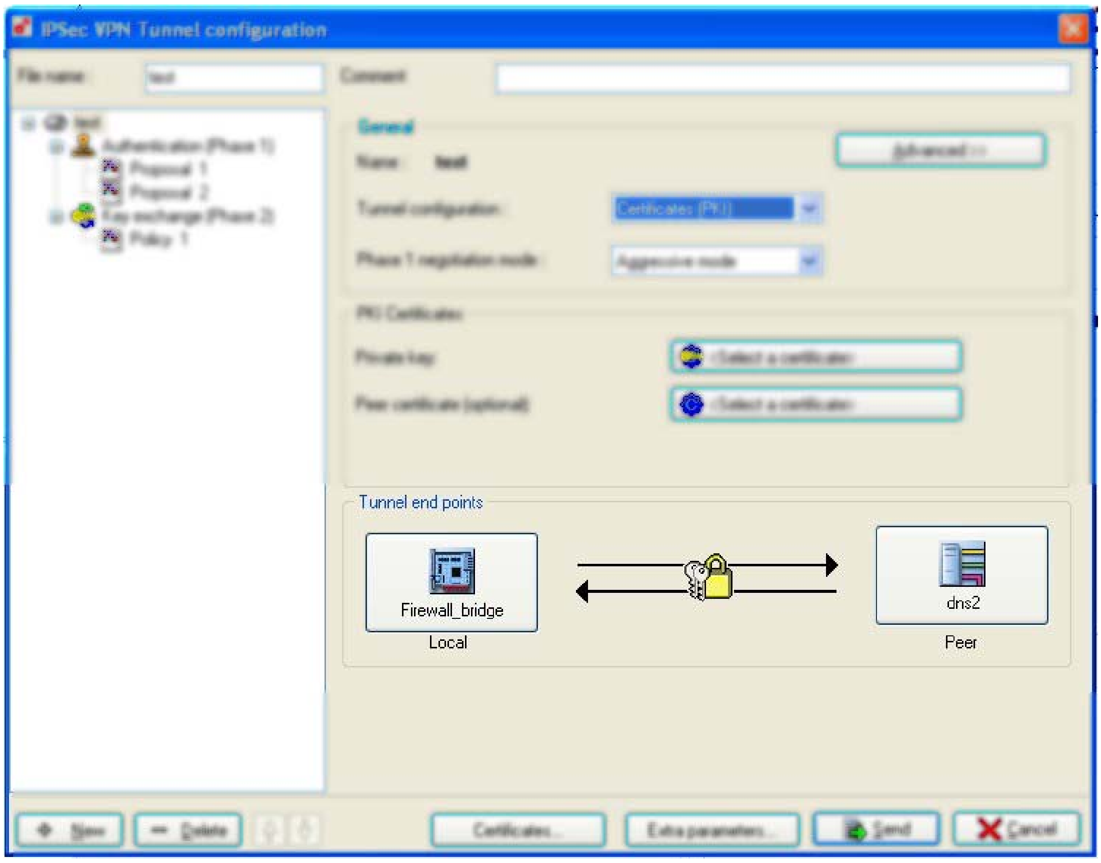


Figure 219: Configuring IPSec VPN tunnels – Advanced configuration

A button at the top right corner of the window enables switching to **Advanced configuration**. The following can be modified in advanced configuration:

- the action mode.
- the “Responder only” option.
- the “Advanced mode” option.
- options in the configuration of VPN with Certificates.

Action mode

The action modes determine the IPSEC server’s behavior in Phase 1 during the negotiation of PFS (Perfect Forward Secrecy) options and SA lifetime:

- **Strict**: accepts only options equal to or stricter than its own (higher PFS, shorter SA lifetime).
- **Claim**: accepts only options equal to or less strict than its own (lower PFS, longer SA lifetime), but always chooses the strictest options.
- **Exact**: accepts only options as strict as its own (same PFS level, SA lifetime strictly equal).
- **Obey**: accepts every option (PFS level, SA lifetime).

WARNING
The action modes “Obey” and “Claim” are not covered by the Common Criteria.

Responder only

The option "Responder only" puts the IPSEC server in a waiting mode. It won't initiate tunnel negotiation. This option is used in the case where the peer is a mobile host.

Advanced mode

The “advanced mode” option allows using “any” for both peers. Thanks to this feature, a NETASQ Firewall may be used as a channel for Hub & Spoke for example.

WARNING
This function should be used with caution as it leads to possible “wrong” configurations.

Hub & Spoke allows a satellite LAN’s hosts using VBox Agency or NETASQ Firewall appliances to access LANs from other satellite sites and/or from the outside, all through a tunnel with the central site. The NETASQ Firewall therefore analyzes all the traffic.

Certificates

It is possible to automatically send the local certificate to the peer by using the "Send certificate" option.

It is possible to automatically retrieve the peer certificate if it does not exist in the local database using the “Send certificate request if there is no local certificate” option.

DPD (Dead Peer Detection)

This menu enables configuring the VPN feature called DPD (Dead Peer Detection). When DPD has been enabled on a peer, the peer will regularly send packets to the other peer, to which the latter peer will respond by signaling its presence. These exchanges are secured via ISAKMP SAs (Phase 1). If it is detected that a peer is no longer responding, the negotiated SAs (Phase 1 and 2) will be destroyed with this SA, and DPD will purge everything.

WARNING
This feature provides stability to the VPN service on NETASQ Firewalls on the condition that the DPD has been correctly configured.

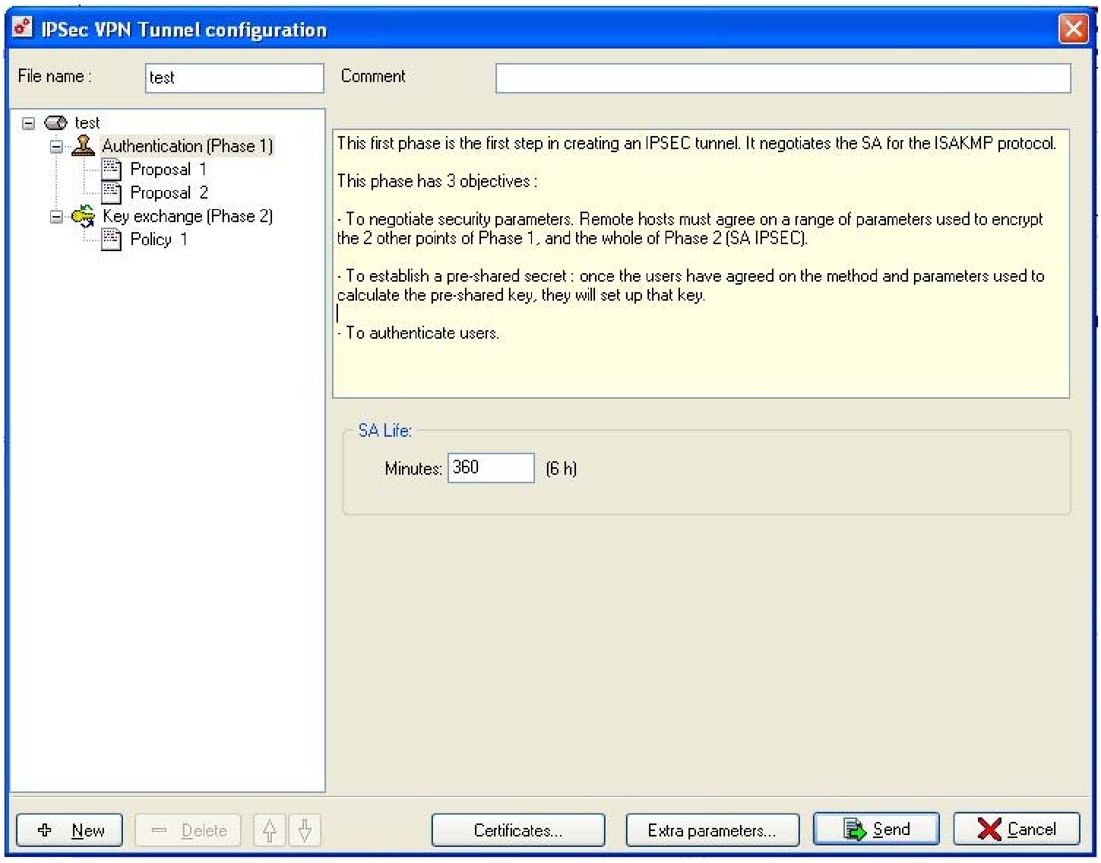
Four choices are available for configuring **DPD**:

- **Passive**: DPD requests sent by the peer get a response from the firewall. However, the firewall does not send any.
- **High and Low**: These are two profiles pre-configured for the use of DPD. They differ in the frequency with which DPD packets are sent and in the number of failures after which the peer is considered inactive. In “High”, the frequency is high and the number of failures is low, whereas for “Low”, the frequency is low and the number of failures tolerated is higher.
- **Manual**: this requires configuring DPD manually according to the following parameters:
  - The first parameter, **Delay** corresponds to a waiting period before the next check for the presence of the peer that has responded to a DPD request.

  - The second parameter, **Retry**, corresponds to a waiting period before the next check for the presence of the peer that has not responded to a DPD request.

- The last parameter, **Max fail**, corresponds to the number of failures when checking for the presence of the peer, after which it is considered that there is no longer a peer. SAs will then be deleted.

General authentication parameters (IKE Phase 1)



File name : test

Comment

This first phase is the first step in creating an IPSEC tunnel. It negotiates the SA for the ISAKMP protocol.

This phase has 3 objectives :

- To negotiate security parameters. Remote hosts must agree on a range of parameters used to encrypt the 2 other points of Phase 1, and the whole of Phase 2 (SA IPSEC).

- To establish a pre-shared secret : once the users have agreed on the method and parameters used to calculate the pre-shared key, they will set up that key.

- To authenticate users.

SA Life:

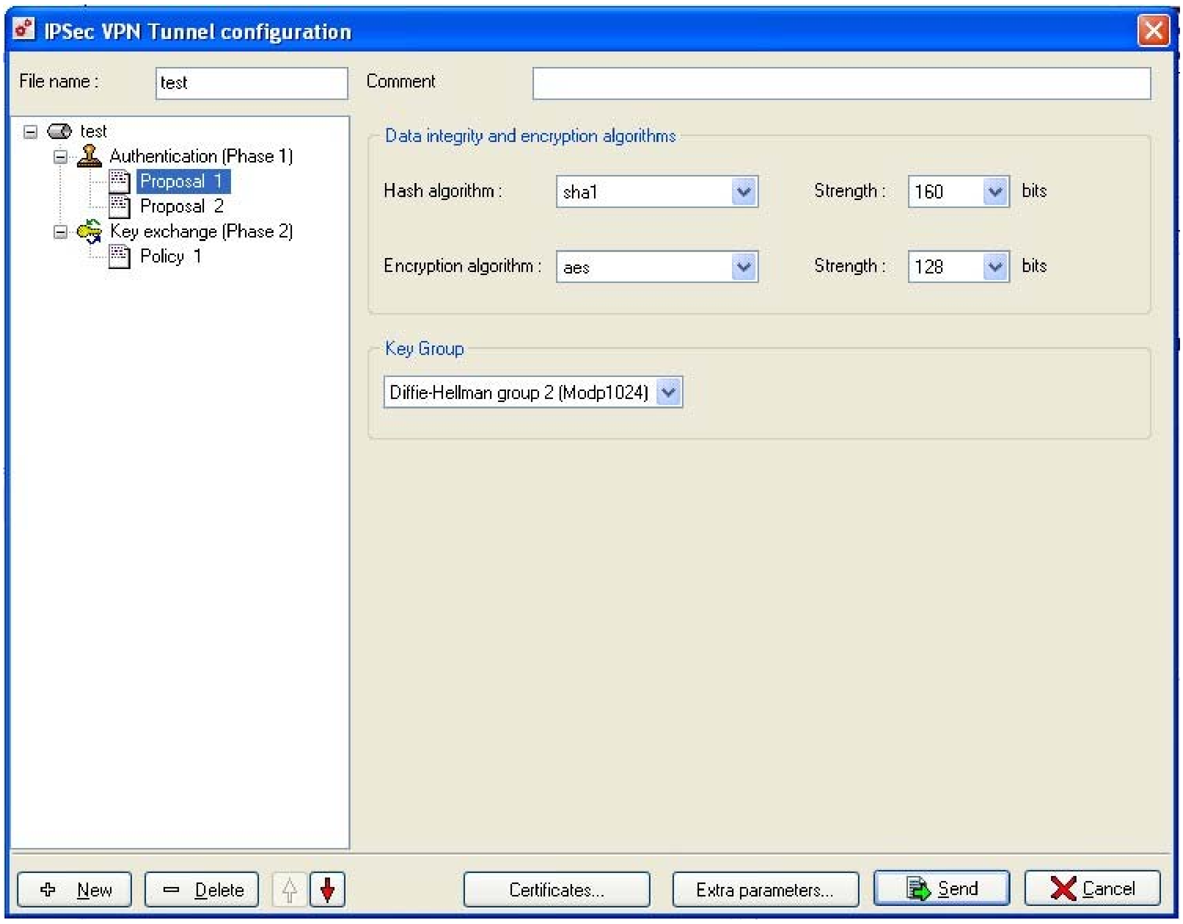
Minutes: 360 (6 h)

Figure 220: Configuring IPSec VPN tunnels – SA lifetime

The general parameters of Phase 1 are:

SA Life	Period of time, beyond which Phase 1's elements will be renegotiated. By default, the period is 360 minutes.

Algorithms supported for Phase 1 of this tunnel



IPSec VPN Tunnel configuration

File name : test

Comment :

Data integrity and encryption algorithms

Hash algorithm : sha1 Strength : 160 bits

Encryption algorithm : aes Strength : 128 bits

Key Group

Diffie-Hellman group 2 (Modp1024)

Figure 221: Configuring IPSec VPN tunnels – Phase 1 algorithms

The proposals match the various authentication and encryption algorithms the Firewall supports in Phase 1 for this tunnel. If a remote host wants to establish Phase 1 of the IPSEC protocol, at least one of these proposals must be shared with the Firewall.

You can establish several proposals for a single tunnel.

The proposal's parameters are:

Hash algorithm Algorithm used to guarantee data integrity. NETASQ Firewalls support the following hash functions:

- SHA1 (160 bits)
- MD5 (128 bits)
- Sha2_256
- Sha2_384
- Sha2_512

Encryption algorithm:	Algorithm used to encrypt data. NETASQ Firewalls offer the following: ● DES ● 3DES ● BLOWFISH ● CAST128 ● AES **WARNING** NETASQ strongly recommends that you use AES as security-wise and throughput-wise, it is the most powerful algorithm. It is pertinent to note that the algorithms set out above do not have the same performance and throughput. AES is currently the best encryption algorithm.
Key Group:	Method used to calculate the keys. In aggressive mode, this method is shared by all proposals and is chosen in Phase 1's general parameters. ● Diffie-Hellman group 1 (Modp768) ● Diffie-Hellman group 2 (Modp 1024) ● Diffie-Helman group 5 (Modp 1536)

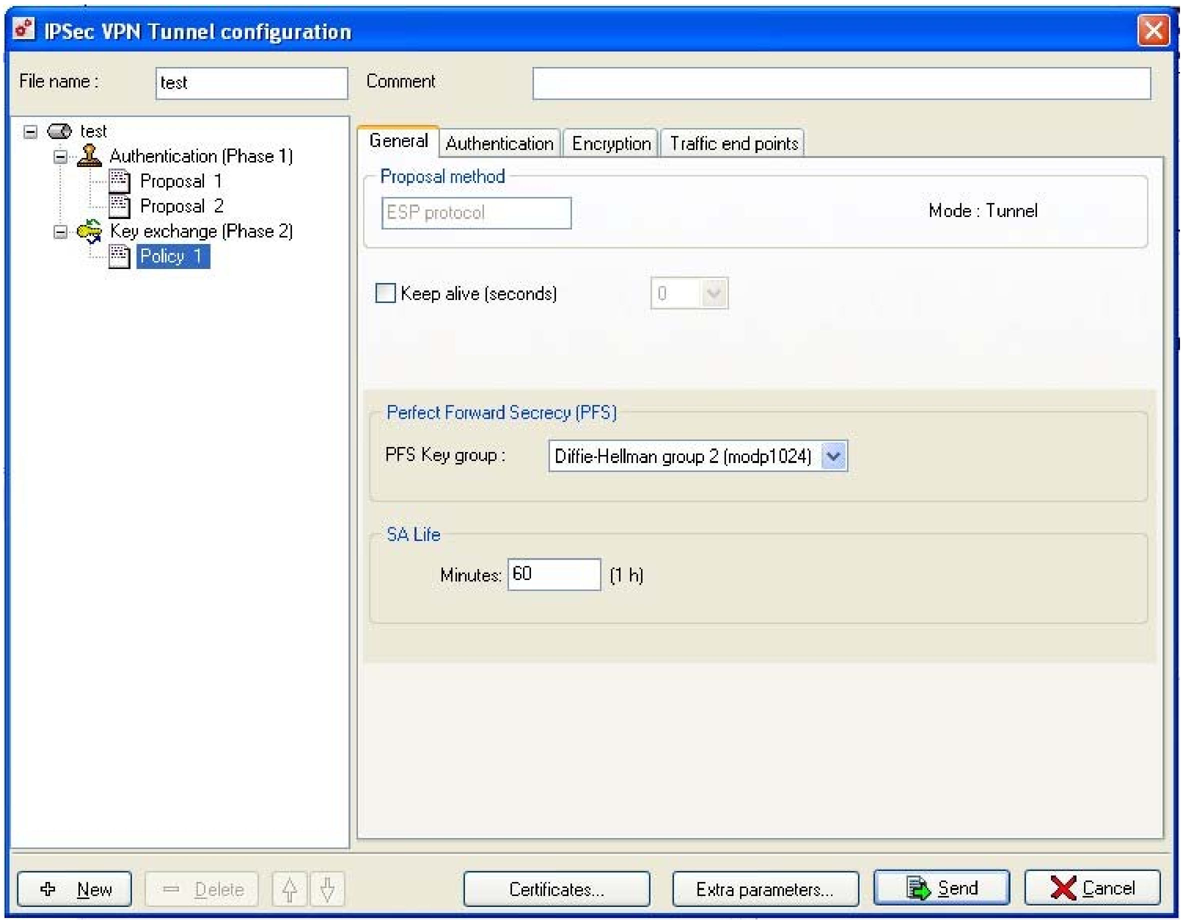
General key exchange parameters (IKE Phase 2)

In this phase, exchanges are authenticated and encrypted with symmetrical secret keys, which have been negotiated in Phase 1 (SA ISAKMP).

3 objectives:

1) **Negotiation of security parameters**: peers agree on the values of certain parameters concerning the IPSec tunnel. Traffic endpoints will be checked.
2) **Key generation for IPSec**: by using the SA negotiated in Phase 1, peers agree on the keys to be used in the IPSec tunnel.
3) **Anti-replay protection:** Replay of IPSec packets is prevented. This protection is configured in Phase 2 of the negotiation.

General tab



IPSec VPN Tunnel configuration

File name : test

Comment

Proposal method: ESP protocol

Mode : Tunnel

□ Keep alive (seconds) 0

Perfect Forward Secrecy (PFS)

PFS Key group : Diffie-Hellman group 2 (modp1024)

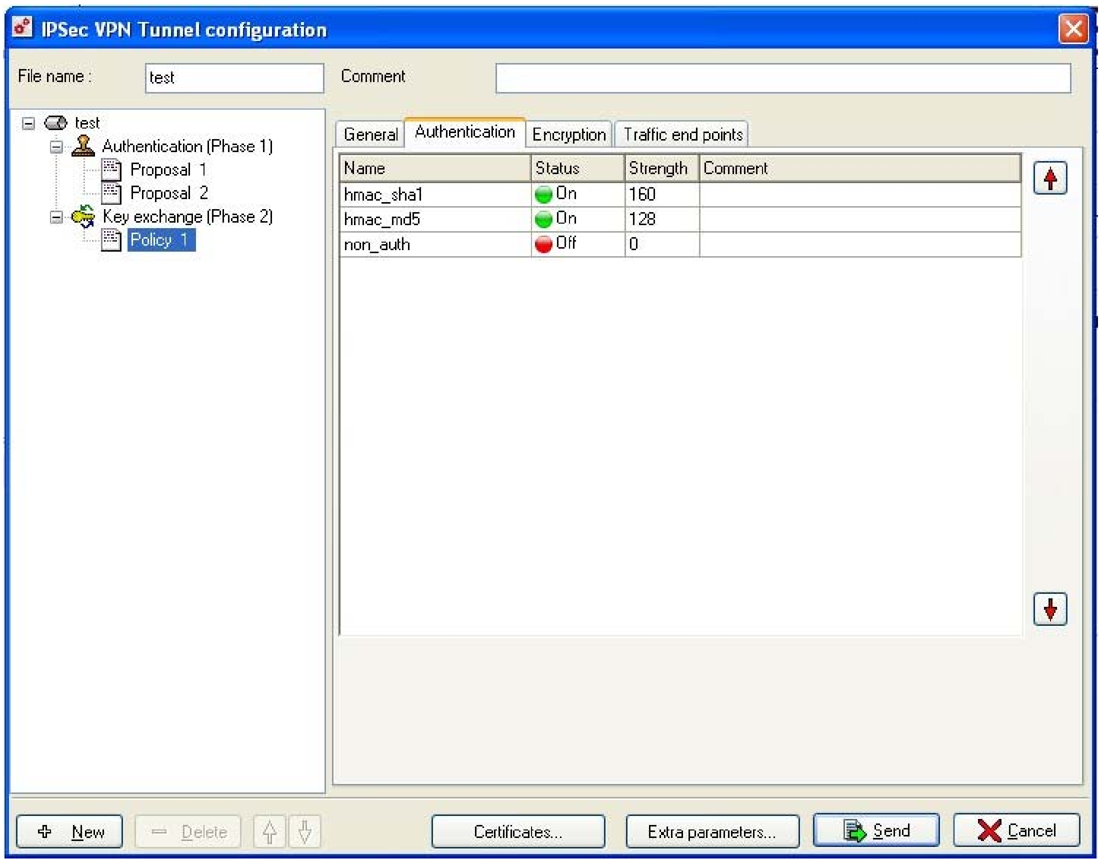
SA Life

Minutes: 60 (1 h)

Figure 222: Configuring IPSec VPN tunnels - General

Proposal method	Selection of the IPSEC protocols used in the tunnel: ● ESP protocol (encryption)
Keep alive (seconds)	Time elapsed in seconds between the sending of two packets through a VPN tunnel in order to keep the tunnel alive. These packets sent are only used for keeping this tunnel alive.
Perfect Forward Secrecy	Guarantees that there is no link between the different keys of each session. The Diffie-Hellman algorithm selected recalculates keys. The higher the number (none, 1, 2 or 5), the higher the level of security. 2 is the most widely-used PFS level.
SA lifetime	Period of time beyond which keys will be renegotiated. The default period is 60 minutes.

Authentication tab



Name	Status	Strength	Comment
hmac_sha1	● On	160	
hmac_md5	● On	128	
non_auth	● Off	0	

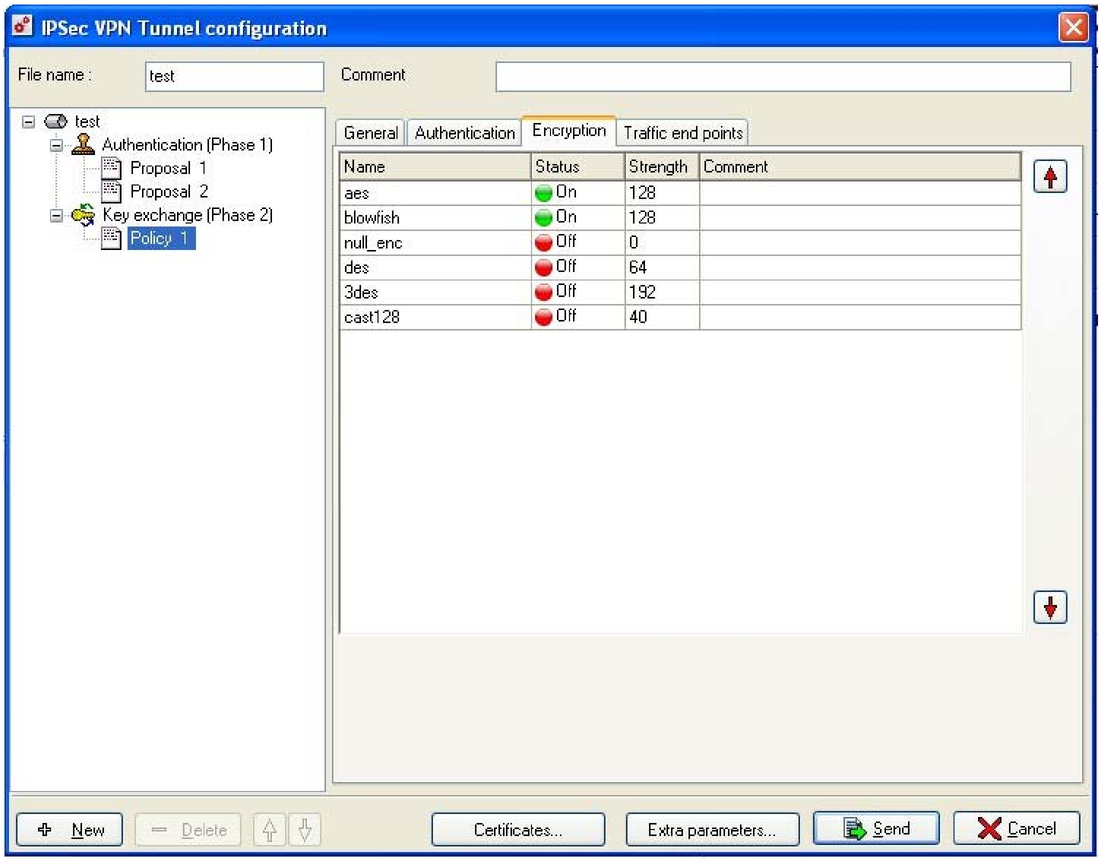
Figure 223: Configuring IPSec VPN tunnels – Authentication

The **`Authentication`** tab allows you to select the authentication algorithms accepted by this proposal.

The Firewall supports the following algorithms:

- No authentication
- HMAC-SHA1
- HMAC-MD5

Encryption tab



Name	Status	Strength	Comment
aes	● On	128	
blowfish	● On	128	
null_enc	● Off	0	
des	● Off	64	
3des	● Off	192	
cast128	● Off	40	

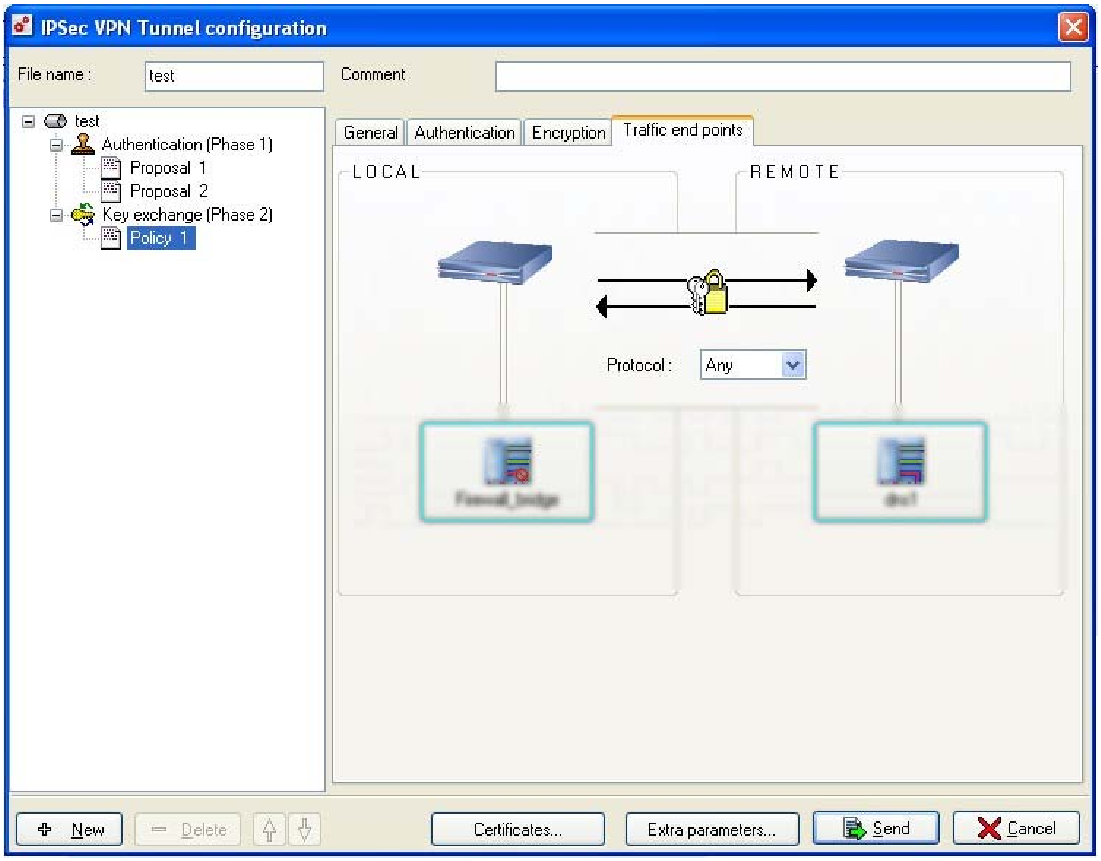
Figure 224: Configuring IPSec VPN tunnels – Encryption

The **Encryption** tab allows you to select the encryption algorithms accepted by this proposal:

The Firewall supports the following algorithms:

- No_enc
- DES
- 3DES
- BLOWFISH
- CAST128
- AES

Traffic endpoints tab



IPSec VPN Tunnel configuration

File name : test

Comment

Protocol : Any

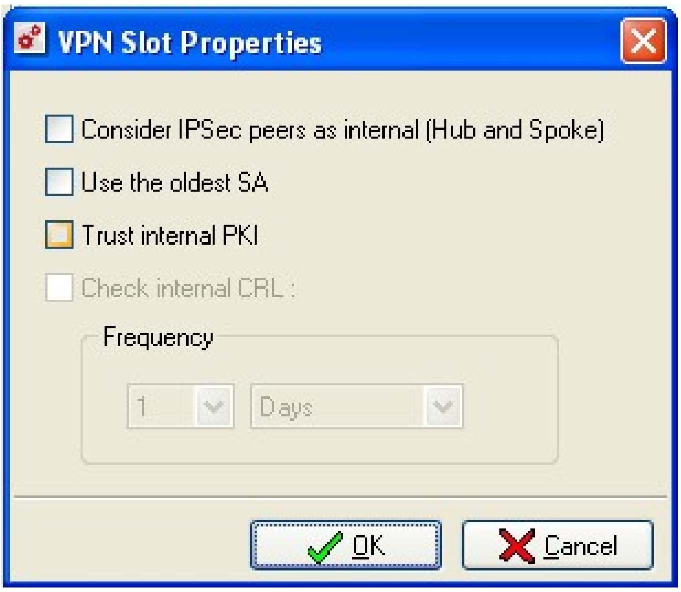
Figure 225: Configuring IPSec VPN tunnels – Traffic endpoints

This section allows you to define which local users will use the tunnel, and if required, for which protocols.

Select the remote hosts or networks from the list of declared objects and, if required, a particular protocol to be encrypted.

Extra parameters

- Click on **Extra parameters** in the VPN configuration window:



VPN Slot Properties

□ Consider IPSec peers as internal (Hub and Spoke)

□ Use the oldest SA

□ Trust internal PKI

□ Check internal CRL :

Frequency: 1 Days

Figure 226: Properties of the VPN slot

This menu allows managing extra parameters for an IPSEC tunnel. These parameters are available for either static or dynamic tunnels.

This is where the selected tunnel's general behavior is configured.

Consider IPSEC peers as internal
By checking this option, IPSEC interfaces will be considered as internal interfaces. Therefore, they will be "protected" like all internal interfaces. This option is necessary especially for Hub & Spoke configuration.

Use the oldest SA
When SAs are renewed, the old and new SAs will coexist for some time. By default, an IPSec peer has to use the most recent SA (newly negotiated). Selecting the option "Use the oldest SA" means that the oldest SA will be used until its expiry. The aim of this option is to make the firewall interoperable with implementations that use SAs until their expiry.

WARNING
This feature should be used only when strictly necessary.

Trust internal PKI
When you use a VPN tunnel with digital certificates and this option has been selected, it will allow you to compare IPSec peer certificates against the firewall's internal PKI.

Check internal CRL
Select this option in order to define the update frequency of the certificate revocation list (CRL). It is possible to conduct regular checks, you only need to configure the time base (in minutes, hours, days or months).

The shorter the period, the more often the Firewall will have to check the CRL when this tunnel is active. Do not set value which is too short (performance lowered) or too long (risk of using an obsolete CRL). The period has to be coherent with the issuance frequency of the CRL.

Certificates

➲ Click on **Certificates**:

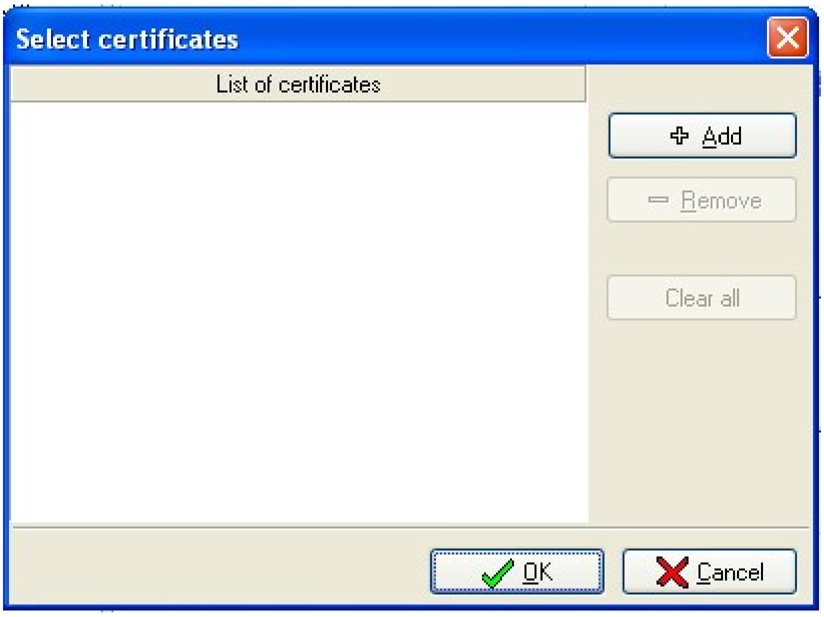


Figure 227: Selecting certificates

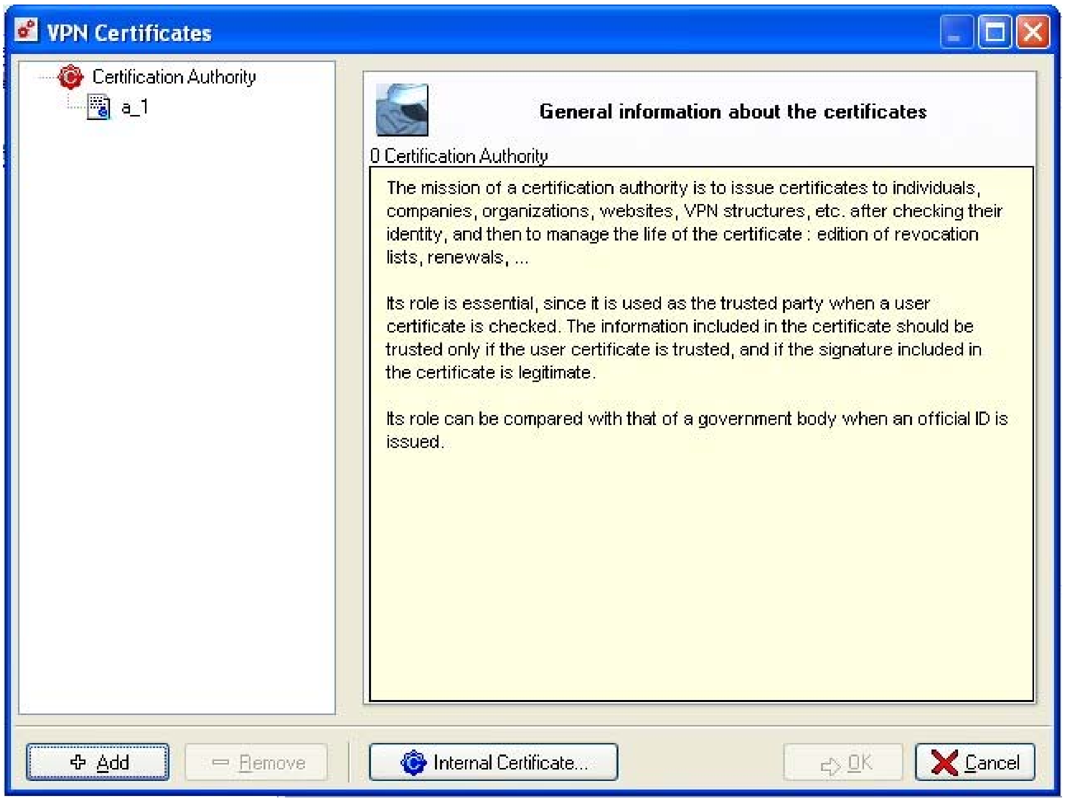
When certificates from external certification authorities are inserted into the list of certificates, the Firewall will automatically recognize as valid all user certificates signed by these certification authorities.

In order to use these recognized certification authorities, the list of certification authorities that have to be validated for this VPN configuration slot must be specified in VPN policy configuration, in the “Certificate” menu (of the VPN tunnel general configuration panel). This list of certification authorities is specific to the configured slot even though the global list of all certification authorities that the administrator has allowed, can be found in a single location – the “Certificates” configuration menu in the NETASQ UNIFIED MANAGER menu directory.

The procedure for adding a certification authority to the list of recognized authorities for the configured VPN slot, is as follows:

1 Click on **Certificates** in the VPN tunnel general configuration panel.

2 Click on **Add** in the certificate configuration panel. The following window will appear:



0 Certification Authority

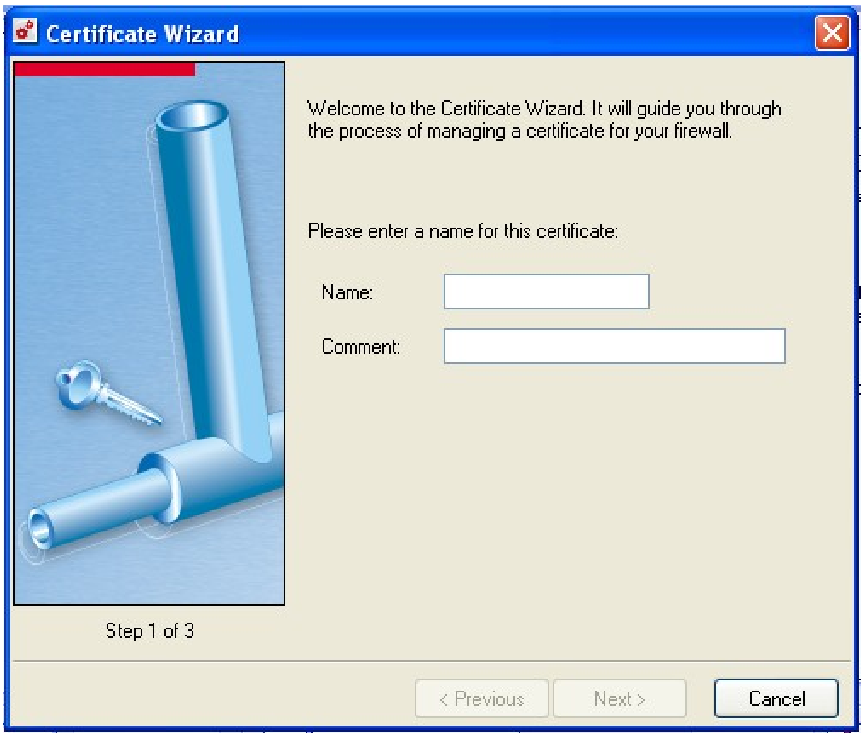
The mission of a certification authority is to issue certificates to individuals, companies, organizations, websites, VPN structures, etc. after checking their identity, and then to manage the life of the certificate : edition of revocation lists, renewals, ...

Its role is essential, since it is used as the trusted party when a user certificate is checked. The information included in the certificate should be trusted only if the user certificate is trusted, and if the signature included in the certificate is legitimate.

Its role can be compared with that of a government body when an official ID is issued.

Figure 228: VPN Certificates

3 Click on **Add**. The following window will appear:



Welcome to the Certificate Wizard. It will guide you through the process of managing a certificate for your firewall.

Please enter a name for this certificate:

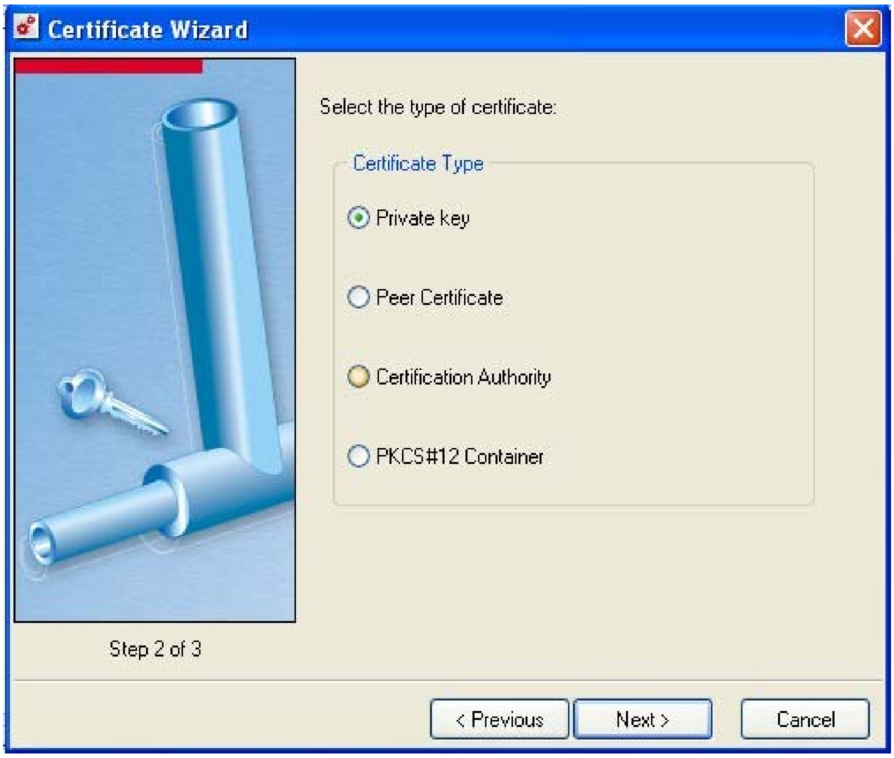
Name:

Comment:

Figure 229: Certificate wizard - Step 1

4 Name the certificate and enter a description.

3 Click on **Next**. The following window will appear:



Select the type of certificate:

Certificate Type

● Private key

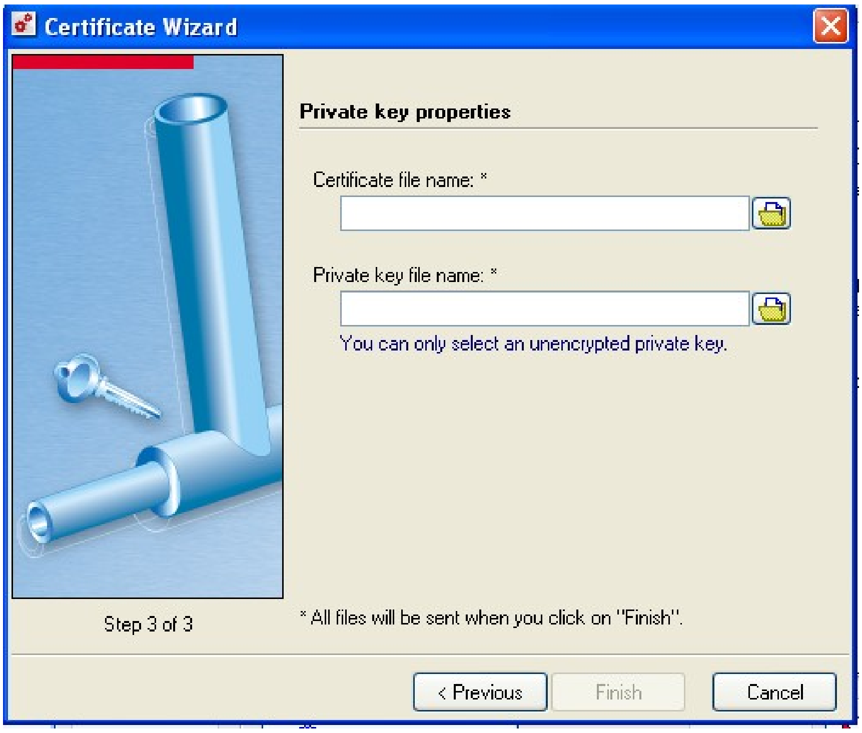
○ Peer Certificate

○ Certification Authority

○ PKCS#12 Container

Figure 230: Certificate wizard - Step 2

5 Select the type of certificate then click on **Next**. The following window will appear:



Private key properties

Certificate file name: *

Private key file name: *

You can only select an unencrypted private key.

* All files will be sent when you click on "Finish".

Figure 231: Certificate wizard - Step 3

Select the files.

6 Lastly, confirm the addition of these certificates by sending the VPN slot configuration.

8.3.4. Filter rules

After configuring the VPN tunnel(s), a set of rules have to be defined, enabling the establishment of the tunnel(s) and the transmission of encrypted information. Two actions have to be performed for this to be done:

- Activation of implicit VPN rules.
- Edition of filter rules for allowing traffic through the IPSEC tunnel.

8.3.4.1. Activating implicit VPN rules

NETASQ Firewalls can automatically generate filter rules to establish VPN tunnels, therefore the administrator does not need to define the rules explicitly when editing filter slots.

➲ Implicit rules are activated using the menu **`Policy\Implicit rules`**.

Activate the option **VPN services** then click on **OK**.

WARNING
Implicit rules are only generated for Gateway to Gateway IPSEC tunnels. For anonymous tunnels, rules have to be defined explicitly in the filter slots.

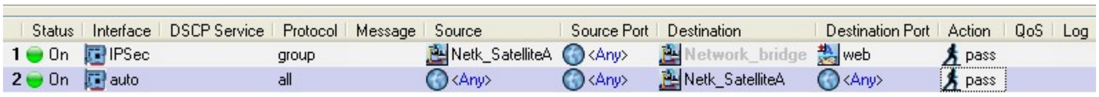
For anonymous tunnels, you need to configure the following explicit rules:

Status	Protocol	Source	Destination	Destination port	Action
On	UDP	Any	Firewall_out	isakmp	Pass
On	Vpn-esp	Any	Firewall_out		Pass
On	Vpn-esp	Firewall_out	Any		Pass

In this example, the address range used by the nomad VPN clients is unknown, therefore the object "ANY" is used. If the address range used by nomad clients is known (address range of the access provider, for example), then you are advised to limit the rules to this address range.

8.3.4.2. Editing filter rules

Without explicit filter rules for traffic passing through an IPSEC VPN tunnel, no traffic will be able to pass through this tunnel (even if the tunnel is already active). To allow traffic through the Firewall, you need to add filter rules such as those in the following example:



	Status	Interface	DSCP Service	Protocol	Message	Source	Source Port	Destination	Destination Port	Action	QoS	Log
1	On	IPSec		group		Netk_SatelliteA	<Any>	Network_bridge	web	pass		
2	On	auto		all		<Any>	<Any>	Netk_SatelliteA	<Any>	pass		

Figure 232: Editing filter rules

> **Example**
> Hosts from the remote network (Netwk_SatelliteA) have access to hosts in the internal network (Network_bridge) for WEB services. Hosts in the internal network (Network_bridge) have access to all hosts on the remote network for all services (Netwk_SatelliteA).

WARNING

Filter rules which apply to traffic coming from the remote network have to use the selected “IPSEC” interface. Filter rules which apply to traffic going to the remote network have to use the selected “Auto” interface.

8.3.5. Gateway to gateway VPN tunnels

In this section, several basic VPN tunnel configurations are touched upon. In particular, it describes:

- The creation of a G2G tunnel with pre-shared key.
- The creation of a G2G tunnel with certificates.
- The creation of a static G2G VPN tunnel (this configuration type, now obsolete, is only supported for compatibility reasons).

8.3.5.1. IPSec VPN Tunnel with pre-shared keys

The following example illustrates the configuration necessary for establishing a gateway-to-gateway VPN tunnel with pre-shared keys.

DEFINITION
VPN tunnels established between two VPN-compatible network elements which act as endpoints from a gateway (essentially Firewall to Firewall) are called **Gateway-to-gateway VPN tunnels**.

The following diagram represents this architecture:

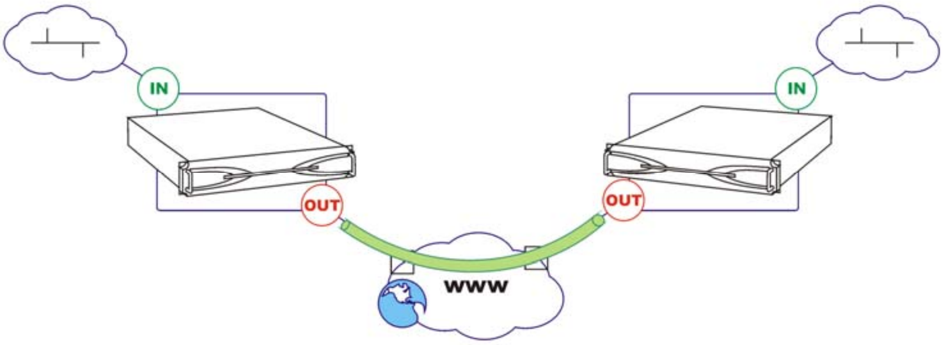


Figure 233: IPSec VPN tunnel with pre-shared keys

Tunnel configuration

In order to configure the tunnel, select the VPN slot in which you wish to establish the tunnel. The VPN wizard will then guide you along in the VPN configuration.

This configuration has to be performed on each Firewall participating in the VPN tunnel. However, don’t forget to invert the traffic and tunnel endpoints.

The first screen in the VPN wizard will appear. Select a name you wish to assign to this tunnel (the slot name will automatically be assigned the same name but you will be able to modify it later). Click on **Next** to continue configuring.

In Step 2 of the VPN wizard, select the tunnel type you wish to establish (for example, dynamic with pre-shared keys here). Click on **Next**.

Steps 3 and 4 enable specifying the different network elements at the tunnel endpoints first then the traffic endpoints flowing inside the VPN tunnel.

> ❗ WARNING
> In the example, “Firewall_out” is used as the tunnel endpoint. If your Firewall is directly connected to a modem, you have to use the dialup interface which corresponds to your active internet connection.

Once the endpoints have been defined, click on **Next** to end the tunnel configuration. A general window will give you a quick roundup of the configuration defined in the wizard. You can modify this configuration before sending the specified VPN configuration to the Firewall.

> ❗ WARNING
> To negotiate a VPN tunnel, it has to possess a valid default gateway (even during a test phase).
>
> Don’t forget to perform the necessary filtering on VPN traffic from Firewalls participating in the tunnel.

Pre-shared key configuration

Please refer to the chapter *Part 8/Chapter 2: Pre-shared keys*.

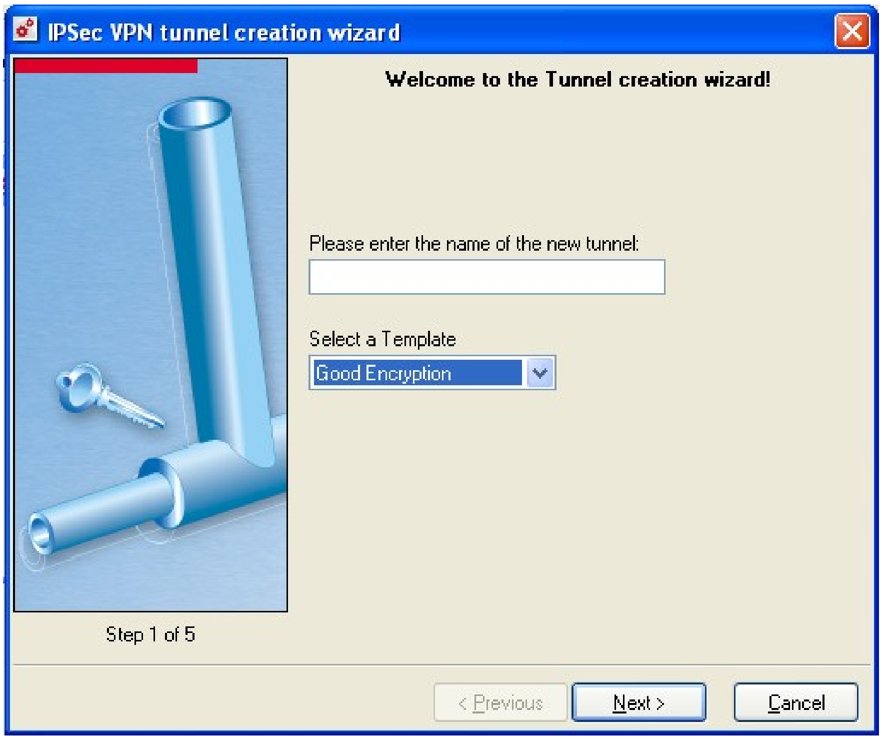
8.3.5.2. IPSec VPN Tunnel with certificates

Tunnel configuration

In order to configure the tunnel, select the VPN slot in which you wish to establish the tunnel. The VPN wizard will then guide you along in the VPN configuration.

This configuration has to be performed on each Firewall participating in the VPN tunnel. However, don’t forget to invert the traffic and tunnel endpoints.

1 Step 1



Welcome to the Tunnel creation wizard!

Please enter the name of the new tunnel:

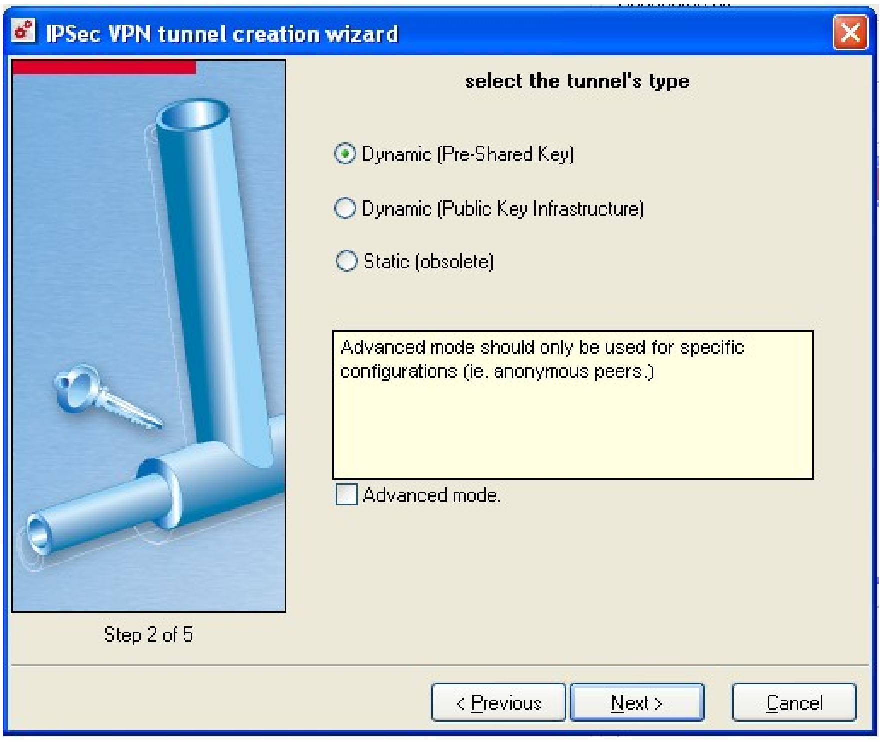
Select a Template: Good Encryption

Step 1 of 5

Figure 234: Creating IPSec tunnels - Step 1

The first step in creating a tunnel is to select a name you wish to assign to this tunnel (the slot name will automatically be assigned this name but you will be able to modify it later). Click on **Next** to continue configuring.

2 Step 2



select the tunnel's type

● Dynamic (Pre-Shared Key)

○ Dynamic (Public Key Infrastructure)

○ Static (obsolete)

Advanced mode should only be used for specific configurations (ie. anonymous peers.)

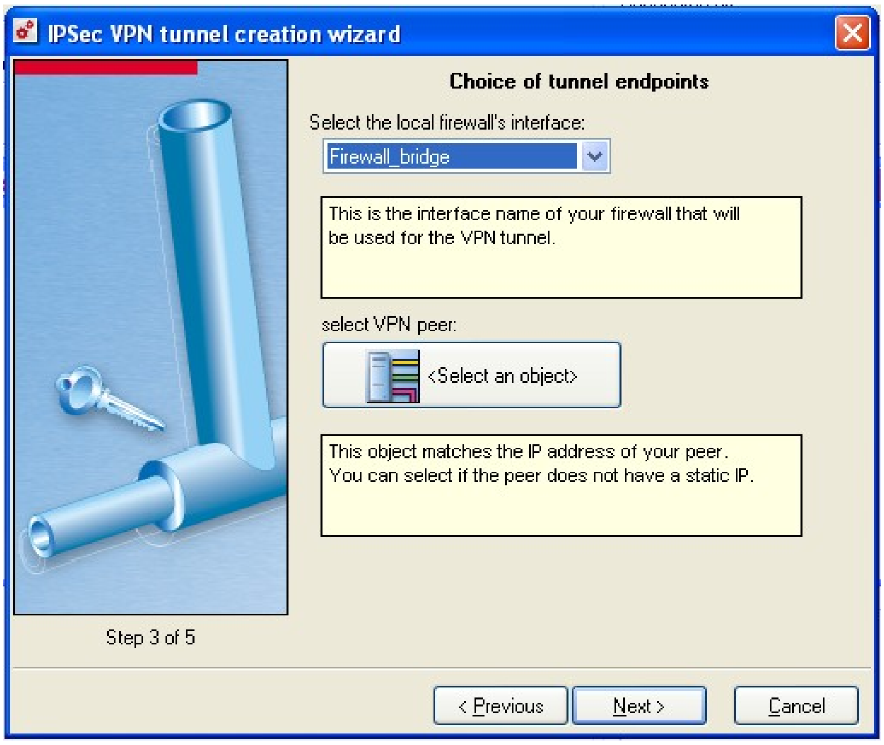
□ Advanced mode.

Step 2 of 5

Figure 235: Creating IPSec tunnels - Step 2

In Step 2 of the VPN wizard, select the tunnel type you wish to establish (for example, dynamic with certificates here). Click on **Next**.

3 Step 3



Choice of tunnel endpoints

Select the local firewall's interface:

Firewall_bridge

This is the interface name of your firewall that will be used for the VPN tunnel.

select VPN peer:

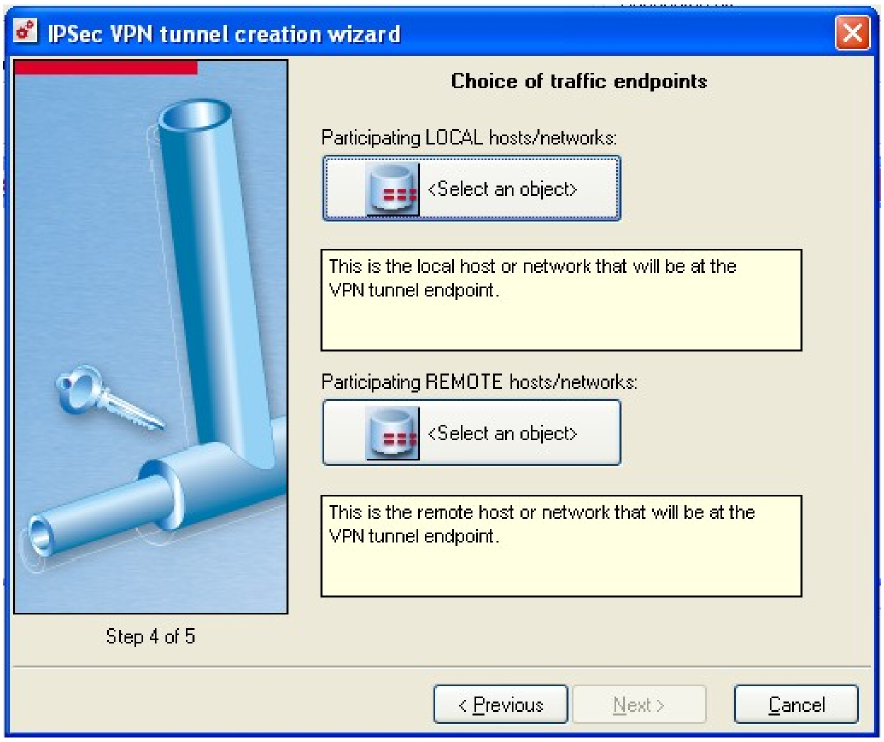
<Select an object>

This object matches the IP address of your peer. You can select if the peer does not have a static IP.

Step 3 of 5

Figure 236: Creating IPSec tunnels - Step 3

4 Step 4



Choice of traffic endpoints

Participating LOCAL hosts/networks:

<Select an object>

This is the local host or network that will be at the VPN tunnel endpoint.

Participating REMOTE hosts/networks:

<Select an object>

This is the remote host or network that will be at the VPN tunnel endpoint.

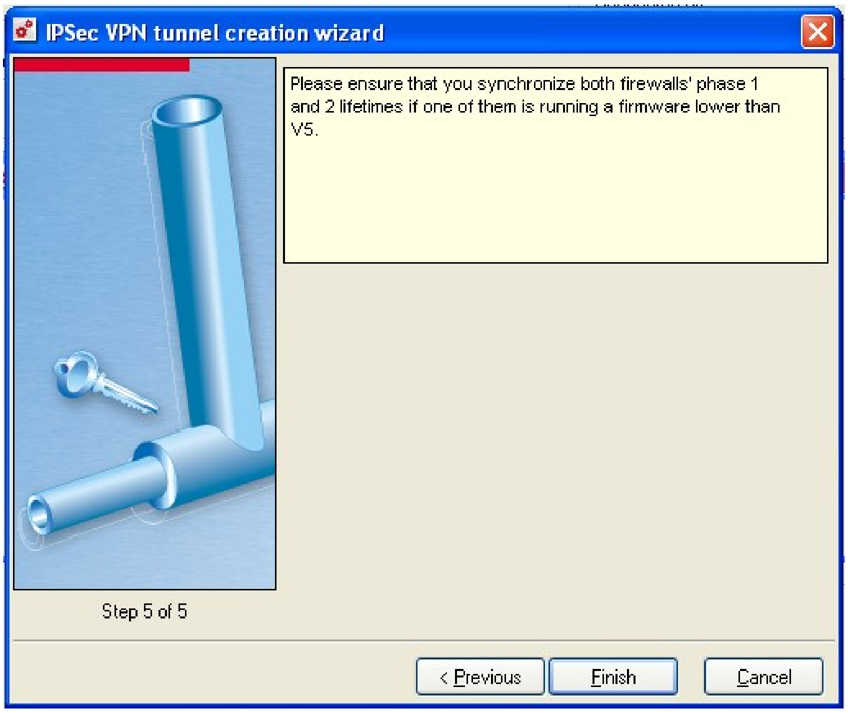
Step 4 of 5

Figure 237: Creating IPSec tunnels - Step 4

Steps 3 and 4 enable specifying the different network elements at the tunnel endpoints first then the traffic endpoints flowing inside the VPN tunnel.

WARNING
In the example, “Firewall_out” is used as the tunnel endpoint. If your Firewall is directly connected to a modem, you have to use the dialup interface which corresponds to your active internet connection.

Step 5



Please ensure that you synchronize both firewalls' phase 1 and 2 lifetimes if one of them is running a firmware lower than V5.

Figure 238: Creating IPSec tunnels - Step 5

Once the endpoints have been defined, click on **Next** to end the tunnel configuration. A general window will give you a quick roundup of the configuration defined in the wizard.

WARNING
To negotiate a VPN tunnel, it has to possess a valid default gateway (even during a test phase).

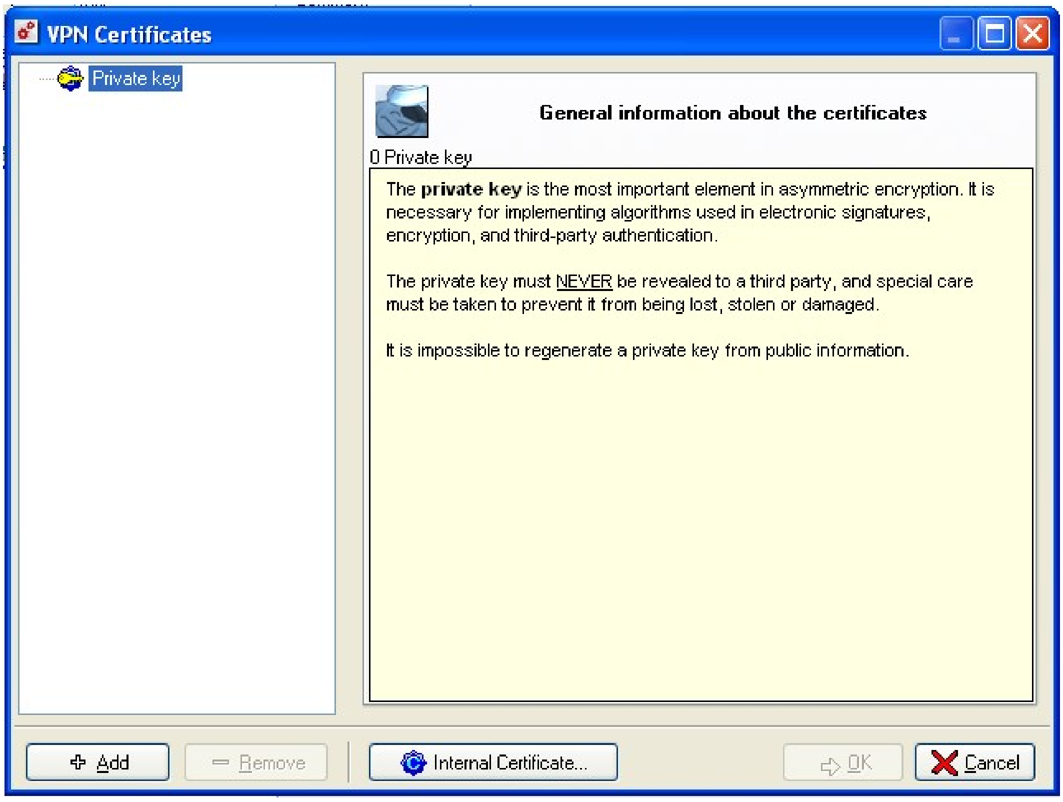
Don’t forget to perform the necessary filtering on VPN traffic from Firewalls participating in the tunnel.

Certificate configuration

After tunnel configuration, you are advised to configure certificates. In the “PKI Certificates” section of the IPSEC VPN tunnel configuration, click on **Select a certificate.**

You will then be able to generate a digital certificate for the Firewall. In order to do this, click on **Internal certificate**, then on **Create a VPN certificate** and indicate the Firewall’s CA password. Once it has been generated, the certificate will appear in the “Private key” section.

Only one certificate can be generated.



General information about the certificates

0 Private key

The **private key** is the most important element in asymmetric encryption. It is necessary for implementing algorithms used in electronic signatures, encryption, and third-party authentication.

The private key must NEVER be revealed to a third party, and special care must be taken to prevent it from being lost, stolen or damaged.

It is impossible to regenerate a private key from public information.

Figure 239: VPN certificates

WARNING
Certificates can only be generated when the internal PKI service has been configured and is active on the Firewall.

Advanced configuration with certificates

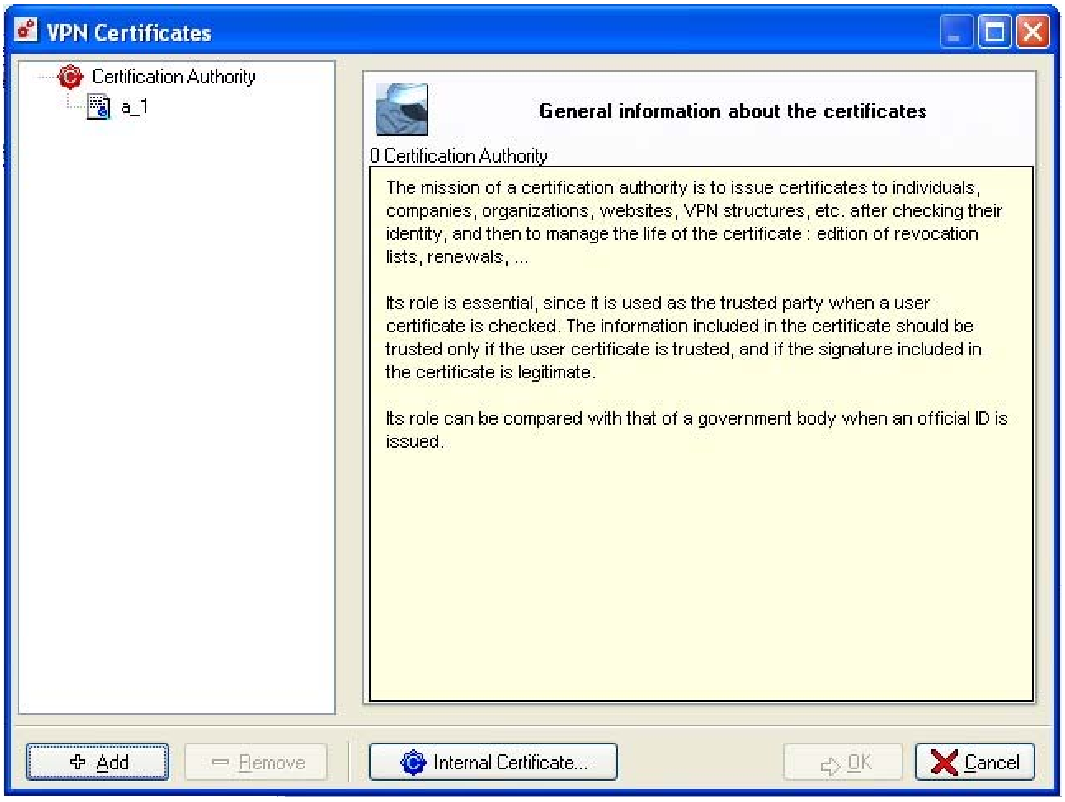
If the peer is a mobile client, you can define his certificate in the user form by using the IPSEC client. (*Cf. Part 4/Chapter 3: Objects\Users*).

If the peer is another VPN gateway:

- You can export your internal CA into the other Firewall (*Cf. Part 12: Authentication*) and import the remote Firewall's CA into the "Certification Authority" section (in a crisscross manner).
- You can define the remote Firewall as a user. In this case, you have to add a user form (*Cf. Part 4/Chapter 3: Objects\Users*) for the remote Firewall and generate the certificate. You have to save this certificate and import it into the "Private keys and certificates" section of the remote Firewall.

Integrating the VPN architecture into an external PKI

The NETASQ Firewall can integrate certificates coming from an external PKI. These certificates therefore have to be imported at the Firewall level. Before importation, the VPN Certificates window only contains the Firewall's certificate.



VPN Certificates

Certification Authority

a_1

General information about the certificates

0 Certification Authority

The mission of a certification authority is to issue certificates to individuals, companies, organizations, websites, VPN structures, etc. after checking their identity, and then to manage the life of the certificate : edition of revocation lists, renewals, ...

Its role is essential, since it is used as the trusted party when a user certificate is checked. The information included in the certificate should be trusted only if the user certificate is trusted, and if the signature included in the certificate is legitimate.

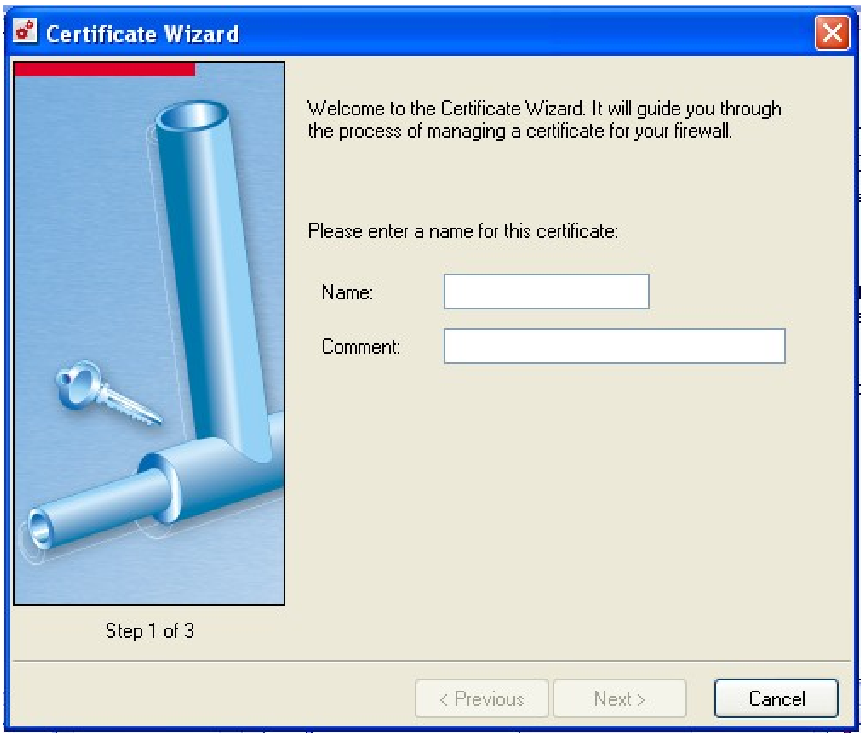
Its role can be compared with that of a government body when an official ID is issued.

Figure 240: VPN Certificates – Certificate authority

The left column displays three types of certificates. When you select a certificate type, an explanation on the key type will appear.

To add a certificate coming from an external PKI, the procedure is as follows:

1 Click on **Add**. A certificate wizard will appear, allowing you to enter a name for the certificate.



Certificate Wizard

Welcome to the Certificate Wizard. It will guide you through the process of managing a certificate for your firewall.

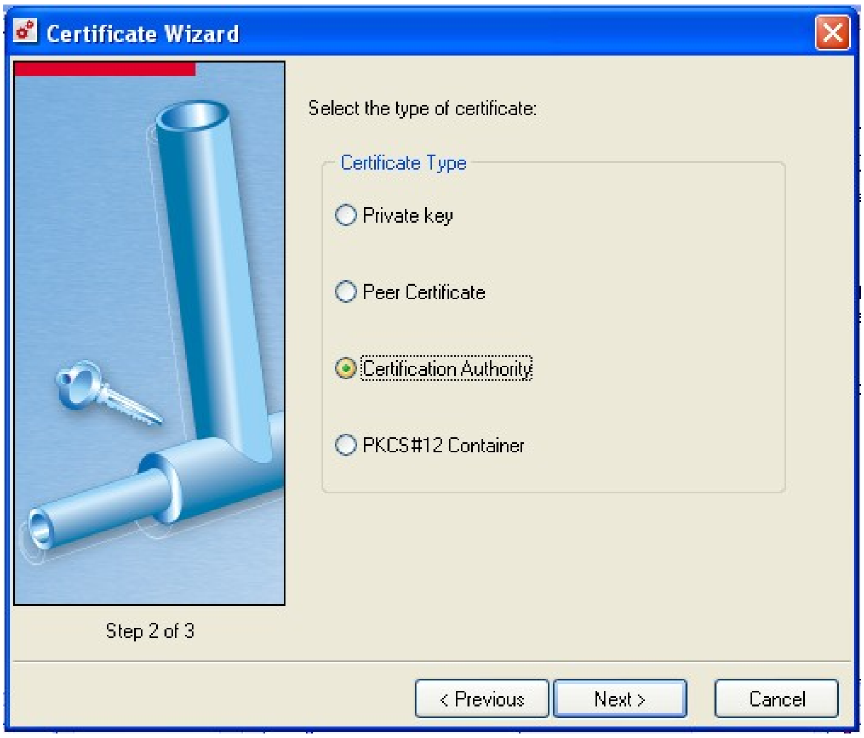
Please enter a name for this certificate:

Name:

Comment:

Figure 241: Certificate wizard - Step 1

2 The second step allows you to select the certificate type.



Select the type of certificate:

Certificate Type

○ Private key

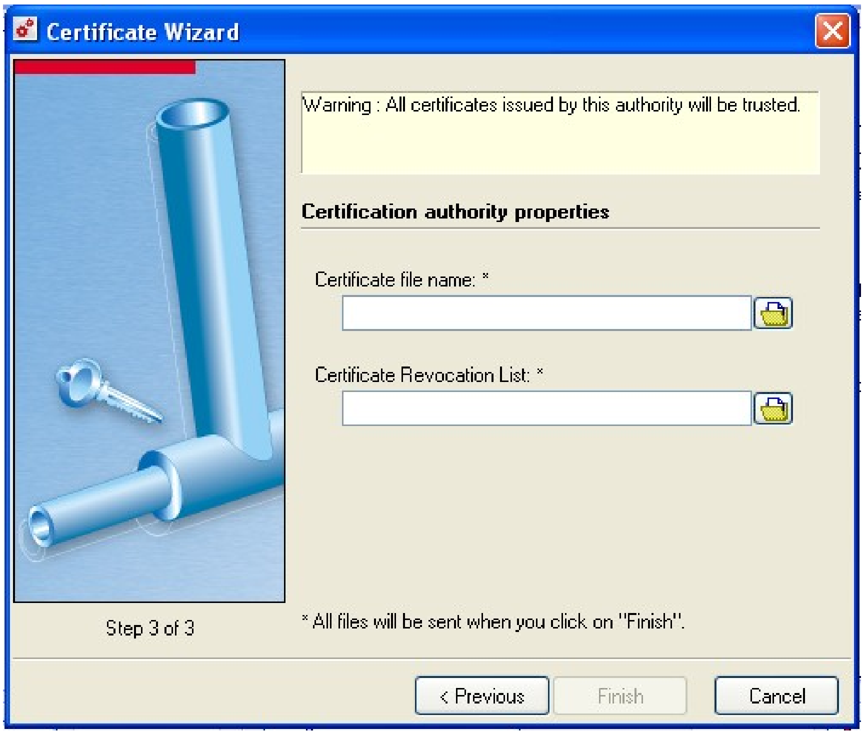
○ Peer Certificate

● Certification Authority

○ PKCS#12 Container

Figure 242: Certificate wizard - Step 2

3 The second step allows you to select the certificate type.



Warning : All certificates issued by this authority will be trusted.

Certification authority properties

Certificate file name: *

Certificate Revocation List: *

* All files will be sent when you click on "Finish".

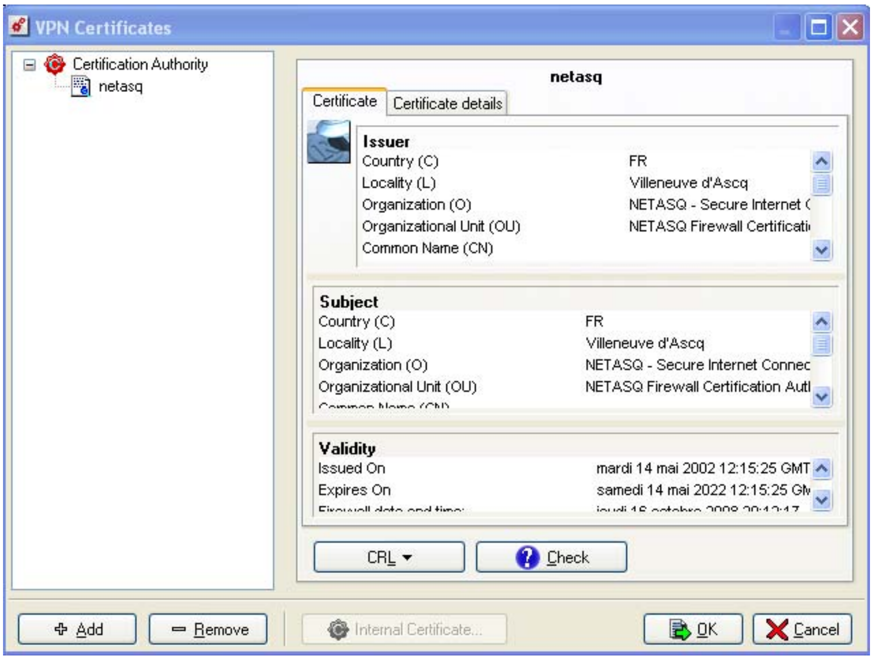
Figure 243: Certificate wizard - Step 3

Depending on the type of certificate, the certificate wizard will require different file types during the third step.

- The choice **Private keys** makes it possible to load the certificate (in *.cer, *.der or *.pem) and the private key (in *.key or *.pem unencrypted, i.e., in plaintext) in two different files.
The Firewall tests to see if the certificate corresponds to the private key.
- The choice **Peer Certificate** makes it possible to load the certificate (in *.cer, *.der or *.pem)
- **Certification Authority** makes it possible to load the certificate (in *.cer, *.der or *.pem) as well as the certificate revocation list (in *.crl or *.pem)
The use of a revocation list is optional. However, once a file is configured, the list has to be updated once it expires. Otherwise, the certification authority cannot be used.

- **PKCS12 Container** makes it possible to load a PKCS#12 file. A PKCS#12 container contains a private key, public key and certificate. All this information is encrypted by using a password to be specified.

The contents of the certificate may be viewed in the right side of the window by using the **`Certificate`** and **`Certificate Details`** tab.



Issuer

Country (C)	FR
Locality (L)	Villeneuve d'Ascq
Organization (O)	NETASQ - Secure Internet (
Organizational Unit (OU)	NETASQ Firewall Certificati
Common Name (CN)	

Subject

Country (C)	FR
Locality (L)	Villeneuve d'Ascq
Organization (O)	NETASQ - Secure Internet Connec
Organizational Unit (OU)	NETASQ Firewall Certification Autl
Common Name (CN)	

Validity

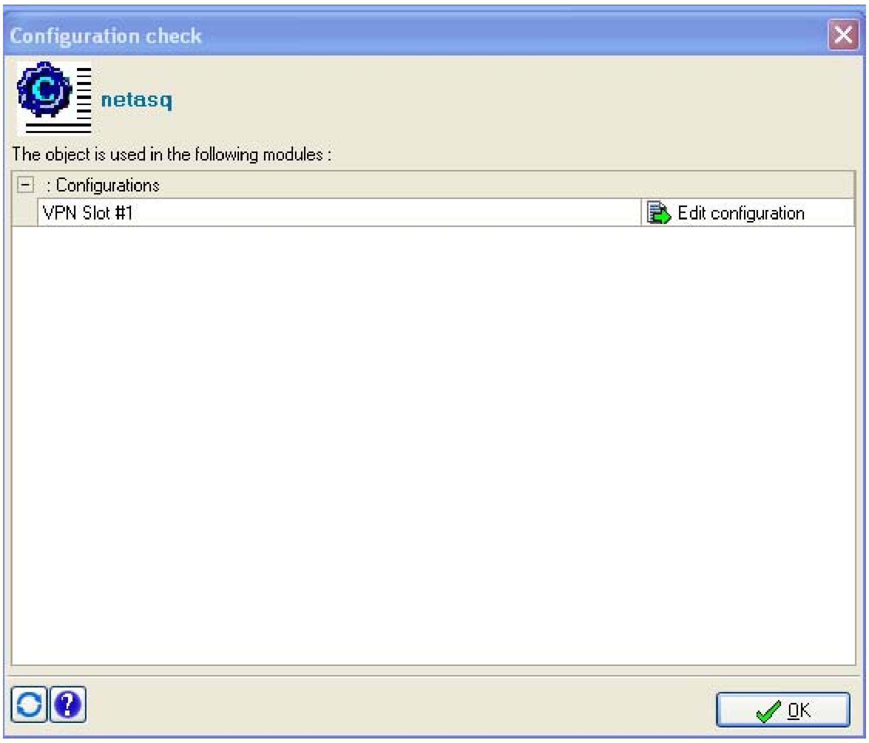
Issued On	mardi 14 mai 2002 12:15:25 GMT
Expires On	samedi 14 mai 2022 12:15:25 GM
Firewall date and time:	jeudi 16 octobre 2008 20:12:17

Figure 244: VPN Certificates - Certificate

REMARK

You will find, among other things, the certificate owner, the certification authority which signed the certificate and the certificate's validity period. If the certificate is no longer valid, it will be displayed in gray.
When an external certification authority is inserted into the cetificate menu, all certificates signed by this certification authority will automatically be recognized as valid certificates when their owners authenticate.

The **Check** button will take you to the following window:



Configuration check

netasq

The object is used in the following modules :

⊟ : Configurations

VPN Slot #1 | Edit configuration

Figure 245: Checking the configuration

This is a search window that allows you to locate the policy in which the certification authority has been used.

You will access the IPSec tunnel configuration windows when you click on **Edit configuration**.

8.3.5.3. Static IPSec VPN Tunnel

The following example illustrates the configuration necessary for establishing a gateway-to-gateway VPN tunnel with pre-shared keys.

DEFINITION
VPN tunnels established between two VPN-compatible network elements which act as endpoints from a gateway (essentially Firewall to Firewall) are called "gateway-to-gateway VPN tunnels".

The following diagram represents this architecture:

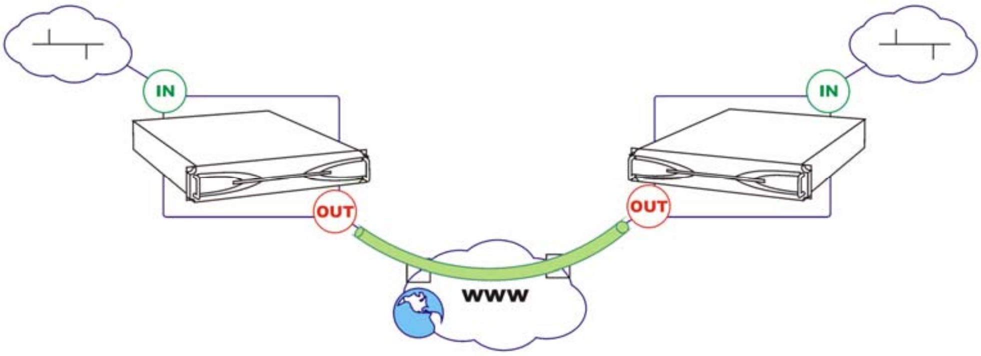


Figure 246: Static IPSec VPN tunnel

Tunnel configuration

In order to configure the tunnel, select the VPN slot in which you wish to establish the tunnel. The VPN wizard will then guide you along in the VPN configuration.

This configuration has to be performed on each Firewall participating in the VPN tunnel. However, don't forget to invert the traffic and tunnel endpoints. The first window of the VPN wizard will appear:

The first step in the VPN tunnel creation wizard is to select a name you wish to assign to this tunnel (the slot name will automatically be assigned the same name but you will be able to modify it later). Click on **Next** to continue configuring.

In Step 2 of the VPN wizard, select the tunnel type you wish to establish (for example, a static (obsolete) tunnel here). The following message will appear:

> "Manual tunnels are obsolete. Create a manual tunnel anyway?"

Click on **Yes** then on **Next**.

Steps 3 and 4 enable specifying the different network elements at the tunnel endpoints first then the traffic endpoints flowing inside the VPN tunnel.

> **WARNING**
> In the example, "Firewall_out" is used as the tunnel endpoint. If your Firewall is directly connected to a modem, you have to use the dialup interface which corresponds to your active internet connection.

Once the endpoints have been defined, click on **Next** to end the tunnel configuration. A general window will give you a quick roundup of the configuration defined in the wizard.

> **WARNING**
> To negotiate a VPN tunnel, it has to possess a valid default gateway (even during a test phase). Don't forget to perform the necessary filtering on VPN traffic from Firewalls participating in the tunnel.

Manual key configuration

In order to complete the configuration of static VPN tunnels, select Policy 1 in the menu directory to access the configuration menu for manual keys.

In general configuration, the following parameters are to be configured:

Proposal method	This unmodifiable option indicates that the protocol used for this tunnel is the ESP

	protocol in tunnel mode.
Authentication	Algorithm used to guarantee data integrity. NETASQ Firewalls support the following hash functions: ● no_auth (no authentication) ● HMAC-SHA1 ● HMAC-MD5 The corresponding static key is configured by clicking on the icon in the shape of a key.
Encryption	Algorithm used to encrypt data. NETASQ Firewalls offer the following: ● no_enc ● DES ● 3-DES ● BLOWFISH ● CAST128 ● AES WARNING NETASQ strongly recommends that you use AES as security-wise and throughput-wise, it is the most powerful algorithm. It is pertinent to note that the algorithms set out above do not have the same performance and throughput. AES is currently the best encryption algorithm. The corresponding static key is configured by clicking on the icon in the shape of a key.
SPI IN data	Identification of the inbound tunnel. Single value calculated by default by the Firewall.
SPI OUT data	Identification of the outbound tunnel. Single value calculated by default by the Firewall.
Keep alive (seconds)	Time elapsed in seconds between the sending of two packets through a VPN tunnel in order to keep the tunnel alive. These packets sent are only used for keeping this tunnel alive.

WARNING
SPI values have to be inverted (inbound and outbound) in the tunnel configuration.

The manual key is defined in this window:

In the **`Traffic endpoints`** tab, specify the hosts which will use this tunnel and for which connection type.

Select the local hosts or networks by clicking on the host on the left and the remote networks or hosts by clicking on the host on the right.

WARNING
In a static tunnel, “Any” cannot be selected as a traffic end point.

CHAPTER 4: PPTP

8.4.1. Introduction

8.4.1.1. Principle

PPTP allows you to connect remotely on the local network in a safe way. A **PPTP** client (available in Windows or MAC OSX) is installed on the client station, which connects to the Firewall and identifies the user

The user is identified by a login/password. The user profiles are saved on the Firewall in the LDAP database containing internal user records.

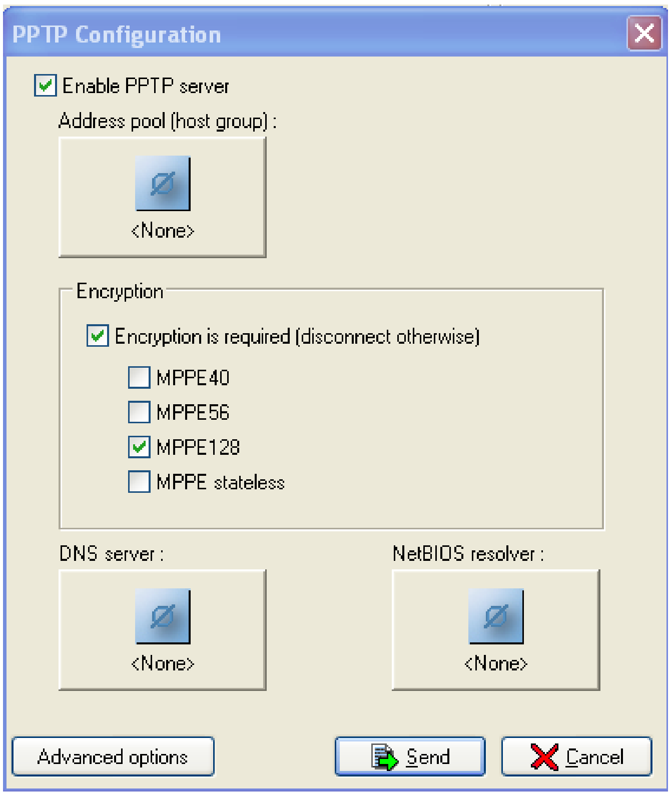
> ❗ **WARNING**
> Using IPSec is preferable to PPTP as the level of security is higher.

8.4.2. Configuration

8.4.2.1. Setup

This menu enables configuring the following parameters:

- Address pools.
- Encryption parameters.
- DNS server and Netbios Resolver



☑ Enable PPTP server

Address pool (host group) : <None>

Encryption

☑ Encryption is required (disconnect otherwise)

□ MPPE40

□ MPPE56

☑ MPPE128

□ MPPE stateless

DNS server : <None>

NetBIOS resolver : <None>

Figure 247: PPTP configuration

Step 1: activating the server
Activating/Configuring the **PPTP** server on the firewall in the menu **VPN \PPTP** by selecting **Activate the PPTP server**.

Step 2: address pools
Once the PPTP server has been activated, a private IP address pool has to be created. The firewall will then assign an available IP address from the pool to the client that connects in **PPTP**. A host group containing reserved addresses or an address range from the objects database has to be created.
The address pool is a host group containing IP addresses or an address range reserved for **PPTP** connections. (see Step 1).

Step 3: encryption (optional)
When encryption is enabled, connections can be established between clients and the server.

The possible encryption parameters are:

Encryption is required (disconnect otherwise)	Authorizes the connection only if the client encrypts his data.
MPPE40	Authorizes the use of the encryption protocol MPPE 40 bits
MPPE56	Authorizes the use of the encryption protocol MPPE 56 bits
MPPE128	Authorizes the use of the encryption protocol MPPE 128 bits
MPPE stateless	Enables deleting the preservation of the tunnel's status. This speeds up encryption but recovery is slower when packets are lost.

Step 4: The DNS server and NetBIOS resolver
The **DNS server** field allows you to send the IP address of the DNS server to the client host.
The **NetBIOS Resolver** field allows sending the site's WINS server IP address to the client.

Step 5: User profiles

Creation of user profiles. The PPTP connection is authenticated by login/password. PPTP user passwords may be defined in the user files (*Cf.* Part 4/Chapter 3: **Objects\Users**.)

6 Step 6: Advanced options

If you wish to create a new PPTP server but you have reached the maximum number of dynamic PPTPs allowed, you can increase the number.

When this limit has been reached, NETASQ UNIFIED MANAGER will suggest the advanced parameters window, which will allow you to set the number of dynamic PPTP servers possible.

PPTP servers are added in blocks, but in a way that is fully transparent for the user – for example, assuming you have a U70 appliance. In this case, a maximum of 48 PPTP servers are allowed by default but 0 are configured. Assume also that servers are added in blocks of 8.

You wish to configure a server:

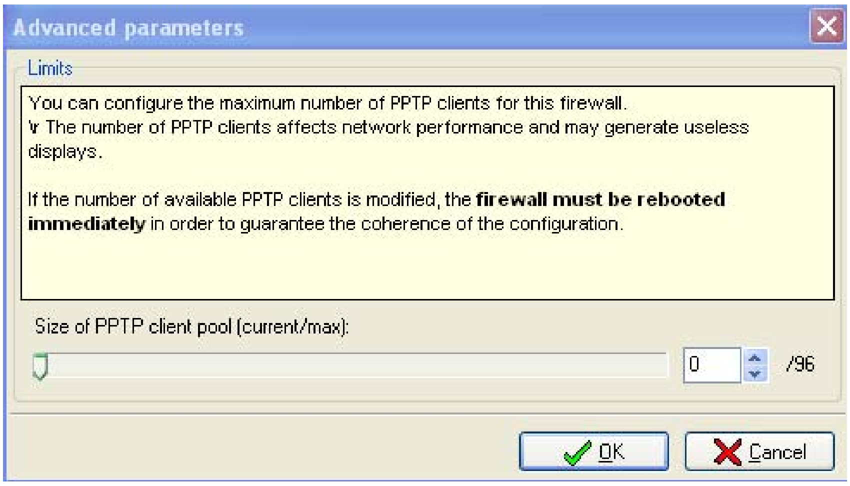
- The NETASQ UNIFIED MANAGER graphical interface will direct you to the advanced parameters window to increase the number of PPTP servers and informs you that you need to reboot the appliance. A block of 8 PPTP servers is assigned to you. You proceed to configure the 1st server, but you can configure 7 more without having to reboot the appliance.
- You wish to configure a 9th server, so you will need a new block. You will be informed that the firewall will reboot. Then you can configure the server.

When your appliance is in factory settings, a maximum number of servers will be assigned according to the model. The table below indicates the maximum number of servers assigned:

Models	Max no. of VLANs
U30, U70	48
U120, U250, U450	96
U1100, U1500	192
U6000	192

In the network interfaces configuration panel, you will find the **Advanced parameters** button that will allow you to increase your maximum number of servers.

The following window appears when you click on this button:



You can configure the maximum number of PPTP clients for this firewall.
\r The number of PPTP clients affects network performance and may generate useless displays.

If the number of available PPTP clients is modified, the **firewall must be rebooted immediately** in order to guarantee the coherence of the configuration.

Size of PPTP client pool (current/max): 0 /96

Figure 248: Advanced parameters

This window allows you to choose the desired number of servers. You merely need to slide the scale to increase or decrease the number. If the number of servers indicated corresponds to a new block, the firewall will need to reboot before the servers can be configured (adding or deleting).

WARNING

Any modifications to the network configuration before increasing the number of dynamic PPTP servers will be lost since this window will be closed. A warning message will inform you.

CHAPTER 5: SSL VPN

8.5.1. Introduction

When IPSEC technology is used, the administrator's intervention is required on client workstations, be it for software installation or the management of VPN tunnels. However, this becomes tedious when there is a large number of workstations to work on (installation, configuration and maintenance), difficult when a particular client is sought for peripherals such as PDA, and expensive since licenses have to be purchased for each workstation concerned.

Fortunately, with NETASQ's SSL VPN technology and a simple web browser, all users have to do is to log on to NETASQ's authentication portal, which will enable them to justify their identities before being able to access the resources that the administrator would have authorized. Communications are then encrypted in SSL, and confidentiality is ensured.

➲ This feature can be configured in the **`VPN\SSL VPN`** menu in the menu directory found in the Manager graphical interface.

The port used is now TCP port 443. Web and Java applet access use SSL, which connects via port 443. This modification impacts links in web pages that are accessible from the SSL VPN. In fact, links will be modified in the "Host" section (which is rarely found in links) of the "Path" section.

8.5.1.1. Using SSL VPN with the NETASQ Firewall

This feature allows you to access company resources protected by the Firewall, without having to install client software on the user workstation. Mobile users who retrieve e-mail when they are on the move provide an example of how this feature is used. While the above example is already possible with IPSEC VPN, it requires the installation of a client software, which penalizes the mobile user. Now, with SSL VPN technology, the mobile user can retrieve his mail (or visit the company's intranet site, access a private server, etc) securely (traffic is encrypted), without even needing to install a client software. He can therefore connect from a cybercafe, or a computer that is not his own, etc.

8.5.1.2. Operation

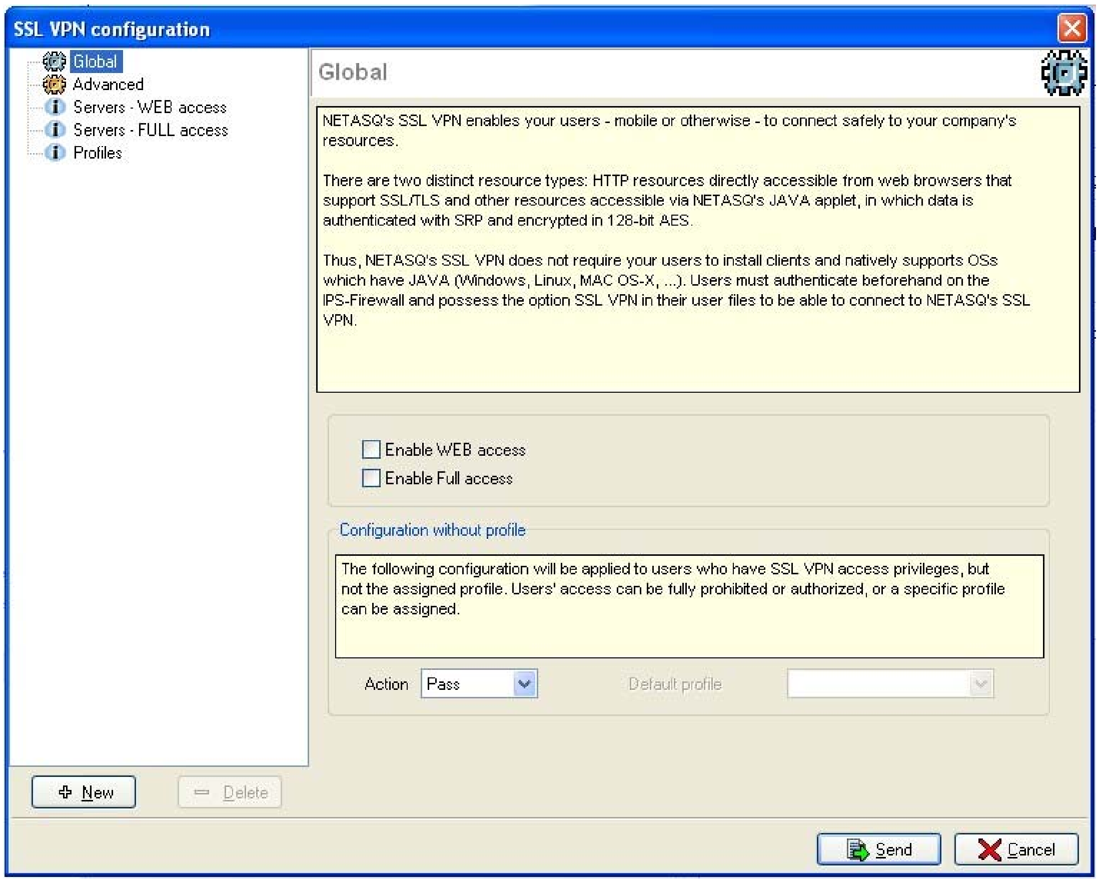
SSL VPN technology is separated into two features depending on the access type you wish to obtain: access to web resources (intranet, internet, etc) or other accesses (mail server, private application servers).

The SSL VPN configuration screen consists of two sections:

- On the left, a directory displaying the different features of the SSL VPN menu,
- On the right, the options that can be configured.

8.5.2. Configuration

8.5.2.1. Global



NETASQ's SSL VPN enables your users - mobile or otherwise - to connect safely to your company's resources.

There are two distinct resource types: HTTP resources directly accessible from web browsers that support SSL/TLS and other resources accessible via NETASQ's JAVA applet, in which data is authenticated with SRP and encrypted in 128-bit AES.

Thus, NETASQ's SSL VPN does not require your users to install clients and natively supports OSs which have JAVA (Windows, Linux, MAC OS-X, ...). Users must authenticate beforehand on the IPS-Firewall and possess the option SSL VPN in their user files to be able to connect to NETASQ's SSL VPN.

☐ Enable WEB access
☐ Enable Full access

Configuration without profile

The following configuration will be applied to users who have SSL VPN access privileges, but not the assigned profile. Users' access can be fully prohibited or authorized, or a specific profile can be assigned.

Action: Pass
Default profile:

Figure 249: Configuring the SSL VPN – Global

Enabling SSL VPN

Enable web access	Uses the SSL VPN module to access web resources.
Enable full access	Uses the SSL VPN module to access all other TCP traffic resources

The difference between both technologies lies in the use of JAVA applets to access resources other than the web. The JAVA applet inserted in the pages of the NETASQ web portal enables redirecting traffic to authorized servers.

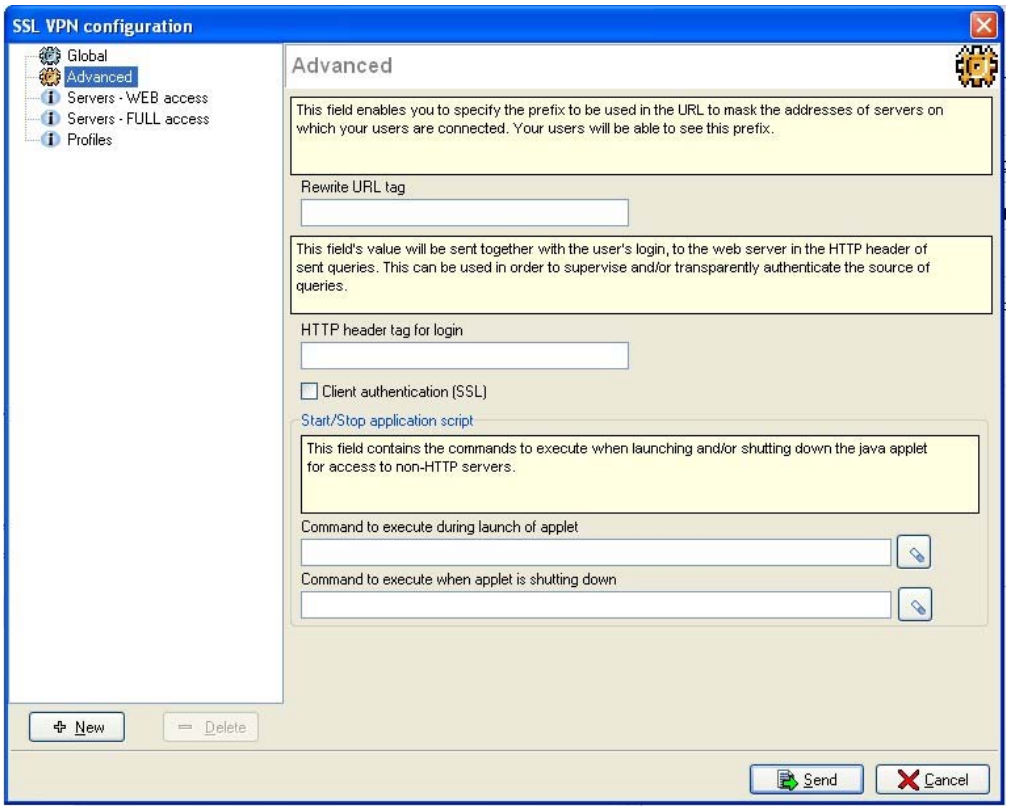
Configuration without profile

The options in the section “Configure without a profile” enable the definition of different types of access to SSL VPN features on Firewalls if the user does not have the specific profile defined in his user file (see *Part 4: Objects*). The types of access are explained in the table below:

Pass	If the action in this section is “Pass”, all the servers that the administrator has configured will be visible to users without specific profiles.
Block	If the action in this section is “Block”, none of the servers that the administrator has configured will be visible to users without specific profiles.
Default	If the action in this section is “Default”, the configured servers that form part of the

"default profile" will be visible to users without specific profiles.

8.5.2.2. Advanced


SSL VPN configuration

Advanced

This field enables you to specify the prefix to be used in the URL to mask the addresses of servers on which your users are connected. Your users will be able to see this prefix.

Rewrite URL tag

This field's value will be sent together with the user's login, to the web server in the HTTP header of sent queries. This can be used in order to supervise and/or transparently authenticate the source of queries.

HTTP header tag for login

□ Client authentication (SSL)

Start/Stop application script

This field contains the commands to execute when launching and/or shutting down the java applet for access to non-HTTP servers.

Command to execute during launch of applet

Command to execute when applet is shutting down

Figure 250: Configuring the SSL VPN - Advanced

Rewrite URL tag

NETASQ's SSL VPN technology enables masking the real addresses of servers to which users are redirected, by rewriting all URLs contained in HTTP pages visited. These URLs will then be replaced by a prefixed followed by 4 digits. This field enables defining the prefix to be used.

HTTP header tag for login

This field's value will be sent to the web server in the HTTP header of outgoing queries, along with the user's login. This value can be used for checks and/or transparent authentication on the source of the queries.

In the event the server to which HTTP traffic is redirected requests authentication, a login can be defined in the header of the HTTP packet. This login may be useful in indicating, for example, that this traffic arriving on the server come from the firewall and can be accepted by the server without authentication.

Client authentication (SSL)

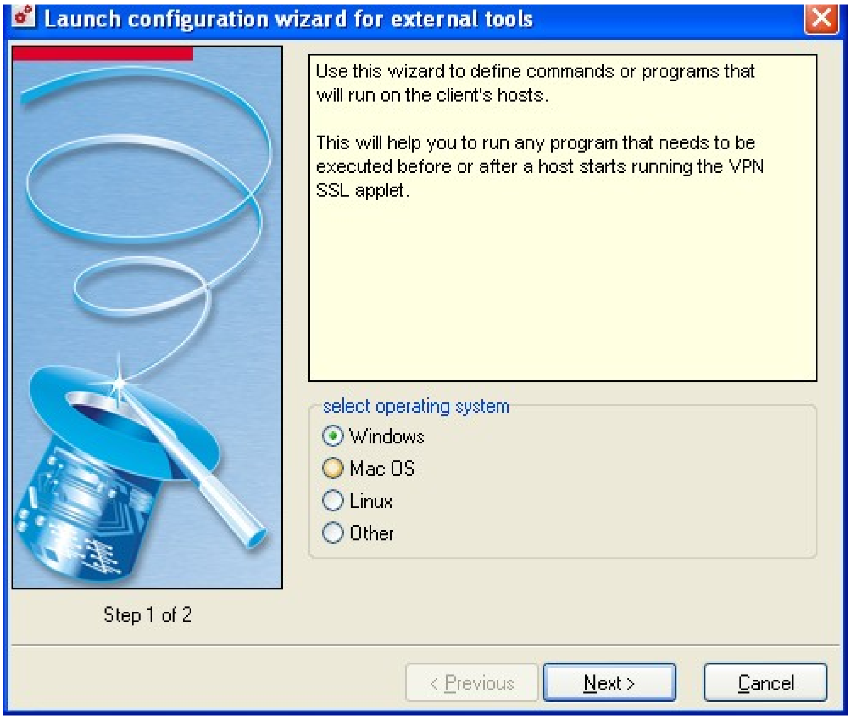
If the option **Client authentication (SSL)** is selected, each request that passes through the NETASQ Firewall's SSL VPN module must be authenticated with the certificate of the user who sent the request.

Command to execute during launch of applet

This command, which is launched when the applet is launched, allows the administrator to define actions to perform before displaying the applet. For example, this command may launch a script (installed on a server) which will modify the parameters of the user's mail account in such a way that when the applet is launched, SMTP and POP traffic will be automatically redirected, all without the user's intervention.

When you click on ✎, the configuration wizard will appear:

1 Step 1



Launch configuration wizard for external tools

Use this wizard to define commands or programs that will run on the client's hosts.

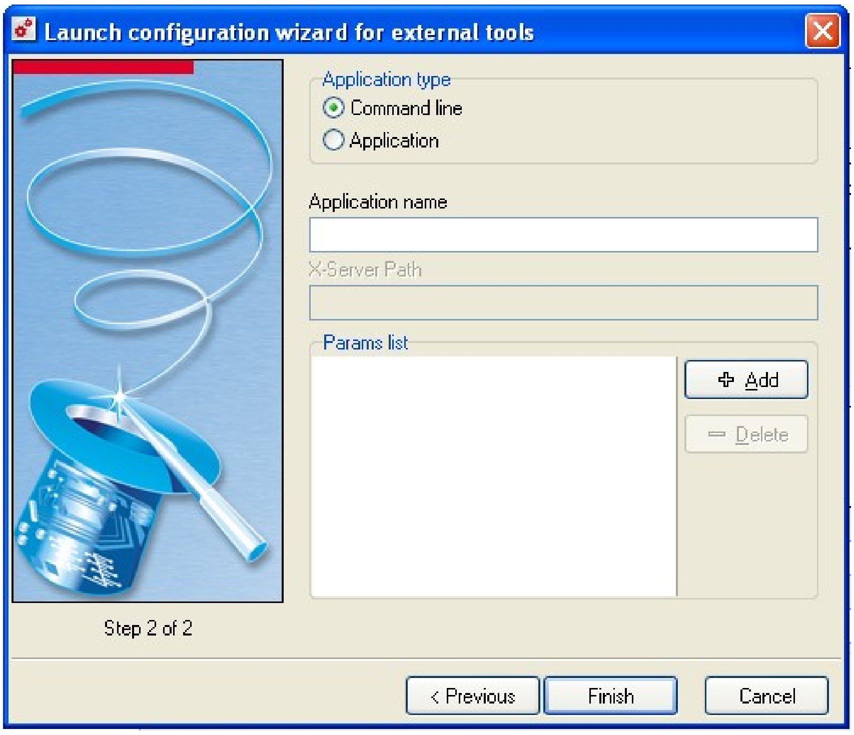
This will help you to run any program that needs to be executed before or after a host starts running the VPN SSL applet.

select operating system
- ● Windows
- ○ Mac OS
- ○ Linux
- ○ Other

Figure 251: Configuration wizard for external tools - Step 1

Select the operating system from among the four options suggested then click on **Next**.

2 Step 2



Launch configuration wizard for external tools

Application type

● Command line

○ Application

Application name

X-Server Path

Params list

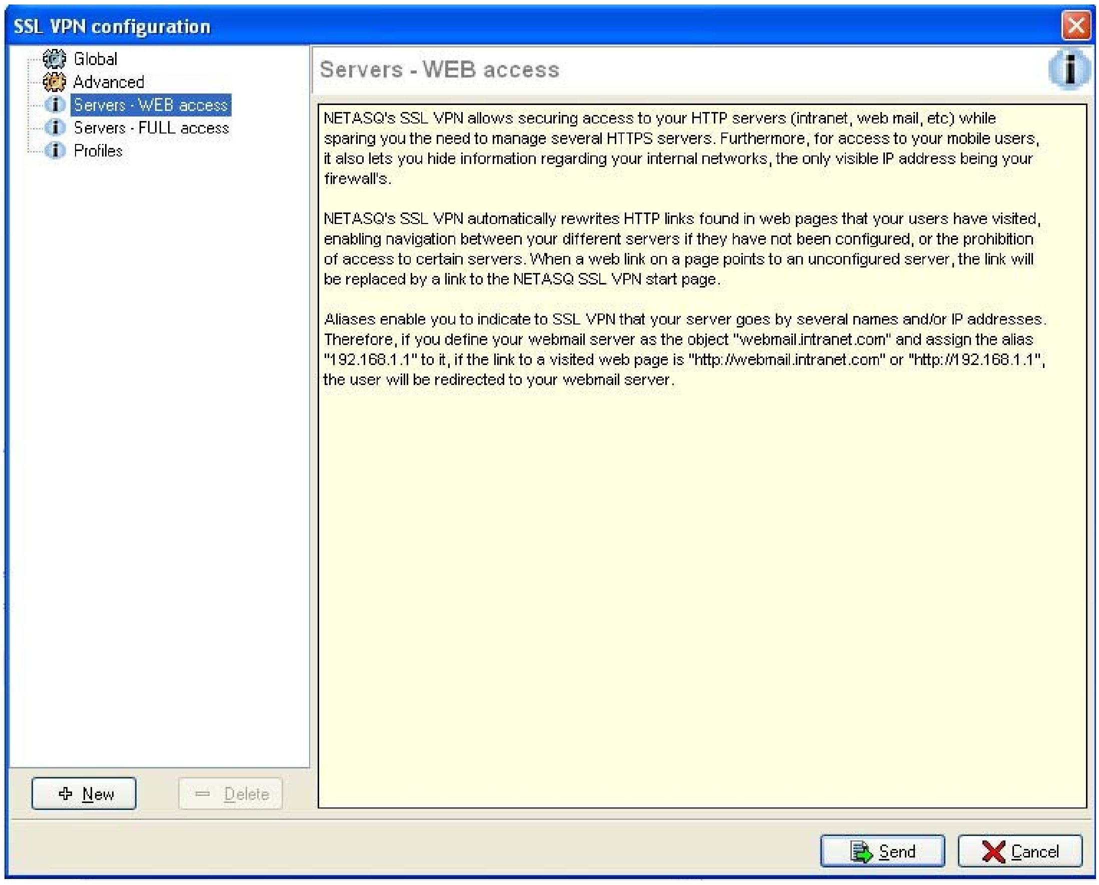
Figure 252: Configuration wizard for external tools - Step 2

Define the type of application (**Command line** or **Application**), then indicate a name for the application and add a value for the parameter.

Command to execute when applet is shutting down

This command, which is launched when the applet is shut down, allows the administrator to define actions to perform before shutting down the applet. For example, this command may launch a script (installed on a server) which will modify the parameters of the user's mail account in such a way that when the applet is shut down, SMTP and POP traffic will no longer be automatically redirected, all without the user's intervention.

8.5.2.3. Servers-Web access



NETASQ's SSL VPN allows securing access to your HTTP servers (intranet, web mail, etc) while sparing you the need to manage several HTTPS servers. Furthermore, for access to your mobile users, it also lets you hide information regarding your internal networks, the only visible IP address being your firewall's.

NETASQ's SSL VPN automatically rewrites HTTP links found in web pages that your users have visited, enabling navigation between your different servers if they have not been configured, or the prohibition of access to certain servers. When a web link on a page points to an unconfigured server, the link will be replaced by a link to the NETASQ SSL VPN start page.

Aliases enable you to indicate to SSL VPN that your server goes by several names and/or IP addresses. Therefore, if you define your webmail server as the object "webmail.intranet.com" and assign the alias "192.168.1.1" to it, if the link to a visited web page is "http://webmail.intranet.com" or "http://192.168.1.1", the user will be redirected to your webmail server.

Figure 253: Configuring the SSL VPN – Servers – Web access

This section groups the servers configured for access to web resources.

SSL VPN serves to secure your HTTP servers and avoids the management of several HTTPS servers. It also allows centralizing the authentication of several servers. Nomad users who wish to access the company's network remotely by masking information about the internal network will also find this useful.

HTTP links are automatically rewritten, thus allowing browsing between different servers if they have been configured, or to prohibit access to certain servers. If the link points to an unconfigured server, the link will be redirected to an error page that would display something like "Your administrator does not allow this link".

Aliases allow indicating to the SSL VPN that your server has several names and/or IP addresses.

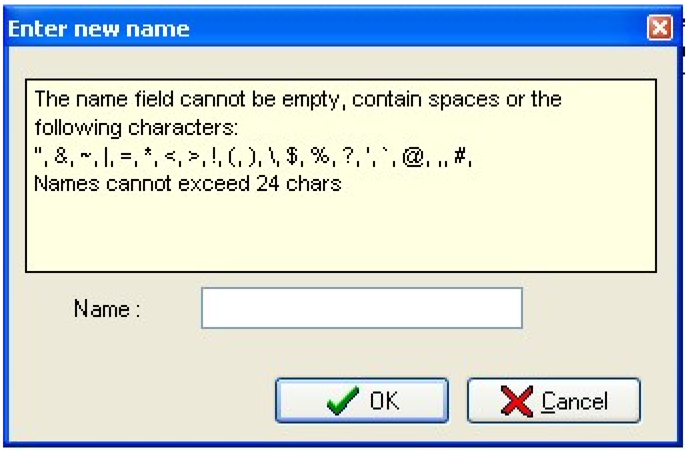
The number of web servers that can be configured varies according to the appliance model:

Model	Max. no. Of http servers	Max. no. Of other servers
U30, U70	64	32
U120, U250, U450	128	64
U1100, U1500	256	128
F5500, U6000	512	256

Adding a web access server

To add a web access server, the procedure is as follows:

1 Click on **New** button at the bottom of the SSL VPN configuration window, then select **`HTTP server`**. The following window will appear:



Enter new name

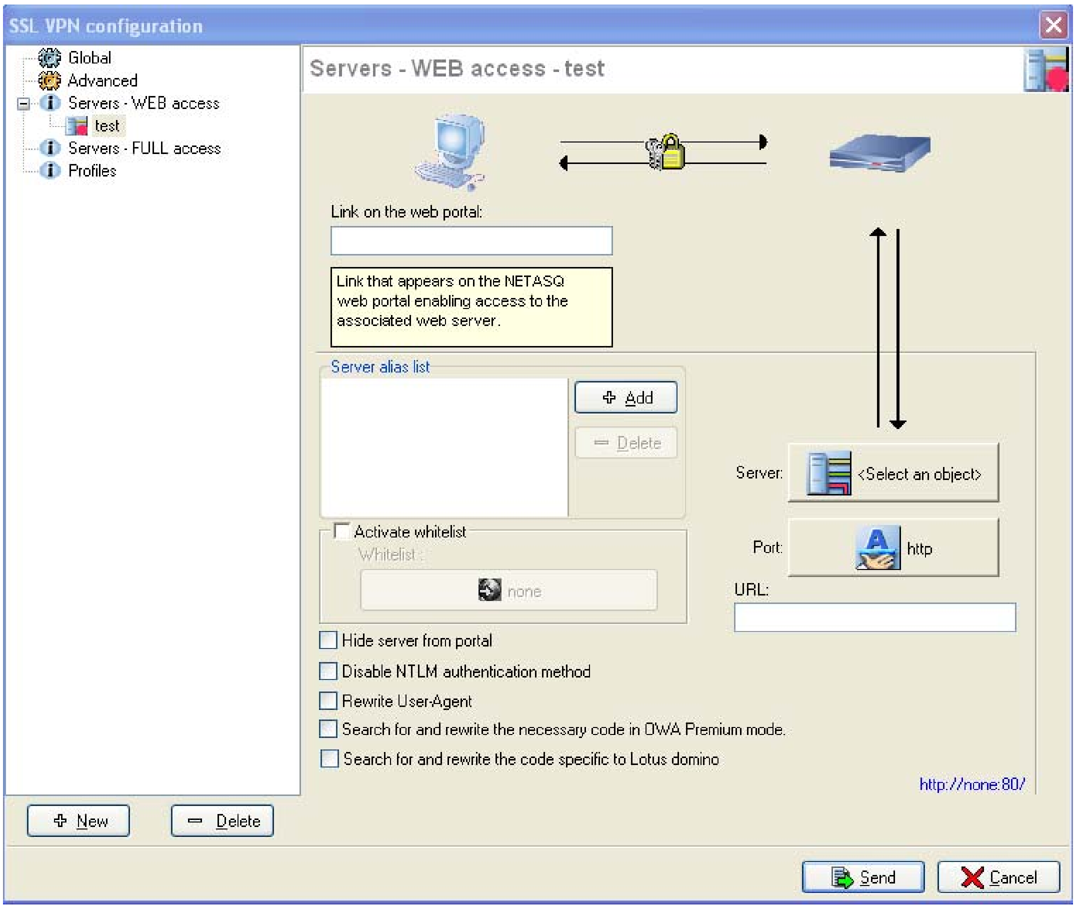
The name field cannot be empty, contain spaces or the following characters:
", &, ~, |, =, *, <, >, !, (,), \, $, %, ?, ', `, @, ., #,
Names cannot exceed 24 chars

Name :

Figure 254: Entering a new name

2 Enter a name for this server.

3 This server's configuration then appears. The different parameters are explained below.



SSL VPN configuration

- Global
- Advanced
- Servers - WEB access
  - test
- Servers - FULL access
- Profiles

Servers - WEB access - test

Link on the web portal:

Link that appears on the NETASQ web portal enabling access to the associated web server.

Server alias list

Server: <Select an object>

Port: http

URL:

□ Activate whitelist

Whitelist : none

□ Hide server from portal

□ Disable NTLM authentication method

□ Rewrite User-Agent

□ Search for and rewrite the necessary code in OWA Premium mode.

□ Search for and rewrite the code specific to Lotus domino

http://none:80/

Figure 255: Configuring the SSL VPN – Servers – Web access - HTTP

Link on the web portal The defined link appears on the NETASQ web portal. When the user clicks on this link, he will be redirected to the corresponding server.

Server The object corresponding to the server accessible to the user can be specified in this field.

WARNING

Make sure that you use an object whose name is identical to the name of the **FQDN** server it refers to. If this is not the case, (e.g. object name: webmail, FQDN name: www.webmail.com), Firewall queries to this server may be refused.

Port The port on the server accessible to the user can be specified in this field. Port 80 is defined for HTTP.

URL This URL enables going directly to the specified page.

Server alias list Aliases allow indicating to the SSL VPN module that the server is known by several names and/or IP addresses. If a mail server is defined as the object "webmail.intranet.com" to which the alias "192.168.1.1" is assigned, the user will be redirected to the mail server whether he visits the link "http://webmail.intranet.com" or "http://192.168.1.1". Clicking on the **Add** button will open the window that will allow you to add a new alias.

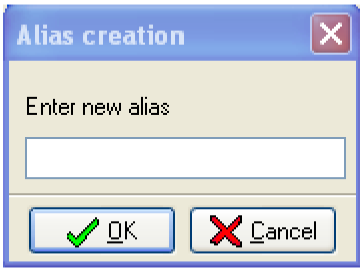
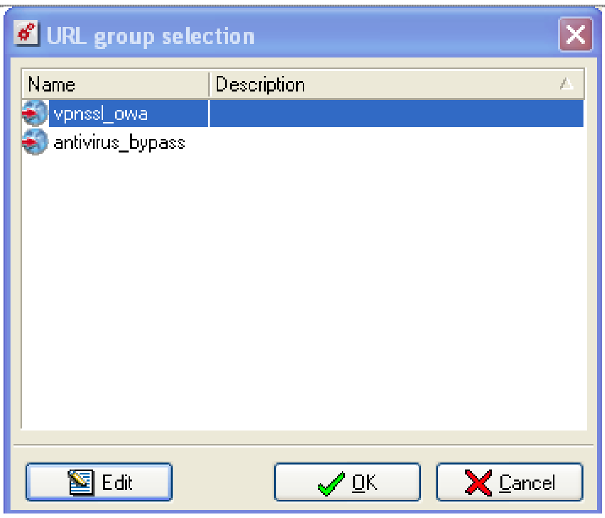


Figure 256: Creating an alias

Activate whitelist Only links that the SSL VPN module has rewritten can be accessed through SSL VPN. If, on an authorized site, there is a link to an external website whose server has not been defined in SSL VPN configuration, the authorized site will no be accessible via SSL VPN.

If the white list has been activated, it will enable access to URLs which have not been rewritten. For example, for webmail SSL VPN access, if you wish to allow users to quit the SSL VPN by clicking on the links contained in their e-mails, you need to add a whitelist containing "*".

The following window will appear when you click on the **Whitelist** button:



Name	Description
vpnssl_owa	
antivirus_bypass	

Figure 257: Selecting a URL group

The **Edit** button in the URL group selection window will bring you to the URL group edition window.

WARNING

If the user clicks on a link in the white list, it will no longer be protected by the NETASQ SSL VPN module.

Hide server from portal

All servers configured in SSL VPN are listed on the NETASQ authentication portal by default. However, it may be necessary for servers to not be accessible through another server, so in this case, the option “Do not display this server on the portal” has to be selected. When this option is selected during the configuration of a server, this server can be accessed via SSL VPN, but will not be on the direct-access list. A link to this server is needed in order to access it. An application can use several servers but have only one entry point, so only one link in the menu of the portal.

Disable NTLM authentication method

Some web servers may request authentication before the transfer of data between the server and the user. This method can be deactivated for servers that do not support this authentication method for traffic passing through the Firewall. By doing so, the user will no longer be able to select this method for authentication on the remote web server.

Rewrite “User-Agent”

The “User-Agent” field in the header of an HTTP request contains the identifier for the web browser used. For example, on Internet Explorer: Mozilla/4.0 (compatible; MSIE 6.0 ...). Rewriting the “User-Agent” value therefore allows modifying the HTTP request in such a way that it gives the impression of coming from a different browser type.

This option is particularly useful in basic mode of Outlook Web Access (OWA). In fact, OWA in premium mode (a very advanced mode), uses Webdav, an extension of HTTP. Since not all types of network equipment support these extensions (the SSL VPN module on Firewalls supports OWA in premium mode), the transmission of such traffic may give rise to compatibility issues, especially in the internet. Instead of all users (internal and external) having to use a more basic mode of OWA, the option “Rewrite User-Agent” enables using “premium” OWA internally (compatibility with premium mode is easy to obtain) and using “basic” mode by passing through SSL VPN (for mobile users, via internet). Since “old” web browsers do not support these extensions, OWA therefore operates in basic mode when it encounters the “User-Agent” on these browsers.

OWA Premium

If this option has been selected, you will enable the specific rewriting rules that allow supporting Outlook Web Access in premium mode.

Lotus domino	If this option has been selected, you will enable the specific rewriting rules that allow supporting Lotus domino web applications.

Adding an HTTP-OWA server

The **SSL VPN** module on NETASQ Firewalls supports OWA (Outlook Web Access) servers

DEFINITION OWA
(Outlook Web Access) allows users to access and use their professional mailboxes remotely via an interface that is accessible on a web browser.

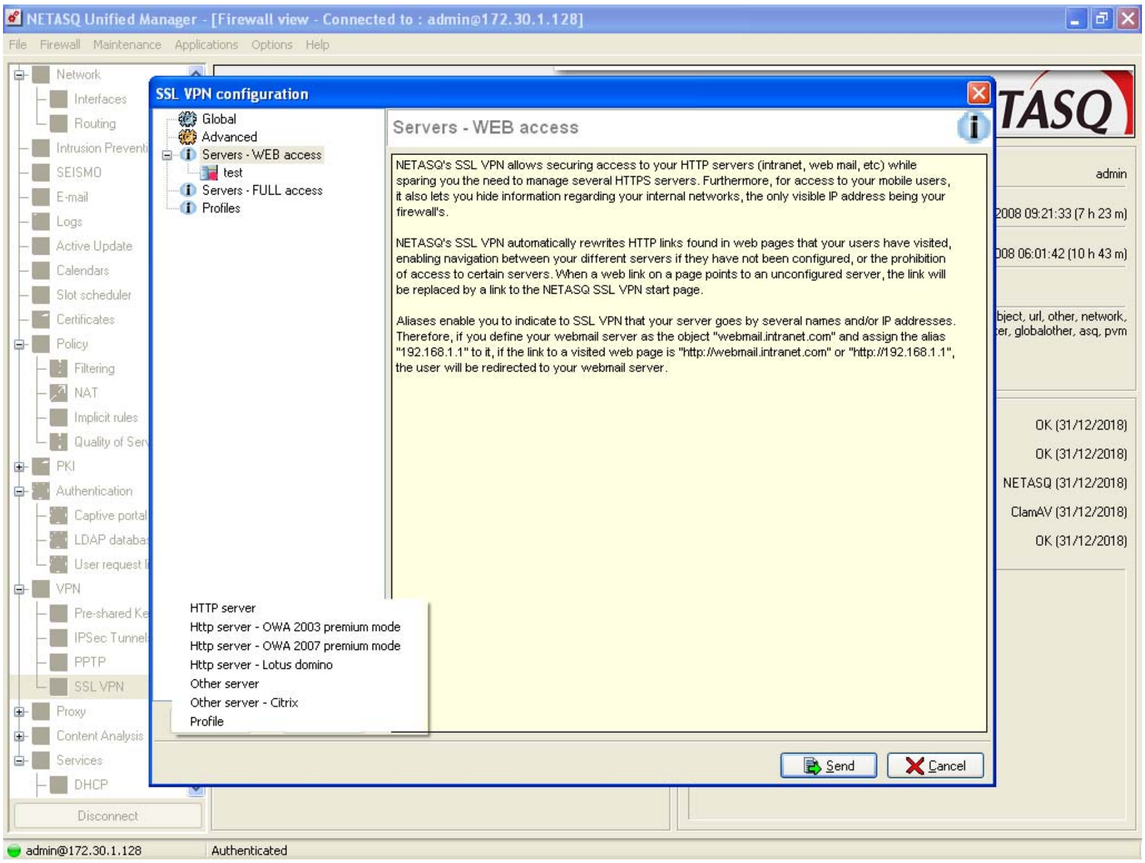
“Premium” mode can only be used in Windows with Internet Explorer 5 and higher. It is based on web technologies such as html, css and javascript but also on Microsoft proprietary technologies such as htc, xml and activeX.

In Exchange 2003, the links are absolute links, regardless of whether they are in HTML pages, javascripts, in XML data, or in XSL sheets, ie, of the “http://www.netasq.com/index.htm” type.

It is therefore possible to add HTTP servers (with specific preset options for perfect compatibility with OWA) to the list of web-access servers.

The procedure for adding an HTTO-OWA server is as follows:

1 Click on the “New” button at the bottom of the SSL VPN configuration window. A contextual menu will appear:



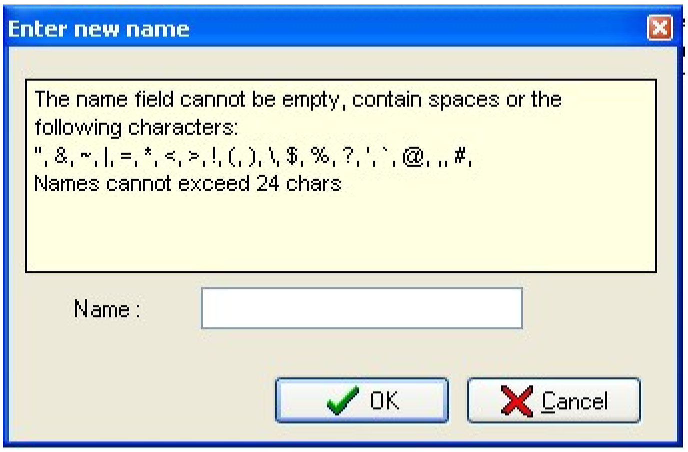
NETASQ's SSL VPN allows securing access to your HTTP servers (intranet, web mail, etc) while sparing you the need to manage several HTTPS servers. Furthermore, for access to your mobile users, it also lets you hide information regarding your internal networks, the only visible IP address being your firewall's.

NETASQ's SSL VPN automatically rewrites HTTP links found in web pages that your users have visited, enabling navigation between your different servers if they have not been configured, or the prohibition of access to certain servers. When a web link on a page points to an unconfigured server, the link will be replaced by a link to the NETASQ SSL VPN start page.

Aliases enable you to indicate to SSL VPN that your server goes by several names and/or IP addresses. Therefore, if you define your webmail server as the object "webmail.intranet.com" and assign the alias "192.168.1.1" to it, if the link to a visited web page is "http://webmail.intranet.com" or "http://192.168.1.1", the user will be redirected to your webmail server.

Figure 258: Configuring the SSL VPN - Servers – Web access

Select **`HTTP-OWA Server 2003`** or **`HTTP-OWA Server premium – OWA 2007 premium`**. The following window will open:



The name field cannot be empty, contain spaces or the following characters:
", &, ~, |, =, *, <, >, !, (,), \, $, %, ?, ', `, @, ,, #,
Names cannot exceed 24 chars

Figure 259: Entering a new name

2 Enter a name for this server

3 The preset options for an OWA 2003 premium server are “Enable whitelist” with an indication of the URL group “owa_sslvpn”, port “http”, the URL field with “exchange” indicated, and the **OWA Premium** field. For an OWA 2007 server, the preset fields are **Enable whitelist** with an indication of the URL group “owa_sslvpn”, port “http”, the URL field with “owa” indicated, and the **OWA Premium** field.
Other options that have not been entered have to be configured in the same way as for a “normal” web-access server.

Adding a Lotus domino HTTP server

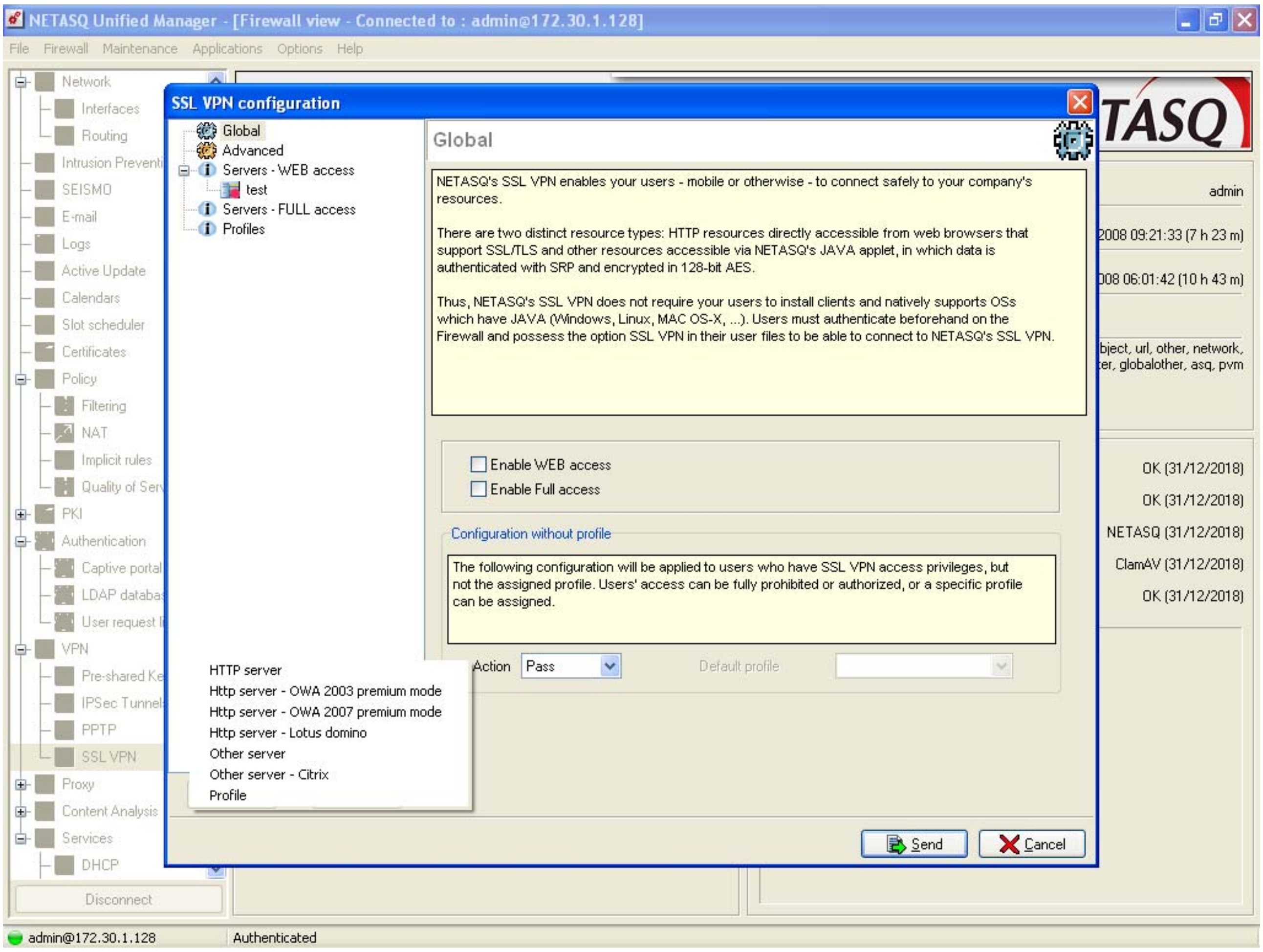
The **SSL VPN** module on NETASQ firewalls supports Lotus domino servers.

> ? **DEFINITION OF LOTUS DOMINO**
> IBM application server by Lotus.

An HTTP server can be added to the list of web access servers with certain options specifically entered before for compatibnility with Lotus Domino.

The procedure for adding an HTTP-Lotus Domino server is as follows:

1 Click on **New** at the bottom of the SSL VPN configuration window, which will open the following contextual menu:



Global

NETASQ's SSL VPN enables your users - mobile or otherwise - to connect safely to your company's resources.

There are two distinct resource types: HTTP resources directly accessible from web browsers that support SSL/TLS and other resources accessible via NETASQ's JAVA applet, in which data is authenticated with SRP and encrypted in 128-bit AES.

Thus, NETASQ's SSL VPN does not require your users to install clients and natively supports OSs which have JAVA (Windows, Linux, MAC OS-X, ...). Users must authenticate beforehand on the Firewall and possess the option SSL VPN in their user files to be able to connect to NETASQ's SSL VPN.

□ Enable WEB access
□ Enable Full access

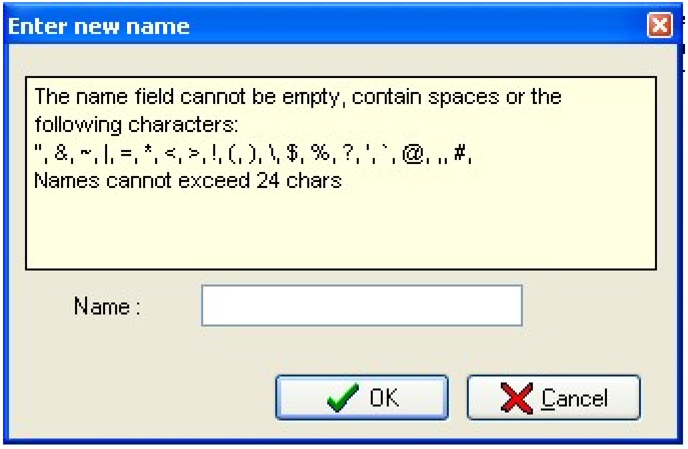
Configuration without profile

The following configuration will be applied to users who have SSL VPN access privileges, but not the assigned profile. Users' access can be fully prohibited or authorized, or a specific profile can be assigned.

Action: Pass   Default profile:

Figure 260: Configuring the SSL VPN - Servers – Web access

Select **`Http server-Lotus domino.`** The following window will appear:



Enter new name

The name field cannot be empty, contain spaces or the following characters:
", &, ~, |, =, *, <, >, !, (,), \, $, %, ?, ', `, @, ,, #,
Names cannot exceed 24 chars

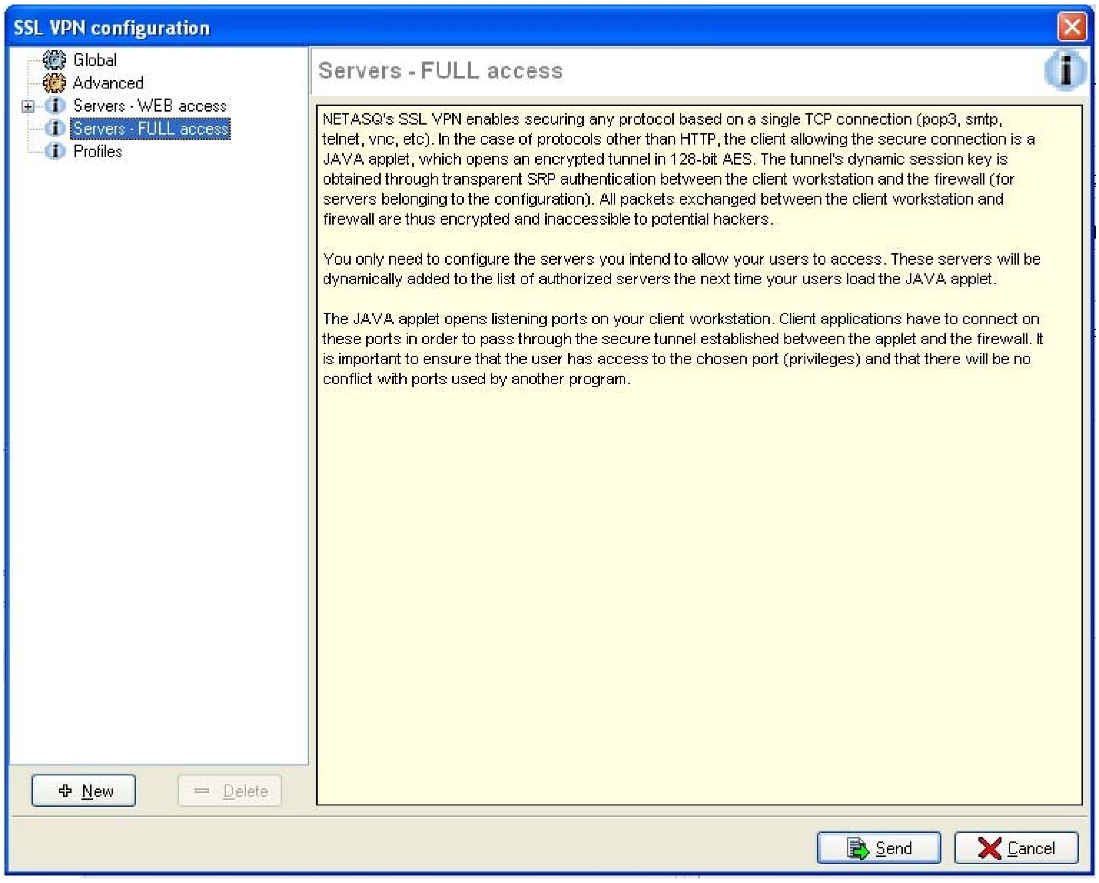
Name :

Figure 261: Entering a new name

2 Name this server.

3 The option that has been entered for a Lotus Domino server is the “Lotus Domino” field, selected by default.

8.5.2.4. Full access



Servers - FULL access

NETASQ's SSL VPN enables securing any protocol based on a single TCP connection (pop3, smtp, telnet, vnc, etc). In the case of protocols other than HTTP, the client allowing the secure connection is a JAVA applet, which opens an encrypted tunnel in 128-bit AES. The tunnel's dynamic session key is obtained through transparent SRP authentication between the client workstation and the firewall (for servers belonging to the configuration). All packets exchanged between the client workstation and firewall are thus encrypted and inaccessible to potential hackers.

You only need to configure the servers you intend to allow your users to access. These servers will be dynamically added to the list of authorized servers the next time your users load the JAVA applet.

The JAVA applet opens listening ports on your client workstation. Client applications have to connect on these ports in order to pass through the secure tunnel established between the applet and the firewall. It is important to ensure that the user has access to the chosen port (privileges) and that there will be no conflict with ports used by another program.

Figure 262: Configuring the SSL VPN – Full access

NETASQ's SSL VPN enables securing any protocol based on a single TCP connection (POP3, SMTP, telenet, remote access, etc). for protocols other than HTTP, the client that allows secure connections is a java applet, which will open an encrypted tunnel. All packets exchanged between the client workstation and the firewall are encrypted.

You only need to configure the servers which you intend to allow your users to access. These servers will be added dynamically to the list of authorized servers the next time your users load the java applet.

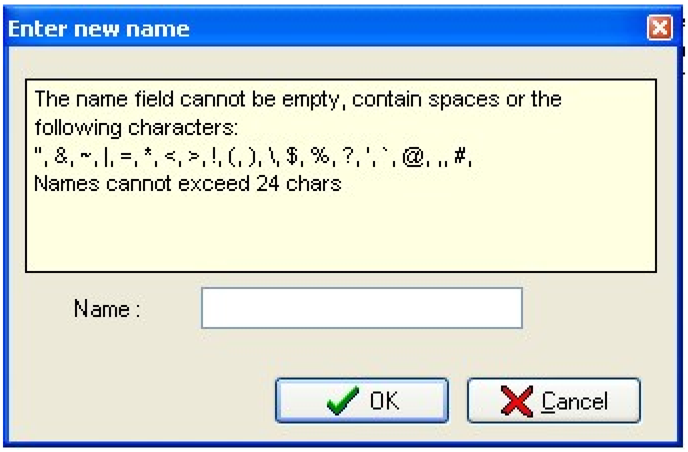
The java applet opens listening ports on the client workstation, and client tools will need to connect to these ports in order to pass through the secure tunnel set up between the applet and the firewall. It is necessary to ensure that the chosen port is accessible to the user (where privileges are concerned) and that there is no conflict with another port used by another program. These servers will be added dynamically. The value of this field will be sent to the web server in the HTTP header of sent requests, as well as the user's ID. These can be used for control purposes and/or transparent authentications on the source of requests.

This section groups the servers configured for access to all other resources except the web.

Adding an access server for all resources excepr the web

This section groups the servers configured for access to all other resources except the web.

1 Click on **New** at the bottom of the SSL VPN configuration window, then select **`Other Server.`** The following window will appear:



Enter new name

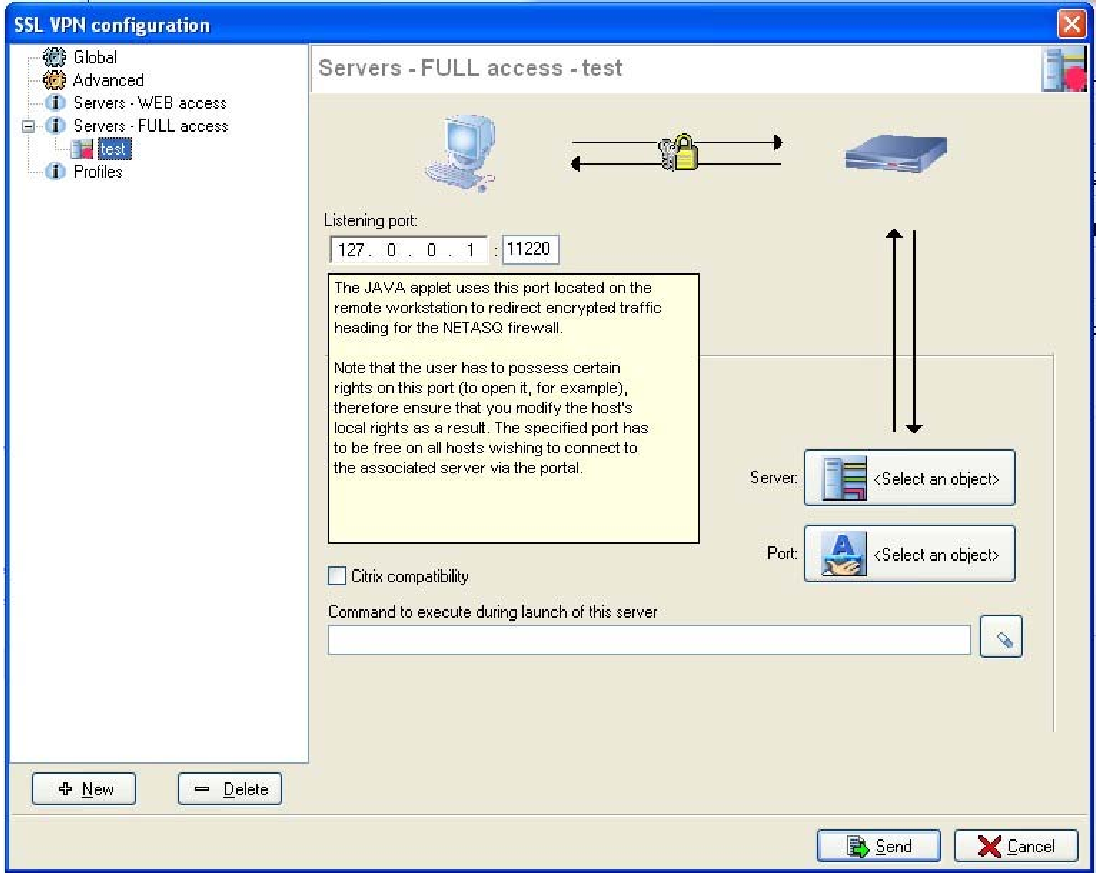
The name field cannot be empty, contain spaces or the following characters:
", &, ~, |, =, *, <, >, !, (,), \, $, %, ?, ', `, @, ,, #,
Names cannot exceed 24 chars

Name :

Figure 263: Entering the new name

2 Enter a name for this server.

3 This server’s configuration then appears. The different parameters are explained below.



SSL VPN configuration

Servers - FULL access - test

Listening port: 127 . 0 . 0 . 1 : 11220

The JAVA applet uses this port located on the remote workstation to redirect encrypted traffic heading for the NETASQ firewall.

Note that the user has to possess certain rights on this port (to open it, for example), therefore ensure that you modify the host's local rights as a result. The specified port has to be free on all hosts wishing to connect to the associated server via the portal.

Server: <Select an object>

Port: <Select an object>

□ Citrix compatibility

Command to execute during launch of this server

Figure 264: Configuring the SSL VPN - Servers – Full access

Listening port	The JAVA applet uses this port, located on the remote workstation, to redirect encrypted traffic going to the NETASQ Firewall. The user must possess certain rights on this port (to open it, for example), therefore make sure that the host’s local administration rights are modified as well. Also, the specified port must be free on all hosts wishing to connect to the associated server via the portal.
Server	The object corresponding to the server accessible to the user can be specified

	in this field.
Citrix Compatibility	Enables compatibility with the Citrix web authentication portal and access via the web browser. This option is useless if the Citrix fat client is used.
Port	The port on the server accessible to the user can be specified in this field.
Command to execute during the launch of this server	This command, which is executed when the server is launched, allows the administrator to define actions to perform before displaying the server. For example, this command may execute a script (installed on a server) that will check the activity of the antivirus installed on the user's host before granting him access to the server.

Example of a configuration with a Citrix server

DEFINITION
Citrix Presentation Server was designed by Citrix Systems.

This software program allows the deployment of programs over a network in order to access it remotely from a client (access through the web browser) or fat clients (installed application).

Its operating principle is such:

- Installation and launch of an application on the server. This application will then use the server's resources.
- Via the local network, the client workstation will receive this application's display and tools so that it can work on it via a web portal after connecting.

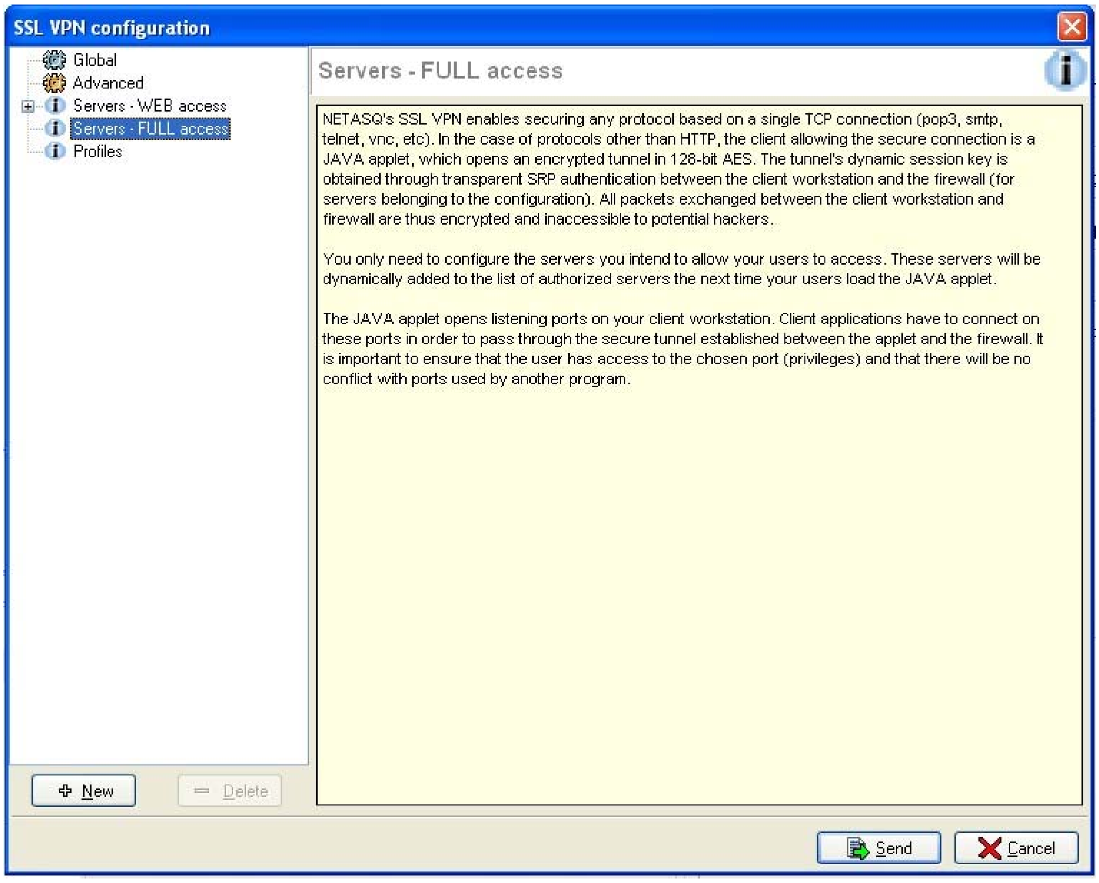
The advantage of it is therefore to make programs available without having to install them on each client workstation, thereby using less resources.

Citrix can operate in two modes:

- In light client mode (Citrix web portal)
- In heavy client mode (application installed on the client workstation)

1 Step 1: Creating an object for the Citrix server
Go to the object database in order to create a host.

2 Step 2: Configuring a full access server
In the menu directory in NETASQ UNIFIED MANAGER, go to **VPN\SSL VPN**. Select **Servers-Full access.** The following window will appear:



Servers - FULL access

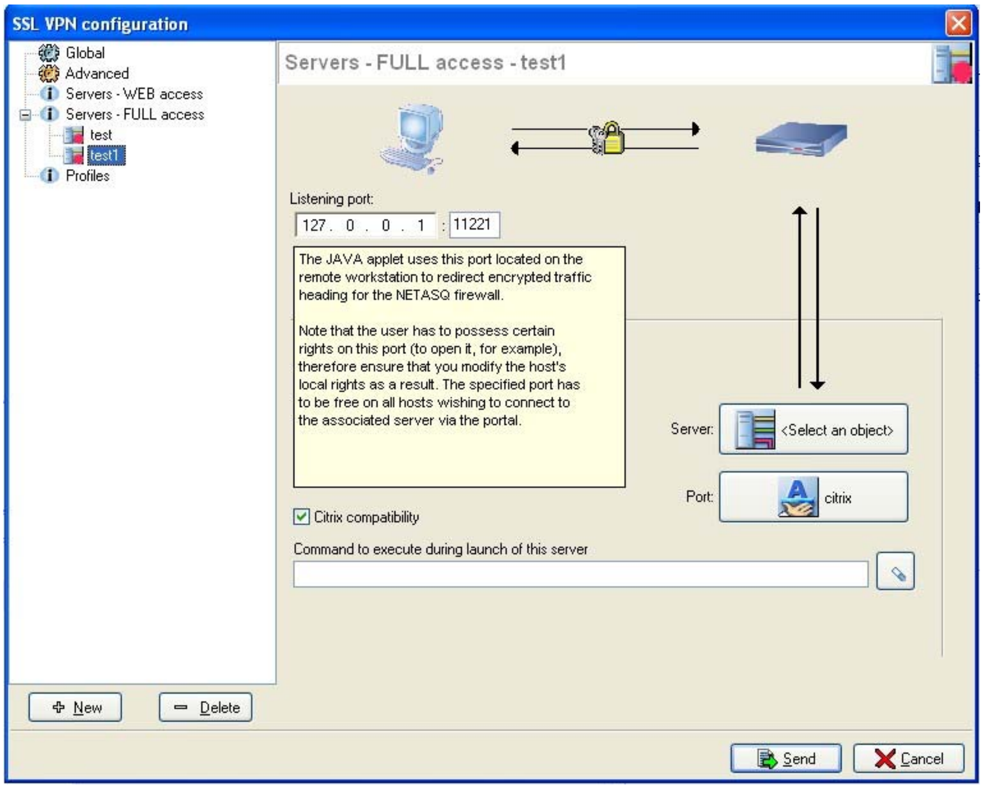
NETASQ's SSL VPN enables securing any protocol based on a single TCP connection (pop3, smtp, telnet, vnc, etc). In the case of protocols other than HTTP, the client allowing the secure connection is a JAVA applet, which opens an encrypted tunnel in 128-bit AES. The tunnel's dynamic session key is obtained through transparent SRP authentication between the client workstation and the firewall (for servers belonging to the configuration). All packets exchanged between the client workstation and firewall are thus encrypted and inaccessible to potential hackers.

You only need to configure the servers you intend to allow your users to access. These servers will be dynamically added to the list of authorized servers the next time your users load the JAVA applet.

The JAVA applet opens listening ports on your client workstation. Client applications have to connect on these ports in order to pass through the secure tunnel established between the applet and the firewall. It is important to ensure that the user has access to the chosen port (privileges) and that there will be no conflict with ports used by another program.

Figure 265: Configuring the SSL VPN - Servers – Full access

Click on **New** then select "Other server -Citrix". Enter a name for the server. The Citrix server configuration window will then appear:



Servers - FULL access - test1

Listening port: 127 . 0 . 0 . 1 : 11221

The JAVA applet uses this port located on the remote workstation to redirect encrypted traffic heading for the NETASQ firewall.

Note that the user has to possess certain rights on this port (to open it, for example), therefore ensure that you modify the host's local rights as a result. The specified port has to be free on all hosts wishing to connect to the associated server via the portal.

Server: <Select an object>

Port: citrix

☑ Citrix compatibility

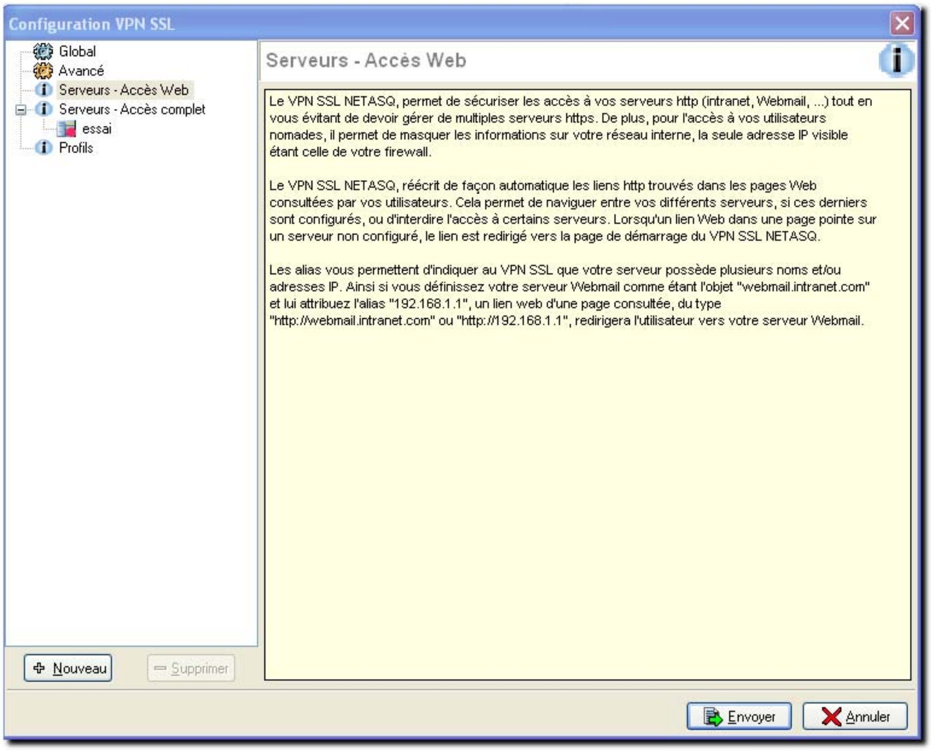
Command to execute during launch of this server

Figure 266: Configuring the SSL VPN - Servers – Full access

Select the Citrix server created earlier in the objects database.

3 Step 3: Configuring a web access server

In the menu directory in NETASQ UNIFIED MANAGER, go to **`VPN\SSL VPN`**. Select **Servers-Web access.** The following window will appear:



Serveurs - Accès Web

Le VPN SSL NETASQ, permet de sécuriser les accès à vos serveurs http (intranet, Webmail, ...) tout en vous évitant de devoir gérer de multiples serveurs https. De plus, pour l'accès à vos utilisateurs nomades, il permet de masquer les informations sur votre réseau interne, la seule adresse IP visible étant celle de votre firewall.

Le VPN SSL NETASQ, réécrit de façon automatique les liens http trouvés dans les pages Web consultées par vos utilisateurs. Cela permet de naviguer entre vos différents serveurs, si ces derniers sont configurés, ou d'interdire l'accès à certains serveurs. Lorsqu'un lien Web dans une page pointe sur un serveur non configuré, le lien est redirigé vers la page de démarrage du VPN SSL NETASQ.

Les alias vous permettent d'indiquer au VPN SSL que votre serveur possède plusieurs noms et/ou adresses IP. Ainsi si vous définissez votre serveur Webmail comme étant l'objet "webmail.intranet.com" et lui attribuez l'alias "192.168.1.1", un lien web d'une page consultée, du type "http://webmail.intranet.com" ou "http://192.168.1.1", redirigera l'utilisateur vers votre serveur Webmail.

Figure 267: Configuring the SSL VPN - Servers – Web access

Click on **New** then select "HTTP server ". Enter a name for the server. The web server configuration window will then appear:

Using the Server button, select your web server. As for the URL, indicate CitrixAccess/auth/login.aspx (if it is the version Presentation Server 4.0).

4 Sending the configuration

Click on **Send**.

5 Accessing the web portal

Open the web browser then identify yourself (https://your firewall's IP address or its name.
Go to "Secure access" then select “Pop up secure-access window” from the drop-down list.

WARNING
It is important for the NETASQ SSL VPN applet to operate as a background task.

NOTE
Applications in the Administration Suite can be opened via the Citrix portal simply by clicking on the relevant icons.

Next, select **`Portal access\Portal`** thenenter your username, password and domain.

8.5.2.5. Removing a server

To remove a server, the procedure is as follows:

1 Select the server to remove
2 Click on **Delete**. The following message will appear:

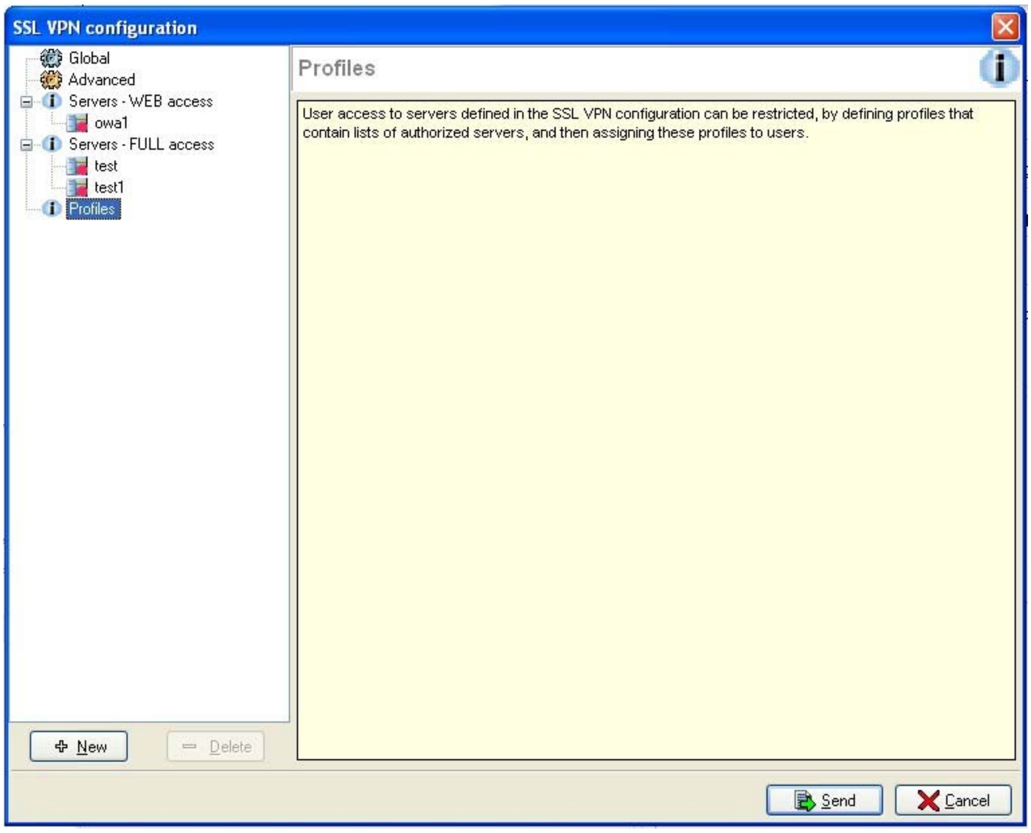
"Delete this server?"

3 Click on **Yes** to confirm the deletion.

WARNING
When a server is removed from the list of configured SSL VPN servers, it will automatically be removed from the profiles to which it belonged.

8.5.2.6. Profiles

If you wish to restrict access to servers in the SSL VPN configuration, you need to define the profiles containing the list of authorized servers, then assign them to users.



User access to servers defined in the SSL VPN configuration can be restricted, by defining profiles that contain lists of authorized servers, and then assigning these profiles to users.

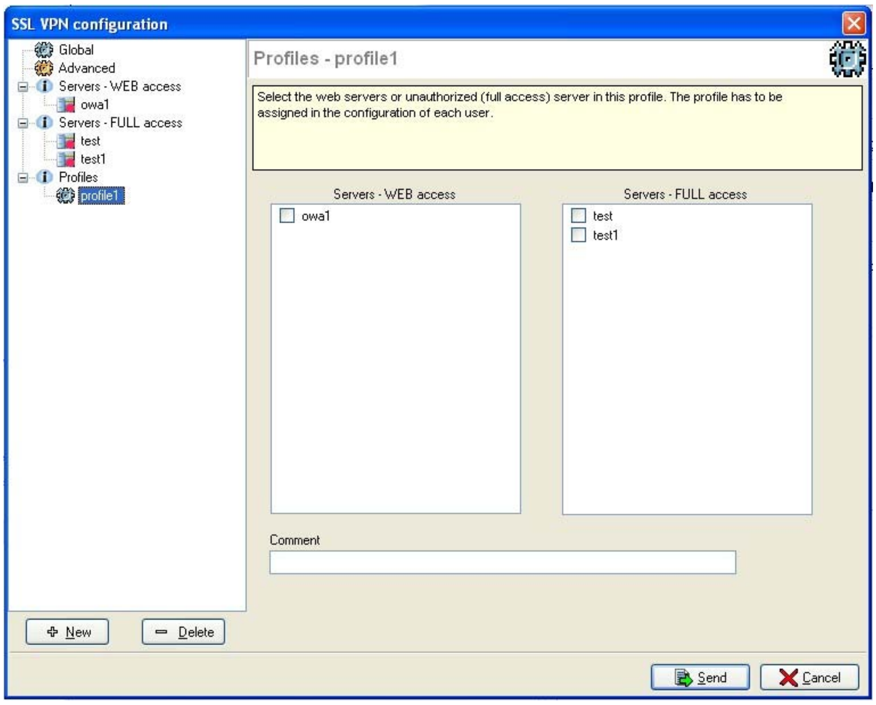
Figure 268: Configuring the SSL VPN – Profiles

Operation

All servers configured in the SSL VPN module are listed on the NETASQ authentication portal by default. As such, users who have the right to access SSL VPN features on the Firewall have access to all the servers configured by the administrator. The concept of using profiles enables determining which users will have access to which servers configured in SSL VPN.

Configuring a profile

Adding a profile



Select the web servers or unauthorized (full access) server in this profile. The profile has to be assigned in the configuration of each user.

Servers - WEB access
□ owa1

Servers - FULL access
□ test
□ test1

Comment

Figure 269: Configuring the SSL VPN - Profiles

The procedure for adding a profile to the list of available SSL VPN profiles is as follows:

1 Click on **New** at the bottom of the SSL VPN configuration window, then specify the name of the profile according to the recommendations given in the window for defining the profile name.

2 From the list of web-access and full-access servers, select the servers that will be accessible to users that belong to this profile.

3 Click on **Send** to activate the configuration.

> **WARNING**
> Profiles cannot be created if there is not at least 1 configured SSL VPN server.

Deleting a profile

The procedure for deleting a profile is as follows:

1. Select the profile you wish to delete.
2. Click on **Delete**.

Using a profile

Profiles can be used in 2 ways – either as a default profile in SSL VPN configuration, or assigned to one or several users as the specific profile of these users.

Using a profile as a default profile

The procedure for using a profile as the default profile in SSL VPN configuration (users who do not have a specific profile will be assigned this default profile) is as follows:

1. Define the profile to be used as the default profile (name of the profile and associated servers) in the profile configuration menu.
2. In the **`Global`** menu in SSL VPN configuration, select the action **Default** in the configuration without profile.
3. Indicate the predefined profile in the option **Default profile**, then click on **Send** to apply the changes.

Using a profile as the specific profile for one or several users

The procedure for using a profile as the specific profile for one or several users (regardless of the list of servers defined by the default profile, these users will possess a list of specific servers) is as follows:

1. Define the profile to be used as the default profile (name of the profile and associated servers) in the profile configuration menu, then click on **Send** to apply the changes.
2. From the list of users in the **`Objects`** menu in NETASQ UNIFIED MANAGER, select the user to whom you wish to associate the predefined profile.
3. Select the **`Access`** tab in his user file and check the option **Via SSL VPN** if it has not yet been done.
4. Select the option **Use a specific profile** and indicate the profile you wish to assign to this user, then click on **Send** to apply the changes.

8.5.2.7. SSL VPN services on the NETASQ web portal

When authentication is activated on the Firewall (see *Part 12: Authentication*), the NETASQ web portal enables users to access NETASQ's SSL VPN features.

To access **SSL VPN** features, the procedure is as follows:

1. Open the web browser.
2. Indicate the URL "https:// Firewall_address" in the address bar.
3. The Firewall authentication page appears; the user has to log in.
4. If the user has the privileges to use VPN features the **`Secure access`** menu will appear, enabling access to SSL VPN features.

Accessing your conpagny's web sites via an SSL tunnel

This menu displays the list of websites the administrator has configured and to which users have access.

The link "Other methods of secures access" enables accessing other secure sites configured by the administrator.

Accessing your compagny's resources via an SSL tunnel

This menu displays the list of other servers the administrator has configured and to which users have access.

> ❗ **WARNING**
> No links are available on this page. However, this window must be kept open throughout the duration of the connection (the window can be reduced), otherwise the connection will be lost..

To access resources the administrator has configured, it has to be indicated to the client software (e.g. a mail client) that the server to which he has to connect to retrieve mail is no longer the usual mail server. An address like "127.0.0.1: Listening_port" where "Listening_port" is the port specified on the server configuration, has to be indicated.

The listening port for each configured server will be displayed in the NETASQ web portal page.

PART 9: PROXY CONFIGURATION

CHAPTER 1. PRESENTATION

A proxy is a system that relays connections that it intercepts or which have been addressed to it. As such, the proxy stands in for the initiator of the connection and fully recreates a new connection to the initial destination. Proxy systems can be used in particular for antivirus scans or for filtering connections.

The "Proxy" module available on NETASQ firewalls allows the configuration of the HTTP, SMTP POP3 and FTP proxies.

- The HTTP proxy relates to visited websites and requested web pages. Using this module, an antivirus analysis as well as URL filter functions can be performed.
- The SMTP proxy relates to the sending of e-mails. Antivirus and antispam functions can be performed.
- The POP3 proxy relates to the receipt of e-mails. Antivirus and antispam functions can be performed.
- The FTP proxy relates to file transfers. Antivirus functions can be performed.

9.1.1. For this chapter, you will need to have completed these steps

- Part 2: Installation, pre-configuration, integration
- Part 4: Objects

9.1.2. Purpose of this section

This part allows you to activate the HTTP and SMTP, FTP proxies, to redirect HTTP traffic to external proxy servers and to filter SMTP anjd POP3 traffic.

9.1.3. Accessing this section

➲ Access the dialog box by the **`Proxy`** menu in the NETASQ UNIFIED MANAGER menu directory.

You have to be connected with the modification privileges to be able to perform these modifications.

Before making any significant modification to your NETASQ firewall, we recommend that you perform a backup. As such, in case of a wrong move, you will be able to return to your previous configuration. For more information on backups, please refer to "*Backup".*

9.1.4. Introduction to this section

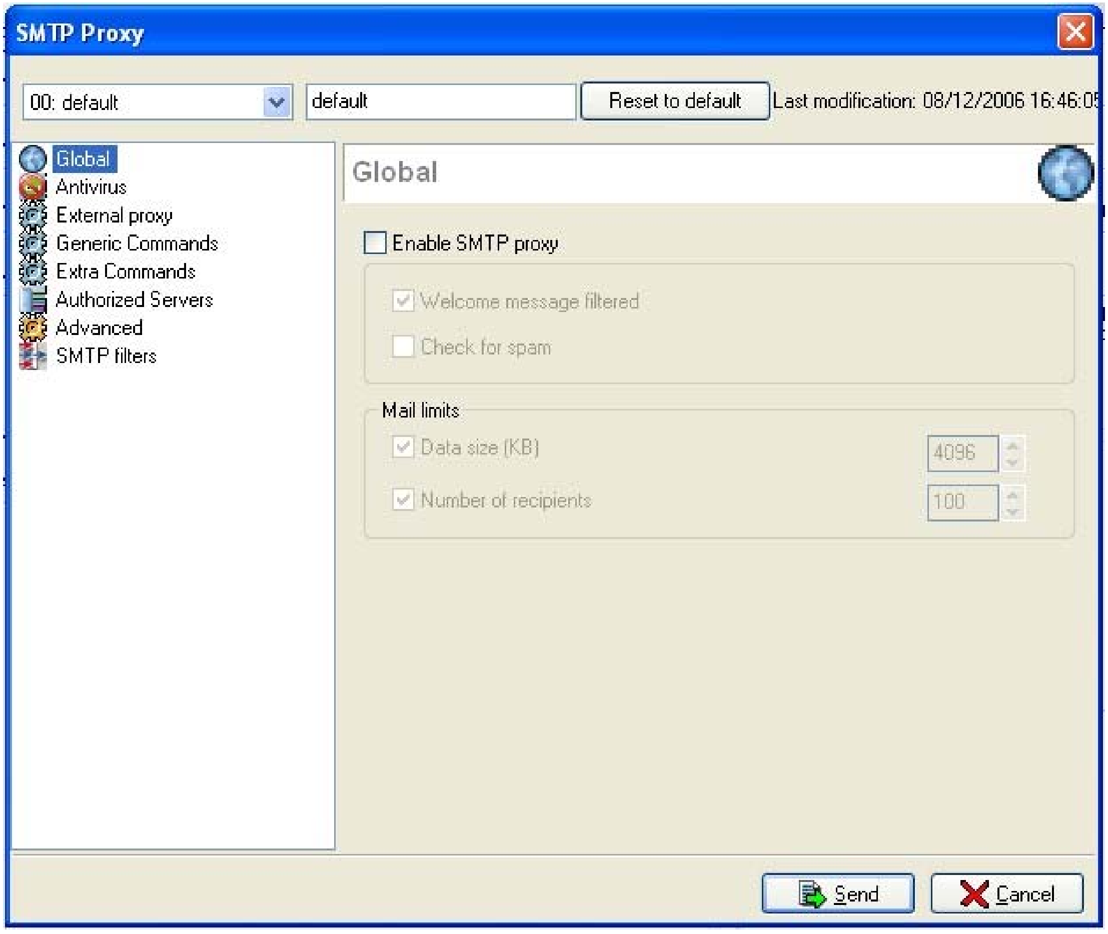
URL filtering tables are stored on the NETASQ firewall in slots (configuration files numbered from 01 to 10).

Each slot can be programmed for a precise time in the week, overriding the configuration of a previously activated slot. (see *Part 7/Chapter 3: "Slot Scheduler*").

9.1.5. The proxy window

This window consists of two parts:

- On the left, a directory showing the various features of **the various proxies.**
- On the right, the options that can be configured.



□ Enable SMTP proxy

☑ Welcome message filtered

□ Check for spam

Mail limits

☑ Data size (KB) 4096

☑ Number of recipients 100

Figure 270: Example of a proxy configuration screen

Four proxy profiles can now be created in order to adapt the proxy analysis to the source interface of the traffic. This will enable disabling certain features on authorized outgoing traffic but not on incoming traffic

These profiles are:

- 00: default
- 01: default 01
- 02: default 02

- 03: default 03

The action bar at the top of the screen indicates the HTTP profile currently on display. You can name each of the profiles in the **Name** field.

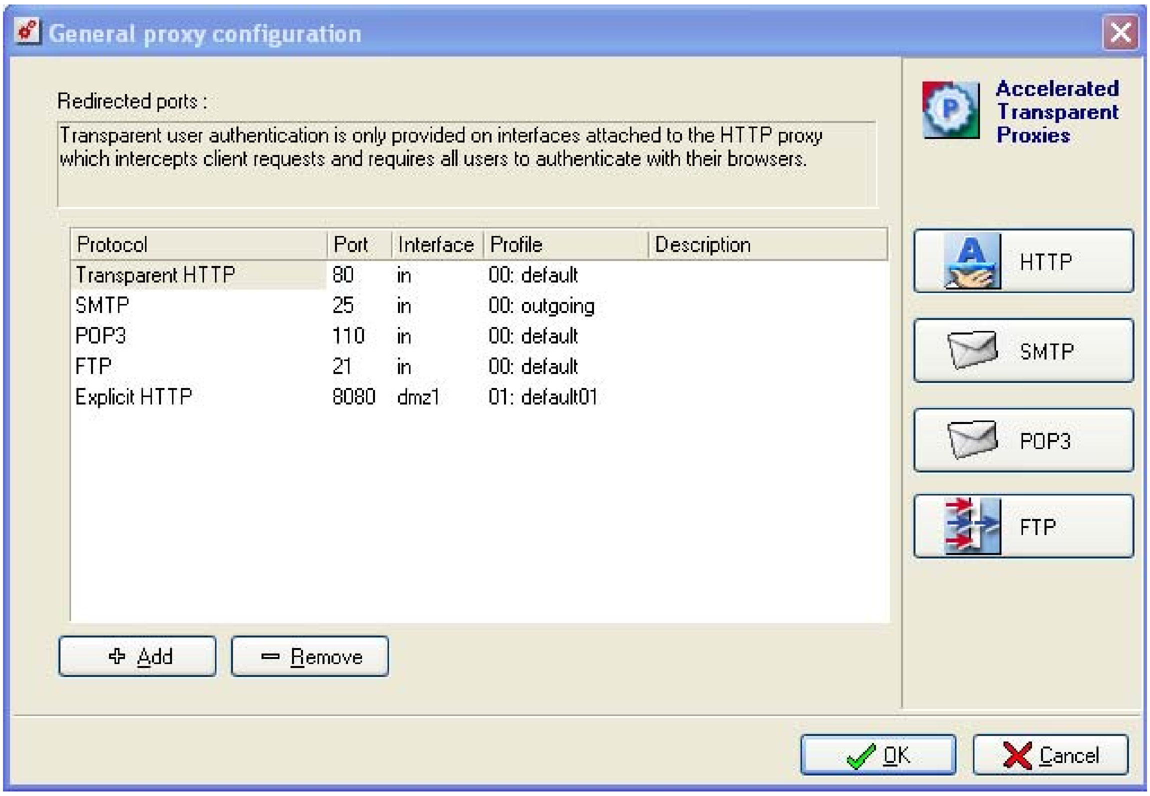
The **Reset configuration** button enables you to redefine the parameters of HTTP profiles in their original configuration.

The date located next to the button indicates the date the configuration was last modified.

CHAPTER 2. REDIRECTING TRAFFIC TO PROXIES ("GENERAL" MENU)

You can choose the ports and interfaces on which proxies will act. When a connection comes from the interface indicated and requests the service configured in this section, the proxy will intercept and manage the connection.

➲ This configuration is accessed via the menu `Proxy\General`.



Redirected ports :

Transparent user authentication is only provided on interfaces attached to the HTTP proxy which intercepts client requests and requires all users to authenticate with their browsers.

Protocol	Port	Interface	Profile	Description
Transparent HTTP	80	in	00: default	
SMTP	25	in	00: outgoing	
POP3	110	in	00: default	
FTP	21	in	00: default	
Explicit HTTP	8080	dmz1	01: default01	

Figure 271: General proxy configuration

The following parameters must be defined in order to redirect traffic to the proxies:

Protocol	Protocol managed by the proxy
Port	Port on which the proxy has to listen.
Interface	Interface on which the proxy listens.
Profile	Associates a Proxy profile to the proxy analysis, to enable different configurations according to interfaces, for example.
Comment	Comments associated to this row.

Ports of interfaces to filter are added or deleted with the **Add/Remove** buttons. By default URL filtering (HTTP proxy) applies to port 80 solely for hosts on the internal network, URL filtering (HTTP proxy) applies to port 8080, SMTP filtering applies to port 25 for hosts on the internal network, POP3 filtering applies to port 110, also for hosts on the internal network and FTP filtering on port 21. The listening ports can be modified except for the explicit proxy (8080).

The buttons to the right of the table (**HTTP**, **SMTP**, **POP3** and **FTP**) give direct access to the configuration windows of each proxy.

URL filters can be applied when a rule file is activated (see *Part 10/Chapter 4: URL filters*).

WARNING
Implicit rules are created for traffic intercepted by the proxies. You must therefore apply the Internet access rules only to URL filtering. If you activate a URL filter slot, the proxy will automatically be activated.

REMARK
Transparent authentication (the authentication page is automatically displayed to the user when he attempts to connect to the internet) is provided only to interfaces linked to the HTTP proxy which intercepts client requests. URL filtering does not apply to HTTPS requests.

CHAPTER 3. HTTP PROXY

9.3.1. Description

The HTTP proxy filters access to certain websites, meaning that it determines the web pages that the firewall will allow or block.

The HTTP proxy can operate in 2 modes – “transparent” mode and “explicit” mode.

9.3.1.1. Transparent mode

In transparent mode, a translation rule allows redirecting the traffic to the proxy’s listening port. The transparent proxy relies on address translation to identify the real destination of the server that the client seeks to query.

The explicit proxy allows referencing the proxy in a browser and sending HTTP requests directly to it.

This is how a web page is transported in transparent moode: The internal user requests a web page (for example http://www.Webserver.com/index.html). The firewall intercepts the request and checks that it complies with the URL filter rules before relaying the request. The web server responds to the internal user’s request and returns the requested web page. The firewall intercepts the server’s response and performs an antivirus scan on the contents and relays the page to the user.

9.3.1.2. Explicit mode

In explicit mode, your workstation connects to the proxy referenced in the web browser in the network parameters.

This mode offers two advantages:

- If you wish to identify several users that use the same IP address.

In explicit mode, the internal user requests a web page by typing its address (example http://www.Webserver.com/index.html). The browser transmits the request to the explicit proxy. After it has checked that the request complies with the URL filter rules, the firewall resolves the domain name www.Webserver.com by sending a DNS query. Then it sends the request to the web server to request the index.html page. Upon receiving the response page, the firewall performs the antivirus scan on the contents and relays the page to the user.

For web browsers to know which explicit proxy they have to use to reach a given URL, there are several possible configuration modes:

- Automatic detection (the information will be given by DHCP through a PAC file)
- Definition of the URL of the configuration file.
- Manual configuration (via the web browser).

For an automatic detection, there are 3 steps to perform in the firewall configuration:

1 Selecting a PAC file in the menu Part 12: Authentication\Web portal.

2 Authorizing the publication of the PAC file in the menu Part 12: Authentication\Internal interfaces.

3 Configuration of Part 11/Chapter 1: DHCP to generate a PAC file.

DEFINITION

The PAC file allows redirecting all HTTP and HTTPS requests to the explicit proxy, with the exceptions of requests on the firewall's authentication portal and requests on other protocols.

This file should contain:

```
Function FindProxyForURL(url, host)
{
// Exclusion of the proxy for the portal
if (host == "NUM_SERIE") {
return "DIRECT";
} else {
// For all URLs (http|https)
if (shExpMatch(url, "http:*") || shExpMatch(url, "https:*"))
return "PROXY NUM_SERIE:8080" ;
return "DIRECT";
}
}
```

The value of NUM_SERIE corresponds to either the NETASQ appliance's serial number or to a domain name. If a domain name is used, a specific certificate has to be inserted in the portal so as to replace the default certificate which corresponds to the serial number.

For further information on the explicit proxy, please refer to the Technical Note "Configuration HTTP-V1".

9.3.2. To use this feature, you will need to have completed these steps

9.3.2.1. For the transparent proxy:

- Part 5: Network configuration
- Part 4/Chapter 3: Users
- Part 12: Authentication
- Part 7/Chapter 2: Filters
- Part 10/Chapter 3: Antivirus
- Part 10/Chapter 4: URLFilters

9.3.2.2. For the explicit proxy:

- Part 5: Network configuration
- Part 4/Chapter 3: Users
- Part 7/Chapter 2: Filters
- Part 10/Chapter 3: Antivirus
- Part 10/Chapter 4: URL Filters

9.3.3. The steps after the configuration of the explicit HTTP proxy

- Part 11/Chapter 1: DHCP (Optional)
- Configuration of the DNS cache service
- Modification of the configuration of the Part 12/Chapter 1: Captive portal
- Configuration of client workstations. (Cf. *See Technical Note on HTTP configuration)*

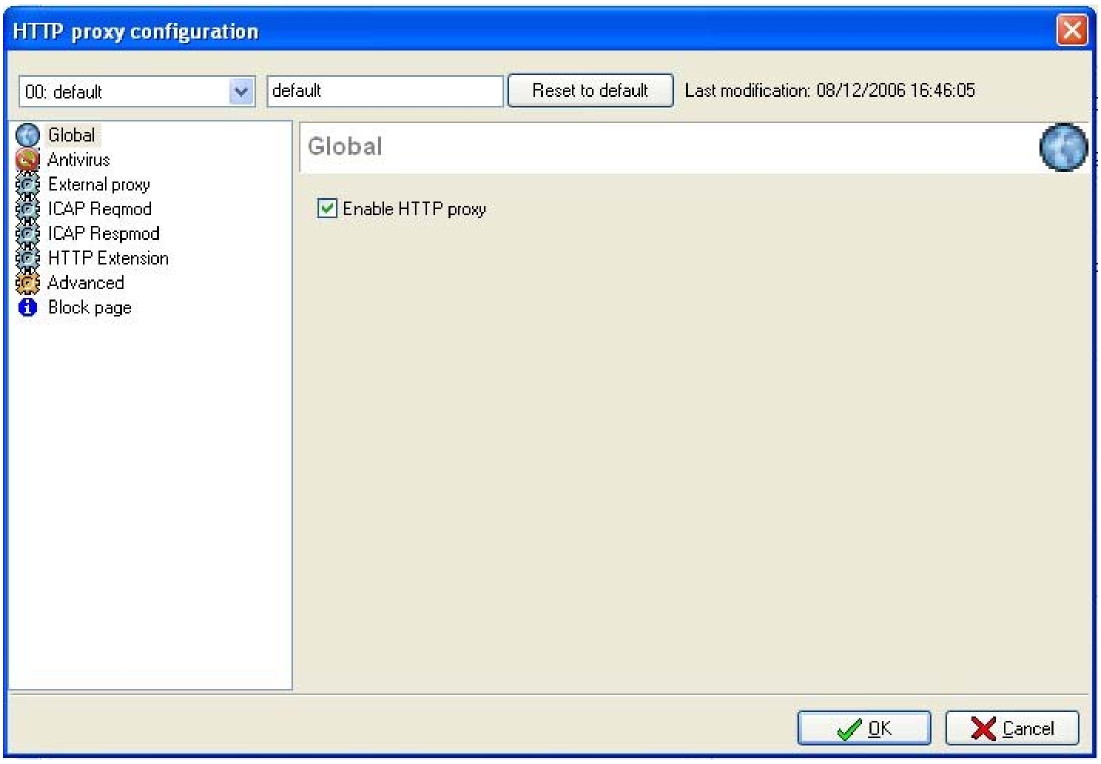
9.3.4. Accessing this feature

Go to the **`HTTP Proxy`** menu from the NETASQ UNIFIED MANAGER menu directory.

9.3.5. Description of the configuration windows

9.3.5.1. Global

The HTTP proxy has to be enabled in order for it to be used – via the menu **`Proxy\HTTP Proxy.`**The following window will appear:



HTTP proxy configuration

00: default | default | Reset to default | Last modification: 08/12/2006 16:46:05

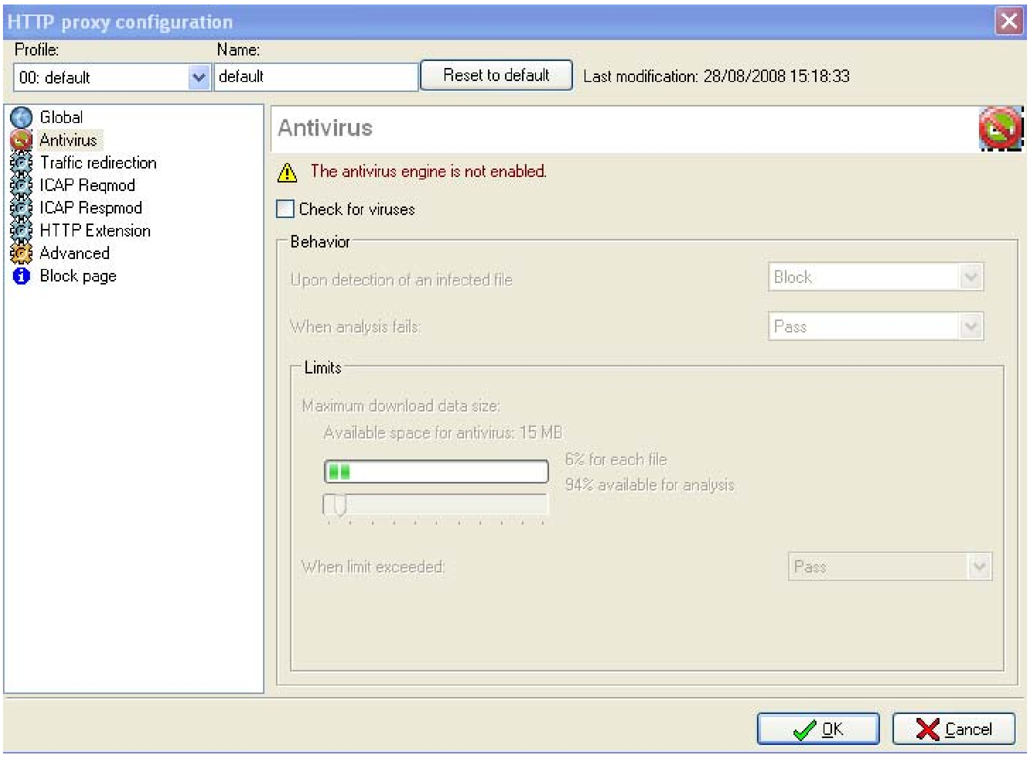
Global

☑ Enable HTTP proxy

Figure 272: Configuring the HTTP proxy

Enable HTTP proxy	Activates the HTTP proxy and performs the analyses specified in the menus that follow.

9.3.5.2. Antivirus



HTTP proxy configuration

Profile: 00: default | Name: default | Reset to default | Last modification: 28/08/2008 15:18:33

Antivirus

The antivirus engine is not enabled.

□ Check for viruses

Behavior

Upon detection of an infected file: Block

When analysis fails: Pass

Limits

Maximum download data size:

Available space for antivirus: 15 MB

6% for each file

94% available for analysis

When limit exceeded: Pass

Figure 273: Configuring the HTTP proxy - Antivirus

Activating the HTTP proxy enables the activation of the antivirus module for HTTP traffic (only on GET queries). The procedure for activating the antivirus module is as follows:

Check for viruses

Activates the antivirus module by selecting the option **Check for viruses** in the `Antivirus` menu.

Behavior

The **Behavior** section describes the antivirus module's reaction to certain events.

The option **Upon detection of an infected file** contains two options – "Pass" and "Block". If "Block" is selected, the analyzed file will not be transmitted. If "Pass" is selected, the antivirus module will transmit the file being analyzed.

The option **When analysis fails** defines how the module will behave if the analysis of the file it is scanning, fails.

> **Example**
>
> If the file is locked, the antivirus module will not succeed in analysing it.

If **Block** has been specified, the file being analysed will not be transmitted.
If **Pass** has been specified, the file being analysed will be transmitted.

Limits

The option **Maximum download data size** depends on the hardware capacities on each Firewall model but can be adapted to the needs of the enterprise by moving the scale.

WARNING

When manually defining a size limit for analyzed data, ensure that all values are coherent. The total memory space, represented by the scale, corresponds to a common space for all the resources reserved for the Antivirus service. If you define the size limit for analyzed data on HTTP as 100% of the total size, no other files can be analyzed at the same time.

The option **When limit exceeded** defines how the module will behave if the size of the file being analysed exceeds the authorized limit.

If **Block** has been specified, the file being analysed will not be transmitted.
If **Pass** has been specified, the file being analysed will be transmitted.

9.3.5.3. External proxy

The HTTP proxy is used for URL filtering (see *Part 10/Chapter 4: URL filters*) but it also redirects users' HTTP requests from internal network users to external proxies.

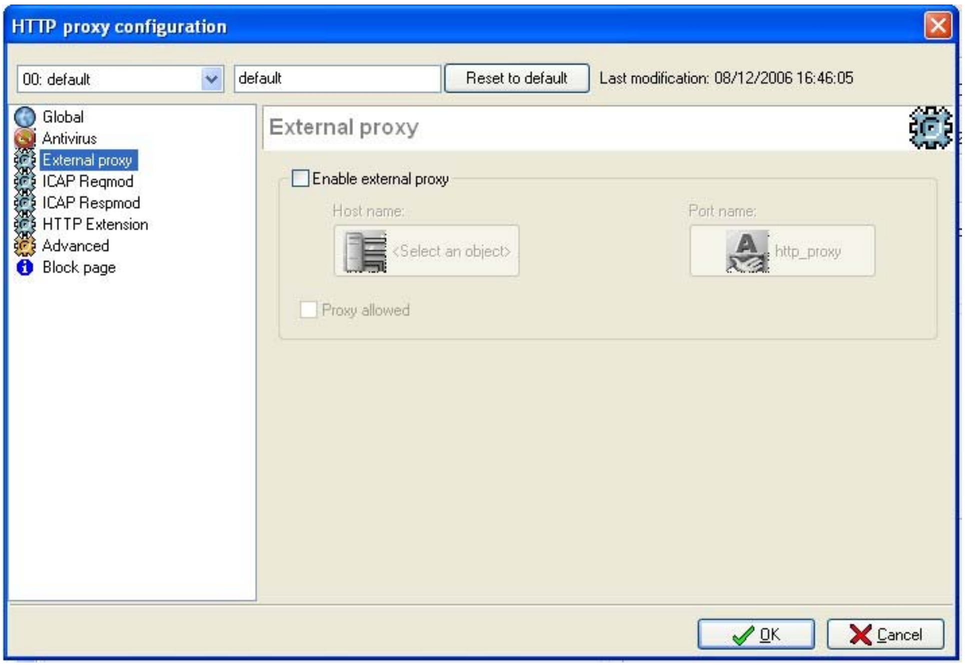
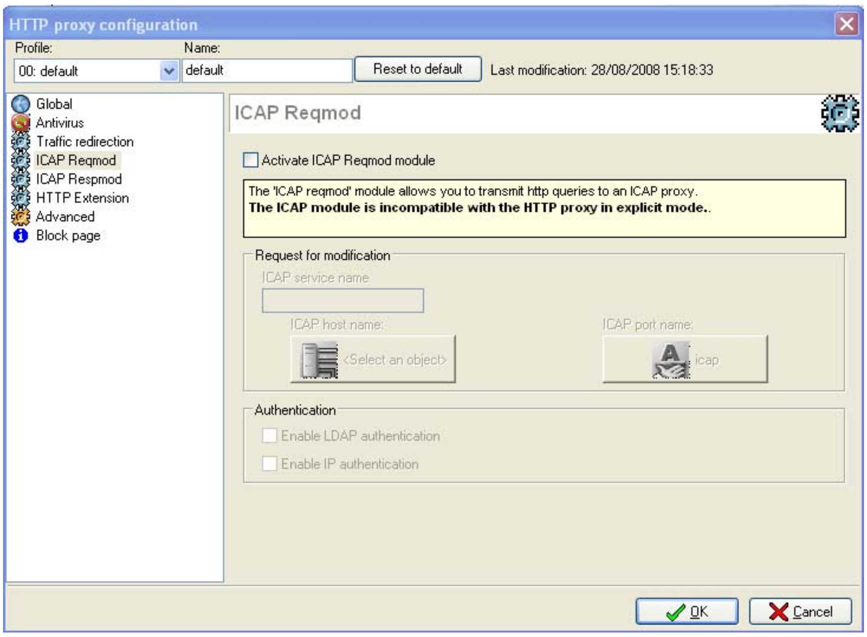


Figure 274: Configuring the HTTP proxy – External proxy

Enable external proxy	To activate this redirection, check the corresponding box and then specify the server's IP address and the port on which it receives requests. If the administrator has specified a server group in the option **Hostname**, the Firewall will perform load balancing between the different external proxies of the group according to the source host (a source host will always use the same external proxy).
Proxy allowed	If the external HTTP proxy requires user authentication, the administrator can select the option **Proxy allowed** in the **External proxy** menu in order to send information on the user (obtained from the Firewall's authentication module) to the proxy.

9.3.5.4. ICAP Reqmod



The 'ICAP reqmod' module allows you to transmit http queries to an ICAP proxy.
The ICAP module is incompatible with the HTTP proxy in explicit mode.

Figure 275: Configuring the HTTP proxy – ICAP Reqmod

Definition

ICAP or **Internet Content Adaptation Protocol** ensures interoperability with content analysis and treatment solutions such as WebWasher and allows URL filtering or content filtering services. It functions in two modes: **Reqmod** and **Respmod**.

Reqmod (**Request for Modification**) functions according to the following principle:

- An HTTP client sends an HTTP request.
- The request arrives on the firewall and is sent to the ICAP server.
- The ICAP server sends a reply to the Firewall which transmits it to the web server concerned.

Respmod functions in the opposite direction.

The NETASQ Firewall supports both modes: **Icap Reqmod** and **Icap Respmod**.

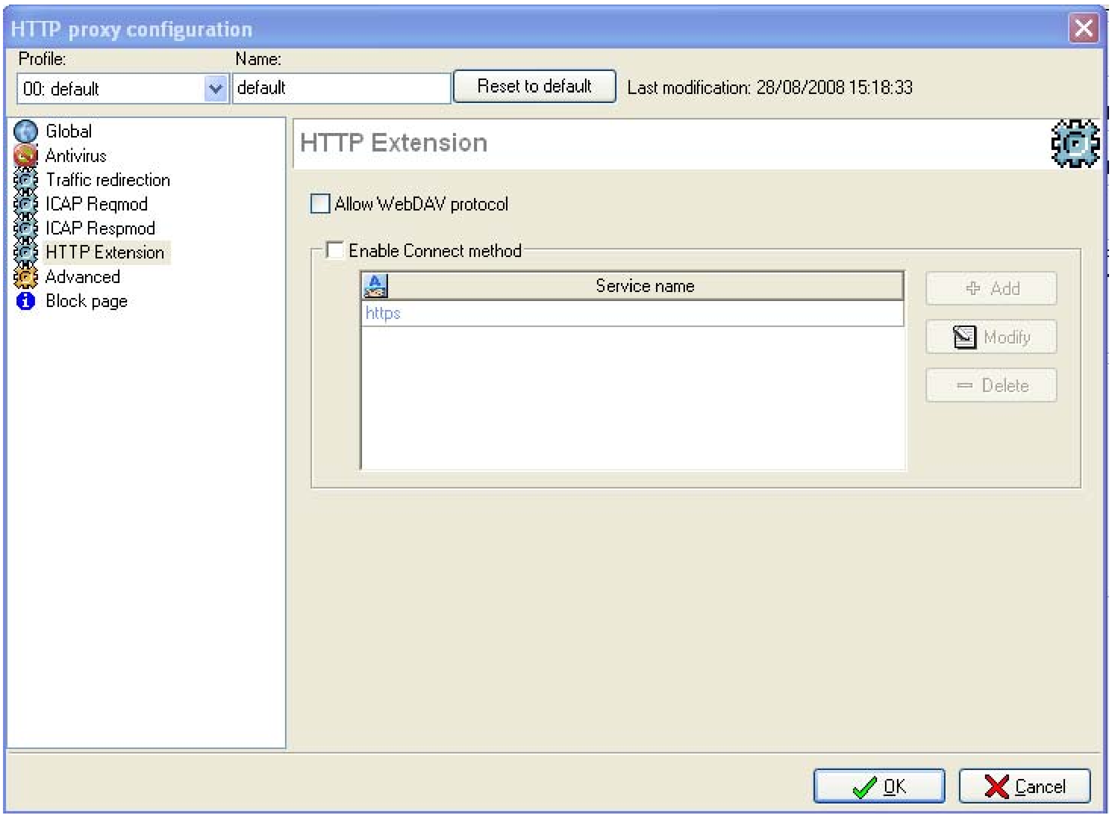
Activate ICAP Reqmod module	Activates the ICAP Reqmod module and performs the analyses specified in the menus that follow.
Request for modification	Indicates the name of the service to be set up. This varies according to the solution used. The ICAP server and the port used are needed for setting up the ICAP service.
Authentication	Information available on the Firewall can be used to perform ICAP services. **Example** it is possible to define that such and such a site is only accessible by such and such a person in an ICAP server. In this case, you can filter according to an LDAP identifier or an IP address. The option **Enable LDAP Authentication** allows using information relating to the LDAP database (namely the identifier of an authenticated user). The option **Enable IP Authentication** allows using the IP addresses of HTTP clients requesting to “adapt”.

9.3.5.5. ICAP Respmod

Activate ICAP Reqmod module	Enables the ICAP Respmod and conducts the analyses specified in the following menus.
Request for modification	Indicates the name of the service to be set up. This information varies according to the solution used, the ICAP server as well as the port used.
Authentication	Information available on the firewall can be used for ICAP services. **Example** It is possible to define in an ICAP server that a particular site can only be intended for a particular person. In this case, you can filter according to an LDAP identifier or an IP address. The option **Enable LDAP authentication** allows using information relating to the LDAP database (especially the identifier of an authenticated user). The option **Enable IP authentication** allows using IP addresses of HTTP clients that make the request that is to be adapted.

WARNING
The ICAP Respmod cannot be used when an HTTP virus search has been enabled. The following message appears: “Cannot enable ICAP Respmod and antivirus on HTTP simultaneously”.

9.3.5.6. HTTP extension tab



Profile: 00: default
Name: default
Last modification: 28/08/2008 15:18:33

□ Allow WebDAV protocol

□ Enable Connect method

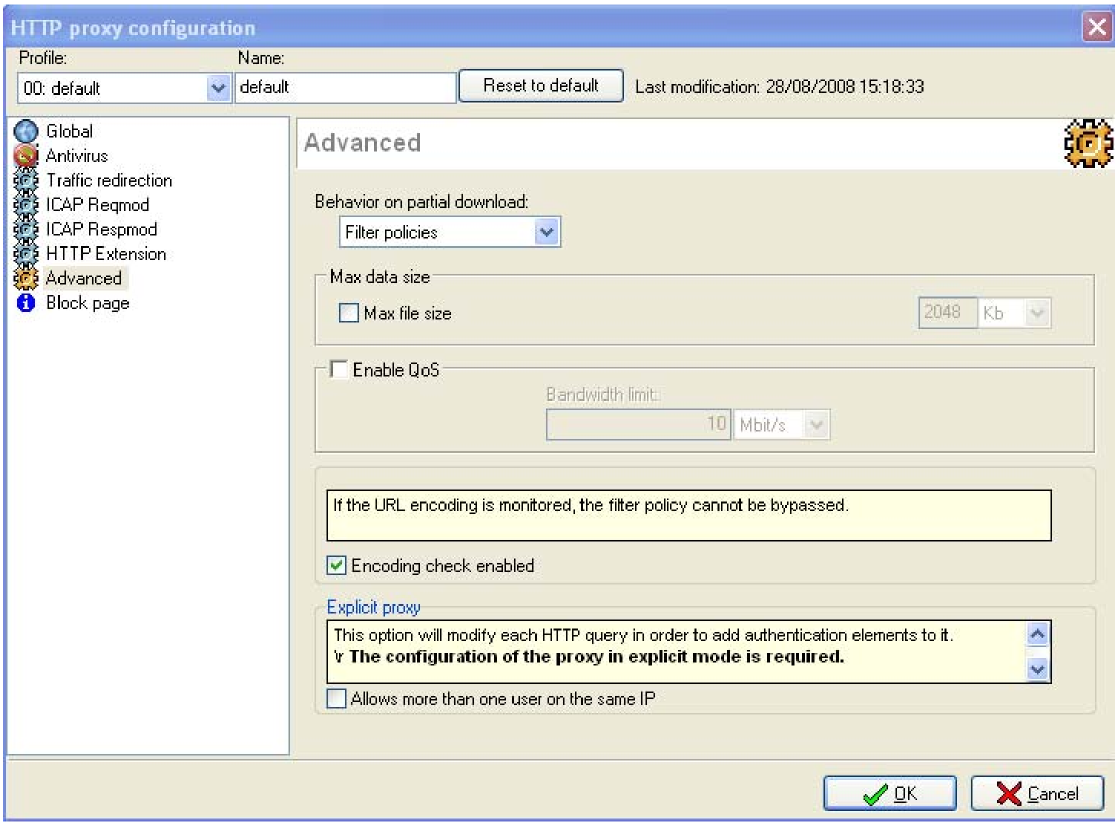
Service name
https

Figure 276: Configuring the HTTP proxy - HTTP Extension

The **`HTTP Extension`** tab allows configuring the following parameters:

Allow WebDAV protocol	WebDAV is a set of extensions to the HTTP protocol concerning the edition and collaborative management of documents. If this option has been selected, the WebDav protocol will be authorized in the NETASQ Firewall.
Enable CONNECT Method	The **CONNECT** method allows building secure tunnels through proxy servers. The field “Service name” is used for specifying the types of services which may use such a method. If this option has been selected, the **CONNECT** method will be authorized in the NETASQ Firewall. The **Add** button allows you to add services via the object database. The **Modify** button allows you to replace a previously selected service with another. The **Delete** button allows you to delete the selected service. A “Delete service…” message will appear to confirm the deletion.

9.3.5.7. Advanced tab



Profile: 00: default

Name: default

Last modification: 28/08/2008 15:18:33

Behavior on partial download: Filter policies

Max data size

□ Max file size 2048 Kb

□ Enable QoS

Bandwidth limit: 10 Mbit/s

If the URL encoding is monitored, the filter policy cannot be bypassed.

☑ Encoding check enabled

Explicit proxy

This option will modify each HTTP query in order to add authentication elements to it.
The configuration of the proxy in explicit mode is required.

□ Allows more than one user on the same IP

Figure 277: Configuring the HTTP proxy - Advanced

The **Advanced** menu allows configuring the following parameters:

Behavior on partial download	When a download is incomplete, for example, due to a connection failure during a file download via FTP, the user can continue to download from where the error occured, instead of having to download the whole file again. This is called a partial download – the download does not correspond to a whole file. The option **Behavior on partial download** allows defining the behavior of the Firewall's HTTP proxy towards this type of download. ● **Block**: partial downloads are prohibited ● **Filter policies**: partial downloads are authorized and the antivirus module filters the traffic. ● **Pass**: partial downloads are authorized but there will not be any antivirus analysis.
Max data size	When files downloaded off the internet via HTTP get too huge, they can deteriorate the internet bandwidth for quite a long stretch of time. To avoid this situation, select the option **Max file size** and indicate the maximum size (in Kilobytes) that can be downloaded by HTTP.
Enable QoS	Regulation of HTTP traffic. This option allows you to define a maximum throughput for this traffic type. A derivative of the traffic curve allows the determination of whether packets have to be deleted so as not to exceed the limit.
Encoding check	The filter policy cannot be bypassed if this option is selected.

enabled	
Allow more than one user on the same IP	If this option is selected, the “basic” HTTP authentication method will be enabled. Several users can be behind the same source IP address. This option is to be used with the explicit proxy. *For further information on the topic of multiple authentication, please refer to the Technical Note “Authentication of multiple users”.*

Authentication of multiple users

Users sharing the same IP address can be authenticated. In this case, the explicit HTTP proxy has to be enabled. The configuration requires 5 steps:

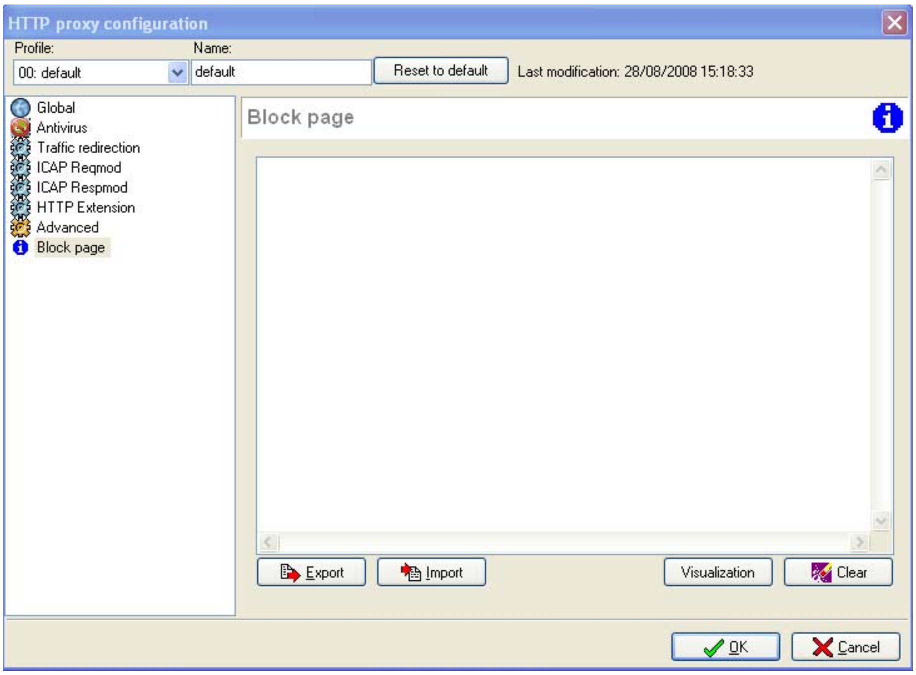
1 Configuration of the Explicit HTTP proxy which is necessary for multiple authentication.
2 Configuration of the DNS cache service.
3 Configuration of URL filter rules
4 Configuration of authentication and the portal (Part 12).

Setting up a multiple authentication for users with the same IP address requires the prior creation of an LDAP database as well as the addition of users before they are authenticated.

For further information on the topic of multiple authentication, please refer to the Technical Note “Authentication of multiple users”.

9.3.5.8. Block page

➲ Select the menu **Block page**. The following window will appear:



HTTP proxy configuration

Profile: 00: default
Name: default
Last modification: 28/08/2008 15:18:33

Figure 278: Configuring the HTTP proxy – Block page

This page appears when the HTTP proxy rejects a user’s HTTP request (unauthorized URL).

This page is displayed in the user’s navigator instead of the Web page requested.

A NETASQ page is displayed by default; this informs the user that his request cannot be complied with because of the filter rule.

You can replace this default page with your own page by entering the HTML code of the page to be displayed in this window.

You can add the following data to this page:

- $rule: name of the category
- $host: name of the HTTP destination host (e.g.: www.google.com)
- $url: blocked URL

> **Example**
> /search?hl=fr&q=test&btng=rechercher&meta=

REMARK
Use an HTML editor to create your own block messages, then save the document in HTML. You can then import it using the **Import** button.
Any page edited in the **`block page`** section can be saved and imported to another Firewall using the **Export** button.
You can display the contents of the HTML page by clicking on the **Visualization** button. This will open your machine's default navigator automatically.
If the page you have created does not suit you anymore, the **Clear** button allows you to delete it and use the default NETASQ page.

9.3.5.9. Optimizing the display time of web pages

Changes have been made to pipelining and chunking, allowing a significant improvement to web pages in the browser.

CHAPTER 4. SMTP PROXY

9.4.1. Introduction

9.4.1.1. Definition

In the last few years, electronic mail has become a communication tool widely used by companies and government bodies. The speedy and high-performance transmission of information enables cost reduction and a remarkable improvement in competitiveness

However, without the right traffic management, the use of this tool may prove disastrous to productivity.

Mass unsolicited mail (such as advertisements and newsletters) may affect the availability of your bandwidth. Furthermore, receiving infected messages from the internet creates flaws in your security.

These pitfalls can generally be attributed to the use of the mail program for personal purposes.

DEFINITION
SMTP (*Simple Mail Transfer Protocol*), a TCP/IP communication protocol, is used for electronic mail exchanges on the internet.

This is a protocol which functions in connected mode, encapsulated in a TCP/IP frame. Mail is directly placed in the recipient's mail server. **SMTP** functions with text commands sent to the **SMTP** server (on port 25 by default). Each of the commands the client sends (validated by the ASCII CR/LF character string, the equivalent of pressing the Enter key) is followed by the **SMTP** server's response comprising a number and descriptive message.

It is therefore possible to send mail using telnet on port 25 of the **SMTP** server.

9.4.1.2. Various possible uses of the SMTP proxy

The SMTP proxy can be used to filter various types of traffic:

Traffic between internal network users and the mail gateway

The gateway must be located in the DMZ. In this case mail sent by the internal network message service's clients to the internal gateway can be filtered.

Consequences

The mail server may be relieved of messages which are too bulky (an error message is sent to the mail client if a message is rejected; the internal users cannot use the server for **SMTP** relaying). Your server may be protected from HAWKs by blocking messages sent to several recipients simultaneously.

DEFINITION
HAWK: method used by certain viruses to propagate using contacts taken from the OUTLOOK address book .

Configuration

Activate **SMTP** redirection on port 25 and the internal interface.

SMTP traffic from the mail gateway to the Internet

The Firewall is located between the internal gateway and the Internet. The mail sent by the internal gateway to the Internet is filtered.

Consequences

SMTP relaying is impossible when using the internal gateway. However, the outward transmission of attachments (this prevents leaking data and confidential documents, for example) can be limited.

WARNING
The messages are completely destroyed. It deletes the SMTP server's welcome banner.

Configuration

Activate **SMTP** redirection on port 25 and on the interface on which the mail server is situated.

SMTP traffic from the Internet to the internal gateway

The Firewall is located between the internal gateway and the Internet. Mail received by the gateway is filtered.

Consequences

You can limit the size of incoming mail to avoid overloading the server. You may limit spam mail and prohibit mail from certain senders.

Configuration

Activate **SMTP** redirection on port 25 and the OUT interface.

9.4.2. To use this feature, you will need to have completed these steps

- The domain names allowed for outgoing traffic in SMTP on your network.
- The e-mail filter policy that you wish to implement.

9.4.3. Accessing this feature

➲ The SMTP proxy has to be activated in order to be used, via the menu **`Proxy`\`SMTP Proxy.`**

A default profile can now be created to manage proxy bypass.

The action bar at the top of the screen indicates the SMTP proxy profile currently displayed. You can name each of the profiles.

9.4.4. Description of the configuration windows

9.4.4.1. Global

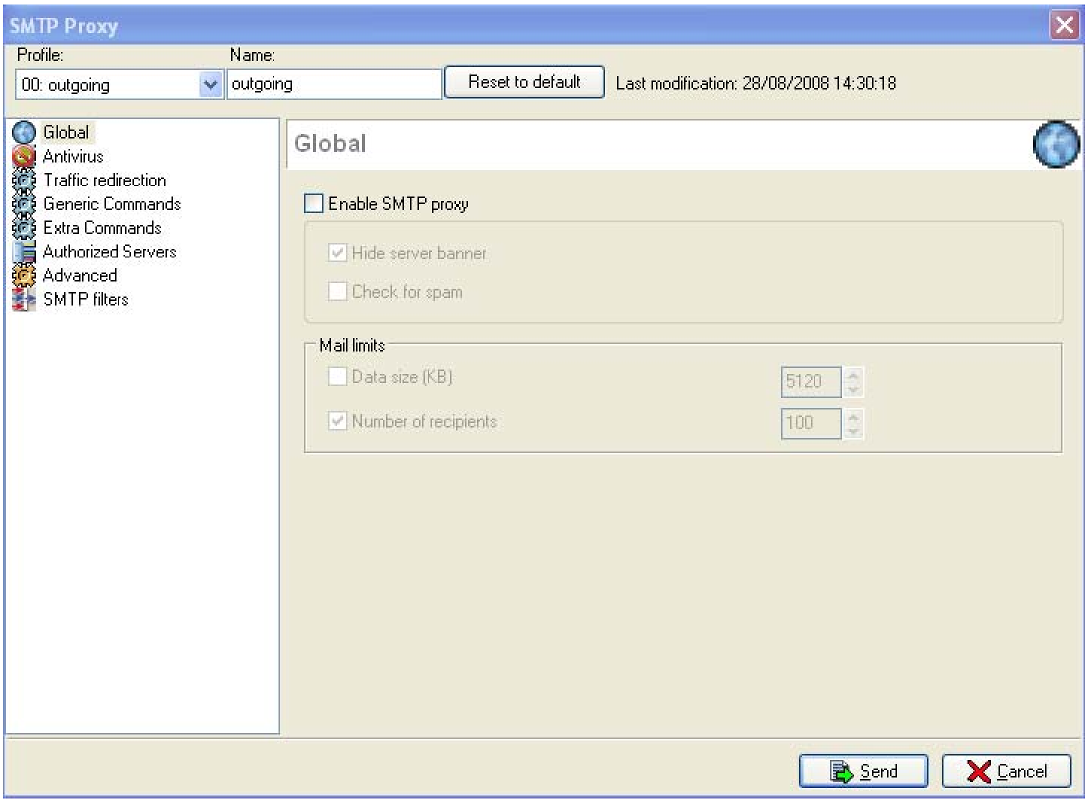
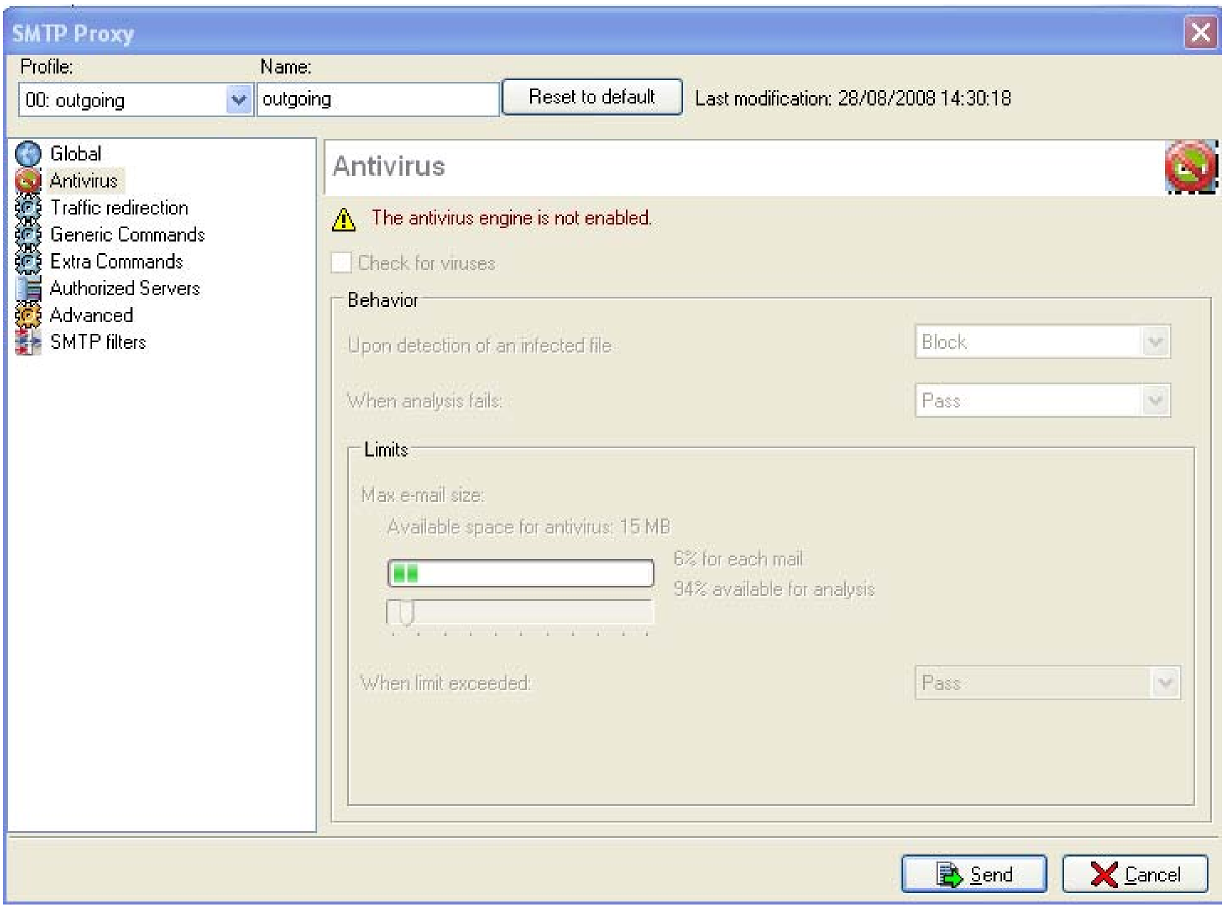


Figure 279: SMTP Proxy - Global

The **Global** menu enables configuring the following parameters:

Enable SMTP proxy	Activates the SMTP proxy and performs the analyses specified in the menus that follow. In particular, activating the SMTP proxy also allows searching for viruses in SMTP traffic.
Welcome message filtered	When this option is ticked your message server's banner is no longer transmitted in an SMTP connection. In fact this banner contains data which may be exploited by hackers (type of server, software version etc.).
Check for spam	Activates the SMTP proxy features that check for spam
Data size (KB)	Specify in Kbytes the maximum size of messages passing through the NETASQ Firewall. The Firewall will delete messages which are too large (an error message is sent to the sender). If a line exceeds 2048 bytes, a log will be kept.
Number of recipients	Specify the maximum number of recipients a message may contain. The Firewall will delete messages with too many recipients (an error message is sent to the sender). Allows restricting spam mail.

9.4.4.2. Antivirus



SMTP Proxy

Profile: 00: outgoing

Name: outgoing

Reset to default

Last modification: 28/08/2008 14:30:18

Antivirus

The antivirus engine is not enabled.

□ Check for viruses

Behavior

Upon detection of an infected file: Block

When analysis fails: Pass

Limits

Max e-mail size:

Available space for antivirus: 15 MB

6% for each mail

94% available for analysis

When limit exceeded: Pass

Figure 280: SMTP Proxy - Antivirus

Check for viruses Activates the SMTP proxy features that check for viruses when the option **Enable SMTP Proxy** is enabled in the **Global** menu.

Behavior The "Behavior" section describes the antivirus module's reaction to certain events.

The option **Upon detection of an infected file** contains two options – "Pass" and "Block". If "Block" is selected, the analyzed file will not be transmitted. If "Pass" is selected, the antivirus module will transmit the file even if it has been detected as infected.

The option **When analysis fails** defines how the module will behave if the analysis of the file it is scanning, fails.

> **Example**
> If the file is locked, the antivirus module will not succeed in analysing it.

If **Block** has been specified, the file being analysed will not be transmitted.
If **Pass** has been specified, the file being analysed will be transmitted.

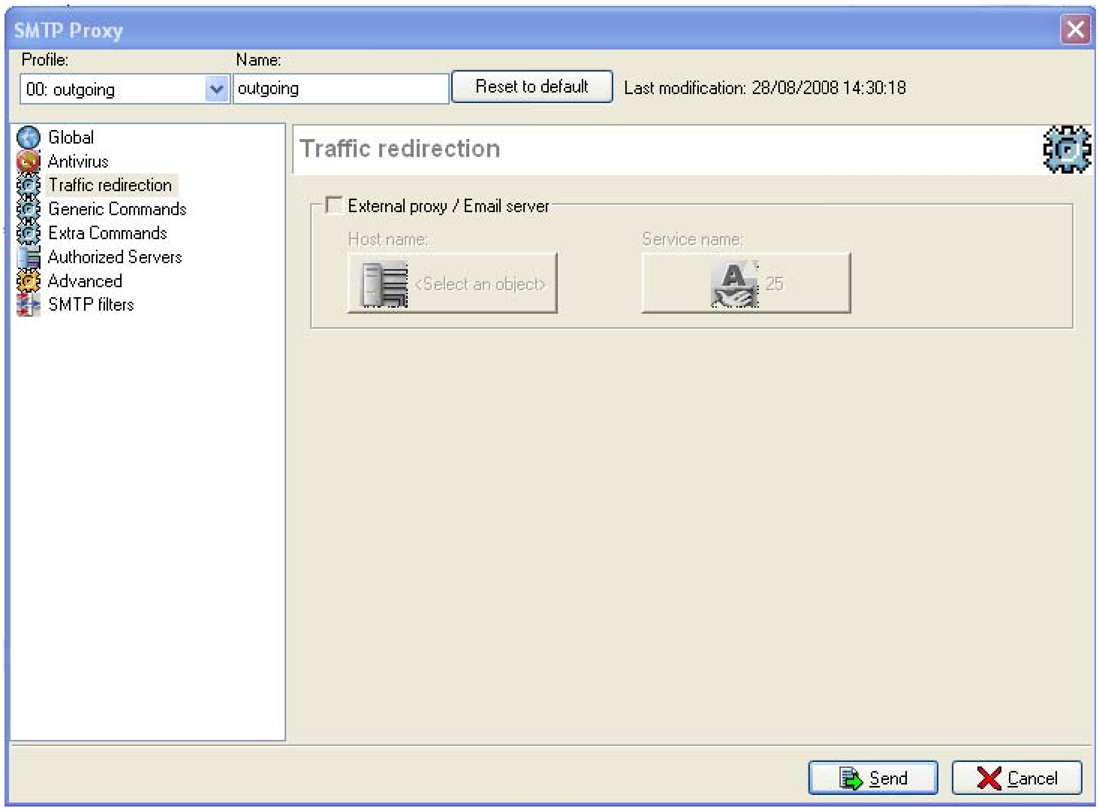
Limits The option **Available space for antivirus** depends on the hardware capacities on each Firewall model but can be adapted to the needs of the enterprise by moving the scale.

The option **When limit exceeded** defines how the module will behave if the size of the file being analysed exceeds the authorized limit.

	If **Block** has been specified, the file being analysed will not be transmitted. If **Pass** has been specified, the file being analysed will be transmitted.

WARNING
When manually defining a size limit for analyzed data, ensure that all values are coherent. The total memory space, represented by the scale, corresponds to al lthe resources reserved for the Antivirus service. If you define the size limit for analyzed data on SMTP as 100% of the total size, no other files can be analyzed at the same time.

9.4.4.3. Traffic redirection



Profile: 00: outgoing
Name: outgoing
Last modification: 28/08/2008 14:30:18

Traffic redirection

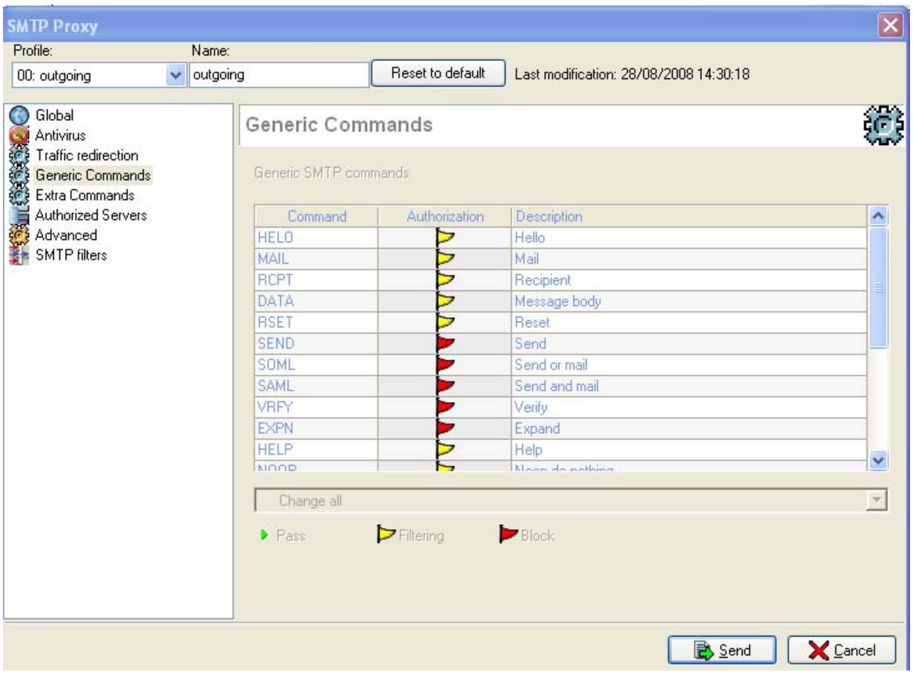
□ External proxy / Email server
Host name: <Select an object>
Service name: 25

Figure 281: SMTP Proxy – External proxy

The SMTP proxy enables the redirection of SMTP requests from users on the internal network to external proxies.

To activate this redirection, select the **External proxy** checkbox then enter the IP address of the server as well as of the service on which requests are received. . If the administrator has specified a server group in the option **Hostname**, the Firewall will perform load balancing between the different external proxies of the group according to the source host (a source host will always use the same external proxy).

9.4.4.4. Generic commands



Profile: 00: outgoing
Name: outgoing
Last modification: 28/08/2008 14:30:18

Generic Commands

Generic SMTP commands

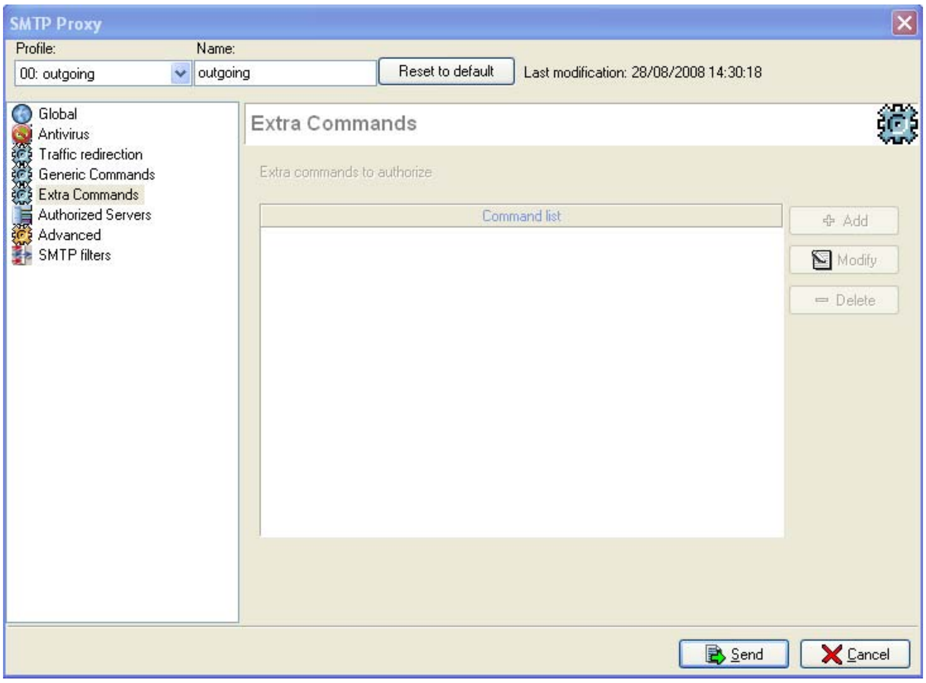
Command	Authorization	Description
HELO	🟨	Hello
MAIL	🟨	Mail
RCPT	🟨	Recipient
DATA	🟨	Message body
RSET	🟨	Reset
SEND	🟥	Send
SOML	🟥	Send or mail
SAML	🟥	Send and mail
VRFY	🟥	Verify
EXPN	🟥	Expand
HELP	🟨	Help
NOOP	🟨	Noop do nothing

▶ Pass 🟨 Filtering 🟥 Block

Figure 282: SMTP Proxy – Generic commands

This menu allows you to authorize or reject SMTP commands defined in the RFCs. You can authorize or prohibit a command or check that the command syntax complies with the RFC in force.

9.4.4.5. Extra commands



Profile: 00: outgoing
Name: outgoing
Last modification: 28/08/2008 14:30:18

Extra Commands

Extra commands to authorize

Command list

Figure 283: SMTP Proxy – Extra commands

All commands which are not specified in the RFCs are prohibited by default. However, some mail systems use non-standardized additional commands. You may therefore add these commands to allow them through the Firewall

The **Add**, **Modify** and **Delete** buttons allow making changes to the list of commands.

9.4.4.6. Authorized Servers

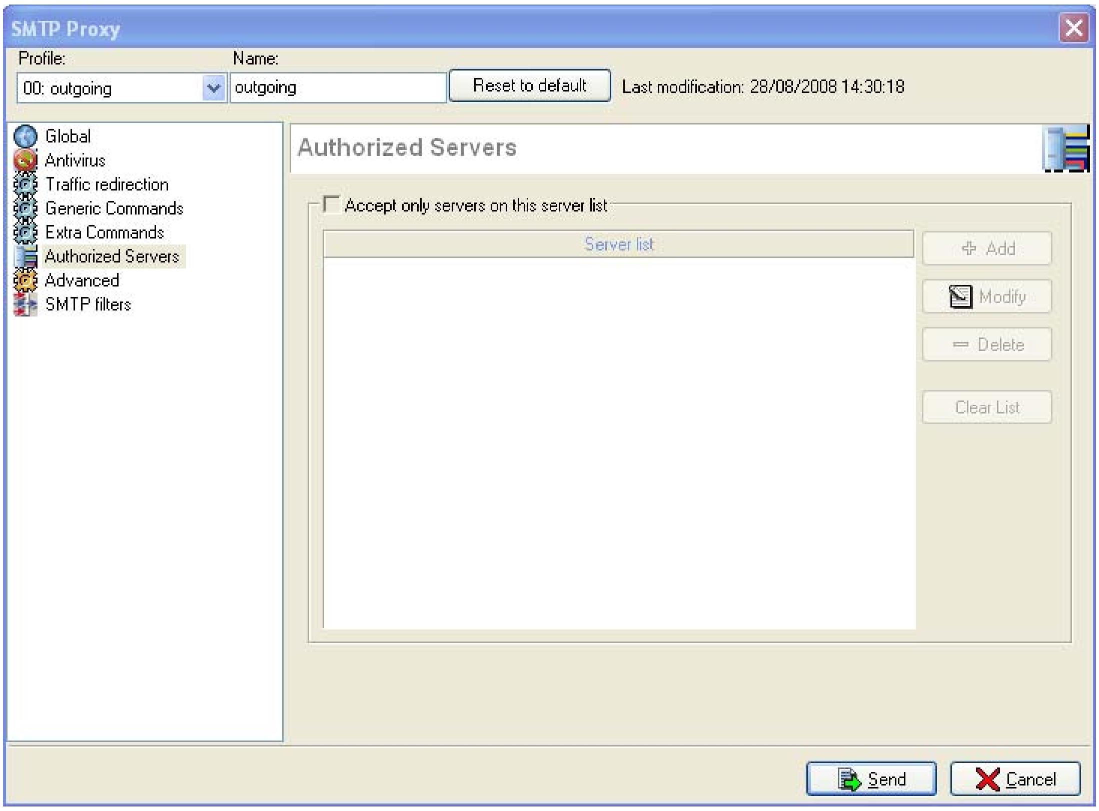
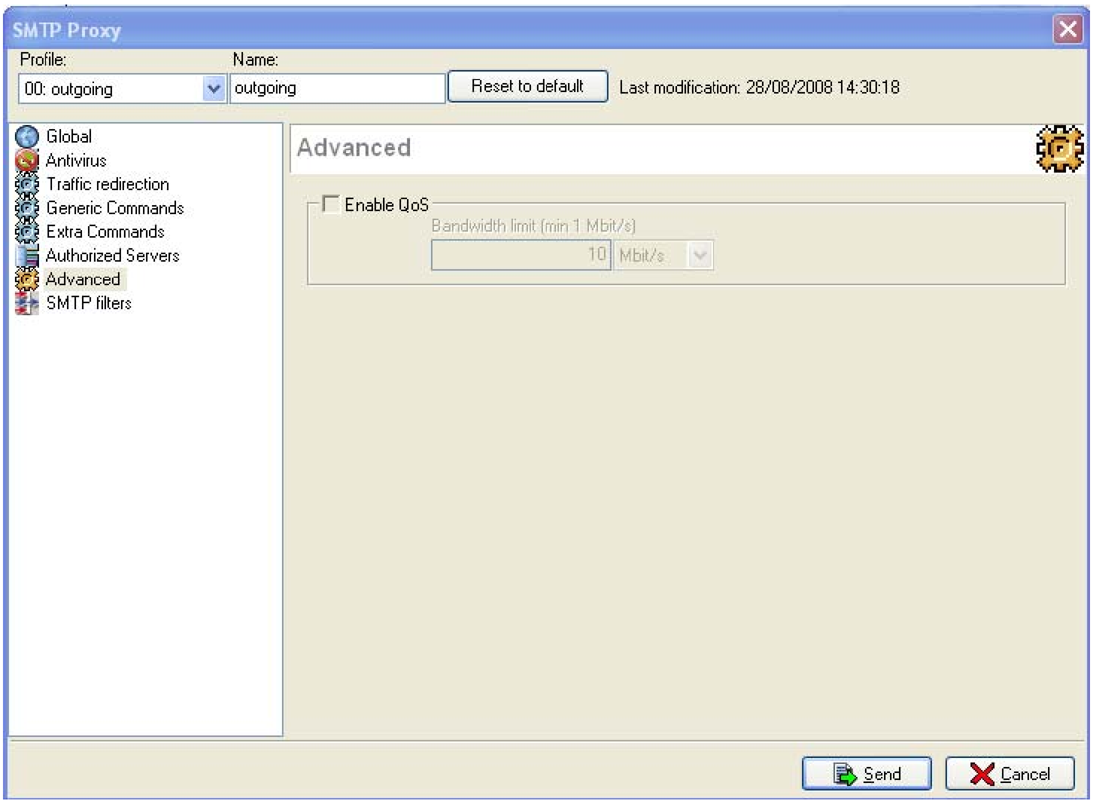


Figure 284: SMTP Proxy – Authorized servers

By selecting the option **Accept only servers on this server list**, you will authorize only SMTP traffic heading for servers specified in this list.

The action buttons in the right side of the window allow you to select authorized servers in the list of objects. Messages headed for a server which is not on the list will be deleted by the Firewall. If this box is not checked, all mail will be authorized.

9.4.4.7. Advanced



Profile: 00: outgoing
Name: outgoing
Last modification: 28/08/2008 14:30:18

Advanced

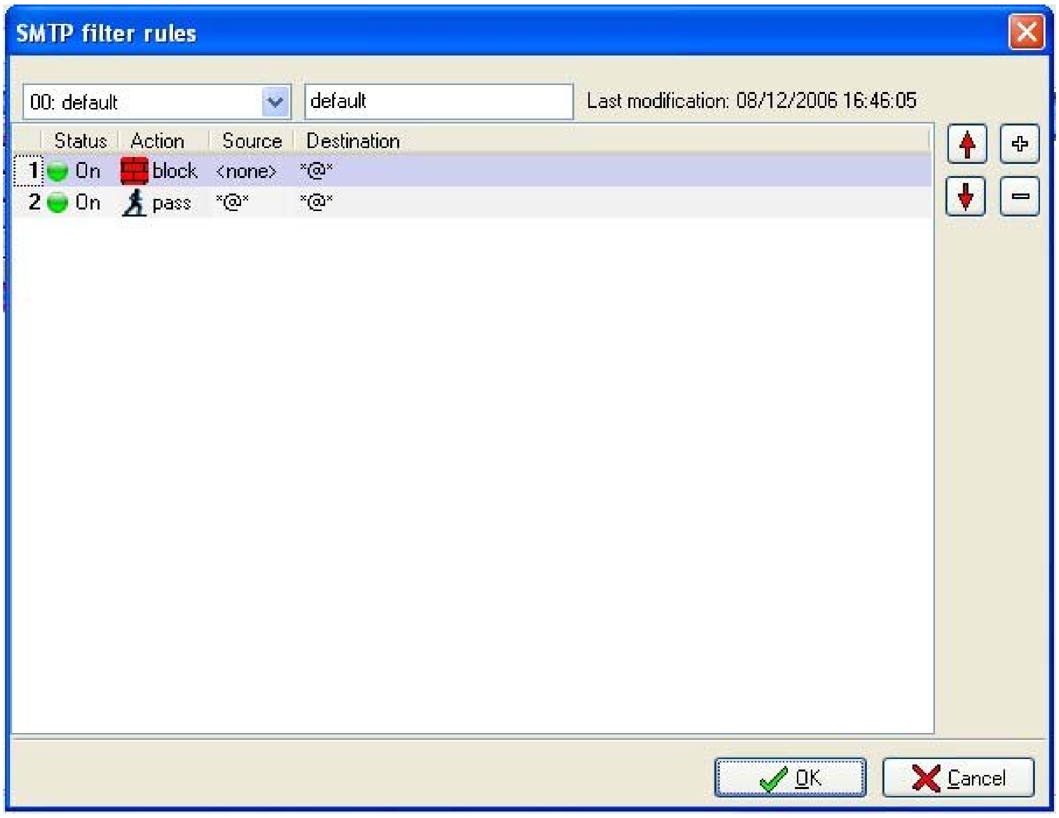
□ Enable QoS
Bandwidth limit (min 1 Mbit/s)
10 Mbit/s

Figure 285: SMTP Proxy - Advanced

The **Advanced** tab enables the configuration of the following parameter:

Enable QoS	Regulation of SMTP traffic. This option allows you to define a maximum throughput for this traffic type. A derivative of the traffic curve allows the determination of whether packets have to be deleted so as not to exceed the limit.

9.4.4.8. SMTP filters



00: default | default | Last modification: 08/12/2006 16:46:05

	Status	Action	Source	Destination
1	On	block	<none>	*@*
2	On	pass	*@*	*@*

Figure 286: Default filter rules

This menu enables filtering e-mails that you send or receive. The configuration menu appears when you click on the **`SMTP filters`** menu. This menu comprises two sections:

- A grid where e-mail filter rules are defined.
- Action buttons.

Actions buttons

The action buttons are explained in the table below:

↑	Places the selected row before the row directly above it..
↓	Places the selected row after the row directly below it.
+	Inserts a new row after the selected row.
−	Deletes the selected row.
✓ OK	Applies the changes made.
✗ Cancel	Cancels changes made.

Creating an e-mail filter rule

The grid enables you to implement an e-mail filter policy. The columns in the grid represent:

Status	🟢 **ON**: The rule is used for filtering. 🔴 **OFF**: The rule is not used for filtering .
Action	Action that the selected e-mail filter rule performs. Select from **Pass** or **Block**.
Source	Mail sender.
Destination	Mail recipient.

E-mail masks can contain the following syntax:

- *: Replaces any character sequence.

> **Example**
> *.netasq.com/* defines the internet domain for NETASQ.

- ?: Replaces a character.

> **Example**
> commerce?@netasq.com is equivalent to commerce1@netasq.com or to commercea@netasq.com but not to commerce12@netasq.com.

- [a-z]: Replaces a character space.

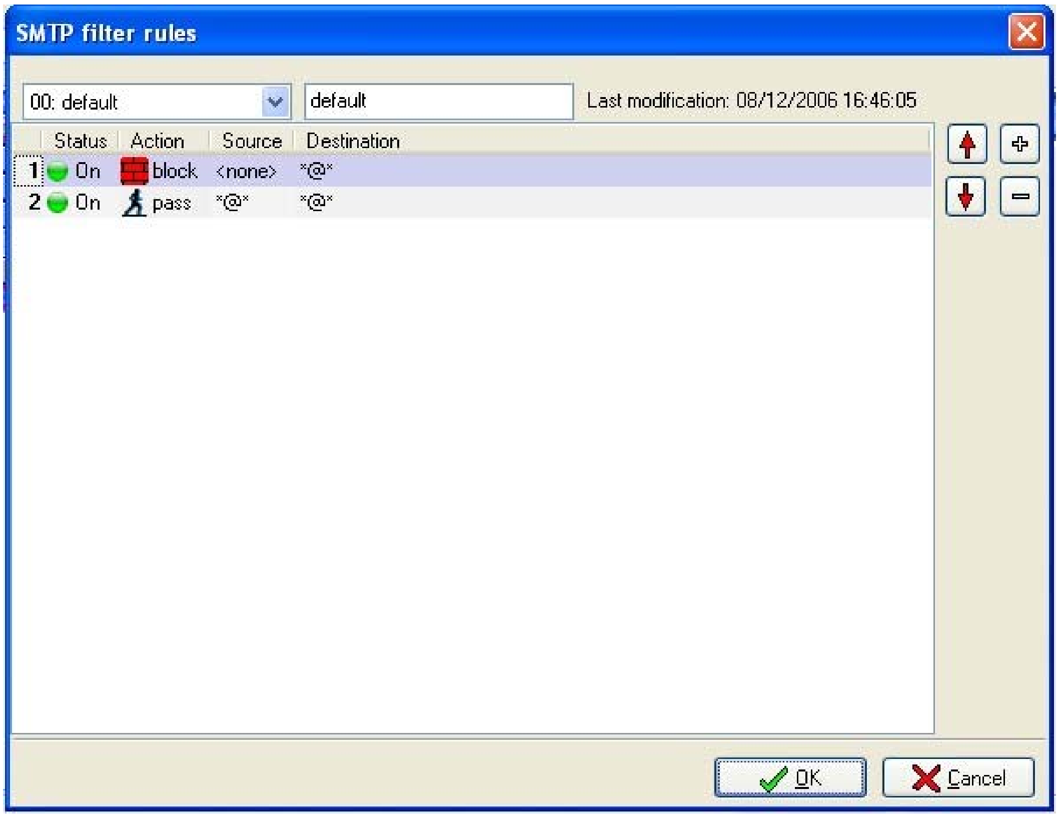
> **Example**
> commerce[1-2]@netasq.com is equivalent to commerce1@netasq.com and to commerce2@netasq.com

- <none>: This value can only be obtained when the **Source** field is empty, and is used only for “Mailer Daemons”.

When an e-mail cannot find its recipient on a remote mail server, the remote mail server will send back an error message, indicating that there is an error regarding the recipient. In this case, the **Source** field in this error message will be empty.

SMTP filters and initial configuration observations

SMTP filters operate in WhiteList (anything that is not explicitly authorized will be prohibited) mode by default. By default, SMTP filters are configured with two SMTP filter rules.


SMTP filter rules

00: default | default | Last modification: 08/12/2006 16:46:05

	Status	Action	Source	Destination
1	● On	block	<none>	*@*
2	● On	pass	*@*	*@*

Figure 287: Operation of the filters

Rule 1 blocks mailer daemon messages by default. When an e-mail cannot find its recipient on a remote mail server, the remote mail server will send back an error message, indicating that there is an error regarding the recipient. In this case, the “Source” field in this error message will be empty. Rule 1 is an explicit adaptation of a rule that previously took on an implicit form.

By default, Rule 2 authorizes the transmission of messages from all possible senders to all possible recipients. When Rule 2 is deleted and the SMTP proxy is activated, messages from unauthorized senders or to unauthorized recipients will be blocked.

CHAPTER 5. POP3 PROXY

9.5.1. Introduction

In the previous section, the operation and advantages of NETASQ’s **SMTP** proxy were covered. As mentioned, this proxy is implemented in an architecture where the Firewall will protect the mail server on the internal network (or in the DMZ) by analyzing **SMTP** traffic and making your network immune to virus threats thanks to the KASPERSKY antivirus integrated into the Firewall.

Mail traffic is based not only on **SMTP** but also on **POP3**. This protocol will enable a user to retrieve mail from distant servers onto his workstation using a mail software. Since this mail server can be located outside the local network or on a separate interface, **POP3** traffic passes through and is analyzed by the Firewall.

9.5.2. To use this feature, you will need to know

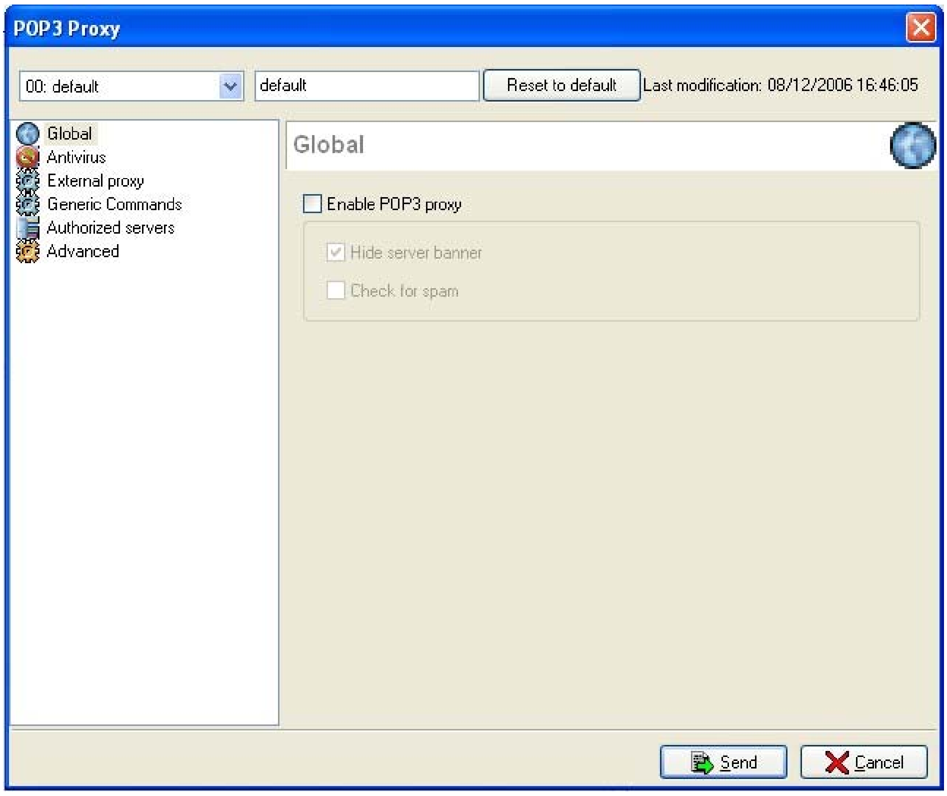
- The domain names allowed for outgoing traffic in SMTP and POP3 on your network.
- The e-mail filter policy that you wish to implement.

9.5.3. Accessing this feature

- POP3 has to be activated in order to be used via the menu **`Proxy\POP3 Proxy`**.

9.5.4. Description of the configuration windows

9.5.4.1. Global



00: default

default

Last modification: 08/12/2006 16:46:05

Global

□ Enable POP3 proxy

☑ Hide server banner

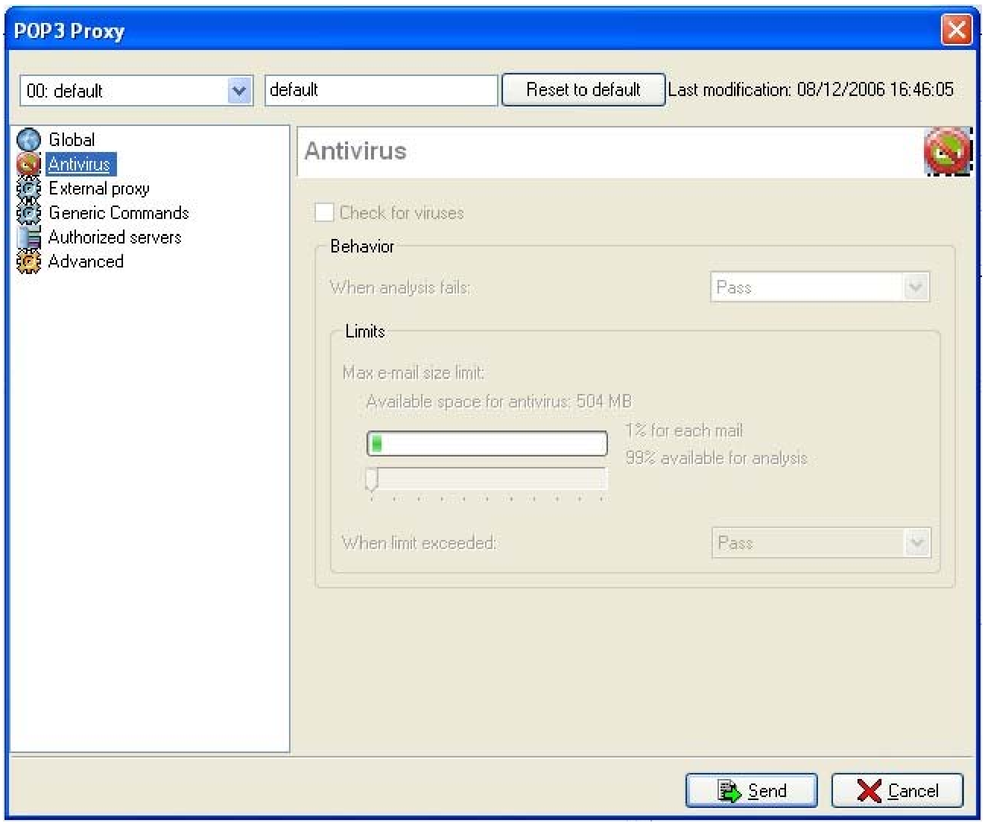
□ Check for spam

Figure 288: POP3 proxy - Global

The **`Global`** menu enables configuring the following parameters:

Enable POP3 proxy	Activates the POP3 proxy and performs the analyses specified in the menus that follow. In particular, activating the POP3 proxy also allows searching for viruses in POP3 traffic.
Hide server banner	When this option is ticked your message server's banner is no longer transmitted in a POP3 connection. In fact this banner contains data which may be exploited by hackers (type of server, software version etc.).
Check for spam	Activates the POP3 proxy features that check for spam

9.5.4.2. Antivirus



00: default

default

Last modification: 08/12/2006 16:46:05

Antivirus

□ Check for viruses

Behavior

When analysis fails: Pass

Limits

Max e-mail size limit:

Available space for antivirus: 504 MB

1% for each mail

99% available for analysis

When limit exceeded: Pass

Figure 289: POP3 Proxy - Antivirus

Activating the POP3 proxy enables the activation of the antivirus module for POP3 traffic. The procedure for activating the antivirus module is as follows:

Check for viruses

Activates the SMTP proxy features that check for viruses when the option **Enable SMTP Proxy** is enabled in the **Global** menu.

Behavior

The “Behavior” section describes the antivirus module’s reaction to certain events.

The option **When analysis fails** defines how the module will behave if the analysis of the file it is scanning, fails.

Example

If the file is locked, the antivirus module will not succeed in analysing it.

If **Block** has been specified, the file being analysed will not be transmitted.
If **Pass** has been specified, the file being analysed will be transmitted.

Limits

The option **Max e-mail size limit** depends on the hardware capacities on each Firewall model but can be adapted to the needs of the enterprise by adjusting the scale.

WARNING

When manually defining a size limit for analyzed data, ensure that all values are coherent. The total memory space, represented by the scale, corresponds to al lthe resources reserved for the Antivirus service. If you define the size limit for analyzed data on POP3 as 100% of the total size, no other files can be analyzed at the same time.

The option **When limit exceeded** defines how the module will behave if the size of the file being analysed exceeds the authorized limit.

If **Block** has been specified, the file being analysed will not be transmitted.
If **Pass** has been specified, the file being analysed will be transmitted.

9.5.4.3. External proxy

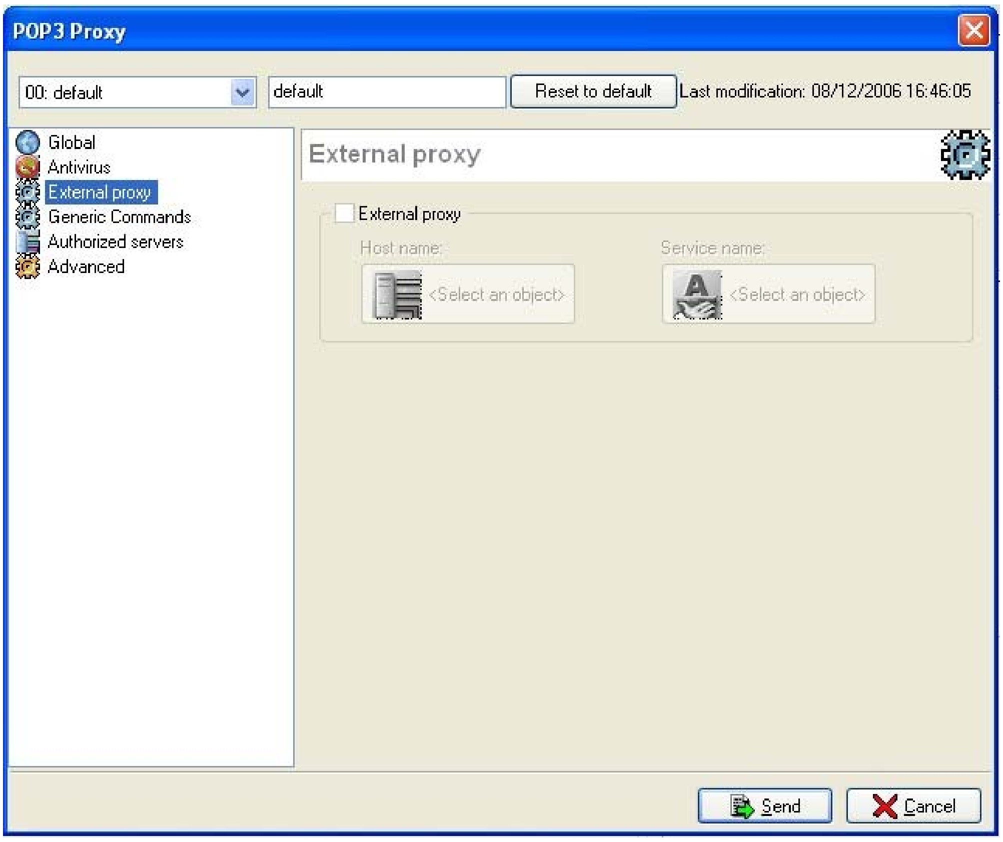
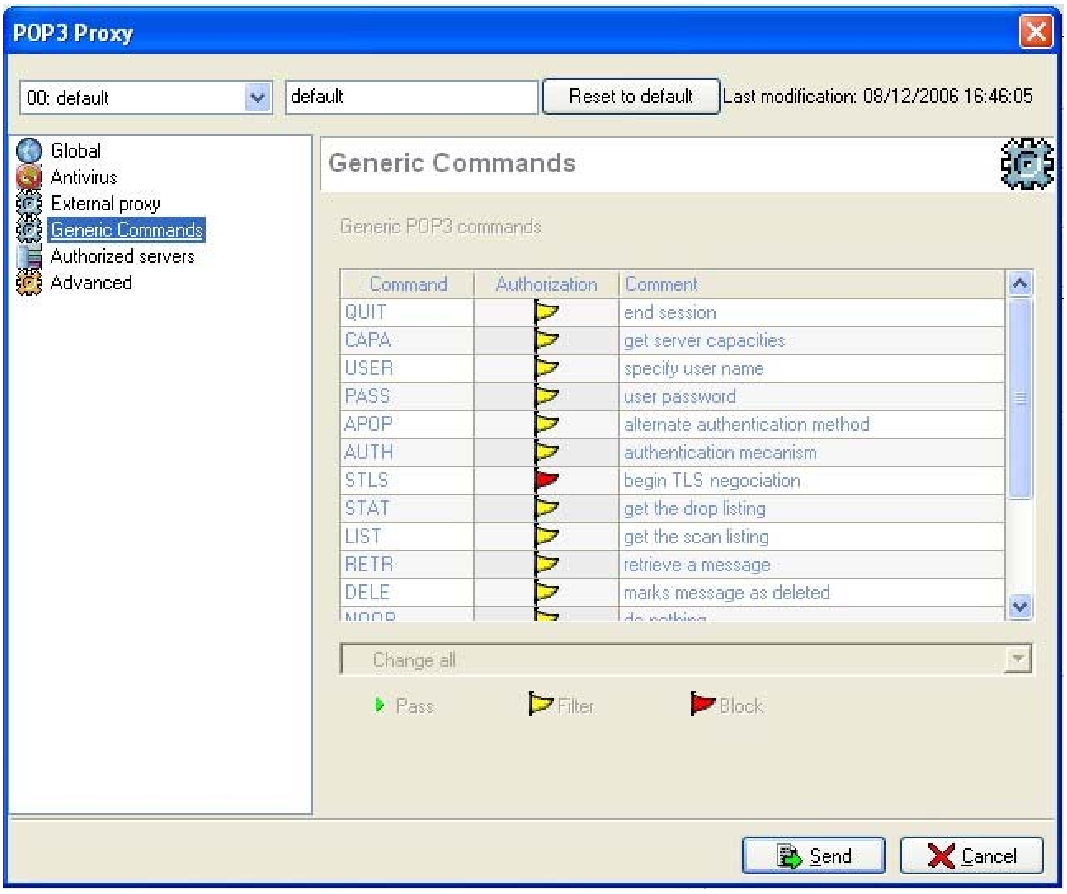


Figure 290: POP3 Proxy – External proxy

The POP3 proxy enables the redirection of POP3 requests from users on the internal network to external proxies.

To activate this redirection, select the corresponding checkbox then enter the IP address of the server as well as of the port on which requests are received.

9.5.4.4. Generic commands



Last modification: 08/12/2006 16:46:05

Generic Commands

Generic POP3 commands

Command	Authorization	Comment
QUIT	⚐	end session
CAPA	⚐	get server capacities
USER	⚐	specify user name
PASS	⚐	user password
APOP	⚐	alternate authentication method
AUTH	⚐	authentication mecanism
STLS	⚑	begin TLS negociation
STAT	⚐	get the drop listing
LIST	⚐	get the scan listing
RETR	⚐	retrieve a message
DELE	⚐	marks message as deleted
NOOP	⚐	do nothing

▶ Pass ⚐ Filter ⚑ Block

Figure 291: POP3 Proxy – Generic commands

This option allows you to authorize or reject POP3 commands defined in the RFCs. You can authorize a command, prohibit it or check that the command syntax complies with the RFC in force.

DEFINITION: RFC
A series of documents that communicate information governing the internet. Anyone can submit comments, but only the Internet Engineering Task Force (IETF) decides whether the standards become RFCs. A number is assigned to each RFC, and once it is published, cannot be modified.

9.5.4.5. Authorized servers

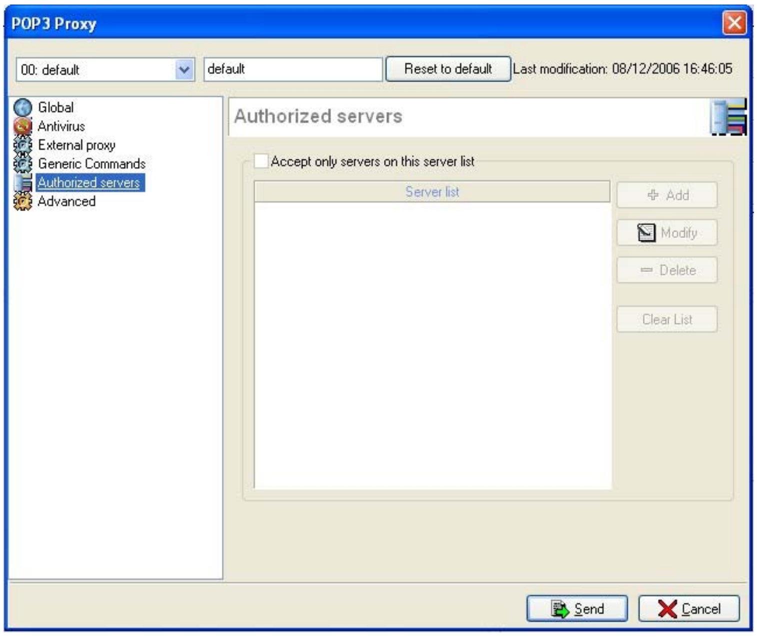


Figure 292: POP3 Proxy – Authorized servers

By selecting the option **Accept only servers on this server list**, you will authorize only POP3 traffic heading for servers specified in this list.

The action buttons in the right side of the window allow you to select authorized servers in the list of objects. Messages headed for a server which is not on the list will be deleted by the Firewall. If this box is not checked, all mail will be authorized.

9.5.4.6. Advanced

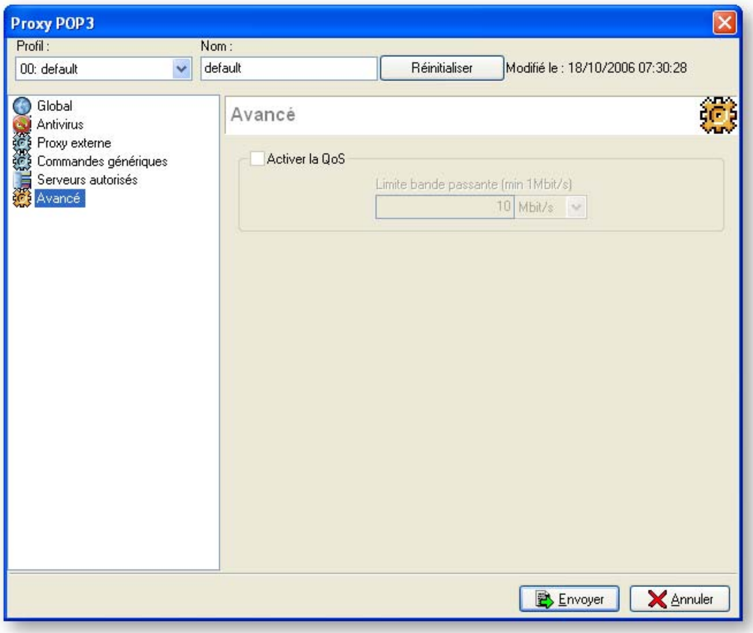


Figure 293: POP3 Proxy – Advanced

The **Advanced** tab enables the configuration of the following parameter:

Enable QoS	Regulates POP3 traffic. A calculation derived from the traffic curve determines whether to delete packets in order to avoid exceeding the maximum throughput.

CHAPTER 6. FTP PROXY

9.6.1. Description

FTP (*File transfer Protocol*)
This protocol enables the exchange of files over a TCP/IP network. It allows files to be copied from one computer to another on the network.

In FTP, the client sends requests to which the server responds.

FTP enables the download of files from a server to the client, and also allows uploading files from the client to the server, for example, for the update of personal web pages.

The proxy is used for checking FTP commands and for performing antivirus scans on transferred files (uploads and downloads). Only file transfers undergo the antivirus scan. Since the protocol has been analyzed by the ASQ engine, the FTP proxy analyzes in particular the number and nature of command arguments by offering 3 levels of checks:

- Unconditional blocking of the command.
- Verfication of the command's validity.
- Unconditional acceptance of the command.

The protocol can be used in two different ways when the NETASQ firewall is used for packet filtering.

- In active mode: the FTP client determines the connection port to use for authorizing the data transfer.
- In passive mode: the FTP server itself determines the connection port to use for authorizing the data transfer and communicates it to the client.

The implementation of the FTP proxy feature serves most of all to allow scanning data passing through FTP.

NOTE
The FTP proxy complies with the RFC and various extensions.

9.6.2. Steps before the configuration of FTP proxy

- Part 5: Network configuration.

9.6.3. Steps after the configuration of FTP proxy

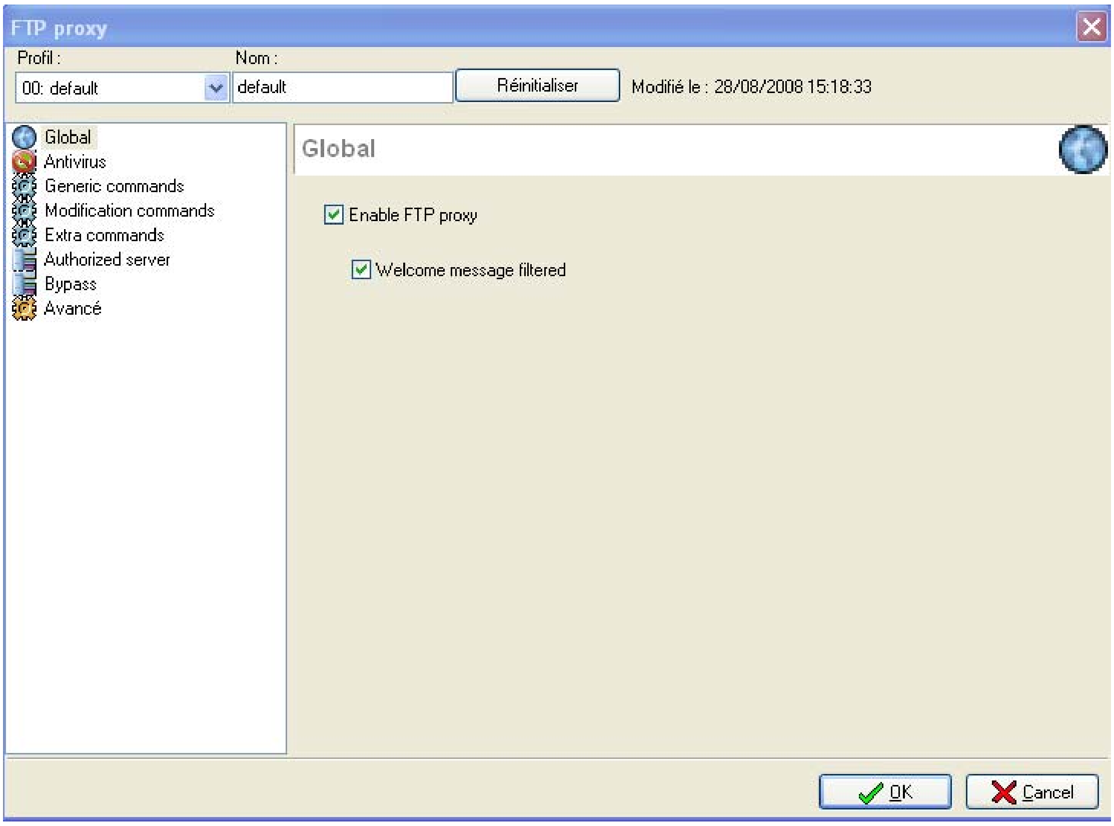
- Part 10/Chapter 3: Antivirus

9.6.4. Accessing this feature

➲ The FTP proxy has to be enabled before it can be used. You can enable it in the menu **`Proxy\FTP Proxy`**.

9.6.5. Description of the configuration windows

9.6.5.1. Global



☑ Enable FTP proxy

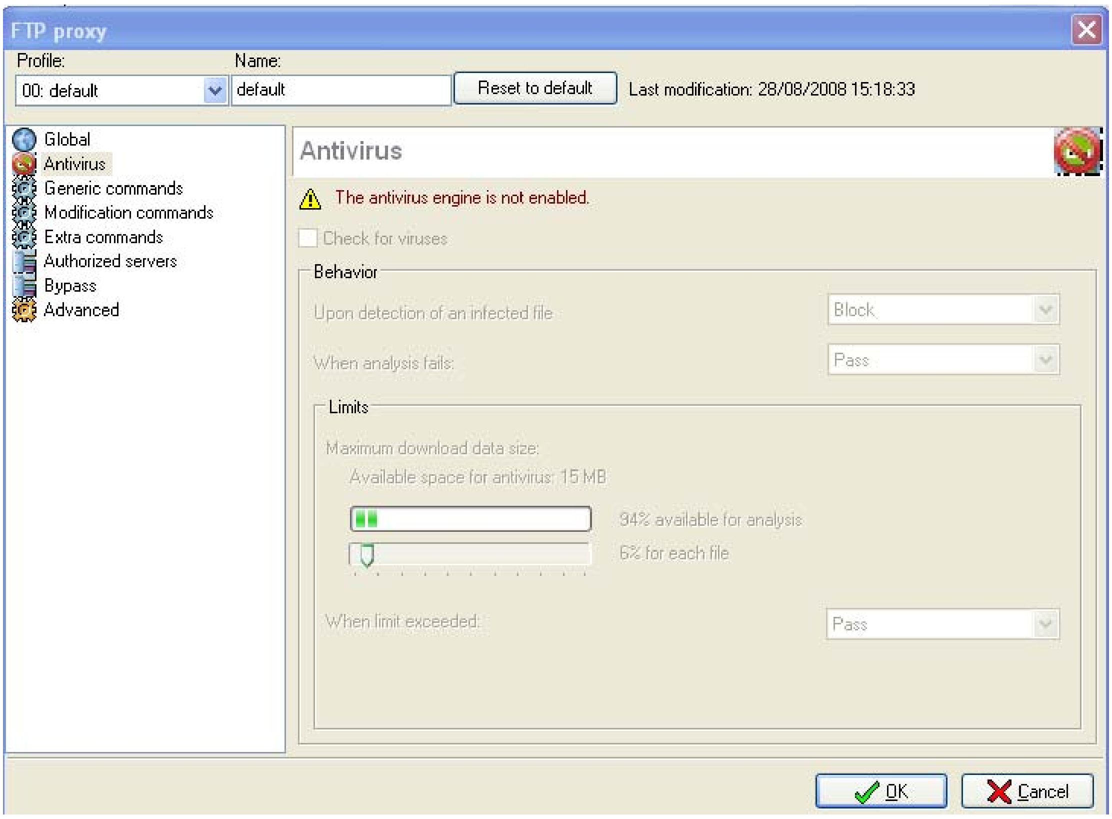
☑ Welcome message filtered

Figure 294: FTP Proxy - Global

The **`Global`** menu allows configuring the following parameters:

Enable FTP proxy	Enables the **FTP** proxy and performs the analyses specified in the following menu.
Welcome message filtered	Allows filtering the welcome message.

9.6.5.2. Antivirus



FTP proxy

Profile: 00: default

Name: default

Reset to default

Last modification: 28/08/2008 15:18:33

Antivirus

⚠ The antivirus engine is not enabled.

□ Check for viruses

Behavior

Upon detection of an infected file: Block

When analysis fails: Pass

Limits

Maximum download data size:

Available space for antivirus: 15 MB

94% available for analysis

6% for each file

When limit exceeded: Pass

Figure 295: FTP Proxy - Antivirus

Enabling the FTP proxy allows the antivirus to be configured.

The message "The antivirus engine is not enabled" indicates that you need to enable it. However, the configuration of the antivirus within the proxy is not totally necessary.

Check for viruses

Activates the antivirus module by selecting the option **Enable FTP proxy** in the **Global** menu.

Behavior

The **Behavior** section describes the antivirus module's reaction to certain events.

The option **Upon detection of an infected file** contains two options – "Pass" and "Block". If "Block" is selected, the analyzed file will not be transmitted. If "Pass" is selected, the antivirus module will transmit the file being analyzed.

The option **When analysis fails** defines how the module will behave if the analysis of the file it is scanning, fails.

> **Example**
> If the file is locked, the antivirus module will not succeed in analysing it.

If **Block** has been specified, the file being analysed will not be transmitted.
If **Pass** has been specified, the file being analysed will be transmitted.

Limits

The maximum size used for scanning files can be determined here. For this, move the scale. You can also configure the action to take if the file size is higher than the size allowed.

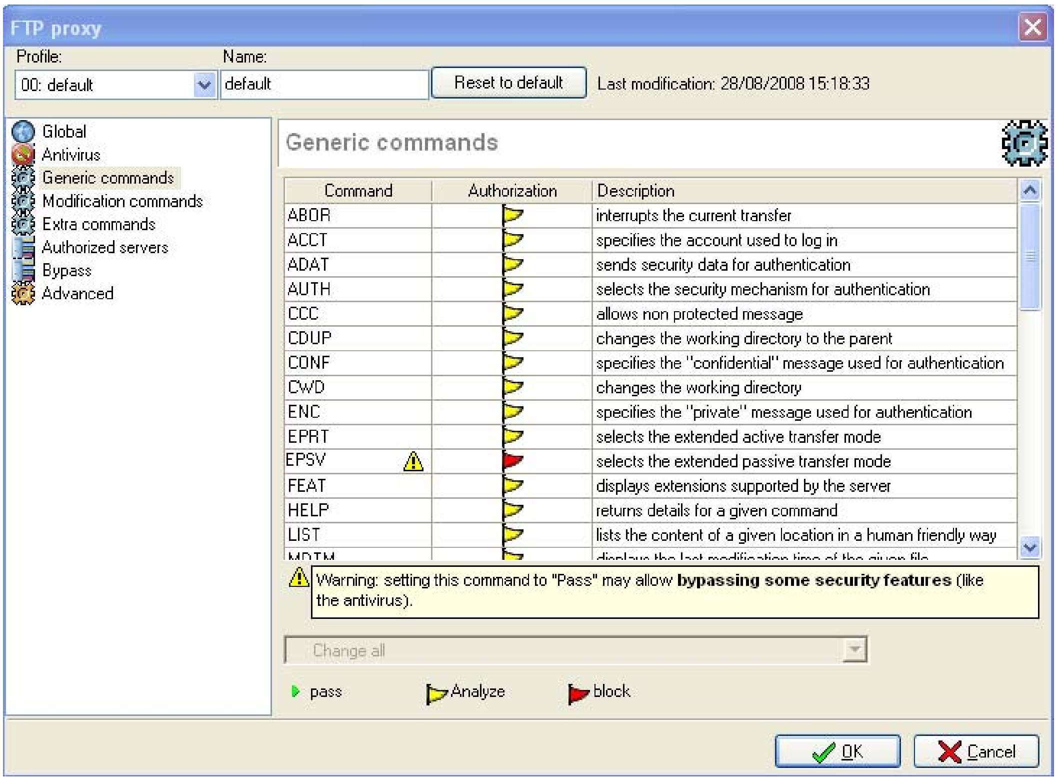
WARNING

When manually defining a size limit for analyzed data, ensure that all values are coherent. The total memory space, represented by the scale, corresponds to a common space for all the resources reserved for the Antivirus service. If you define the size limit for analyzed data on SMTP as 100% of the total size, no other files can be analyzed at the same time.

The option **When limit exceeded** defines how the module will behave if the size of the file being analysed exceeds the authorized limit.

If **Block** has been specified, the file being analysed will not be transmitted.
If **Pass** has been specified, the file being analysed will be transmitted.

9.6.5.3. Generic commands



Profile: 00: default

Name: default

Last modification: 28/08/2008 15:18:33

Command		Authorization	Description
ABOR		⚐	interrupts the current transfer
ACCT		⚐	specifies the account used to log in
ADAT		⚐	sends security data for authentication
AUTH		⚐	selects the security mechanism for authentication
CCC		⚐	allows non protected message
CDUP		⚐	changes the working directory to the parent
CONF		⚐	specifies the "confidential" message used for authentication
CWD		⚐	changes the working directory
ENC		⚐	specifies the "private" message used for authentication
EPRT		⚐	selects the extended active transfer mode
EPSV	⚠	⚑	selects the extended passive transfer mode
FEAT		⚐	displays extensions supported by the server
HELP		⚐	returns details for a given command
LIST		⚐	lists the content of a given location in a human friendly way
MDTM		⚐	displays the last modification time of the given file

⚠ Warning: setting this command to "Pass" may allow **bypassing some security features** (like the antivirus).

▶ pass ⚐ Analyze ⚑ block

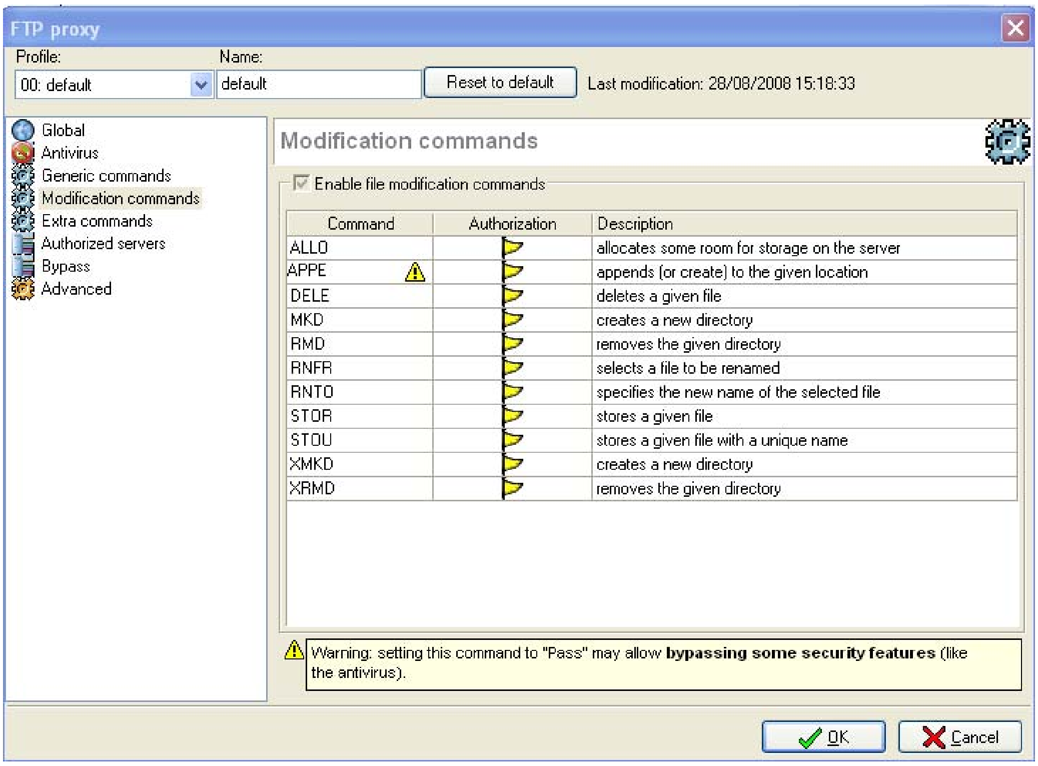
Figure 296: FTP Proxy – Generic commands

This menu allows you to authorize or reject "generic" FTP commands defined in the RFCs. You can authorize or prohibit a command or check that the command syntax complies with the RFC in force.

Cf. *Appendix Q: List of generic FTP commands and details of filtering*.

Command	Name of the command. The WARNING icon (which appears for certain commands) indicates that you can modify the status of the said command without any risk. These commands will be blocked by default.
Authorization	3 authorizations are possible – "Pass", "Analyze" and "Block".
Description	Description of the command.

9.6.5.4. Modification commands



Profile: 00: default
Name: default
Last modification: 28/08/2008 15:18:33

Modification commands

☑ Enable file modification commands

Command	Authorization	Description
ALLO	⚑	allocates some room for storage on the server
APPE ⚠	⚑	appends (or create) to the given location
DELE	⚑	deletes a given file
MKD	⚑	creates a new directory
RMD	⚑	removes the given directory
RNFR	⚑	selects a file to be renamed
RNTO	⚑	specifies the new name of the selected file
STOR	⚑	stores a given file
STOU	⚑	stores a given file with a unique name
XMKD	⚑	creates a new directory
XRMD	⚑	removes the given directory

⚠ Warning: setting this command to "Pass" may allow **bypassing some security features** (like the antivirus).

Figure 297: FTP Proxy – Modification commands

This menu allows you to accept or reject “modification” FTP commands defined in the RFCs. These are commands that can lead to changes in the server, such as the deletion of data or even the creation of folders. These commands operate in the same way as for “generic” commands – you can authorize or prohibit a command or check that the command syntax complies with the RFC in force.

Enable file modification commands	This option allows switching the server to “read only”. 1) If this option is selected, you can define an action for each command – “Block”, “Analyze” or “Pass”. By default, all commands are set to “Analyze”. 2) If this option is not selected, the modification commands will be set to “Block”. In this case, the status of a command cannot be modified.
Command	Name of the command. The WARNING icon (which appears for certain commands) indicates that you can modify the status of the said command without any risk. These commands will be blocked by default.
Authorization	3 authorizations are possible – “Pass”, “Analyze” and “Block”.
Description	Description of the command.

Cf. Appendix R: List of FTP modification commands and details of filtering.

9.6.5.5. Extra commands

This menu allows you to specify a list of commands that will be allowed to pass through the FTP proxy. If non-standard commands that do not appear on this list pass through, the firewall will block them.

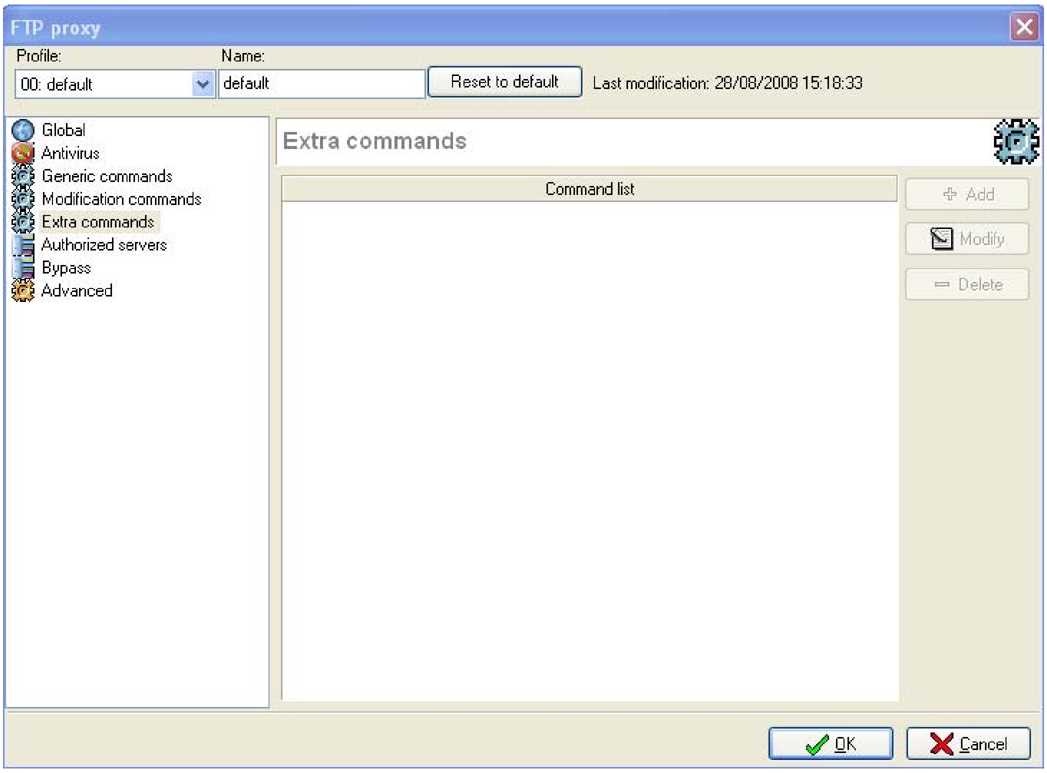
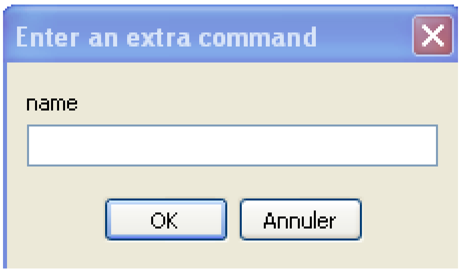
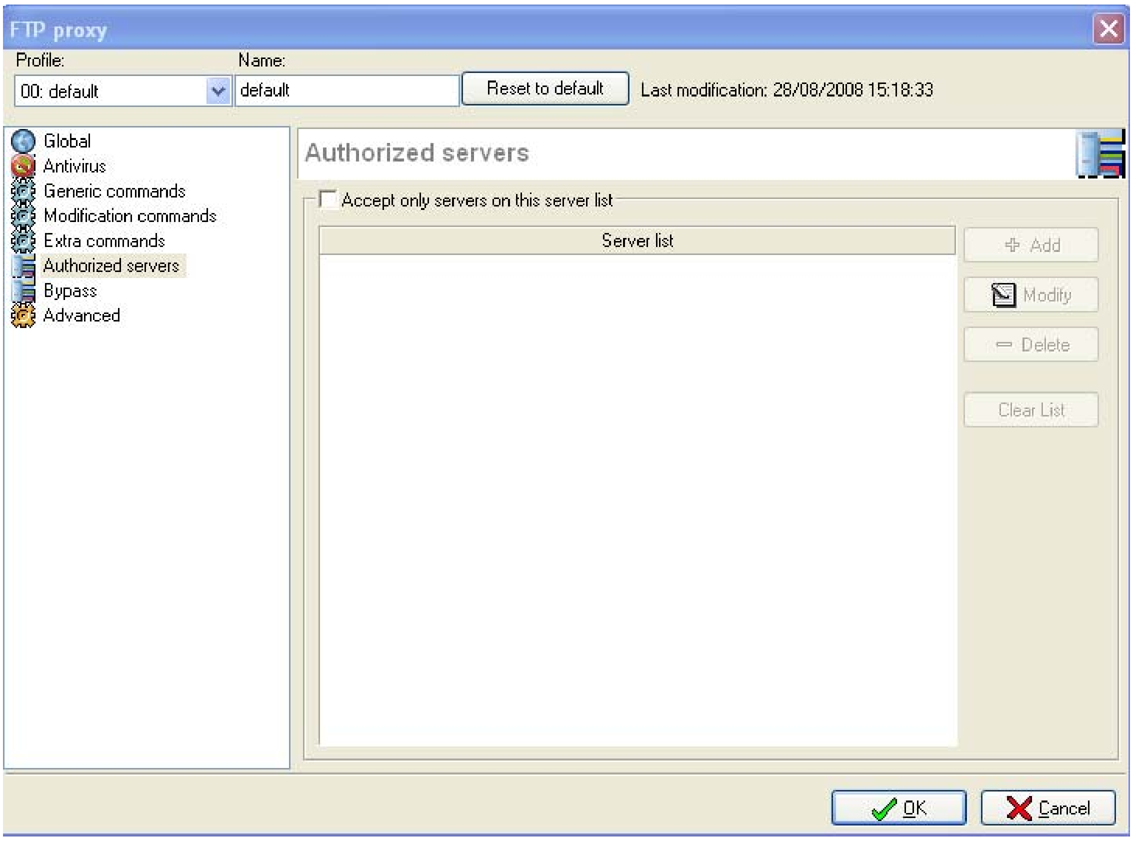


Figure 298: FTP Proxy – Extra commands

Add	When you click on **Add**, the following window will appear, allowing you to enter the name of a new command.  *Figure 299: Entering a command*
Modify	Clicking on this button allows you to modify the name of the command.
Delete	Once the command has been selected, when you click on this button, the message "Delete command X?" will appear. Confirm or cancel the deletion.

9.6.5.6. Authorized Servers

This menu allows defining a list of servers that are allowed to pass. In other words, only FTP servers from this list will be allowed.



FTP proxy

Profile: 00: default

Name: default

Reset to default

Last modification: 28/08/2008 15:18:33

Authorized servers

☐ Accept only servers on this server list

Server list

Figure 300: FTP Proxy - Authorized servers

Accept only servers on this server list	This option lets users define a list of servers (in the form of HOST objects) that are allowed to pass. Once activated, all FTP traffic that is not going to these hosts will be blocked. This option is not enabled by default in order to avoid blocking FTP traffic.
Add	By clicking on the **Add** button, the “Hosts” object database will appear so that servers can be selected.
Modify	By clicking on this button, you can replace the server that was previously selected with another from the “Hosts” object database.
Delete	Once the server has been selected, when you click on this button, the message “Delete host X?” will appear. Confirm or cancel the deletion.
Clear list	This option deletes all the servers indicated in the list.

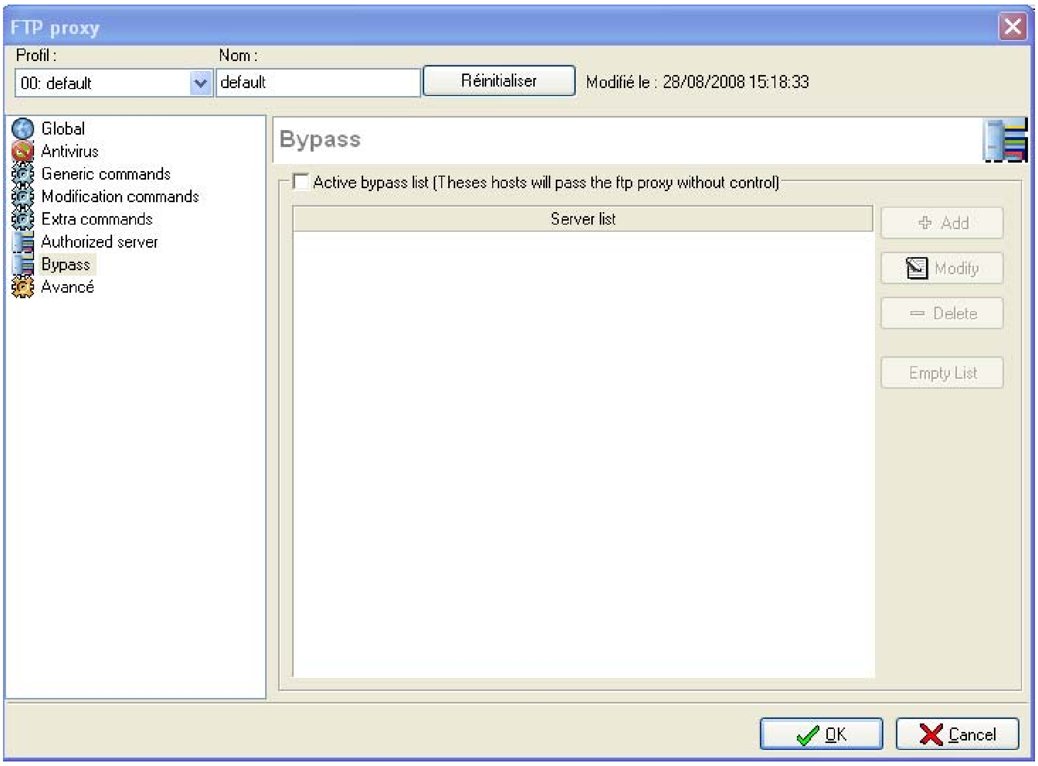
9.6.5.7. Bypass

This menu allows listing the servers that will not be scanned.

The treatments include:

- Verification of commands.
- Antivirus scans.

This list may contain up to 128 servers.


FTP proxy

Profil : 00: default

Nom : default

Réinitialiser

Modifié le : 28/08/2008 15:18:33

☐ Active bypass list (Theses hosts will pass the ftp proxy without control)

Server list

Figure 301: FTP Proxy - Bypass

The **Bypass** menu allows the configuration of the following parameters:

Enable Bypass list (No security checks will be performed for these hosts)	This command allows authorizing a list of servers to pass through the FTP proxy without having the commands analyzed and without any antivirus scan.
Add	By clicking on the **Add** button, the "Hosts" object database will appear so that servers can be selected.
Modify	By clicking on this button, you can replace the server that was previously selected with another from the "Hosts" object database.
Delete	Once the server has been selected, when you click on this button, the message "Delete host X?" will appear. Confirm or cancel the deletion.
Clear list	This option deletes all the servers indicated in the list.

9.6.5.8. Advanced

The Advanced menu allows setting the transfer modes between the client and the proxy as well as between the proxy and the server. The transfer mode shows the entities that initiate connections:

The FTP proxy also allows finely setting the transfer modes (any/active/passive). By default, the transfer mode used for client-proxy and proxy-server connections is the mode specified by the client.

By defining a particular mode for server connections, this transfer mode will be used regardless of the mode chosen by the client. However, defining a particular mode for client connections means that FTP errors may be sent indicating to the client that the selected transfer mode is not authorized.

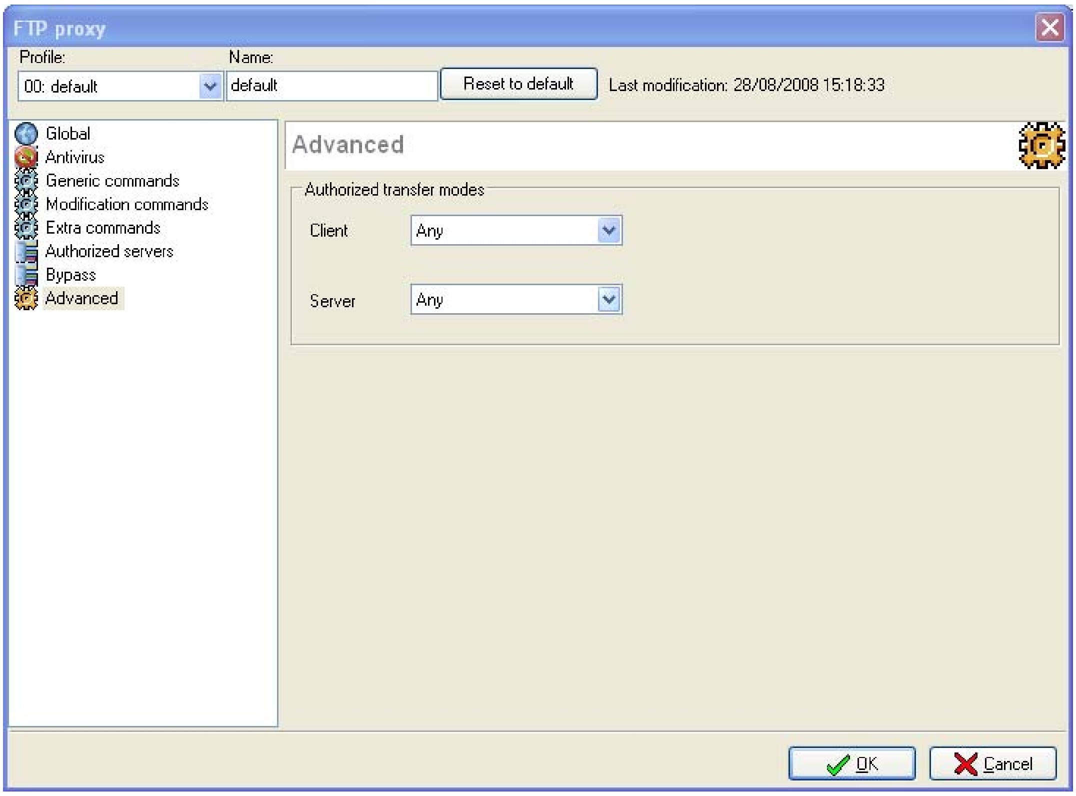
- In passive mode: the client indicates its wish to use the passive mode. The server then indicates the connection parameters de connexions (IP, port). The client then connects to the address and port indicated.

- In active mode, the client indicates its wish to use the active mode by sending connection parameters de connexion (IP, port). The FTP server then connects to the address and ports indicated.

When the transfer mode has been established, data can then be transferred (uploads or downloads).

Data transfer takes place in two stages when an antivirus scan is performed with the FTP Proxy:

- During a download, the proxy will start the file transfer as soon as the connection begins, in order to prevent the client (or the server) from disconnecting when no data are seen arriving.
- During an upload, the proxy will retrieve data from the FTP client and will perform the scan before sending the data to the server.



Profile: 00: default

Name: default

Last modification: 28/08/2008 15:18:33

Advanced

Authorized transfer modes

Client: Any

Server: Any

Figure 302: FTP Proxy – Advanced

- By default, both parameters are set to “Any”:

In this case, the mode used between the proxy and the FTP server will be the same as the one used by the client. For example, if the client requests a transfer in passive mode, the proxy will use the passive mode with the FTP server.

- The client is in any mode/The server is in active or passive mode:

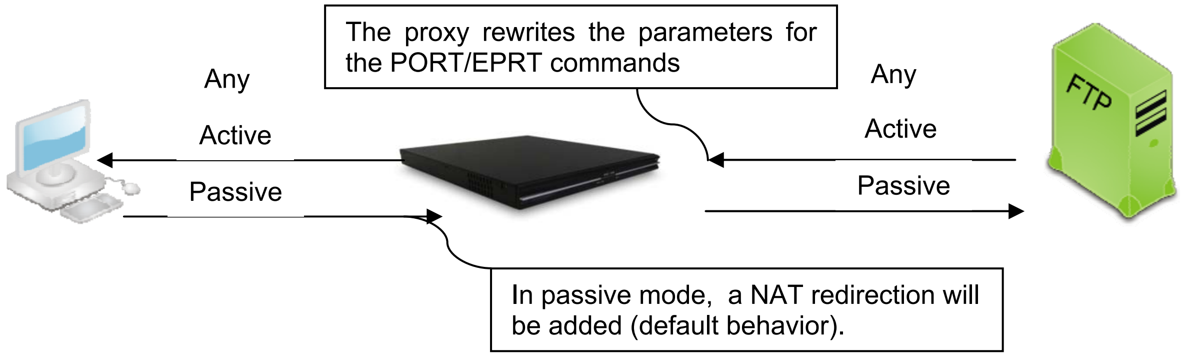
Management of connections to the server.

- The client is in active or passive mode / The server is in any mode:

In this case, the authorized mode is managed by the client.

If the modes specified are different, the proxy will automatically convert the command that specifies the mode used. If the FTP client requests to use the passive mode and the configuration forces the use of the passive mode between the proxy and the server, the proxy will not initiate any connection (the client and the server will both connect to the proxy).

Traffic is intercepted as follows:


The proxy rewrites the parameters for the PORT/EPRT commands
Any
Active
Passive
Any
Active
Passive
FTP
In passive mode, a NAT redirection will be added (default behavior).

9.6.5.9. FTP postprocessing

Data flow subject to antivirus scans

Only transfers regarding the sending or receiving of files will be xsubject to antivirus scans.

Post-processing

The FTP proxy's post-processing is able to handle a large number of transfer types. Indeed, it manages the active and passive mode both for receiving and sending files.

The FTP Proxy sends only the strict minimum for keeping the connection open. FTP clients download the file directly from the permanent location. To avoid partially downloading a file that contains a virus, the proxy will send as few as possible. As a result, the real-time throughput at the beginning of the transfer will be practically nonexistent whereas it will be at its highest at the end of the transfer.

9.6.5.10. Command grouping

The list of FTP commands is significant. There is a group of FTP commands that operate in writing mode, thus allowing the protection of a server by only allowing clients access in read-only mode.

The commands grouped in MODIFY mode are:

- STOR
- STOU
- APPE
- ALLO
- RNFR
- DELE
- RMD
- MKD
- XRMD
- XMKD

PART 10: CONTENT ANALYSIS

CHAPTER 1. INTRODUCTION

10.1.1 For this chapter, you will need to have completed these steps:

- Part 2: Installation, pre-configuration, integration.
- Definiting interfaces, Objects and kernel configuration.
- HTTP, SMTP and POP3 proxies

10.1.2. For this chapter, you will need to know:

- The company's URL filter policy.
- The addresses of the different proxies.

10.1.3. Purpose of this section

This part explains the definition of the URL-filter rules to apply to the hosts of your internal network.

10.1.4. Accessing this section

➲ Access this section by clicking on **Content Analysis** in the NETASQ UNIFIED MANAGER menu directory.

You have to be connected with modification privileges to make these modifications. Before making any significant modification to your NETASQ Firewall, we recommend that you perform a backup. As such, in case of a wrong move, you will be able to return to your previous configuration. For more information on backups, please refer to the relevant chapter. (See *Part 18: Maintenance*).

10.1.5. Introduction to this section

You can impose authentication for URL filtering. If a user wants to access the web, he will have to authenticate. If URL filtering is active and a user has to authenticate, a specific authentication page will appear in the web browser.

URL filtering tables are stored on the NETASQ Firewall in slots (configuration files numbered from 01 to 10). Each slot can be scheduled to run at a precise hour of the day or week, replacing the previously active configuration slot parameters. (See *Part 7/Chapter 3: Slot Scheduler).*

CHAPTER 2. ANTISPAM

10.2.1. Introduction

The exceptional development of the internet and the now common use of e-mail have been particularly conducive to the growth of what we call “spam”. Those annoying e-mails that boast of incredible products or services pollute the mailboxes of webmail users as much as ever and show no sign of slowing down.

Furthermore, spammers, in their constant quest for new spamming techniques, succeed in beating one by one the countermeasures that network administrators set up to protect their users’ mailboxes. To remain relevant, new countermeasures therefore have to multiply their methods of analysis in order to handle spam that is as varied and variable as possible.

NETASQ’s built-in antispam module on its UTM appliances is based on 4 complementary methods of analysis – DNS blacklist analysis, heuristic analysis, domain blacklist filtering and domain whitelist filtering.

10.2.1.1. DNS blacklist analysis or RBL DNS

The DNS blacklist analysis or **RBL** (*Realtime Blackhole List*) enables identifying the message as spam through RBL servers, which contain lists of IP addresses that identifiy spammers and all servers that relay spam messages without blocking them.

For each message to be analyzed, the UTM appliance will query the **RBL** servers on whether the sender of the message or any of the mail relays through which the message passed is considered a spammer. The UTM appliance will then rely on their response to decide whether to label a message as spam.

REMARK
The license for the "NETASQ Antispam module" is necessary for the analysis to run.

10.2.1.2. Heuristic or Bayesian analysis

The heuristic analysis is based on GOTO Software’s VadeRetro, which uses 7 methods of analysis to assess the legitimacy of an analysed e-mail.

REMARK
The “OEM Antispam module” license is necessary for heuristic analyses.

Empirical rule analysis

The analysis by empirical rules is based on the use of unpredictable rules, deduced from the in-depth analysis of all the message’s components (header fields, subject text, body text, html, attachments, etc). These rules, which have been defined by the specialists at VadeRetro, define a set of characteristics that are common to certain types of messages (such as messages sent by robots), and therefore allow identifying future messages with the same characteristics.

Semantic analysis

In a semantic analysis, the text contents of the message are compared against a predefined dictionary of typical words and phrases used in spam or legitimate messages. VadeRetro's phrase lookup technology has a novel approach, as it allows not only searching for logical word combinations, but also for words with an approximative spelling.

Counter-reaction

Filters like these are no doubt the most original and efficient aspect of the VadeRetro filter engine. Their main function consists of detecting in messages, the techniques that spammers use to get around anti-spam solutions that use "classic" filter methods.

Analysis of embedded HTML code

When part of the message contains HTML, the antispam will compute an exclusive HTML code footprint (HTML pattern), which is then compared to a list of known patterns typical of generated spam. This technique, combined with statistics on the image sizes within, provide for a particularly effective filtering of spam mainly or exclusively made of online images.

Non-latin character set languages

For IT environments restricted to Western languages, Vade Retro can consistently detect usage of non-Latin character sets, either through declaration or effective use, which provides for quick identification of the ever growing spam of Asian or Slavonic origin.

Anti-Scams

Cyber-scams are often financial propositions that dangle get-rich-quick offers with the aim of luring victims to purportedly lucrative overseas investments. Originally carried out by ordinary mail or by fax, these days these scams take the form of spam e-mails that do not exactly resemble other advertising messages that are usually filtered. VadeRetro's technology include a specific scam detection module to combat such messages.

Anti-virus and SMTP delivery failure notifications

Nowadays, mail servers are saturated with notifications caused by the spread of e-mail viruses. Such viruses exploit the address books of infected machines and send messages from fraudulent addresses. VadeRetro features a special module identifying notifications sent by SMTP servers during the detection of viruses or during the delivery failure of a message to a non-existent e-mail address.

10.2.1.3. Domain blacklist filtering

The first two very sophisticated analyses in NETASQ's Antispam module are complemented by basic domain filters. The domain blacklist filter contains a list of the domains that have to be systematically considered as spammers.

10.2.1.4. Domain whitelist filtering

The domain whitelist filter defines what goes on the list of domains that must be systematically considered legitimate.

10.2.2. Using antispam on NETASQ UTM Firewalls

The antispam feature enables marking e-mails which correspond to its definition of spam, making it possible to automatically classify these e-mails with your mail client's "filter" functions. NETASQ recommends creating mail filters and placing a special spam filter right at the end of all your filters so that in the event legitimate e-mails happen to be marked as spam, your personal filters will first file them before the spam filter treats them.

> NOTE
> The **Antispam** module determines a level of confidence (from 1 to 3) that defines a level of certainty of the Antispam module detecting a spam message (1 for "unsure", 3 for "very sure"). This level of confidence is found in the configuration of RBL servers.

10.2.3. Operation

The SMTP and POP3 proxies have to be activated in order for the Antispam module to run. In fact, the Antispam analyses only operate via proxies.

Once these analyses become available, they can be enabled or disabled. Furthermore, for the antispam to work, it depends on the license, SMTP/POP3 proxies and the appliance's DNS configuration.

Antispam must first be activated before it can be used on the Firewall. This service is activated using the menu **`Content analysis\Antispam`** in the menu directory.

> WARNING
> The DNS proxy must be activated for antispam to operate.

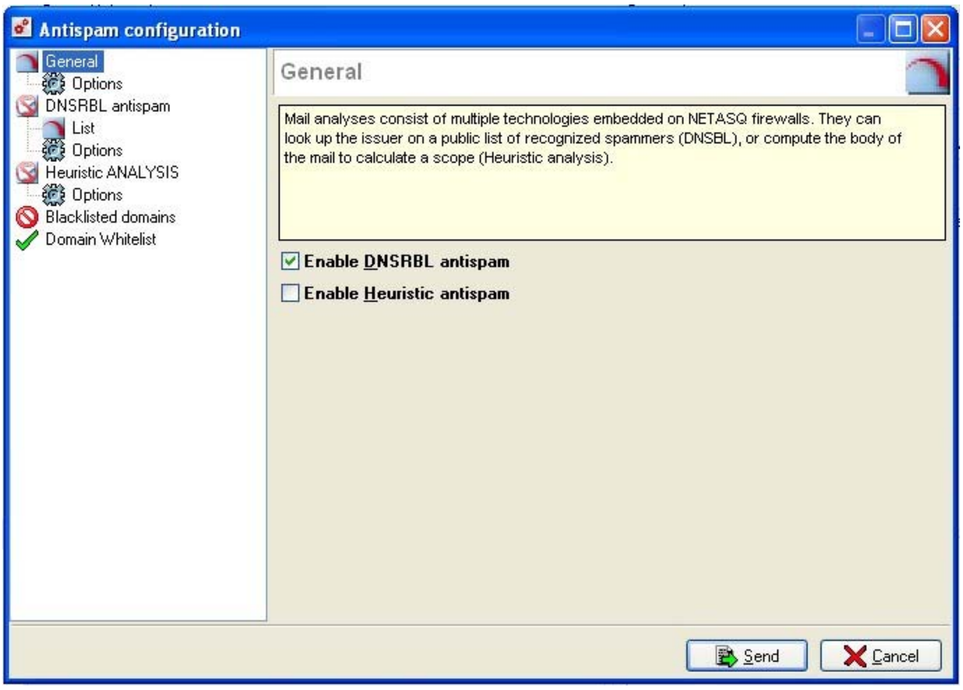
The Antispam configuration screen comprises two sections:

- On the left, a menu setting out the various features in the **`Antispam`** service**.**
- On the right, the options that can be configured.

The configuration of this module does not affect other modules.

The buttons **Send** and **Cancel** in the lower corner of the window respectively enable the application or cancellation of changes.

10.2.3.1. General



Mail analyses consist of multiple technologies embedded on NETASQ firewalls. They can look up the issuer on a public list of recognized spammers (DNSBL), or compute the body of the mail to calculate a scope (Heuristic analysis).

☑ Enable DNSRBL antispam

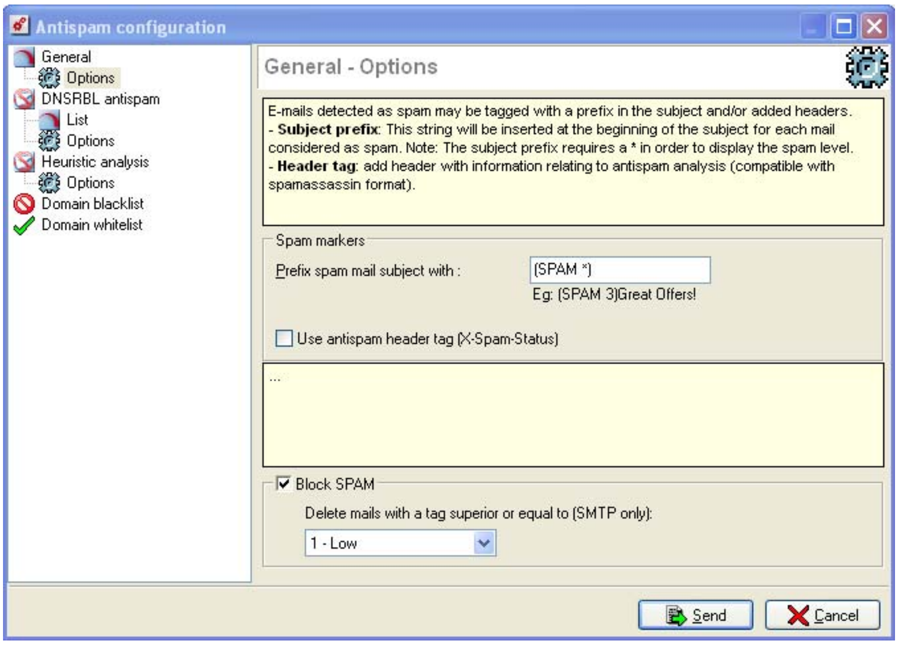
□ Enable Heuristic antispam

Figure 303: Antispam general window

Antispam is activated when you determine the analyses to be activated. Two choices are available on the firewall: The first allows validating the issuer from a public list of known spammers (DNSRBL). The second allows studying the contents of the e-mail to determine a scope.

Enable DNS RBL analysis	Activates the DNS blacklist analysis.
Enable heuristic antispam	Activates the VadeRetro Antispam module.

Options



E-mails detected as spam may be tagged with a prefix in the subject and/or added headers.
- **Subject prefix**: This string will be inserted at the beginning of the subject for each mail considered as spam. Note: The subject prefix requires a * in order to display the spam level.
- **Header tag**: add header with information relating to antispam analysis (compatible with spamassassin format).

Spam markers

Prefix spam mail subject with : [SPAM *]

Eg: [SPAM 3]Great Offers!

☐ Use antispam header tag (X-Spam-Status)

...

☑ Block SPAM

Delete mails with a tag superior or equal to (SMTP only): 1 - Low

Figure 304: Antispam general options

The Antispam module on NETASQ UTM appliances does not delete messages that are identified as spam. However, it modifies messages detected as spam in such a way that the webmail client can process it in the future, for example. There are two ways of tagging messages:

Prefix spam mail subject with

The subject of messages identified as spam will be preceded by a string of defined characters. By default, this string is "**SPAM***" where "*****" is the assigned level of confidence. This score ranges from 1 to 3, a higher number meaning the higher the possibility of the e-mail being spam. Regardless of the character string used, it is necessary to expect the insertion of the level of confidence in this string by using "*". This "*" will thereafter be replaced by the score. The maximum length of the prefix can be 128 characters. E-mails identified as spam will be transmitted without being deleted.

WARNING

The following characters will not be allowed: **"** (double quotes), **'** (apostrophes) and # (number sign).

Use Antispam header tag (X-Spam status)

When this option is selected, the Antispam module will add a header summarizing the result of its analysis to messages identified as spam. The webmail client can then use this antispam header, in "spamassassin" format, to perform the necessary actions on the tagged message.

Block SPAM

If this option is selected, the SMTP proxy will respond to the remote SMTP server by indicating that the e-mail has been rejected as it has been deemed to be spam. The option **Delete mails with a tag superior or equal to (SMTP only)** allows defining the confidence threshold beyond which an e-mail will be rejected. The thresholds are: "1 – Low", "2 – Medium", "3 – High".
For example, if you set a limit of 500 for the heuristic analysis, e-mails higher than 500 will be considered spam. From 500 to 1000, the level of confidence will be low, from 1000 to 1500 it will be moderate and from 1500 to 2000, it will be high.

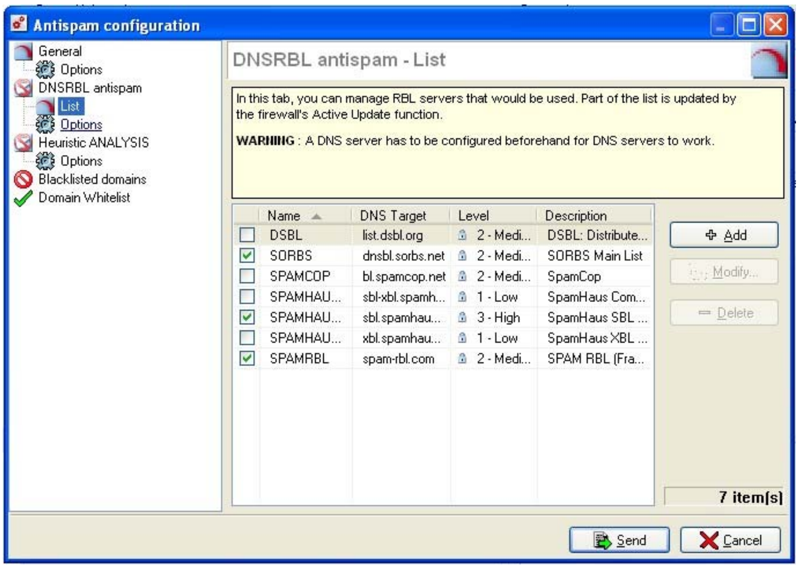
If you have indicated a moderate level of confidence for this option, all e-mails of moderate and high level (from 1000 to 2000) will be rejected whereas those from 500 to 1000 will be kept.

REMARK
When several methods of anlaysis are used simultaneously, the highest score will be assigned.

10.2.3.2. DNS blacklist analysis

DNS blacklist or **RBL** (*Realtime Blackhole List*) analyses enable the identification of messages as spam through RBL servers. The following menus are instrumental in the configuration of RBL servers which will be used for this analysis as well as the level of confidence assigned to each server.

List



DNSRBL antispam - List

In this tab, you can manage RBL servers that would be used. Part of the list is updated by the firewall's Active Update function.

WARNING : A DNS server has to be configured beforehand for DNS servers to work.

	Name	DNS Target	Level	Description
□	DSBL	list.dsbl.org	2 - Medi...	DSBL: Distribute...
☑	SORBS	dnsbl.sorbs.net	2 - Medi...	SORBS Main List
□	SPAMCOP	bl.spamcop.net	2 - Medi...	SpamCop
□	SPAMHAU...	sbl-xbl.spamh...	1 - Low	SpamHaus Com...
☑	SPAMHAU...	sbl.spamhau...	3 - High	SpamHaus SBL ...
□	SPAMHAU...	xbl.spamhau...	1 - Low	SpamHaus XBL ...
☑	SPAMRBL	spam-rbl.com	2 - Medi...	SPAM RBL (Fra...

7 item(s)

Figure 305: Blacklist analysis - List

In this section, a table displays the list of RBL servers which the Firewall queries to check that an e-mail is not spam. This list is updated by Active Update and cannot be modified, but certain servers can be deactivated by clicking on the checkbox at the start of each line.

The levels indicated in the fourth column of the table refer to the levels of confidence assigned to the respective servers.

You can also configure the RBL servers to which you would like your Firewall to connect. To add a server, click on **Add**. The following window will appear:

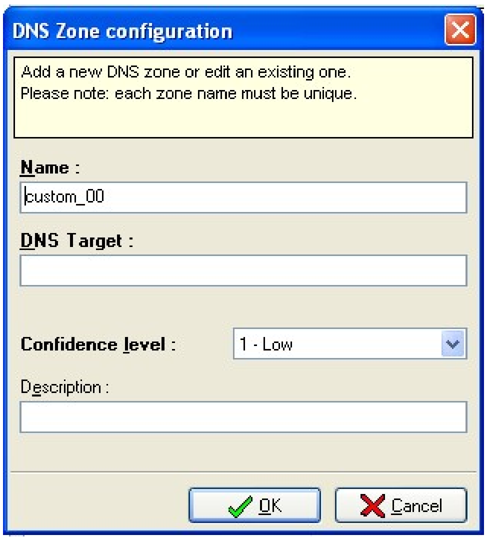


Figure 306: Configuring the DNS zone

Specify a name for this server (a unique name for the RBL server list), a DNS target (DNS name only, which should be a valid domain name), a level of confidence (Low, Medium and High) and comments (optional). Click on **OK.**

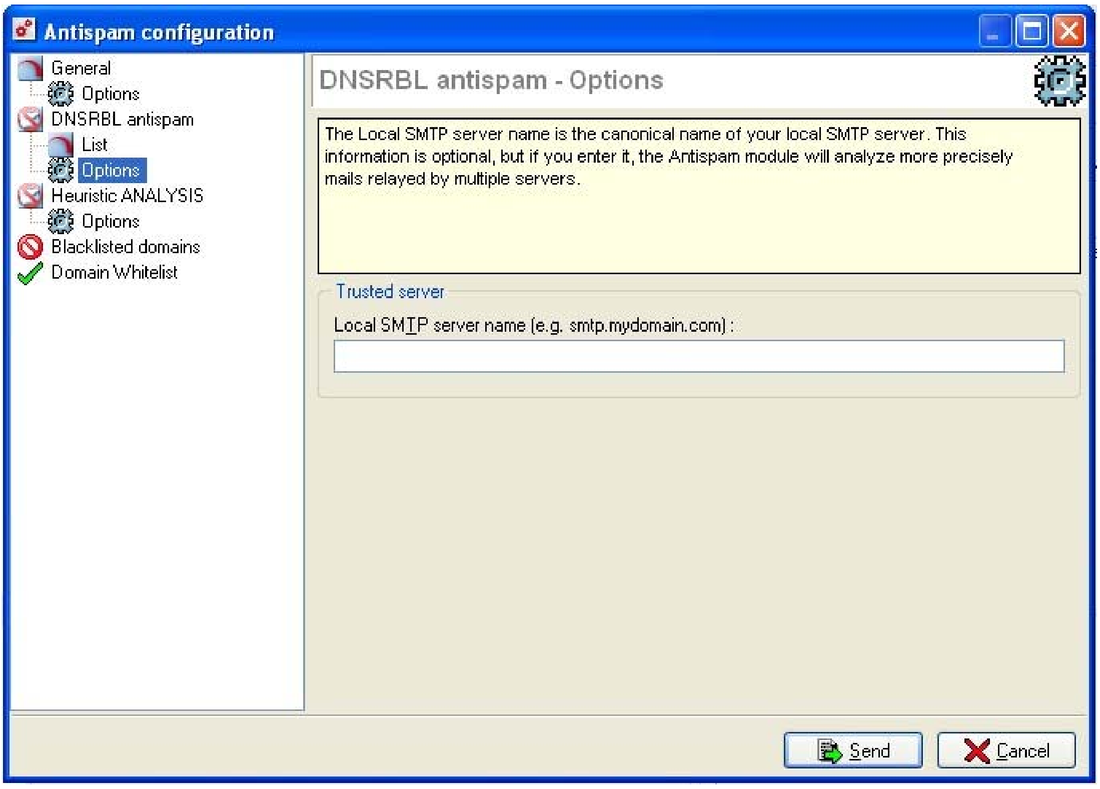
The buttons **Modify** and **Delete** enable you to respectively modify or delete configured servers.

NOTE
The DNS proxy must be activated for antispam to operate.

Note that **RBL** servers in NETASQ's native configuration are differentiated from customized servers by a padlock symbol (🔒).

✪ Reminder: **Active Update** only updates the list of these native servers.

Options



The Local SMTP server name is the canonical name of your local SMTP server. This information is optional, but if you enter it, the Antispam module will analyze more precisely mails relayed by multiple servers.

Trusted server

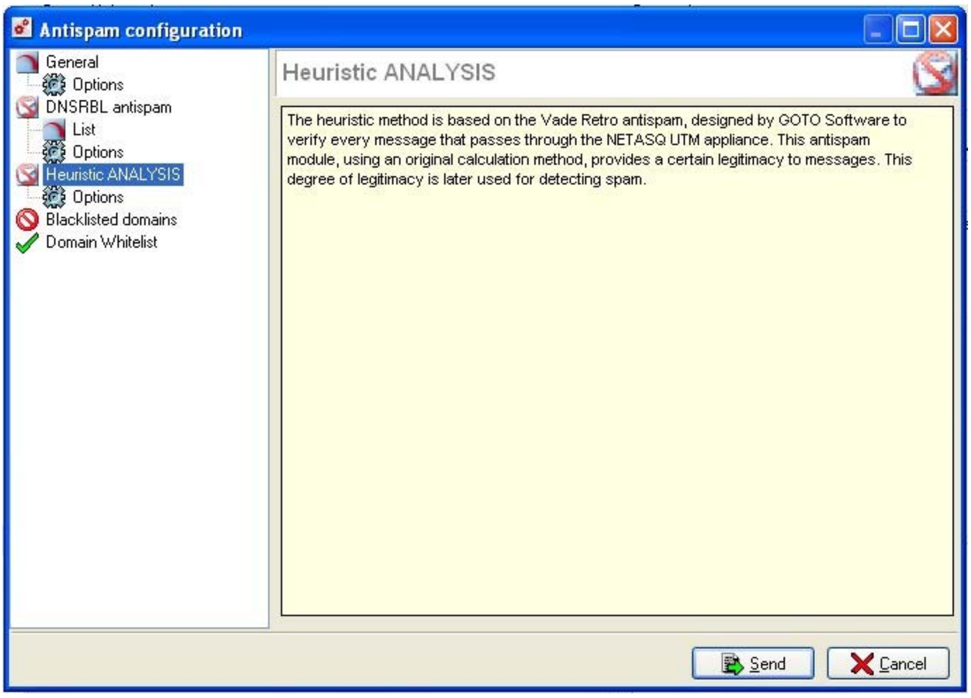
Local SMTP server name (e.g. smtp.mydomain.com) :

Figure 307: DNS blacklist analysis - Options

The trusted server concerns the SMTP server. This field is optional, but if you fill it in, e-mails will be more finely scanned by the antispam module.

Local SMTP server name (e.g.: smtp.mydomain.com	The local **SMTP** server assigns the canonical name of your SMTP server. This information is optional, but if it is entered, the antispam module will more thoroughly analyze e-mails relayed by multiple servers.

10.2.3.3. Heuristic analysis

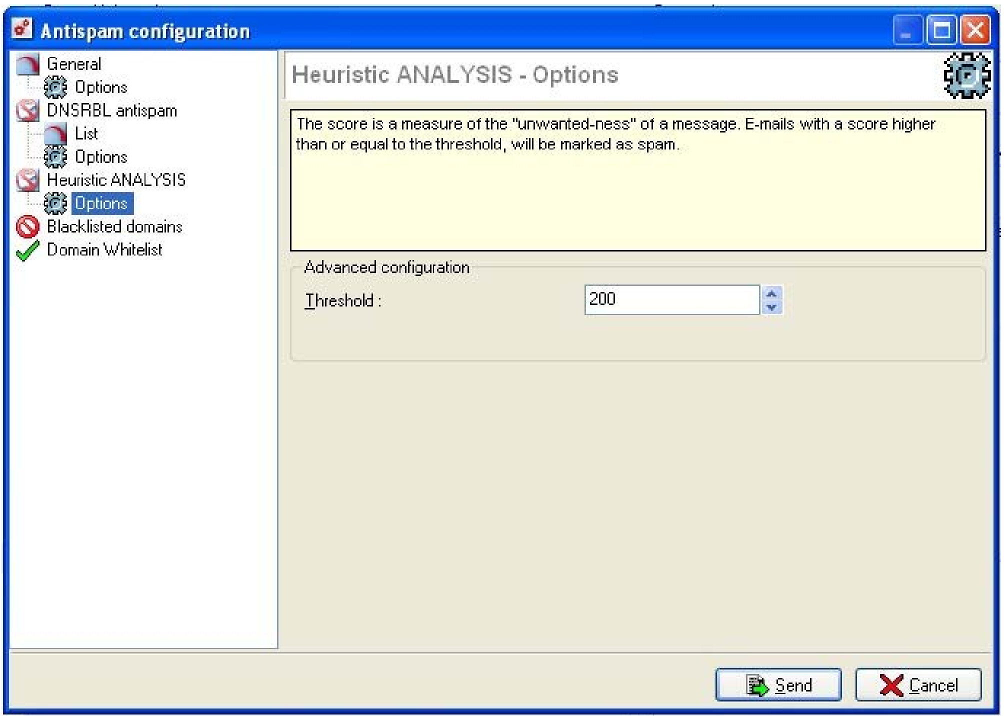


The heuristic method is based on the Vade Retro antispam, designed by GOTO Software to verify every message that passes through the NETASQ UTM appliance. This antispam module, using an original calculation method, provides a certain legitimacy to messages. This degree of legitimacy is later used for detecting spam.

Figure 308: Heuristic analysis

The heuristic analysis is based on GOTO Software's VadeRetro antispam. Using a set of caculations, this antispam will derive a message's degree of legitimacy. The VadeRetro analysis is configured in the menu **`Options`** in the heuristic analysis menu.

Options



The score is a measure of the "unwanted-ness" of a message. E-mails with a score higher than or equal to the threshold, will be marked as spam.

Threshold : 200

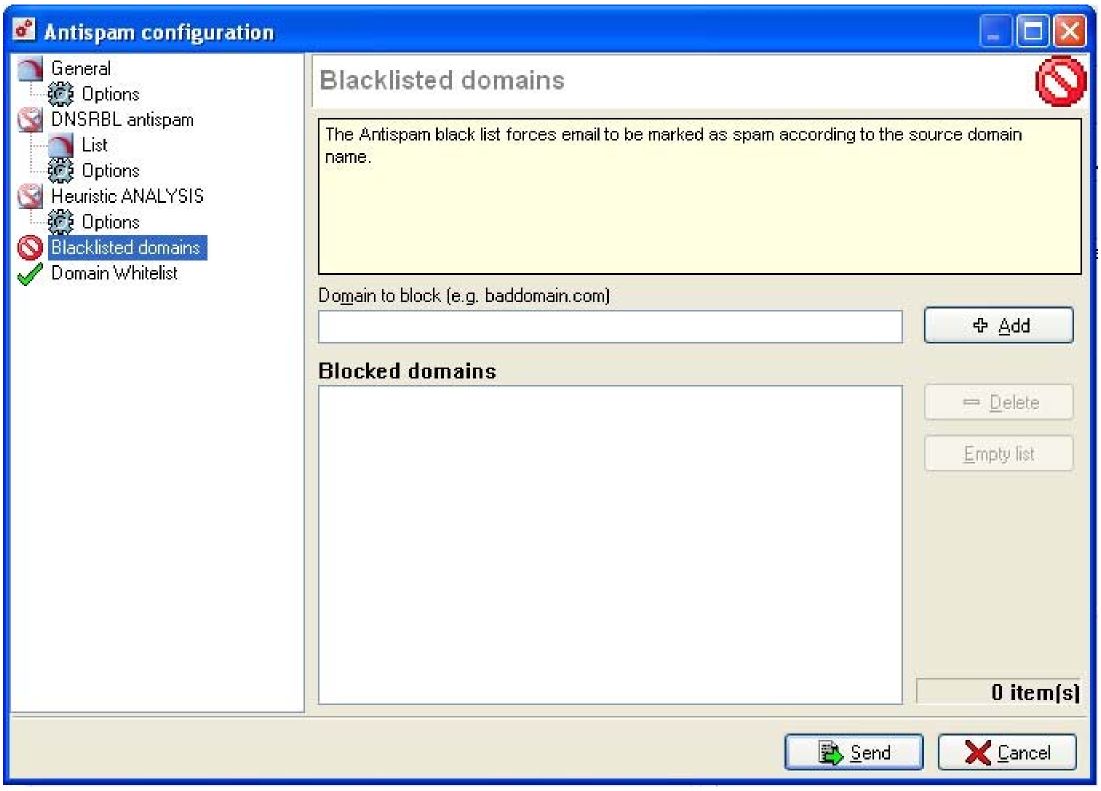
Figure 309: Heuristic analysis - Options

Threshold

The heuristic analysis performed by the Antispam module calculates a value that defines a message's "unwantedness" (the extent to which a message is undesirable). E-mails that obtain a value exceeding or equal to the threshold set will be considered as spam. This section enables the definition of a threshold to apply. NETASQ's default value is 200.

The higher the calculated value, the higher will be the level of confidence that the antispam module gives to the analysis. Thresholds for the levels of confidence cannot be configured in NETASQ UNIFIED MANAGER.

10.2.3.4. Blacklisted domains



Blacklisted domains

The Antispam black list forces email to be marked as spam according to the source domain name.

Domain to block (e.g. baddomain.com)

Blocked domains

0 item(s)

Figure 310: Blacklisted domains

This section enables the definition of domains from which analyzed messages will be systematically defined as spam. The procedure for adding a domain is as follows:

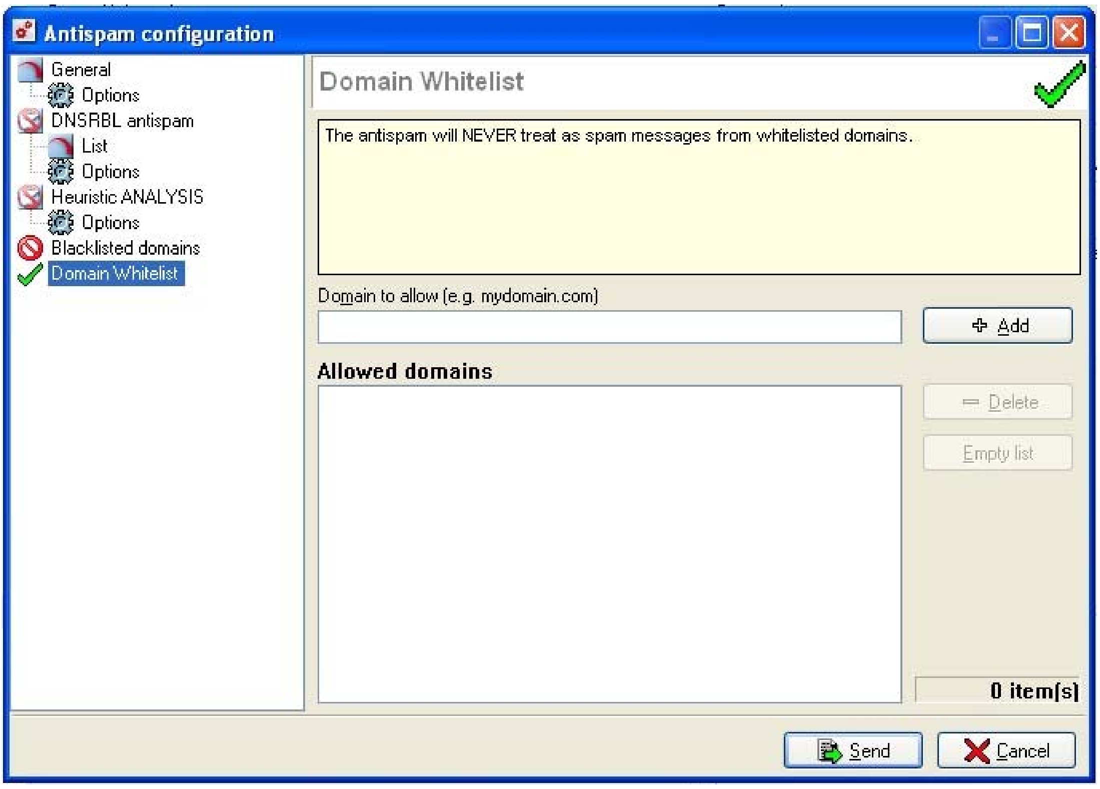
Domain to block (ex.baddomain.com)

Specify the domain to be blocked.

Click on **Add**.

The added domain will then appear in the list of blacklisted domains. Messages that are treated as spam because their domains are blacklisted will have the highest level of confidence (3). To delete a domain or the whole list of domains, click on **Delete** and **Clear list** respectively.

10.2.3.5. Whitelisted domains



The antispam will NEVER treat as spam messages from whitelisted domains.

Domain to allow (e.g. mydomain.com)

Allowed domains

0 item(s)

Figure 311: Whitelisted domains

This section enables the definition of domains from which analyzed messages will be systematically treated as **legitimate**. The procedure for adding an authorized domain is as follows:

Domain to allow (ex: mydomain.com)	Specifies the domain to be allowed. Click on **Add**. The added domain will then appear in the list of whitelisted domains. To delete a domain or the whole list of domains, click on **Delete** and **Clear list** respectively.

10.2.3.6. Remarks on blacklisted and whitelisted domains

Blacklisting and whitelisting prevail over DNS blacklist analyses and heuristic analyses. The domain name of the sender is compared against blacklisted and whitelisted domain in succession.

For each of these lists, up to 50 domains can be defined. The same domain name cannot appear more than once in the same list. However, a domain name can appear in both the whitelist and the blacklist. In this case, the blacklist has priority.

Domain names can contain alphanumeric characters, as well as "_", "-" and ".". Wildcard characters "*" and "?" are also allowed. The length of the domain name must not exceed 128 characters.

CHAPTER 3. ANTIVIRUS

By reason of its central position on your network, the NETASQ Firewall is an important element of your company's security policy. As an indispensable gateway to the internet, your Firewall protects you from intrusions notably thanks to ASQ, its intrusion detection and prevention engine.

This protection is strengthened by an antivirus service that enables filtering the contents of traffic passing through your Firewall, and sniffing out viruses, backdoors, Trojan horses and other types of malware found on the internet.

The Antivirus service range on NETASQ Firewalls comprises two solutions.

10.3.1. The ClamAV antivirus service

The ClamAV Open-source antivirus project is embedded by default and at no additional charge on NETASQ Firewall products, and thus provides protection against viruses and completes NETASQ's all-in-one range of Firewalls.

ClamAV, which is a multi-thread (it can perform several tasks simultaneously), quick, flexible and extendable daemon, is a powerful solution to problems caused by viruses spreading over the internet. It has a database containing 36,000 virus, worm and Trojan horse signatures, thereby providing protection that becomes more complete by the day.

10.3.2. The Kaspersky antivirus service

Kaspersky Labs is an international publisher of antivirus, anti-hacking and anti-spam software, founded in 1997.

Hard work and deep involvement have made of Kaspersky Labs a leader in the development of antivirus defense systems. Kaspersky Labs was the first to develop numerous technology standards in the antivirus industry, including wide-ranging solutions for Linux, Unix and NetWare, a second-generation heuristic analyzer designed to detect as yet unknown viruses, an efficient defense system against polymorph and giant viruses, a regularly updated antivirus database **(currently containing more than 120,000 signatures)** and the ability to search for viruses in archived files.

The Kaspersky antivirus service is now embedded in the NETASQ Administration Suite. All you need is to install a compatible license then select this service in NETASQ UNIFIED MANAGER.

WARNING

1) Setting up the NETASQ Firewall Antivirus service does not provide an overall solution to problems posed by viruses.
2) Setting up a solution which analyzes workstations and servers to protect your network resources from the insertion of viruses via such means as physical data transport systems (e.g., diskettes) is INDISPENSABLE.

10.3.3. Using the NETASQ Firewall's Antivirus service

As a complement to filtering carried out by **SMTP**, **HTTP** and **POP3** (the proxies have to be activated beforehand in order to use the Antivirus service), the Antivirus service protects you from viruses hiding in SMTP, HTTP and POP3 traffic.

> ❗ WARNING
> The antivirus service only works on interfaces on which **SMTP**, **HTTP** and **POP3** have been activated. If you wish to protect your network against viruses originating from external SMTP traffic, you have to activate the SMTP proxy for incoming traffic (See *Part 9: HTTP, SMTP and POP3 proxies*).

10.3.4. Operation

➲ The Antivirus service has to be activated in order to be used via the menu **`Content Analysis`** \**`Antivirus`** in the menu directory.

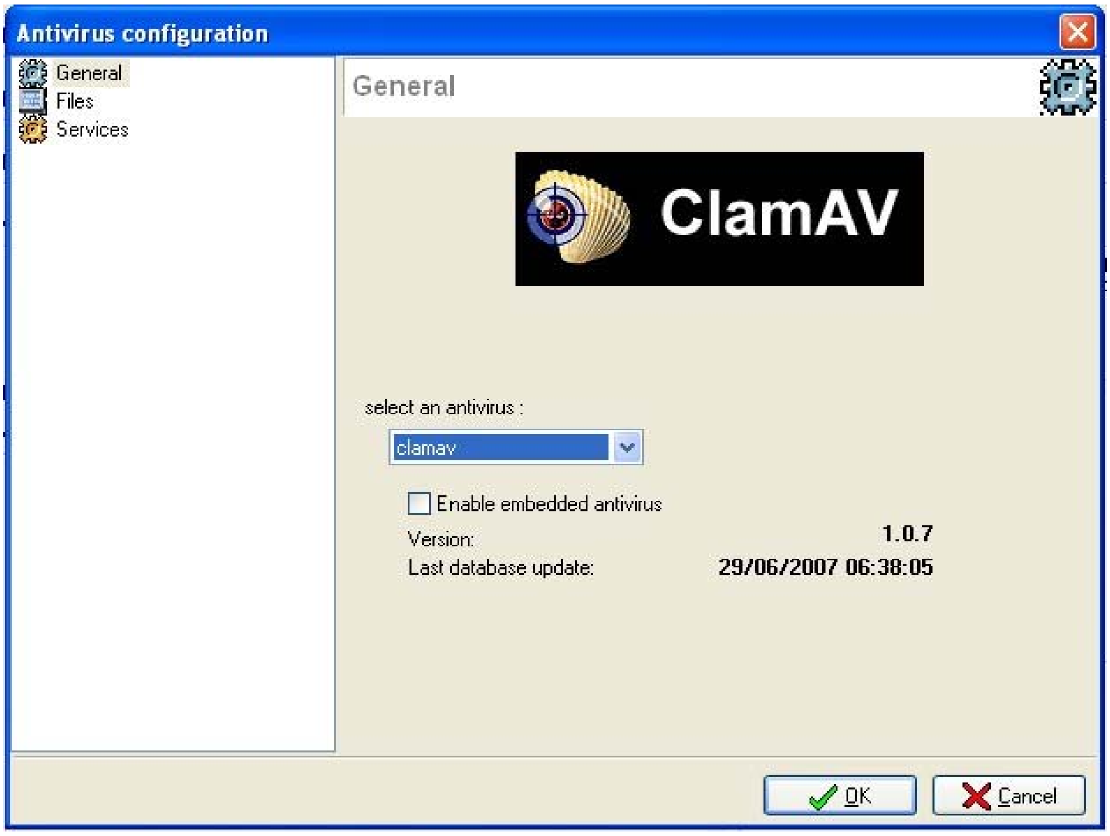
The anitvirus service configuration window comprises two sections:

- On the left, the various features of the Antivirus menu.
- On the right, the configurable options.

Activating the NETASQ Firewall Antivirus service requires certain preliminary operations::

1. Activation of proxies from the menu **`SMTP Proxy`**, **`POP3 Proxy`** and **`HTTP Proxy.`**
2. Activation of the antivirus from the menu **`Content Analysis\Antivirus`**.

10.3.5. General



select an antivirus : clamav

☐ Enable embedded antivirus

Version: 1.0.7

Last database update: 29/06/2007 06:38:05

Figure 312: Configuring the antivirus - General

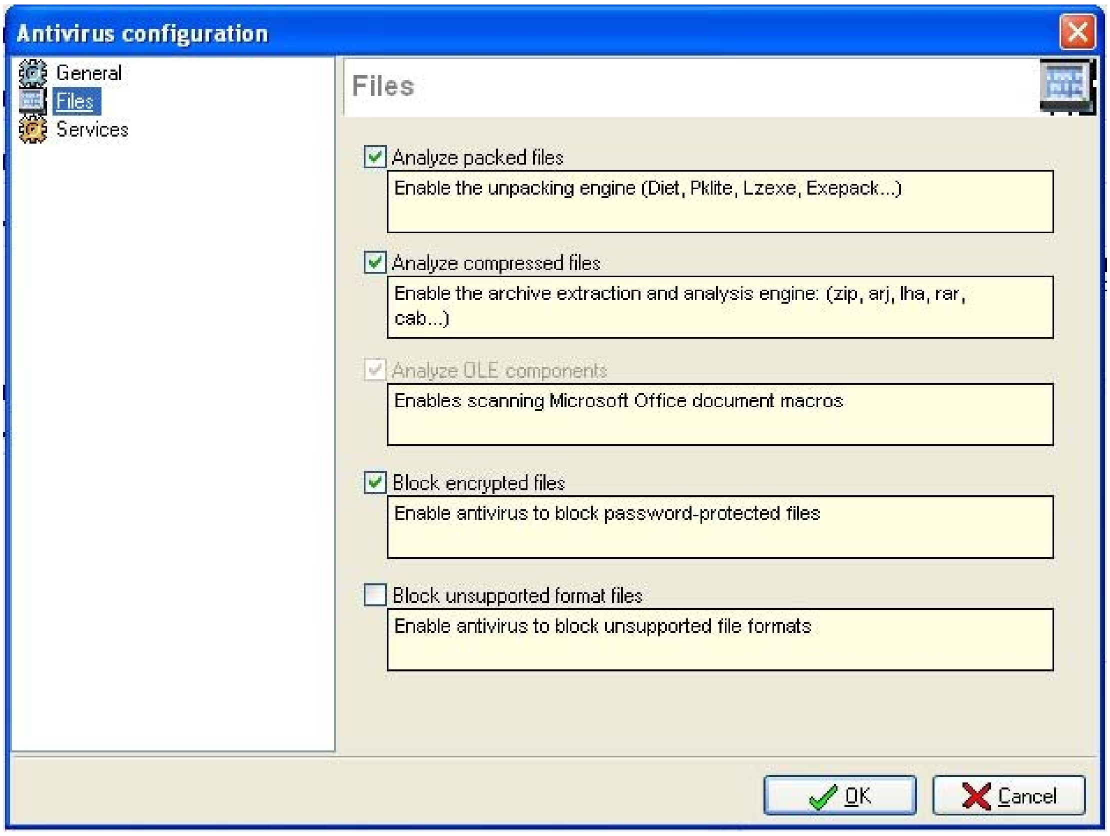
The activation of the service enables the analysis of **SMTP**, **HTTP** and **POP3** traffic (See *Part 9: HTTP, SMTP and POP3 proxies*).
The general configuration menu of the NETASQ Firewall antivirus service comprises several options set out in the table below:

Figure 313: Selecting an antivirus

Select an antivirus	Select the antivirus of your choice from the drop-down menu – Clamav or Kaspersky.
Enable embedded antivirus	Select the option in order to activate virus protection. The **ClamAV** antivirus is used by default, but you can also benefit from the Kaspersky antivirus service. For this, contact your distributor.
Version	Data on the version of the antivirus engine embedded in the NETASQ Firewall.
Last database update	Data indicating the data of the last successful update of the antivirus' database. Updating the antivirus database is an important part of guaranteeing a powerful and effective antivirus service. When new viruses appear, it is important to benefit from their signatures soonest possible in order to be protected from them.

	The modalities for automatically updating the antivirus database are defined in **Active Update.**

10.3.6. Files



☑ Analyze packed files
Enable the unpacking engine (Diet, Pklite, Lzexe, Exepack...)

☑ Analyze compressed files
Enable the archive extraction and analysis engine: (zip, arj, lha, rar, cab...)

☑ Analyze OLE components
Enables scanning Microsoft Office document macros

☑ Block encrypted files
Enable antivirus to block password-protected files

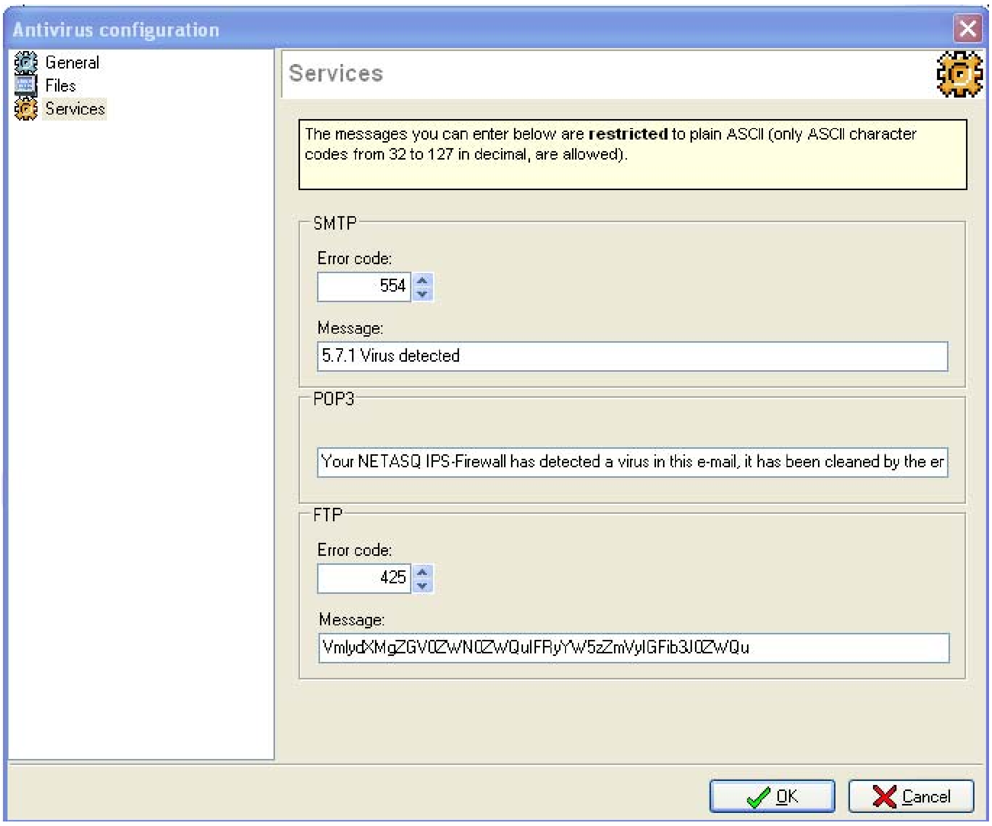
☐ Block unsupported format files
Enable antivirus to block unsupported file formats

Figure 314: Configuring the antivirus – Files

In this menu, you can configure the file types which have to be analyzed by the NETASQ Firewall Antivirus service.

Analyze packed files	This option allows activating the decompressor.
Analyze compressed files	This option allows activating the extraction engine and analyzing the archives.
Analyze OLE components	This option allows activating the analysis of Microsoft Office document macros.
Block encrypted files	This option allows activating the antivirus in order to block password-protected files.
Block unsupported file formats	This option allows activating the antivirus in order to block file formats that cannot be analyzed.

10.3.7. Services



The messages you can enter below are **restricted** to plain ASCII (only ASCII character codes from 32 to 127 in decimal, are allowed).

SMTP

Error code: 554

Message: 5.7.1 Virus detected

POP3

Your NETASQ IPS-Firewall has detected a virus in this e-mail, it has been cleaned by the er

FTP

Error code: 425

Message: VmlydXMgZGV0ZWN0ZWQuIFRyYW5zZmVyIGFib3J0ZWQu

Figure 315: Configuring the antivirus - Services

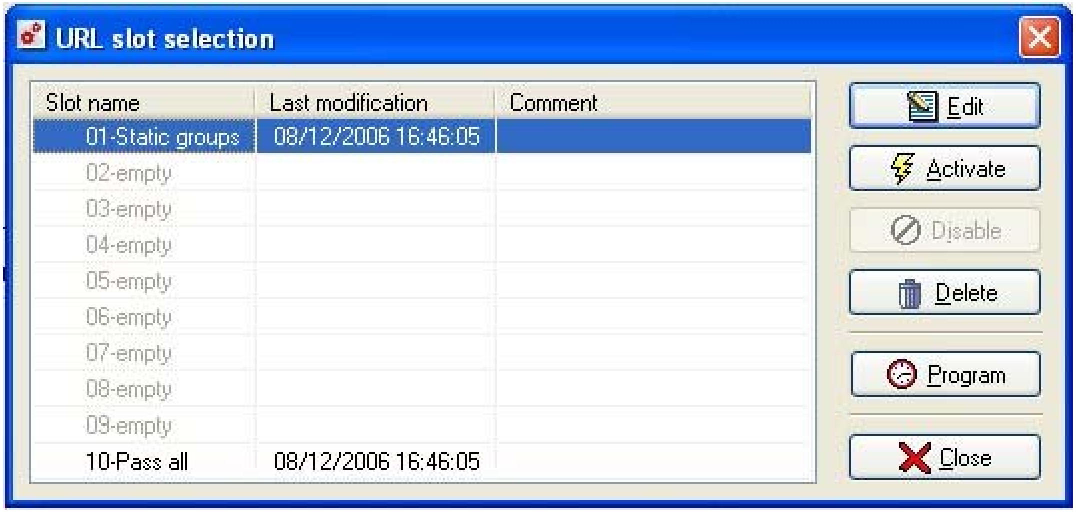
Advanced **Kaspersky** Configuring the antivirus enables customizing the responses sent to users when an e-mail contains a virus. The different parameters are explained as follows:

Error code	SMTP error code that the sender will receive when a virus is detected in the SMTP traffic.
Message	Message attached to the SMTP error code.
Custom message for POP3 antivirus service	When a virus is detected in the POP3 traffic, the NETASQ Firewall will generate an e-mail, which will contain the message indicated in this field and part of the original e-mail (mainly the sender, intended recipient and subject). The Firewall will then send this e-mail to the sender of the POP3 request on which the virus was discovered.
Custom message for FTP antivirus service	When a virus is detected in the FTP traffic, the NETASQ Firewall will generate an e-mail, which will contain an error code and the message indicated in this field as well as part of the original e-mail (mainly the sender, intended recipient and subject). The Firewall will then send this e-mail to the sender of the FTP request on which the virus was discovered.

CHAPTER 4. URL FILTERS

Defining a URL filter policy consists of creating rules in order to determine the web pages that will be allowed or blocked by the firewall. This is exclusively used for http traffic and allows blocking access to certain ites according to defined criteria.

➲ When you select the submenu **`Content analysis\URL filtering\Filter rules`** a dialog box will appear, allowing you to handle the slots associated with URL filtering.



Slot name	Last modification	Comment
01-Static groups	08/12/2006 16:46:05	
02-empty		
03-empty		
04-empty		
05-empty		
06-empty		
07-empty		
08-empty		
09-empty		
10-Pass all	08/12/2006 16:46:05	

Figure 316: Selecting the URL slot

❗ **WARNING**
URL filtering will be enabled if one of the http proxy profiles is active.

It consists of two zones:

Left	List of policies or slots.
Right	Actions on selected slot.

10.4.1. List of slots

The list of slots is found in this part of the dialog box. There are 10, numbered from 01 to 10.

Each policy has a name, a date/time of activity and the date of the last change carried out on this slot. The activation of these slots can be programmed using the slot scheduler (See Part 7/Chapter 3: Slot Scheduler).

A small green arrow to the right of its name indicates the active slot. A slot is "active" when the parameters it contains are in use. There can be no more than one active slot because the parameters of the last active slot overwrite those of the previously active slot.

If you change a slot, you must reactivate it for the changes to be registered. A slot that has been modified but not reactivated is signaled by the icon ❗ instead of the usual green arrow.

It is possible for no slot to be active, implying that all web sites are blocked (default action) except if a rule allowing HTTP is added to the filter rules.

Each slot does not necessarily have to contain parameters.

A slot for which no configuration file exists on the NETASQ Firewall appears under the name "empty" in the list.

A slot is selected when you simply click on its name with the mouse. Once you have selected it, you can edit or activate it.

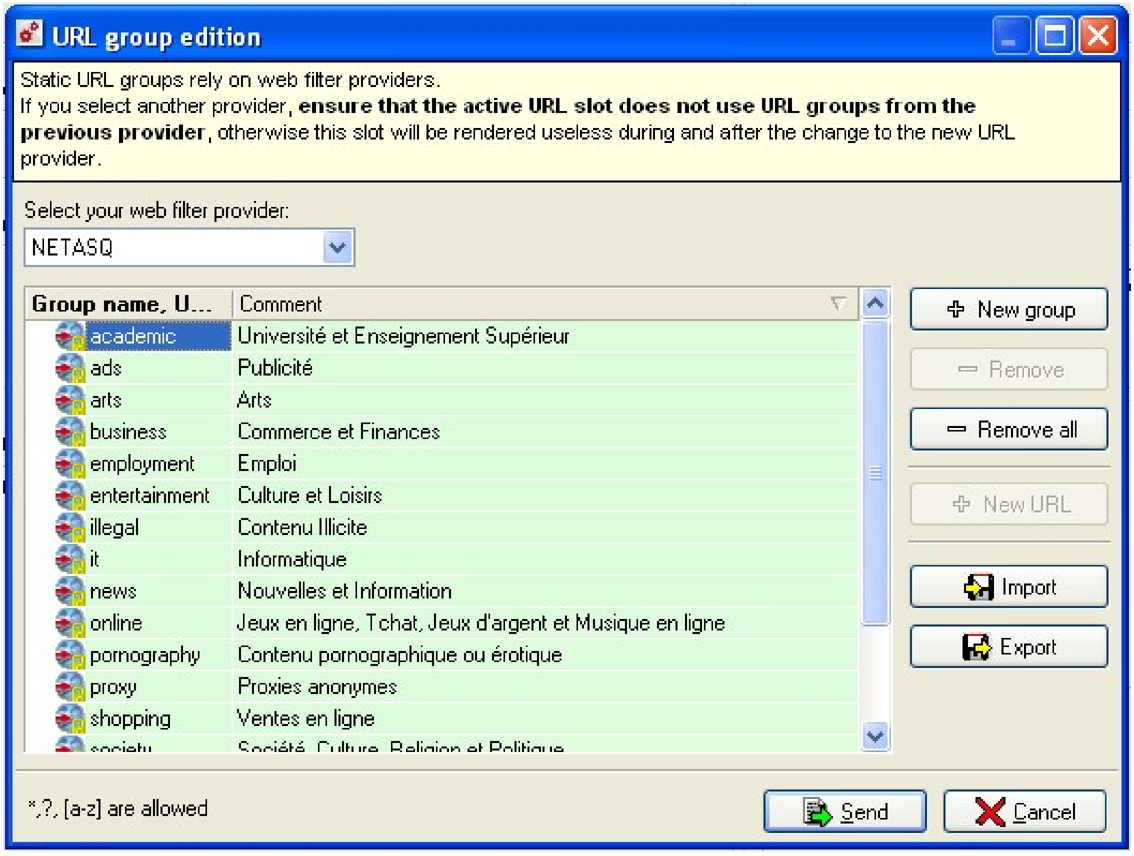
10.4.2. Actions on selected slot

A URL filter slot has been configured by default. It is not active but can be and is an example of the possibilities provided by NETASQ's URL filtering.

10.4.3. URL Groups

URL groups speed up the creation of filter rules. Each group contains a list of URL masks and allows, for example, representing the needs of each department in an enterprise.

➲ You can create URL groups via the `Content analysis\URL filtering\URL Groups` menu.



URL group edition

Static URL groups rely on web filter providers.
If you select another provider, **ensure that the active URL slot does not use URL groups from the previous provider**, otherwise this slot will be rendered useless during and after the change to the new URL provider.

Select your web filter provider: NETASQ

Group name, U...	Comment
academic	Université et Enseignement Supérieur
ads	Publicité
arts	Arts
business	Commerce et Finances
employment	Emploi
entertainment	Culture et Loisirs
illegal	Contenu Illicite
it	Informatique
news	Nouvelles et Information
online	Jeux en ligne, Tchat, Jeux d'argent et Musique en ligne
pornography	Contenu pornographique ou érotique
proxy	Proxies anonymes
shopping	Ventes en ligne
society	Société, Culture, Religion et Politique

*,?, [a-z] are allowed

Figure 317: Editing URL groups

The following actions may be carried out in the configuration of URL groups:

New group	Creates a new group.
Remove	Deletes an existing group or URL. Select the row to delete then click on this button.

Remove all	Deletes all URL groups.
New URL	Adds a URL to a group. First, select the group to which you wish to add a URL then click on this button.
Import	Imports a URL list contained in .txt file. First, you have to create a new group and give it a name. Then click on this button and select the file concerned. URLs contained in the file will then be integrated into the group. ❗WARNING If this group already contains URLs, they will be overwritten.
Export	Exports a URL list contained in a group. Select the group from which you wish to export the list, then click on this button. The list will be saved in a text file.
Select your web filter provider	There are two types of URL groups: static (manually entered by the administrator) and dynamic (see “Dynamic URL filtering” below). The requested provider is the web filter provider, NETASQ by default.

10.4.3.1. Format of the URL file

The text files for importing and exporting URLs have to be formatted as follows:

URL1
URL2
URL3
…

You can edit your own lists with a text editor and import them to the Firewall.

The URL mask may have the following syntax:

*****	Replaces any character sequence. **Example** *.netasq.com/* defines the internet domain for NETASQ.
?	Replaces a character. **Example** ???.netasq.com is equivalent to www.netasq.com or to ftp.netasq.com but not to www1.netasq.com.
[a-z]	Replaces a character space. **Example** ftp[1-2].netasq.com is equivalent to ftp1.netasq.com and to ftp2.netasq.com.

A URL mask can contain a full URL (**example:** www.netasq.com*) or keywords contained in the URL (**example:** *mail*).

You can also filter file extensions:

> **Example**
> the following URL mask '*.exe' will filter executable files.

You can show or hide the contents of each URL group by clicking on the "+" or "-" icons.

10.4.3.2. Dynamic URL filtering

Dynamic URL filtering is available as an option on NETASQ appliances and allows you to filter URLs through a list of URLs provided and updated dynamically using the “Active Update” feature (see *Part 18: Active Update*).

These URLs are classified according to categories (among the following: pornography, business, employment, entertainment, illegal, IT, news, online, shopping, society, warez, arts, proxy, academic and ads). Each of these categories contains a list of URLs that you can authorize or block.

The URLs contained in these groups cannot be viewed as they are compressed and optimized for treatment by the Firewall, and so cannot be modified. Dynamic URL groups are identified by the padlock symbol 🔒 in front of its group name.

10.4.3.3. URL list provider

Depending on the maintenance service subscribed (***see NETASQ’s current pricing policy***), the available lists of URLs are updated dynamically by different providers (either NETASQ or OPTENET). NETASQ has recently categorized two provider types – NETASQ itself and OPTENET. By default, when a “standard” maintenance service has been subscribed, NETASQ URL lists will be proposed.

If you are subscribed to the maintenance service that includes OPTENET, to activate the URL filter feature on OPTENET URL lists, select “OPTENET” from the list of proposed providers. When shutting down the URL groups menu, the appliance will apply the request and will download new URL lists through the **Active Update** module.

WARNING
When modifying the web filter provider, ensure that the active URL filter slot will not be affected by the removal of old URL groups. If the active slot is affected, disable it.

10.4.3.4. Request to add URL

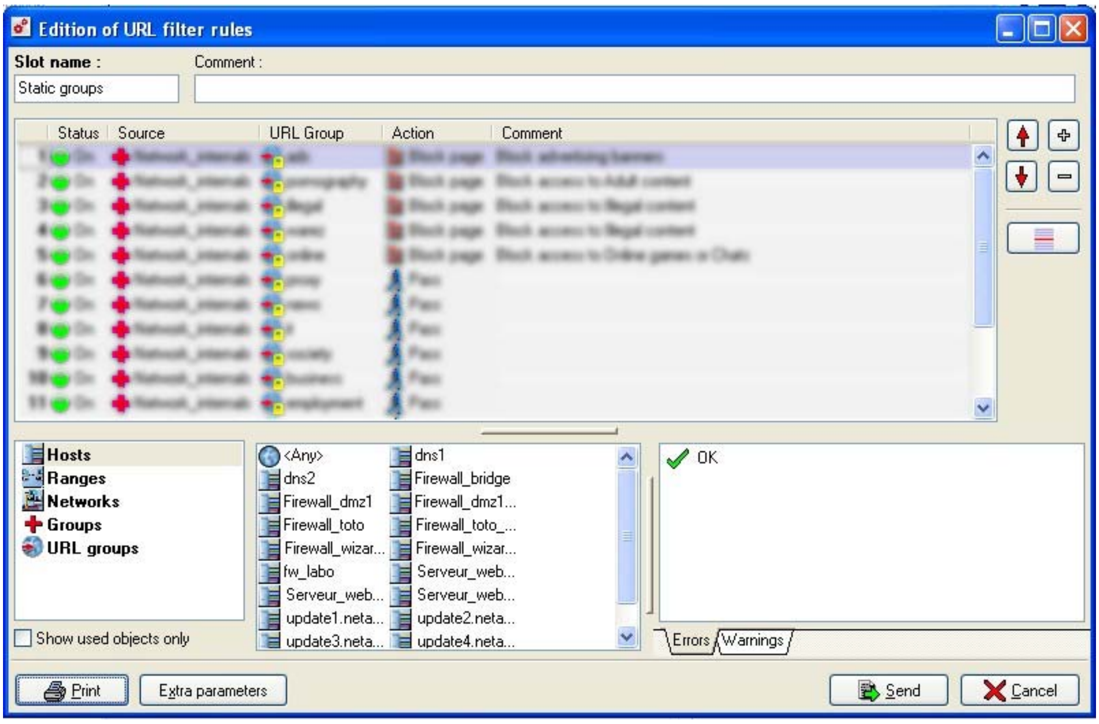
NETASQ has made available on its website a form allowing you to submit a request to add a URL that dynamic URL groups do not yet recognize. This form can be found at the following address: **http://www.netasq.com/updates/url.en.php**. NETASQ reserves the right to not accede to this request (due to the validity of the request, or the address does not correspond to any defined categoriy, etc)

NOTE
You can manually add addresses to the “static” URL group and add it to the filters.

10.4.4. Filter rules

The procedure for editing a URL filter slot is as follows:

1 Select a slot from the list of URL filter slots.
2 Click on **Edit** in the dialog box containing the list of URL filter slots.



Edition of URL filter rules

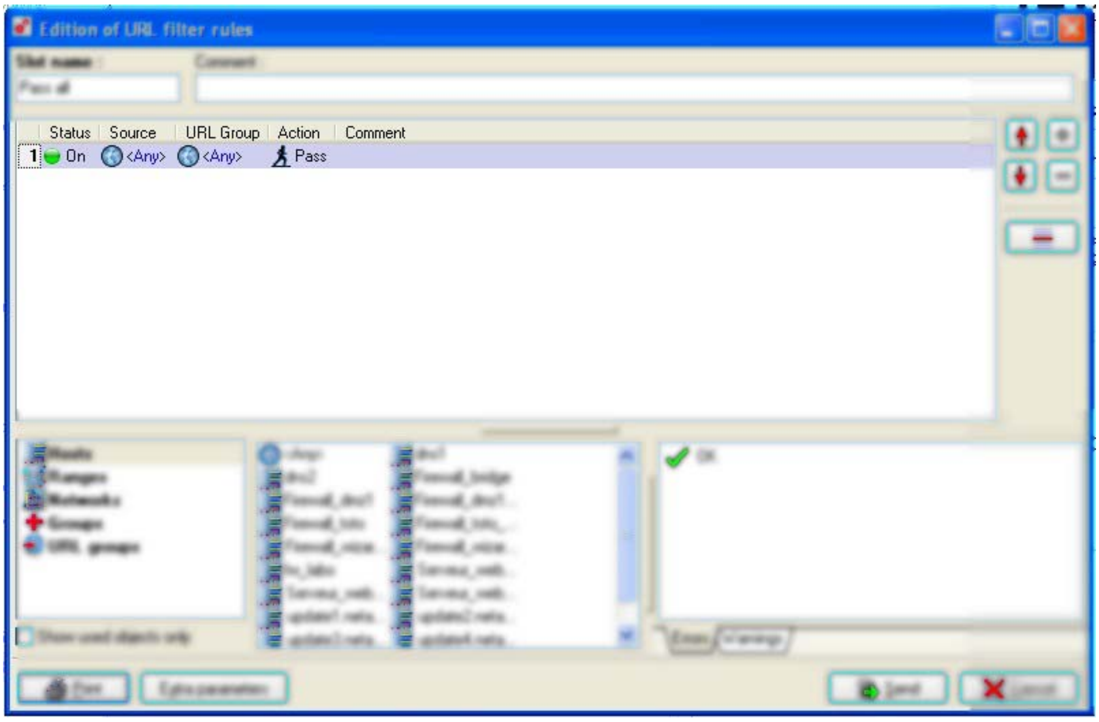
Slot name : Static groups

Comment :

Figure 318: Editing URL filter rules

The URL filter slot edition window, which comprises two parts, appears.

- A section consisting of URL filter rules.
- A drag & drop menu
- A rule compliance analyzer
- A section with the possible actions to perform.



Edition of URL filter rules

Slot name : Pass all

Comment :

	Status	Source	URL Group	Action	Comment
1	● On	<Any>	<Any>	Pass	

Figure 319: Table of rules

This part of the dialog box has a grid allowing you to specify which URL filter rules to apply. You can edit these rules by double-clicking on the part you want to change.

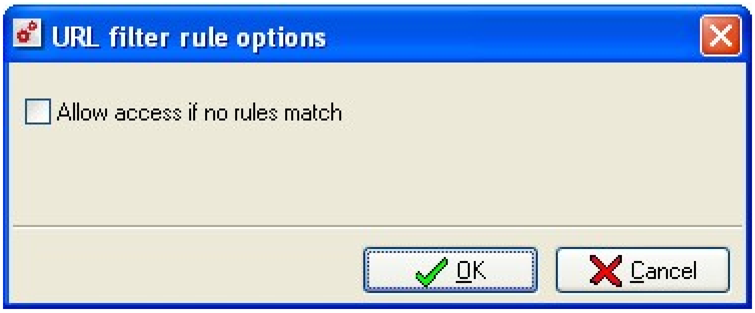
ID This refers to the number of the rule in the policy. There can be as many numbers as there are rules in a URL filter policy. This field cannot be edited as it corresponds to the rule's order

Status Rule's status

● **ON**, the rule will be active when this filter slot is active.

● **OFF**, the rule will not be active when this slot is active. When the rule If Off, the row will be grayed out to show that it has been disabled.

The Firewall will evaluate these rules individually, starting from the top. As soon as it finds a rule matching the request, it carries out the specified action and does not move down the list of rules. If no rule is applicable, the Firewall will then use the default configuration (authorizing or blocking depending on whether the option "Allow access if no rules match" has been selected).



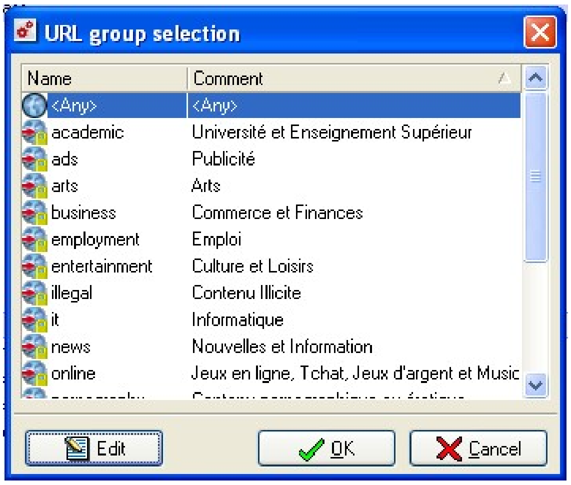
URL filter rule options

□ Allow access if no rules match

Figure 320: Options for URL filter rules

Source Indicates the user, host, address range, user group, host group or network applies to which the rule applies. When the source is a user or a user group, an additional

	group is needed in order to obtain the object user@host.
URL Group	The name of a URL group previously created. By double-clicking on the field, a dialog box prompts you to select a URL group.



URL group selection

Name	Comment
<Any>	<Any>
academic	Université et Enseignement Supérieur
ads	Publicité
arts	Arts
business	Commerce et Finances
employment	Emploi
entertainment	Culture et Loisirs
illegal	Contenu Illicite
it	Informatique
news	Nouvelles et Information
online	Jeux en ligne, Tchat, Jeux d'argent et Music

Figure 321: Selecting a URL group

	The group <Any> corresponds to all the URLs.
Action	Specifies the result of the rule, **pass** to authorize the site, **block** to prohibit access without error message, **block page** to prohibit access and displays the block page.
Comment	Comments associated to the rule.

As for the source, you may define users or user groups which have to authenticate to access certain sites (you can authorize certain sites only for certain users). The user who has to authenticate will see an authentication page appear in his browser when he attempts to connect to a web site.

10.4.4.1. Possible actions

Slot name	Name given to the configuration file.
Comments	Comments associated to the filter slot
Insert +	Inserts a new row after the selected row.
Delete −	Deletes the selected row.
↑	Places the selected row before the row directly above it.
↓	Places the selected row after the row directly below it.
Insert a separator ≡	This option enables inserting a separator above the selected row in order to add a comment when editing filters. To define a separator, only a comment and colour need to be be specified for this separator.
Print	Opens the print dialog box allowing you to print your translation rules.
Extra parameters	Enables specifying how URL filtering will work. Check the option **Allow access if no rules match** to function in URL blacklist mode.

REMARK
Here, the drag & drop function only applies to the Source and URL group fields since they use the objects database.

10.4.4.2. Grid display

The display of data contained in the grid can be defined according to the administrator’s preferences from the following options: large icons, small icons, details or lists.

10.4.4.3. Display options

There are two available options for displaying data from the drag & drop menu grid.

Hide unused objects

As its name implies, this option enables displaying only objects currently used in filter rules.

10.4.5. Rule compliance analyser

In the same way as for the edition of filter and translation rules, the URL filter rule edition window has a rule compliance analyzer that that warns the administrator whenever a rule contradicts another or when there is an error on a rule.

This analyzer, which is divided into two tabs, groups all the errors during the creation of rules in the **`Errors`** tab and coherence errors in the **`Warning`** tab.

10.4.6. Sending modifications to the NETASQ Firewall

Click on the button **Send** to store the file under the specified name in the 'Name' field.

When a slot is sent to the NETASQ Firewall, the configuration software checks the name it has been given. In no circumstances can the file name be empty, or have the same name as an existing file. If such is the case, the software will display a dialog box prompting you to modify the slot name.

After clicking on **OK**, you can modify the **Name** field as well as all other parameters.

> ❗ WARNING
> Modifications of URL filter slots are not dynamic actions. They will take effect only the next time the slot is activated on the NETASQ Firewall.

PART 11: SERVICES

CHAPTER 1. DHCP

11.1.1. Introduction

DHCP provides configuration parameters for internet hosts. It comprises two parts: a protocol for the delivery of specific host configuration parameters from a DHCP server and a mechanism which allocates network addresses to hosts.

DHCP is based on the client-server model.

> **DEFINITION**
> The term **server** refers to a host which provides initialization parameters through DHCP and the term **client** refers to a host which uses DHCP to obtain configuration parameters such as a network address.

11.1.2. Using the NETASQ Firewall's DHCP service

> **DEFINITION**
> NETASQ's DHCP service is a server which allows you to allocate network address and to issue configuration parameters to dynamically configured hosts.

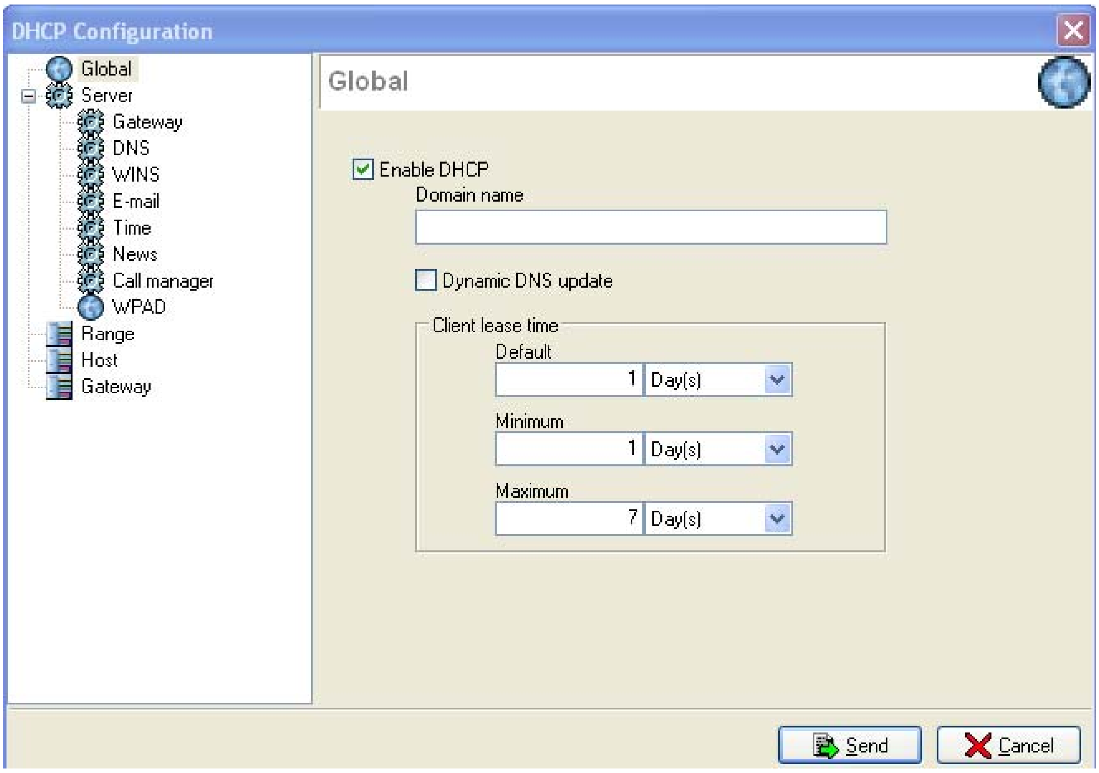
11.1.3. Operation

The DHCP service has to be activated in order to be used via the menu **`Services\DHCP`**.

The DHCP service configuration window comprises two sections:

- On the left, the various features of the **`DHCP`** service menu.
- On the right, the options that can be configured

11.1.4. Global



☑ Enable DHCP

Domain name

□ Dynamic DNS update

Client lease time

Default: 1 Day(s)

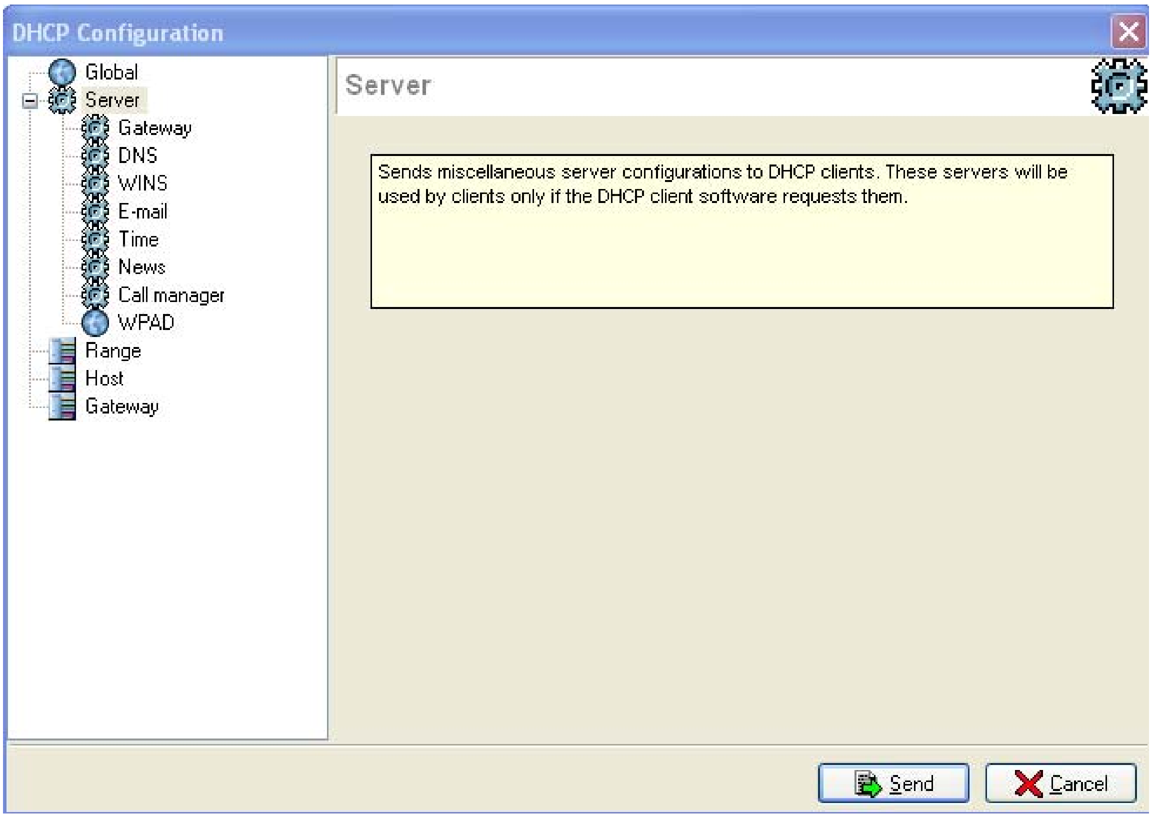
Minimum: 1 Day(s)

Maximum: 7 Day(s)

Figure 322: Configuring the DHCP: Global

Domain name	Domain name used to define users.
Dynamic DNS update	Dynamic update of the DNS. When information contained in the DHCP server is modified, DNS server 1 (configured in the DNS server menu) is dynamically updated.
Client lease time	Time during which stations will keep the same IP address. A default value, maximum and minimum values are to be specified.

11.1.5. Server



Sends miscellaneous server configurations to DHCP clients. These servers will be used by clients only if the DHCP client software requests them.

Figure 323: Configuring the DHCP - Server

This menu is reserved for the configuration of addresses of different servers: Gateway, DNS, WINS, E-mail (**SMTP** and **POP**), Time (**NTP**), News and Call Manager. These addresses will automatically be sent to stations so that they may contact peer servers.

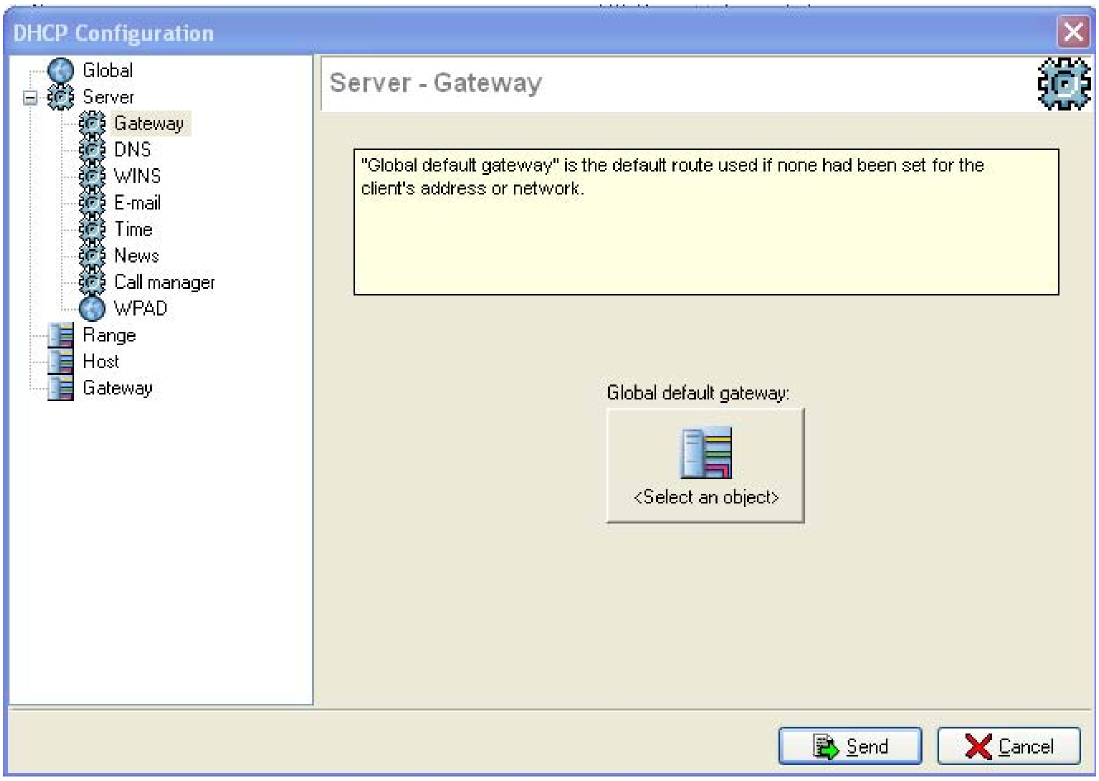
Two attribution modes are possible:

- By range
- By host

When attribution by range is selected, you can specify a group of addresses to be allocated to users. The address is then allocated for the time determined in global configuration. In **DHCP** configuration by host, the address allocated by the service is always the same – the address indicated in the **`Host`** menu. In reality, this is “static” addressing, but it allows “liberating” the client post from its network configuration.

11.1.5.1. Gateway

The default gateway is the default route used if no other route has been specified for the client’s or network’s address.

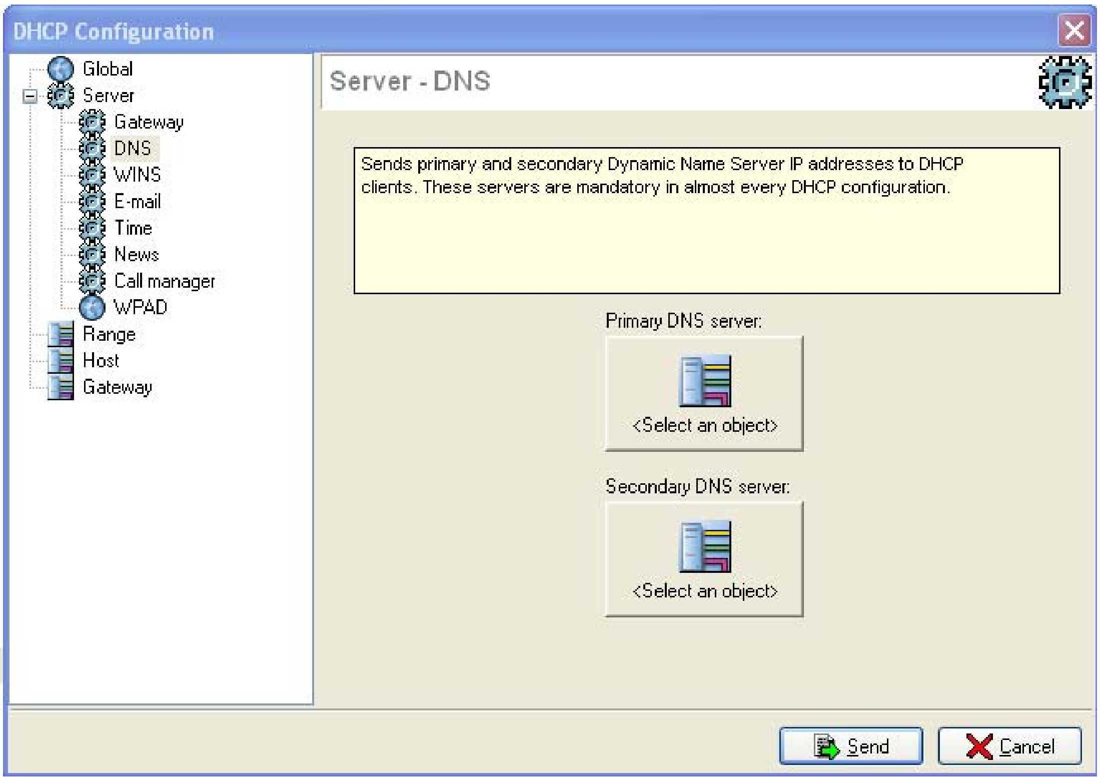


"Global default gateway" is the default route used if none had been set for the client's address or network.

Global default gateway:
<Select an object>

Figure 324: Configuring the DHCP - Server - Gateway

11.1.5.2. DNS Servers



Sends primary and secondary Dynamic Name Server IP addresses to DHCP clients. These servers are mandatory in almost every DHCP configuration.

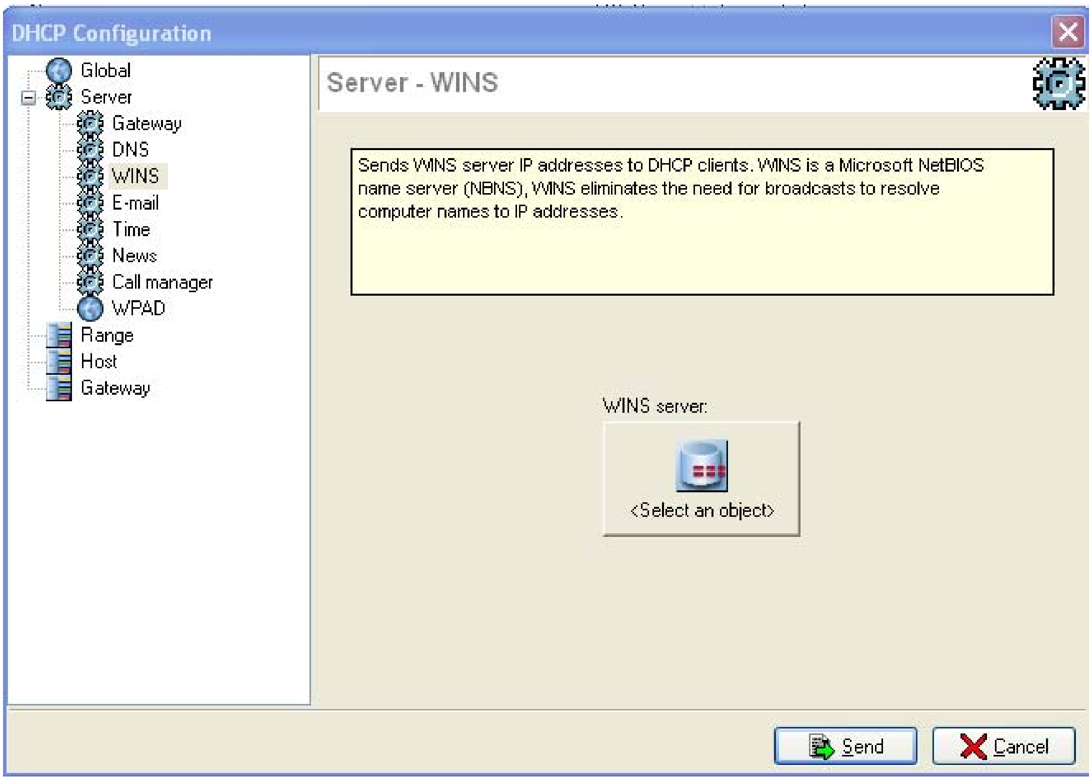
Primary DNS server:
<Select an object>

Secondary DNS server:
<Select an object>

Figure 325: Configuring the DHCP - Server - DNS

If the Firewall obtains the IP address of an interface via DHCP and the option “DNS Queries” has been configured, the DNS servers obtained by the Firewall from the access provider cannot be defined in the configuration of the DHCP service. In the configuration of objects, these servers are identified as the hosts “Firewall_<interface name>_dns1” and “Firewall_<interface name>_dns2”.

11.1.5.3. WINS



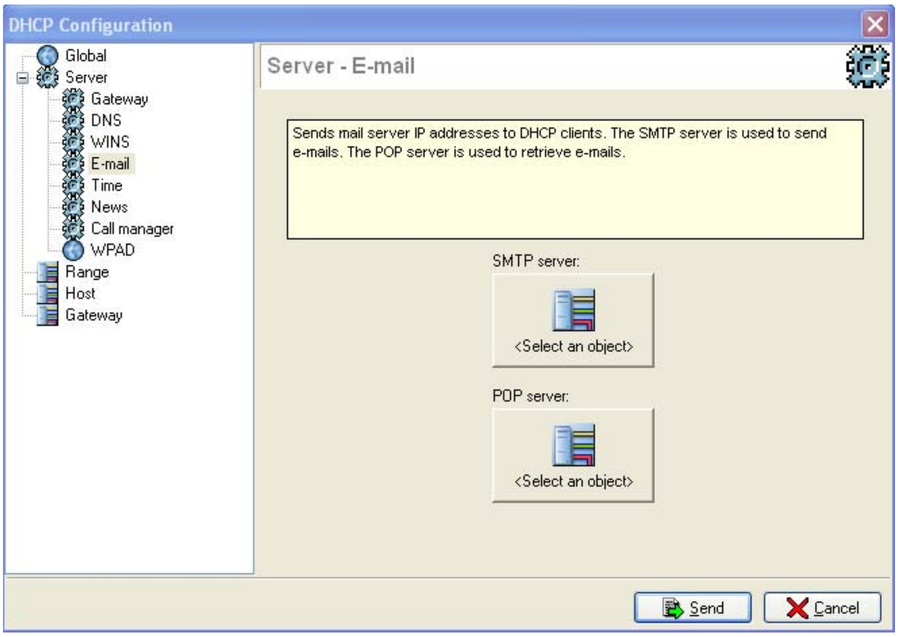
Sends WINS server IP addresses to DHCP clients. WINS is a Microsoft NetBIOS name server (NBNS), WINS eliminates the need for broadcasts to resolve computer names to IP addresses.

WINS server: <Select an object>

Figure 326: Configuring the DHCP - Server - WINS

Definition: WINS *(Windows Internet Naming Service)*
A name and service server for hosts that use NetBIOS.
It is also a database to which clients can send queries in order to find out a host’s IP address instead of sending broadcasts. This reduces the amount of traffic over the network.

11.1.5.4. E-mail

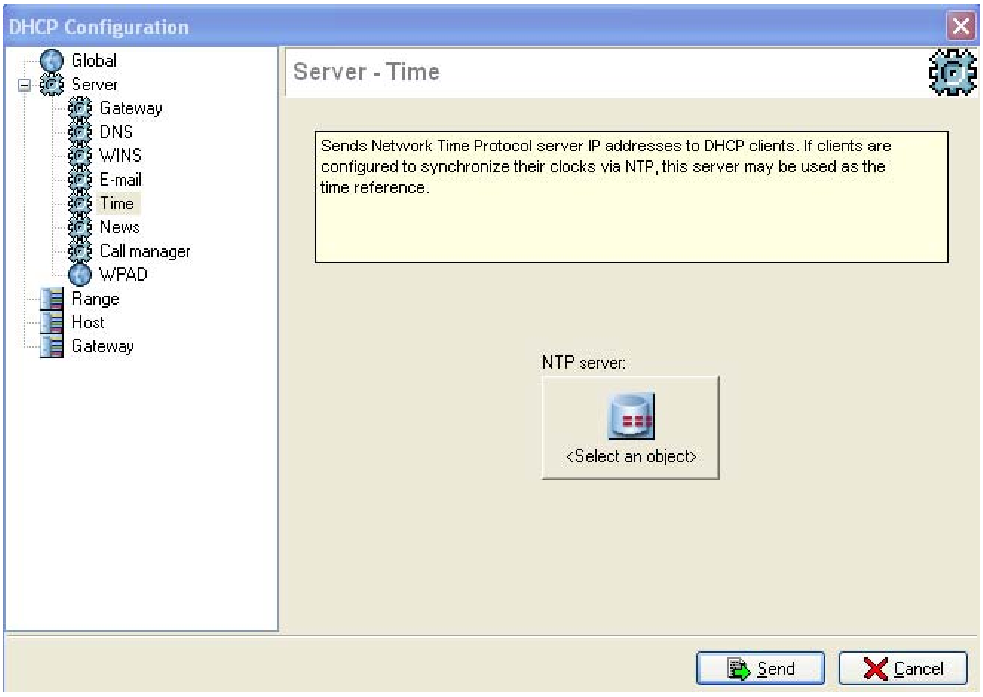


Sends mail server IP addresses to DHCP clients. The SMTP server is used to send e-mails. The POP server is used to retrieve e-mails.

Figure 327: Configuring the DHCP - Server - E-mail

This window allows sending the server's e-mail address to DHCP clients. The SMTP server is used for sending e-mails whereas the POP servers are used for receiving them. Objects are selected when you click on them.

11.1.5.5. Time (NTP)

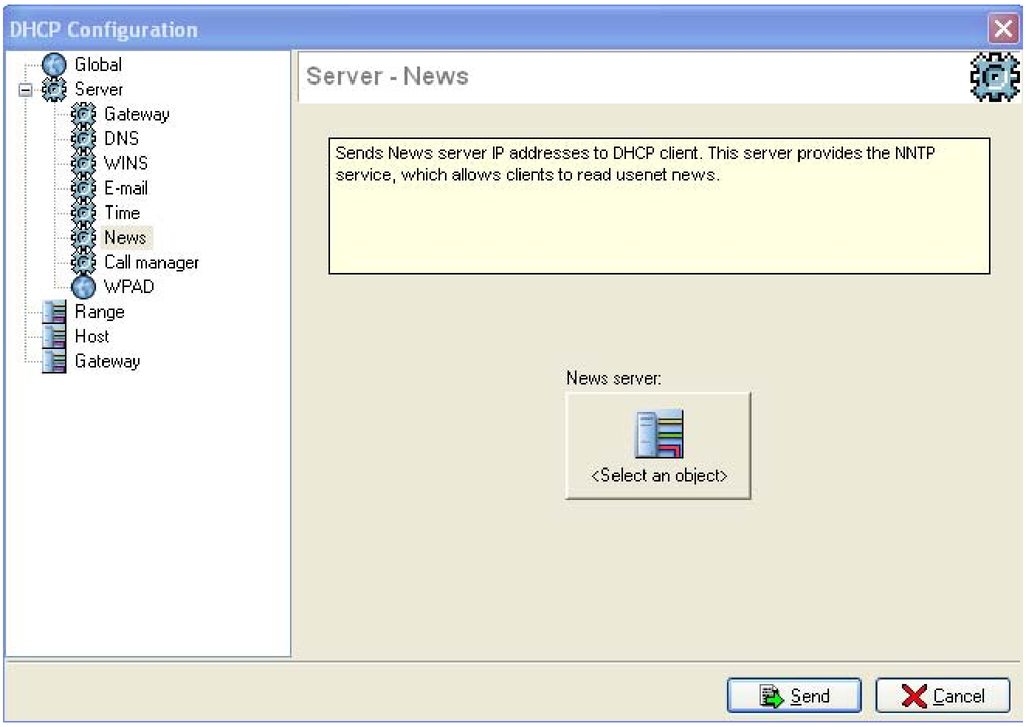


Sends Network Time Protocol server IP addresses to DHCP clients. If clients are configured to synchronize their clocks via NTP, this server may be used as the time reference.

Figure 328: Configuring the DHCP - Server – Time (NTP)

From this window, the NTP server's e-mail address can be sent to DHCP clients. If clients have been configured to synchronize their NTP clocks, this server has to be used as a time reference.

11.1.5.6. News



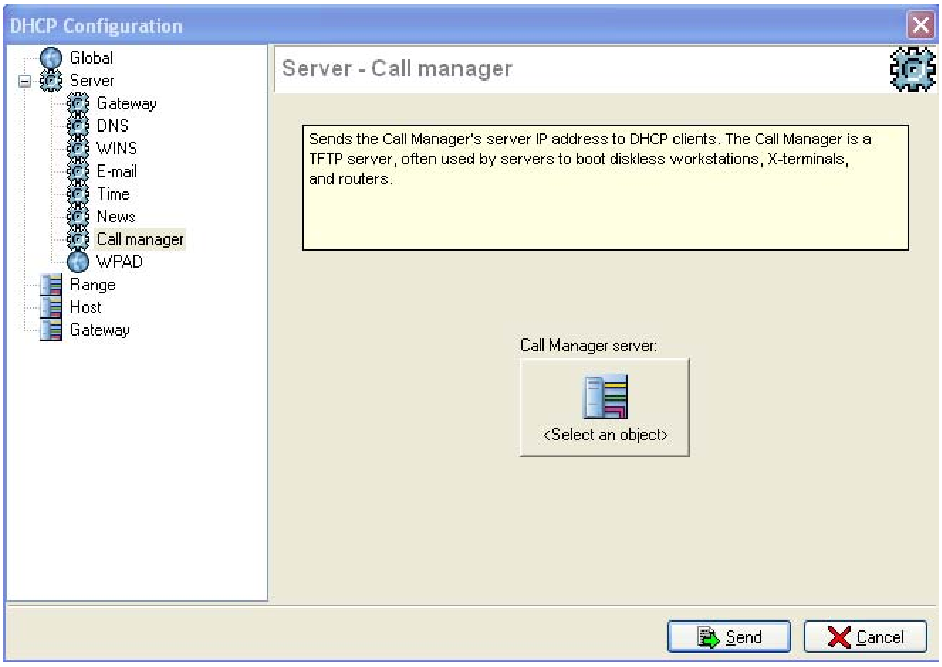
Sends News server IP addresses to DHCP client. This server provides the NNTP service, which allows clients to read usenet news.

Figure 329: Configuring the DHCP - Server - News

From this window, the news server's e-mail address can be sent to DHCP clients. This server provides the NNTP service, which allows clients to read Usenet news.

11.1.5.7. Call Manager

From this window, the Call Manager server's e-mail address can be sent to DHCP clients. The Call Manager server acts as a switch for telephones over IP and is also a TFTP server. It can therefore be used as such for starting up network equipment such as routers, X-terminals or workstations without hard disks.



Sends the Call Manager's server IP address to DHCP clients. The Call Manager is a TFTP server, often used by servers to boot diskless workstations, X-terminals, and routers.

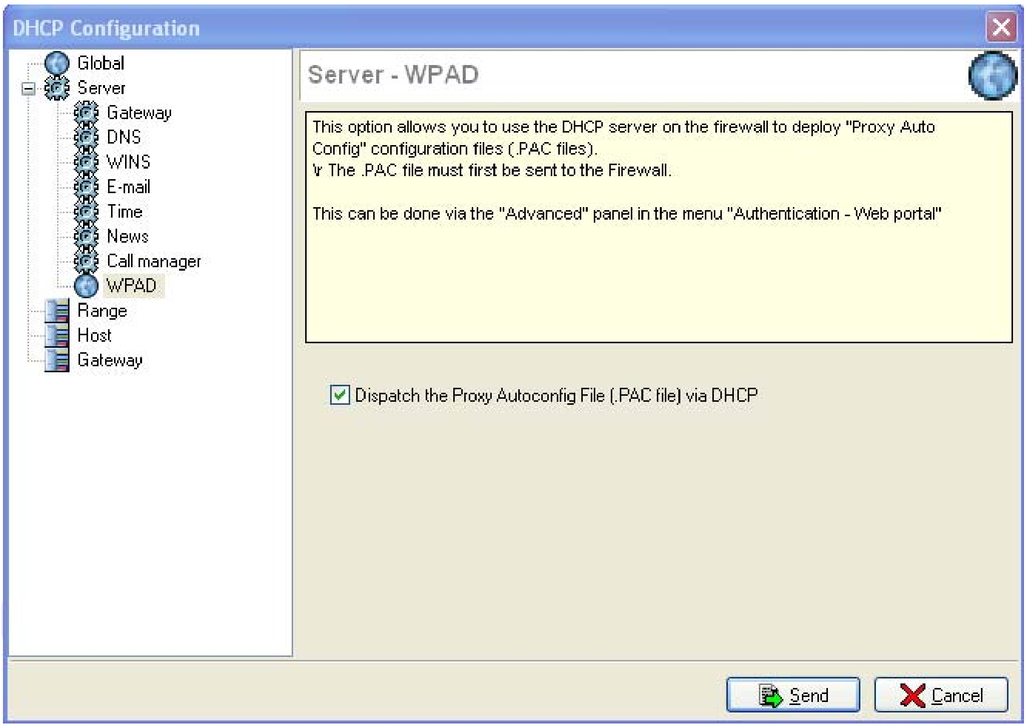
Call Manager server: <Select an object>

Figure 330: Server - Call manager

11.1.5.8. WPAD

DEFINITION
WPAD (Web Proxy Auto-Discovery) is a protocol that allows the automatic setup of the browser's internet access.

The following window will appear when the **WPAD** menu is selected:



This option allows you to use the DHCP server on the firewall to deploy "Proxy Auto Config" configuration files (.PAC files).
\r The .PAC file must first be sent to the Firewall.

This can be done via the "Advanced" panel in the menu "Authentication - Web portal"

☑ Dispatch the Proxy Autoconfig File (.PAC file) via DHCP

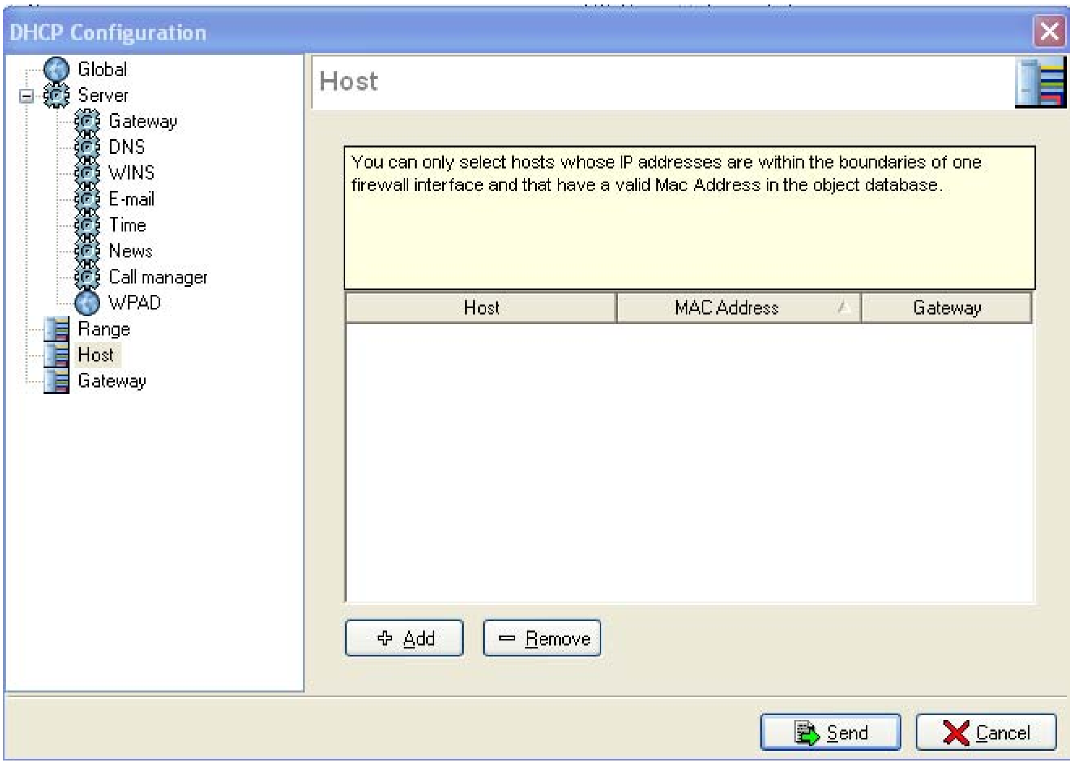
Figure 331: Configuring the DHCP – Server - WPAD

The option **Dispatch the Proxy Autoconfig File (.PAC file) via DHCP** allows the server to distribute the proxy configuration through a PAC file to DHCP clients that request an address.

The .PAC file is transmitted in the DHCP response (option field 252:WPAD-URL).

If this option is selected, the user will be told to enable the sharing of internal and/or external interfaces in the authentication window. Cf. Part 12: Authentication.

11.1.7. Host



You can only select hosts whose IP addresses are within the boundaries of one firewall interface and that have a valid Mac Address in the object database.

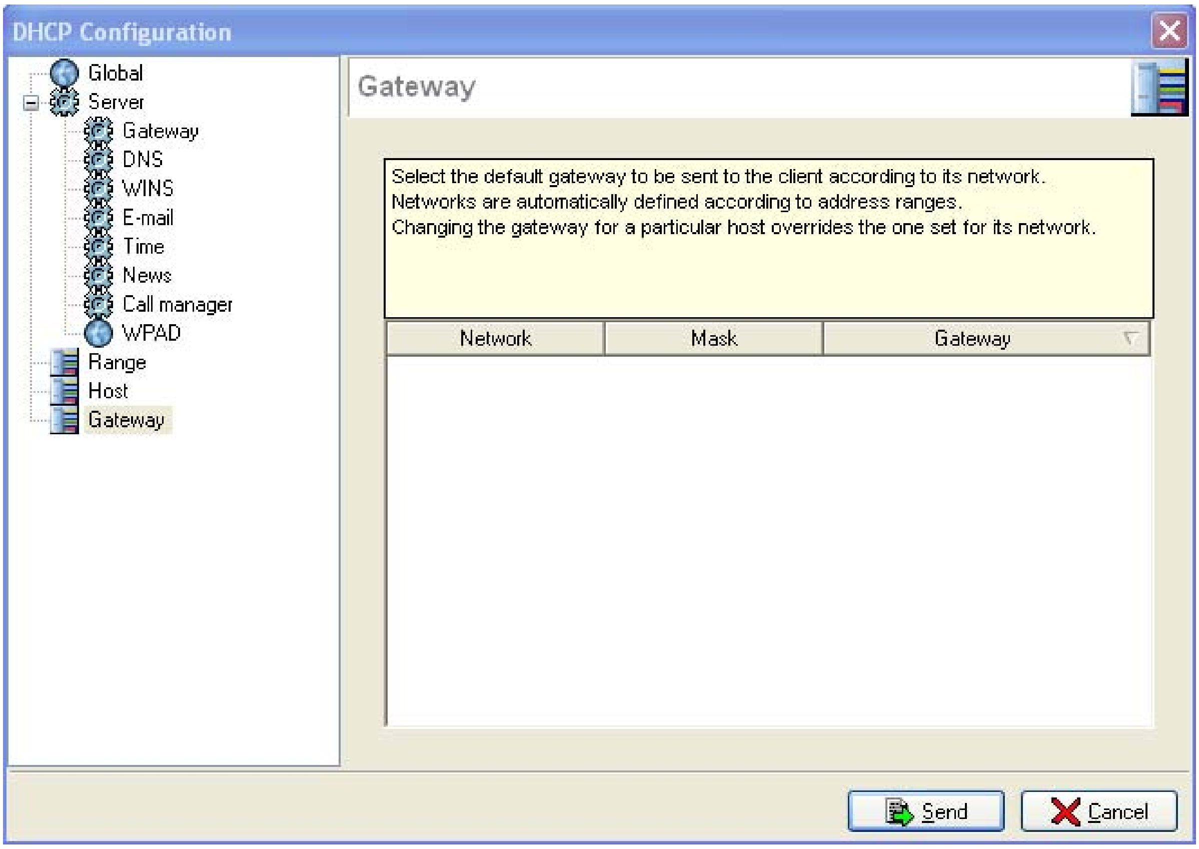
Host	MAC Address	Gateway

Figure 332: Configuring the DHCP - Host

In the **`Host`** menu, it is possible to define a specific IP address and default gateway for a client post having a given MAC address. This configuration is close to static addressing but nothing is indicated on the client post. As such, the management of allocated addresses and of client post configuration is simplified.

The table displays the host, MAC address and gateway.

11.1.8. Gateway



Select the default gateway to be sent to the client according to its network.
Networks are automatically defined according to address ranges.
Changing the gateway for a particular host overrides the one set for its network.

Network	Mask	Gateway

Figure 333: Configuring the DHCP – Gateway

This window determines the default gateway to be transmitted to the client according to his network. Networks are automatically determined according to the address range configuration. The gateway defined for a specific client will overwrite the gateway defined for his network.

CHAPTER 2. DNS

11.2.1. Introduction

In this section, we intend go back on a few principles of how DNS operates

DNS functions in client-server mode. The client part is called the *resolver*, which is a library. The server part is called the *name server*.

Three types of name servers exist:

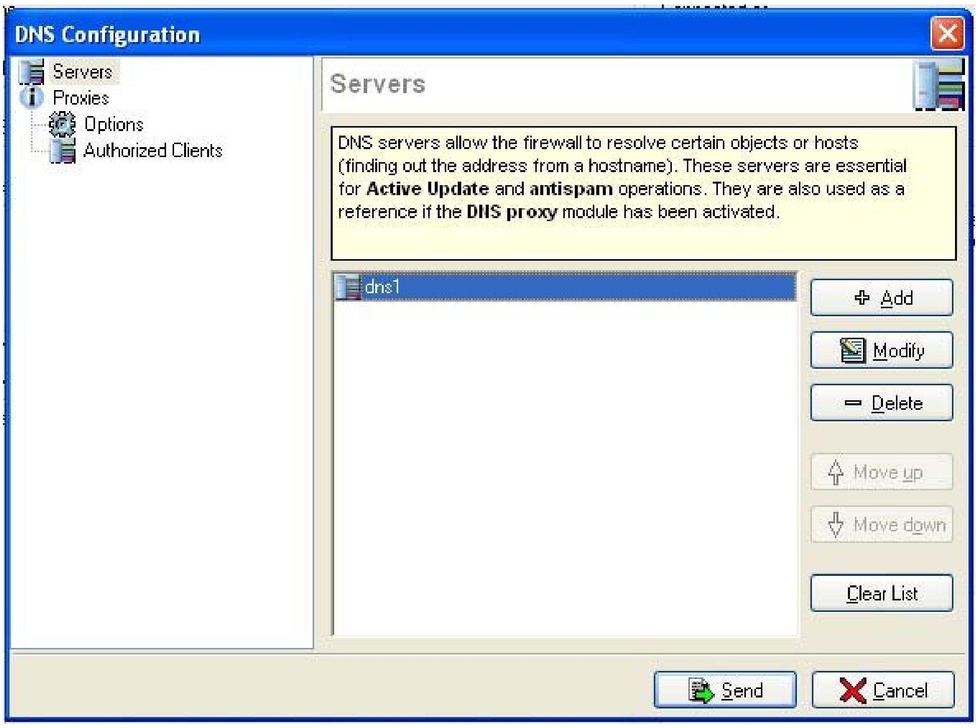
- **Primary**: possesses up-to-date tables on a domain.
- **Secondary**: possesses tables from another server.
- **Cache**: possesses tables formed from processed information.

11.2.2. Using the NETASQ UTM Firewall's DNS service

NETASQ's DNS service is a cache. A DNS request is sent through the Firewall, the Firewall stores (in the **DNS** cache) the response and this guarantees better response time during the next similar DNS request. Furthermore, the Firewall intercepts and receives the requests, thereby ensuring optimal security.

11.2.3. Operation

➲ The DNS service has to be activated in order to be used, via the menu **`Services\DNS`**.



DNS servers allow the firewall to resolve certain objects or hosts (finding out the address from a hostname). These servers are essential for **Active Update** and **antispam** operations. They are also used as a reference if the **DNS proxy** module has been activated.

Figure 334: Configuring the DNS - Servers

The **DNS** service configuration screen consists of two sections:

- On the left, a directory displaying the various features of the **DNS** service menu
- On the right, the options that can be configured

The **DNS** service proposed by the NETASQ Firewall is a **DNS** cache, which serves to store **DNS** responses matching domain names and IP addresses.

11.2.4. Servers

Servers enable the Firewall to resolve (find out a host's IP address from its name) certain objects or hosts. These servers are essential for Active Update and Antispam to function and are also used as a reference if the DNS proxy has been activated.

When servers are configured, antispam, antivirus and object resolution modules send their queries to these servers without necessarily activating the Firewall's DNS proxy (DNS cache). In this case, if a user sends a DNS request on an unconfigured server, the Firewall will transmit the request to the said server and the user sending a DNS query to the Firewall will see his query being refused.

If the option **Enable DNS** has been selected in the **`Proxies`** menu, antispam, antivirus and object resolution modules will send their queries to configured servers without having to consult the DNS cache. If a user sends a DNS query to an unconfigured server, the Firewall will transmit the query to the said server, and when a user sends a DNS query to the Firewall, the DNS cache will treat his query.

Finally, if the DNS proxy has been activated and the transparent mode configured (see transparent mode configuration above) antispam, antivirus and object resolution modules send their queries to configured servers using the DNS cache. If a user sends a DNS query to an unconfigured server, the Firewall will transparently redirect the query to the configured servers in this module, and when a user sends a DNS query to the Firewall, the DNS cache will treat his query.

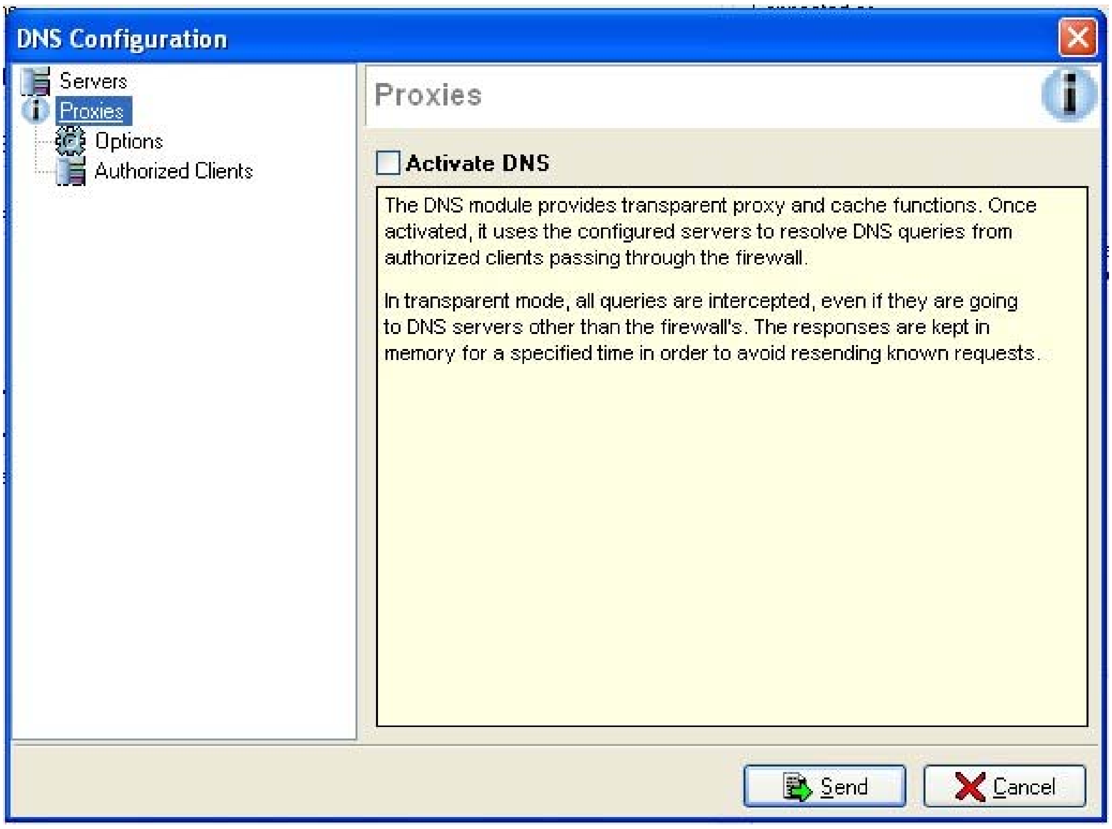
11.2.4.1. Action bar

Add	Adds a DNS server. The objects database will appear so that Hosts, Address Ranges and Groups can be selected.
Edit	Modifies the selected DNS server.
Delete	Removes the selected DNS server.
Move up	Places the selected row before the row directly above it.
Move down	Places the selected row after the row directly below it.
Clear list	Deletes the whole list of servers.

11.2.5. Proxies

The DNS module offers cache and transparent proxy functions. Once it is enabled, DNS queries from authorized clients passing through the firewall will be resolved by the module, using the configured servers.

In transparent mode, all queries will be intercepted, even if they are headed to DNS servers other than the firewall. Responses are kept in memory for a certain period in order to avoid re-sending requests that have already been sent.

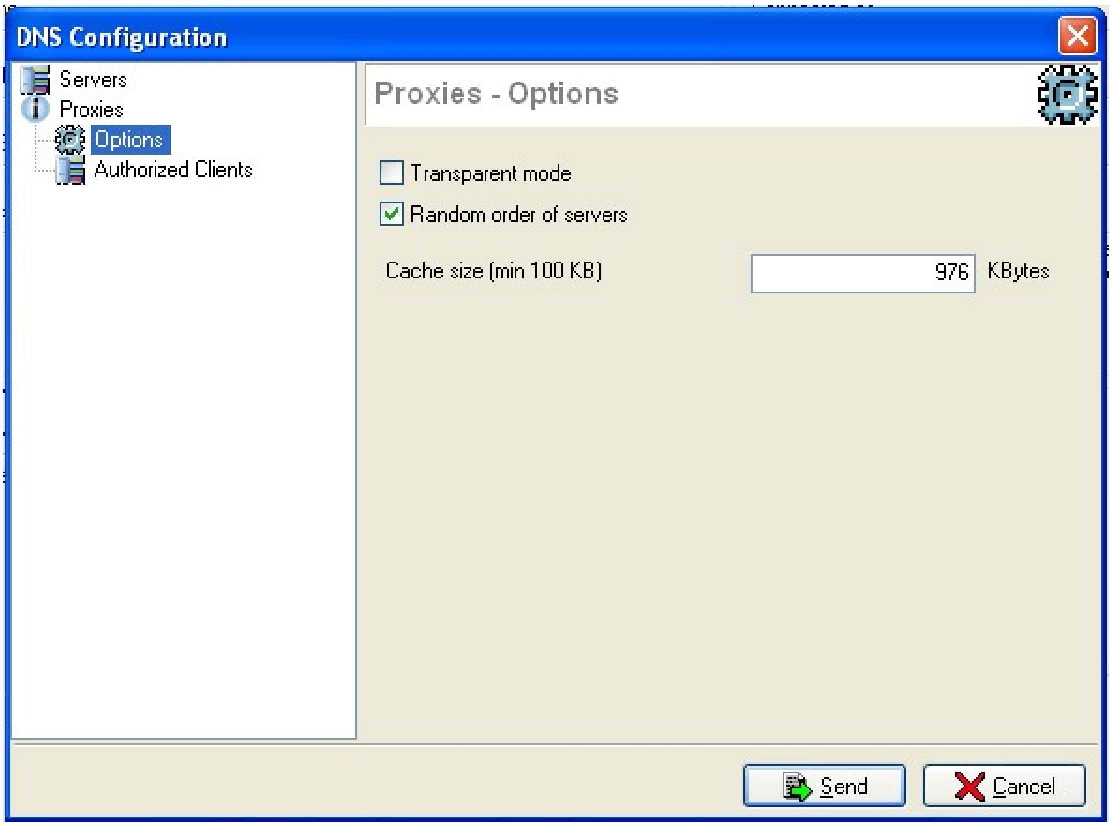


□ Activate DNS

The DNS module provides transparent proxy and cache functions. Once activated, it uses the configured servers to resolve DNS queries from authorized clients passing through the firewall.

In transparent mode, all queries are intercepted, even if they are going to DNS servers other than the firewall's. The responses are kept in memory for a specified time in order to avoid resending known requests.

Figure 335: Configuring the DNS - Proxies



□ Transparent mode

☑ Random order of servers

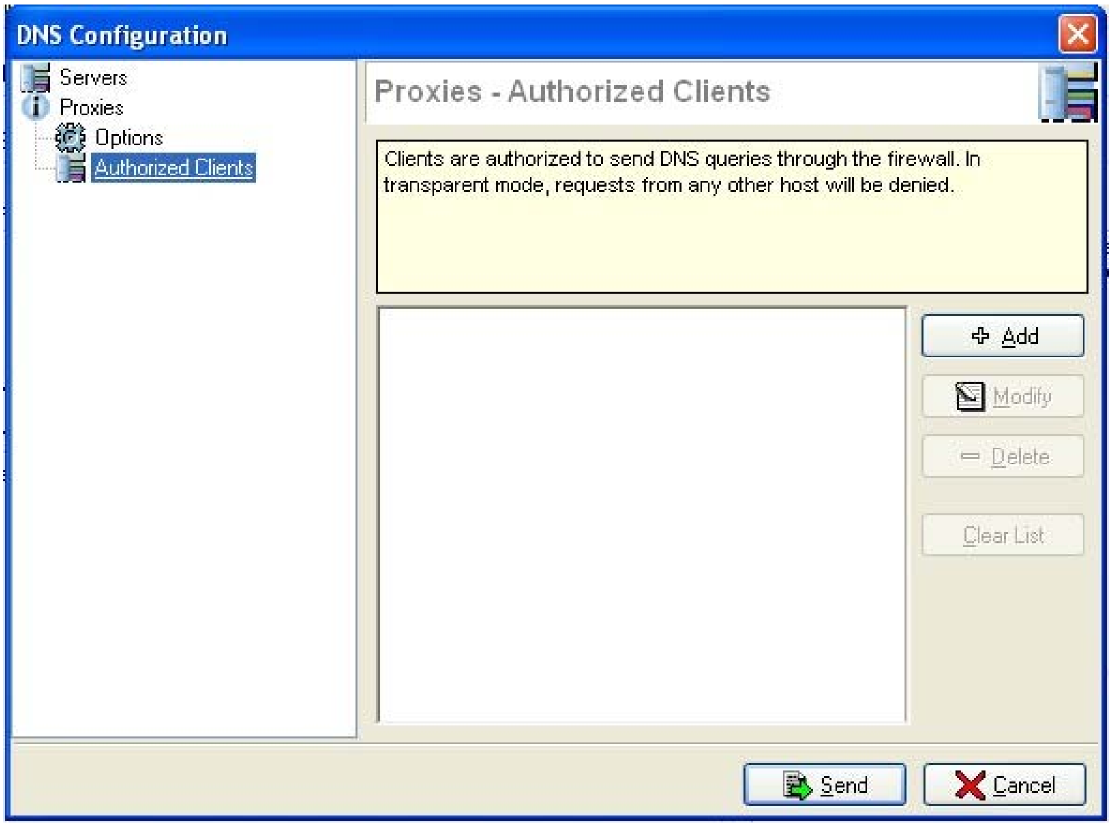
Cache size (min 100 KB) 976 KBytes

Figure 336: Configuring the DNS - Proxies - Options

11.2.5.1. Options

Transparent mode	As its name implies, this option aims at making the NETASQ Firewall DNS service transparent. As such, when this option is activated, the redirection of DNS flows to the DNS cache will be invisible to users who think they are accessing their DNS server.
Random order of servers	Allows the firewall to select a DNS server at random from the list.
Cache size (min 100 KB)	Size allocated to the DNS cache

11.2.5.2. Authorized clients



Clients are authorized to send DNS queries through the firewall. In transparent mode, requests from any other host will be denied.

Figure 337: Configuring the DNS – Authorized clients

Authorized Clients: List of clients authorized to send DNS requests. This list may contain networks. In transparent mode, requests from any other machines will not be treated.

CHAPTER 3. NTP

11.3.1. Introduction

This protocol allows synchronizing clients' and servers' real-time clock. NTP is based on UDP, which makes it an unconnected protocol. In fact, it is an upgraded version of Time Protocol and ICMP Timestamp Message protocols and an appropriate replacement.

NTP provides time synchronization mechanisms with a nanosecond precision, while preserving an unambiguous date. This protocol includes the possibility of specifying information on the precision and error estimated in the local clock as well as indications on the reference clock with which it can synchronize.

11.3.2. Using the NETASQ Firewall's NTP service

NTP is based on a hierarchical structure in which the firewall is only a client.

11.3.3. Operation

➲ The NTP service has to be activated in order to be used, via the menu **`Services\NTP`**.

> **REMARK**
> The other elements in the window will be enabled or disabled depending on whether NTP has been enabled.

The NTP service configuration window comprises two sections:

- The **`Servers`** tab: list of public or private NTP servers.
- The **`Keys`** tab: list of authentication keys.

> **REMARK**
> A star will appear in the window's title bar when changes are made to the configuration to information the user that data may have been changed.

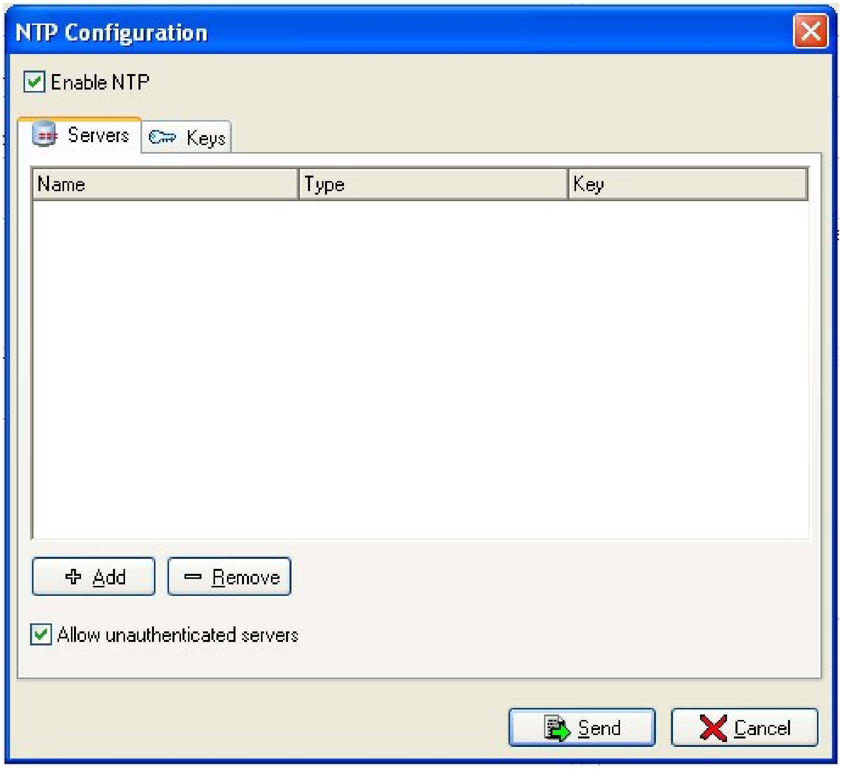
11.3.4. Servers

This window allows adding, editing or deleting NTP servers and allows assigning keys to them if necessary.

It comprises 3 columns: the object name, type (host, address range or group) and the associated key where applicable (with an indication of "none" or a number between 1 and 15, or "invalid" if the associated key no longer exists).

Authentication keys can be selected in this window, or deleted by selecting "None" in the drop-down list.

A key cannot be used more than once in the table.



NTP Configuration

☑ Enable NTP

Name	Type	Key

☑ Allow unauthenticated servers

Figure 338: Configuring the NTP - Servers

Servers	List of public or private NTP servers to which the Firewall can connect to synchronize.
Add	Accesses the objects database in order to select servers.
Demove	Deletes a selected server from the table.
Allow unauthenticated servers	This option allows you to authorize the use of servers which do not request authentication (i.e., with no associated keys).

11.3.5. Keys

This tab allows you to configure keys for authentication with NTP servers. This key is visible if you connect with modification rights, otherwise it is masked.

Keys are defined by a number ranging from 1 to 15. Any attempt to add a sixteenth key will cause an error message to appear.

Keys can be modified directly in the table. However, if the key key is longer than 8 characters, an erro message will appear. The number of the key can also be modified. In this case, only numbers that have not yet been assigned will be suggested.

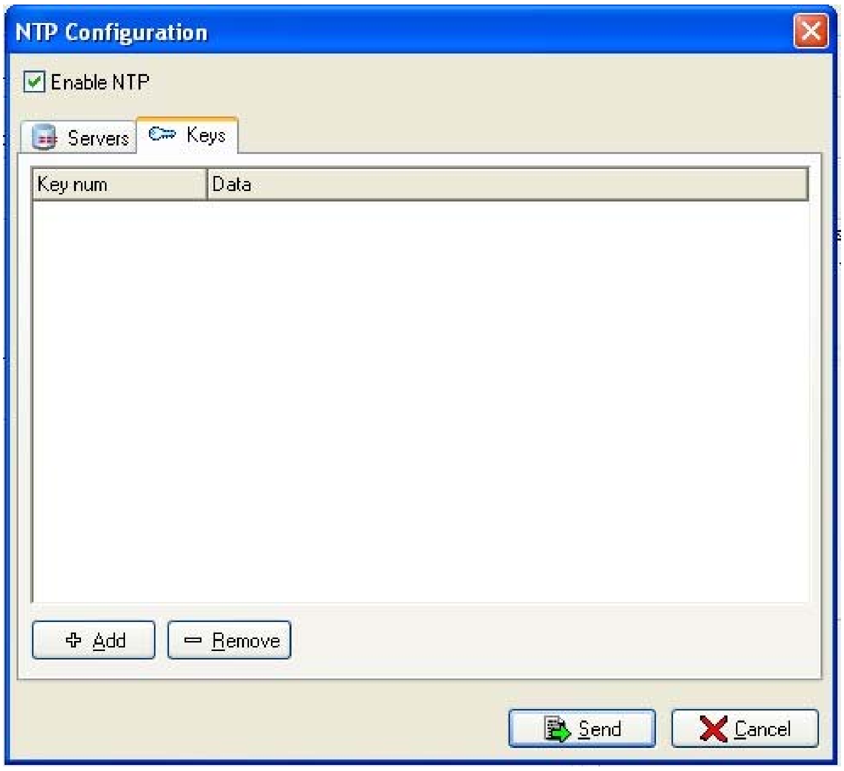
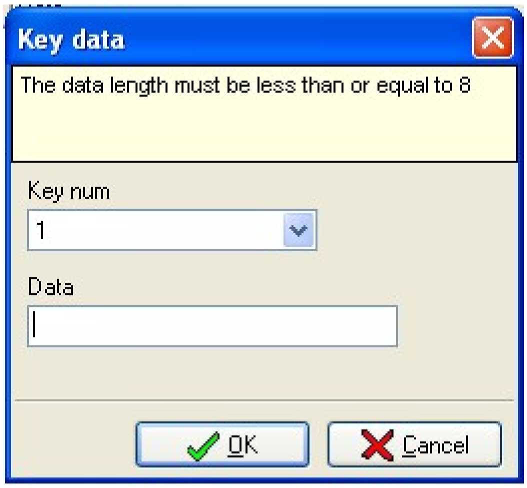


Figure 339: Configuring the NTP – Keys

Add	The following cindow appears when you click on this button:



The data length must be less than or equal to 8

Figure 340: Key data

Indicate a number for the key then indicate a value in the “Data” field.

REMARK

The length of the data has to be 8 or less.

Delete	Deletes a selected key from the table.

11.3.5.1. Sending

By clicking on **Send**, data will be checked and sent.

The checking stage allows determining whether the keys associated with each server actually exist. If they do not, an error message will appear and sending will be aborted.

If the option "Allow unauthenticated servers" has not been selected, an error message will appear if there are servers that do not have associated keys.

Enabled NTP configurations cannot be sent if no servers have been indicated.

If the checking procedure runs smoothly, the configuration can be sent.

CHAPTER 4. SNMP

11.4.1. Introduction

Management of a network is ensured by applications which monitor and supervise the status of different network elements. These elements may be workstations, servers, or gateways containing management agents required by these management applications. The agents generate management information which is used by the applications. SNMP is used for communication between agents and applications.

SNMP uses UDP; as a consequence, packets exchanged between the management station (client) and the agent (server) on the network element are datagrams with no delivery guarantee.

Two types of client-server exchanges exist:

- Either the client sends a request and the server responds; or
- The server takes the initiative by sending messages (trap) to the management station to indicate that an important event has occurred.

The agent (server) listens on the UDP port 161 and the management station listens to the traps on port 162.

11.4.2. Using the NETASQ Firewall's SNMP service

The NETASQ Firewall's SNMP service is a server which allows you to monitor the Firewall's status. Therefore the Firewall can be integrated into a network management solution such as Tivoli or HP OpenView.

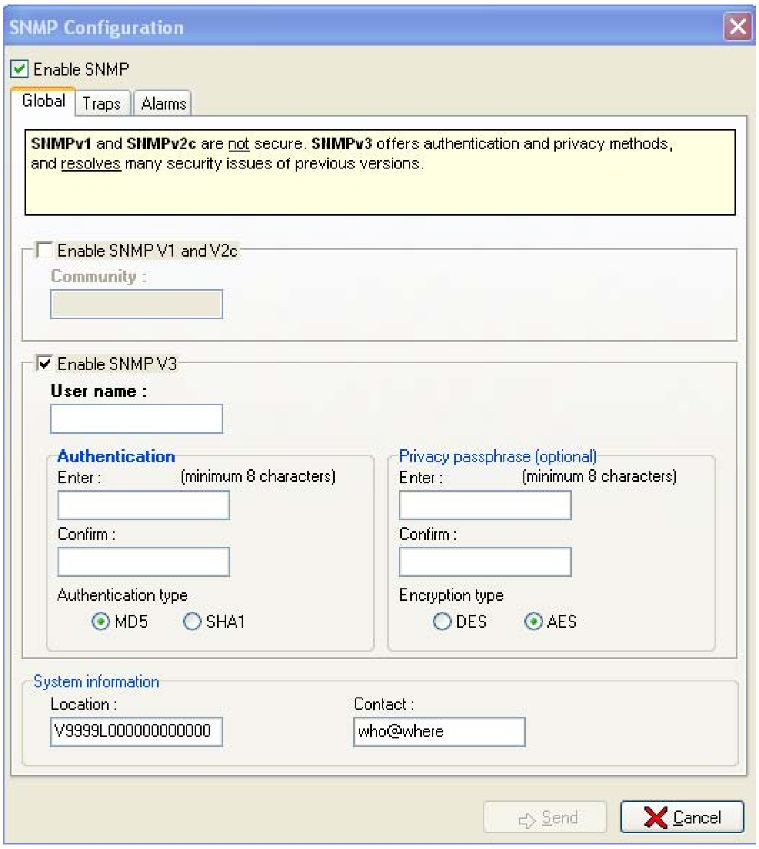
11.4.3. Operation

➲ The SNMP service has to be activated in order to be used, via the menu **`Services\SNMP`**.

The SNMP service configuration window comprises two sections:

- The **Global** tab: this window allows you to specify the SNMP version used and information relating to each version,
- The **Events** tab: in this tab, you can specify the hosts to which information generated by the Firewall has to be sent.
- The Alarms (Traps)tab: enables defining the type (System/ASQ) of alarms monitored according to their severity.

11.4.4. Global



SNMPv1 and **SNMPv2c** are not secure. **SNMPv3** offers authentication and privacy methods, and resolves many security issues of previous versions.

Location : V9999L000000000000

Contact : who@where

Figure 341: Configuring the SNMP - Global

SNMP functions in two “modes”. Either a management station seeks information from the network element, or the network element generates this management information to a specified station.

In this tab, you can configure the information necessary for the establishment of a connection between the Firewall and the management station when the latter tries to obtain management data.

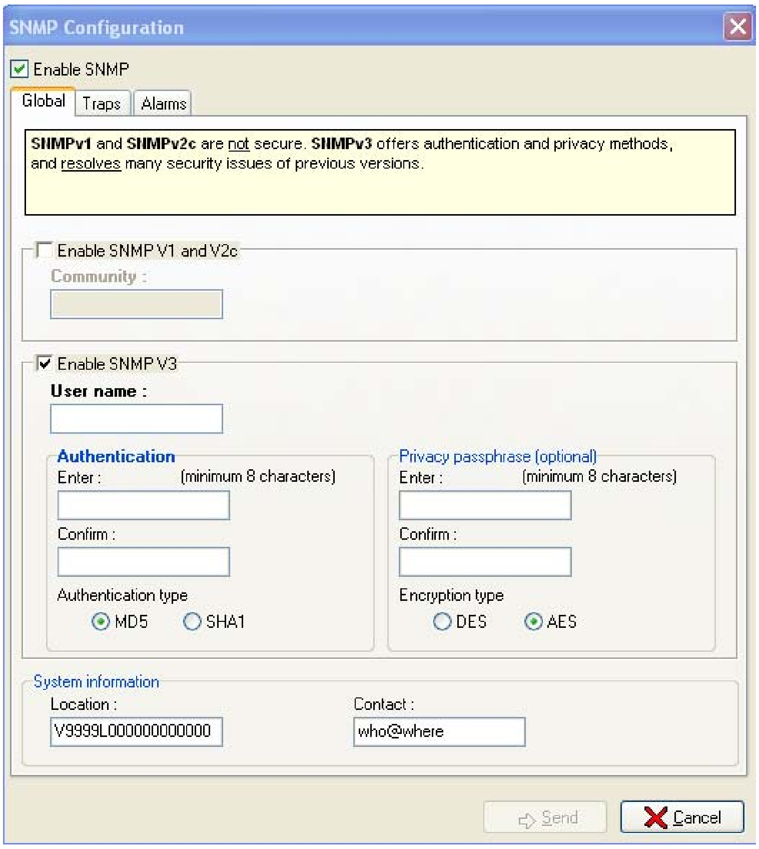
WARNING
SNMPv1 and SNMPv2c are not secure.

11.4.4.1. Activating SNMP V1 and V2c

The earliest versions of **SNMP** are not safe, as the only field necessary is the community name. By default, the RFC offers the name “public”.

WARNING
For security reasons, we recommend that you do not use it.

If you wish to enter several communities, separate them with commas as shown below:



☑ Enable SNMP

SNMPv1 and **SNMPv2c** are not secure. **SNMPv3** offers authentication and privacy methods, and resolves many security issues of previous versions.

☐ Enable SNMP V1 and V2c
Community :

☑ Enable SNMP V3
User name :

Authentication
Enter : (minimum 8 characters)
Confirm :
Authentication type ● MD5 ○ SHA1

Privacy passphrase (optional)
Enter : (minimum 8 characters)
Confirm :
Encryption type ○ DES ● AES

System information
Location : V9999L000000000000
Contact : who@where

Figure 342: Configuring the SNMP - Global

11.4.4.2. Activating SNMP V3

Since December 2002, a new standard has been introduced for SNMP, providing a significant advance in security.

SNMPv3 offers authentication and encryption methods and resolves certain security issues from earlier versions. The following parameters are required for configuration:

User name	User name used for the connection
Authentication type	Two types of authentication are available: MD5 (hash algorithm that calculates a 128-bit digest) and SHA1 (hash algorithm that calculates a 160-bit digest).
Authentication	User's password
Encryption (optional)	SNMP packets are encrypted in DES, you may define an encryption key. By default, the authentication key is used. **WARNING** You are highly advised to use a specific key.

DEFINITION: ENCRYPTION
Encryption comes in two forms: symmetrical encryption and asymmetrical encryption.
- A symmetrical encryption system uses the same key to encrypt and decrypt.
- An asymmetrical encryption system uses different keys – a public key to encrypt and a private key to decrypt.

The best known encryption methods are DES and AES.
DES is a method that uses 56-bit keys. Usually, Triple DES is used.
AES is a symmetrical encryption algorithm, whose key can be either 128, 192 or 26 bits.

11.4.4.3. System information

Location	The serial number or any other information describing the physical location of the equipment
Contact	E-mail address of the administrator to contact when a problem arises.

11.4.5. Traps

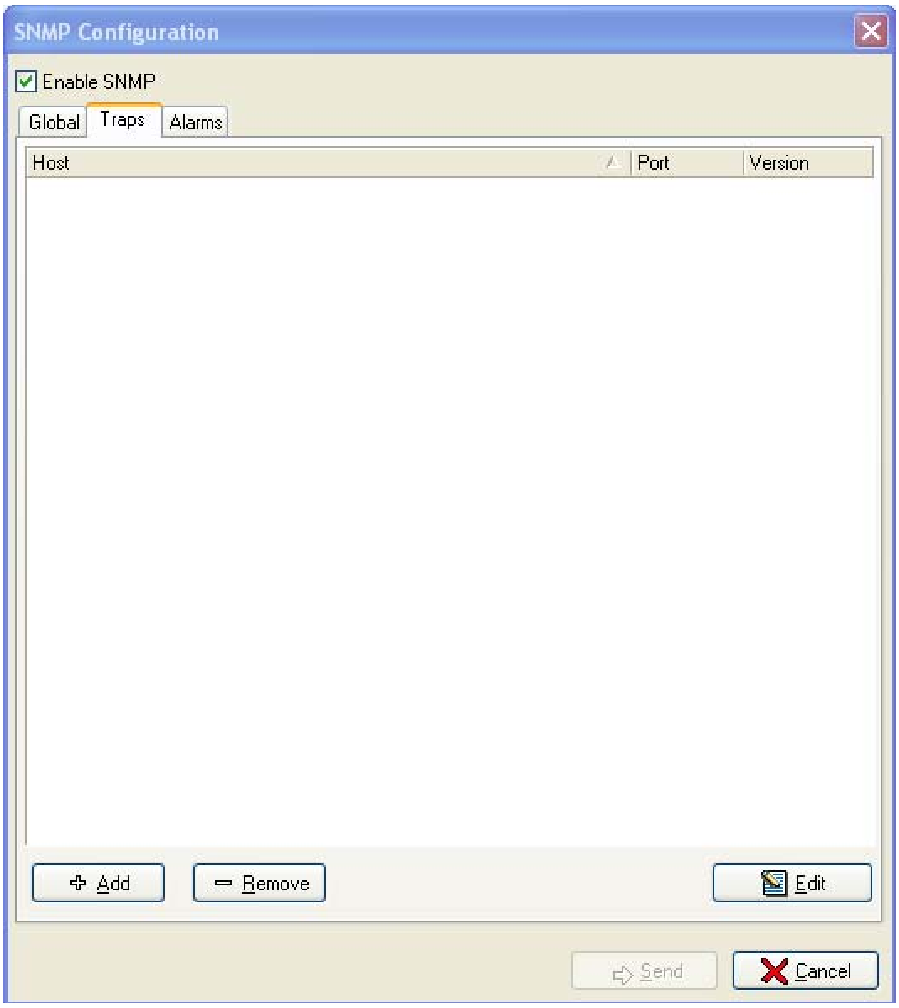


Figure 343: Configuring the SNMP - Traps

In this tab, you can configure the stations that the Firewall must contact when it attempts to send an SNMP Trap. If no station (host) has been specified, the Firewall will not send any message.

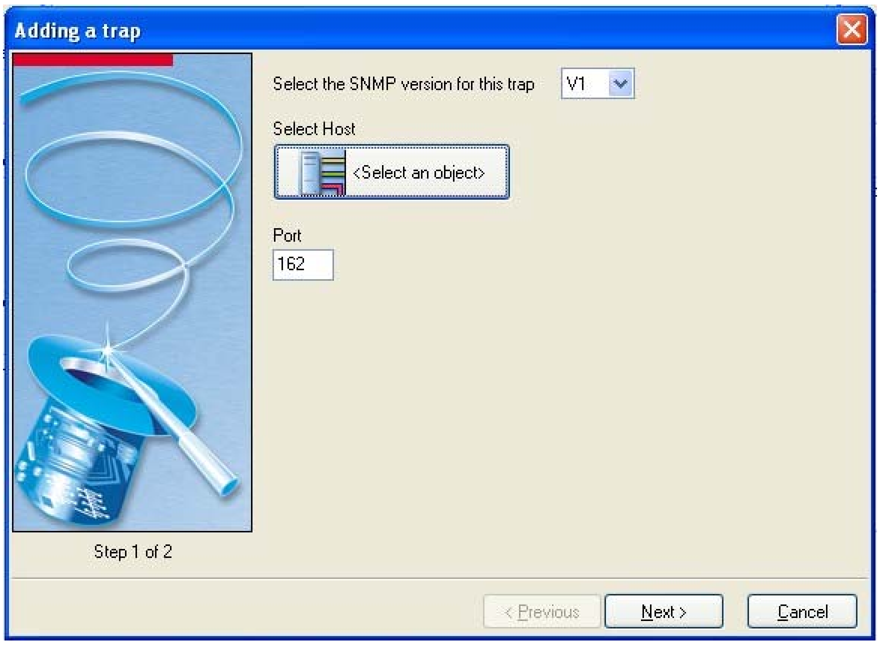
By activating the option **Enable authentication error trap**, you will be able to receive information regarding authentication errors.

A Wizard will guide you in the configuration of hosts.

Configuring a host in the Wizard takes place in the same manner as for the Global tab. Selecting an SNMP version will determine the configuration type to carry out.

The button **Edit** will allow you to modify information regarding a host once it has been created.

Step 1


Adding a trap

Select the SNMP version for this trap: V1

Select Host: <Select an object>

Port: 162

Step 1 of 2

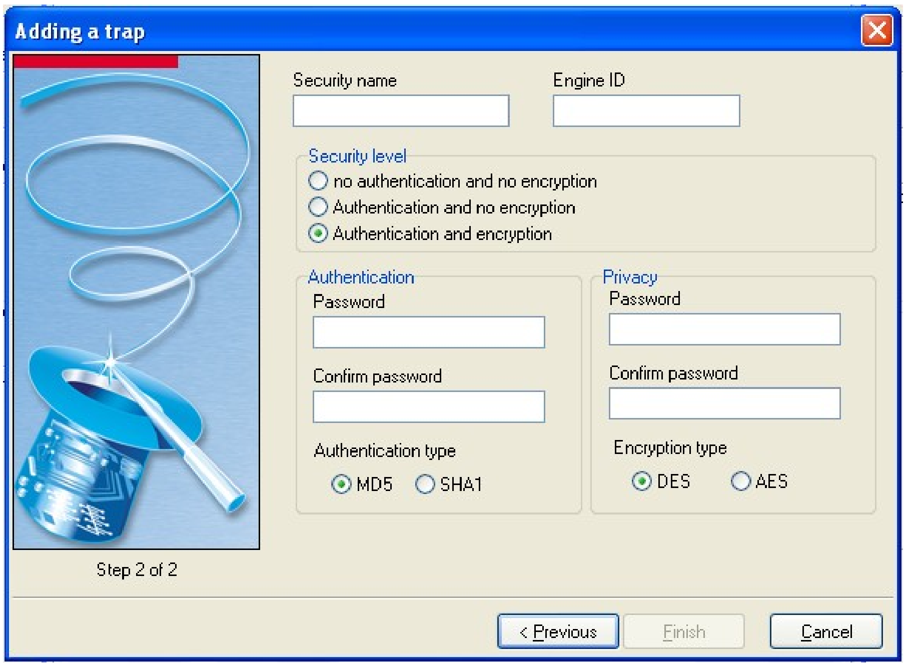
Figure 344: Adding a trap (event) - Step 1

Select the SNMP version from 3 possible options - V1, V2c and V3.
By clicking on **Select an object**, the objects database will appear.

Step 2
- When you select SNMP V1 or V2c

Only a community name is necessary.

- When you select SNMP V3:



Adding a trap

Security name

Engine ID

Security level
○ no authentication and no encryption
○ Authentication and no encryption
● Authentication and encryption

Authentication
Password

Confirm password

Authentication type
● MD5 ○ SHA1

Privacy
Password

Confirm password

Encryption type
● DES ○ AES

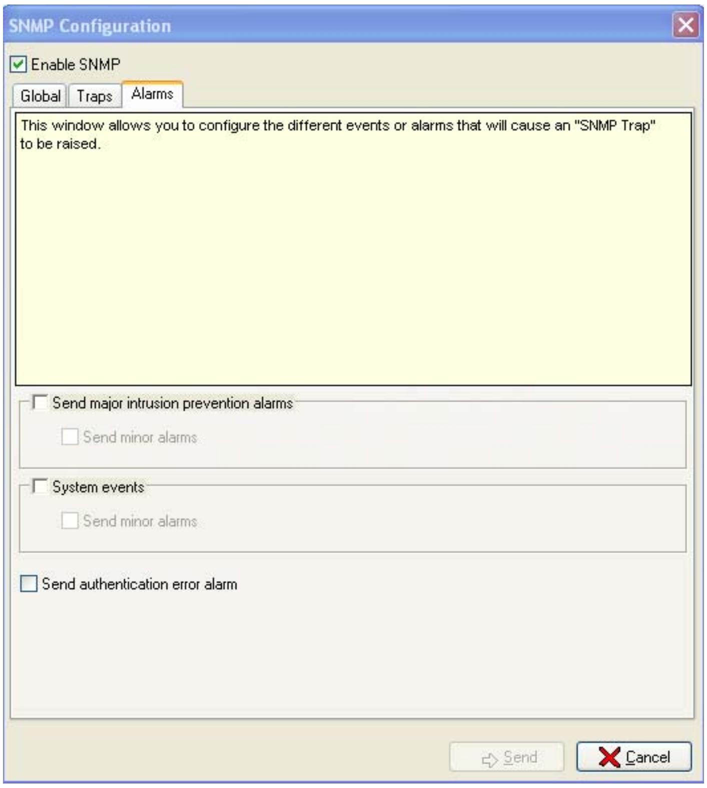
Step 2 of 2

Figure 345: Adding a trap (event) - Step 2

The parameters for configuring SNMP V3 events are as follows:

Security name	Name of the user authorized to send a trap on the management station.
Engine ID	0x0011223344 hexadecimal string (with or without the 0x in front) created by the management station to identify the user. From version 8.0 onwards, the Engine ID has to be at least 5 bytes and at most 32 bytes.
Security Level	Different security levels are available for the SNMP version: ● **No authentication and encryption**: no security ● **Authentication and no encryption**: authentication without trap encryption ● **Authentication and encryption**: if the encryption password field is left blank, the authentication password will be used for encryption.
Authentication password	User password
Encryption password	SNMP packets are encrypted in DES, you may define an encryption key. By default, the authentication key is used. **WARNING** You are highly advised to use a specific key.
Authentication type	Two types of authentication are available: MD5 and SHA1.
Encryption type	Two types of encryption are available: DES and AES.

11.4.6. Alarms (Traps)



This window allows you to configure the different events or alarms that will cause an "SNMP Trap" to be raised.

□ Send major intrusion prevention alarms
□ Send minor alarms
□ System events
□ Send minor alarms
□ Send authentication error alarm
Send
Cancel

Figure 346: Configuring the SNMP - Alarms

Send major intrusion prevention alarms	If this option is selected, you can receive major ASQ alarms. If you also select the option **Send minor alarms**, minor ASQ alarms will also be sent (via traps and/or MIB lookups).
System events	If this option is selected, you can receive major System alarms. If you also select the option **Send minor alarms**, minor System alarms will also be sent (via traps and/or MIB lookups).
Send authentication error alarms	This option allows the system to send traps in the event of an authentication failure (attempt to access the SNMP service with the wrong community (V1/V2c/wrong authentication in V3).

PART 12: AUTHENTICATION

12.1.1. Introduction

Identification/authentication functions allow a user to indicate his login (identification) and to verify that the user is really the person he claims to be by providing elements which only this user is supposed to be capable of providing (authentication). When authentication is successful, the user's login will be assigned, through a table of authenticated users, to the host from which he has identified himself and associated to all IP packets originating from it, for a period specified by the user. The user can also manually remove himself from the table of authenticated users before the expiry of this period.

12.1.1.1 For this section, you will need to have completed these steps

- Part 2: Installation, pre-configuration, integration.
- Part 5/Chapter 2: Interfaces, Part 4: Objects and kernel configuration.

12.1.1.2 For this section, you need to know

- Information regarding each user (name, surname, email ...)

12.1.1.3 Purpose of this section

This part will explain how to configure the user database, how to create the certification authority for generating digital certificates and how to choose the authentication method that will be used by internal users.

Authentication is based on a **LDAP** database (***Lightweight Directory Access Protocol***) on which are stored user files and possibly, digital certificates. An LDAP database is embedded on each Firewall but you can use an external LDAP database. As such, you will be able to centralize your user records on one external LDAP database and several Firewalls will be able to use the same database. NETASQ Firewalls support authentication via external RADIUS, Kerberos or NTLM servers.

NETASQ also supports the use of SRP for authenticating users. This protocol, which does not reveal passwords, resists passive listening attacks just as well as active attacks based on modifying or inserting packets in the authentication sequence. It uses a reusable password that the user provides, and remains resistant to attacks even if the password becomes less random.

In real terms, the Firewall, with its HTTP server capacities, provides web enrolment forms which allow it to identify itself, to authenticate specifying the session duration and to close the session manually. The HTTP session does not have to last for the session to remain active. A JAVA applet downloaded from the Firewall to the user workstations performs the different stages of SRP. This applet acts as the password that the user provides to carry the steps in SRP. Thanks to this enrolment, the administrator's task is simplified as these are users who request the creation of their access accounts (to the internet, mail server, all services which require authentication according to your filter policy) by providing themselves information concerning them.

12.1.2. Captive portal

Before activating authentication, you must already have configured the LDAP database (see LDAP Database configuration) via the menu **`Authentication\Captive portal.`**

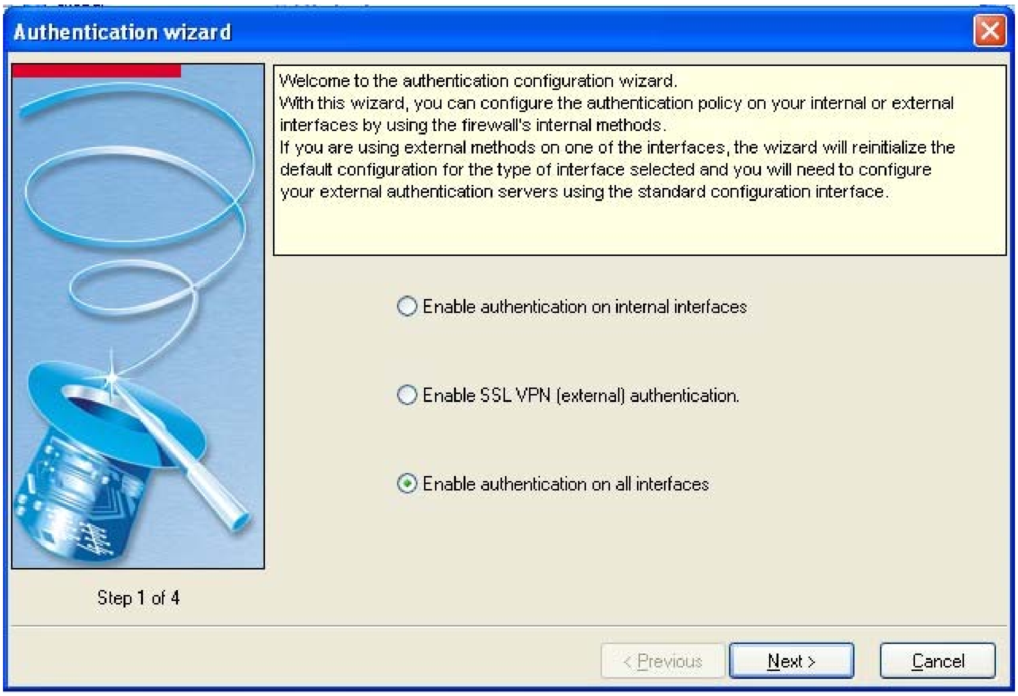
The authentication configuration window comprises three sections:

- On the left, a directory of the various features in the authentication configuration menu.
- On the right, the options that can be configured.
- Action buttons at the bottom of the screen.

12.1.2.1. Action buttons

Authentication configuration wizard button

1 Step 1: Welcome



Authentication wizard

Welcome to the authentication configuration wizard.
With this wizard, you can configure the authentication policy on your internal or external interfaces by using the firewall's internal methods.
If you are using external methods on one of the interfaces, the wizard will reinitialize the default configuration for the type of interface selected and you will need to configure your external authentication servers using the standard configuration interface.

○ Enable authentication on internal interfaces

○ Enable SSL VPN (external) authentication.

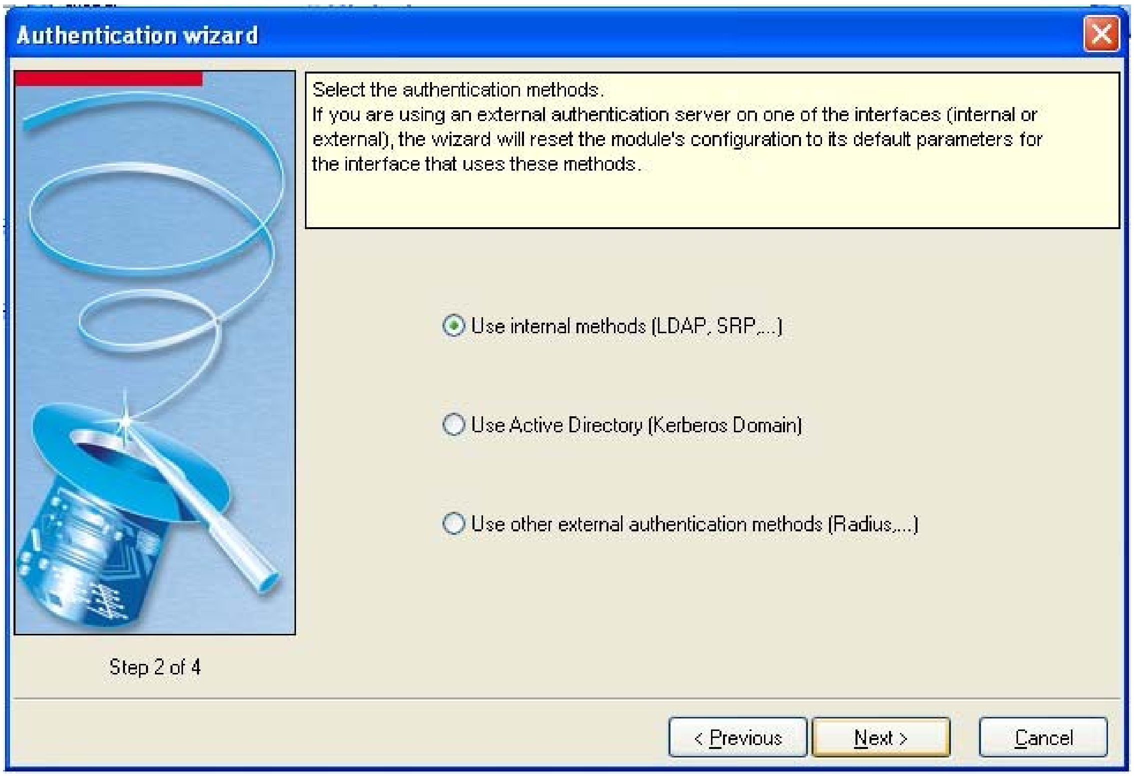
● Enable authentication on all interfaces

Step 1 of 4

Figure 347: Authentication wizard - Step 1

There are two interfaces for authentication methods – this interface allows the internal configuration of the firewall.

2 Authentication methods



Select the authentication methods.
If you are using an external authentication server on one of the interfaces (internal or external), the wizard will reset the module's configuration to its default parameters for the interface that uses these methods.

● Use internal methods (LDAP, SRP,...)

○ Use Active Directory (Kerberos Domain)

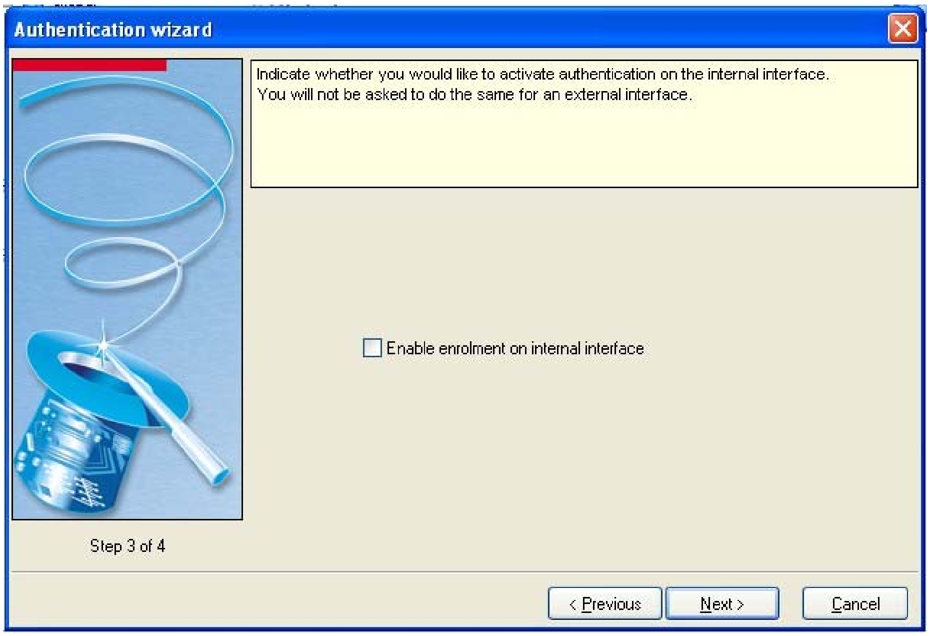
○ Use other external authentication methods (Radius,...)

Figure 348: Authentication wizard - Step 2

In this window, the authentication method can be selected from:

- Internal authentication methods (LDAP, SRP,…)
- Active Directory (Kerberos domain)
- Other external authentication methods (RADIUS,…)

3 Enrolment



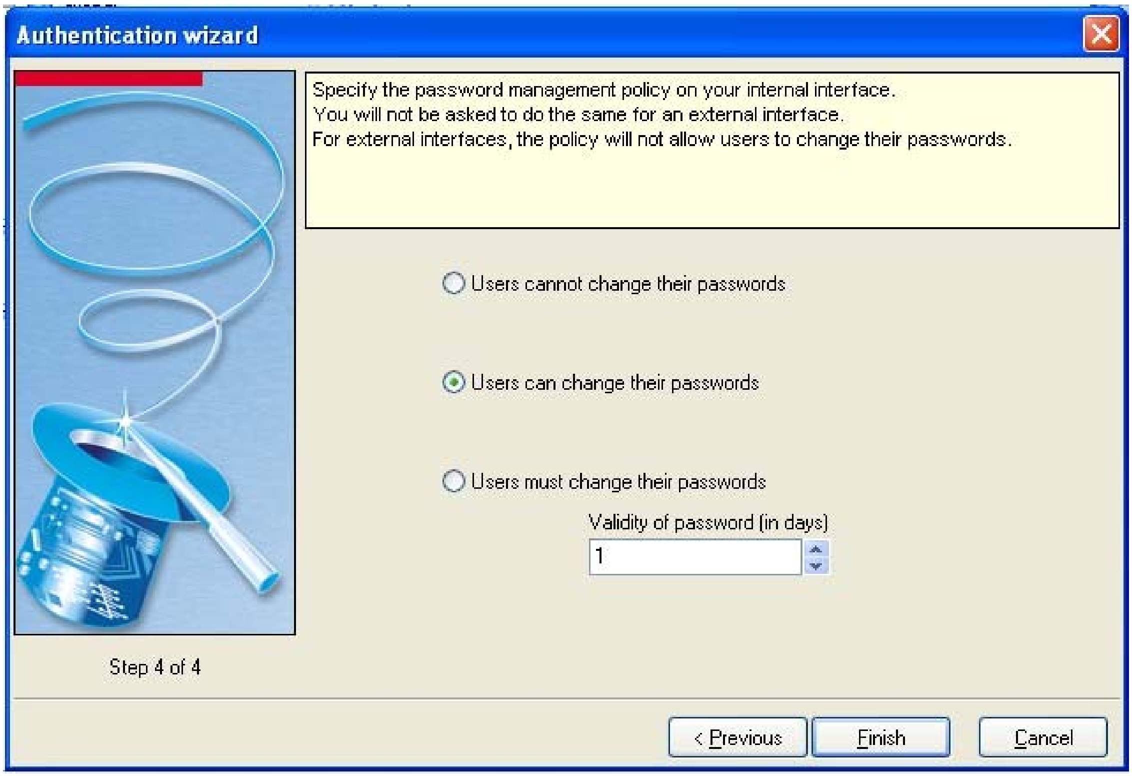
Indicate whether you would like to activate authentication on the internal interface.
You will not be asked to do the same for an external interface.

□ Enable enrolment on internal interface

Figure 349: Authentication wizard - Step 3

When the option **Enable enrolment on internal interface** has been selected, authentication will be activated on the internal interfaces.

4 **Password**



Specify the password management policy on your internal interface.
You will not be asked to do the same for an external interface.
For external interfaces, the policy will not allow users to change their passwords.

○ Users cannot change their passwords

● Users can change their passwords

○ Users must change their passwords

Validity of password (in days)
1

Figure 350: Authentication wizard - Step 4

On internal interfaces, passwords can be modified. In this window, you will be able to indicate your password management policy from the options “Users cannot change their passwords”, “Users can change their passwords” and “Users must not change their passwords”. For the last option, indicate the number of days for which the password will remain valid.

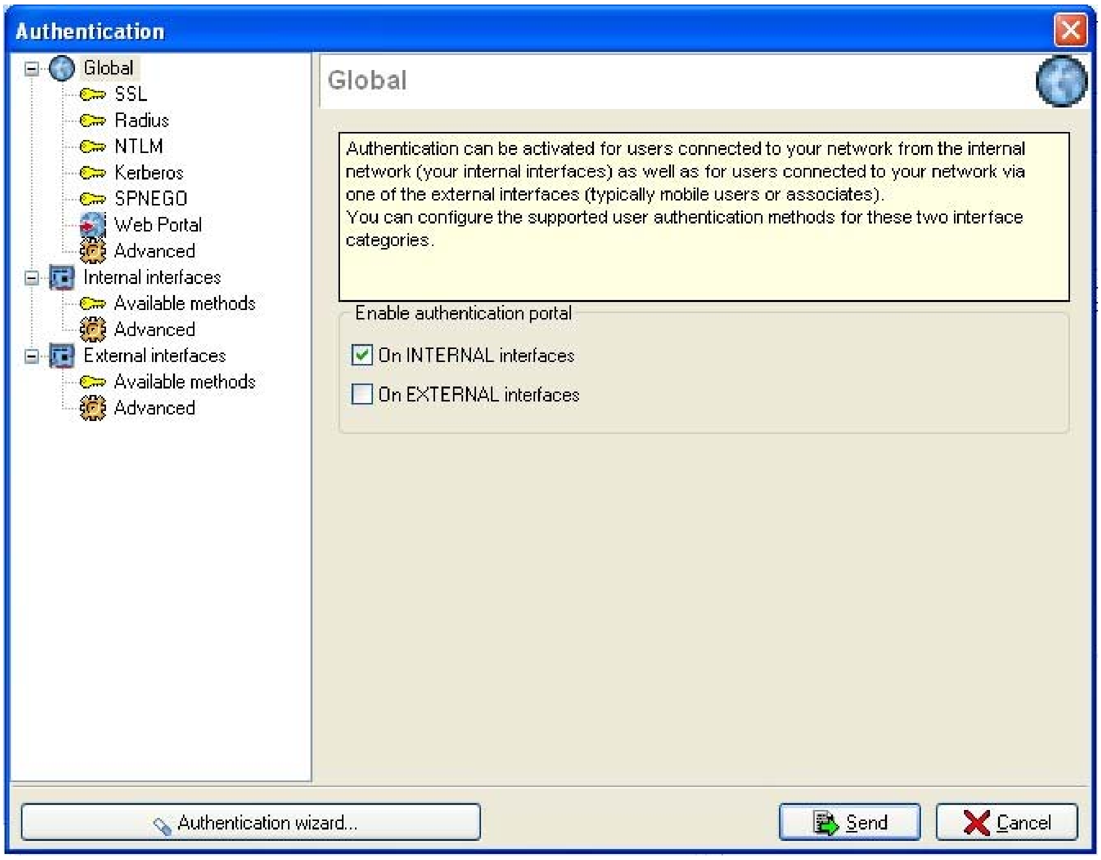
"Send" and"Cancel" buttons

Send	Activates the authentication configuration.
Cancel	Cancels modifications to the configuration in the authentication window.

12.1.2.2. Global

There are two methods by which users can authenticate:

- For users in the internal network (internal interfaces).
- For users connected to the network via an external interface.



Authentication can be activated for users connected to your network from the internal network (your internal interfaces) as well as for users connected to your network via one of the external interfaces (typically mobile users or associates).
You can configure the supported user authentication methods for these two interface categories.

Enable authentication portal

☑ On INTERNAL interfaces

□ On EXTERNAL interfaces

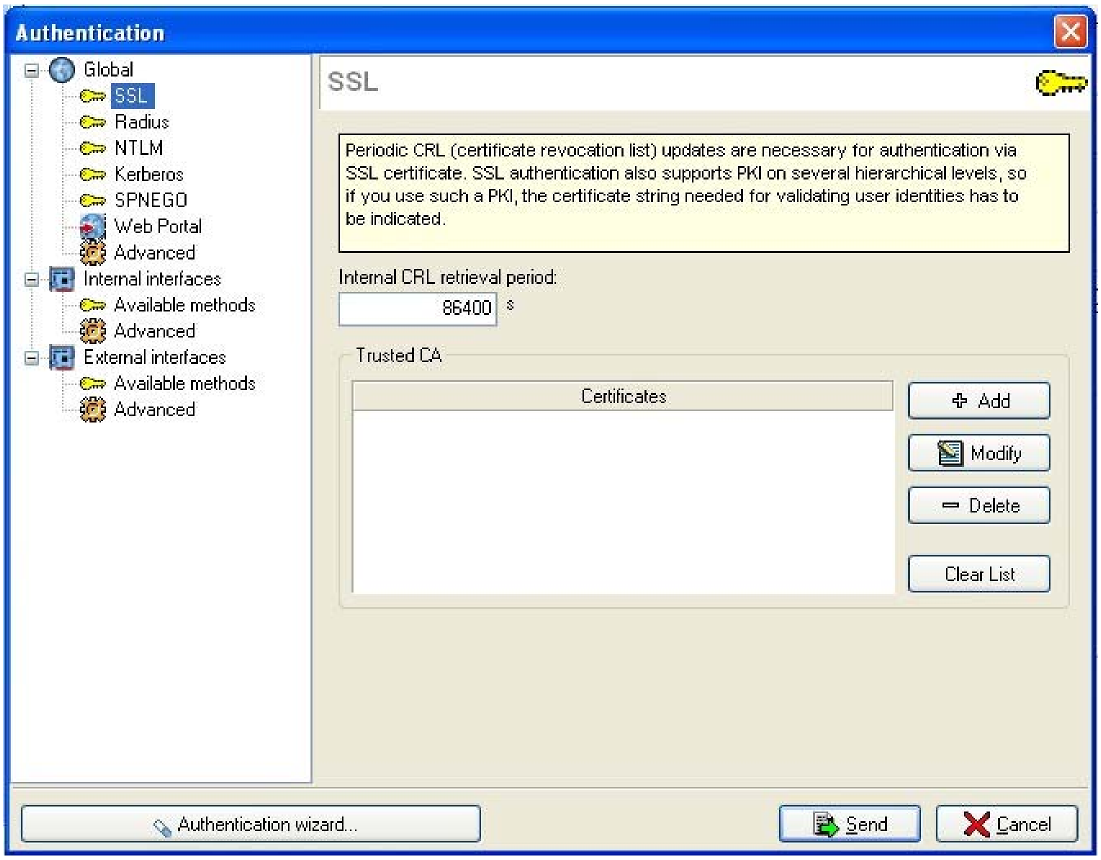
Figure 351: Authentication - Global

Authentication on Firewalls is determined by the interfaces on which traffic arrives. In fact, authentication can be activated only on internal interfaces, only on external interfaces or on both.

To authenticate on a type of interface, select the option on the INTERNAL interfaces and/or on the EXTERNAL interfaces that corresponds to the interface type.

SSL

The certificate revocation list (CRL) is regularly updated. These updates are necessary for authenticating with an SSL certificate. The user’s login has to be indicated for this type of PKI.



SSL

Periodic CRL (certificate revocation list) updates are necessary for authentication via SSL certificate. SSL authentication also supports PKI on several hierarchical levels, so if you use such a PKI, the certificate string needed for validating user identities has to be indicated.

Internal CRL retrieval period: 86400 s

Trusted CA

Certificates

Figure 352: Authentication - SSL

SSL authentication is activated when the SSL method is selected. The options for configuring the SSL method are indicated in the table below:

Internal CRL retrieval period	Amount of time (in seconds) after which the **CRL** has to be retrieved, in order to check the validity of digital certificates created by the Firewall's internal **PKI**.
Trusted CA	The SSL authentication method accepts the use of certificates that have been signed by a certification authority outside the Firewall. This certification authority has to be added in the configuration of the Firewall so that it accepts all certificates that have been signed by this authority. If the certification authority itself is signed by another certification authority, it can then be added to the list of trusted CAs in order to created a "Trusted CA chain". If a trusted CA or trusted CA chain is specified in the configuration of SSL authentication, it will be added to the Firewall's internal CA, which is implicitly checked as soon as there is a valid internal PKI on the Firewall.

Action buttons

Add	Adding a certification authority to a list of trusted certification authorities allows the recognition of this authority and the validation of all certificates signed by this certification authority. Clicking on **Add** leads you to the window that displays external certificates. (See *Certificates*)

	If the certification authority you wish to trust is not on the list of external certificates, click on **Add** in the external certificate window to add this certification authority to the list. Firewalls support multi-level PKIs, so if the user certificate is signed by a certification authority, which is itself signed by another higher certification authority, you can insert the whole certification chain created by this multi-level PKI. In order for the chain to be correctly applied, it is important that you insert every link in the whole chain of authorities between the highest authority you have inserted to the authority just above the user certificate.
Edit	Enables the modification of a certification authority. For example, it is mandatory for each CA to be associated with a CRL, which has a limited lifetime (to regularly apply revoked certificates), but is not modified automatically, therefore it has to be done manually.
Delete	Deletes the selected certification authority.
Clear list	Deletes the full list of configured certificates

WARNING

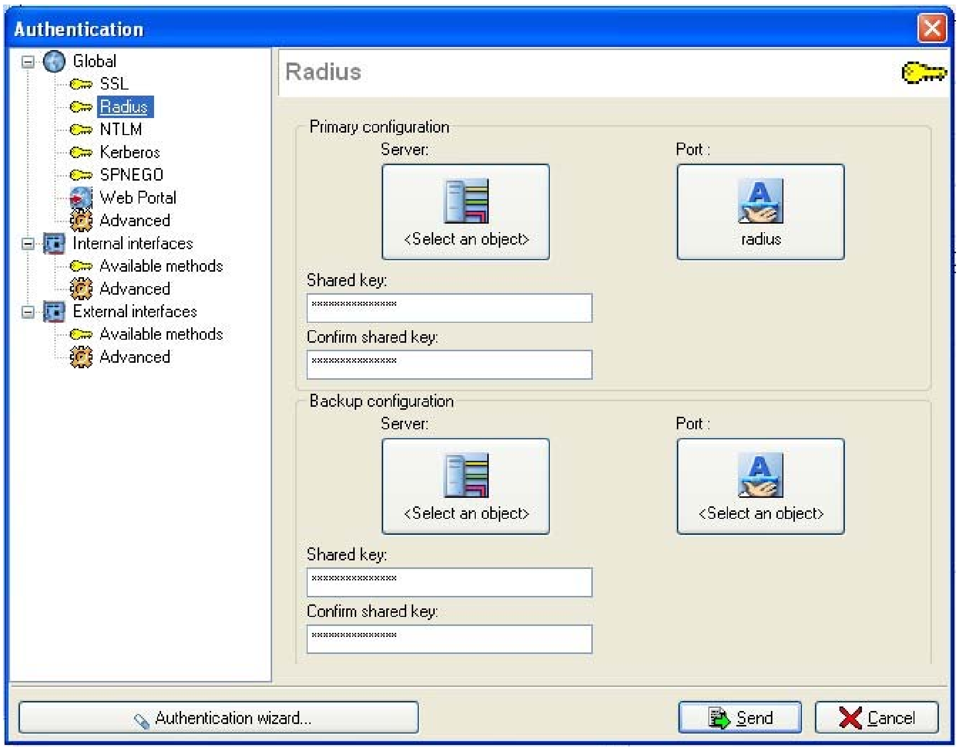
1) When a trusted certification authority is added, a certificate revocation list (CRL) must be associated to this CA. The wizard that adds certification authorities will ask you to add a CRL, but it will not be automatically retrieved as in the case of the internal CRL on NETASQ's PKI.
2) When an external certification authority is used, the e-mail address specified in the user certificate (which will be used for authentication) has to be the same as the address entered in the user file in the Firewall's user database, so that the Firewall can match the certificate with a user identifier in its user database.

RADIUS

Introduction

RADIUS is an authentication protocol functioning in client-server mode. The NETASQ Firewall can act as a RADIUS client. It can therefore address authentication requests for users wishing to pass through the Firewall, to an external RADIUS server. The user will only be authenticated on the Firewall if the RADIUS server accepts the authentication request sent by the Firewall.

All RADIUS transactions (communications between the Firewall and the RADIUS server) are themselves authenticated using a pre-shared secret, which is never transmitted over the network. This same secret will be used to encrypt the user password, which will pass through the Firewall and RADIUS server. RADIUS authentication uses UDP on port 1812.



Radius

Primary configuration

Server: <Select an object>

Port : radius

Shared key: ***************

Confirm shared key: ***************

Backup configuration

Server: <Select an object>

Port : <Select an object>

Shared key: ***************

Confirm shared key: ***************

Figure 353: Authentication - RADIUS

Operation

When RADIUS is selected, RADIUS authentication will be activated. This menu allows you to specify information relating to the external RADIUS server used and the backup RADIUS server, where applicable. For each case, the information in the following tables is required for configuration:

Server	RADIUS server's IP address.
Port	Port used by the RADIUS server.
Shared key	Key used to encrypt exchanges between the Firewall and the RADIUS server.
Confirm shared key	Enter the key again to confirm it.

Switching between the main and backup servers

The Firewall will attempt to connect twice to the main RADIUS server, and in the event of failure, will attempt to connect twice to the backup RADIUS server. If the backup RADIUS server responds, it will become the main RADIUS server. After 600 seconds, a new switch will take place, and the original "main" RADIUS server will become the "main" server again.

NTLM

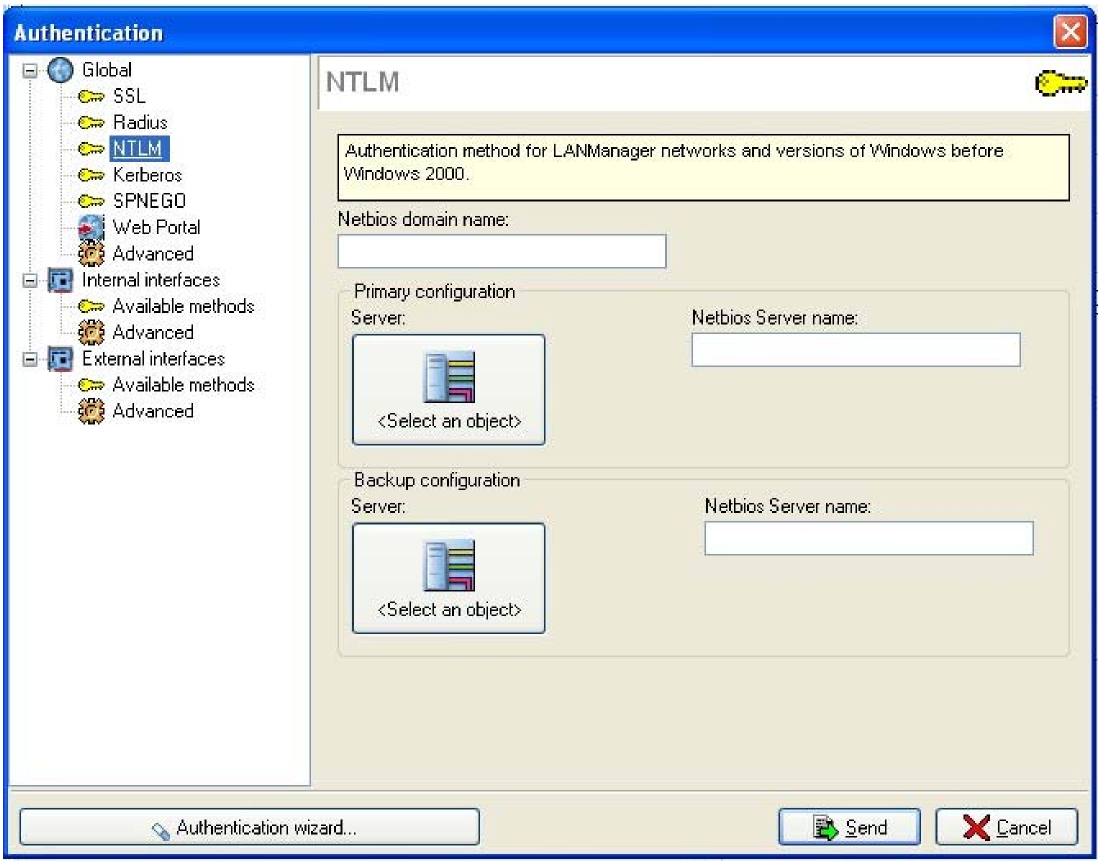
Introduction

NTLM serves as an authentication protocol for transactions between two computers of the same domain, whereby one of the computers executes, or both execute Windows NT 4.0 or an earlier version.

The NTLM protocol authenticates users and computers based on a challenge/response mechanism. Each time a new access is necessary, the Firewall contacts an authentication service on the domain controller to check the user's identity.

The user will be authentication on the Firewall only if the NTLM authentication service accepts the authentication request sent by the Firewall.

The Firewall is therefore compatible with NT authentication.



Authentication method for LANManager networks and versions of Windows before Windows 2000.

Figure 354: Authentication - NTLM

Operation

When NTLM is selected, NTLM authentication will be activated. This menu allows you to specify information relating to the external NTLM server used and the backup NTLM server, where applicable. For each case, the information in the following table is required for configuration:

Netbios domain name	Domain name on which the NTLM server is used.
Server	NTLM server's IP address. When you click on this button, the objects database will appear, allowing you to select a host.

Netbios server name	Name used by the NTLM server.

Switching between tne main and the backup servers

The Firewall will attempt to connect twice to the main NTLM server, and in the event of failure, will attempt to connect twice to the backup NTLM server. If the backup NTLM server responds, it will become the main NTLM server. After 600 seconds, a new switch will take place, and the original “main” NTLM server will become the “main” server again.

KERBEROS

Introduction

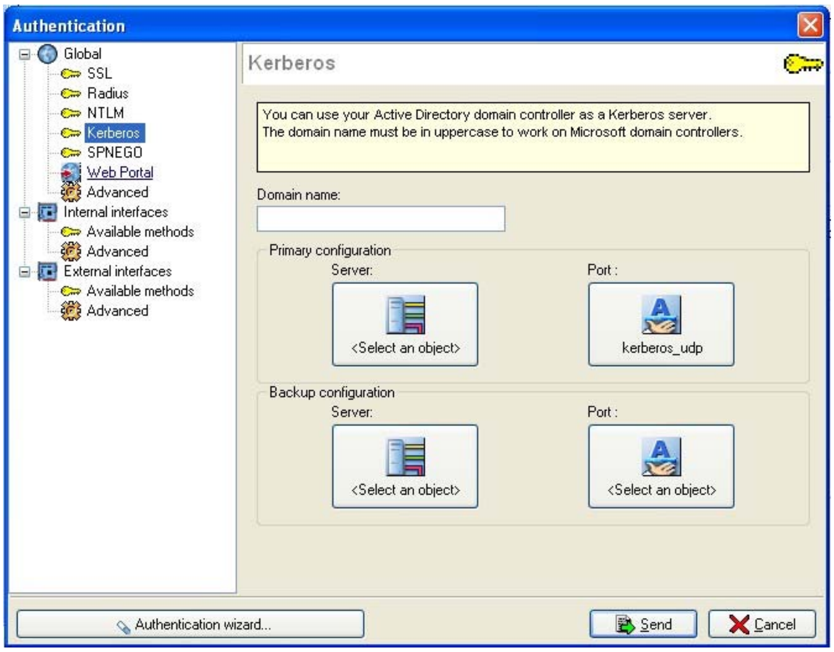
Kerberos is different from other authentication methods. Rather than let authentication take place between each client host and each server, Kerberos uses symmetrical encryption and a reliable program, KDC (Key Distribution Center) to authenticate users on a network.

UDP is used in a standard case but nonetheless requires TCP for requests that are too long. When such requests are detected, the server will switch from UDP to TCP.

Once the user has authenticated, Kerberos stores a ticket unique to this session on the user’s computer and “Kerberized” services will look for this ticket instead of asking the user to authenticate using a password.

During the authentication process, the NETASQ Firewall acts as a client which requests authentication on behalf of the user. This means that even if the user has already authenticated with the KDC to open his Windows session, for example, it is still necessary to re-authenticate with this server even if connection information is identical, in order to pass through the Firewall.

However, the advantage of this mode is that there is only one authentication database to keep up to date. Windows 2000 and XP environments use Kerberos, making the Firewall compatible with the authentication of these systems.



You can use your Active Directory domain controller as a Kerberos server.
The domain name must be in uppercase to work on Microsoft domain controllers.

Domain name:

Primary configuration
Server: <Select an object>
Port : kerberos_udp

Backup configuration
Server: <Select an object>
Port : <Select an object>

Figure 355: Authentication - KERBEROS

Operation

When Kerberos is selected, Kerberos authentication will be activated. This menu allows you to specify information relating to the external Kerberos server used and the backup Kerberos server, where applicable. For each case, the information in the following tables is required for configuration:

Domain name	Domain name on which the Kerberos server is used.
Server	Kerberos server's IP address. When you click on this button, the objects database will appear, allowing you to select a host.
Port	Port used by the Kerberos server. However, sometimes requests may be too long, so the port will then switch automatically to TCP.

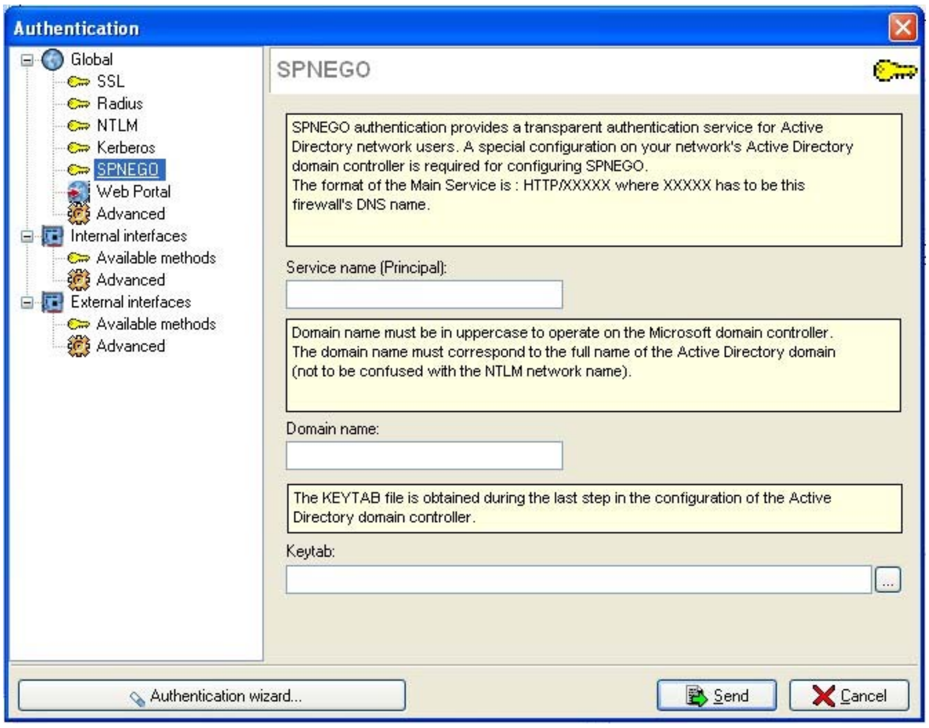
Switching between the main and backup servers

The Firewall will attempt to connect twice to the main Kerberos server, and in the event of failure, will attempt to connect twice to the backup Kerberos server. If the backup Kerberos server responds, it will become the main Kerberos server. After 600 seconds, a new switch will take place, and the original "main" Kerberos server will become the "main" server again.

SPNEGO

Introduction

The SPNEGO method enables Single Sign On to function in web authentication with an external Kerberos authentication server. This means that a user who connects to his domain via a Kerberos-based solution would be automatically authenticated on a NETASQ Firewall when the internet is accessed (requiring authentication in the filter policy on the Firewall) with a web browser (Internet Explorer, Firefox, Mozilla).



SPNEGO

SPNEGO authentication provides a transparent authentication service for Active Directory network users. A special configuration on your network's Active Directory domain controller is required for configuring SPNEGO.
The format of the Main Service is : HTTP/XXXXX where XXXXX has to be this firewall's DNS name.

Service name (Principal):

Domain name must be in uppercase to operate on the Microsoft domain controller.
The domain name must correspond to the full name of the Active Directory domain (not to be confused with the NTLM network name).

Domain name:

The KEYTAB file is obtained during the last step in the configuration of the Active Directory domain controller.

Keytab:

Figure 356: Authentication - SPNEGO

Requirements

NETASQ's solution is embedded like a full Single Sign On solution, therefore certain components have to be installed on the Kerberos server. The procedure for this is as follows:

1 Install a "Service Principal Name" (SPN) on the SPNEGO server to enable encrypting the exchanges between the SPNEGO server, the user and the Firewall.

2 Execute the SPNEGO script that NETASQ has delivered in the Administration Suite CDROM.

3 Retrieve the "Keytab" generated by the script.

Operation

SPNEGO is configured on the Firewall using the options explained in the following table:

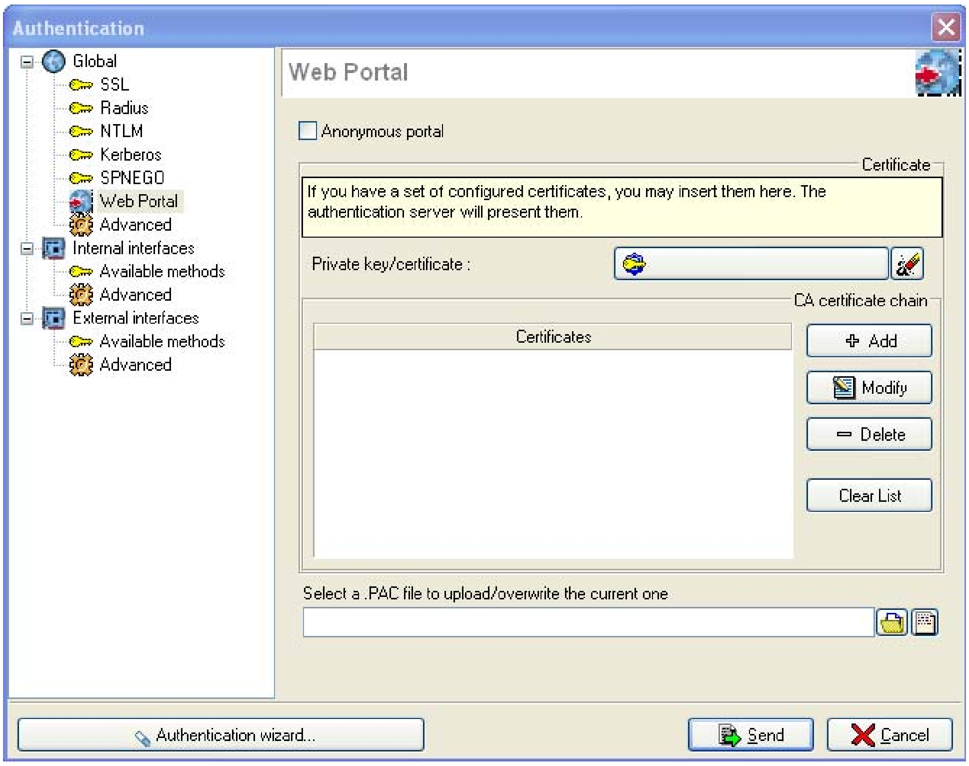
Service name (Main)	Firewall's name or address used for the authentication. This name corresponds to the name indicated in the NETASQ script (see above), and will be prefixed by **HTTP/xxxxx**. **Example** HTTP/U70XXA0Z099020
Domain name	Kerberos server's domain name. This domain name corresponds to the domain name indicated in the script and also corresponds to the full name of the Active Directory domain. It has to be entered in uppercase.
KEYTAB domain	Retrieves the keytab generated by the NETASQ script (see above).

To redirect authentication transparently, activate the **HTTP** proxy (See *Part 9/Chapter 3: HTTP proxy configuration*).

NOTE
Note that web authentication is only activated if an authentication rule has been defined in the filter policy (See *Part 7/Chapter 2*).

Web portal

The authentication server can used certificates that you have defined earlier.



□ Anonymous portal

If you have a set of configured certificates, you may insert them here. The authentication server will present them.

Private key/certificate :

Select a .PAC file to upload/overwrite the current one

Figure 357: Authentication – Web portal

Anonymous portal	When this option is selected, the NETASQ logo on the authentication portal will be hidden.
Private key /certificate	The certificate used by default on the Firewall's authentication module is the Firewall's own certificate, and the name associated to this certificate is the product's serial number. Therefore, when a user attempts to contact the Firewall other than through its serial number, he will see a warning message indicating that the Firewall the user is attempting to contact does not match the certificate it is receiving. To avoid seeing this message, a "server" certificate with an easier name can be specified (user certificates cannot be specified for this feature) on the Firewall authentication module, e.g. www.netasq.com. To obtain this type of certificate, you will need to contact organizations such as Verisign or Thawte. By clicking on Private key/certificate, the certificate configuration window will appear (in this case, for the private key).
Select a .PAC file to upload/overwrite the current one	This field allows you to send the .PAC file to be distributed to the firewall. The user can retrieve a .PAC file or check its contents with the help of the two buttons to the right of the field. The user can specify in his web browser the automatic configuration script located in https://if_firewall>/config/wpad.dat.

CA certificate chain

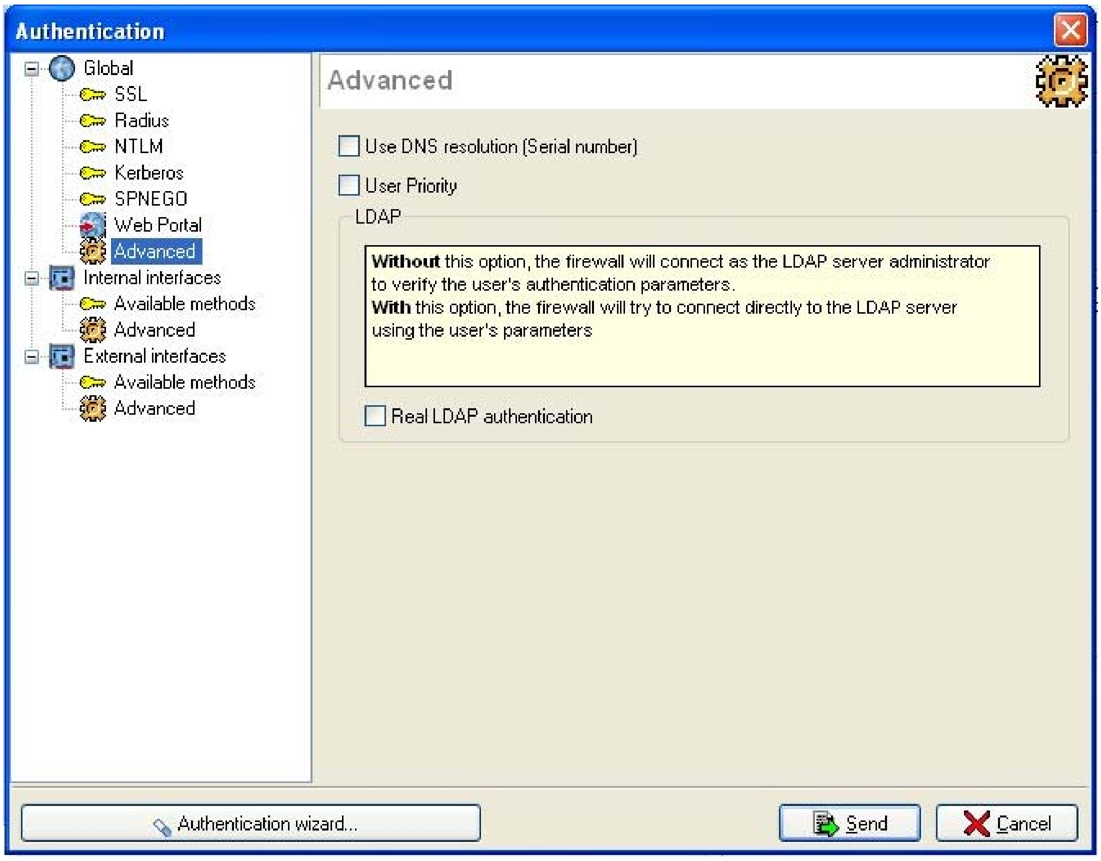
CA certificate chains certify the private keys used in the configuration of the authentication portal. To use this certification authority, it has to be added to the configuration of the Firewall so that the Firewall accepts all certificates (and in particular the private key speficied above) that it signs. If the certification authority itself is signed by another certification authority, the second certification authority can be added to the list of trusted CAs in order to create a "Trusted CA chain".

Add	Adds a certification authority to the list of trusted certification authorities, and allows the recognition of this authority and the validation of all certificates signed by this certifcation authority. Clicking on **Add** leads you to the window that displays external certificates. If the certification authority you wish to trust is not on the list of external certificates, click on **Add** in the external certificate window to add this certification authority to the list. Firewalls support multi-level PKIs, so if the user certificate is signed by a certification authority, which is itself signed by another higher certification authority, you can insert the whole certification chain created by this multi-level PKI. In order for the chain to be correctly applied, it is important that you insert every link in the whole chain of authorities between the highest authority you have inserted to the authority just above the user certificate.
Edit	Enables the modification of a certification authority. **Example** It is mandatory for each CA to be associated with a CRL, which has a limited lifetime (to regularly apply revoked certificates), but is not modified automatically, therefore it has to be done manually.
Delete	Deletes the selected certification authority.
Clear list	Deletes the full list of configured certificates

❗ **WARNING**

When a trusted certification authority is added, a certificate revocation list (CRL) must be associated to this CA. The wizard that adds certification authorities will ask you to add a CRL, but it will not be automatically retrieved as in the case of the internal CRL on NETASQ's PKI.

Advanced



□ Use DNS resolution (Serial number)

□ User Priority

LDAP

Without this option, the firewall will connect as the LDAP server administrator to verify the user's authentication parameters.
With this option, the firewall will try to connect directly to the LDAP server using the user's parameters

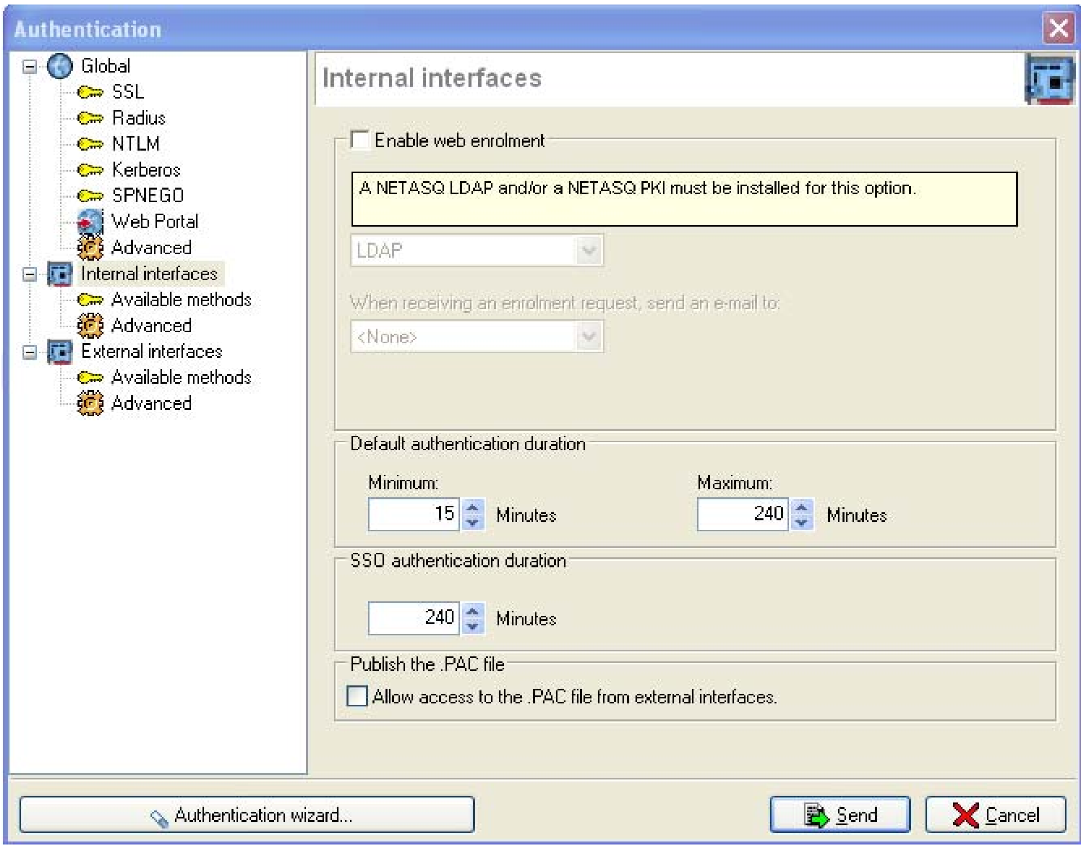
□ Real LDAP authentication

Figure 358: Authentication - Advanced

Use DNS resolution (serial number)	When transparent authentication is active (using URL proxy), users have to authenticate on the Firewall in HTTPS before they access a WEB site. The user's browser checks the Firewall certificate. An error message appears in the browser as the certificate corresponds to the serial number and not to the IP address of the Firewall. **WARNING** In this case, the serial number and the IP address of the Firewall has to be added in the DNS server. (DNS resolution will match the serial number to its IP address).
User priority	If this option has been checked, the Firewall will attempt to authenticate using the method indicated in the user file, regardless of the result of SPNEGO authentication.
Real LDAP authentication	If this option is not selected, the Firewall will connect in the capacity of an administrator on the LDAP server to validate the user's authentication. If this option has been selected, the Firewall will attempt to authenticate on the LDAP server using the user's parameters. If the Firewall's authentication on the LDAP server is unsuccessful, the user will then be denied authentication.

12.1.2.3. Internal and external interfaces

For each interface type, parameters have to be defined before activating authentication. These parameters are the same for internal interfaces (which **do not have** the “External” attribute in network configuration) and for external interfaces (which have the “External” attribute in network configuration).



Internal interfaces

□ Enable web enrolment

A NETASQ LDAP and/or a NETASQ PKI must be installed for this option.

LDAP

When receiving an enrolment request, send an e-mail to:

<None>

Default authentication duration

Minimum: 15 Minutes

Maximum: 240 Minutes

SSO authentication duration

240 Minutes

Publish the .PAC file

□ Allow access to the .PAC file from external interfaces.

Figure 359: Authentication – Internal interfaces

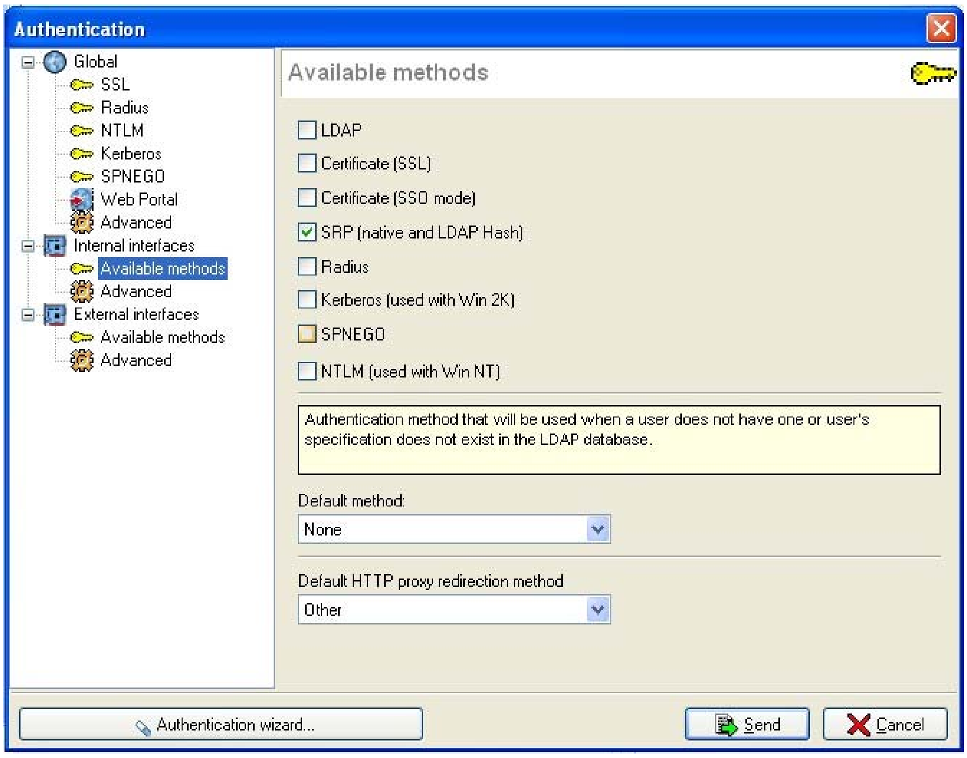
Enable Web enrolment

NETASQ offers web enrolment of users. If a user attempting to connect does not exist in the user database, he may ask for an account to be created for him via web enrolment.

Enable web enrolment	A NETASQ LDAP or PKI has to be installed for this option to function. You can specify two enrolment types available from the web: - **LDAP**: creation of a user account. - **LDAP/PKI**: creation of a user account and certificate.
When receiving an enrolment request, send an e-mail to	When a user requests for an account to be created via web enrolment, this request will be indicated in NETASQ UNIFIED MANAGER. The administrator may also be informed of this request by e-mail if the option **Send requests by e-mail** has been checked. In this case, the NETASQ Firewall uses the e-mail address indicated in the log configuration (See *Part 17: Log Management*).

Default authentication duration	**Minimum**: Minimum time during which the user is authenticated. **Maximum**: Maximum time during which the user is authenticated. At the end of this period, authentication expires and the user has to re-authenticate. The two values above allow the definition of a range of choices for authentication (the user can choose an authentication duration listed in this range). ❗ WARNING In order to avoid a session hijack, you are advised not to set a maximum period which is too high (max 4 hours). However, this means that the user will have to authenticate more often.
SSO authentication duration	When an SSO-based (Single Sign-On) authentication method is selected, this period enables the definition of the duration for which the Firewall will not request transparent re-authentication.
Publish the .PAC file	If the option **Allow access to the .PAC file from external interfaces** is selected, the publication of the .PAC file will be allowed on internal interfaces. Publication of the .PAC file will also be possible for external interfaces.

Available methods



Available methods

☐ LDAP
☐ Certificate (SSL)
☐ Certificate (SSO mode)
☑ SRP (native and LDAP Hash)
☐ Radius
☐ Kerberos (used with Win 2K)
☐ SPNEGO
☐ NTLM (used with Win NT)

Authentication method that will be used when a user does not have one or user's specification does not exist in the LDAP database.

Default method: None

Default HTTP proxy redirection method: Other

Figure 360: Authentication – Available methods

Select the authorized method(s) on the NETASQ Firewall. These are default authentication methods and correspond to different authentication mechanisms. Each user can have a different authentication method but it cannot be used unless it has been selected in this window.

LDAP	The user must enter a login/password. This data transits unencrypted in SSL (if the user accesses the Firewall via https with his Internet navigator). This method uses port 443. WARNING This method is the least secure because it will be possible from now on to access (fraudulently) information contained in the SSL traffic. However, this does not apply to the SSL+Certificate method.
Certificate (SSL)	The user does not need to enter a login/password but a digital certificate generated by the Firewall's internal PKI must be installed on the user's terminal. The user must connect to the Firewall in https with his internet browser in order to authenticate This method uses port 443.
Certificate (SSO Mode)	This method, which is based on the SSL method in an **SSO** (***Single Sign On***) mode, allows simplifying the steps in SSL authentication. The Firewall automatically recognizes the authentication method which will be used for the user.
SRP (native and LDAP hash)	This method uses the **SRP** (***Secure Remote Password***) protocol the password for which is never transmitted. The user must access the Firewall in https and enter a login/password. This method uses port 443 (the port used by the SRP Java applet). It includes native SRP and the SRP_Hash.
RADIUS	This method is used if the authentication is relayed to an external RADIUS server.
KERBEROS (used with Win 2k)	This method is used if the authentication is relayed to an external Kerberos server.
SPNEGO	This method uses the only authentication principle which, under certain conditions when the user is authenticated on a domain after opening his session, enables him to be authenticated on the Firewall as well.
NTLM (used with Win NT)	This method is used if the authentication is relayed to an external NTLM server.

Default method

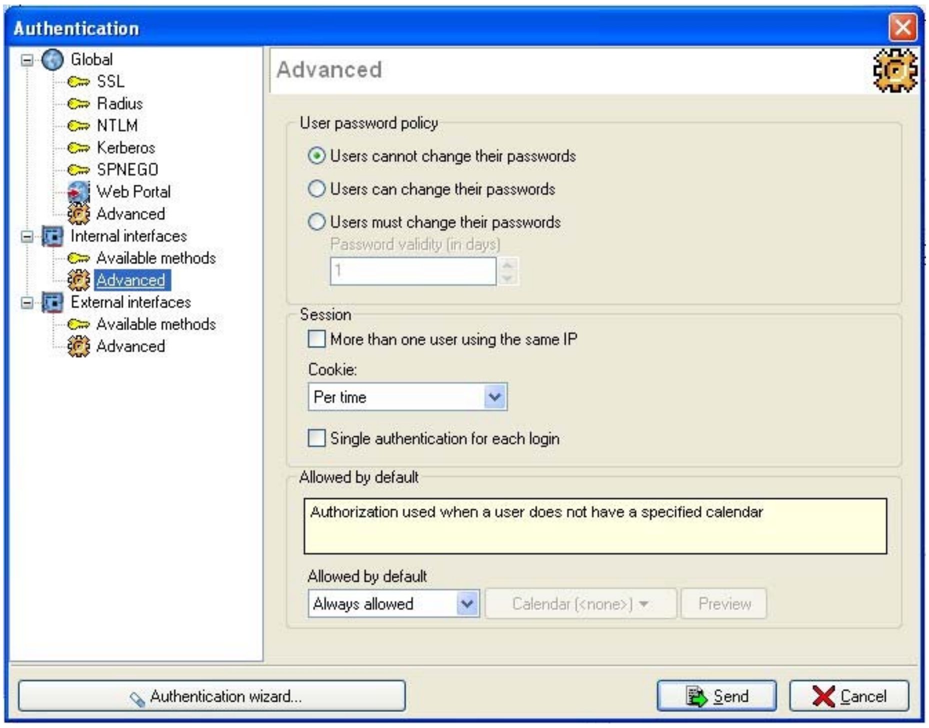
This method is used when a user wishing to authenticate himself does not exist in the internal or external LDAP directory. This option allows you to have some user records on the LDAP database and others on a RADIUS, Kerberos or NTLM server, for instance (in this case, select the relevant option).

> **Example**
> If RADIUS is selected, when a user is not specified in the LDAP database, the Firewall queries the RADIUS server.

Default http proxy redirection method

When a default HTTP proxy redirection method (SRP, Certificate or SPNEGO) is activated the SSO feature for this method will also be activated. For example, in the case of SRP authentication in SSO mode, the authentication portal's SRP applet displays the login and password on the page. Regardless of the authentication methods selected, SRP in SSO mode will be used.

Advanced



Advanced

User password policy

● Users cannot change their passwords

○ Users can change their passwords

○ Users must change their passwords

Password validity (in days) 1

Session

□ More than one user using the same IP

Cookie: Per time

□ Single authentication for each login

Allowed by default

Authorization used when a user does not have a specified calendar

Allowed by default: Always allowed

Calendar (<none>)

Preview

Figure 361: Authentication - Advanced

User password management policy

There are three ways to manage user passwords on NETASQ Firewalls.

- **Users cannot change their passwords**: by selecting this option, users will not be able to change their authentication passwords on the NETASQ Firewall;
- **Users can change their passwords**: by selecting this option, users will be able to change their authentication passwords on the NETASQ Firewall at any time;
- **Users must change their passwords**: by selecting this option, users will need to change their authentication passwords on the NETASQ Firewall on their first connection to the Firewall's authentication portal, and then for each time the password expires. This duration is specified in days without a specific time. This means, for example, that if the user password is valid for 1 day and that the password was initialized for the first time at 2.00 p.m. on 27 July 2005, the password has to be changed from 12.00 midnight on 28 July 2005 and not 24 hours later.

Session

The "Session" section in the configuration of authentication comprises three options set out in the following table:

- **More than one user using the same IP**: The basis of NETASQ authentication is the creation of an entry in the ASQ table that matches a user name to an IP address. By default, multiple logins cannot be registered on the same IP address. If this option is selected, it will be possible to register several logins on the same IP address, thereby enabling the authentication of several users located behind NAT equipment that would mask the users' real addresses with a unique IP address.
- **Cookie**: Managing cookies for user authentication on Firewalls allows securing the authentication process, thereby preventing replay attacks, for example, since possession of the connection cookie is necessary in order to be considered authenticated.

	Cookies are defined by default "per time", meaning that cookies are negotiated only once for the whole duration of authentication. However, "per session" cookies can also be configured, meaning that these cookies will be negotiated each time the web browser is launched. It is possible to not use any cookies, but this option is not recommended as it compromises the security of the authentication. Cookies are essential for the option **More than one user using the same IP**. The web browser negotiates cookies, therefore if authentication is carried out with Internet Explorer, it will not be effective with Firefow or other web browsers. ● **Single authentication for each login**: If this option is selected, users will not be able to authenticate on more than one host.
Allowed by default	When a user is created or when authentication rules concerning him are set up, this user will be associated to a calendar (See *Slot Scheduler*). This calendar specifies time slots during which the user has the right to authenticate. For all other time slots, the connection will be refused. In the event no calendar corresponds to a user, you can configure several actions: ● Always allowed: The user can connect at all the times on all the days defined in the filter rules. ● Always denied: Whatever the authentication result, the connection will be refused. ● Customized: You may specify a default calendar.

12.1.3. LDAP Database

12.1.3.1. Introduction

DEFINITION

LDAP *(Lightweight Directory Access Protocol)* is a standard protocol allowing the management of directories, that is, accessing information databases on a network's users by way of TCP/IP.
LDAP defines the access method to data on the server on the client level, and not the manner according to which information is stored. It presents information in the form of a hierarchical information tree called **DIT** (***Directory Information Tree***), in which information, or entries, (DSE, Directory Service Entry), are represented in the form of branches.
A branch located at the root of a ramification is called the root entry.
Each entry in the LDAP directory corresponds to an abstract or real object

> **Example**
> A person, hardware object, parameters

Each entry consists of a set of key-value pairs called attributes.

12.1.3.2. Using LDAP in NETASQ Firewalls

The LDAP directory contains various firewall configuration elements such as users, user groups and even XVPN profiles.

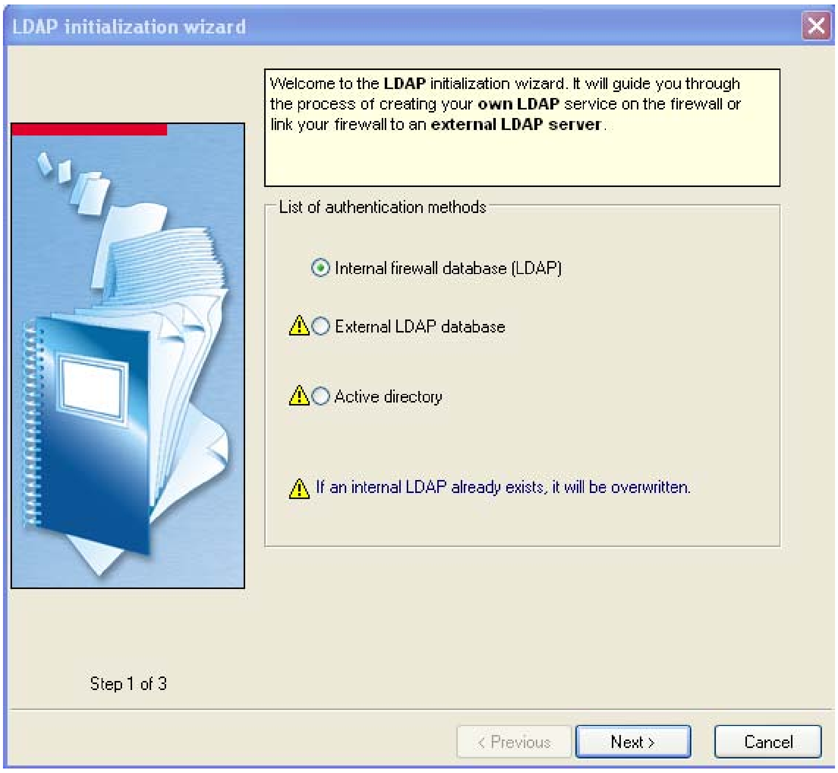
NETASQ Firewalls embed two types of LDAP directories – an internal LDAP database which allows storing information relating to users who have to authenticate to pass through the Firewall, and an external LDAP that is located ona remote host.

12.1.3.3. LDAP initialization wizard

The LDAP wizard helps you to easily configure your LDAP database.

Step 1

➲ The first step in the LDAP configuration wizard can be accessed from the menu **`Authentication\LDAP database`** when the LDAP has not yet been initialized or by clicking on the button in the general configuration window when the LDAP database has been initialized.



Welcome to the **LDAP** initialization wizard. It will guide you through the process of creating your **own LDAP** service on the firewall or link your firewall to an **external LDAP server**.

List of authentication methods

● Internal firewall database (LDAP)

⚠ ○ External LDAP database

⚠ ○ Active directory

⚠ If an internal LDAP already exists, it will be overwritten.

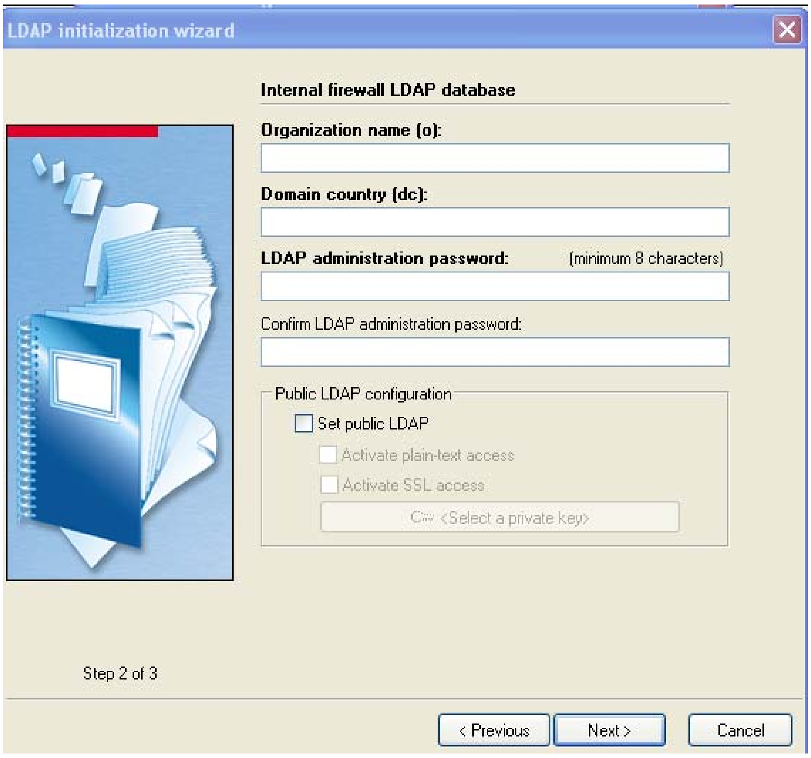
Figure 362: LDAP initialization wizard - Step 1

In this first step, you need to choose whether you wish to create an internal firewall LDAP database or indicate to the firewall to use an external database that you already have.

Depending on your choice, the following step will vary, as the configuration of an external LDAP requires more information.

Step 2: Internal database

During this second step, you need to supply general information regarding the LDAP database that you wish to create. The information entered will reappear in your firewall's LDAP directory schema.



Internal firewall LDAP database

Organization name (o):

Domain country (dc):

LDAP administration password: (minimum 8 characters)

Confirm LDAP administration password:

Public LDAP configuration

□ Set public LDAP

□ Activate plain-text access

□ Activate SSL access

Figure 363: LDAP initialization wizard - Step 2

Organization name (o)	Name of your company (e.g.: NETASQ).
Domain country (dc)	Your company's domain (e.g.: com).
LDAP administration password	This password allows the firewall to connect to the LDAP database.
Confirm LDAP administration password	Confirms the LDAP administration password
Public LDAP configuration	The LDAP database can be accessed from outside by two methods: plaintext access or access via certificate authentication (SSL). In this case, the desired certificate has to be selected.

NOTE
Only the password can be subsequently modified.

WARNING
If external access is not necessary, you are advised against enabling the option **Set public LDAP**.

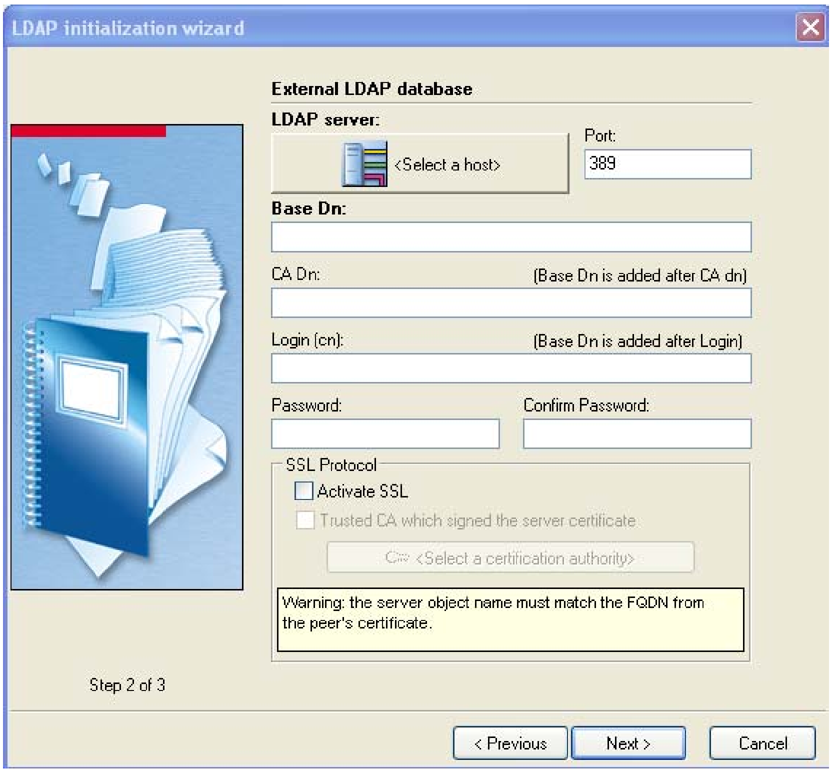
Step 2: External database

In certain architectures, the use of a user database that only the firewall can use may quickly become restrictive. Indeed, this would require the management of several databases and a manual duplication of the information between each database as the user accounts will not be centralized. Also, with an “airtight” database, user accounts that have already been configured on other databases cannot be reused.

To remedy this restriction, NETASQ firewalls allow interfacing with external LDAP databases for a full integration into the information system.

During this second step, you need to enter general information concerning the LDAP database that you own and which the firewall will consult.

This wizard consists of three zones.



LDAP initialization wizard

External LDAP database

LDAP server: <Select a host>

Port: 389

Base Dn:

CA Dn: (Base Dn is added after CA dn)

Login (cn): (Base Dn is added after Login)

Password:

Confirm Password:

SSL Protocol

□ Activate SSL

□ Trusted CA which signed the server certificate

<Select a certification authority>

Warning: the server object name must match the FQDN from the peer's certificate.

Step 2 of 3

Figure 364: LDAP initialization wizard - Step 2

Network configuration of the external LDAP database

You need to select an object that corresponds to your LDAP server. This object has to be created beforehand and must reference the IP address of your LDAP server. The name chosen for the object has to correspond to the Common Name of the certificate of your LDAP server if the SSL protocol is being used, otherwise the name of the object is of little importance.

You need to enter your LDAP server’s listening port. The default ports are:

- 389 for plaintext authentication,
- 636 for SSL authentication.

NOTE
The external LDAP database must embed NETASQ's LDAP schema so that the NETASQ firewall can use it. Contact NETASQ's technical support to find out how to integrate thise schema.

Configuring the security of communications

If your LDAP server has been configured to support SSL and you wish for the firewall to communicate with the server via SSL, you need to select the option "Activate SSL". As an option (by selecting "Trusted CA which signed the server certificate", and by selecting the file containing the authority certificate) you can send to the firewall the certificate of the authority that issued your server's certificate. This will allow checking the validity of the certificate presented by the LDAP server.

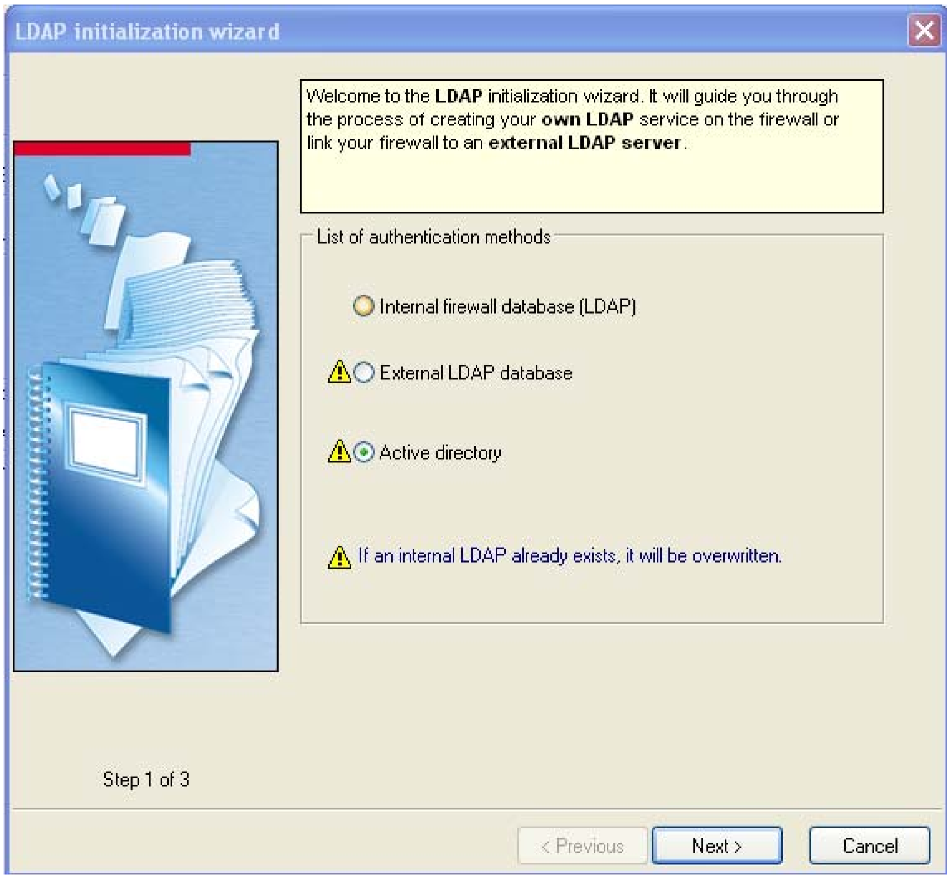
Configuring the LDAP base

Base Dn	Enter the root DN of your database (e.g.: o=NETASQ, dc=COM).
CA Dn	This field is optional and will only be used if you enable the PKI on the firewall. In this case, the authority's certicate and CRL that will be created will be placed in this LDAP entry. (e.g.: cn=Internal authority,ou=Certification authorities).
Login (cn)	User account that allows the firewall to connect to your LDAP server and to read/write certain fields. We recommend that you create a specific account for the firewall and to assign to it rights only for the fields that are necessary. (e.g.: cn=Admin Firewall NETASQ).
Password	Password to allow the user created on the firewall to connect to the LDAP server.
Confirm password	Confirmation of the LDAP administration password.
SSL protocol	If this option is selected, public access to the LDAP will be protected with the SSL protocol. If it has not been selected, the access will not be encrypted.

Step 2: Active directory (based on Windows 2000 or XP)

During this second step, you need to enter general information regarding the Active Directory database that you have and which the firewall will consult.

This wizard consists of three zones:



LDAP initialization wizard

Welcome to the **LDAP** initialization wizard. It will guide you through the process of creating your **own LDAP** service on the firewall or link your firewall to an **external LDAP server**.

List of authentication methods

○ Internal firewall database (LDAP)

⚠ ○ External LDAP database

⚠ ● Active directory

⚠ If an internal LDAP already exists, it will be overwritten.

Step 1 of 3

Figure 365: LDAP initialization wizard - Step 1

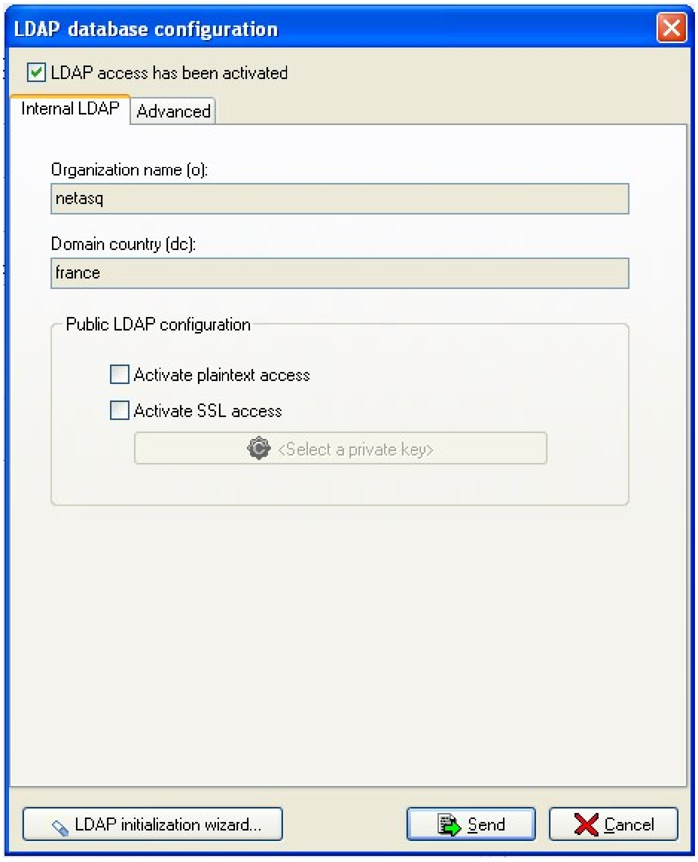
Domain controller	You need to select an object that corresponds to your Active Directory server. This object has to be created beforehand and must reference your server's IP address.
Domain name	You need to enter the domain name corresponding to the Active Directory database.
Login (cn)	User account that allows the firewall to connect to your Active Directory server and to read/write certain fields. We recommend that you create a specific account on the Active Directory database for the firewall and to assign to it rights only for the fields that are necessary. (e.g.: cn=Admin Firewall NETASQ).
Password	Password to allow the user created on the firewall to connect to the Active Directory server.
Confirm password	Confirmation of the LDAP administration password.
Escape characters	For certain external servers, a "\" has to be added so that LDAP requests can be understood.

With the wizard, you can access each of the configuration windows.

12.1.3.3 Configuring the internal LDAP database

➲ The internal LDAP configuration window can be accessed via the menu **`Authentication\LDAP Directory`**. It will allow you to view and configure your internal LDAP database.

Internal LDAP tab



LDAP database configuration

☑ LDAP access has been activated

Internal LDAP | Advanced

Organization name (o): netasq

Domain country (dc): france

Public LDAP configuration

☐ Activate plaintext access

☐ Activate SSL access

Figure 366: Configuring the LDAP base – internal LDAP

It comprises three sections:

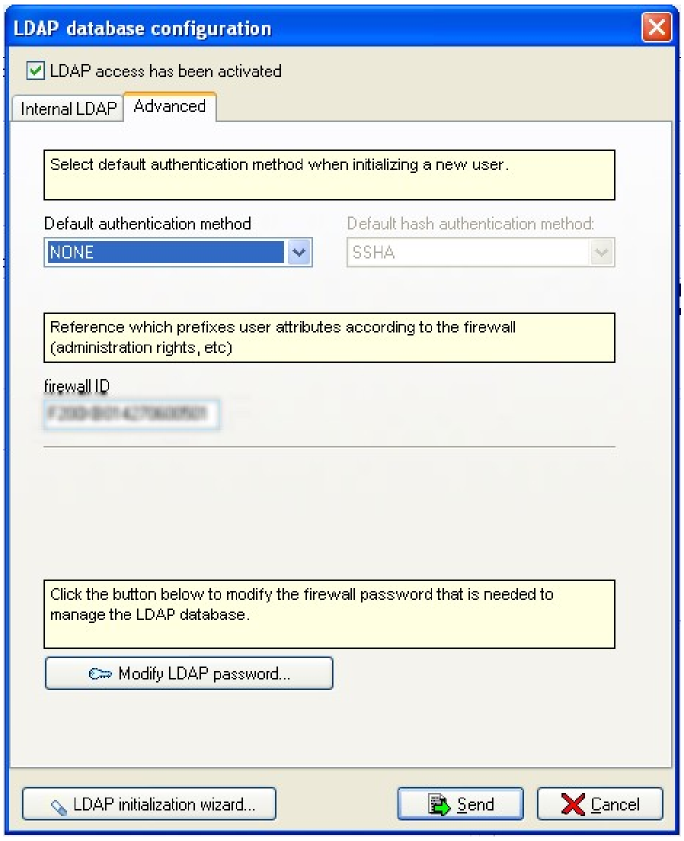
- A check box indicating the current status of access to the LDAP directory. If the box is checked, access is allowed, otherwise you may check the box yourself to allow access. This enables activating and deactivating access to the LDAP directory without destroying the configuration.
- A tab zone and the window corresponding to the chosen tab. The available tabs allow you to view the LDAP database's current configuration and to view and modify your configuration's advanced parameters.
- A zone at the bottom right with three buttons allowing you to initialize your LDAP directory, send your changes to the Firewall or to exit this window without applying the changes.

Organization name (o)	Your company's name (e.g.: NETASQ)
Domain country	Your company's domain (ex: com)
Public LDAP configuration	It is possible to access the LDAP directory from the outside. Two methods are available: plaintext access or access via Certificate (SSL) authentication. In this case, select the desired certificate.

NOTE
The password is the only thing you can change subsequently.

WARNING
If external access is not necessary, you are strongly advised against activating the “Public LDAP configuration” option.

Advanced tab


LDAP database configuration

☑ LDAP access has been activated

Select default authentication method when initializing a new user.

Default authentication method: NONE

Default hash authentication method: SSHA

Reference which prefixes user attributes according to the firewall (administration rights, etc)

firewall ID

Click the button below to modify the firewall password that is needed to manage the LDAP database.

Figure 367: Configuring the LDAP base - Advanced

This option allows you to configure the users’ authentication parameters which will be created thereafter and to change the LDAP database administrator’s password.

Default authentication method

The available authentication methods are as follows:

- **NONE**: users cannot authenticate.
- **LDAP**: authentication by sending the user’s password to the firewall via a protected tunnel (HTTPS) or directly (HTTP).
- **SSL**: users have to present a certificate to the firewall in order to authenticate.
- **SRP**: this method makes it possible to not send the user’s password to the firewall, it is based on a challenge-response protocol. Now when this method is used, the DNS name will be used instead of the firewall’s IP address.
- **SRP_LDAP**: this method is the same as the previous, except that it uses the user’s existing LDAP password to generate an ephemeral SRP key and allows SRP authentication.
- **RADIUS**: this method allows authenticating users on a RADIUS server. The password is sent to the firewall in the same way as for the LDAP method.
- **KERBEROS**: this method allows authenticating users on a Kerberos server.
- **NTLM**: this method allows authenticating users on an NTLM server.

WARNING

The SRP authentication method is one of the safest, we therefore recommend that you use it. The SRP_LDAP method is very useful for external LDAP databases and when users already have a password. In this case, they get greater security without modifying the existing architecture.

Default hash authentication method

For certain authentication methods **(SRP_LDAP, LDAP)** the user password has to be stored as a hash (result of a hash function applied to the password) to avoid storing it in plaintext. You must therefore select a desired hash method:

- **NONE**: no hash, the password is stored in plaintext (not recommended).
- **MD5**: the password is hashed using the MD5 algorithm.
- **SMD5**: the password is hashed using the Salt MD5 algorithm. This variation of the MD5 algorithm uses a random value to diversify the password hash. Two identical passwords will therefore have two different hashes.
- **SHA**: the password is hashed using the SHA-1 algorithm.
- **SSHA**: the password is hashed using the Salt SHA-1 algorithm. This variation of the SHA-1 algorithm uses a random value to diversify the password hash. Two identical passwords will therefore have two different hashes.
- **CRYPT**: the password is protected by the CRYPT algorithm. This is the native method of CRYPT which is derived from the DES algorithm. This is not to be confused with CRYPT UNIX which allows the use of various algorithms, depending on the OS.

WARNING

The safest hash method is **SSHA**, which we recommend that you use. The **SRP** method also stores information for authenticating users, but this information is in the form of a Diffie-Hellmann key and a random seed, which are stored in the fields of the NETASQ LDAP schema.

Firewall ID

All users of the LDAP database are prefixed with the serial number of the firewall on which the LDAP database was created (prefixed by default). But when the firewall is replaced or when the configuration of the LDAP database backed up then restored on another firewall, the default prefix will no longer be valid. This option allows specifying a prefix that has no attachment to the firewall.

Modify LDAP

This option allows modifying the password of the LDAP database configuration.

password	

Internal LDAP wizard

The LDAP initialization wizard allows you to configure your LDAP database without difficulty.

Step 1

This first stage of the LDAP database configuration wizard can be accessed via the menu **`Authentication\LDAP Directory`** when the LDAP base is not initialized or by a button on the general configuration screen when the LDAP base has already been initialized

At this initial stage you must decide whether you want to create an internal LDAP directory on the Firewall or to order it to use an existing external directory.

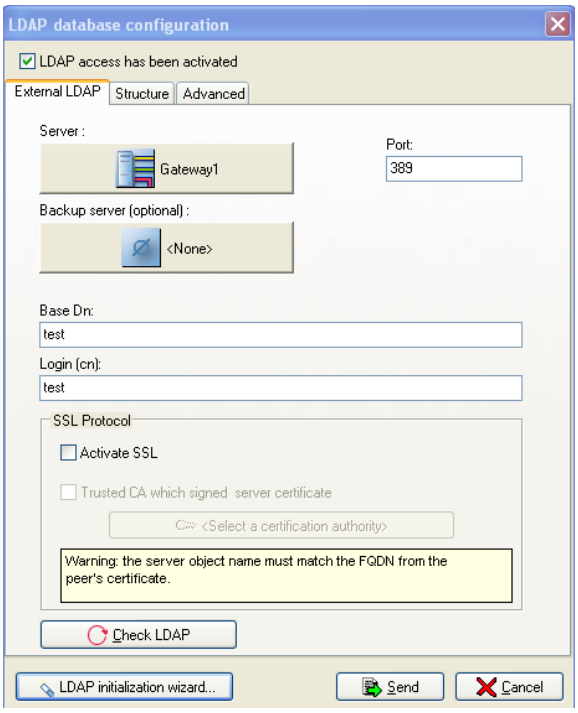
The next stage varies, depending on your choice; configuration of the external LDAP needs more information.

Step 2: Internal directory

At this stage you must provide the general data for the LDAP base you want to create. The data to be entered can be found in the Firewall’s LDAP directory.

12.1.3.4. Configuring the external LDAP base

External LDAP tab (for an external LDAP or Active Directory)



☑ LDAP access has been activated

Server : Gateway1

Port: 389

Backup server (optional) : <None>

Base Dn: test

Login (cn): test

SSL Protocol

☐ Activate SSL

☐ Trusted CA which signed server certificate

<Select a certification authority>

Warning: the server object name must match the FQDN from the peer's certificate.

Figure 368: Configuring the LDAP base – External LDAP

<u>Network configuration of the external LDAP server</u>

You need to select an object that corresponds to your LDAP server. This object has to be created beforehand and must reference the IP address of your LDAP server. The name chosen for the object has to correspond to the Common Name of the certificate of your LDAP server if the SSL protocol is being used, otherwise the name of the object is of little importance.

You need to enter your LDAP server’s listening port. The default ports are:

- 389 for plaintext authentication,
- 636 for SSL authentication.

An external backup server can be configured, but its configuration is subject to the same configuration requirements as for the "main" external LDAP server.

Configuring the security of communications

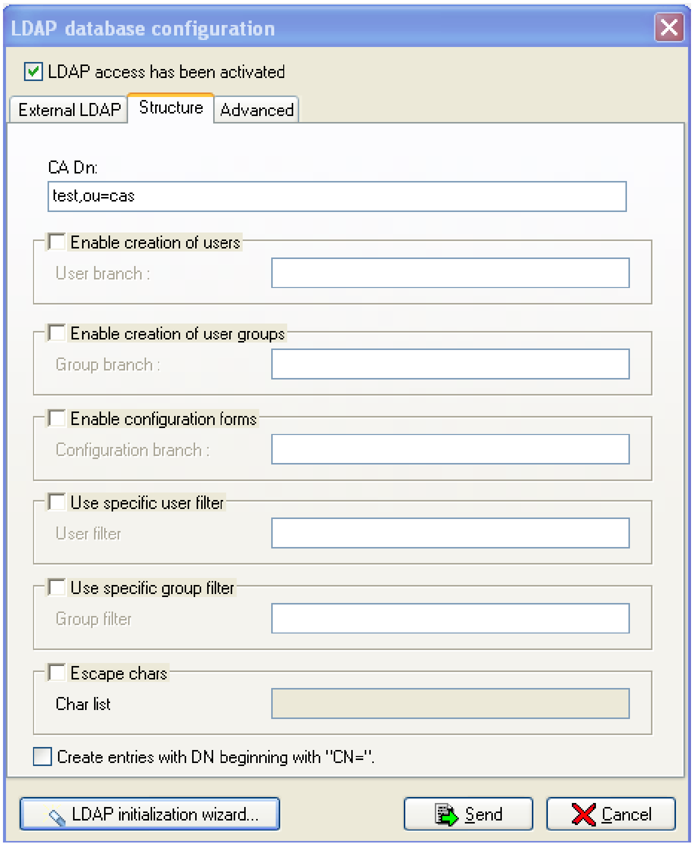
If your LDAP server has been configured to support SSL and you wish for the firewall to communicate with the server via SSL, you need to select the option "Activate SSL". As an option (by selecting "Trusted CA which signed the server certificate", and by selecting the file containing the authority certificate) you can send to the firewall the certificate of the authority that issued your server's certificate. This will allow checking the validity of the certificate presented by the LDAP server.

Configuring the LDAP base

Base Dn	Enter the root DN of your database (e.g.: o=NETASQ, dc=COM).
Login (cn)	User account that allows the firewall to connect to your LDAP server and to read/write certain fields. We recommend that you create a specific account for the firewall and to assign to it rights only for the fields that are necessary. (e.g.: cn=Admin Firewall NETASQ).

The button **Check LDAP** allows checking whether the external LDAP is accessible.

Structure tab



LDAP database configuration

☑ LDAP access has been activated

CA Dn:
test,ou=cas

□ Enable creation of users
User branch :

□ Enable creation of user groups
Group branch :

□ Enable configuration forms
Configuration branch :

□ Use specific user filter
User filter

□ Use specific group filter
Group filter

□ Escape chars
Char list

□ Create entries with DN beginning with "CN=".

Figure 369: Configuring the LDAP base - Structure

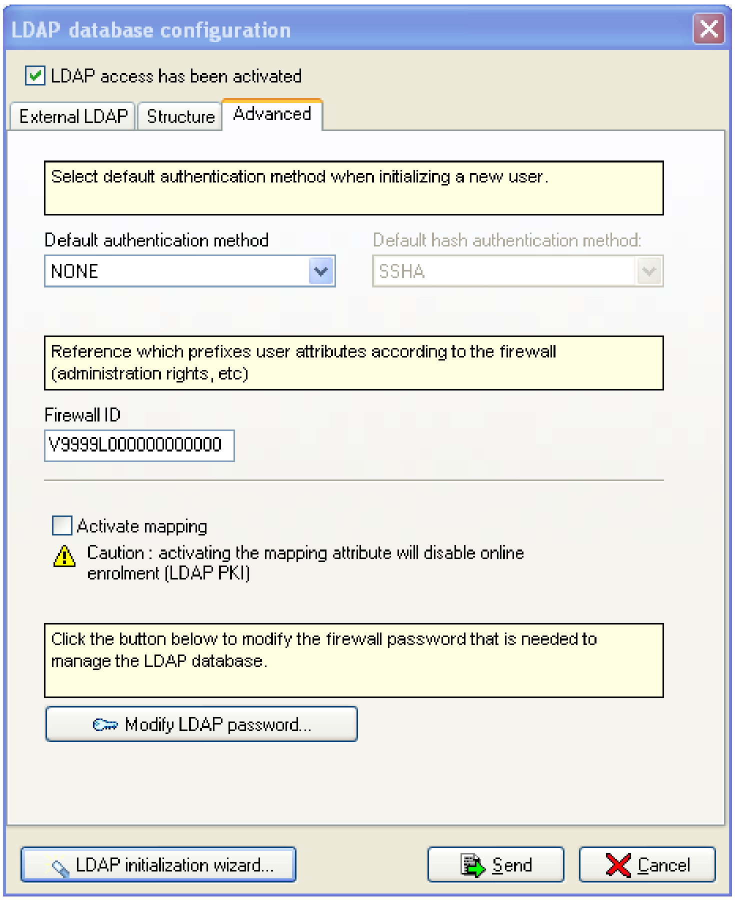
This tab is added when an external LDAP database or Active Directory is used.

The options for this tab allow you to add, in the external LDAP database or Active Directory, user entries created in objects configuration. Users and groups will each be stored in a specific branch of the LDAP database or Active Directory.

CA Dn	This field defines the location of the certification authority in the external LDAP database or Active Directory. This location is used particularly when searching the CA for the SSL authentication method. The configuration of this field is not totally necessary but in this case, to ensure that the SSL authentication method works, the CA has to be specified in the list of trusted CAs in the configuration of the SSL method (See "SSL authentication method").
Enable creation of users	Enter the name of the LDAP branch for storing users. Example: ou=users.
Enable creation of user groups	Enter the name of the LDAP branch for storing user groups. Example: ou=groups.
Enable configuration forms	Enter the name of the LDAP branch for storing configurations. Example: ou=configuration.
Use specific user filter	When the firewall is used in interaction with an external database, only users matching the filter will be used. By default this filter corresponds to ObjectClass = InetOrgPerson.

Use specific group filter	When the firewall is used in interaction with an external database, only groups matching the filter will be used. By default this filter corresponds to ObjectClass = GroupOfNames.
Escape characters	For certain external servers, a “\” has to be added so that LDAP requests can be understood.
Create entries with DN beginning with “CN=”	…

Advanced tab



☑ LDAP access has been activated

Select default authentication method when initializing a new user.

Default authentication method: NONE

Default hash authentication method: SSHA

Reference which prefixes user attributes according to the firewall (administration rights, etc)

Firewall ID: V9999L000000000000

□ Activate mapping

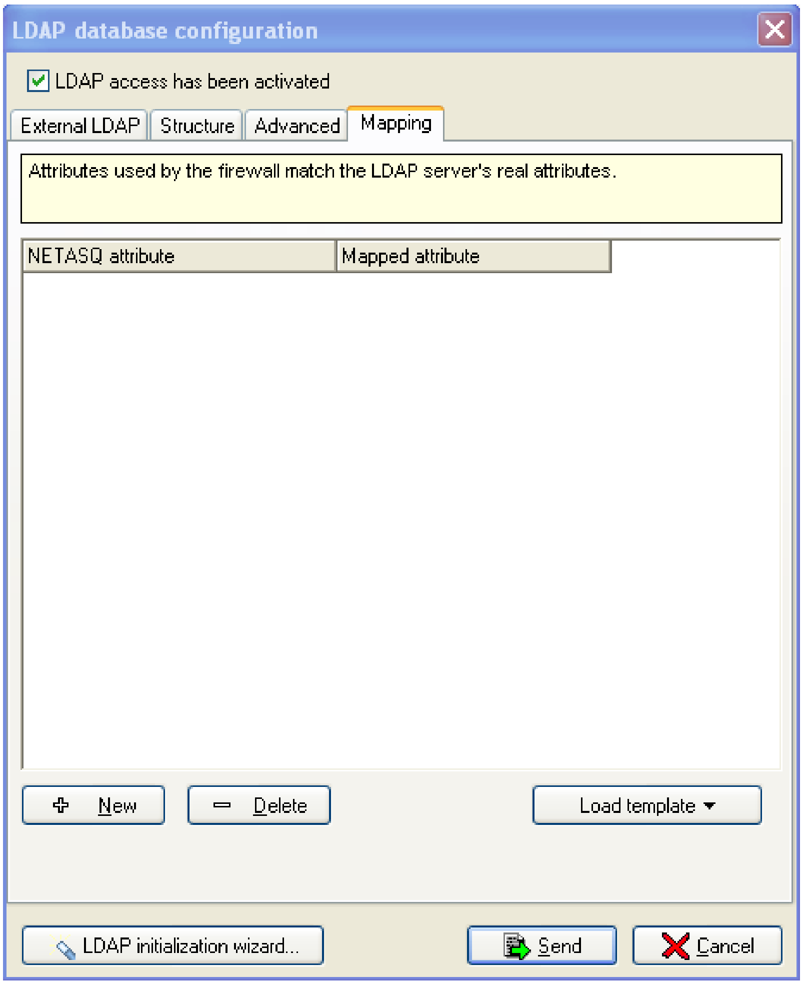
Caution : activating the mapping attribute will disable online enrolment (LDAP PKI)

Click the button below to modify the firewall password that is needed to manage the LDAP database.

Figure 370: Configuring the LDAP base – Advanced

The `Advanced` tab for configuring an external database has an additional option – **Activate mapping**. This option enables mapping (or matching) objects in the NETASQ LDAP schema, objects used by the firewall and objects from other databases. If this option has been selected, a new tab – `Mapping` – will appear.

Mapping tab



☑ LDAP access has been activated

Attributes used by the firewall match the LDAP server's real attributes.

NETASQ attribute	Mapped attribute

Figure 371: Configuring the LDAP base – Mapping attributes

This tab appears when an external LDAP database or Active Directory is used and the **Activate mapping** option in the `Advanced` tab has been selected (by default).

The options in this tab allow you to indicate matches in attributes used by NETASQ and those used in the external database.

For example: the NETASQ attribute <uid> = the Active Directory attribute <sAMAccountName>

You can add or delete mapped attributes using the **New** and **Delete** buttons.

Loading templates

This button allows you to specify a list of matches, already defined by NETASQ, with market solutions (Active Directory, OpenDirectory, etc).

PART 13: PKI

CHAPTER 1. PRESENTATION

13.1.1. What is a PKI?

DEFINITION
PKI or Public Key Infrastructure is a cryptographic system (based on asymmetrical cryptography). It uses signature mechanisms and certifies public keys (by associating a key to a user) which allow encrypting and signing messages as well as traffic in order to ensure confidentiality, authentication, integrity and non-repudiation.

These four notions (confidentiality, authentication, integrity and non-repudiation) are the bases of any security solution. However, they are not expanded upon in this document. If you feel the need to widen your knowledge on these concepts, you will be able to find out the necessary information in any generic work on security.

13.1.2. Principle

PKI is a system based on a confidence authority (your NETASQ Firewall, for instance) which signs and issues certificates containing a bi-key associated with information belonging to a user.

These certificates are electronic passports which are used to authenticate users. Furthermore, they contain encryption and decryption keys which guarantee data confidentiality.

13.1.3. Advantage of the PKI

A PKI is an additional security layer with regard to an authentication system “simply” based on an LDAP directory. The bi-key, certificate and confidence authority are used to secure exchanges on the internet.

The certificate is an alternative to logon systems as the user does not have to remember a password. The certificate’s portability allows its integration into solutions using USB keys, for example.

Likewise, a certificate can be used for VPN tunnels. It is no longer necessary to share a secret which is difficult to exchange away from the prying eyes of web users.

13.1.4. General

All NETASQ Firewalls have an internal PKI (except for U30 and U70 models), allowing you to create digital certificates for your users. These certificates can be used to authenticate users through the Firewall and for VPN authentication. They can also be used by your computer system’s applications.

This window can be accessed via the **`PKI\General`** sub-menu. It allows you to view and configure your PKI after its initialization.

It comprises two sections:

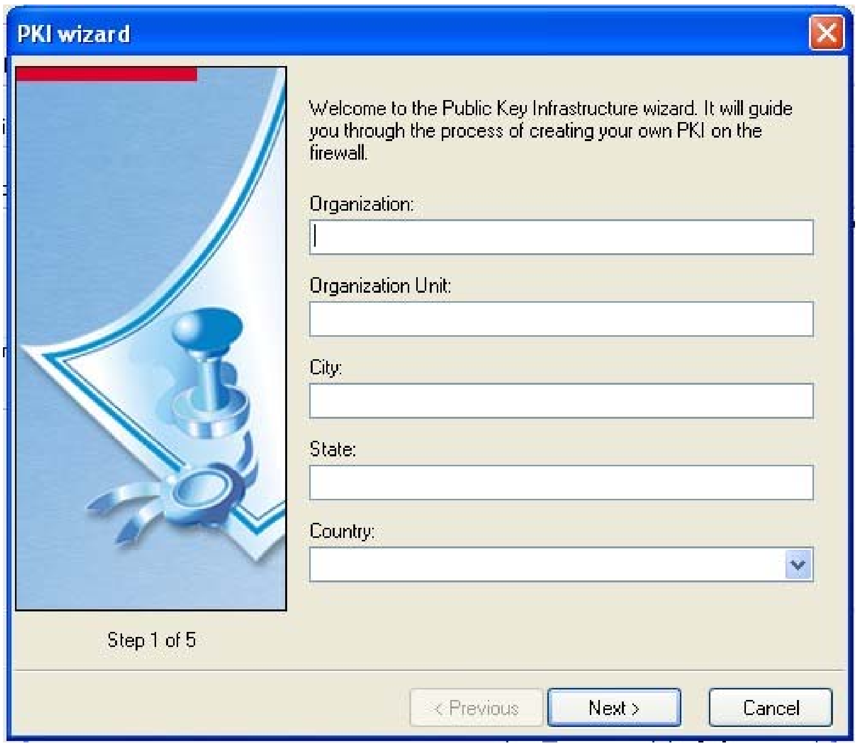
- a tab zone and the window corresponding to the tab chosen. The available tabs allow you to view your configuration information, modify certain options or view information on your PKI,
- a zone at the bottom with two buttons allowing you to send your changes to the Firewall or to exit this window without applying the changes.

When you access this section for the first time you must configure the PKI using the PKI wizard.

CHAPTER 2. PKI WIZARD

This Wizard automatically launches the first time the **`PKI\General`** sub-menu is accessed or when you click on the **PKI creation wizard** button on the general configuration screen.

Step 1: Welcome



PKI wizard

Welcome to the Public Key Infrastructure wizard. It will guide you through the process of creating your own PKI on the firewall.

Organization:

Organization Unit:

City:

State:

Country:

Step 1 of 5

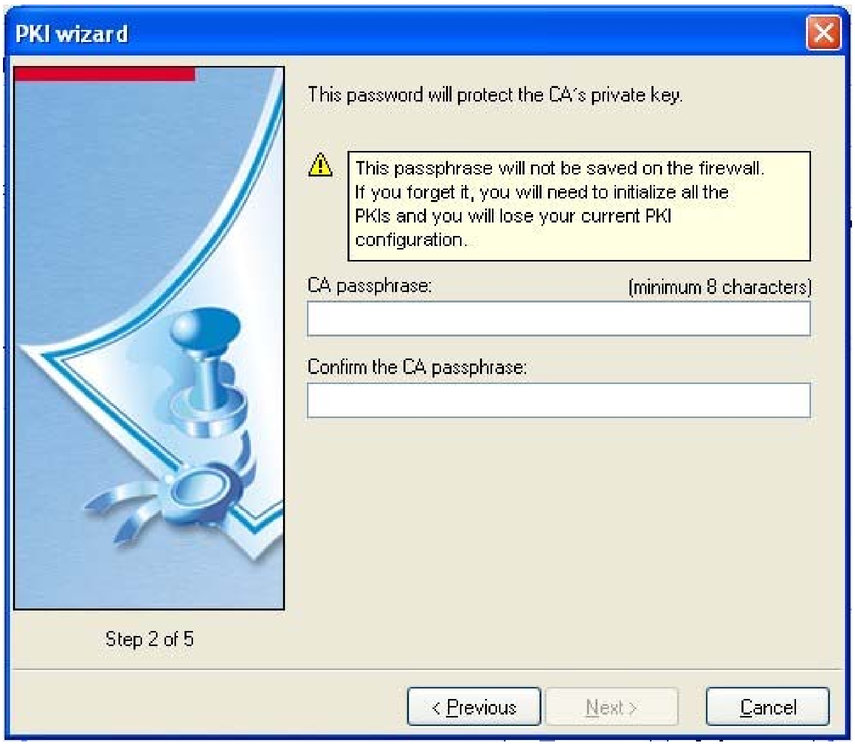
Figure 372: PKI wizard - Step 1

At this initial stage you must provide the general data concerning the PKI you want to use. These data can be found in the certificate issued by your certification authority and in your users' certificates.

Organization	Your company's name (e.g.: NETASQ)
Organization unit	Your company branch (e.g.: INTERNAL)
Locality	City where your company is located (e.g.: Villeneuve d'Ascq)

State	State in which your company is located (e.g.: Nord).
Country	Your country's ISO code (e.g.: FR)

2 Step 2: Password



This password will protect the CA's private key.

This passphrase will not be saved on the firewall. If you forget it, you will need to initialize all the PKIs and you will lose your current PKI configuration.

CA passphrase: (minimum 8 characters)

Confirm the CA passphrase:

Step 2 of 5

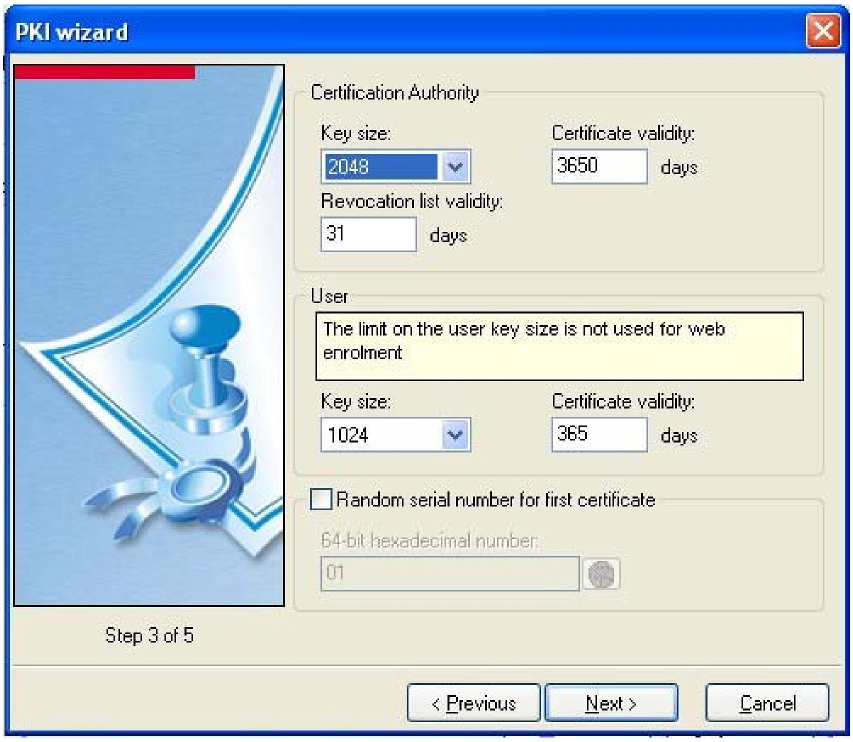
Figure 373: PKI wizard - Step 2

In the second stage of the PKI configuration wizard you must provide a password (min. 8 characters) to protect the private key of your certification authority.
The Admin account can delete the existing PKI without having to entere a password. However, other administration accounts will need to enter this password. This enables recreating a new PKI if the password is lost.

WARNING
Do not choose a password which is too easy. We recommend that you combine upper and lower case letters, numbers and special characters.

The initialization of the PKI may take some time, as the internal certification authority will also be generated.

3 Step 3: Certification authority, user, key size



PKI wizard

Certification Authority

Key size: 2048

Certificate validity: 3650 days

Revocation list validity: 31 days

User

The limit on the user key size is not used for web enrolment

Key size: 1024

Certificate validity: 365 days

□ Random serial number for first certificate

64-bit hexadecimal number: 01

Figure 374: PKI wizard - Step 3

In the third step of the PKI configuration wizard, you have to enter the configuration concerning your PKI's cryptographic hardware.

This step has two parts:

- Configuration of cryptographic hardware for the certification authority
- Configuration of cryptographic hardware for users.

Crytographic hardware for the certification authority

Key size: your authority's key size in bits. This value cannot be changed later. The greater the size, the higher the security.

Certificate validity: the number of days during which your authority certificate and consequently your PKI will be valid. This date affects all aspects of your PKI. Once it has expired all the user certificates expire with it. This value cannot be changed later

Revocation List validity: the number of days during which your CRL will be valid.

WARNING
It is usual for your CRL to be updated regularly, therefore its validity date should not be too long. It can be changed later.

Cryptographic hardware for users

Key size: your users' key size in bits. This value can be changed later.

Certificate validity: the number of days during which the users' certificates will be valid. This value can be changed later.

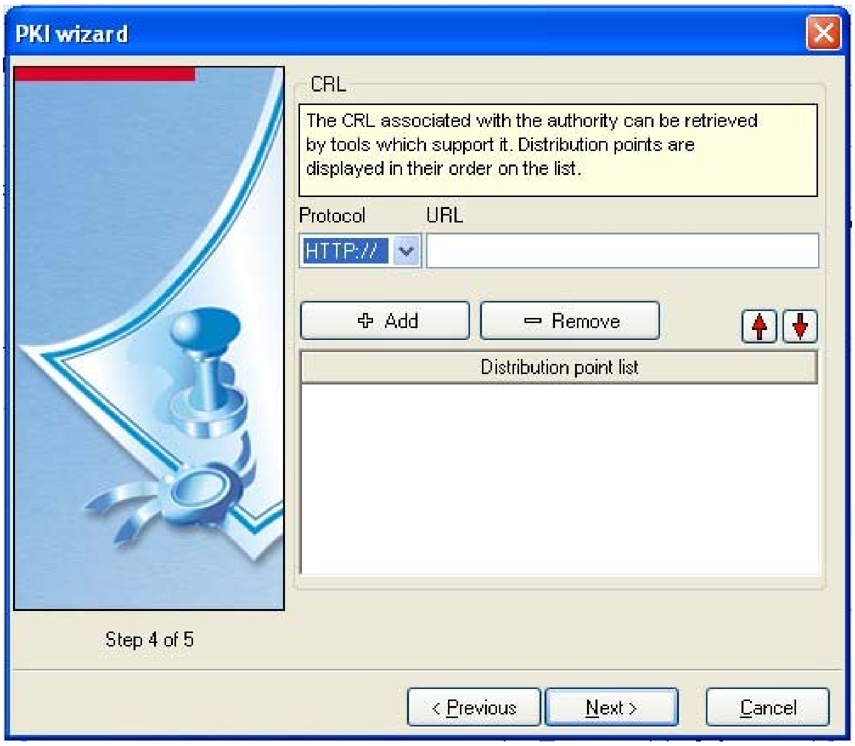
Random serial number for first certificate

This feature enables manually or randomly defining the first number of the certificate that the PKI generates, therefore preventing a third party from finding out how many certificates the PKI has generated.

> **Example**
> If the first number is 10245 and the administrator generates 15 certificates, the fifteenth certificate will bear the number 10259, and there is no way of finding out if indeed 10259 certificates had been generated.

The field **64-bit hexadecimal number** enables specifying the number of the first certicate generated in the form of a 64-bit hexadecimal number. The button with the symbol of a die generates this number randomly.

4 Step 4: CRL



PKI wizard

CRL

The CRL associated with the authority can be retrieved by tools which support it. Distribution points are displayed in their order on the list.

Protocol: HTTP://
URL:

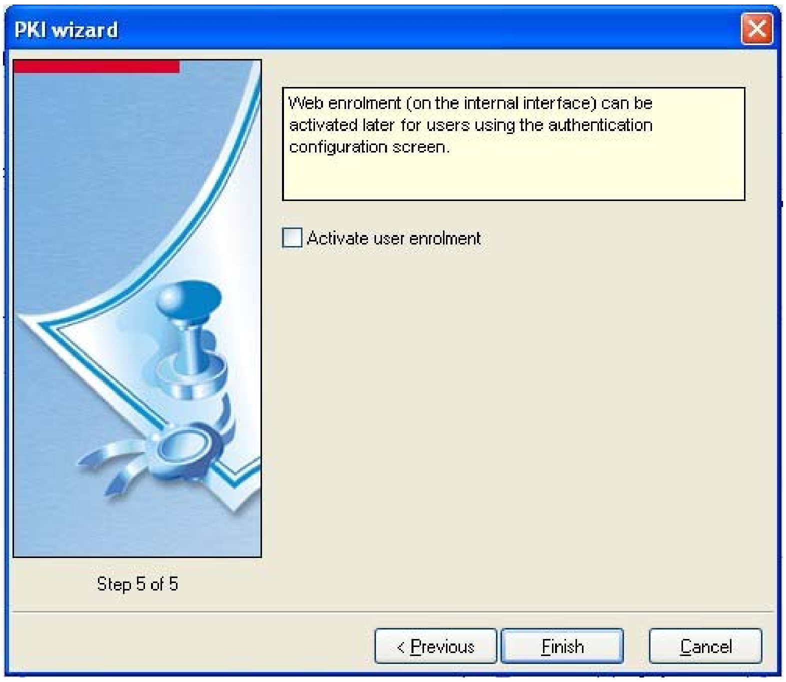
Figure 375: PKI wizard - Step 4

In this step of the PKI configuration wizard, you have to enter the configuration concerning CRL distribution. This information will be incorporated in the certificates generated and will allow applications using this certificate to automatically retrieve the CRL so as to check the certificate's validity.

When using an internal PKI, it is highly recommended to export the NETASQ CA and CRL to a web server (see the ***Authority*** tab) and to specify the URL of both these files stored on the web server. This operation should be performed regularly so that the CRL on the web server is as up to date as possible. When the **Protocol** and **URL** fields have been entered, you must click on **Add** to create the distribution point.

Protocol	Protocol used for CRL distribution
URL	Address of the CRL distribution point
Distribution point list	List of all distribution points configured with the two fields above.

5 Step 5: User enrolment



Web enrolment (on the internal interface) can be activated later for users using the authentication configuration screen.

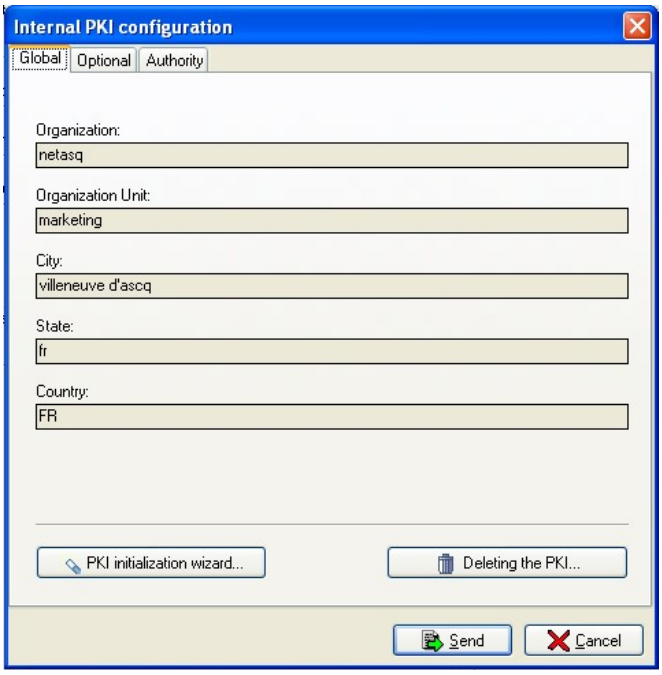
□ Activate user enrolment

Figure 376: PKI wizard - Step 5

In the last step of configuring the NETASQ PKI, only user enrolment needs to be specified using the **Activate user enrolment** option.

CHAPTER 3. CONFIGURING THE PKI

13.3.1. Global tab



Internal PKI configuration

Organization: netasq

Organization Unit: marketing

City: villeneuve d'ascq

State: fr

Country: FR

Figure 377: Configuring the internal PKI - Global

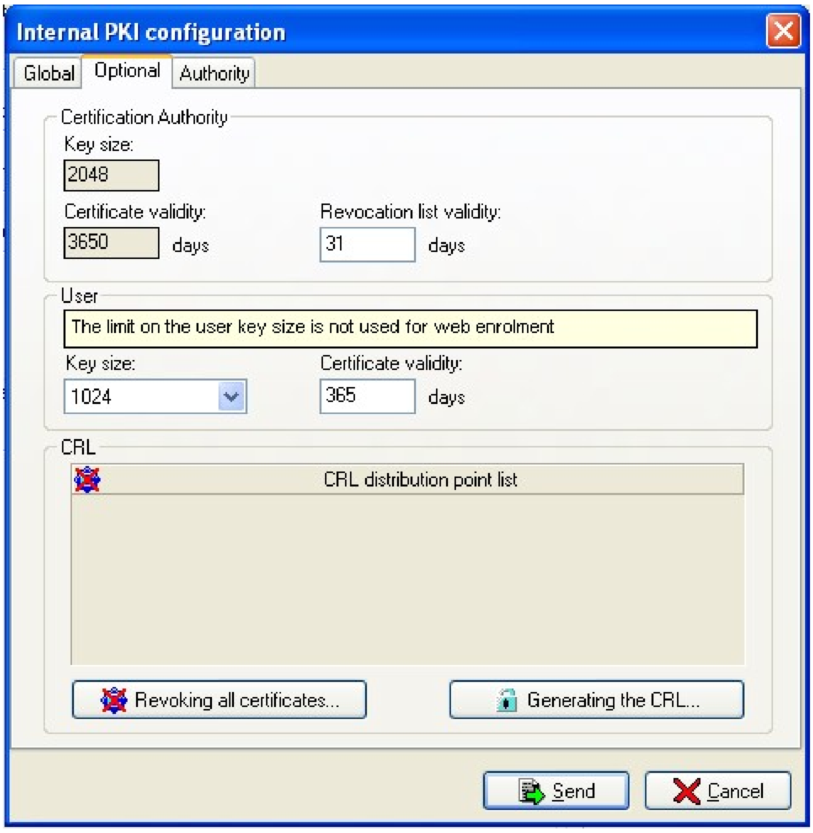
This window comprises three sections:

- A zone showing the current configuration of the PKI. The information displayed is the same as the information entered in the first step of the PKI initialization wizard.
- A zone with 2 buttons allowing the initialization of a new PKI (destroys the current PKI) and the destruction oof the current PKI.
- A zone at the bottom right containing two buttons that allow you to send changes to the firewall or to exit this window without applying the changes.

WARNING

The "admin" account allows you to delete a PKI without having to indicate the certificate authority’s password. Therefore, even if the administrator has forgotten his password, he will be able to delete a PKI.

13.3.2. Options tab



Internal PKI configuration

Global | Optional | Authority

Certification Authority

Key size: 2048

Certificate validity: 3650 days

Revocation list validity: 31 days

User

The limit on the user key size is not used for web enrolment

Key size: 1024

Certificate validity: 365 days

CRL

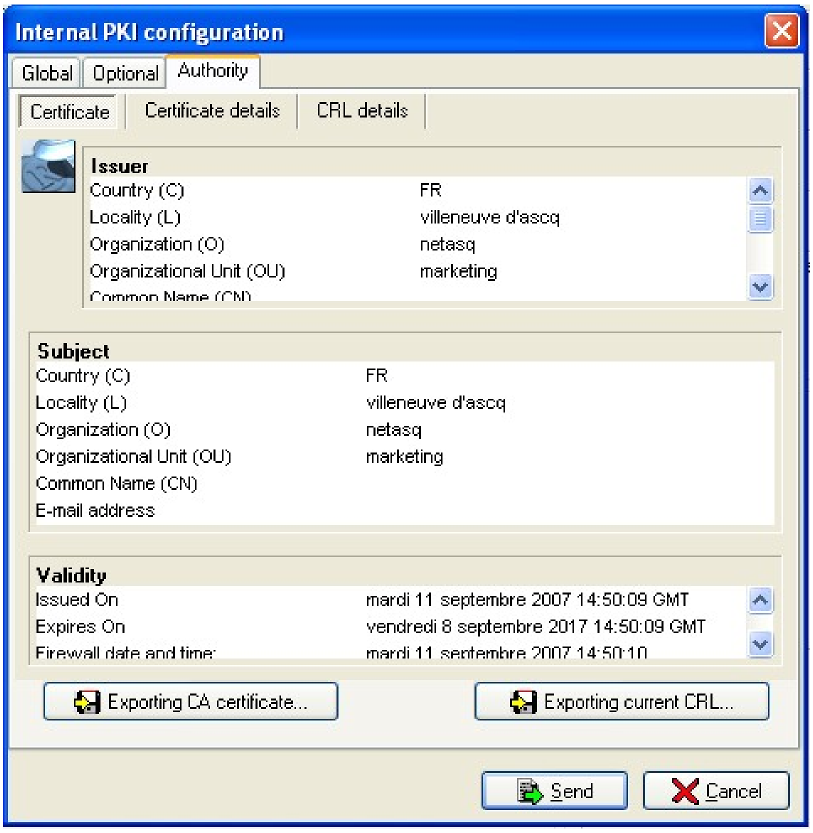
CRL distribution point list

Figure 378: Configuring the internal PKI - Optional

This tab comprises five parts:

- An information zone on the configuration of the cryptographic hardware for the certificate authority. The data displayed is that given in the second step of the PKI initialization wizard. The validity period of the CRL can be modified.
- An information zone on the configuration of the cryptographic hardware for users. The data displayed is that given in the second step of the PKI initialization wizard. The fields in this zone can be modified. PKI.
- A zone providing information on CRL distribution points
- A zone with two buttons: to revoke all the users' certificates (in this case they will be unusable) and to generate a new CRL.
- A zone (bottom right) with two buttons to enable you to send your changes to the Firewall or to exit the window without applying them.

13.3.3. Authority tab



Issuer

Country (C)	FR
Locality (L)	villeneuve d'ascq
Organization (O)	netasq
Organizational Unit (OU)	marketing
Common Name (CN)	

Subject

Country (C)	FR
Locality (L)	villeneuve d'ascq
Organization (O)	netasq
Organizational Unit (OU)	marketing
Common Name (CN)	
E-mail address	

Validity

Issued On	mardi 11 septembre 2007 14:50:09 GMT
Expires On	vendredi 8 septembre 2017 14:50:09 GMT
Firewall date and time:	mardi 11 septembre 2007 14:50:10

Figure 379: Configuring the internal PKI - Authority

This tab comprises three parts:

- A zone with three options which enable you to obtain: A general view of the certificate's contents (**Certificate** tab). The complete contents of the certificate (**Certificate details** tab). The complete contents of the CRL (**CRL details** tab). You can see the certificates which have been revoked.
- A zone with two buttons which enable you to export the certification authority's certificate in **.DER** format and export the certification authority's CRL in **.CRL** format
- A zone (bottom right) with two buttons to enable you to send your changes to the Firewall or to exit the window without applying them.

CHAPTER 4. LIST OF USER REQUESTS

When authentication is activated the user must go through a recognition phase before trying to connect through the Firewall. Two circumstances might arise:

13.4.1. URL filtering has been activated on the Firewall

When URL filtering and authentication are activated on the Firewall the user does not need to access the Firewall for authentication. The authentication page will be sent to him automatically when he wants to access a web site. The user will therefore be authenticated for all the services for which he is authorized during the whole authentication period.

13.4.2. URL filtering has not been activated on the Firewall

In this case the user must be authenticated on the Firewall before trying to make a connection which requires authentication. The user must connect to the Firewall via his Internet navigator and the URL to be used is the following: https:\\<Firewall's IP address>

> **Example**
>
> https://10.0.0.254

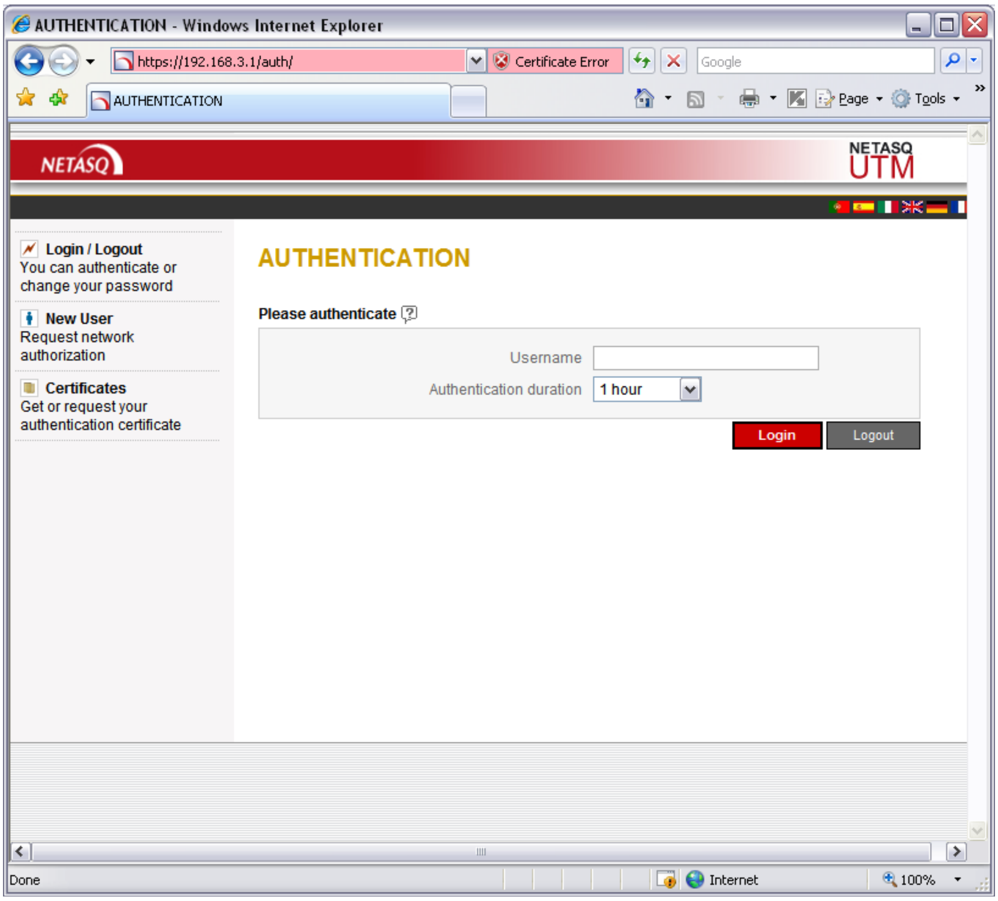
13.4.3. The administrator's missions

The administrator vouches for the proper use of authentication features that equipment from his network offers, particularly the NETASQ Firewall. NETASQ takes this opportunity to remind users that increasing user awareness on the use of authentication pages enables limiting improper use.

This awareness comprises:

- help in defining passwords which have a high random factor (See *Part 13/Chapter 6: User Awareness*).
- training on the use of features found on the authentication pages.
- creating awareness of the stakes on resource, asset and personal security.

13.4.4. Login



Login / Logout
You can authenticate or change your password

New User
Request network authorization

Certificates
Get or request your authentication certificate

AUTHENTICATION

Please authenticate

Username:

Authentication duration: 1 hour

Login Logout

Figure 380: Portal authentication

For authentication in both cases the user must then enter his login and the period during which he wants to be authenticated, then click on “Login. When this period has elapsed he must seek re-authentication.

> **WARNING**
> Do not specify too long a time period (the user might leave his terminal without locking it and his session might be intercepted).

Depending on the method chosen the user must either enter his password or choose a digital certificate.

- **For the LDAP method:** enter the password
- **For the certificate method (SSL):** choose a certificate (this certificate has to be installed beforehand on the user’s computer),
- **For the SRP method:** enter the password (a Java applet will be launched and will allow the DNS name to be used instead of the firewall’s IP address. Therefore, authentication is now possible even when the NETASQ UTM’s IP address is different from the IP address that the browser receives.

> **WARNING**
> Using SRP involves the installation of a JVM (*Java Virtual Machine*) on the user’s computer (most web browsers integrate such a virtual machine). Sun’s JVM (version 1.4) is highly recommended.

13.4.5. Logout

To log off you must access the Firewall in HTTPS (see above) enter the user login and then click on **Logout**. The user must enter his password again in order to log off (to prevent users from logging off other users).

> **WARNING**
> When a user leaves his workstation before the end of the authentication period, he has to log out so that his session does not get intercepted.

13.4.6. Changing passwords

The user can remotely change his authentication password. He needs only to enter the login and Click on **Changez votre password**.

Now he only needs to change his password.

> **NOTE**
> Changes to the password will not be applied for SSL authentication with certificates or for authentication with an external RADIUS server.

CHAPTER 5. USER ENROLMENT

When an authentication service is set up, each authorized user has to be defined by creating a "user" object (see *Part 4: Objects*). The larger the company, the more demanding the task. NETASQ's web enrolment service makes this task easier. Now, it is the "unknown" user who requests the creation of his account and certificate (if a PKI has been defined by the administrator).

13.5.1. User requests

When the administrator has specified the "Enable web enrolment" option in the authentication global setup (see *Part 12: Authentication*), the enrolment service will be activated. The web authentication portal also contains a "New user" button.

By clicking on **New user**, the user will be able to access the enrolment menu and can therefore send in his enrolment request.

Depending on the enrolment method (LDAP or LDAP and PKI), there are different fields to fill in:

First name	User's first name (mandatory field).
Last name	User's last name (mandatory field).
E-mail address	E-mail address (mandatory field)
Description	Brief description of the user.
Telephone number	Telephone number
Password	User's password for authentication.
Confirm password	Confirmation of password.
Cryptographic Service Providers	User's private key size (only in LDAP and PKI enrolment).

13.5.2. Request management

When a user has sent out a request, the administrator can manage these pending requests. Two menus are used for request management:

- **User Request List:** manages requests for user account creation, this list is accessible via the **`Authentication\User Request List`** menu,
- **Certificate Request List:** manages requests for certificate creation, this list is accessible via the **`PKI\Certificate Request List`** menu.

Configuration options for these two menus are almost the same.

13.5.2.1. Request validation and rejection

When you access the **`User Request List`** menu (or the **`Certificate Request List`** menu), the request management window appears.

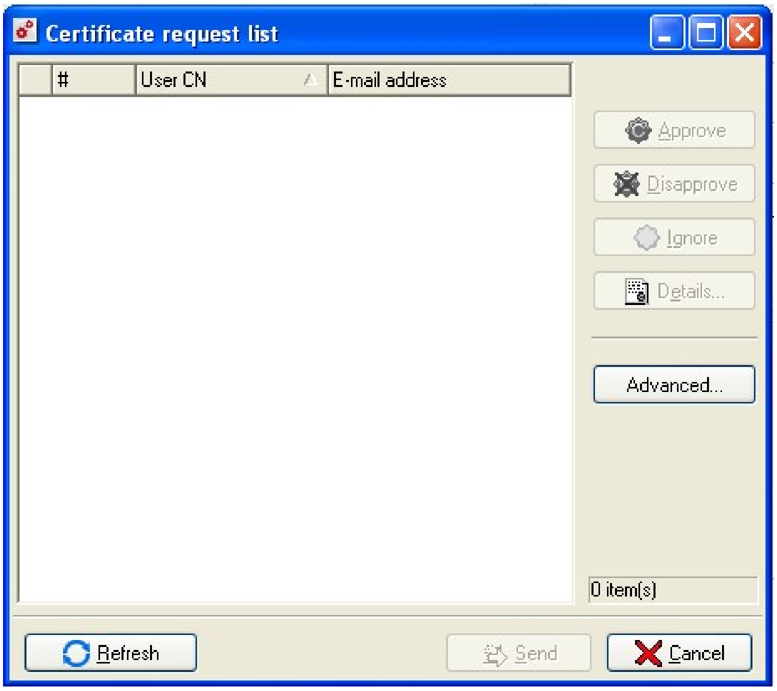


Figure 381: Certfiicate request list

This screen comprises two sections:

- On the left, the list of pending requests,
- On the right, actions which can be carried out.

Approve	This button allows you to approve the user's request.
Reject	This button allows you to reject the user's request.
Ignore	This button allows you to ignore the user's request.
Details	This button allows you to view the details of the user's request.
Advanced	This button allows you to access to web enrolment options.

Any action performed in this window is only validated when you click on **Send**. If you accidentally validate (or reject) a request, you can use the **Ignore** button to put the user request on hold again.

13.5.2.2. Requests options

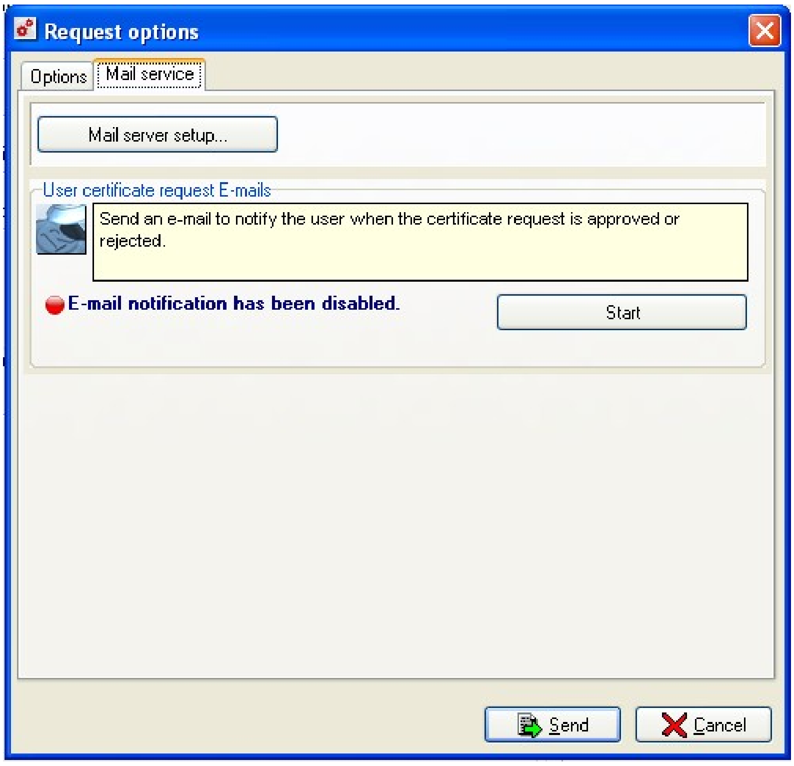
Clicking on **Advanced** in the **`User Request List`** (or **`Certificate Request List`**) menu gives you access to the configuration menu for request options. This window comprises three tabs:

- **Options**: configuration of general options for enrolment:

DEFINITION

1) **Format string**: configuration for this string is explained in the application
2) **Automatically approve certificate request**: (only in the **`User Request List`** menu): this option allows you to automatically validate certificate requests. When the administrator validates the request for the creation of a user account, the application will automatically validate the creation of the certificate associated to this user.

- **Mail Service:** activates the automatic sending of responses to requests. You can only launch this service if you have activated the sending of alarm notifications in the **ASQ** menu beforehand. This option enables sending an e-mail to the user to tell him whether his request has been validated and that he may authenticate or obtain his certificate.



Send an e-mail to notify the user when the certificate request is approved or rejected.

E-mail notification has been disabled.

Figure 382: Request options

When the administrator has validated the user's request, the user can authenticate on the Firewall to enjoy services to which he has access. He is informed of this validation by e-mail if the e-mail service has been activated.

When the request for the creation of a certificate has been validated, the user may obtain his certificate:

- either on the Firewall (default) at **https:\\< firewall's address>** by clicking on the "**Certificates**" button on the page,
- or at the address specified by the administrator on an external post.

CHAPTER 6. USER AWARENESS

The Firewall administrator is in charge of instructing users on network security, the equipment which make up the network and the information which passes through it.

Most users in a network are computer novices and even more so in network security. It is thus incumbent upon the administrator or person in charge of network security to organize training sessions or at least programs to create user awareness of network security.

These sessions should be used to state the importance of managing user passwords and the work environment as well as the management of users' access to the company's resources.

13.6.1. User password management

Throughout the evolution of information technologies, numerous authentication mechanisms have been invented and implemented to guarantee that companies' information systems possess better security. The result of this multiplication of mechanisms is a complexity which contributes to the deterioration of company network security today.

Users (novices and untrained users) tend to choose "simplistic" passwords, in general drawn from their own lives and which often correspond to words found in a dictionary. This behavior, quite understandably, leads to a considerable deterioration of the information system's security.

Dictionary attacks being an exceedingly powerful tool is a fact that has to be reckoned with. A study conducted in 1993 has already proven this point. The following is a reference to this study: (**http://www.klein.com/dvk/publications/**). The most disturbing revelation of this study is surely the table set out below (based on 8-character passwords):

Type of password	Number of characters	Number of passwords	Cracking time
English vocabulary 8 char. and +	Special	250000	< 1 second
Lowercase only	26	208827064576	9 hours
Lowercase + 1 uppercase	26/special	1670616516608	3 days
Upper- and lowercase	52	53459728531456	96 days
Letters + numbers	62	218340105584896	1 year
Printable characters	95	6634204312890620	30 years
Set of 7-bit ASCII characters	128	72057594037927900	350 years

Another tendency which has been curbed but which is still happening is worth mentioning: those now-famous post-its pasted under keyboards.

The administrator has to organize actions (training, creating user awareness, etc) in order to modify or correct these "habits".

> **Example**
>
> - encourage your users to choose passwords which exceed 7 characters,
> - remind them to use letters and uppercase characters,
> - make them change their passwords on a regular basis,
> - and last but not least, never to note down the password they have just chosen.

One classic method of choosing a good password is to choose a sentence that you know by heart (a verse of poetry, lyrics from a song) and to take the first letter of each word. This set of characters can then be used as a password. For example:

- "**N**ETASQ, **L**eading **F**rench **m**anufacturer **o**f **F**IREWALL **a**nd **V**PN **a**ppliances…"

The password can then be the following: **NLFmoFaVa**.

13.6.2. Work environment

The office is often a place where many people pass through everyday, be they from the company or visitors, therefore users have to be aware of the fact that certain persons (suppliers, customers, workers, etc) can access their workspace and by doing so, obtain information about the company.

It is important that the user realizes that he should never disclose his password either by telephone or by e-mail (social engineering) and that he should type his password away from prying eyes.

13.6.3. User access management

To round up this chapter on creating user awareness of network security, the administrator has to tackle the management of user access. In fact, a NETASQ Firewall's authentication mechanism, like many other systems, is based on a login/password system and does not necessarily mean that when the application enabling this authentication is closed, the user is logged off. This observation may not always be apparent to the uninitiated user. As such, despite having shut down the application in question, the user (who is under the impression that he is no longer connected) remains authenticated. If he leaves his workstation for just a moment, an ill-intentioned person can then usurp his identity and access information contained in the application.

Remind users to lock their sessions before they leave their workstations unattended. This seemingly tedious task can be made easier with the use of authentication mechanisms which automate session locking (for example, a USB token).

PART 14: HIGH AVAILABILITY

14.1.1. Introduction

14.1.1.1. For this chapter, you will need to have completed these steps

- *Part 2: Installation, pre-configuration, integration*.
- Requested activation keys from NETASQ for high availability,

14.1.1.2. For this chapter, you will need to know

- The company's security policy
- The password for the "HA" user.
- The IP address you want to assign to each high availability interface

14.1.1.3. Purpose of this section

This part allows you to configure the high availability feature. This feature can only be used if you possess two Firewalls.

The principle is to switch the connections on the active Firewall to the second (passive) Firewall, if there is a dysfunction on the active Firewall.

14.1.1.4. Accessing this section

➲ You can access the dialog box via the menu **`Firewall\High availability`**.

You have to possess two Firewalls and be connected with modification privileges in order to make these changes.

14.1.2. Licenses

You must have two Firewalls in order to use the high availability option.

You must ask NETASQ for two special activation keys (one for each Firewall) and they must be installed using the graphical interface (See *Part 19/Chapter 1: Miscellaneous actions\License*).

14.1.2.1. Main/Backup notion

One of the two Firewalls is regarded as the main and the other as the backup (the status of each Firewall will be determined by the activation key installed).

The main-backup distinction operates in the following cases:

- If both Firewalls start up simultaneously
- If the status of both Firewalls is the same (following a communication breakdown in the Ethernet interface, for example),
- To differentiate the IP addresses assigned to each side of the high availability link.

> ❗ **WARNING**
> Watchdog and High availability options are only installed on Firewalls produced or returned to the After-Sales Department after October 2001. If your Firewall is older you can still benefit from these options. However, in this case the Firewall must be returned to NETASQ for modification.

14.1.3. Operation

No network element is safe from the risk of breakdown so high availability (or fault resilience) operations on NETASQ Firewalls ensure continued service even if there is a malfunction on a firewall.

This option calls for the use of two Firewalls which the network treats as a single entity. They have the same configuration but only one is active at any given moment (a single Firewall manages the connections). The second is only activated when the first is no longer in normal operational mode (active connections will be reactivated after the reboot.)

The passive Firewall’s network interfaces are deactivated and are only reactivated automatically when the Firewall is active once more.

High availability communications (activity tests, configuration transfers...) can use an Ethernet connection. One or two network interfaces therefore have to be assigned on each appliance and both interfaces have to be linked via Ethernet links. You can either dedicate these interfaces to high availability or configure high availability based on VLANs.

The Ethernet link

NETASQ has chosen not to support high availability on the serial link anymore as throughput on serial links was insufficient for the information databases to be duplicated between both Firewalls. In the case of the Ethernet link, throughput is much higher and the configuration transfer time is shorter and updating the LDAP database is faster.

> ❗ **WARNING**
> With the high availability function, it is recommended to use an external authentication database, in order to avoid internal LDAP databases replications between Firewalls.
>
> It is possible to install Firewalls in different locations.

High availability on VLANs

High availability on VLANs enable using the Ethernet link as the control link between both Firewalls in high availability without having to dedicate this interface. Now that high availability is supported on VLANs, the control interface can then be used to create a DMZ, for example.

14.1.3.1. Firewall operation test

The passive Firewall is tested by pings (sent over the Ethernet cable connecting the two Firewalls) if the active Firewall is operating. These tests are carried out regularly every T seconds (T being defined by the NETASQ UNIFIED MANAGER, see 'Installation' section). If there is no reply to a certain number of pings (the number can be set by NETASQ UNIFIED MANAGER) the Firewall is regarded as 'frozen', i.e. it no longer responds. In this case the passive Firewall becomes active and manages the connections.

In addition to the pings the Firewalls are cross-tested:

- Each Firewall (active or passive) regularly ascertains the status of the other in order to detect when two Firewalls are active (when the serial cable has been disconnected). In this case, the main Firewall remains active and the backup becomes passive.
- If the active Firewall has fewer Ethernet boards in operation than the passive Firewall (malfunction of a board) it will be switched into the passive mode and the passive will become active.
- If the active Firewall does not respond an "HA: Firewall failure" alarm will be sent.
- If two control links have been configured, the firewalls will first check their connectivity through the first control link. If this link has been broken, the second control link will be tested before there is an actual switchover.

14.1.3.2. High availability on two control links

NETASQ's high availability configuration is viable only if both appliances forming part of a high availability cluster are not activated simultaneously at any given moment. Indeed, in the event both appliances are activated at the same time, grave network problems will arise as each appliance has the same IP and MAC addresses as its high availability peer.

To alleviate this network problem, both control links can be configured in such a way that if connectivity between two high availability peers cannot be established on the first control link (loss of an interface, dead link, etc), it will be tested on the second control link before activating the passive firewall.

Specificity of the second control link

The first control link is in charge of not only verifying connectivity between both appliances in a high availability cluster, but also of synchronizing information between the active and passive appliances (synchronization of the configuration, exchange of operation tables, etc). While the second control link only enables the verification of connectivity between both appliances, it enables the prevention of unnecessary switchovers (passive to active) on the passive appliance.

14.1.4. Installation

Before reading this chapter you must read the chapter on **Licenses** and you must have installed the two activation keys.

14.1.4.1. Installation

The procedure for installing a high availability architecture is as follows:

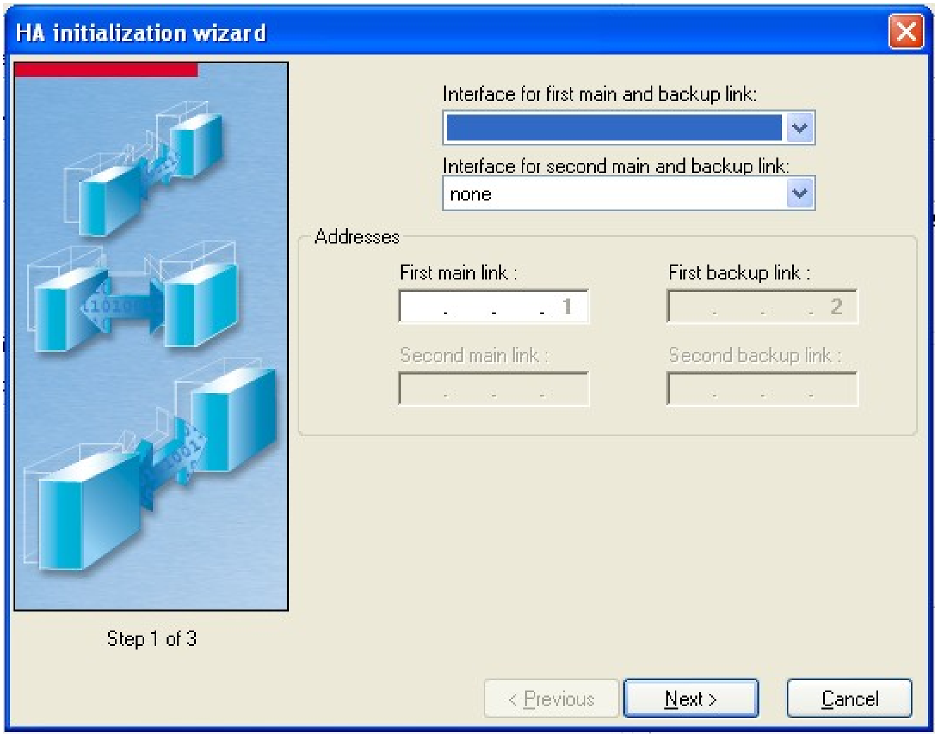
1 Both Firewalls must be disconnected from the local network (if not, there may be problems regarding conflicting addresses) but left on.

2 Connect to the backup Firewall by changing the IP address of the bridge (for example, take the address 10.0.0.253). It is essential that this address is different from that of the main Firewall. The Firewall must be rebooted.

3 Link the two Firewalls with the Ethernet cable.

4 Connect to the main Firewall. A wizard will guide you in the configuration of the high availability feature (HA initialization wizard button).

1 **Step 1**



HA initialization wizard

Interface for first main and backup link:

Interface for second main and backup link: none

Addresses

First main link : . . . 1

First backup link : . . . 2

Second main link : . . .

Second backup link : . . .

Step 1 of 3

Figure 383: HA wizard - Step 1

Choose the high availability interface (for main and backup) and the main Firewall's IP address (backup's IP address = main's IP address +1). If a VLAN interface has been configured, it can be used for high availability. In this case, the Ethernet interface to which the VLAN interface is attached is no longer dedicated to high availability.

Second control link

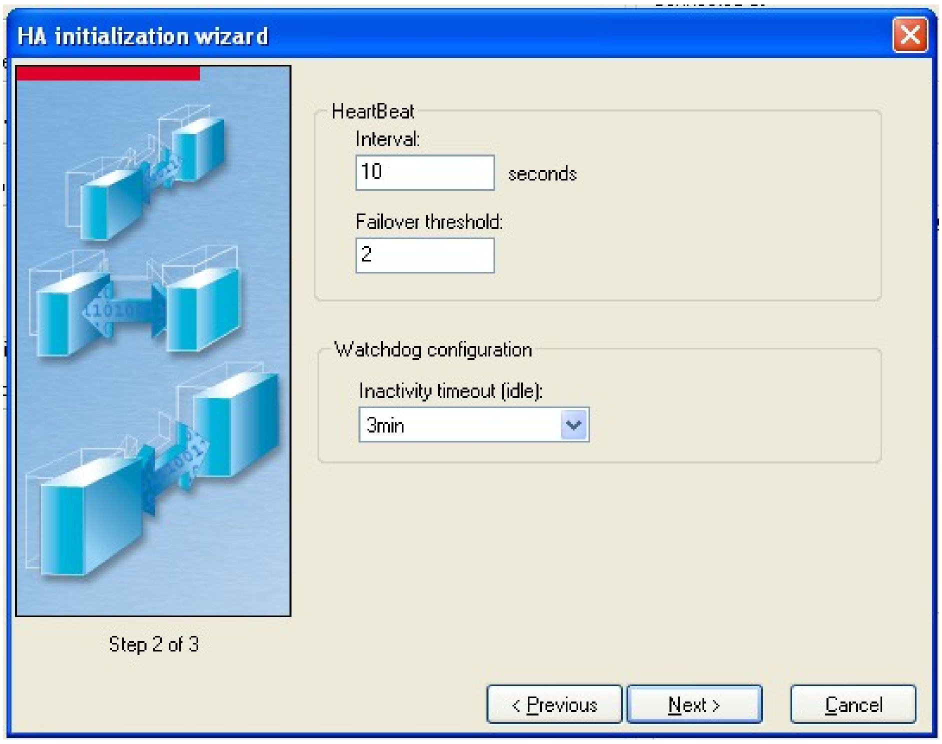
Two control links can be configured using the high availability configuration wizard. This second control link is only used for testing the existing connectivity between two appliances forming a high availability cluster.

High availability interface addresses

In Step 1, the address range used by the interfaces on the appliances participating in the control link will be defined. The wizard will allow you to define the network address, but it will assign the addresses for each interface.

Note that any address range can be defined. However, if you define a "public" address range, it will be impossible to reach websites that use this address range. You are advised to use a private address range (one that is different from the range used by the other interfaces).

2 Step 2



HA initialization wizard

HeartBeat

Interval: 10 seconds

Failover threshold: 2

Watchdog configuration

Inactivity timeout (idle): 3min

Step 2 of 3

Figure 384: HA wizard - Step 2

You can specify the time between two pings in the 'interval' field as well as the accepted number of pings without response (failover threshold) before the active Firewall is switched to the passive Firewall

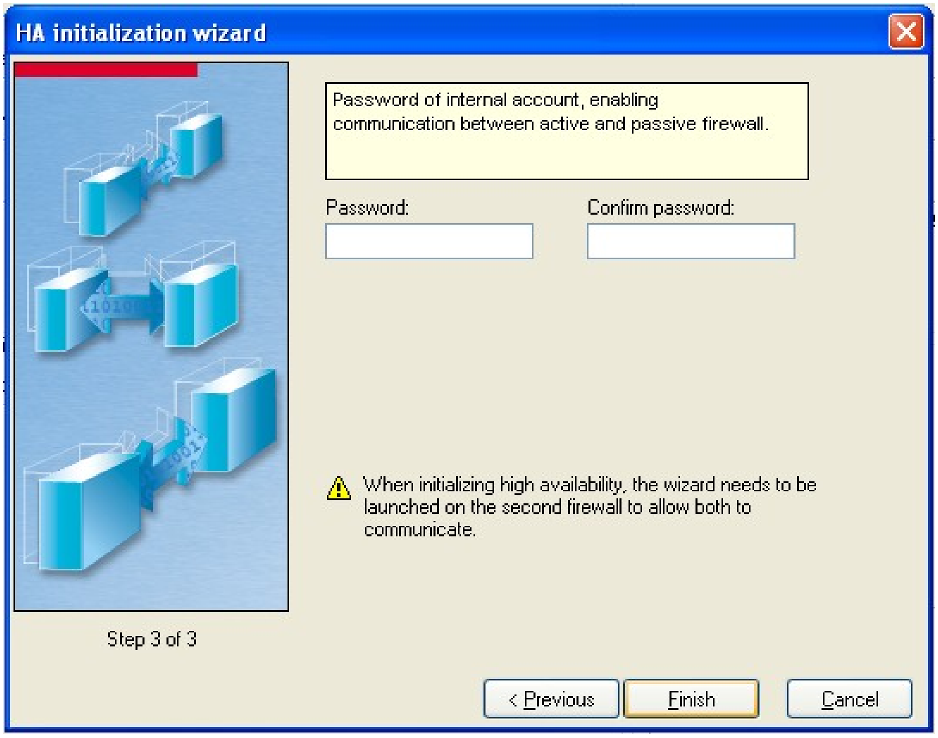
The failure threshold cannot be less than 2 tryouts and it is highly inadvisable to specify an interval of less than 5 seconds.

WARNING

A 15-second interval and a failure threshold of 2 are recommended.

The maximum time of inactivity before the Firewall reboots could be set in the **Watchdog Configuration** section.

3 Step 3



HA initialization wizard

Password of internal account, enabling communication between active and passive firewall.

Password:

Confirm password:

⚠ When initializing high availability, the wizard needs to be launched on the second firewall to allow both to communicate.

Step 3 of 3

Figure 385: HA wizard - Step 3

Lastly, indicate the password used to encrypt communications between both Firewalls. Firewalls communicate with each other on port 1300 and data is encrypted in AES.

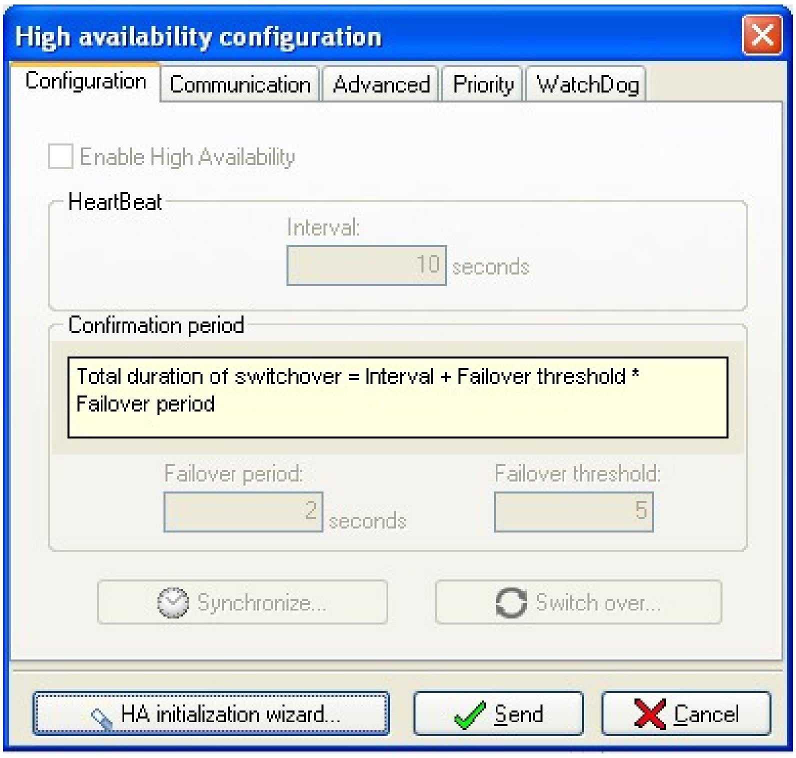
All these parameters may be modified later

1 Connect to the other Firewall (backup) and start the Wizard

WARNING

Interfaces, IP addresses and passwords of the main and the backup have to be the same.

2 As soon as the wizard has finished with both Firewalls, you have to connect to the MAIN Firewall (if only the BACKUP responds, conduct a manual permutation) and synchronize both Firewalls (see below). The first synchronization must be started from the MAIN Firewall to the BACKUP, in order to replicate MAC addresses on both Firewalls.



□ Enable High Availability

HeartBeat

Interval: 10 seconds

Confirmation period

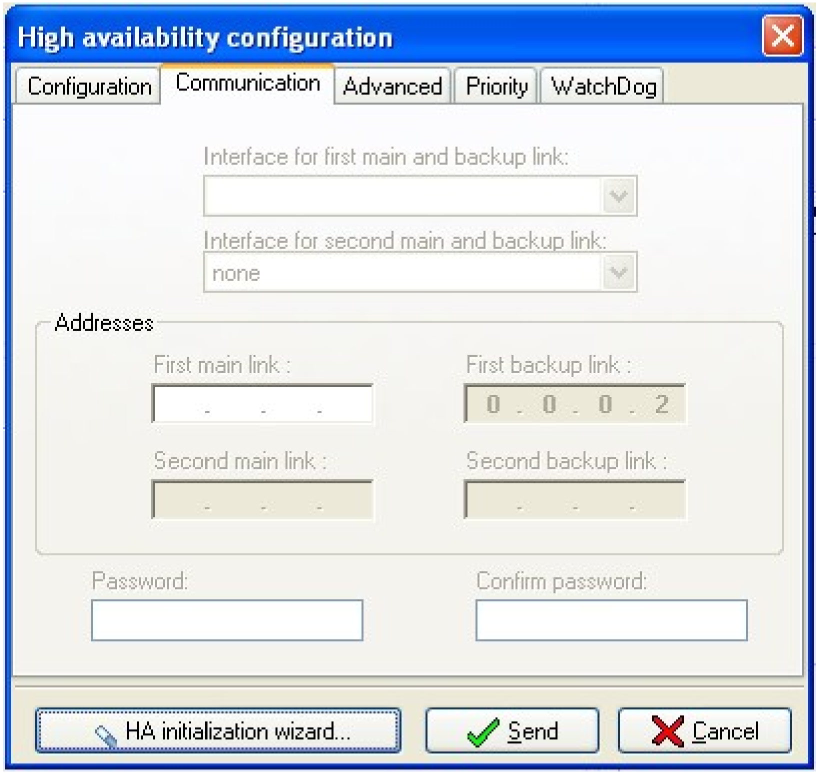
Total duration of switchover = Interval + Failover threshold * Failover period

Failover period: 2 seconds

Failover threshold: 5

Figure 386: Configuring HA - Configuration

14.1.4.2. Communication tab



Interface for first main and backup link:

Interface for second main and backup link: none

Addresses

First main link : . . .

First backup link : 0 . 0 . 0 . 2

Second main link : . . .

Second backup link : . . .

Password:

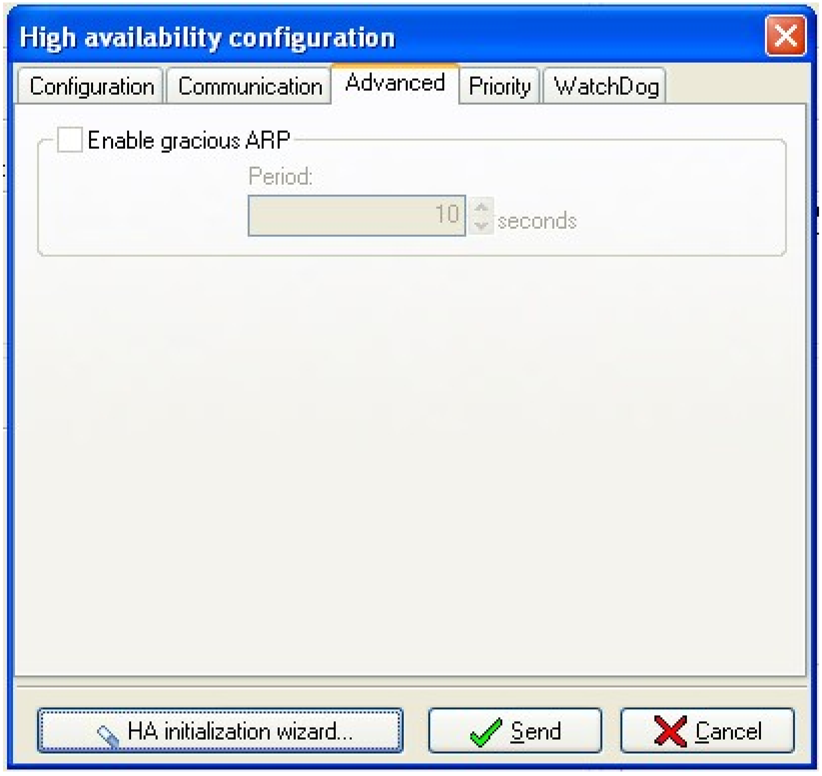
Confirm password:

Figure 387: Configuring HA - Communication

In this menu you may modify the parameters defined in the Wizard.

Interface for the 1st main and backup link	Main interface used for linking the Firewalls that make up the cluster.
Interface for the 2nd main and backup link	Secondary interface used for linking the Firewalls that make up the cluster.
Addresses	IP addresses allocated to different Firewalls.
Password	Password used to encrypt communications between both Firewalls.

9.1.4.3. Advanced tab


High availability configuration

Tabs: Configuration | Communication | Advanced | Priority | WatchDog

□ Enable gracious ARP

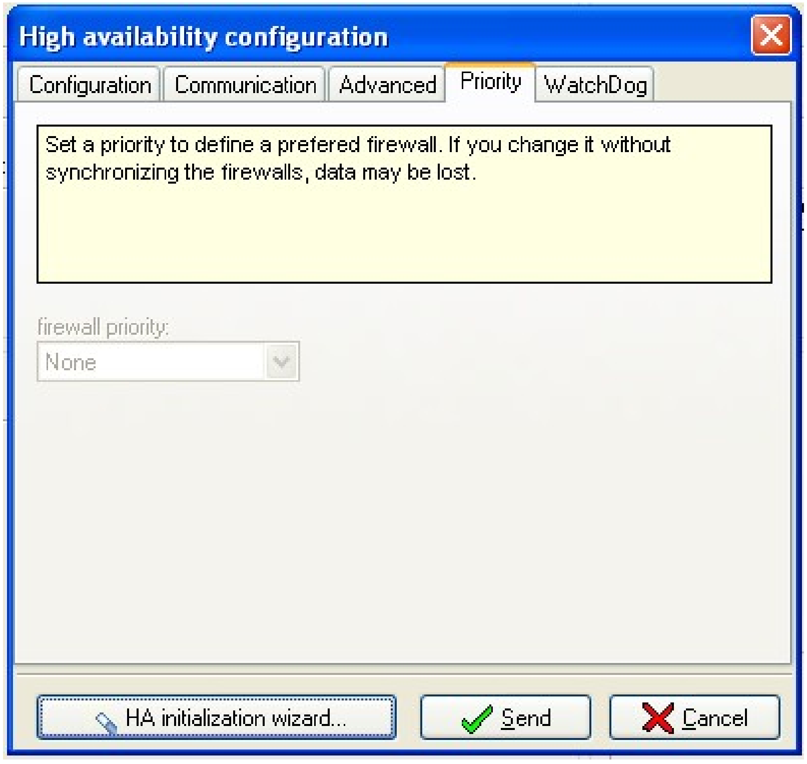
Period: 10 seconds

Figure 388: Configuring HA – Advanced

This menu allows you to activate sending “Gracious ARP” packets. This means that the Firewall regularly publishes its IP and MAC addresses on the network.

Period	Interval between the sending of each packet.

14.1.4.4. Priority Tab



Set a priority to define a prefered firewall. If you change it without synchronizing the firewalls, data may be lost.

firewall priority: None

Figure 389: Configuring HA - Priority

When both Firewalls are active or start up at the same time, the Priority option allows specifying the Firewall that will be the active and which will be the passive.

Firewall Priority	Selection of the Firewall that will have priority.

14.1.4.5. Watchdog tab

For this point, you will need to have completed these steps

- Part 2: Installation, pre-installation, integration.

Purpose of this point

This section enables you to configure WatchDog, a hardware element which tests the Firewall regularly in order to detect any inactivity. The Watchdog can force a firewall to reboot if the Firewall freezes.

Accessing this point

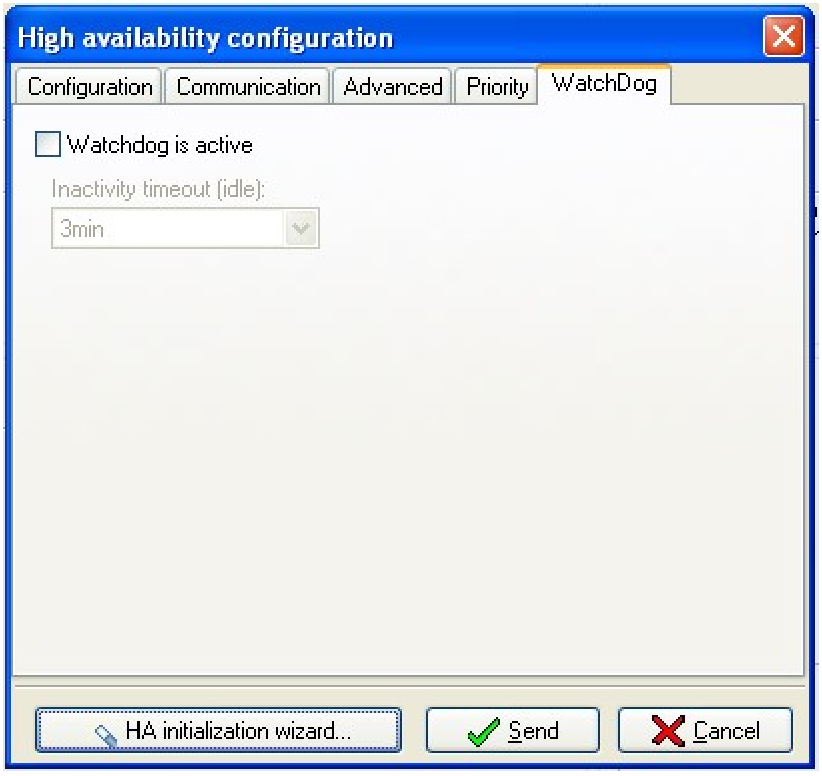
- You can access the dialog box via the menu **`Firewall\High Availability`**.

Important

WARNING
Watchdog and High availability options are only installed on Firewalls produced or returned to the After-Sales Department after October 2001. If your Firewall is older you can still benefit from these options. However, in this case the Firewall must be returned to NETASQ for modification.

The Watchdog option enables you to reboot the Firewall automatically if it freezes. The principle is simple: Watchdog is a hardware component which carries out tests on Firewall activity at regular intervals. After a certain amount of time (configurable) without response, the Firewall will shut down and reboot.

The configuration is very simple. You only have to check the 'Watchdog is active' option in the High Availability menu (**`Firewall`** tab) and to specify the maximum inactivity time. Active connections will be reactivated after the reboot.



□ Watchdog is active

Inactivity timeout (idle): 3min

Figure 390: Configuring HA – WatchDog

WARNING
Do not make the inactivity time limit too short (less than 1 minute) or you may run the risk of rebooting the Firewall frequently, which may not be necessary. The Firewall may not reply for several seconds and then recommence normal activity soon afterwards without the need for a reboot.

This option is available independently of the high availability option.

14.1.4.6. Synchronizing the Firewalls

Synchronizing the Firewalls allows the active Firewall configuration to be replicated on the passive Firewall. This synchronization is carried out on the whole configuration, passwords and date changes.

Synchronization may either be forced by clicking on **Synchronize** in the **`Configuration`** tab or requested by the firewall when you exit.

WARNING

If you carry out the synchronization manually, the Firewalls will be indicated as non-synchronized even though synchronization has taken place. To check the synchronization, use the Firewall Monitor which indicates the synchronization status of both Firewalls.

14.1.4.7. Swapping the Firewalls

If you want to make the passive Firewall active, click on **Swap** button in the **`Configuration`** tab.

14.1.5. Architecture examples

Diagram on the installation of High Availability with two U450/4 Firewalls and 3 x 4-port 10/100Mbit Hubs with the 3 available Firewall interfaces (the fourth is used for high availability).

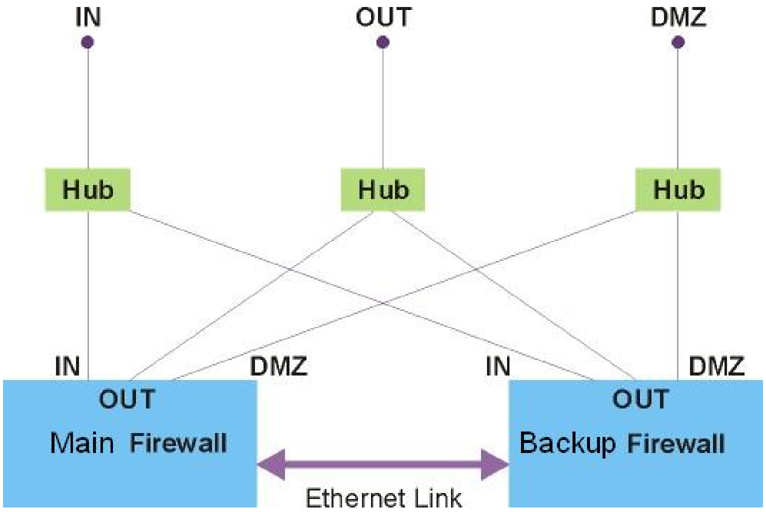


Figure 391: HA

Using an Ethernet link allows you to physically separate both appliances. In fact, you can even place each Firewall in a different location. However, you will lose an Ethernet interface per appliance (used for high availability).

NOTE

Switches can be used instead of hubs but it is highly inadvisable because of the ‘intelligent’ nature of the switches. Furthermore hubs are much less expensive than switches.

14.1.6. Shutting down high availability

If you want to stop using the high availability feature you should observe the following procedure:

1. Shut down one of the Firewalls
2. Disable the high availability option on the working Firewall, then shut it down.

3 Start up the first Firewall, then disable the high availability option on this Firewall (change its IP addresses if necessary).

> **WARNING**
> Shutting down high availability on only one Firewall may cause IP and MAC address conflicts.

14.1.7. Remarks

When you try to connect to the cluster (both Firewalls) via NETASQ UNIFIED MANAGER or NETASQ REAL-TIME MONITOR, the connection must be established using the active Firewall. To connect to the passive Firewall, the latter must be activated (using the **Permute** button in the **Configuration** tab).

The passive Firewall must be rebooted to synchronize the Firewalls after a change in the configuration of the active Firewall.

Log files are not shared. A file will only contain logs retrieved when the Firewall was active. To centralize logs on both Firewalls they must be redirected to an identical external syslog server or to the NETASQ SYSLOG server.

A full system backup (on the backup partition) should only be carried out on the active Firewall.

To test high availability you can disconnect an interface network from the active Firewall; the second Firewall should become active after a given time.

Update procedure

To update your Firewalls in high availability, you have two possibilities:

- Updating through the active firewall.
- Updating through the passive Firewall (can be carried out only for minor updates starting from version 5).

Updating through the active firewall

When a software update of the active Firewall is performed, there is no permutation when the active Firewall restarts.

Once the active Firewall has been updated, you have to carry out a manual permutation of both Firewalls by clicking on the **Permute** button in the **Configuration** tab.

Disconnect then reconnect (you will then be connected to the other Firewall).

Carry out the software update again. The consecutive reboot will cause the Firewalls to reboot so that the update will be in the previous configuration.

This procedure allows retrieving at least one Firewall in the old software version if the update did not take place correctly.

Updating through the passive Firewall

The Firewall update wizard’s **Passive Update** option allows you to update the passive Firewall before the active Firewall. In this case, you will be updating the passive Firewall from the active Firewall.

Once the passive Firewall has started up, you may manually permute it to repeat the operation (updating the passive Firewall).

Once the second Firewall has started up, you may manually permute the Firewalls so that the update will be in the previous configuration.

This procedure allows retrieving at least one Firewall in the old software version if the update did not take place correctly without interruption of service.

PART 15: SEISMO

15.1.1. Introduction

15.1.1.1. Introduction to this part

How does NETASQ SEISMO work?

NETASQ SEISMO is a module that allows the network administrator to collect information in real time and to analyze it in order to sift out possible vulnerabilities that may compromise his network. Among other things, it also allows raising alerts from ASQ and as such, to maintain an optimal security policy.

NETASQ SEISMO gathers and archives information relating in particular to the operating system, various active services and installed applications. There are two types of applications:

- Products that correspond to client applications installed on a host (example: Firefox 1.5)
- Services that correspond to server applications attached to a port (example: openSSH 3.5)

As for detected applications, they can be grouped according to family. By pairing this information with its vulnerability database, NETASQ SEISMO shows probable security loopholes relating to these applications.

Gathering this information makes it possible to create descriptive profiles of each network element.

NETASQ SEISMO aims to do the following:

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

The procedure is set out below:

1 NETASQ's intrusion prevention engine (ASQ) extracts data in real time using the network protocols that it knows.
2 SEISMO combines and weights these data.
3 If a vulnerability is detected, it may then be treated thanks to dynamically-indexed databases. The gathered information will be used in Monitor so that flaws in the network can be corrected, prohibited software can be detected, or the actual risk of an attack can be obtained in real time.
4 The profile is then complete.
5 One or several solutions can be considered.

> **Example**
> Company A has a public website that it updates twice monthly via FTP. When connections are established, at a specific date and time, vulnerabilities that would potentially affect FTP servers are raised and immediately embedded in Monitor. This allows the administrator to detect it almost simultaneously.
> This vulnerability is represented by a line that indicates the number of affected hosts and whether a solution exists.
> When this line is deployed, details of the hosts concerned will be displayed alongside the service that the vulnerability affects. A help file, made mostly up of links, may be suggested to correct the detected flaw.

Once the network administrator becomes aware of the vulnerability, he will be able to fix it at any time, quarantine the affected host(s) and generate a report.

NETASQ SEISMO can also create weekly, monthly or yearly reports via the application **NETASQ EVENT REPORTER** (Autoreport). (Cf. ***NETASQ EVENT REPORTER*** *User manual*)

Why do profiles need to be configured?

ASQ includes a dynamic packet filtering engine (stateful inspection) with rule optimization that allows applying a vulnerability profile quickly and safely. The implementation of profile features is based on the comparison of the attributes of each IP packet received against the criteria of each rule in the created vulnerability profile.

In the NETASQ SEISMO module, some profiles are created by default, and there are 4 such profiles. However, you will be able to create as many profiles as you wish.

Vulnerability rules are stored on in profiles on the NETASQ firewall.

It is a simple principle: when a packet arrives on the NETASQ UTM product, it will be moved down the list of vulnerability rules. If the packet meets a rule's selection criteria, the action associated with this rule will be applied, otherwise the packet will be deleted automatically. Once an applicable rule is found, the packet will no longer be compared against the rules that follow.

The way vulnerability rules are ordered is very important. In fact, ensuring that this order is coherent is the most difficult part in configuring your firewall.

15.1.1.2. For this chapter, you will need to know

The profiles you wish to establish.

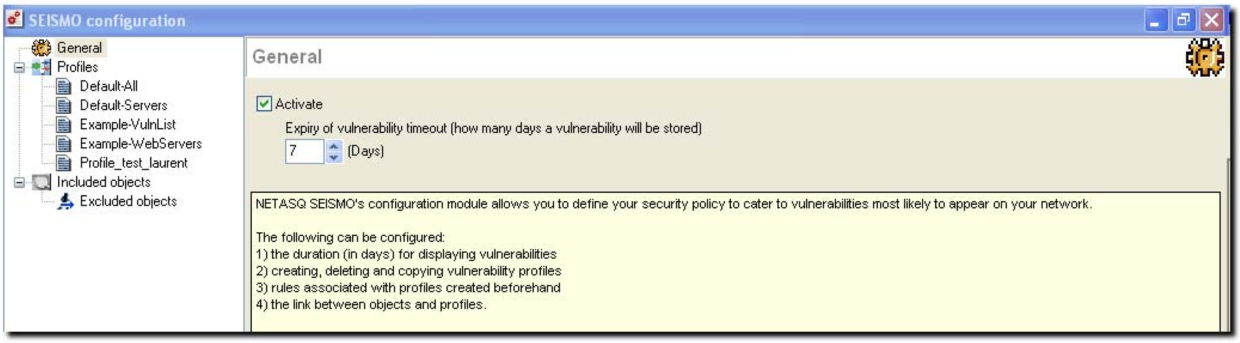
15.1.1.3. Purpose of this section

This section allows you to define the vulnerability profiles and the rules associated with them.

15.1.1.4. Accessing this section

➲ Select **SEISMO** in the menu directory in NETASQ UNIFIED MANAGER to access the configuration of the SEISMO module.

15.1.2. Presentation



☑ Activate

Expiry of vulnerability timeout (how many days a vulnerability will be stored)

7 (Days)

NETASQ SEISMO's configuration module allows you to define your security policy to cater to vulnerabilities most likely to appear on your network.

The following can be configured:
1) the duration (in days) for displaying vulnerabilities
2) creating, deleting and copying vulnerability profiles
3) rules associated with profiles created beforehand
4) the link between objects and profiles.

Figure 392: Configuring SEISMO - General

This section allows you to define the profiles and associated rules, and also to manage your security policy with regards to vulnerabilities.

In this configuration menu, you will be able to configure your security policy to tackle vulnerabilities likely to surface on your network.

Configuration consists of:

- Configuring the duration for which lines of vulnerabilities will be displayed
- Creating, deleting and copying vulnerability profiles (excluding the profile Default-all)
- Configuring the rules associated with the profiles already created
- Linking objects to profiles

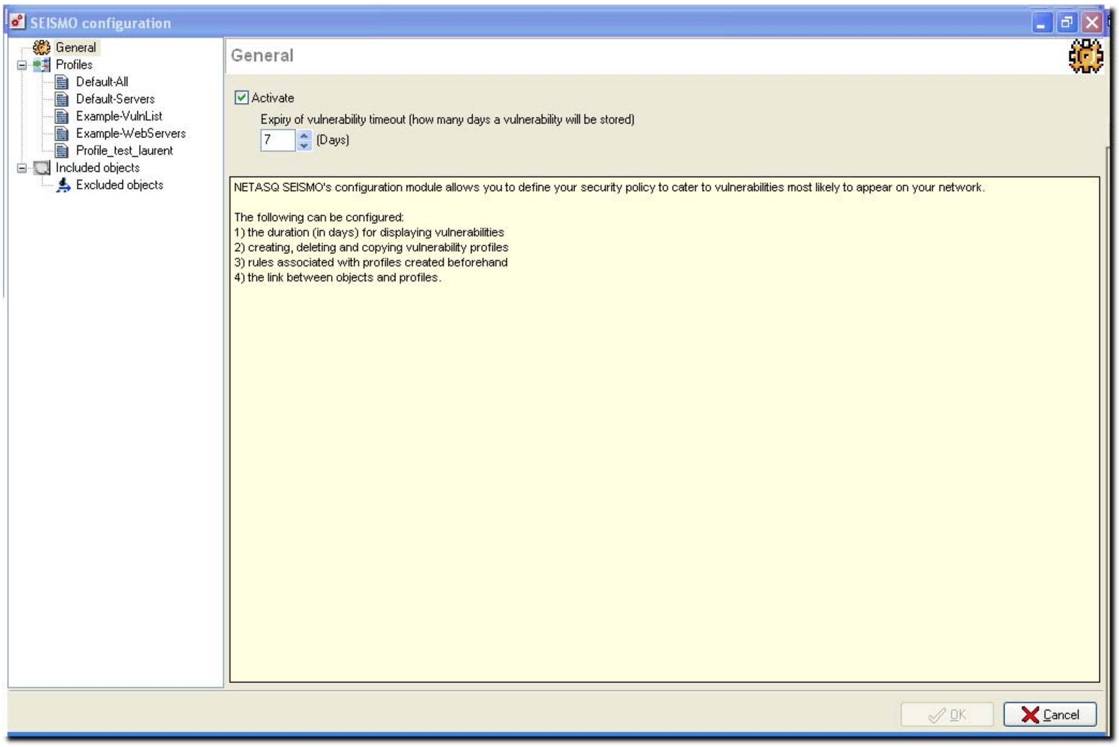
There are two distinct zones on the screen:

- A menu directory that enables moving from one screen to another when configuring NETASQ SEISMO.
- A miscellaneous configuration screen.

This configuration can be carried out when viewing SEISMO logs in NETASQ REAL-TIME MONITOR and NETASQ EVENT REPORTER.

15.1.3. General

- The **`General`** menu can be accessed from the menu directory in the SEISMO configuration window:



General

☑ Activate

Expiry of vulnerability timeout (how many days a vulnerability will be stored)

7 (Days)

NETASQ SEISMO's configuration module allows you to define your security policy to cater to vulnerabilities most likely to appear on your network.

The following can be configured:
1) the duration (in days) for displaying vulnerabilities
2) creating, deleting and copying vulnerability profiles
3) rules associated with profiles created beforehand
4) the link between objects and profiles.

Figure 393: Configuring SEISMO - General

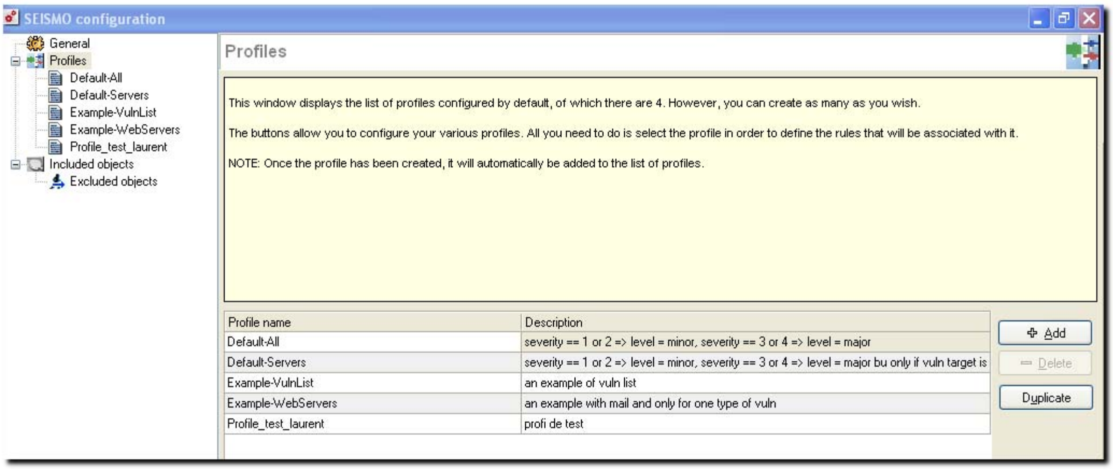
Activate	Check the **Activate** option to display information relating to the NETASQ SEISMO module. It will then be possible to determine the number of days during which the vulnerability lines will be displayed in Monitor and Reporter. This information will not be visible if this option is not selected. **REMARK** During updates (and if you have a valid license), the NETASQ SEISMO module will be enabled by default. Alarms will be raised if the existing configuration calls for it.
Vulnerability timeout (Number of days vulnerability has been stored)	This option enables determining the maximum number of days vulnerability lines will be displayed once these vulnerabilities appear.

15.1.4. Profiles

➲ The **`Profiles`** menu is found in the SEISMO configuration menu directory:

This window sets out the list of the 4 profiles configured by default. You will be able to create your own profiles.

REMARK
The profile you create will be added automatically to the list of profiles in the menu directory.



This window displays the list of profiles configured by default, of which there are 4. However, you can create as many as you wish.

The buttons allow you to configure your various profiles. All you need to do is select the profile in order to define the rules that will be associated with it.

NOTE: Once the profile has been created, it will automatically be added to the list of profiles.

Profile name	Description
Default-All	severity == 1 or 2 => level = minor, severity == 3 or 4 => level = major
Default-Servers	severity == 1 or 2 => level = minor, severity == 3 or 4 => level = major bu only if vuln target is
Example-VulnList	an example of vuln list
Example-WebServers	an example with mail and only for one type of vuln
Profile_test_laurent	profi de test

Figure 394: Configuring SEISMO - Profiles

There are 2 specific parts to this window:

Left	List of created profiles.
Right	Buttons to perform action on selected profiles.

The table that indicates the different types of profiles created will display the following information:

Profile name	Indicates the name given to the profile.
Description	Description of the profile. It would be useful to indicate the level of severity here. **Example** severity==1or2=>level=minor, severity==3or 4=>level=major

15.1.4.1. List of profiles

The list of profiles is found in this part of the dialog box. There are 4 by default, and each profile has a name and description.

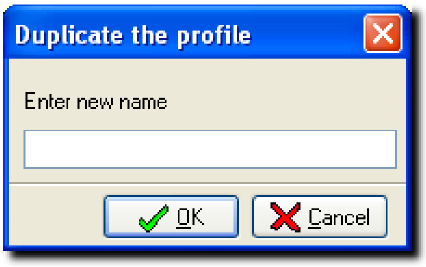
The created profile will then need to be associated with an object.

WARNING
Only one profile can be associated with an object.

A profile is selected when you click on its name. Thereafter, you will be able to delete of duplicate it.

15.1.4.2. Possible actions

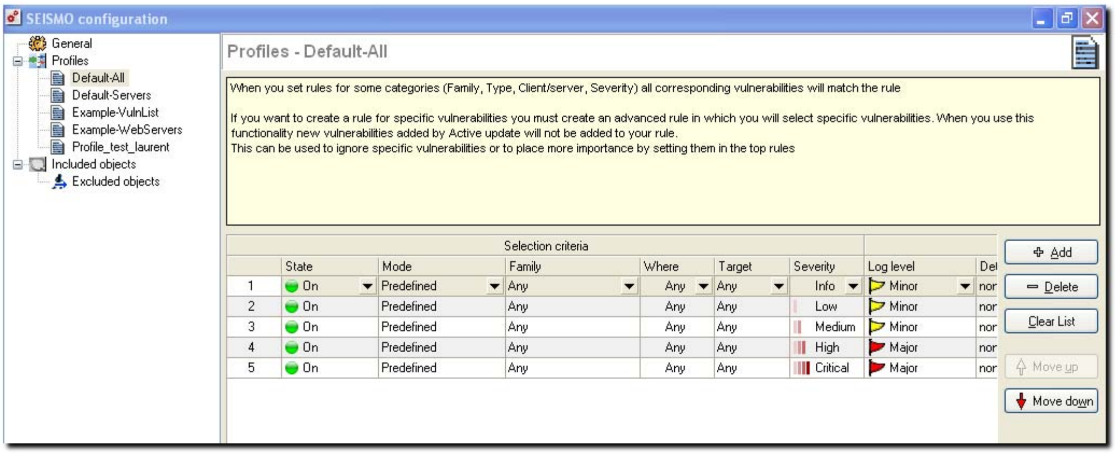
In this window, you will be able to perform several actions:

Add	This button allows you add profiles to the table. **NOTE** The created profile is added automatically to the SEISMO configuration menu directory.
Delete	Select the profile to be deleted then click on the button. The profile Default-All cannot be deleted. **WARNING** There will be no confirmation message when you delete a profile, therefore the removal will be immediate.
Duplicate	Select the profile you wish to duplicate. The following screen will then appear:  *Figure 395: Duplicating the profile* Enter a name for this profile and click on **OK**. The new profile will be displayed in the table and in the SEISMO menu directory. Rules in this new profile are those from the profile that was already duplicated.

15.1.4.3. Editing a profile

The procedure for editing a profile is as follows:

1 Select a profile from the **`Profiles`** menu directory. The rule dialog box for the selected profile will open.



When you set rules for some categories (Family, Type, Client/server, Severity) all corresponding vulnerabilities will match the rule

If you want to create a rule for specific vulnerabilities you must create an advanced rule in which you will select specific vulnerabilities. When you use this functionality new vulnerabilities added by Active update will not be added to your rule.
This can be used to ignore specific vulnerabilities or to place more importance by setting them in the top rules

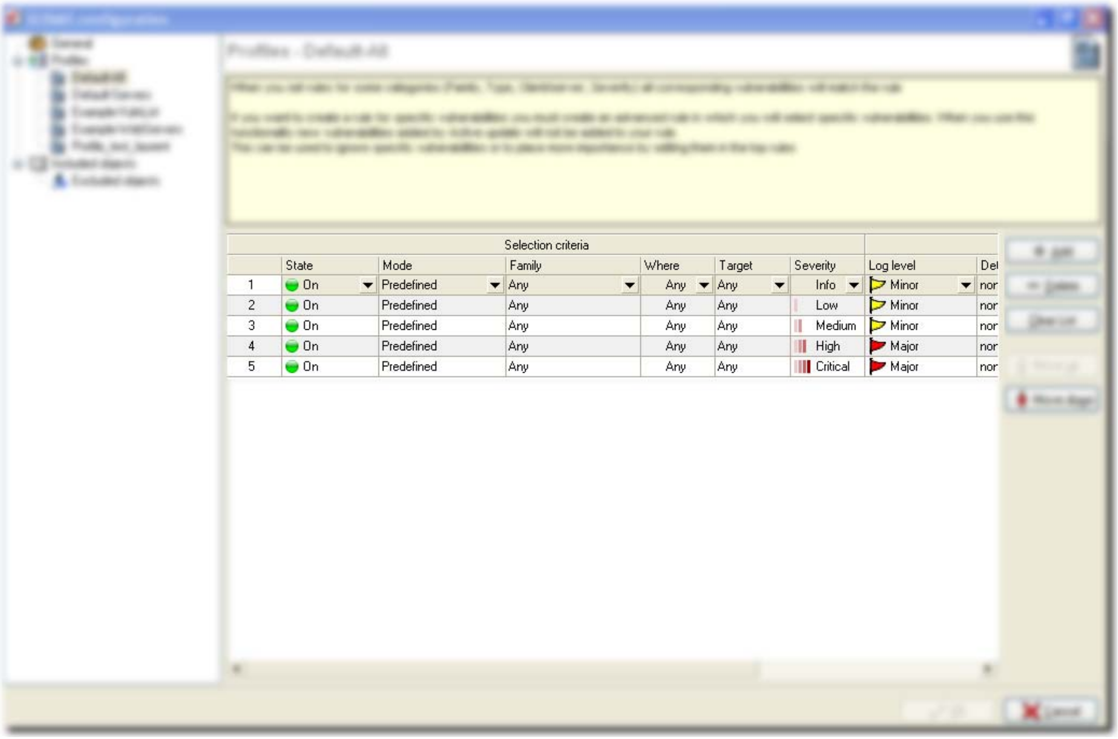
	Selection criteria							
	State	Mode	Family	Where	Target	Severity	Log level	Del
1	On	Predefined	Any	Any	Any	Info	Minor	nor
2	On	Predefined	Any	Any	Any	Low	Minor	nor
3	On	Predefined	Any	Any	Any	Medium	Minor	nor
4	On	Predefined	Any	Any	Any	High	Major	nor
5	On	Predefined	Any	Any	Any	Critical	Major	nor

Figure 396: Configuring SEISMO - Profiles

This window consists of two zones:

- A zone containing the vulnerability rules in the form of a table.
- A zone allowing several actions to be performed.

Vulnerability rules



	Selection criteria							
	State	Mode	Family	Where	Target	Severity	Log level	Det
1	● On	Predefined	Any	Any	Any	Info	Minor	nor
2	● On	Predefined	Any	Any	Any	Low	Minor	nor
3	● On	Predefined	Any	Any	Any	Medium	Minor	nor
4	● On	Predefined	Any	Any	Any	High	Major	nor
5	● On	Predefined	Any	Any	Any	Critical	Major	nor

Figure 397: Selection criteria

This grid allows you to define the rules used in each vulnerability profile to be applied. Ensure that your rules are in the right order to get a coherent result. In fact, the firewall executes rules according to the order in which they appear on the screen and stop as soon as an action applies to the traffic that attempts to pass through. Therefore it is best to arrange the rules **from the most detailed to the most general**.

	Rule number.
Status	2 statuses are possible: **On** and **Off**. A green LED means that the rule will be applied, a red one means it will not. This allows defining the rules to be used later or temporarily disabling certain rules for the purpose of conducting tests.
Mode	2 modes are possible: **Predefined** and **Customized**. In predefined mode, the rule is applied to a family of vulnerabilities (e.g., the Peer-to-Peer family) whereas in Customized mode the choice is refined: you will be able to select vulnerabilities of a specific family to which the rule will apply. (For example, you can choose only 2 vulnerabilities from the FTP Client family). Here, each vulnerability has its own severity.

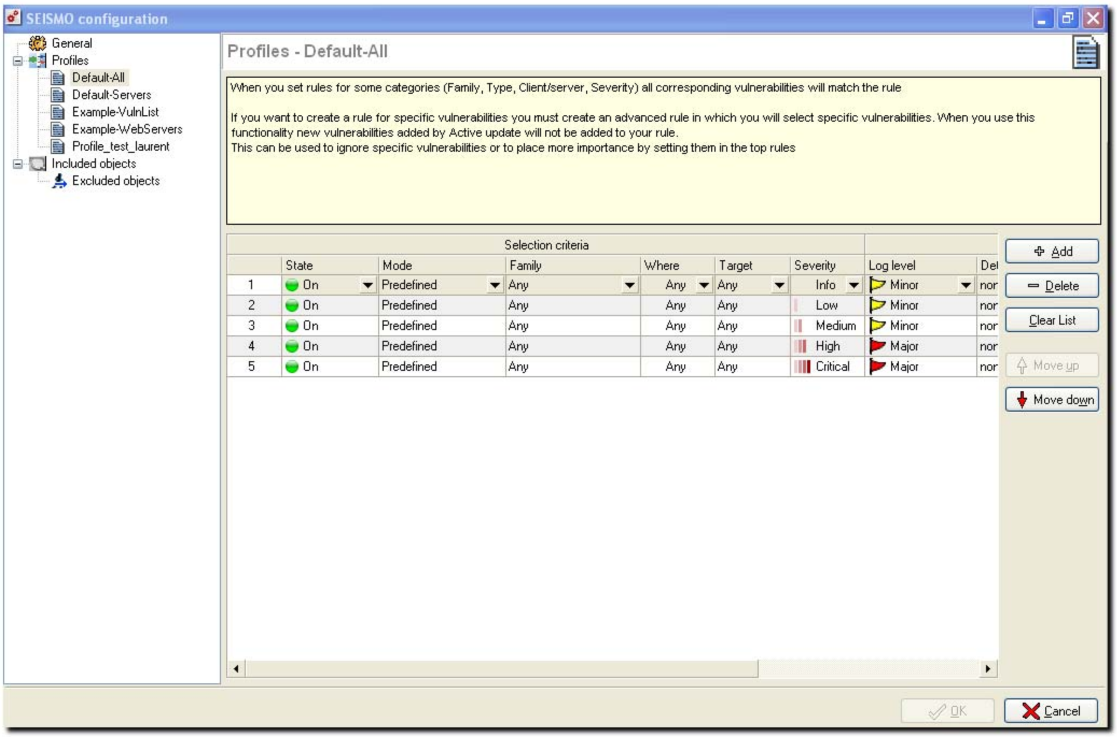
Family	Family to which the vulnerability belongs. The contents are dynamically supplied. (*Cf. Appendix*). **Example** DNS server FTP client
Exploit	The vulnerability can be accessed locally, remotely (via the network) or both. It allows exploiting the vulnerability.
Target	Here, the target of the rule is determined. 3 modes are possible: **Any**, **Client** and **Server**.
Severity	Level of the vulnerability's severity: Any, Information, Low, Medium, High, Critical.
Log level	3 levels: Ignore, Minor and Major.
Detailed report	Lists of vulnerabilities can be sent to users who may need to administer and analyze logs. For this, user groups would have to be created beforehand so that reports can be sent to them via e-mail. This configuration is generated from the E-mails menu in the NETASQ UNIFIED MANAGER menu directory.
Simplified report	Simplified reports containing lists of vulnerabilities can also be sent to another group of recipients. For this, user groups would have to be created beforehand so that reports can be sent to them via e-mail. This configuration is generated from the E-mails menu in the NETASQ UNIFIED MANAGER menu directory.
Description	Description of the rule.

Actions that can be performed on rules

Add	Adds a rule to the selected profile.
Delete	Deletes a selected rule.
Clear list	Deletes the list of rules from the profile.
Up	Moves the selected rule up line by line.
Down	Moves the selected rule down line by line.

A line is selected when one of its elements is selected (in reverse video).

15.1.4.4. Creating vulnerability rules



Profiles - Default-All

When you set rules for some categories (Family, Type, Client/server, Severity) all corresponding vulnerabilities will match the rule

If you want to create a rule for specific vulnerabilities you must create an advanced rule in which you will select specific vulnerabilities. When you use this functionality new vulnerabilities added by Active update will not be added to your rule.
This can be used to ignore specific vulnerabilities or to place more importance by setting them in the top rules

	Selection criteria							
	State	Mode	Family	Where	Target	Severity	Log level	Del
1	● On	Predefined	Any	Any	Any	Info	Minor	nor
2	● On	Predefined	Any	Any	Any	Low	Minor	nor
3	● On	Predefined	Any	Any	Any	Medium	Minor	nor
4	● On	Predefined	Any	Any	Any	High	Major	nor
5	● On	Predefined	Any	Any	Any	Critical	Major	nor

Figure 398: Configuring SEISMO - Profiles

This section goes into detail on how to create your vulnerability rules. The order of these rules is important as the firewall will read them from top down and stops when it finds a rule that matches the IP packet (except if it is only executing an option).

Activating and deactivating a rule

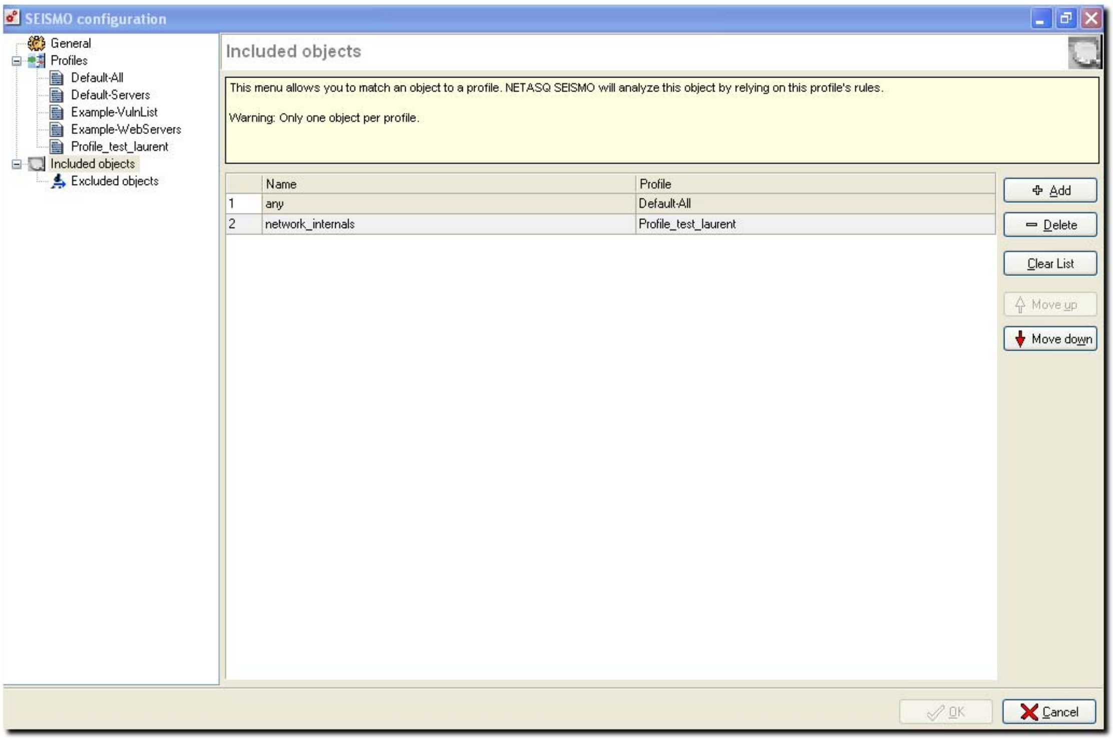
● **On**: The rule has been enabled to filter vulnerabilities.
● **Off**: The rule has not been enabled.

Activating and deactivating rules makes it easier to fine-tune your filters. When using a profile, the NETASQ firewall will ignore disabled rules.

15.1.5. Included and excluded objects

Once profiles are created, you will be able to associate objects to them. As such, the NETASQ SEISMO engine will analyze the object, based on the rules created in a profile.

➲ To select objects for the profile that you wish to implement, go to the menu directory **`Seismo\Included objects`**. The following window will open:



This menu allows you to match an object to a profile. NETASQ SEISMO will analyze this object by relying on this profile's rules.

Warning: Only one object per profile.

	Name	Profile
1	any	Default-All
2	network_internals	Profile_test_laurent

Figure 399: Configuring SEISMO – Included objects

There are two zones to this window:

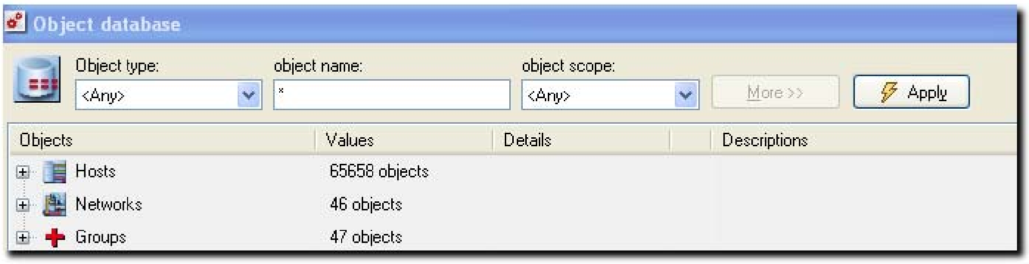
- A zone displaying the included objects.
- A zone allowing you to add or delete objects.

15.1.5.1. Choix de l'object

The object relating to the rule can only be a host, host group or network.

To add an object:

1 Click on the **Add** button then select the object from the object database. The following window will open:



Object type: <Any>

object name: *

object scope: <Any>

Objects	Values	Details	Descriptions
Hosts	65658 objects		
Networks	46 objects		
Groups	47 objects		

Figure 400: Object database

2 Selecting the profile

15.1.5.2. Choix du profil

To select the profile:

1 Click on the triangle that appears when you are in the “Profile” column in order to select the profile relating to the object.
2 Click on **OK** to confirm the list of included objects.

15.1.5.3. Excluded objects

Once objects are associated to a profile, objects can be excluded from the NETASQ SEISMO analysis.

➲ To select the objects to exclude, go to the menu directory **`Seismo\Excluded objects`**. The following window will then open:

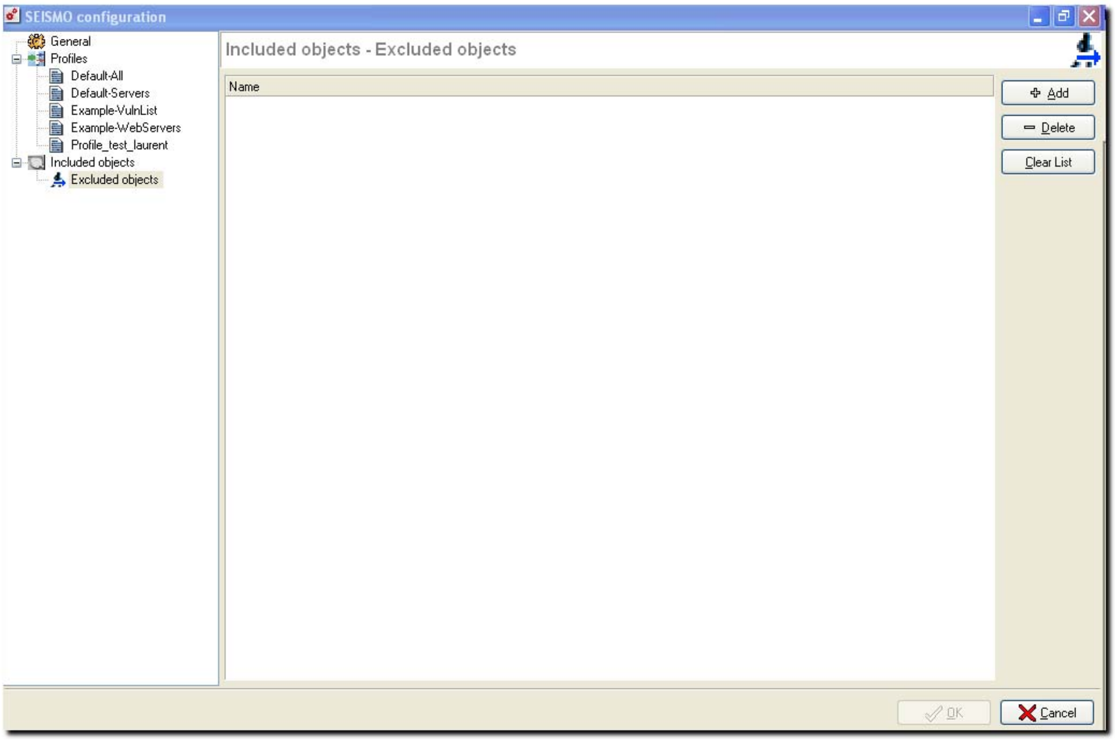


Figure 401: Configuring SEISMO – Excluded objects

To exclude an object:

1 Click on the **Add** button in order to select the object to be excluded from the object database.
2 Click on **OK** to confirm your selection. The window will then display the excluded objects.
3 Click on **OK** to confirm the configuration.

PART 16: E-MAIL CONFIGURATION

16.1.1. Introduction

16.1.1.1. For this chapter, you will need to know

The configuration parameters of the e-mail server and groups you wish to set up.

16.1.1.2. Purpose of this section

In this part, you will be able to define the configuration of the e-mail system in order to allow the NETASQ firewall to send e-mails when certain events arise. E-mail groups can be created, and you will also be able to configure how alarms are sent to mail group. There are also preconfigured e-mail models.

> **NOTE**
> NETASQ SEISMO has its own configuration window for sending simplified and detailed reports regarding vulnerabilities.

16.1.1.3. Introduction to this section

Different mail applications are now centrally managed in NETASQ UNIFIED MANAGER.

In this window, you will be able to:

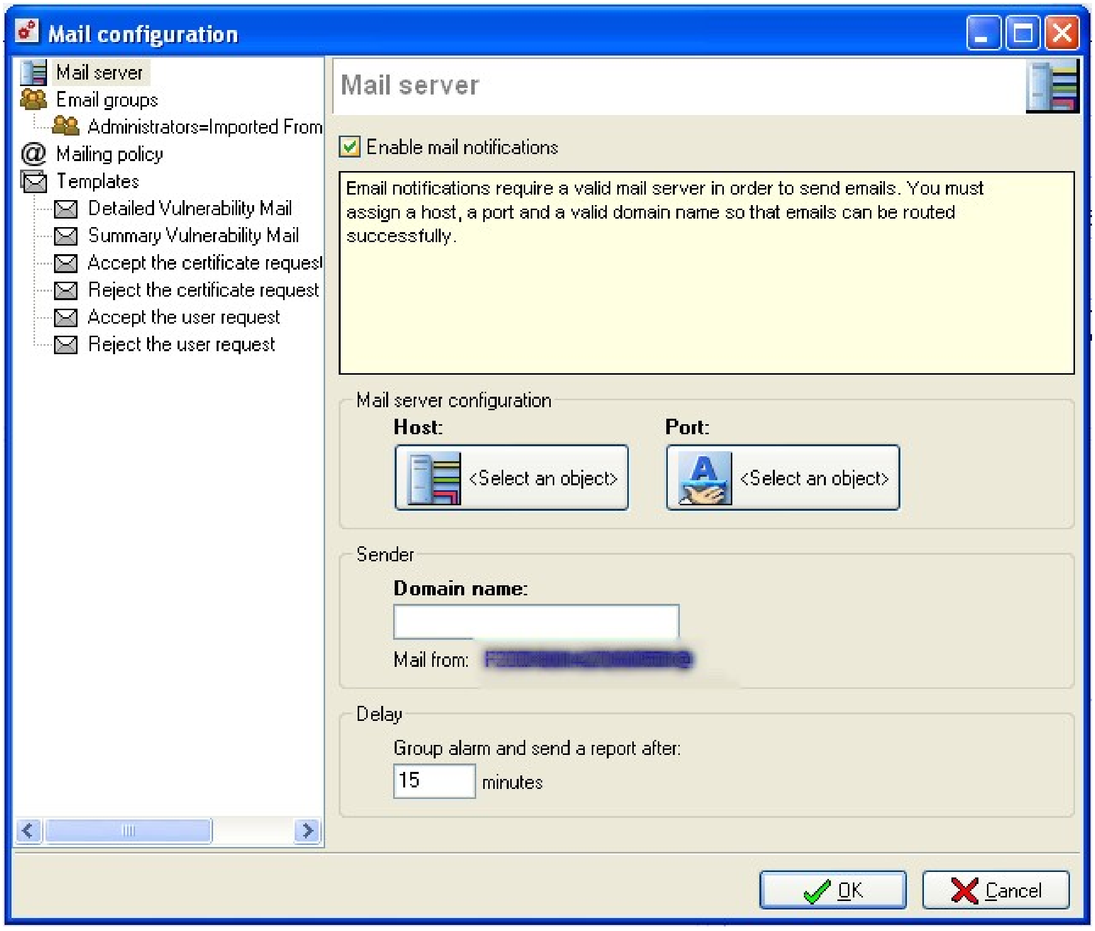
- Configure access to a mail server.
- Define groups of recipients.
- Define the group of recipients for intrusion prevention (ASQ) alarms and for system events.
- Modify preconfigured mail models.

16.1.1.4. Accessing this section

➲ The dialog box for this section can be accessed via the menu **`E-Mails.`**

15.1.2. Configuring the e-mail server

This window groups together the parameters for configuring the firewall’s access to a mail server.
The configuration panel has the following fields:



Mail configuration
Mail server
Email groups
Administrators=Imported From
Mailing policy
Templates
Detailed Vulnerability Mail
Summary Vulnerability Mail
Accept the certificate request
Reject the certificate request
Accept the user request
Reject the user request
Mail server
OK
Cancel

☑ Enable mail notifications

Email notifications require a valid mail server in order to send emails. You must assign a host, a port and a valid domain name so that emails can be routed successfully.

Mail server configuration

Host: <Select an object>

Port: <Select an object>

Sender

Domain name:

Mail from: [redacted]

Delay

Group alarm and send a report after:

15 minutes

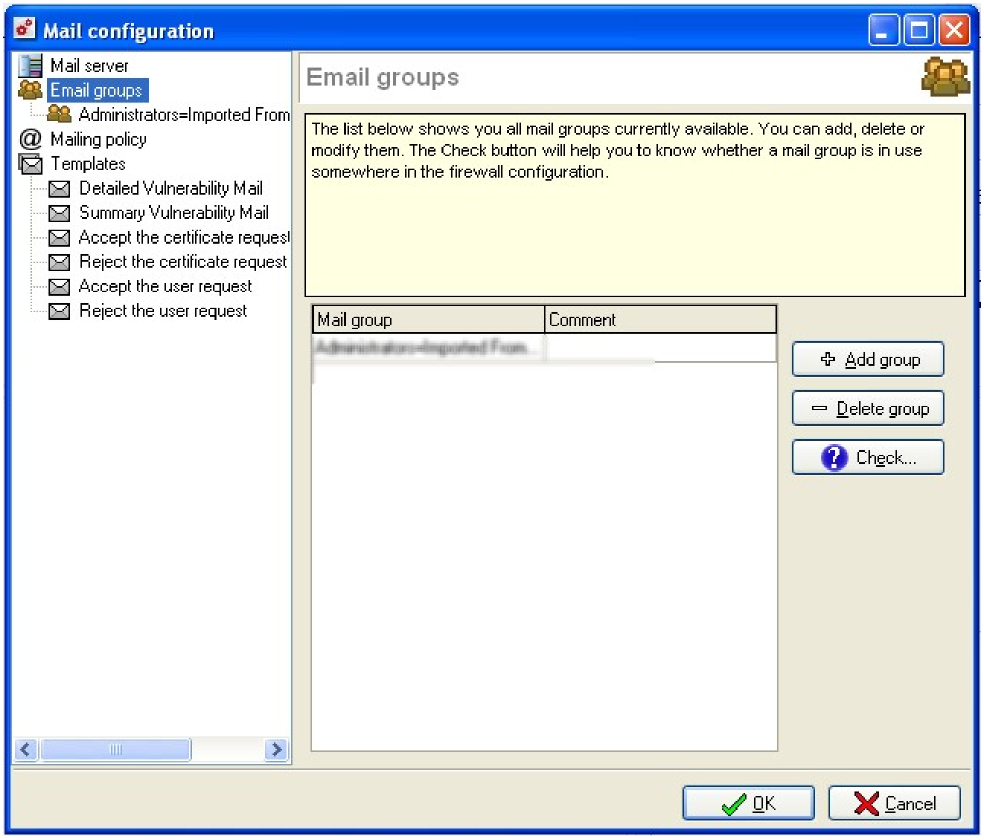
Figure 402: Configuring e-mails – Mail server

Enable mail notifications	Enables sending messages. If this option is disabled, none of the configuration elements will be accessible as the firewall will not send any e-mails. **REMARK** E-mail notification requires a mail server that can receive e-mails coming from the firewall.
Host (*)	Indicates the host (SMTP server) to which the firewall will send e-mails. Select it from the objects database.
Port (*)	SMTP server port to which e-mails will be sent.
Domain name (*)	Useful when indicating the name that is displayed as the mail sender. The e-mail address of the sender will therefore be indicated as follows: <firewall_name >@<domain_name>.
Group alarm and send a report after	Allows you to specify the frequency at which reports are sent. A report will contain all the alarms detected since te previous report. As such, e-mails will only be received at a specified time slot instead of by alarm raised.

16.1.3. E-mail groups

E-mail groups allow you to send e-mails to several recipients at one go. Up to 50 groups can be created.

There are no preconfigured groups. However, you can add new groups, change their names and description or even delete them. Groups have to contain at least one e-mail address, but there is no maximum number of addresses in each group.



The list below shows you all mail groups currently available. You can add, delete or modify them. The Check button will help you to know whether a mail group is in use somewhere in the firewall configuration.

Mail group	Comment
Administrators=Imported From...	

Figure 403: E-mail groups

The list above shows the e-mail groups that have been created. You can create or delete groups and select one to which detailed or simplified reports can be sent, via the SEISMO menu.

Creating a group

1 Click on **Add.** A new line will appear in te list and in the e-mail configuration directory.
2 Edit the group name if necessary (this should be a unique nameYou can also add a description for this group.

Once the group has been created, it will appear in the e-mail configuration menu directory.

Any e-mail address can be added but its format will be checked. Users from the objects database can also be added instead of e-mail addresses.

Deleting a group

1 Select the line to delete. It will appear in reverse video.
2 Click on **Delete**. The group will be deleted from the list and the menu directory of the e-mail configuration window without any confirmation message.

REMARK

Groups can only be deleted if they have not be used in another configuration on the firewall.

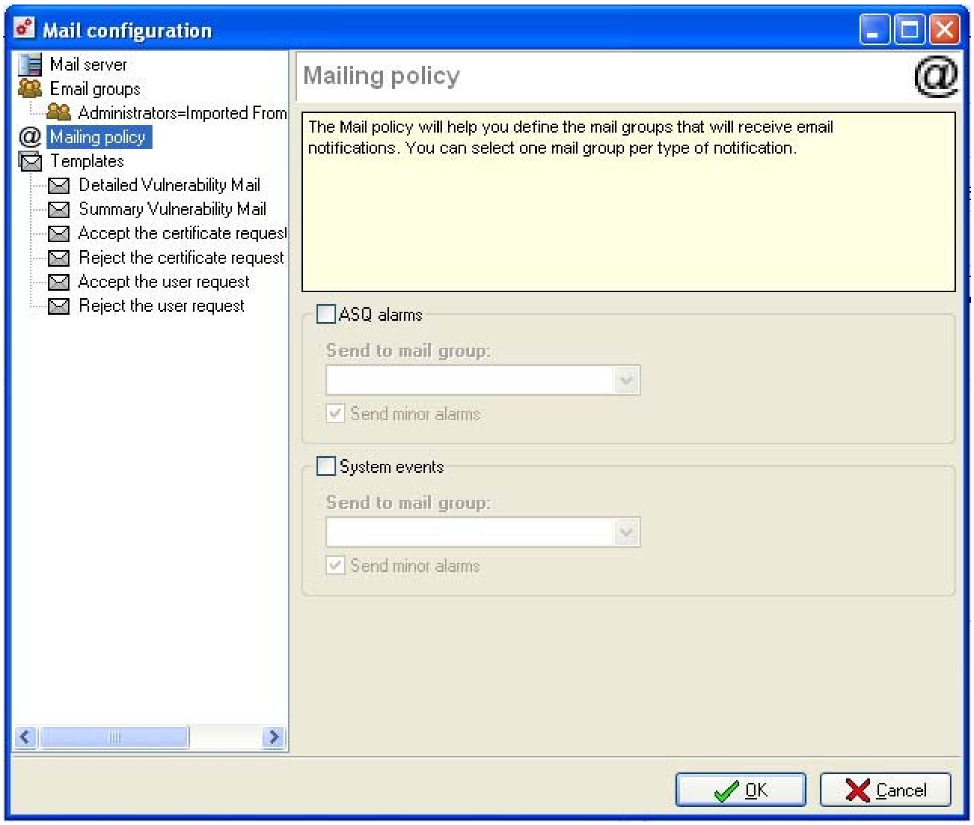
Testing a group

The button **Test** allows you to check whether an e-mail group is used in other configuration modules on the firewall so that when it has to be deleted, it can be done without affecting the other modules.

1 Select the line to test.

2 Click on **Test** to test the line.

16.1.4. Configuring mailing policy



Mail configuration
Mail server
Email groups
Administrators=Imported From
Mailing policy
Templates
Detailed Vulnerability Mail
Summary Vulnerability Mail
Accept the certificate request
Reject the certificate request
Accept the user request
Reject the user request
Mailing policy
OK
Cancel

The Mail policy will help you define the mail groups that will receive email notifications. You can select one mail group per type of notification.

☐ ASQ alarms
Send to mail group:
☑ Send minor alarms

☐ System events
Send to mail group:
☑ Send minor alarms

Figure 404: Mailing policy

The mailing policy allows you to notify a group when ASQ alarms are received and a different group for system events.

The list of alarms and system events are sent in the body of the e-mail to the specified group.

The frequency with which alarm reports and system events are sent can be modified in the field “Frequency” in the `Mail server` menu.

> **Example**
>
> If you specify 15 minutes in the “Frequency” field, you will receive an e-mail alert every 15 minutes of alarms and system events that have occurred on the firewall during this period.

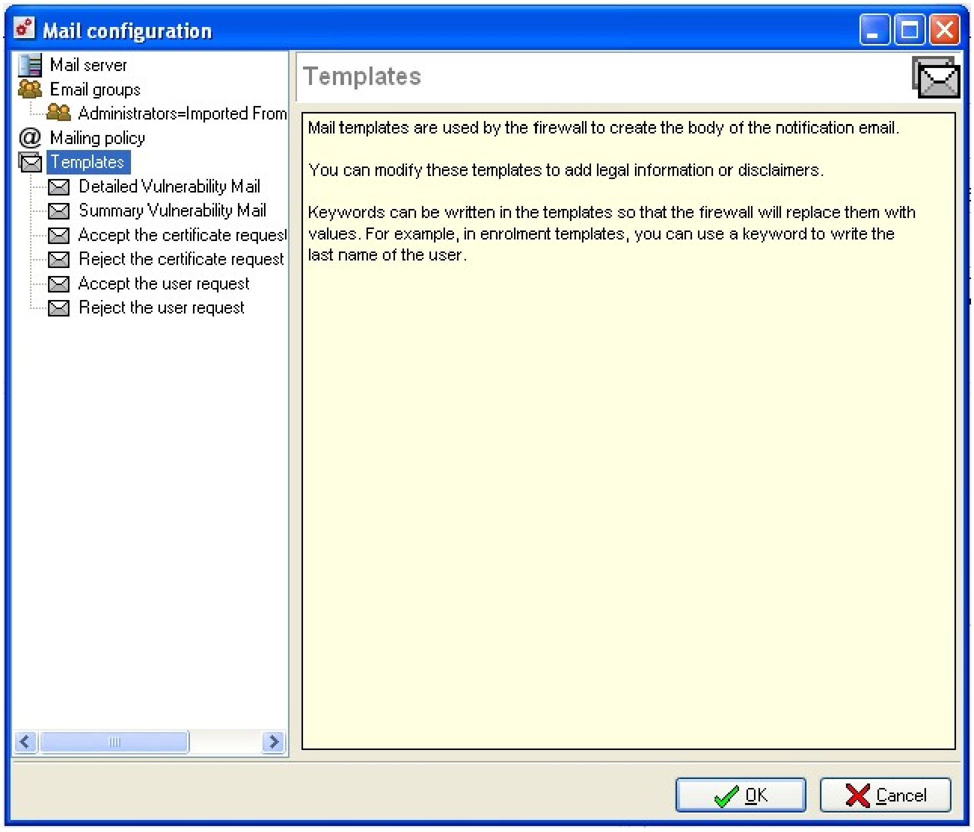
If the option **Send minor alarms** has been selected, the group will also receive the list of minor alarms. (Major alarms are sent systematically).

The group specified for receiving system events will obtain the list of System logs containing the date of the event as well as the service and message.

> **Example**
> 07:17:39 sysevent Active Update: update successful Kaspersky.

WARNING
E-mail alerts that are sent for each alarm can be configured, alarm by alarm, in the menu *Part 6: Intrusion prevention (ASQ).*

16.1.5. Templates


Mail configuration
Mail server
Email groups
Administrators=Imported From
Mailing policy
Templates
Detailed Vulnerability Mail
Summary Vulnerability Mail
Accept the certificate request
Reject the certificate request
Accept the user request
Reject the user request
Templates
OK
Cancel

Mail templates are used by the firewall to create the body of the notification email.

You can modify these templates to add legal information or disclaimers.

Keywords can be written in the templates so that the firewall will replace them with values. For example, in enrolment templates, you can use a keyword to write the last name of the user.

Figure 405: Templates

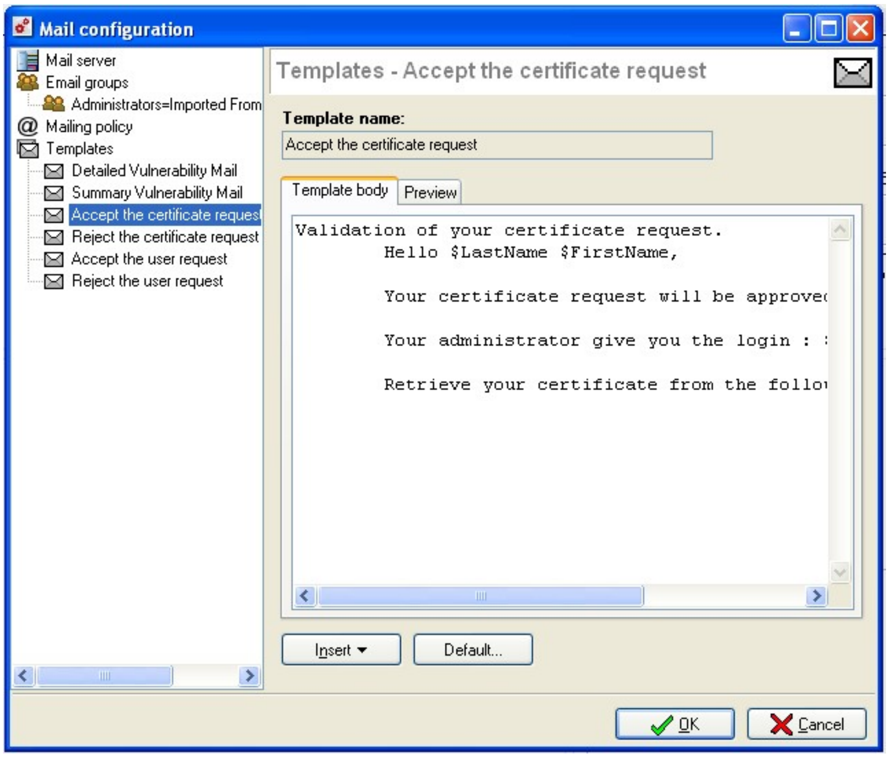
List

Six e-mail models are available, each containing a different body text according to the intended message:

- E-mail detailing a vulnerability
- E-mail summarizing a vulnerability
- E-mail to indicate that a request for user enrolment has been accepted (a)
- E-mail to indicate that a request for user enrolment has been denied (a)
- E-mail to indicate that a request for user certificate has been accepted (a)
- E-mail to indicate that a request for user certificate has been denied (a)

(a) These models are used in *User enrolment*

Body



Mail configuration
Mail server
Email groups
Administrators=Imported From
Mailing policy
Templates
Detailed Vulnerability Mail
Summary Vulnerability Mail
Accept the certificate request
Reject the certificate request
Accept the user request
Reject the user request
Templates - Accept the certificate request
Template body
Preview
Insert
Default...
OK
Cancel

Template name: Accept the certificate request

```
Validation of your certificate request.
        Hello $LastName $FirstName,

        Your certificate request will be approvec

        Your administrator give you the login : :

        Retrieve your certificate from the follo
```

Figure 406: Configuring e-mails - Body

Every model contains what is called a “body” (as in an HTML page). This is a text zone that may contain simple HTML markers.

These models can be modified and may contain keywords that will be replaced with values. For example, a keyword may automatically display the username.

2 buttons allow you to modify the body of the message:

Insert	This button allows you to select keywords that will be replaced with real values when the message is sent.
Default...	Enables resetting the model to its original form. When you click on this button, the following message will appear: "Confirm resetting of the model "Model name" ?"

List of special fields

Models "Detailed Vulnerability Mail" and "Summary Vulnerability Mail":

- $Title: Subjet of the e-mail
- $SubTitle: Sub-title of the e-mail

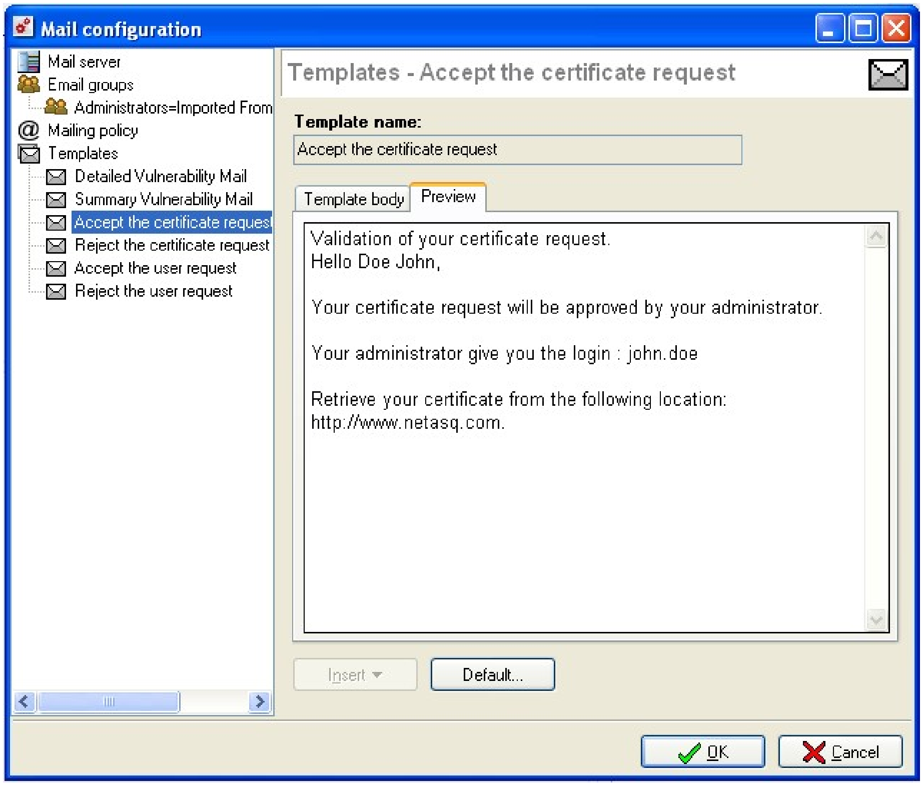
- $MailSummary: Summary of the e-mail
- $VulnSummary: Summary of the vulnerabilities
- $HostsByVuln: List of hists affected by the vulnerabilities
- $VulnByProduct: List of vulnerabilities by product
- $Footer: Page footer in the e-mail

Models for web enrolment (user/certificate request)

- $LastName: Last name of the enrolled user
- $FirstName: First name of the enrolled user
- $Date: Date of the enrolment request
- $UID: User login
- $URL: URL of the enrolment website for downloading the certificats (if approved)

Preview

In this window, you will be able to see a preview of the e-mail model.


Mail configuration
Mail server
Email groups
Administrators=Imported From
Mailing policy
Templates
Detailed Vulnerability Mail
Summary Vulnerability Mail
Accept the certificate request
Reject the certificate request
Accept the user request
Reject the user request
Templates - Accept the certificate request
Template body
Preview
Insert
Default...
OK
Cancel

Template name: Accept the certificate request

Validation of your certificate request.
Hello Doe John,

Your certificate request will be approved by your administrator.

Your administrator give you the login : john.doe

Retrieve your certificate from the following location:
http://www.netasq.com.

Figure 407: Configuring e-mails - Preview

Example of a report received by e-mail on alarms

Type	minor
Action	pass
Date	2006-03-02 12:47:20
Interface	in
Protocol	tcp
Source	192.168.6.1:2756 (peer_192_168_6_1:2756)

Destination	10.2.0.110:80 (PPTP_DNS:http)
Description	Sequence of slashes in the URL

PART 17: LOG MANAGEMENT

CHAPTER 1. LOG CONFIGURATION

17.1.1. Introduction

17.1.1.1. For this chapter, you will need to have completed these steps

- Part 2/Chapter 1: Graphical interface.
- Part 2: Installation, integration and pre-configuration.
- Interfaces, Objects and kernel configuration.
- Setting up policies (translations, filtering, VPN).
- Part 9: Proxy Configuration.
- Part 12: Authentication.
- Part 14: High availability.

17.1.1.2. For this chapter, you will need to know

- The way you wish to be notified of alarms.
- The statistics you need.

17.1.1.3. Purpose of this section

This part allows you to configure the management of different log files and to configure statistics. It also allows you to redirect logs to an external SYSLOG server.

17.1.1.4. Introduction to this section

The Firewall manages a certain number of log files, which capture events detected by log functions. Security events concern the following files:

- **Filter policies**: events relating to the application of filter functions.
- **Server:** events relating to the firewall administration server: "serverd".
- **Alarms**: events relating to the application of intrusion prevention functions.
- **Web:** web traffic events.
- **SMTP:** SMTP traffic events.
- **VPN**: events relating to the the establishment of SAs.
- **Connection:** events relating to connections through and to the firewall.
- **Authentication**: events relating to user authentication.

- **System events**: shutdown/startup of log functions. System events (Firewall startup/shutdown, system errors, etc) are recorded in this log. If log functions are started up or shut down, the daemons that generate these logs will also be started up or shut down.
- **Plugins:** events relating to the treatment of ASQ plugins.
- **SSL VPN:** events relating to the establishment of SSL VPN.
- **POP3:** events relating to the sending of messages.
- **Monitor:** events relating to real time monitoring.
- **SEISMO:** events relating to the vulnerability consultation application on the NETASQ SEISMO network.

Files share a common storage space with other log files. The administrator with “*+M” rights can specify the maximum percentage that each log file can occupy in this total space.

When the maximum has been reached, the Firewall will perform one of the three following configured actions for each file:

- **File rotation**: the most recent logs overwrite the oldest,
- **Stop writing to files**: logs will no longer be written on the Firewall,
- **Shut down Firewall**: the Firewall does not actually shut down but blocks all traffic except firewall connections from the internal network.

“Authentication” files are each allocated a fixed space and are protected from rotation actions in the event of saturation.

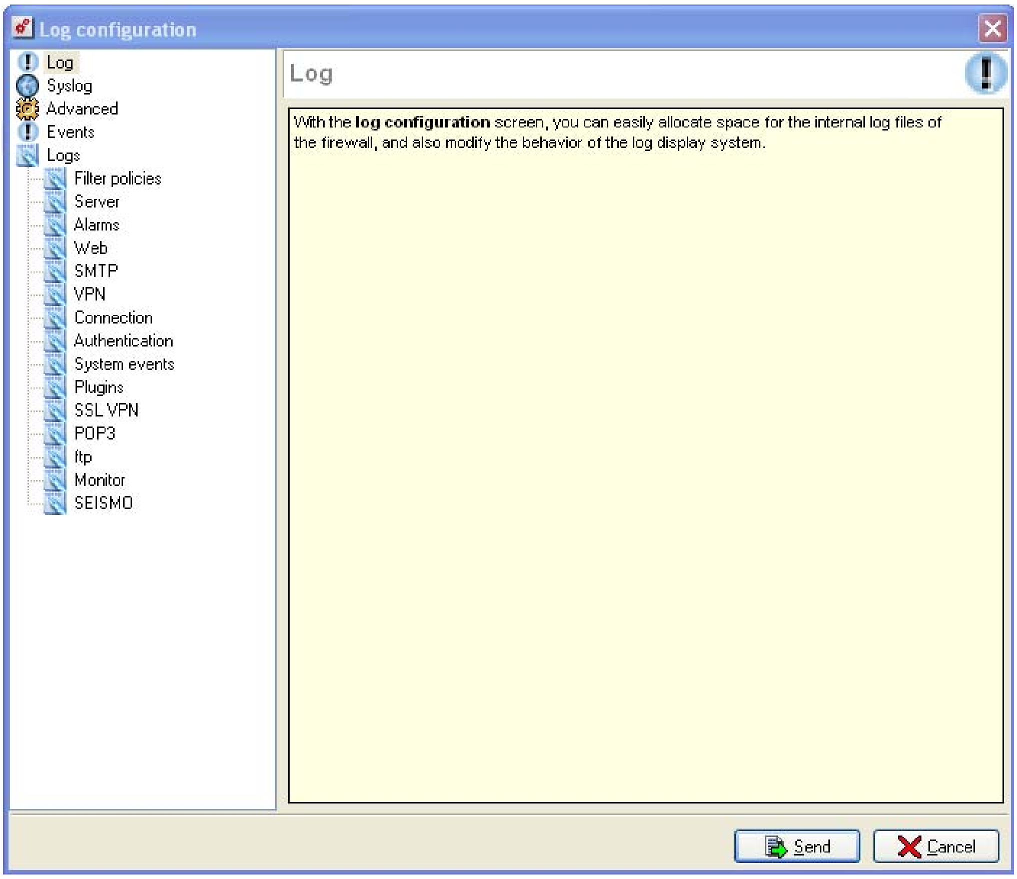
17.1.1.5. Accessing this section

➲ The dialog box is accessed via the **Logs** menu in the menu directory.

17.1.2. Log

➲ By selecting the **Logs** menu in the NETASQ configuration interface’s menu directory, the log configuration screen appears.

Log configuration allows the allocation of disk space for each log type on the firewall. The menu also allows modifying the firewall’s behavior when these logs are saved and sent.



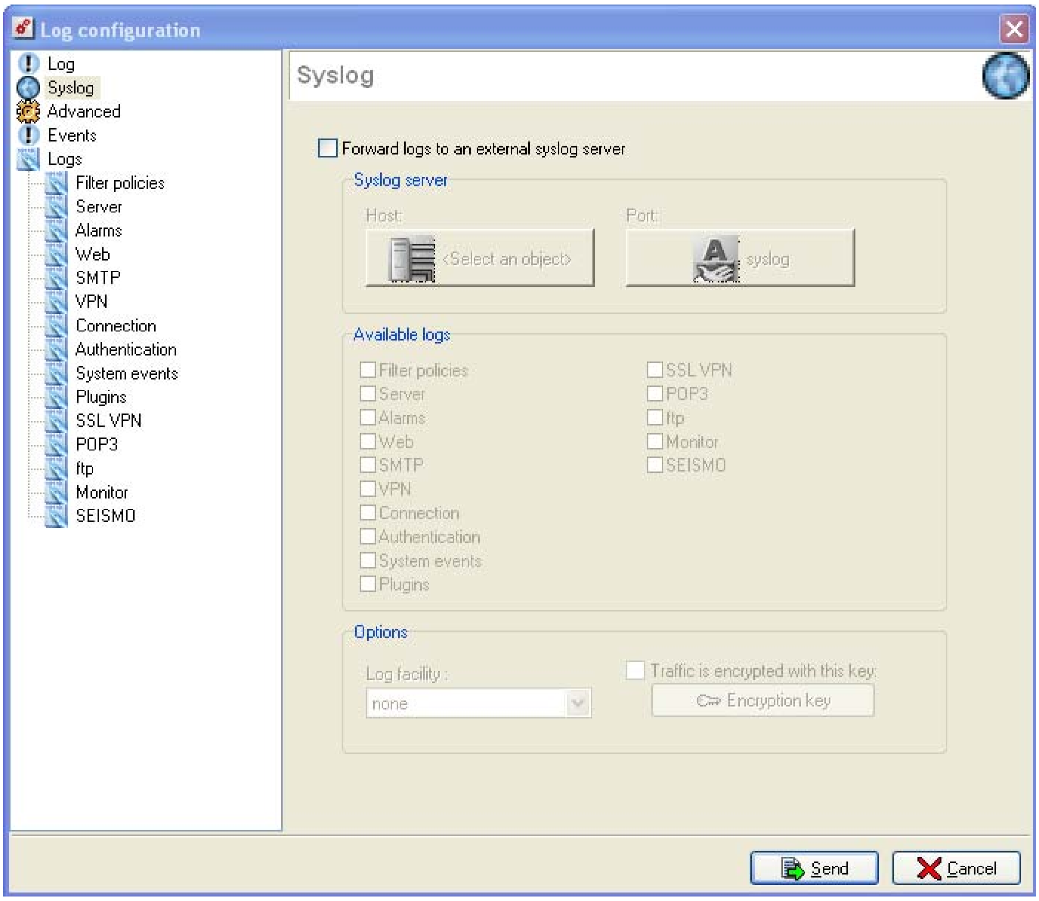
With the **log configuration** screen, you can easily allocate space for the internal log files of the firewall, and also modify the behavior of the log display system.

Figure 408: Configuring logs - Log

This screen comprises two sections:

- On the left, a tree structure setting out the **Log** menu's miscellaneous features,
- On the right: the options that can be configured.

17.1.3. Syslog Menu



□ Forward logs to an external syslog server

Syslog server

Host: <Select an object>

Port: syslog

Available logs

□ Filter policies
□ Server
□ Alarms
□ Web
□ SMTP
□ VPN
□ Connection
□ Authentication
□ System events
□ Plugins
□ SSL VPN
□ POP3
□ ftp
□ Monitor
□ SEISMO

Options

Log facility : none

□ Traffic is encrypted with this key:

Encryption key

Figure 409: Configuring logs - Syslog

Forwarding logs to an external Syslog server

The NETASQ Firewall lets you automatically send logs to a dedicated server. The logs are sent in WELF format. The server could be a SYSLOG server, the NETASQ SYSLOG or the NETASQ LOG ANALYZER.

To send logs, simply select the option **Send messages to an external syslog server** then enter the IP address of the server as well as its communication port.

You can also select the log facility (an orientation towards different files in order to sort information), as well as the categories of files to be sent (alarms, connection, web, filter, SMTP).

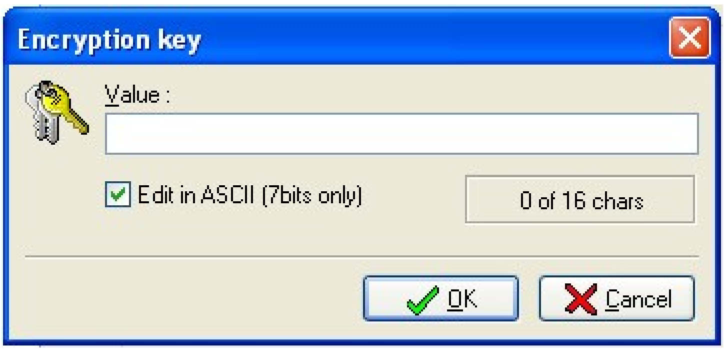
Sending logs to NETASQ SYSLOG or NETASQ LOG ANALYZER

NETASQ SYSLOG is a utility program installed on an administration host which offers a SYSLOG service to retrieve and manage logs. This option is particularly advantageous for U30 and U70 Firewalls which cannot store logs on the Firewall. The logs are therefore stored locally on the administration host.

NETASQ LOG ANALYZER is an optional powerful tool developed by NETASQ. This tool can receive logs from several Firewalls and store them in an SQL database, improving performance in data processing.

Logs can be sent to NETASQ Syslog by indicating the IP address of the host on which the option and the port is installed.

Communications between the Firewall and NETASQ SYSLOG can be encrypted in AES from the Firewall. In order to do so, you should activate the **Encrypt traffic** option and enter the encryption key used by clicking on the **Encryption Key** button.


Encryption key

Value :

☑ Edit in ASCII (7bits only)

0 of 16 chars

Figure 410: Encryption key

The encryption key can be specified in the Value field.

> **WARNING**
> Encryption can only be used to redirect logs to NETASQ SYSLOG or NETASQ LOG ANALYZER and not for any other SYSLOG server. The Traffic is encrypted with this key option must therefore be deactivated for any other Syslog server. However, it is highly recommended to activate encryption for NETASQ SYSLOG. Communications between the Firewalls and Log Analyzer are always encrypted.

Logs can also be stored on the Firewall (except for U30 and U70 models).

To configure NETASQ SYSLOG:

1 Enble the option **Forward logs to an external SYSLOG server.**

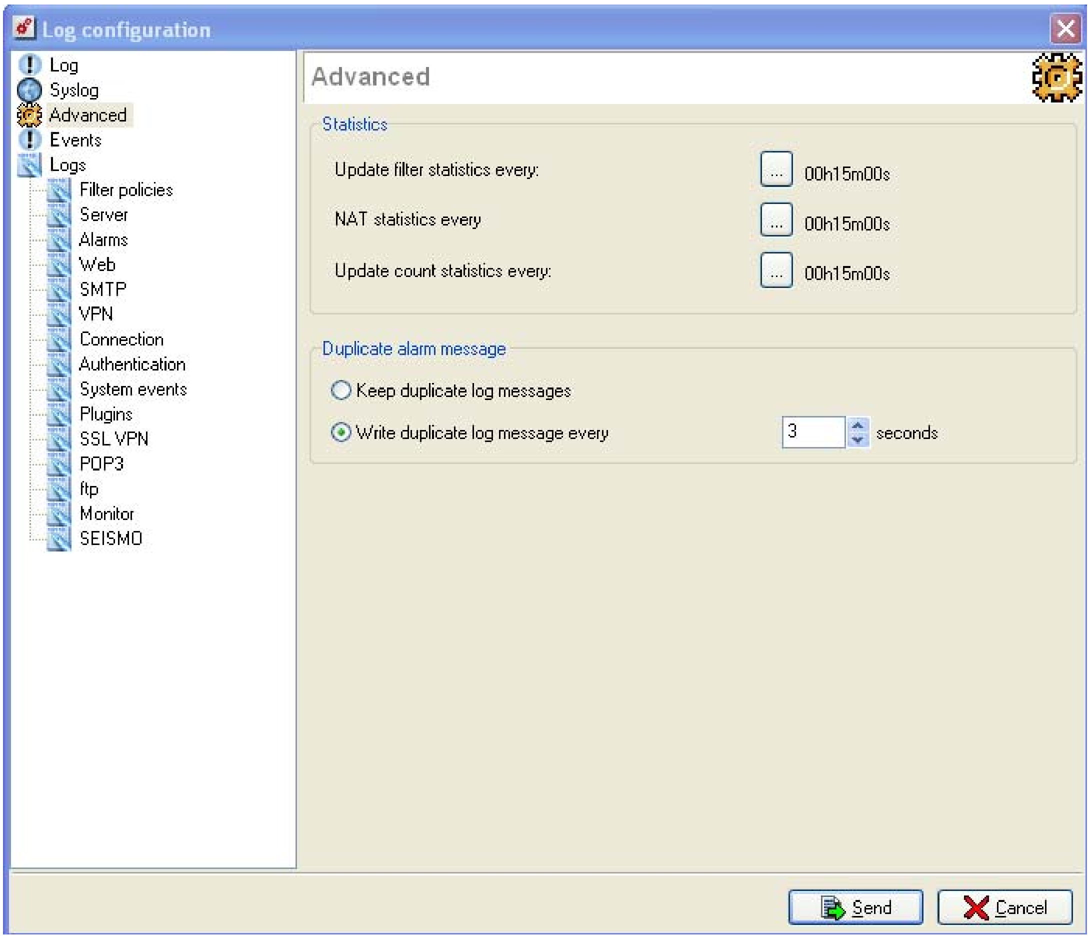
2 Specify the IP address of the host where NETASQ SYSLOG is installed, using the button **Select an object**, then click on **Syslog** and check that the value of the connection port is 514.

3 Specify the log types which will be sent from the Firewall to NETASQ SYSLOG (Alarm, Connection, web, VPN, Authentication, Filter, SMTP, System, SLL VPN, Plugins, POP3, Monitor, SEISMO…).

4 The Log facility has to be set at **none.**

5 **Traffic is encrypted with this key**: Traffic passing between the Firewall and NETASQ SYSLOG may be encrypted in AES. To activate encryption, select the option **Traffic is encrypted with this key**, then click on the **Encryption key** button. Enter the encryption key used (the same key value will be configured on NETASQ SYSLOG). **Activation of encryption on NETASQ SYSLOG is compulsory**.

17.1.4. Advanced Menu



Statistics

Update filter statistics every: ... 00h15m00s

NAT statistics every ... 00h15m00s

Update count statistics every: ... 00h15m00s

Duplicate alarm message

○ Keep duplicate log messages

● Write duplicate log message every 3 seconds

Figure 411: Configuring logs – Advanced

Statistics

This window allows you to configure several types of statistics:

- The duration of updates for filter statistics.
- The duration of NAT statistics.
- Refreshment rate of filter rules containing the “Count” option.

In each section, simply select the frequency with which statistics will be calculated. A report will be generated for each period you configure.

Once your choices have been made, click on the **Send** button to send the information to the NETASQ Firewall.

We recommend that you use granularities of less than a day only for a short period so as not to flood the NETASQ Firewall’s disk.

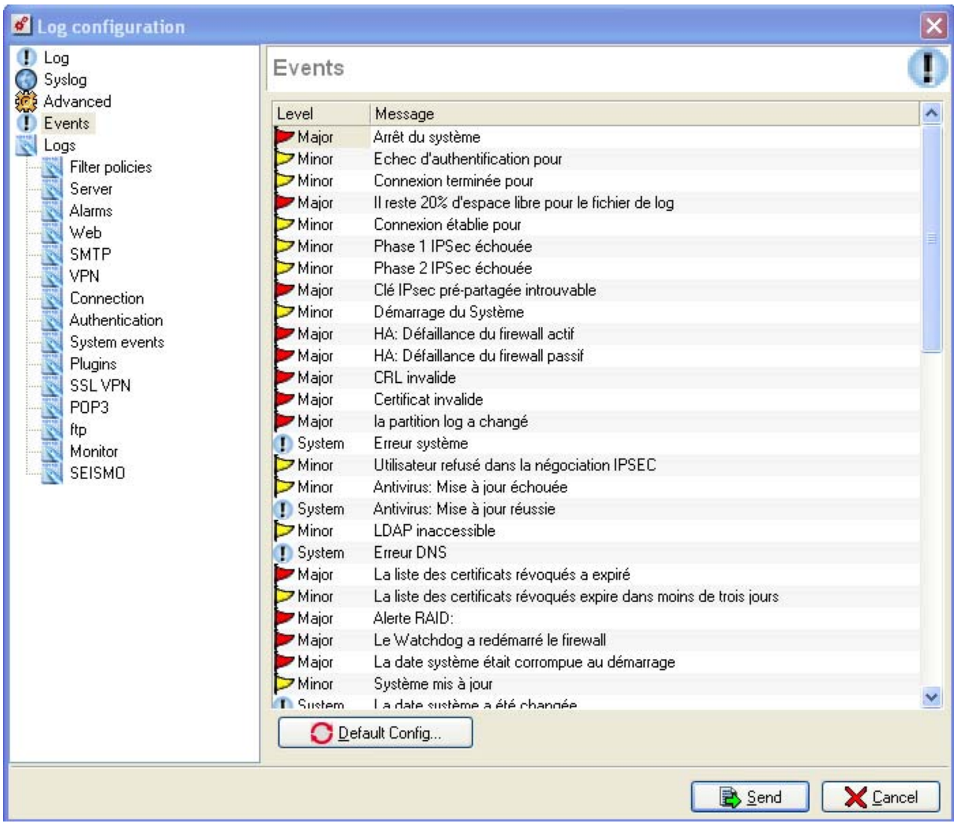
Duplicate alarm messages

Two options in the “Duplicate alarm messages” zone are available in the advanced menu:

- **Keep duplicate log messages:** in this case, all alarms are saved in the logs (even if they are identical).
- **Write duplicate log message every:** here, you select a time window in which an alarm is saved only once in the logs even if the alarm has been raised several times.

17.1.5. Events menu

This menu allows you to modify default actions to take when certain event types are raised. These do not depend on traffic conditions. The list set out in this window groups together all the events that the Firewall can generate.



Level	Message
Major	Arrêt du système
Minor	Echec d'authentification pour
Minor	Connexion terminée pour
Major	Il reste 20% d'espace libre pour le fichier de log
Minor	Connexion établie pour
Minor	Phase 1 IPSec échouée
Minor	Phase 2 IPSec échouée
Major	Clé IPsec pré-partagée introuvable
Minor	Démarrage du Système
Major	HA: Défaillance du firewall actif
Major	HA: Défaillance du firewall passif
Major	CRL invalide
Major	Certificat invalide
Major	la partition log a changé
System	Erreur système
Minor	Utilisateur refusé dans la négociation IPSEC
Minor	Antivirus: Mise à jour échouée
System	Antivirus: Mise à jour réussie
Minor	LDAP inaccessible
System	Erreur DNS
Major	La liste des certificats révoqués a expiré
Minor	La liste des certificats révoqués expire dans moins de trois jours
Major	Alerte RAID:
Major	Le Watchdog a redémarré le firewall
Major	La date système était corrompue au démarrage
Minor	Système mis à jour
System	La date système a été changée

Figure 412: Configuring logs – Events

The grid has two parts:

- On the left, the actions to take when an event is raised,
- On the right, the type of event.

The possible actions in the “Level” column are:

Ignore	No notification.
Minor	Generates a minor alarm
Major	Generates a major alarm
System	Generates an entry in the system log.

The **Default configuration** button enables you to redefine event parameters in their original configuration. When you click on this button, the following message will appear:

"The default configuration will be applied to the firewall. Continue?"

Once your modifications have been made, click on **Send** to send the information to the NETASQ Firewall.

17.1.6. Logs

This menu enables you to configure several log-related parameters: size, action to take when a threshold is reached, etc. When you select this menu, the following window will show you a graphical preview of the current distribution of space reserved for each log file type.

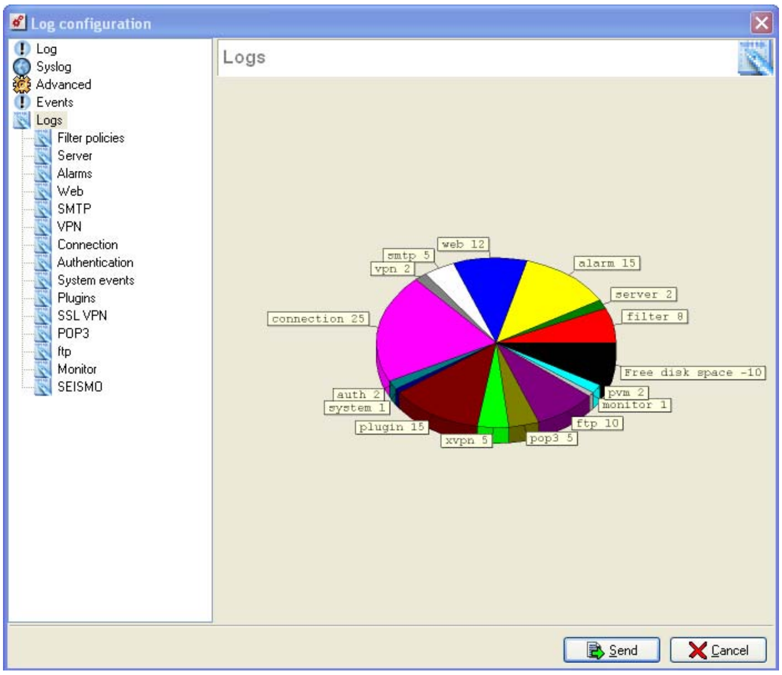


Figure 413: Configuring logs - Logs

17.1.6.1. Log file management

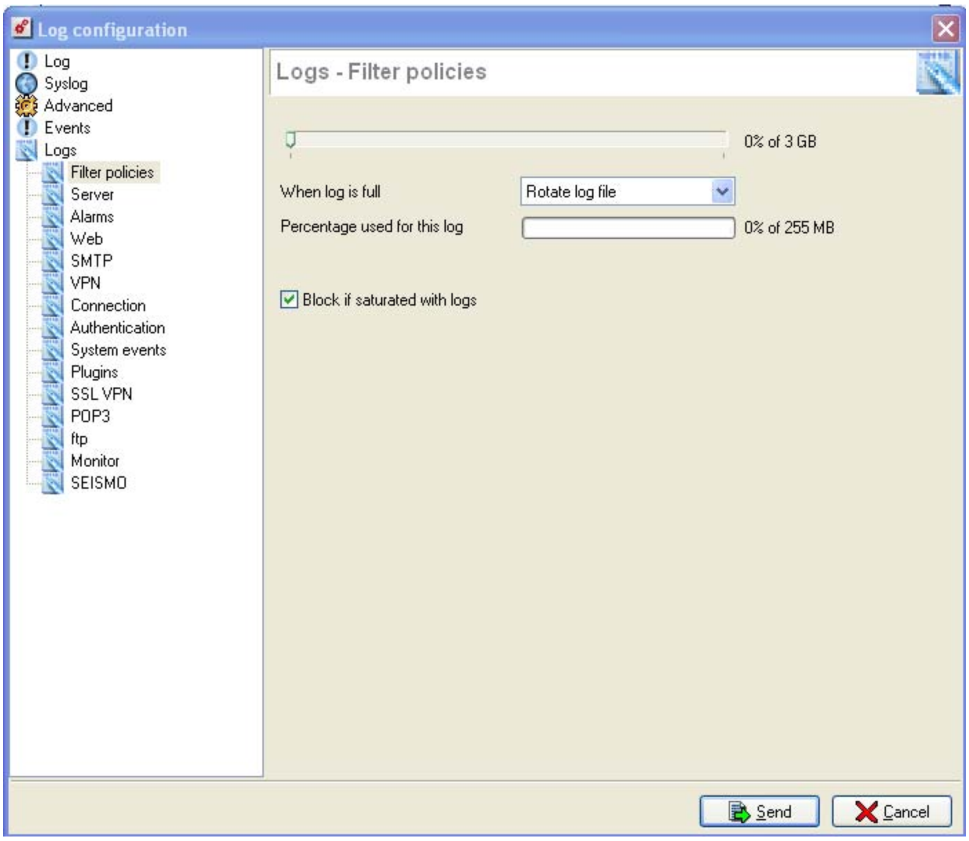
For each log menu (filter, server, alarm, web, SMTP, VPN, connection, auth, system, plugin, xvpn, pop3 and monitor), you are able to restrict the size of the filtering log file by selecting the file size by percentage of space reserved for log files.

You may also choose the action to take once this limit has been reached. Choices of action are:

- **Rotate log file**: the oldest files will be replaced by the most recent ones
- **Stop writing to log**: logs will be no longer written on the Firewall
- **Shutdown firewall**: the Firewall will not really shut down, but blocks all traffic except NETASQ UNIFIED MANAGER’s connections from the internal network.

A graph representing the current percentage of space used is also displayed.

17.1.6.2. Filter policies



Logs - Filter policies

0% of 3 GB

When log is full: Rotate log file

Percentage used for this log: 0% of 255 MB

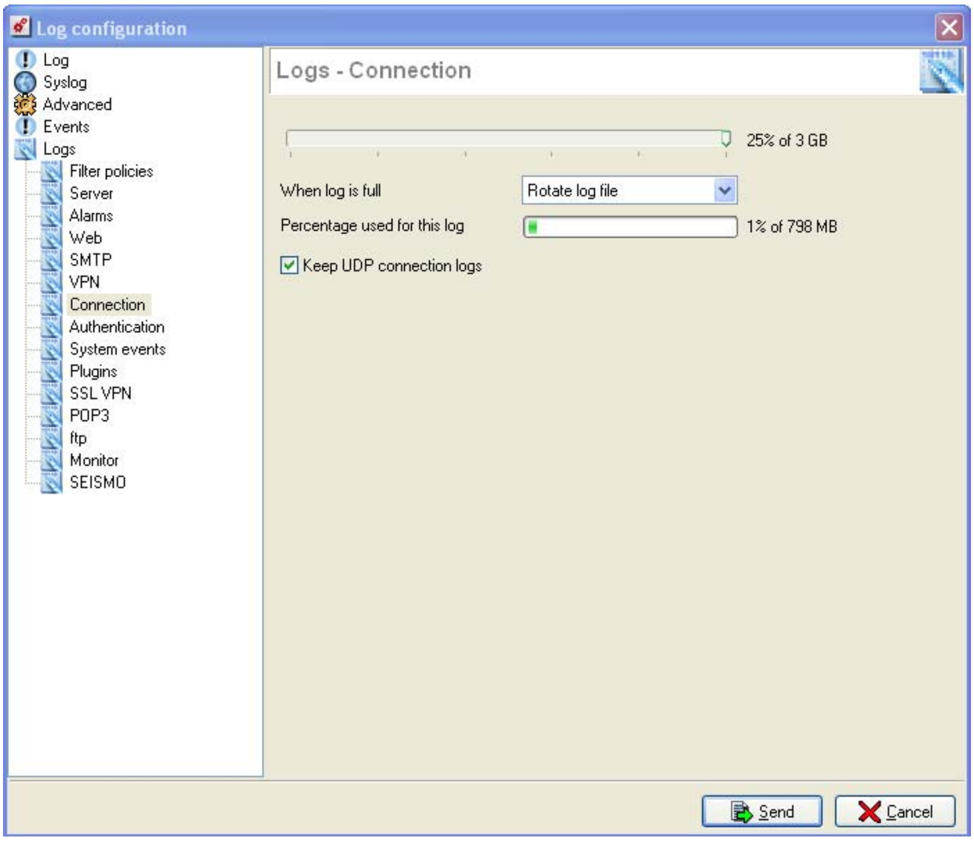
☑ Block if saturated with logs

Figure 414: Configuring logs – Filter policies

The option **Block if saturated with logs** in the menus **`Filter`** and **`Alarm`** defines whether filter-authorized traffic will still be blocked if logs cannot be saved (e.g. when reserved space is saturated or the appliance is overloaded). This condition only applies to “pass” traffic with the “log” option selected in the filter rule.

If this option is not selected, “pass” traffic (on which the **Log** option has been selected) will be authorized even if it cannot be logged.

17.1.6.3. Connection



25% of 3 GB

When log is full: Rotate log file

Percentage used for this log: 1% of 798 MB

☑ Keep UDP connection logs

Figure 415: Configuring logs - Connection

The option **Keep UDP connection logs** in the **Connection** menu allows logging UDP datagrams as well. due to the nature of this traffic type (1 datagram sent = 1 connection), logs may be more quickly congested.

WARNING
Due to the nature of this traffic type (1 datagram sent = 1 connection), logs may be more quickly congested.

CHAPTER 2. RECEIVING ALARMS AND LOGS

17.2.1. Introduction

The NETASQ Firewall distinguishes two types of alarm:

- Major alarms
- Minor alarms

Minor alarms are set off by packets arriving on the NETASQ Firewall and corresponding to a filter rule or event for which you have set the "Minor alarm" action.

The NETASQ Firewall automatically generates major alarms when a packet or an action appears genuinely suspicious.

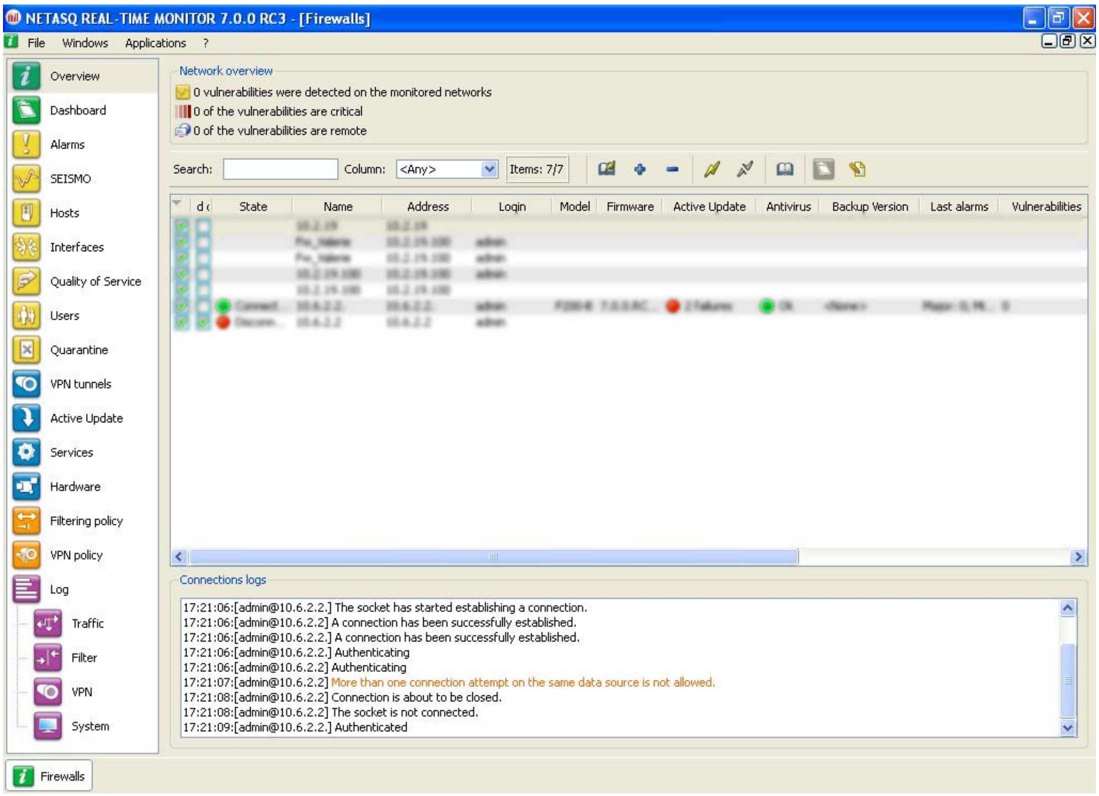
> **Example**
> For example: a SYN Flooding attack.

There are several ways of being informed of alarms raised by the Firewall:

- The alarm is sent to the connected real time monitors (the NETASQ REAL-TIME MONITOR application). To receive these alarms on a remote machine, launch the real time monitor and connect to the Firewall to be monitored.
- By e-mail. For this, enter the IP address of the SMTP server in the **SMTP (IP) server** field. You can then enter the e-mail address used for receiving alarm messages.

17.2.2. Presentation of NETASQ REAL-TIME MONITOR

➲ In the directory containing the Windows configuration software ("C:\Program Files\NETASQ\Administration Suite x.x" by default) you will find the "monitor.exe" application. Or simply go to the shortcut in Applications\Launch RealtimeMoniteur in the menu bar.



0 vulnerabilities were detected on the monitored networks
0 of the vulnerabilities are critical
0 of the vulnerabilities are remote

```
17:21:06:[admin@10.6.2.2.] The socket has started establishing a connection.
17:21:06:[admin@10.6.2.2] A connection has been successfully established.
17:21:06:[admin@10.6.2.2.] A connection has been successfully established.
17:21:06:[admin@10.6.2.2.] Authenticating
17:21:06:[admin@10.6.2.2] Authenticating
17:21:07:[admin@10.6.2.2] More than one connection attempt on the same data source is not allowed.
17:21:08:[admin@10.6.2.2] Connection is about to be closed.
17:21:08:[admin@10.6.2.2] The socket is not connected.
17:21:09:[admin@10.6.2.2.] Authenticated
```

Figure 416: Overview

The real time monitor provides a simple display of connections transiting via the Firewall, along with any alarms it has generated.

The monitor receives information from the Firewall if it is connected. You can minimize this window by clicking on the ▬ button. The monitor then runs in the background. To display it on screen once more, double-click on the icon located on the task bar (next to the clock).

By default, this monitor can only be run on a machine connected to the internal network and must be running permanently in order to avoid missing any alarms. You can use it remotely (through the internet) but you would have to explicitly authorize the service (Firewall_srv) in the filter rules.

REMARKS

1) When an alarm is received, NETASQ REAL-TIME MONITOR is activated and a sound may be produced.
2) If the alarm does not reach the monitor, it is nevertheless logged and the "minor" indicator on the front panel of the NETASQ Firewall comes on briefly. Furthermore, if you have entered an e-mail address for sending the alarms, the alarm will be sent to this address.
3) Alarm generation is very handy for tracking possible abuse. You only need to add the “minor alarm” option to the rule whose use you want to track in the filter rules.
4) However, excessive use of this feature will rapidly make it unusable due to the size of the resulting log files, the number of alarms displayed on your monitor and the monitor window constantly coming to the front.

PART 18: MAINTENANCE

18.1.1. Introduction

18.1.1.1. For this chapter, you will need to have completed these steps

- Part 2/Chapter 1: Graphical Interface.
- Part 2: Installation, integration and pre-configuration.

18.1.1.2. For this chapter, you will need to know

- The IP address of the NETASQ Firewall on the internal network.

18.1.1.3. Purpose of this section

It enables you to save/restore all data specific to your NETASQ Firewall.

The administrator with the **maintenance** privilege can save the following in a file on the administration workstation:

- the full configuration
- the Firewall's network configuration (Firewall's addresses, gateways, etc.),
- objects (hosts, networks, services and each group),
- filter rules,
- the LDAP database (local user database).

The file can be encrypted and signed with a password.

Restoring the configuration from a backup file requires maintenance privileges.

Finally, this section explains the method for updating appliances.

18.1.1.4. Accessing this section

- The respective dialog boxes can be accessed via the following sub-menus: **`Maintenance\Backup…`**, **`Maintenance\Restore…`**, **`Maintenance\Find Firmware`** and **`Maintenance\Update firmware`**.

> **REMARK**
> You have to be connected with modification privileges in order to carry out these modifications.

18.1.2. Backup

When you make changes to your NETASQ Firewall, for security reasons no data is stored on the computer on which NETASQ UNIFIED MANAGER is installed.

This offers an additional advantage - you can consult and configure the NETASQ Firewall from any PC equipped with the graphical interface on the internal network.

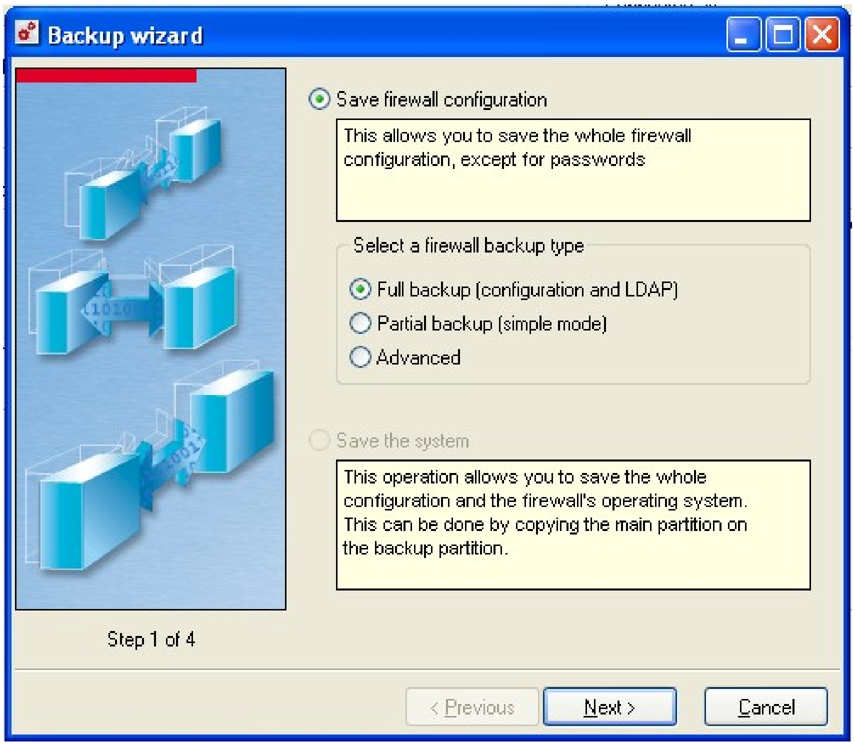
However, it is important to note that this poses a disadvantage: if you make any mistakes during configuration, or if you encounter hardware problems, or if you wish to configure several Firewalls in an almost identical way, you are inconvenienced in a way.

This is why NETASQ UNIFIED MANAGER is equipped with a function allowing you to backup/restore all or a part of your Firewall's configuration files. A backup may be encrypted and signed for the sake of confidentiality and configuration integrity.

18.1.2.1. Backing up the configuration

To back up the NETASQ appliance's configuration, select the sub-menu **`Maintenance\Backup`** from the menu bar located at the top of the Firewall Manager interface. A wizard will guide you through the steps in backing up your NETASQ appliances.

1 Step 1



● Save firewall configuration

This allows you to save the whole firewall configuration, except for passwords

Select a firewall backup type

● Full backup (configuration and LDAP)
○ Partial backup (simple mode)
○ Advanced

○ Save the system

This operation allows you to save the whole configuration and the firewall's operating system. This can be done by copying the main partition on the backup partition.

Figure 417: Backup wizard - Step 1

The first step enables defining what needs to be backed up – the configuration or the system. As indicated in the interface, the configuration backup involves saving an encrypted file containing the appliance's configuration on the administration workstation (this can be a partial or full backup). A system backup involves saving the whole system and configuration directly on the appliance, in a backup partition. Only passwords are not saved.

Type of configuration backup

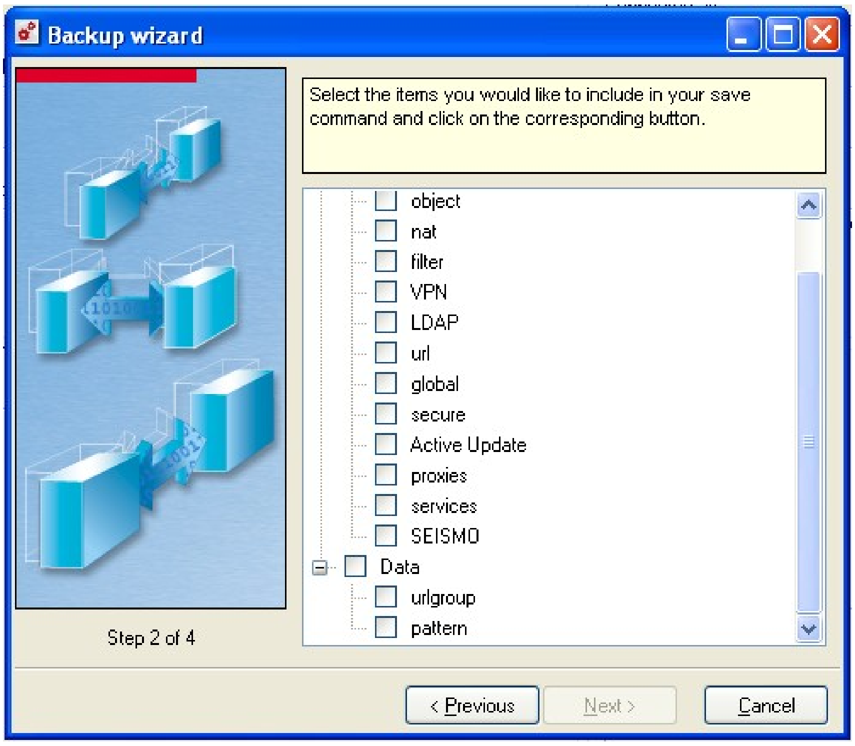
There are three types of configuration backup:

- **Full backup (configuration and LDAP):** this choice allows backing up the appliance's configuration and all the information stored in the LDAP database (user records), without additional options. This configuration backs up everything.
- **Partial backup (simple mode):** this choice allows backing up the appliance's configuration according to the administrator's preferences. Such a partial configuration allows saving, for example, the object database so that it can be restored on another product, thereby facilitating the administrator's job.
- **Partial backup (advanced mode):** this choice, which is more granular than the "simple" option, enables a more specific selection for the backup.

The windows in Step 2 vary according to the selected type of backup.

2 Step 2

Partial backup (simple mode)



Select the items you would like to include in your save command and click on the corresponding button.

- □ object
- □ nat
- □ filter
- □ VPN
- □ LDAP
- □ url
- □ global
- □ secure
- □ Active Update
- □ proxies
- □ services
- □ SEISMO
- ⊟ □ Data
  - □ urlgroup
  - □ pattern

Figure 418: Backup wizard - Step 2

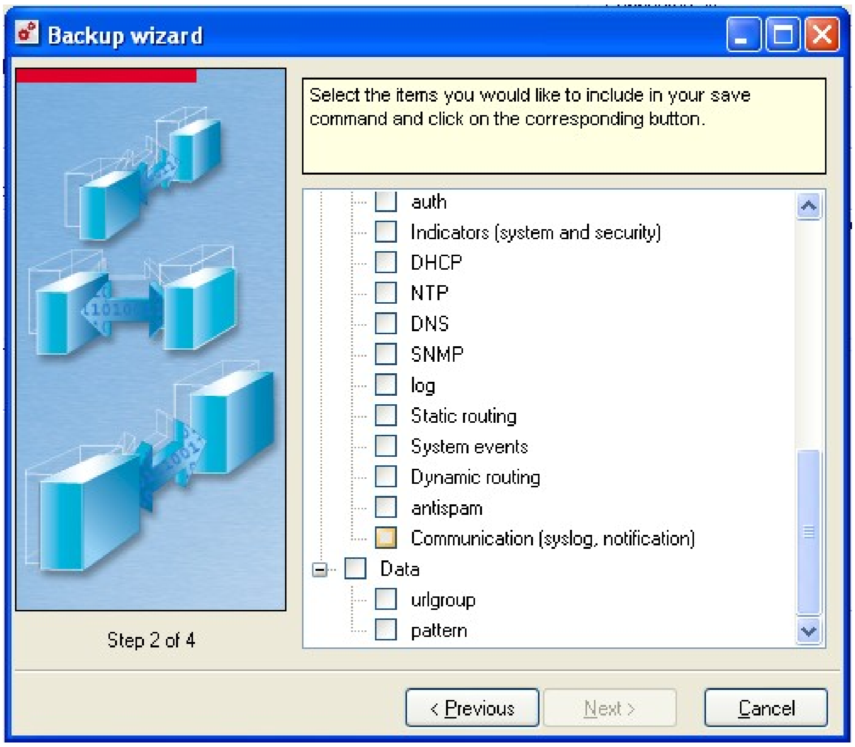
When a simple backup is selected, the options are as follows:

- **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 Policy**: all the address translation configuration slots
- **Filter policies:** all filter configuration slots.
- **vpn**: all configuration slots for IPSec VPN tunnels, pre-shared keys and certificates stored in the `Certificates` menu.
- **LDAP**: 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
- **Services**: configuration of the appliance's services, DHCP, DNS, NTP and SNMP.
- **SEISMO**: configuration of the network vulnerability detection module.
- **Data:** selects all the elements classified under this header.
- **URL groups:** all dynamic URL groups, obtained via Active Update.
- **Contextual signatures:** ASQ signatures obtained via Active Update.

Select the elements you wish to include in your backup by checking them.

Partial backup (advanced mode)



Backup wizard

Select the items you would like to include in your save command and click on the corresponding button.

- □ auth
- □ Indicators (system and security)
- □ DHCP
- □ NTP
- □ DNS
- □ SNMP
- □ log
- □ Static routing
- □ System events
- □ Dynamic routing
- □ antispam
- □ Communication (syslog, notification)
- □ Data
  - □ urlgroup
  - □ pattern

Step 2 of 4

Figure 419: Backup wizard - Step 2

When an advanced backup is selected, the 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.
- **LDAP**: 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 automatic appliance update module.
- **Proxies**: configuration of HTTP, SMTP and POP3 proxies.
- **SEISMO**: configuration of the network vulnerability detection module.
- **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.
- **Slot scheduler**: 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:** appliance’s DHCP service.
- **NTP:** appliance’s NTP service.
- **DNS:** appliance’s DNS service.
- **SNMP**: 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**: configuration of the Antispam module.
- **Communication (syslog, notifications):** appliance’s communication module, notably the sending of logs to to syslog servers and the sending of alarm notifications to administrators.
- **Data:** selects all the elements classified under this header.
- **URL groups:** all dynamic URL groups, obtained via Active Update.
- **Contextual signatures:** ASQ signatures obtained via Active Update.

Select the elements you wish to include in your backup by checking them.

3 Step 3

The following window will appear:

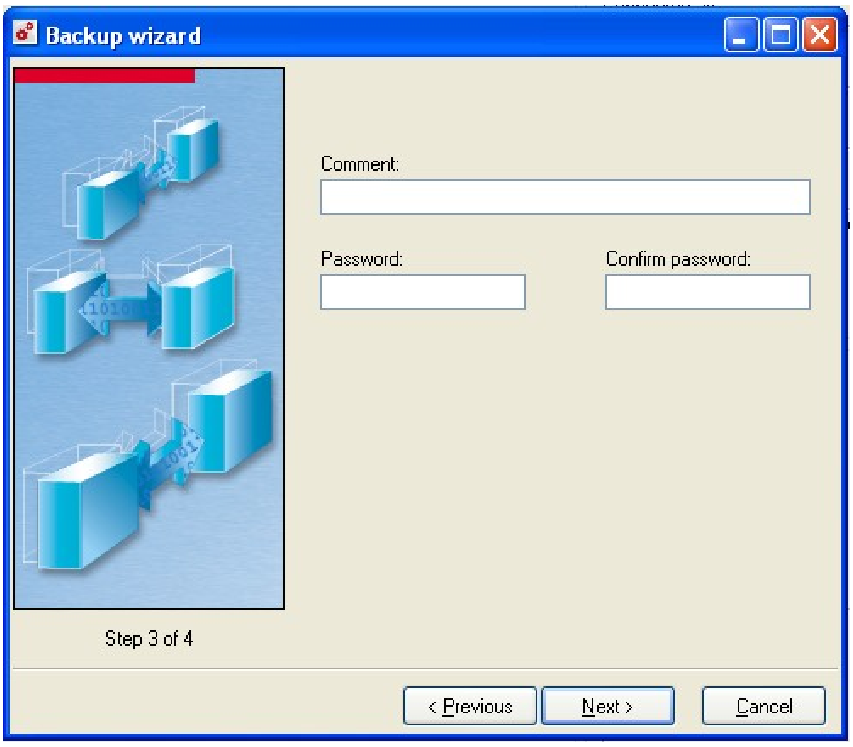


Figure 420: Backup wizard - Step 3

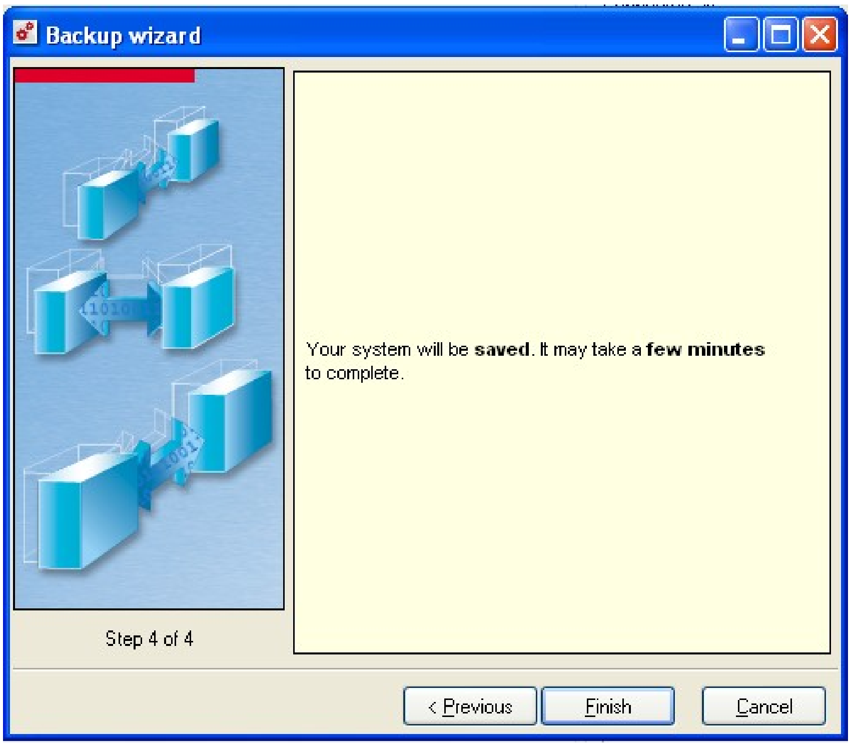
Name your backup and choose its location.

- **Comment**: This description will be displayed when the configuration is restored. In this way you can back up several times and identify each backup.
- **Password** and **confirm password:** You can also encrypt the backup so that it cannot be restored on another Firewall where it can be viewed. In that case specify a password to encrypt it.

WARNING

If the backup is not stored in a reliable and secure medium, you are advised to enable encryption.

4 **Step 4**



Your system will be **saved**. It may take a **few minutes** to complete.

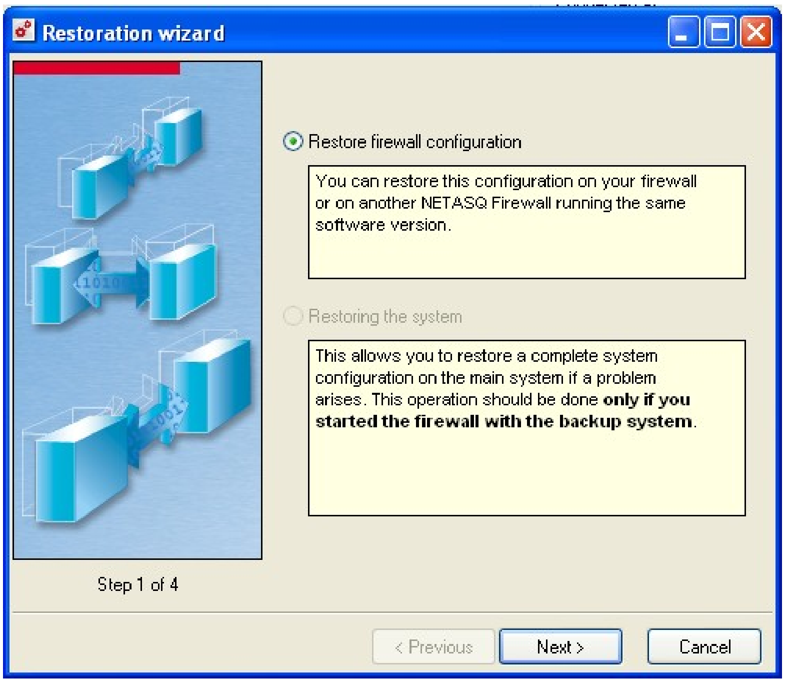
Figure 421: Backup wizard - Step 4

Click on **Finish** to perform the backup.

18.1.3. Restoring the configuration

To restore a configuration on a NETASQ appliance, select the sub-menu **`Maintenance\Restore`** in the menu bar at the top of the NETASQ UNIFIED MANAGER interface. A wizard will guide you through the steps in restoring your NETASQ appliances.

1 Step 1: restoring the firewall and the system



● Restore firewall configuration

You can restore this configuration on your firewall or on another NETASQ Firewall running the same software version.

○ Restoring the system

This allows you to restore a complete system configuration on the main system if a problem arises. This operation should be done **only if you started the firewall with the backup system**.

Figure 422: Restoration wizard - Step 1

In the first step of the wizard, the system can be restored. Click on **Next** to continue.

REMARK
This configuration can be restored on your firewall or any other NETASQ firewall in the same software version.

2 Step 2: Restoration file

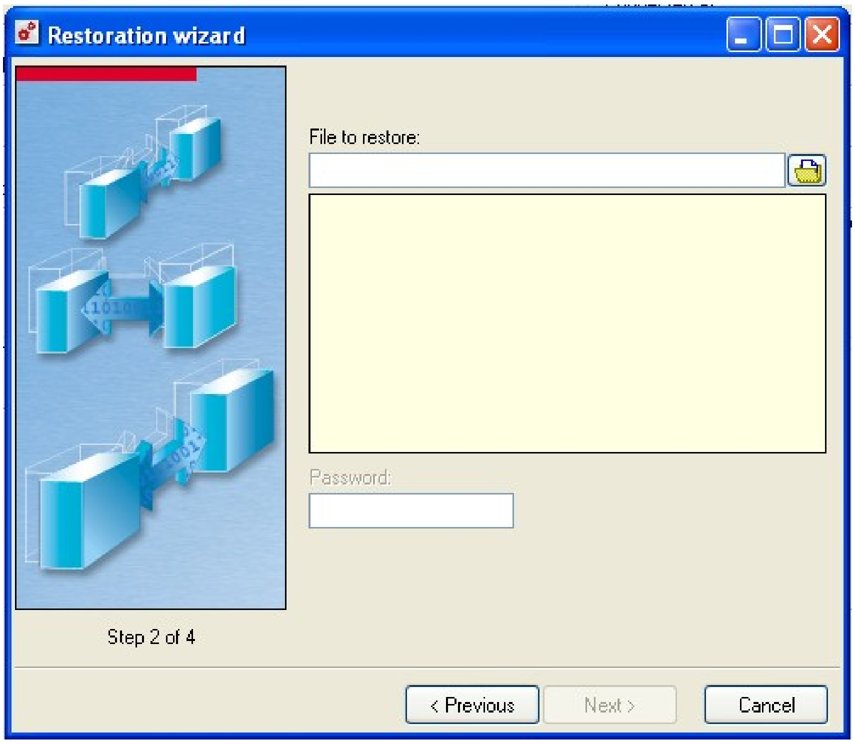
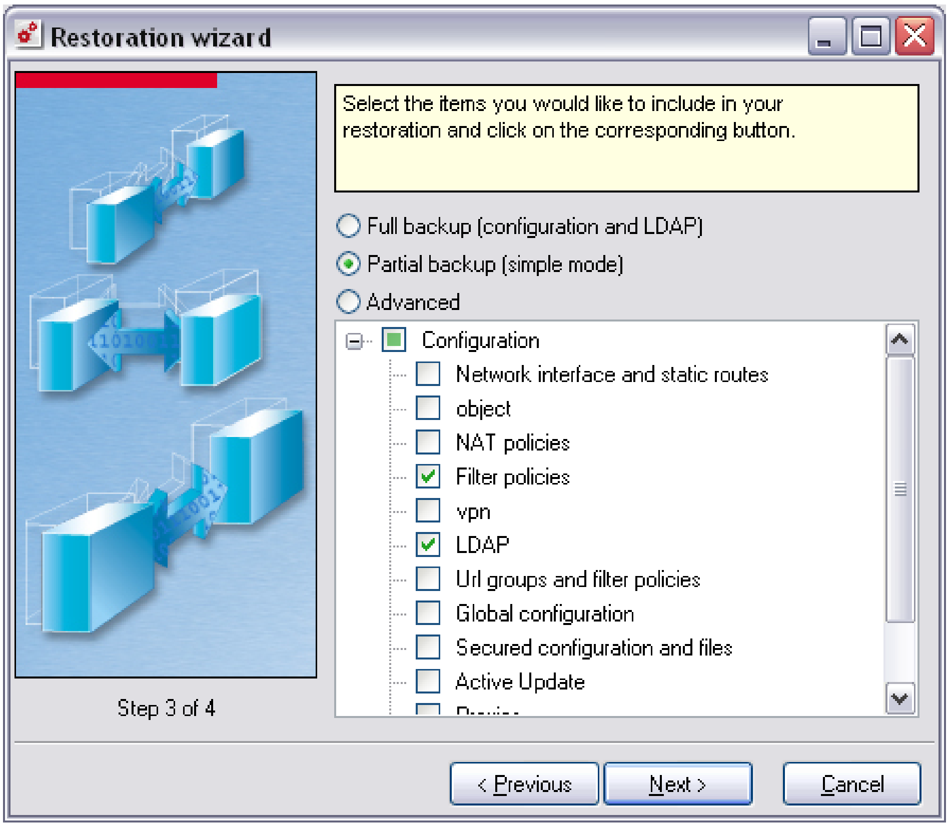


Figure 423: Restoration wizard - Step 2

Indicate the backup file you wish to restore. A description of the backup will appear and will allow you to differentiate the different backups.

3 Step 3: Items to be restored



Select the items you would like to include in your restoration and click on the corresponding button.

○ Full backup (configuration and LDAP)
● Partial backup (simple mode)
○ Advanced

- 🟩 Configuration
  - □ Network interface and static routes
  - □ object
  - □ NAT policies
  - ☑ Filter policies
  - □ vpn
  - ☑ LDAP
  - □ Url groups and filter policies
  - □ Global configuration
  - □ Secured configuration and files
  - □ Active Update

Figure 424: Restoration wizard - Step 3

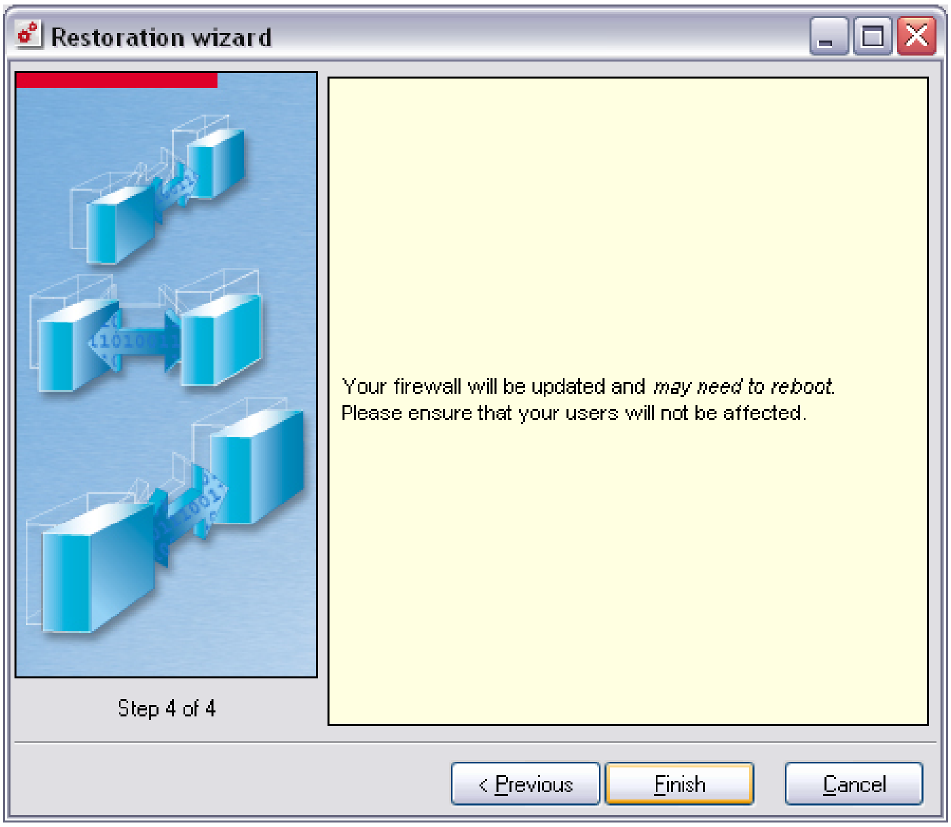
The restoration options will then appear. In the same way as for configuration backups, there are three types of restoration operations, which refer to the three types of backup. Refer to the section “Backing up the configuration” for more information.

> **WARNING**
> You are advised to carry out a configuration file backup each time you make major modifications.

If you only wish to back up a slot, you can use the **copy/paste** function.

> **WARNING**
> Passwords are not saved. They stay the same even after a backup or restoration.

4 **Step 4: Update**



Your firewall will be updated and *may need to reboot*.
Please ensure that your users will not be affected.

Figure 425: Restoration wizard - Step 4

A message will appear, informing you that the firewall would have to be rebooted for an update. Click on **Finish** to restore a configuration.

18.1.4. Warning regarding system backups

This feature allows you to save the whole configuration and the Firewall's operating system (disk image). This allows switching to this backup when the main system is down (hard disk malfunction, unsuccessful update, etc).

Once your configuration is up and running you can carry out a system backup.

> **WARNING**
> Backing up the system may slow down the Firewall when it is in the process of saving (approximately 1 minute).

If there is a problem you should reboot and start up on the system backup.

To do so you need only be connected in console mode (keyboard and screen) when you boot. When the start-up menu appears type 2 to start up on the backup

Once the Firewall starts up you can access it with the graphical interface to re-establish the backup on the main system.

➲ You can also reboot on a partition of your choice via the menu **`Maintenance\Reboot partition`** if there is one on the firewall.

18.1.5. Updates

Every update comprises independent packets. For a major update, all the packets are installed whereas in a minor update, only modified packets are installed.

There are two types of update:

- updates of the Firewall software.
- updates of the configuration graphical interface (NETASQ UNIFIED MANAGER and NETASQ REAL-TIME MONITOR).

The update of the NETASQ Firewall's software functions is a maintenance operation. You will understand that the update of system files on the NETASQ Firewall is a delicate operation which involves interrupting users' service.

WARNING
The update must always be carried out in the following order:

1. Update the Firewall software from the former graphical interface.
2. Uninstall the former configuration graphical interface if you don't want to keep it. Install the new configuration graphical interface.
3. In the case of major updates, it is important to follow the order when updating software; the Firewall will block the passage from an old version to a much more recent version without the intervening updates.

18.1.5.1. Updating the graphical interface

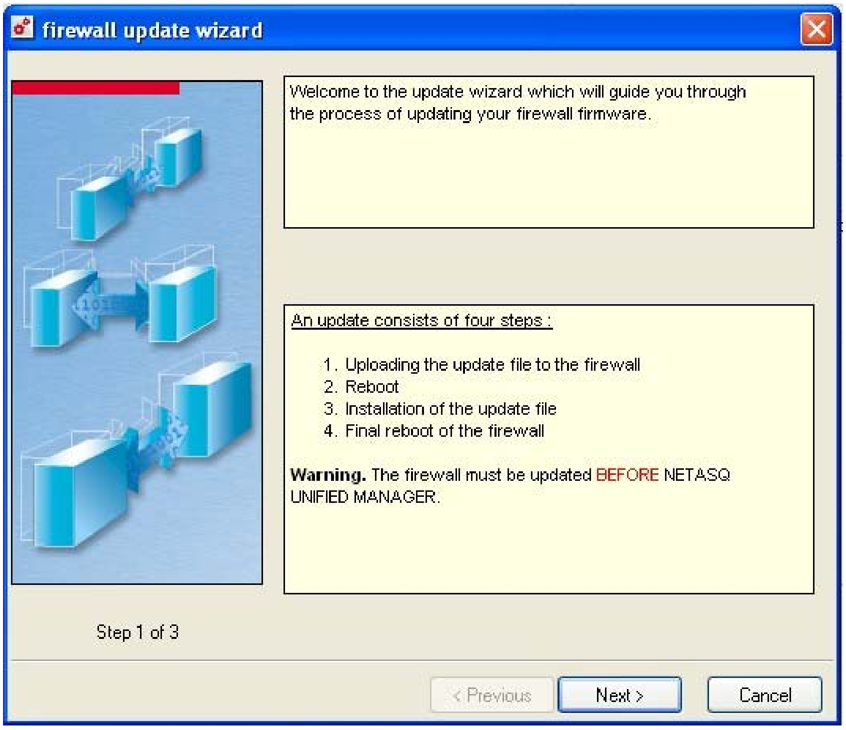
This update is a simple software reinstallation.

You should have a prior backup of the installation on the computer on which you want to install and run it.

18.1.5.2. Updating Firewall

➲ It is very easy to update the Firewall through the graphical interface via the menu **`Maintenance\Update firmware`**.

1 Step 1: Welcome



firewall update wizard

Welcome to the update wizard which will guide you through the process of updating your firewall firmware.

An update consists of four steps :

1. Uploading the update file to the firewall
2. Reboot
3. Installation of the update file
4. Final reboot of the firewall

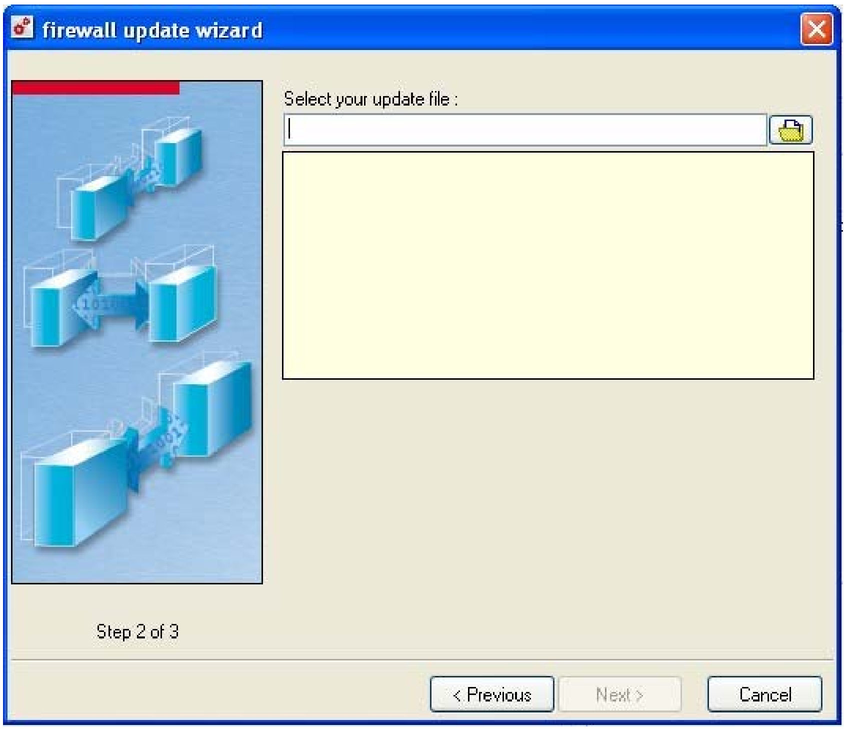
Warning. The firewall must be updated BEFORE NETASQ UNIFIED MANAGER.

Step 1 of 3

Figure 426: Firewall update wizard - Step 1

The first screen will information you that there are 4 steps in the update.

2 Step 2: Selecting the update file



firewall update wizard

Select your update file :

Step 2 of 3

Figure 427: Firewall update wizard - Step 2

The wizard asks you for the location of the file to be updated. You must download this file, which has a **.maj** extension, from NETASQ's web site (www.netasq.com).

Check the update information displayed when inserting the update file in the wizard.

3 Step 3: Message

Then you will see a warning message reminding you that this update involves rebooting the Firewall and that it will sever connections momentarily.

At this level you will also see the lowest version you need to carry out this update.

During the update a progress window is displayed. It indicates that the update is in progress.

When the file has been sent the message informs you that the file has been transferred and the Firewall is rebooting.

At the next connection, you will have a message indicating the result of the change of version.

High availability

If you have two Firewalls in high availability, it is possible for you to update the passive Firewall before the active Firewall (Cf. Part 14: High availability).

Certified update

To check whether a version or update has been certified, connect to NETASQ's website (www.netasq.com) then log in with your account particulars in the Client Corner. In the "Download Center", click on the link **Latest Updates** to check whether the latest version has been certified or on the link **Previous updates** to verify certified versions from a list of previous updates. Each certified version will be indicated.

Downgrading to a lower version

Downgrades can no longer be done. For more information on this, please contact your certified partner or NETASQ's TAC.

18.1.5.3. Remarks

REMARKS

1) The update procedure does not alter your configurations files; these are stocked on the NETASQ Firewall. Configuration files are updated at the same time as the Firewall.

2) The update of system files on the NETASQ Firewall does not systematically involve an update of the remote configuration software. If it does, it will be stipulated when the new version is being downloaded.

3) Conversely, the update of the remote configuration software does not systematically involve an update of the NETASQ Firewall's system files. If it does, it will be stipulated when the new version is downloaded.

WARNING
Modified (faulty, altered, compromised, etc) updates cannot be installed as the update file is encrypted and therefore requires decryption mechanisms and keys from the remote configuration software in order to carry out the update operation.

18.1.6. Web update

The NETASQ Firewall is a security product that often evolves to protect the network from increasingly sophisticated threats. Regular updates are essential for taking into account the new developments, and software programs in the administration suite have to be updated in order to manage new features.

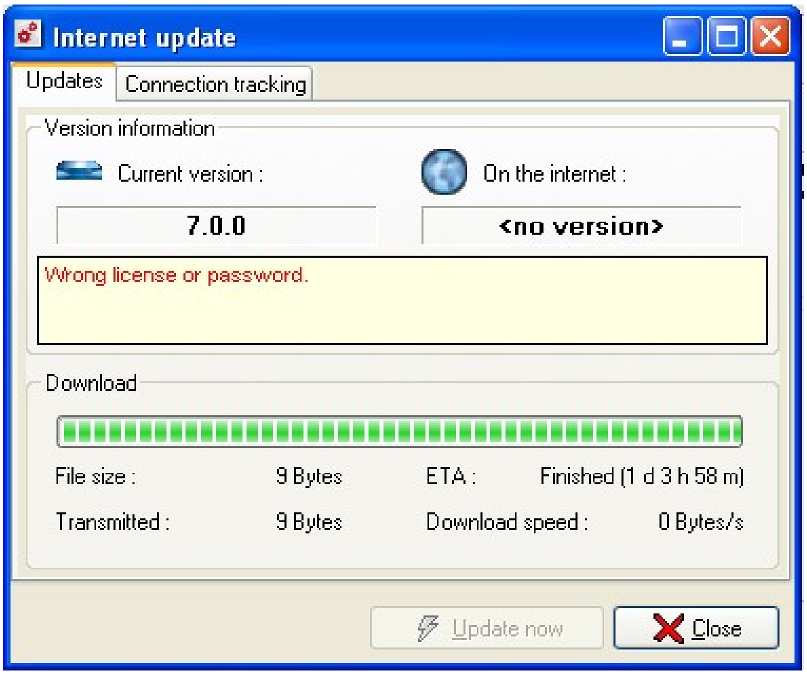
Scheduling mechanisms covered in the section `Options\Preferences\Website access` can look for Firmware and Administration Suite updates automatically or manually.

This section describes the menus that enable manually searching for updates. To access them in NETASQ UNIFIED MANAGER, select the following:

- **`Options\Preferences\Website access`**: to start looking for updates of NETASQ Firewall administration suite products manually.
- **`Maintenance\Find firmware`**: to start looking for updates of NETASQ Firewall firmware products manually.

18.1.6.1. Updating the Administration Suite and Firmware

➲ This update is accessible via the menu **`Maintenance\Check for firmware`**.



Version information
Current version : 7.0.0
On the internet : <no version>

Wrong license or password.

Download
File size : 9 Bytes
ETA : Finished (1 d 3 h 58 m)
Transmitted : 9 Bytes
Download speed : 0 Bytes/s

Figure 428: Internet update – Updates

Updating the Administration Suite and Firmware enables the support of new features available on the Firewall, built in to ensure the most adapted protection against threats circulating on the internet.

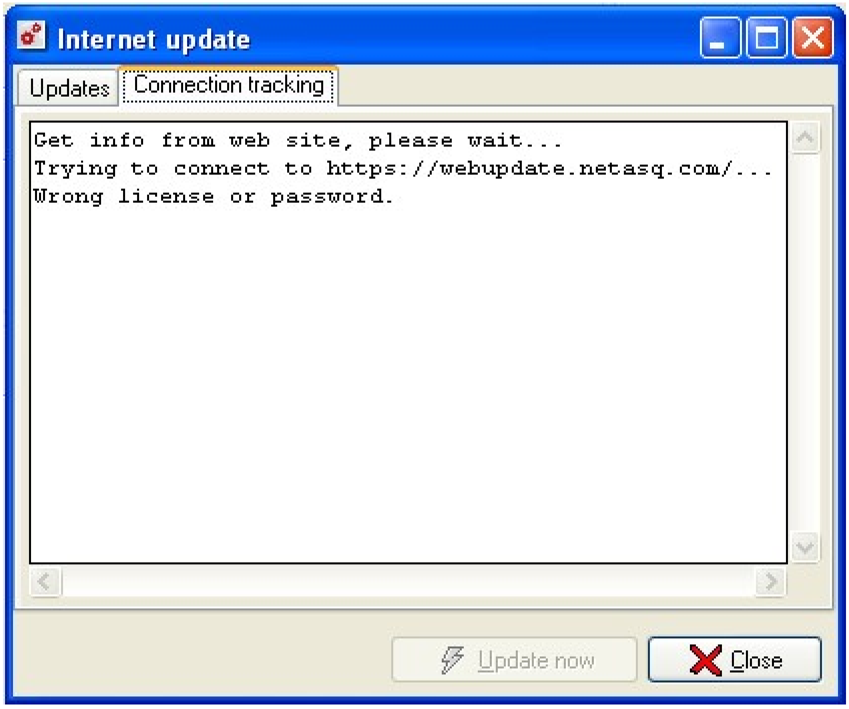
Update information

The table below describes the information displayed in the web update menu regarding the download of updates:

Update tab

Current version	Indicates the version currently installed on the workstation.
On internet	Indicates the version currently available on NETASQ's website.
Size	Size of the download file. In general, the size of an administration suite update is around 60 MB. As for a firmware update, it may take up to 11 MB.
Transmitted	Amount of data in bytes already downloaded.
Remaining	Estimated time remaining for the file to be fully received.
Speed	Speed at which the update is being downloaded.

Connection datatracking tab



```
Get info from web site, please wait...
Trying to connect to https://webupdate.netasq.com/...
Wrong license or password.
```

Figure 429: Internet update – Connection tracking

Connection datatracking for the update displays the different events that occur during the retrieval of information from the NETASQ website in each step of the download (login, password, connection, download).

Update procedure for the administration suite

The procedure for updating the administration suite is as follows:

1 Enter all information necessary for connecting NETASQ UNIFIED MANAGER to NETASQ's website (via the menu **`Options\Preferences\Website access`**).

2 Select the menu **`Maintenance\Find firmware.`**

3 When the menu appears, it will indicate whether there is currently a more recent version of the administration suite on NETASQ's website,

4 Click on **Update**. A download file will be requested if it has not already been specified in the preferences for Web Updates (see menu **`Options\Preferences\Website access`**), and the new administration suite will be installed.

> ❗ WARNING
> If the administration suite update is minor, the new administration suite will be installed over the previous administration suite, thereby overwriting it.
>
> Ensure that the connection is compatible between the new administration suite and the Firewall. NETASQ does not guarantee compatibility between major versions.

Update procedure for the NETASQ UTM Firmware

The procedure for updating the NETASQ UTM firmware is as follows:

1 Enter all information necessary for connecting NETASQ UNIFIED MANAGER to NETASQ's website (via the menu **`Options\Preferences\Website access`**).

2 Select the menu **`Maintenance\Find firmware\Updates.`**

3 When the menu appears, it will indicate whether there is currently a more recent version of the firmware on NETASQ's website,

4 Click on **Update**. A download file will be requested if it has not already been specified in the preferences for Web Updates (see menu **`Options\Preferences\Website access`**), and the firewall update menu will appear. The file to enter for the firmware update will then be indicated.

> ❗ WARNING
> Ensure that the connection is compatible between the new administration suite and the Firewall. NETASQ does not guarantee compatibility between major versions.

18.1.7. Rebooting the firewall

To reboot the NETASQ Firewall

1 Select the menu **`Maintenance\Reboot...`** The following message will appear:

"Reboot the NETASQ firewall?"

2 Click on **Yes** and NETASQ UNIFIED MANAGER will reboot remotely.
Rebooting the NETASQ Firewall will systematically block all packets and therefore all communication passing through NETASQ UNIFIED MANAGER. It will also disconnect from the configuration software in Windows (this can be seen in the main screen by the indicator changing from green to red).

You have to reconnect in order to continue configuring your NETASQ Firewall.

Once the NETASQ Firewall has been rebooted (one minute after the command has been sent), it will reactivate security and log rules in force before rebooting.

18.1.8. Shutting down the Firewall

To shut down the NETASQ Firewall

1 Select the menu `Maintenance\Shutdown...`The following message will appear:

> "Shut down the NETASQ firewall?

2 Click on **Yes** and NETASQ UNIFIED MANAGER will shut down remotely.

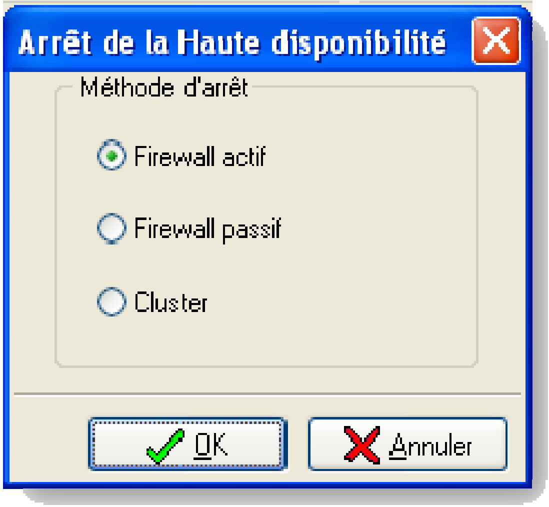
Shutting down the NETASQ Firewall will systematically block all packets passing through the NETASQ Firewall. It will also disconnect from the configuration software in Windows (this can be seen in the main screen by the indicator changing from green to red).

You have to reconnect in order to continue configuring NETASQ UNIFIED MANAGER. This remotely shuts down the NETASQ Firewall. The Firewall is shut down once the “Power” LED is off. The network adapter LEDs (IN, OUT and DMZ) remain in activity. On certain models, you may switch off the appliance with the button on the front panel of the product.

> ! WARNING
> You are strongly advised to wait for the “Power” LED to go off after a manual or remote shutdown request before cutting off power supply to the Firewall.
> Cutting off the power too quickly may lead to writing problems on the Firewall’s disk and cause hardware errors.

High Availability

When your Firewall is part of a cluster (high availability with a second Firewall), a dialog box appears. Using this screen, you can shut down the active Firewall, the passive Firewall or both.



Arrêt de la Haute disponibilité

Méthode d'arrêt

● Firewall actif

○ Firewall passif

○ Cluster

Figure 430: Shutting down HA

18.1.9. Active Update

18.1.9.1. Introduction

The Active Update module, found on all appliances, allows the firewall to automatically download updates for Antispam lists, URL databases, contextual signatures and vulnerability databases, all from a given URL list. It consists of subsystems that each correspond to a feature of the product.

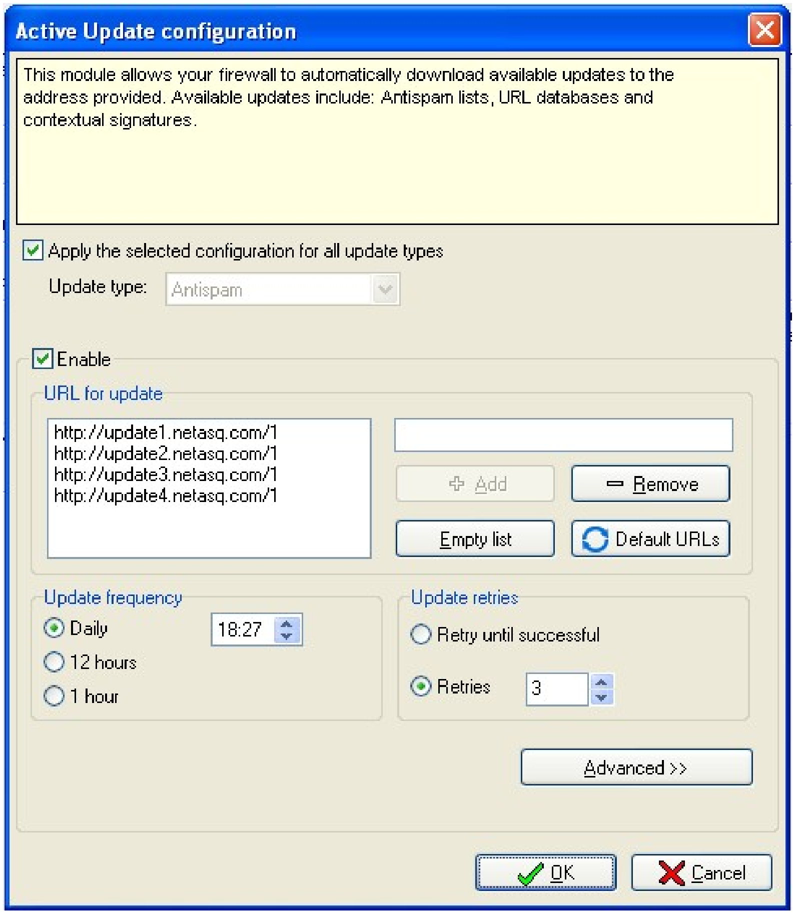
The following ASQ contextual signatures are embedded in the automatic update procedure.:

- Content Filtering
- FTP
- Malware
- SQL injection
- Vulnerability scanner
- Vulnerability service
- Web – Application
- Web – Evasion attempt
- Web – Server
- XSS – Cross Site Scripting

The **Active Update** module can be accessed from the NETASQ UNIFIED MANAGER menu directory.

WARNING
The DNS service needs to be configured in order for this module to function properly (Cf. *Part 11/Chapter 2: Services\DNS*)

NOTE
If the update fails, an automatic backtrack will occur.



Active Update configuration

This module allows your firewall to automatically download available updates to the address provided. Available updates include: Antispam lists, URL databases and contextual signatures.

☑ Apply the selected configuration for all update types

Update type: Antispam

☑ Enable

URL for update

http://update1.netasq.com/1
http://update2.netasq.com/1
http://update3.netasq.com/1
http://update4.netasq.com/1

Update frequency: ● Daily 18:27 ○ 12 hours ○ 1 hour

Update retries: ○ Retry until successful ● Retries 3

Figure 431: Configuring Active Update

18.1.9.2. Operation

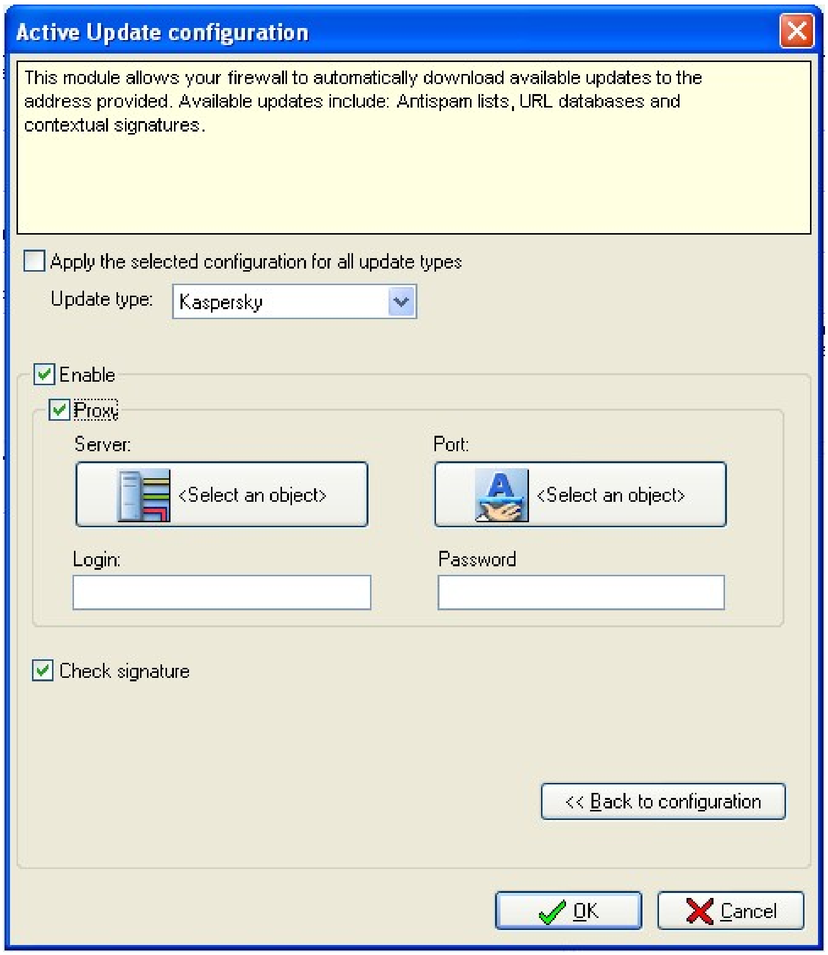
The parameters in the following table need to be configured

Apply the selected configuration to all update types	If this option is selected, global updates will be performed (meaning all possible types of updates). If not, individual updates will be performed for each type to ensure a finer configuration (e.g. in the event some files are on a different server). If the option has been unchecked, select an update type from: "Anti spam", "URLFiltering", "Patterns, "Kaspersky", "Vade retro", "Seismo".
Enable	Enables updates via Active Update for the selected type of update.
URL for the update	The user retrieves update files on the server(s) he has defined. By default, 4 URLs are defined. To add a URL, indicate its address in the text zone then click on **Add**. To remove a URL, select it and click on **Delete**. To delete the whole list of URLs, click on **Delete list**. To reinitialize the list of servers, click on **URL by default**.
Update frequency	Frequency at which to update dynamic URL lists, ASQ contextual signatures and antispam configuration. Select the frequency from: “Daily”, “12 hours” and “1 hour”.
Update retries	The field “Retry until successful”: allows you to specify whether Active Update will reattempt to update before being successful. The field “Retries” enables specifying the number of attempts to update before giving up.

Advanced	This button enables accessing the proxy activation window (See explanation below).

Activation of the proxy

If the Firewall is not directly connected to the internet but through a proxy, this proxy has to be configured so that the update can be performed automatically This configuration is accessible from the button **Advanced configuration**



Active Update configuration

This module allows your firewall to automatically download available updates to the address provided. Available updates include: Antispam lists, URL databases and contextual signatures.

□ Apply the selected configuration for all update types

Update type: Kaspersky

☑ Enable

☑ Proxy

Server: <Select an object>

Port: <Select an object>

Login:

Password

☑ Check signature

Figure 432: Configuring Active Update – Advanced configuration

Apply the selected configuration to all update types	This option allows you to look for a type of update from a drop-down list (e.g.: Kaspersky).
Enable	Automaitcally activates updates.
Proxy	By activating this option, you can select a server and a port from the object database.
Login	Indicates the login for performing automatic updates.
Password	Indicates a password for automatic updates.
Check signature	Enables indicating whether updates obtained via Active Update will be digitally signed by NETASQ's certification authority. The firewall will then check the integrity and source of the updates If this option is left unselected, you willk be able to download updates from a private server. In this case, the source and the integrity of the update will not be checked.

Back to configuration	Returns to the Active Update General configuration window.

18.1.9.3 Interface with other modules

The status of updates of “Active Update” subsystems can be viewed in the menu `Active Update` in NETASQ REALTIME MONITOR.

PART 19: MISCELLANEOUS ACTIONS

19.1.1. Introduction

19.1.1.1. For this chapter, you will need to have completed these steps

- Part 2/Chapter 1: Graphical interface.
- Part 2: Installation, integration and pre-configuration.

19.1.1.2. Purpose of this section

This part allows you to modify general and miscellaneous Firewall configuration parameters.

19.1.2. Options

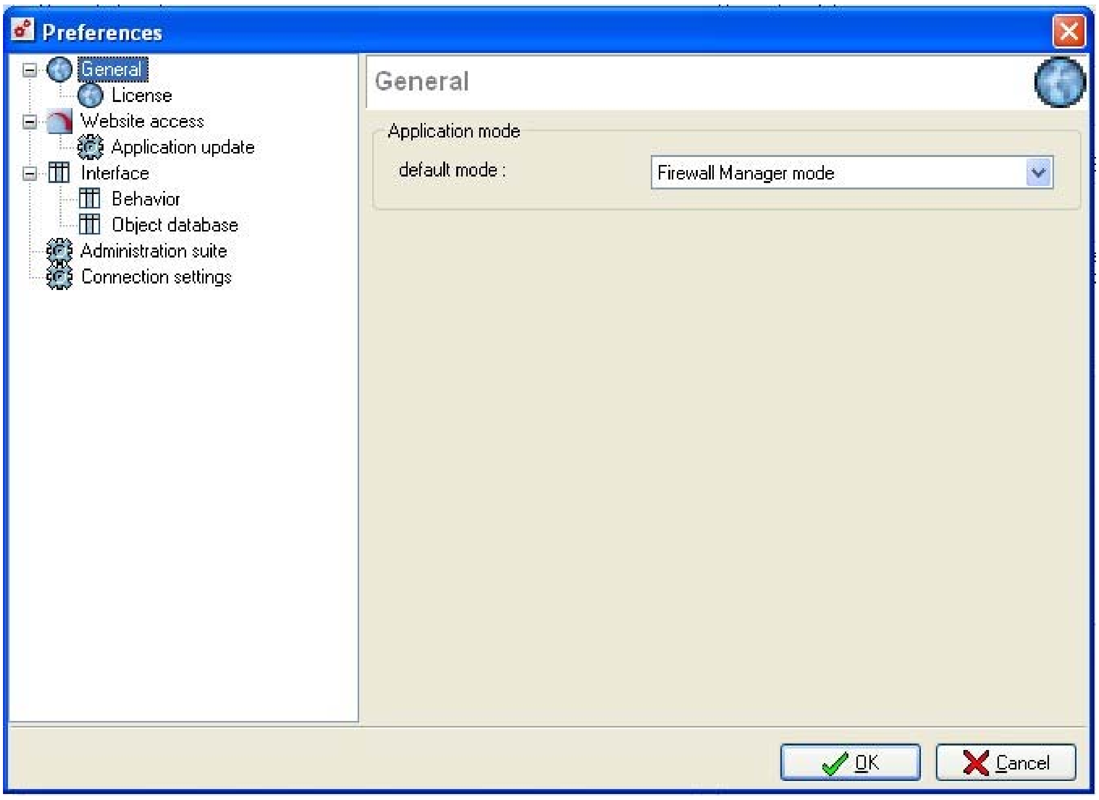
➲ Options for managing the NETASQ UNIFIED MANAGER application are found in the menu **`Options\Preferences.`** Clicking on this menu opens the configuration window for options in the NETASQ UNIFIED MANAGER interface.

The option configuration menu comprises two parts:

- On the left, a directory of the various features in the **`Preferences`** menu**.**
- On the right, options that can be configured

Whoever has access to the workstation on which the NETASQ Firewall interface has been installed, can access these features.

19.1.2.1. General



Preferences

General
License
Website access
Application update
Interface
Behavior
Object database
Administration suite
Connection settings

General

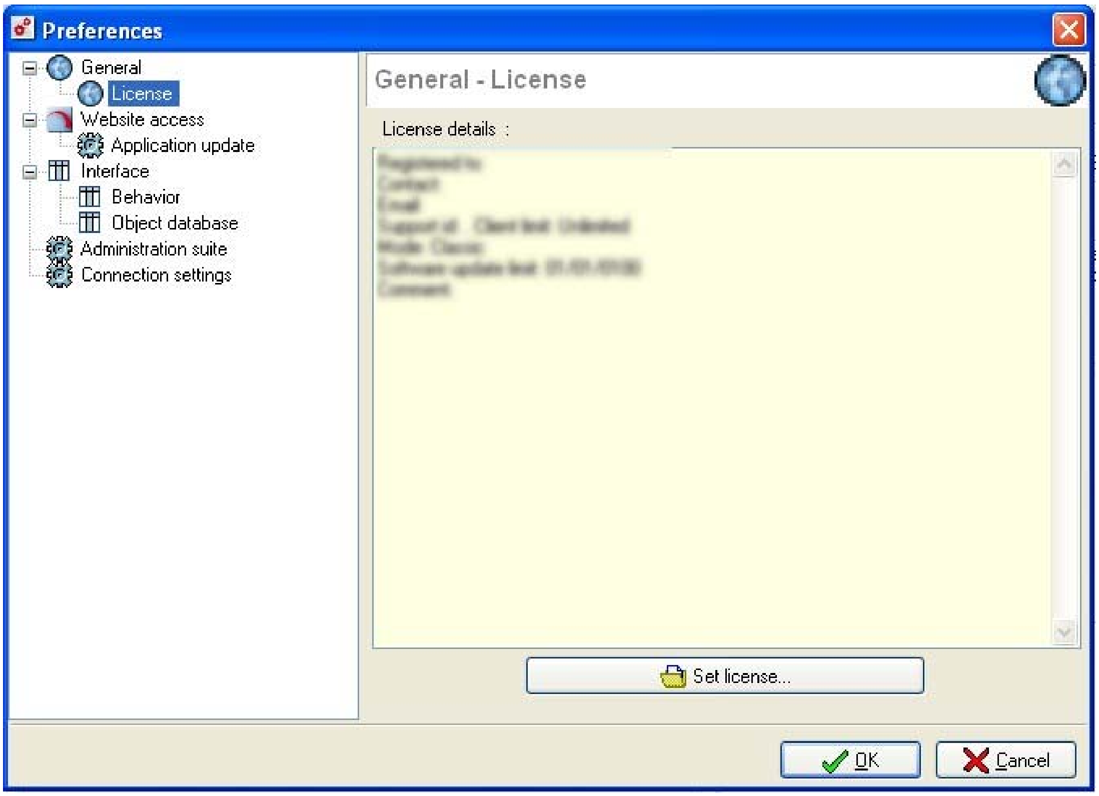
Application mode

default mode : Firewall Manager mode

Figure 433: Preferences - General

Default mode	This option allows you to select the mode in which NETASQ UNIFIED MANAGER will run. The two possible options are "Global Administration Mode" and "Firewall Manager Mode". The first mode enables configuring a fleet of firewalls whereas the second manages the configuration of a firewall.

License



[redacted]

Figure 434: Preferences - License

This view displays the details of licenses in each application.

Registered to:	Name of the company – end user
Contact:	Name of the contact person in the company
E-mail address:	E-mail address of the contact person
Support id:	Company's support number
Mode	
Software update limit	Indicates the expiry date for updates.
Client limit:	Maximum number of clients (NETASQ appliances) that NETASQ Global Administration can manage
Comments	Indicates the type of license…

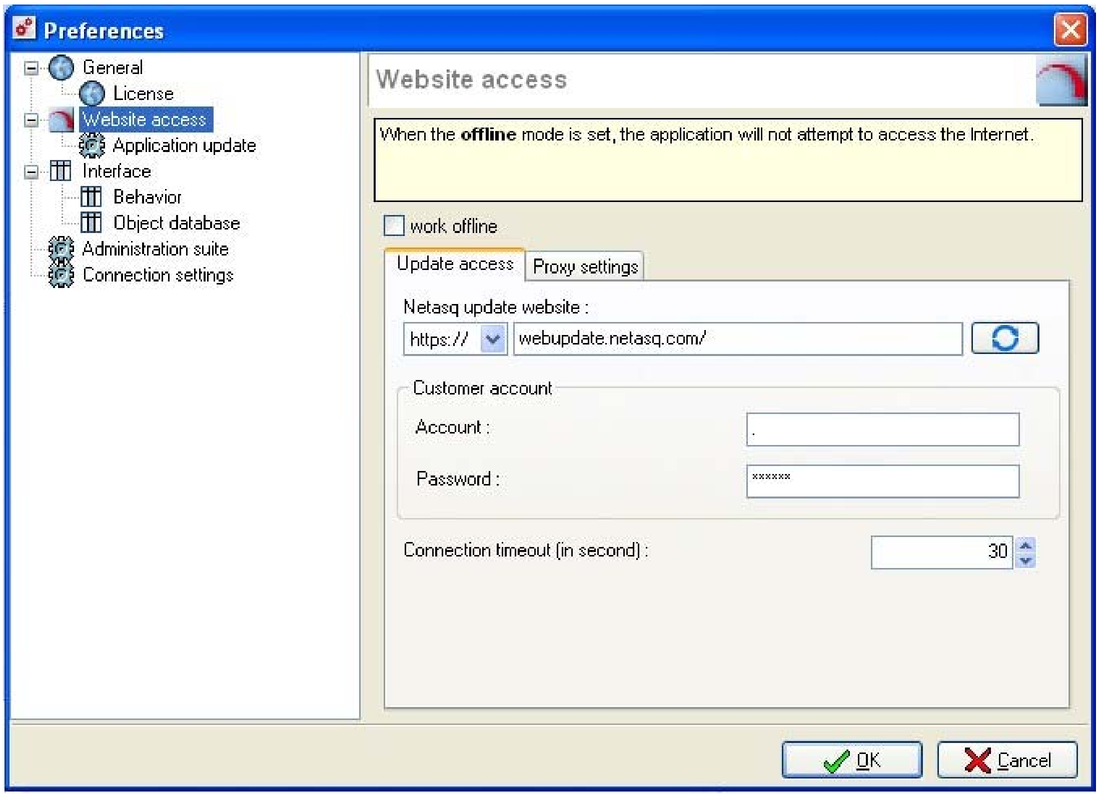
The button **Set license** allows you to retrieve a more recent license that was downloaded earlier on your workstation.

19.1.2.2. Website access

The NETASQ Firewall is a security product that often evolves to protect the network from increasingly sophisticated threats. Regular updates are essential for taking into account the new developments, and software programs in the administration suite have to be updated in order to manage new features.

Accessing for updates

The following options need to be specified in order to look for updates on NETASQ's website:



Website access

When the **offline** mode is set, the application will not attempt to access the Internet.

□ work offline

Netasq update website : https:// webupdate.netasq.com/

Customer account

Account : .

Password : ******

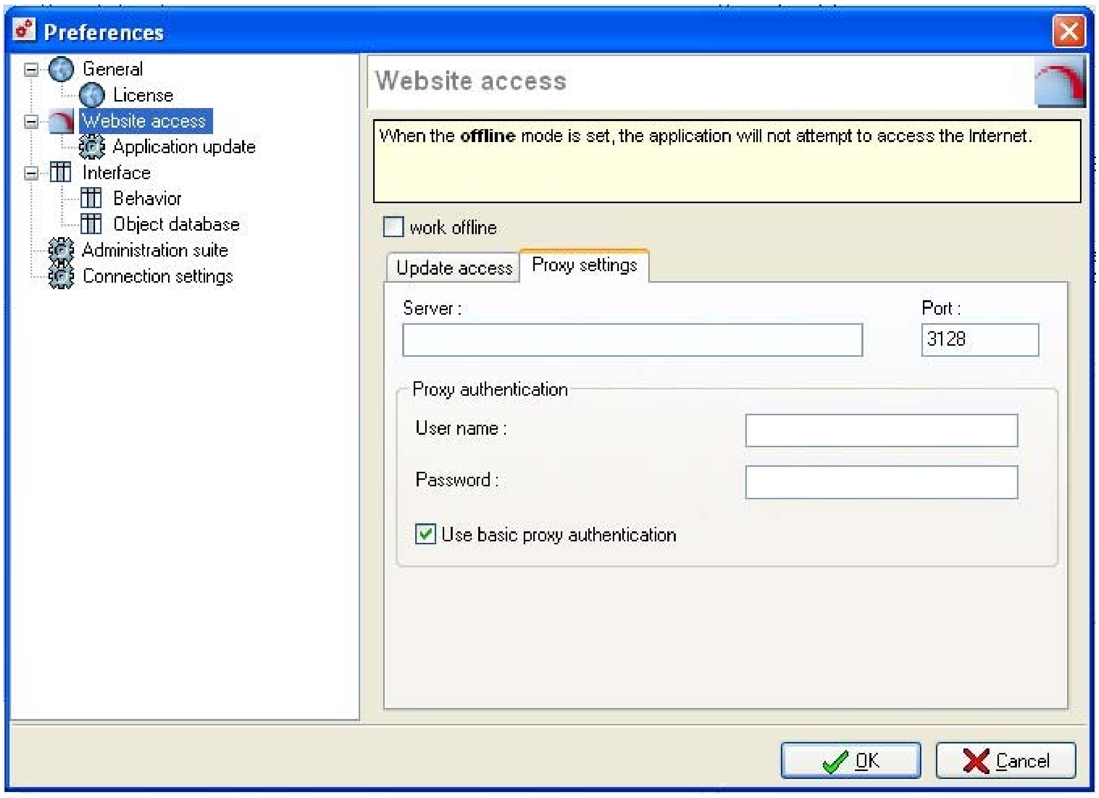
Connection timeout (in second) : 30

Figure 435: Preferences – Website access

Work offline	If this option is selected, the application will not try to access the internet.
NETASQ update website	URL in HTTP or HTTPS that will enable contacting the section of the website that allows checking for updates. The button ↻ brings the user back to the URL address of the site that is specified by default
Customer account	Login for accessing NETASQ's website so that NETASQ Global Administration can retrieve product updates. This is an account that enables access to the client or partner area.
Password	Password associated with the support account mentioned above. By default, this password is the activation code indicated on the label found on the underside of the NETASQ product.
Connection timeout (seconds)	NETASQ Global Administration will attempt to connect to NETASQ's website for the duration indicated. In case of a connection failure, information relating to the website will not be updated.

Proxy configuration

➲ The **`Proxy settings`** tab enables configuring the proxy for internet access.



When the **offline** mode is set, the application will not attempt to access the Internet.

□ work offline

Server :

Port : 3128

Proxy authentication

User name :

Password :

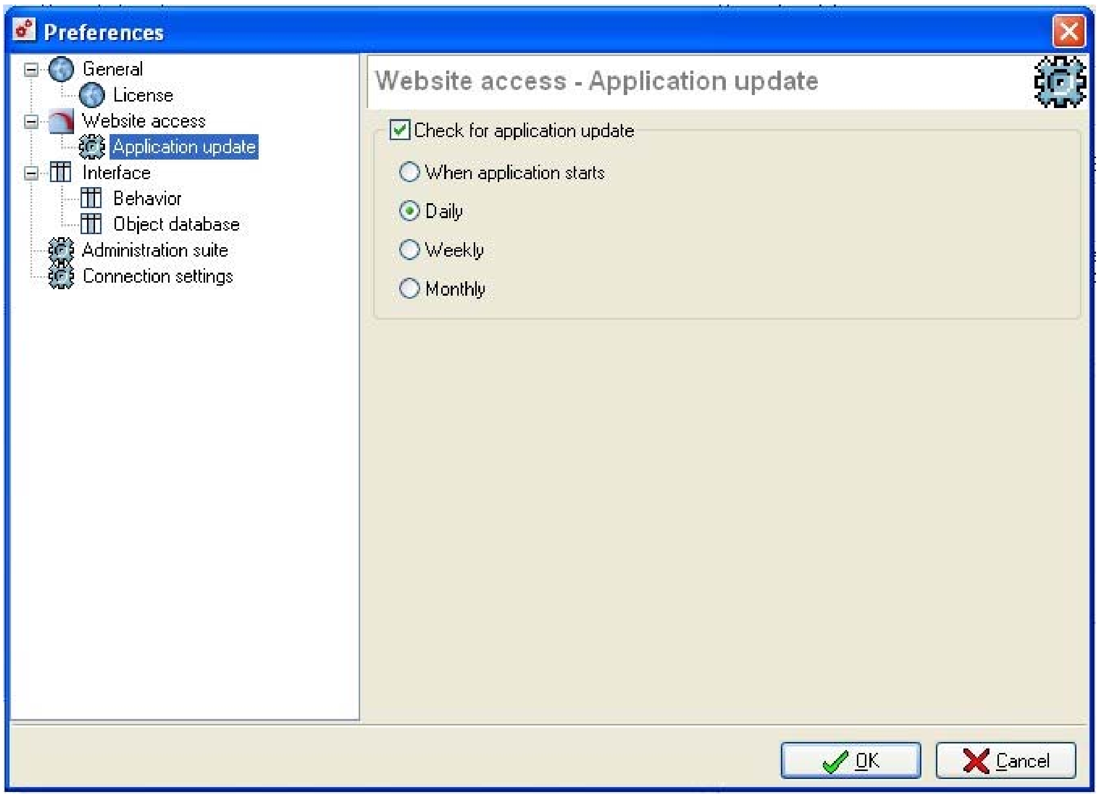
☑ Use basic proxy authentication

Figure 436: Preferences – Proxy settings

If there is a proxy for internet access on the network, it has to be indicated in proxy configuration, otherwise NETASQ UNIFIED MANAGER will not be able to verify the presence of an update on NETASQ's website. The various options are as follows:

Server	Proxy's IP address or hostname through which the administration workstation has to connect in order to access the internet.
Port	Port to use for contacting the proxy, by default it is 3128.
Username	Administration workstation's login if authentication is needed in order to access the proxy.
Password	Password for connecting to the proxy associated with the login.
Use basic proxy authentication	Defines whether authentication has been activated. If the option is not selected, there will be no authentication even if the proxy requires it.

Updating the application



Preferences

- General
  - License
- Website access
  - Application update
- Interface
  - Behavior
  - Object database
- Administration suite
- Connection settings

Website access - Application update

☑ Check for application update

○ When application starts

● Daily

○ Weekly

○ Monthly

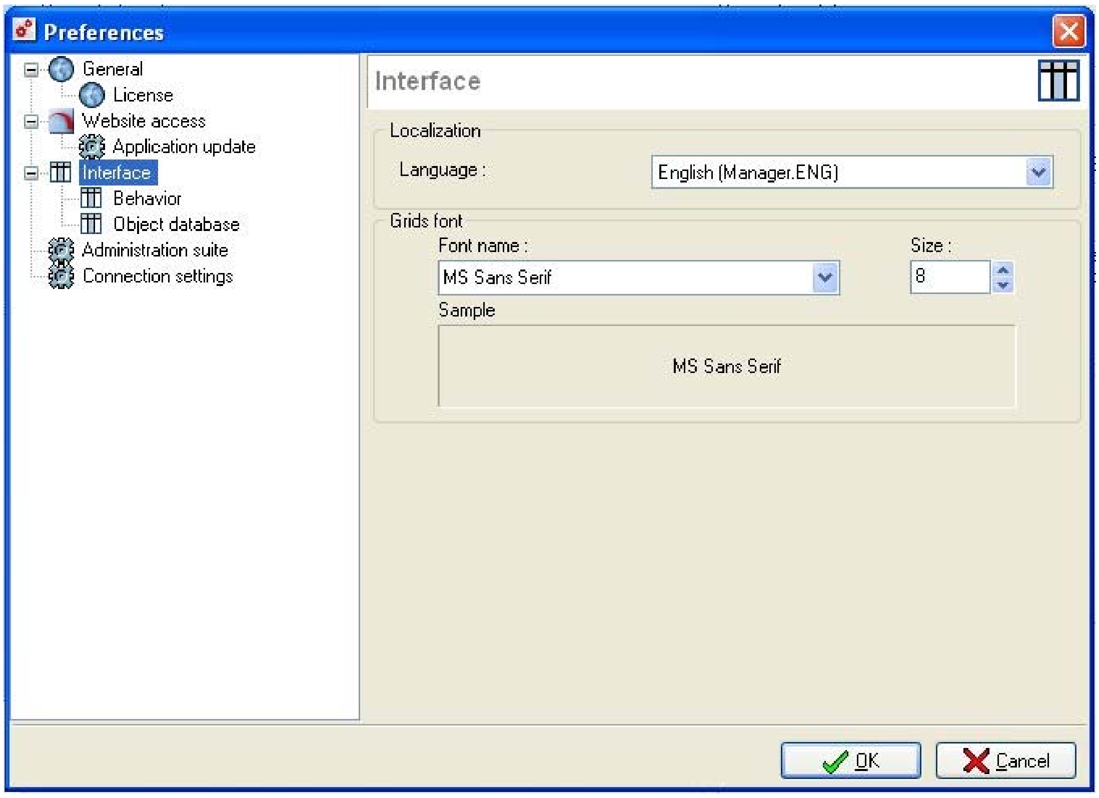
Figure 437: Preferences – Application update

How often you update your Firewall is important because when NETASQ publishes a new critical update, it is best if this update is detected early. By default the frequency of the check for updates is **Daily**, but it can be changed to **At startup**, **Weekly** and **Monthly**.

By default, Active Update checks for updates for the administration suite according to the selected frequency. However, if the option **Check for application updates** is selected, the Firewall will automatically check for updates.

Once the reference period expires, NETASQ UNIFIED MANAGER will check for updates when it starts up. If a firmware or administration suite update is found on NETASQ's website, it will be indicated on the main screen in NETASQ UNIFIED MANAGER.

19.1.2.3. Interface



Localization

Language : English (Manager.ENG)

Grids font

Font name : MS Sans Serif

Size : 8

Sample

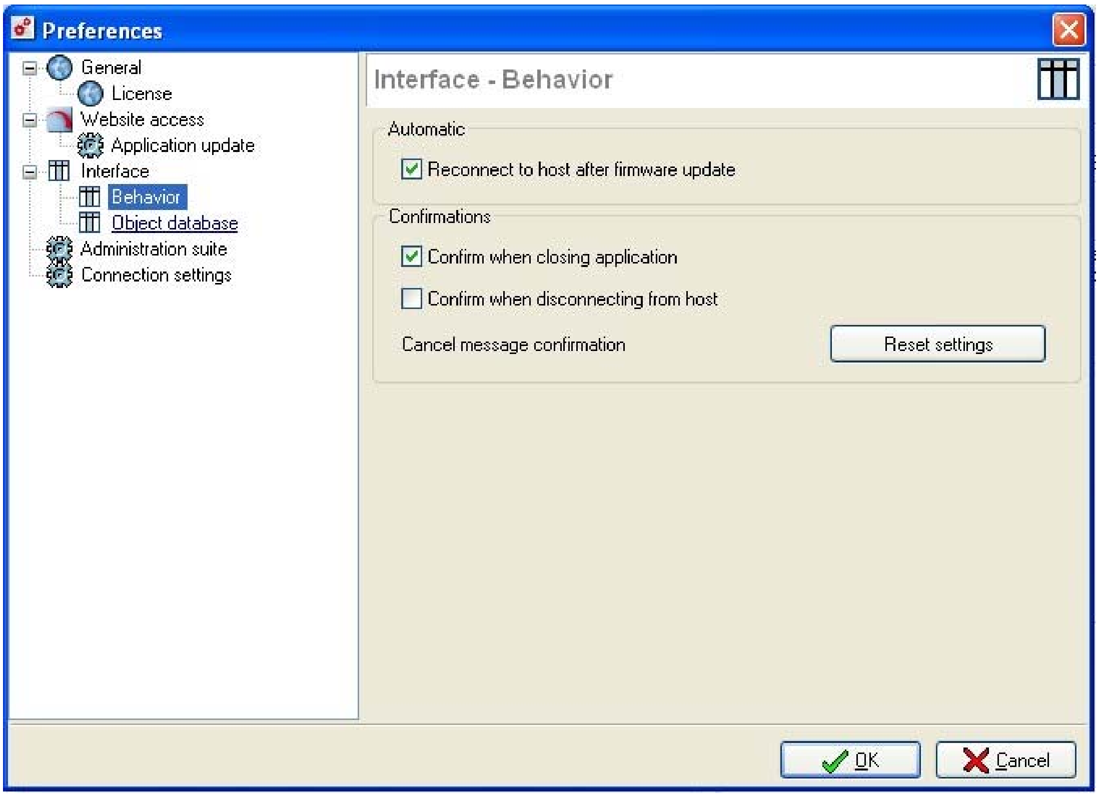
MS Sans Serif

Figure 438: Preferences - Interface

The options for the interface are as follows:

Language	This option allows you to select the language for the interface menus. **WARNING** If the language has been selected, you will need to reboot to apply the changes. **<Automatic selection>** will use the language of the Windows operating system.
Font	Font and font size for information displayed in NETASQ UNIFIED MANAGER's configuration tables (e.g. filter rules).

Behavior



Automatic

☑ Reconnect to host after firmware update

Confirmations

☑ Confirm when closing application

□ Confirm when disconnecting from host

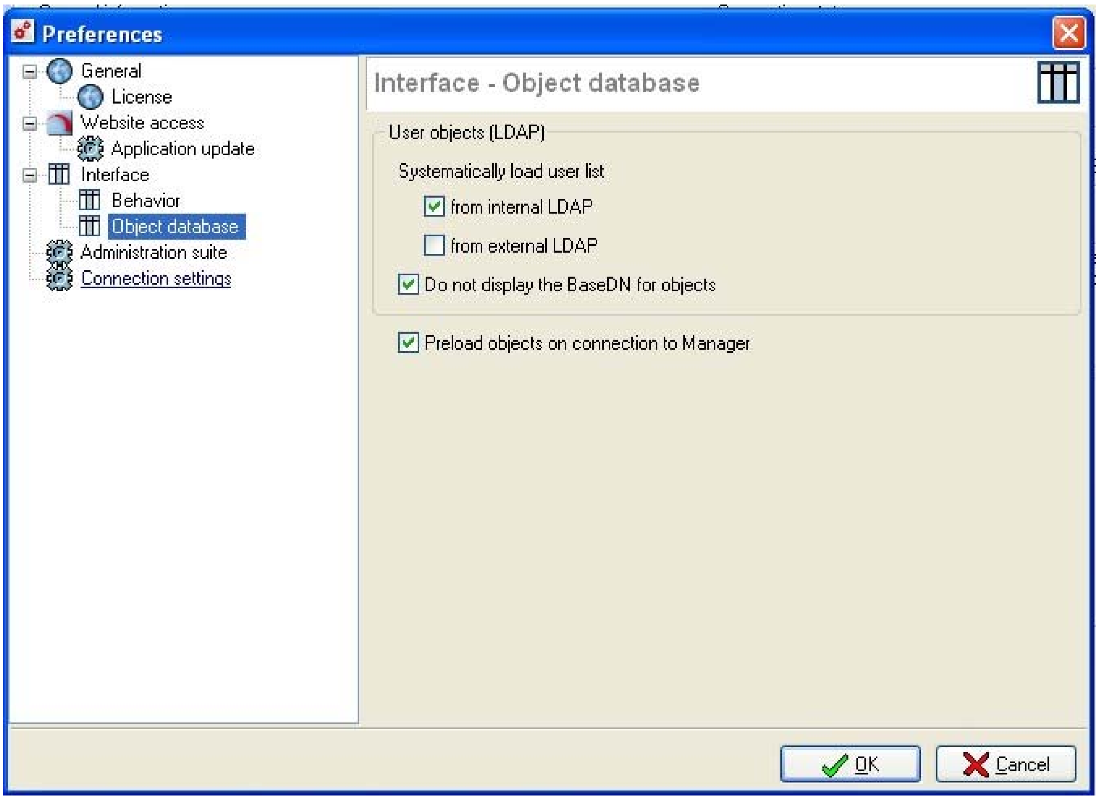
Cancel message confirmation [Reset settings]

Figure 439: Preferences – Behavior

Confirmation options determine how the NETASQ UNIFIED MANAGER shuts down. There are two confirmation options:

Reconnect to host after firmware update	When rebooting a UTM appliance, NETASQ UNIFIED MANAGER can be configured to reconnect automatically to the appliance without having to monitor its actual reboot. (Cf. Part 18/CHAPTER 1: Rebooting the firewall).
Confirm when closing application	A confirmation message aill appear before the NETASQ UNIFIED MANAGER application is shut down.
Confirm when disconnecting from host	A confirmation message appears before NETASQ UNIFIED MANAGER is disconnected from the Firewall
Cancel message confirmation	Certain configuration menus require confirmation to abandon changes before quitting a menu. These messages can be masked. The button **Reset setting** allows resetting masked confirmation messages.

Object database



Interface - Object database

User objects (LDAP)

Systematically load user list

☑ from internal LDAP

□ from external LDAP

☑ Do not display the BaseDN for objects

☑ Preload objects on connection to Manager

Figure 440: Preferences - Object database

Object options are set out in the following table:

Systematically load user list	By default, when the LDAP database is fully loaded in object configuration, NETASQ UNIFIED MANAGER will display a warning message as in certain cases, the LDAP database may turn out to be voluminous and loading will take a long time. De-select this option to avoid having to see this message in the future. If the option **From internal LDAP** is selected, this warning message will be hidden if an internal LDAP database is used. If the option **From external LDAP** is selected, this warning message will be hidden if an external LDAP database is used.
Do not display the BaseDN for objects	Users that are stored in user databases used by (internal or external) NETASQ UTM appliances are identified by their names (called CN or Common Name) and the organization to which they belong (called BaseDN). This BaseDN is the same for all users in the database and contains the fields O (name of the organization) and DC (Country), which were entered during the construction of LDAP databases. If the option **Do not display object BaseDN** is selected, user and user group objects will be displayed more simply, without the **Organization** section.
Preload objects on connection to Manager	This option enables anticipated loading of certain necessary information to perform basic tasks.

19.1.2.4. Administration Suite

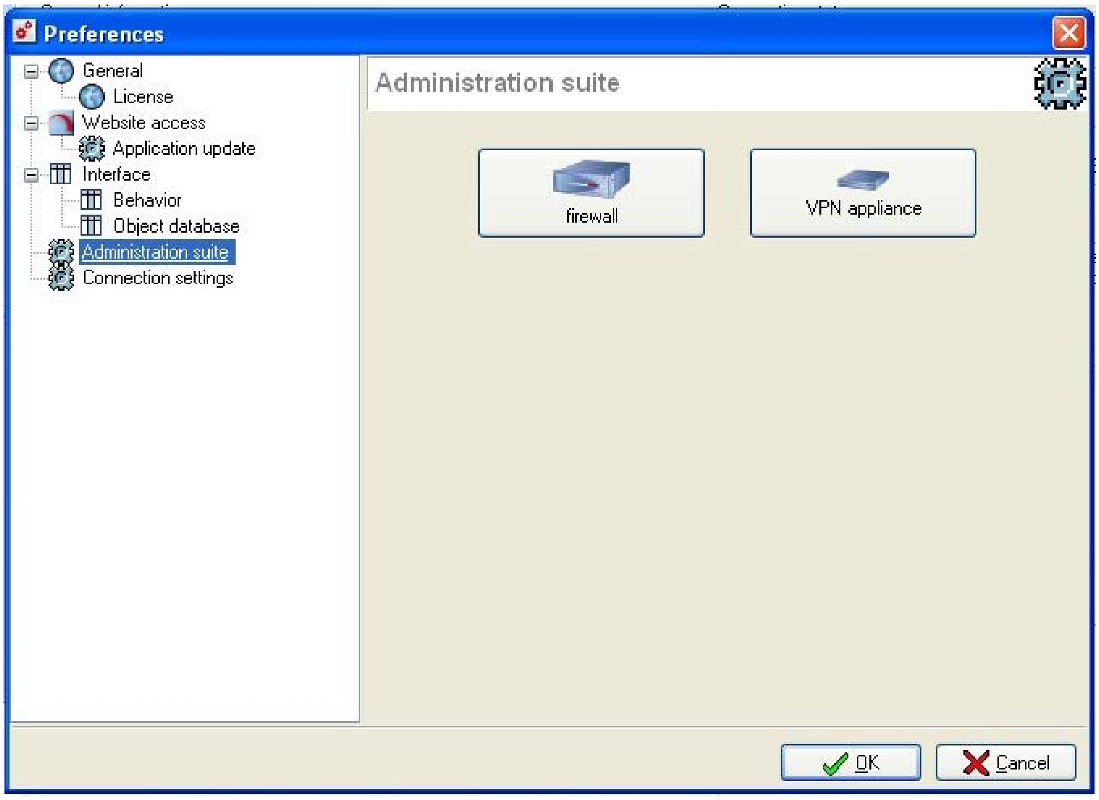


Figure 441: Preferences – Administration Suite

This menu allows defining the access paths to the different NETASQ applications that NETASQ Global Administration uses.

For each appliance type (Firewall, VPN appliance), click on the corresponding button.

Firewall	For firewalls.
VPN appliance	For VBOXes.

In the window that appears, select for each application the path that corresponds to each software version (if your appliance fleet contains products in different software versions, the software to use in each version can be specified here). As such, NETASQ Global Administration will automatically launch the right software program according to the type of appliance and the software version.

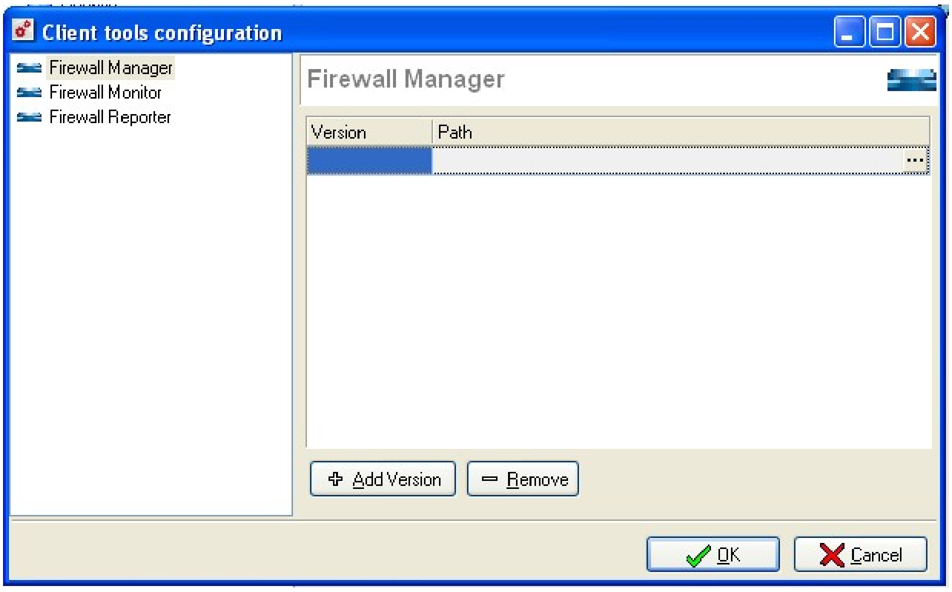


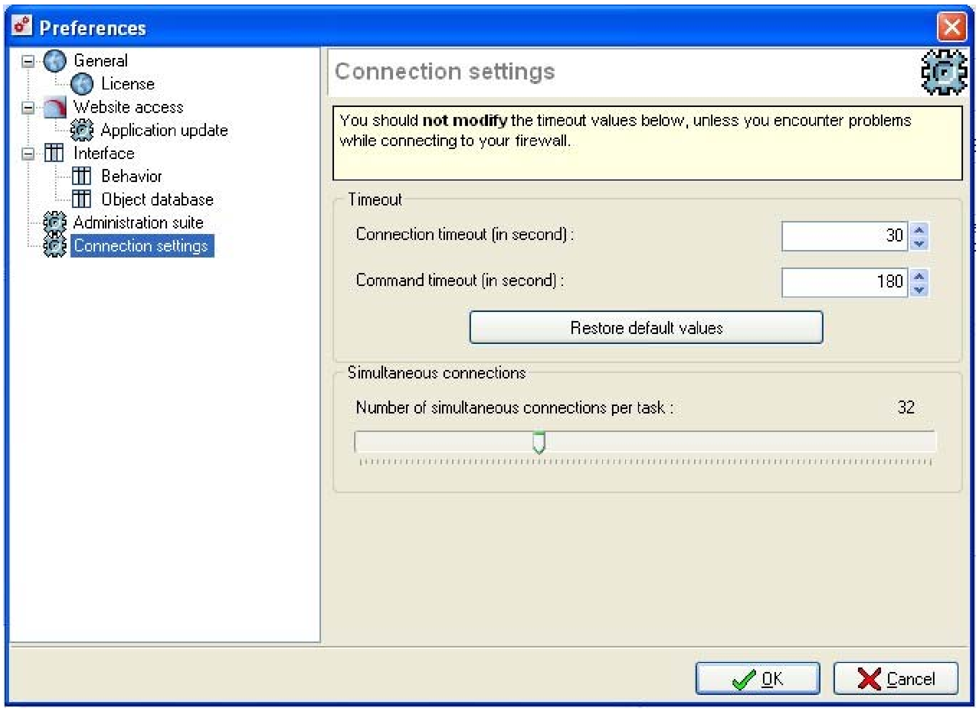
Figure 442: Configuring client tools - Firewall Manager

To add a version and the corresponding path, click on **Add**. Indicate the version number in the "Version" column and select the associated software by clicking on … in the "Path" column.

To delete a version, select is and click on **Remove**.

Click on **OK** once the applications have been configured.

19.1.2.5. Configuring a connection



You should **not modify** the timeout values below, unless you encounter problems while connecting to your firewall.

Connection timeout (in second) : 30

Command timeout (in second) : 180

Number of simultaneous connections per task : 32

Figure 443: Preferences – Connection settings

Connection timeout	Indicates the duration of the connection. In the event of a failure, the connection

(seconds)	will not be made.
Connection timeout (seconds)	Indicates the maximum duration after an attempt to exchange with the firewall.
Restore default values	The default durations will be retored when you click on this button. Modifications you made will be deleted.
Number of simlultaneous connections per task	Indicates the number of simultaneous connections per task. Move the cursor to increase of decrease this number.

19.1.3. Applications

19.1.3.1. Lauching Monitor and Reporter

The **`Applications`** menu in the main interface of NETASQ UNIFIED MANAGER is broken down into two sub-menus:

- Launch NETASQ REAL-TIME MONITOR
- Launch NETASQ EVENT REPORTER

Lancer NETASQ REAL-TIME MONITOR...
Lancer NETASQ EVENT REPORTER...

Figure 444: Monitor and Reporter

These two sub-menus allow you to open the NETASQ REAL-TIME MONITOR and NETASQ EVENT REPORTER software through NETASQ UNIFIED MANAGER. Using both shortcuts provides the advantage of not having to re-authenticate on both applications. If you have been authenticated on NETASQ UNIFIED MANAGER, you will also be authenticated on the other two applications.

19.1.4. License

Every Firewall has a license which sets out all the options available on your Firewall. This key allows you to activate some of the firewall options (URL filtering, strong VPN encryption, updates etc.) You can obtain it from the NETASQ website (www.netasq.com).

19.1.4.1. Initial connexction

When you first connect to the firewall, it will not have a license. Without this license, the firewall cannot be used. The license configuration screen appears when you attempt to connect.

WARNING

Upon receipt of your Firewall, if no message relating to the license appears, this means that the NETASQ Firewall has installed a temporary license in your product. This license corresponds to the minimal NETASQ product license (no options are activated). If an incident arises while the temporary license is still installed on your product, you will not be covered by the guarantee. Therefore, even if your Firewall functions temporarily, you are advised to download your permanent license as soon as possible before the expiry of this temporary license.

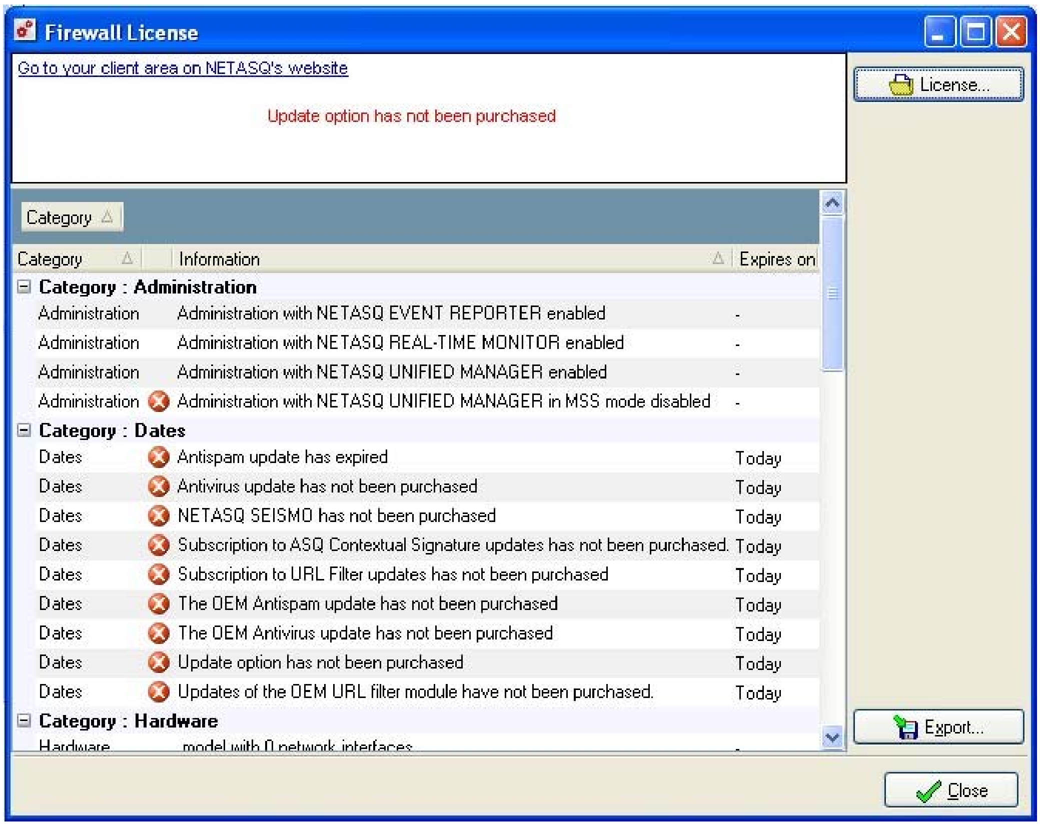
The **License** button allows you to insert the license (which you have retrieved beforehand from NETASQ's website) and to activate your Firewall's configuration.

19.1.4.2. Your firewall's license and its update

NETASQ UNIFIED MANAGER is sold with a license for 5 UTM appliances, which allows the administrator to import address books of any size.

➲ This information is accessible via the menu `Firewall\Licenses` in the main interface of NETASQ UNIFIED MANAGER.

The license configuration screen shows you the version of your Firewall, hardware information and information on the different options with their expiry dates, if applicable.



Go to your client area on NETASQ's website

Update option has not been purchased

Category	Information	Expires on
Category : Administration		
Administration	Administration with NETASQ EVENT REPORTER enabled	-
Administration	Administration with NETASQ REAL-TIME MONITOR enabled	-
Administration	Administration with NETASQ UNIFIED MANAGER enabled	-
Administration	⊗ Administration with NETASQ UNIFIED MANAGER in MSS mode disabled	-
Category : Dates		
Dates	⊗ Antispam update has expired	Today
Dates	⊗ Antivirus update has not been purchased	Today
Dates	⊗ NETASQ SEISMO has not been purchased	Today
Dates	⊗ Subscription to ASQ Contextual Signature updates has not been purchased.	Today
Dates	⊗ Subscription to URL Filter updates has not been purchased	Today
Dates	⊗ The OEM Antispam update has not been purchased	Today
Dates	⊗ The OEM Antivirus update has not been purchased	Today
Dates	⊗ Update option has not been purchased	Today
Dates	⊗ Updates of the OEM URL filter module have not been purchased.	Today
Category : Hardware		
Hardware	model with 0 network interfaces	-

Figure 445: Firewall license

The NETASQ Firewall is delivered with all its features by default. However, certain features (e.g. URL filtering, high availability) are optional and are not activated. On the other hand, other features, such as updates, are time-limited. If the expiry date has lapsed, certain options will be deactivated on the Firewall.

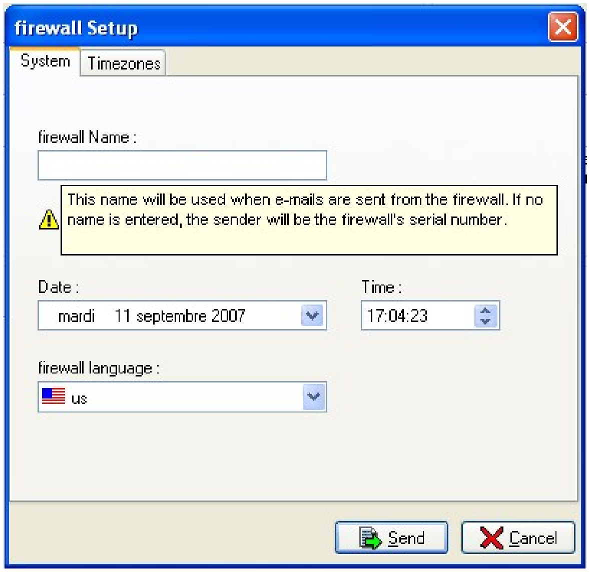
If you opt to use new features or to renew certain options, please contact your dealer. A new key will then be available on NETASQ's website. Enter this key using the "Update license" button at the bottom left, then validate by sending to the Firewall. Information concerning your Firewall will be modified and the new options will be activated on the Firewall.

19.1.5. Configuring system parameters

➲ If you wish to change the NETASQ Firewall's parameters go to the sub-menu **`Firewall\System setup`**. The system configuration screen comprises two tabs:

- The **`System`** tab.
- The **`Timezones`** tab.

19.1.5.1. System tab



firewall Name :

This name will be used when e-mails are sent from the firewall. If no name is entered, the sender will be the firewall's serial number.

Date : mardi 11 septembre 2007

Time : 17:04:23

firewall language : us

Figure 446: Configuring the firewall – System

The System tab allows you to modify the following parameters:

- Firewall name (this name is used in alarm messages sent to the administrator and is displayed on the Firewall's main window). Any name will do,
- Date. Select the date from the calendar,
- Time.
- Firewall language (type of keyboard that the firewall supports).

The date and time to which your NETASQ Firewall is set are important – they allow you to locate an event recorded in the log file. They are also useful in the scheduling of configurations.

Each time this dialog box is opened, the remote configuration software indicates the date and time currently configured on the NETASQ Firewall.

19.1.5.2. Time zone tab

WARNING
Changing time zones will cause the Firewall to reboot.

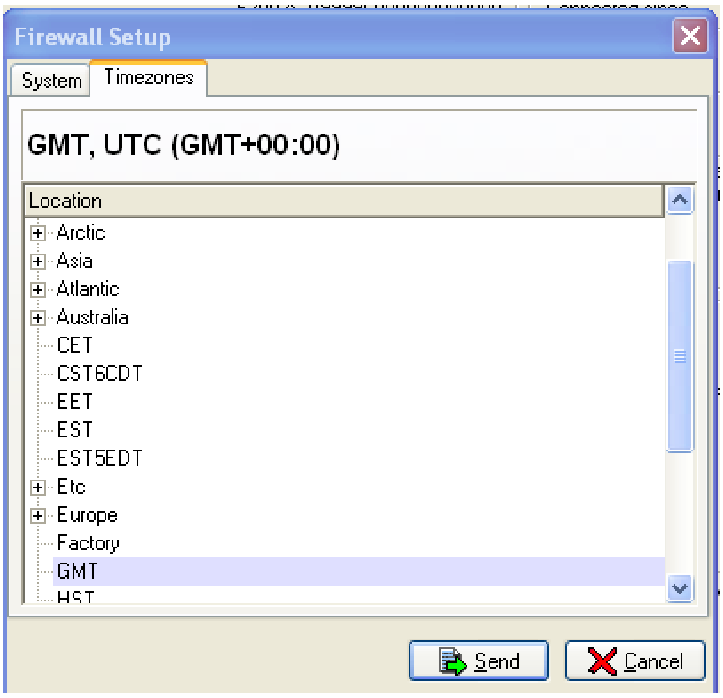


Figure 447: Timezone

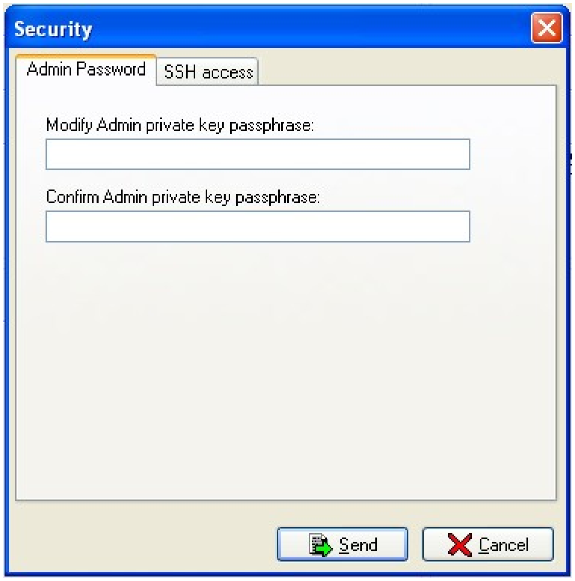
19.1.6. Security

➲ If you wish to change the NETASQ Firewall’s security parameters go to the menu `Firewall\Security`.

This menu has two tabs:

- **`Admin password`**: Allows modifying the password for the super-administrator account, ie, the “admin” account.
- **`SSH access`**: Configures access to the NETASQ appliance via an SSH client in console mode.

Admin password



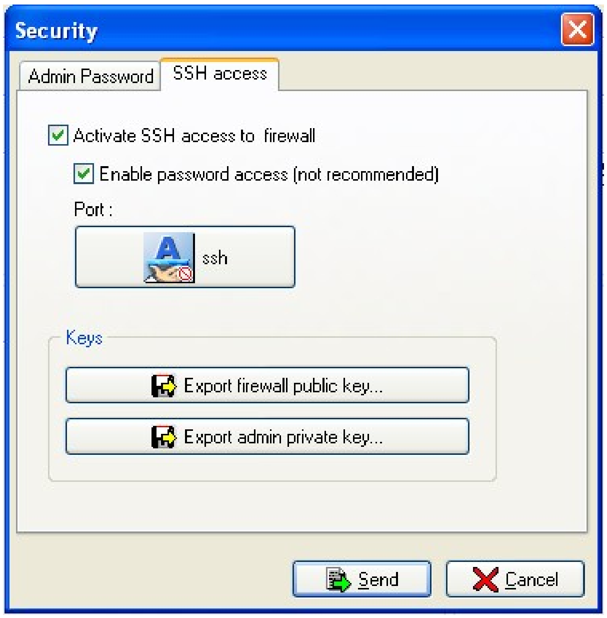
Modify Admin private key passphrase:

Confirm Admin private key passphrase:

Figure 448: Security - Admin Password

The fields “Modify Admin account password” and “Confirm Admin account password” allow you to modify the password used to connect to the Firewall in SSH. This password corresponds to the “admin” account password. If you change the password, you should also use this new password to connect via the graphical interface under the “admin” account.

SSH Access



☑ Activate SSH access to firewall

☑ Enable password access (not recommended)

Port : ssh

Figure 449: Security – SSH access

An SSH server (version 2) is installed on the Firewall. This enables you to access the Firewall in console mode via an SSH client in complete safety. The server’s configuration can be carried out from this option. Communications between a client and an SSH server are encrypted and authenticated for maximum security during configuration. Check the "Activate SSH access to Firewall" box to activate the server. If this box is not checked you will be unable to make a remote connection in console mode

You can use the appropriate buttons to export the Firewall's public key and the administrator's private key to the machine on which the client SSH is installed. The administrator's private key format is from OpenSSH, it is not compliant with SSH.COM.

> ❗ **WARNING**
> SSH operates with certificates. However, you can always activate the option "Enable password access" to have a login/password access, but this option is not recommended.

The Firewall's filtering blocks connections on port 22 (SSH) of the Firewall by default. It is therefore necessary to set up a filter rule in order to allow this communication.

19.1.7. Secure configuration

19.1.7.1. Introduction

Highly sensitive information is contained in the configuration of a firewall, information that exposes network activity and ways to bypass this network's protection mechanisms. Such data can be protected by using the encryption features found in the configuration files of the Firewall.

As these encrypted configuration files can only be decrypted with a secret key shared by the Firewall and the administrator, it is the administrator's duty to prevent its theft and the illicit use of his Firewall. Without decrypting these files, the Firewall cannot be used.

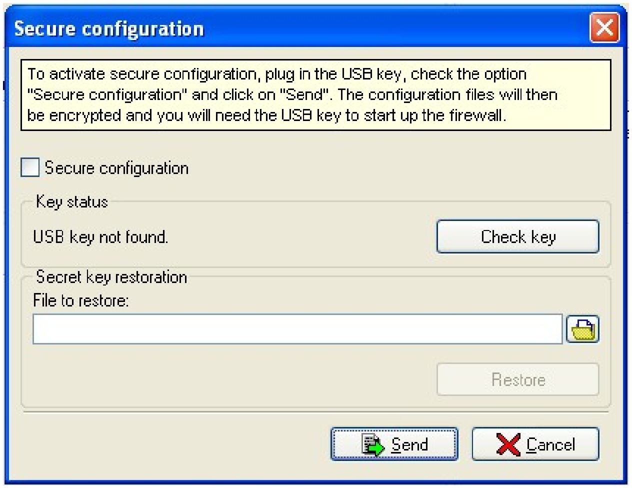
19.1.7.2. Operation

To implement this technology, NETASQ offers the possibility of using USB keys that contain exchanged secret keys. Without this key, the Firewall cannot be started. Once the configuration has been loaded into memory, the USB key can be removed in order to keep configuration files confidential, but will be necessary for the next connection.

> ❗ **WARNING**
> USB keys are compatible with this feature, and only USB keys manufactured and distributed by NETASQ are supported for this feature.
> This feature is only available for products that have an operational USB port.

19.1.7.3. Secure configuration

➲ Secure configuration features can be enabled via the menu **`Firewall\Secure configuration`** in the menu bar in NETASQ UNIFIED MANAGER graphical interface.



To activate secure configuration, plug in the USB key, check the option "Secure configuration" and click on "Send". The configuration files will then be encrypted and you will need the USB key to start up the firewall.

Figure 450: Secure configuration

The options for secure configuration are as follows:

Secure configuration	Button that activates secure configuration. Once it is activated, the Firewall's configuration files will be encrypted, therefore the USB key is essential for decrypting its configuration.
Key status	Value displayed by the Firewall indicating the current status of the key that will be used for storing the decryption secret. There are three different statuses: ● **USB key not found**: the key has not been inserted in the firewall's USB port or has not been formatted according to its file format ● **USB key not initialized**: the key has been detected but does not contain the decryption secret for the Firewall configuration, ● **USB key initialized:** the key has been detected and contains a decryption secret for the Firewall configuration.
Check key	Before displaying the **`Secure Configuration`** menu, NETASQ UNIFIED MANAGER checks the key's status. The **Check key** button refreshes the data on display. If a USB key is inserted after the **`Secure configuration`** menu appears, click on the **Check key** button to refresh data on the key's status.
File to restore	If the key or the secret contained in the key is defective, this backup can then be restored on the same key or on a new key.
Send	Activates secure configuration. Before closing the menu, a path must be specified for backing up the encryption key that was inserted in the USB key.
Cancel	Cancels modified parameters in secure configuration.

Encrypted configuration files

To make it easier to configure, activate and use this feature, the firewall does not offer the choice of encrypting configuration files. By default the files encrypted by the secure configuration feature are:

- Pre-shared keys VPN configuation;
- LDAP directory configuration;
- Authentication configuration;

- Keytab file in SPNEGO configuration;
- The private key of the PKI's certification authority;
- PKI configuration;
- Certificates signed by the PKI's certification authority.

19.1.7.4. Using secure configuration

The configuration encryption feature can only be used with products that have a USB port, and the administrator must have a compatible USB key. Contact your NETASQ partner to obtain a USB key.

Once the secure configuration feature has been enabled, the USB key containing the secret is necessary for starting up the appliance. After the firewall has booted, the administrator can remove the key. The configuration of the appliance is secure.

The procedure for activating secure configuration is as follows:

1. Select the configuration menu **`Firewall\Secure Configuration`**, which will open the secure configuration window.
2. Connect the USB key.
3. Click on **Test key**, which should display the key status as "USB key not initialized".
4. Check the option **Secure configuration**
5. Click on **Send** to activate secure configuration.
6. The key is now initialized, Firewall configuration files are encrypted and you will be asked to specify a path for copying the backup file.

Restoring defective key or creating a backup key

When initializing the USB key containing the secret shared with the firewall, the firewall will back up this secret. It will then be possible to perform backup operations on USB keys.

The procedure for restoring a USB key is as follows:

1. Select the configuration menu **`Firewall\Secure Configuration`**, which will open the secure configuration window.
2. Connect the USB key.
3. The key status should either be "USB key not initialized" or "USB key initialized".
4. The option "Secure configuration" should already have been selected.
5. Select the backup file to restore by clicking on the icon 📂.
6. Click on **Restore** to restore the USB key.
7. Click on **Send** to end the restoration operation.

The procedure for creating a backup USB key is as follows:

1. Select the configuration menu **`Firewall\Secure Configuration`**, which will open the secure configuration window.
2. Connect the new USB key.
3. Click on **Test key**, which should display the key status as "USB key not initialized".

4 The option **Secure configuration** should already have been selected.
5 Select the backup file to restore by clicking on the icon 📂.
6 Click on **Restore** to restore the USB key.
7 Click on **Send** to finish creating the backup USB key.

19.1.8. Importing an address book

➲ Address books can be imported (in .gap format) via the menu File\Import and address book.

For more information regarding address books, go to the section *Part 3/Chapter 2: Address book.*

PART 20: GLOBAL ADMINISTRATION MODE

CHAPTER 1: PRESENTATION

20.1.1. 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.

20.1.2. Access

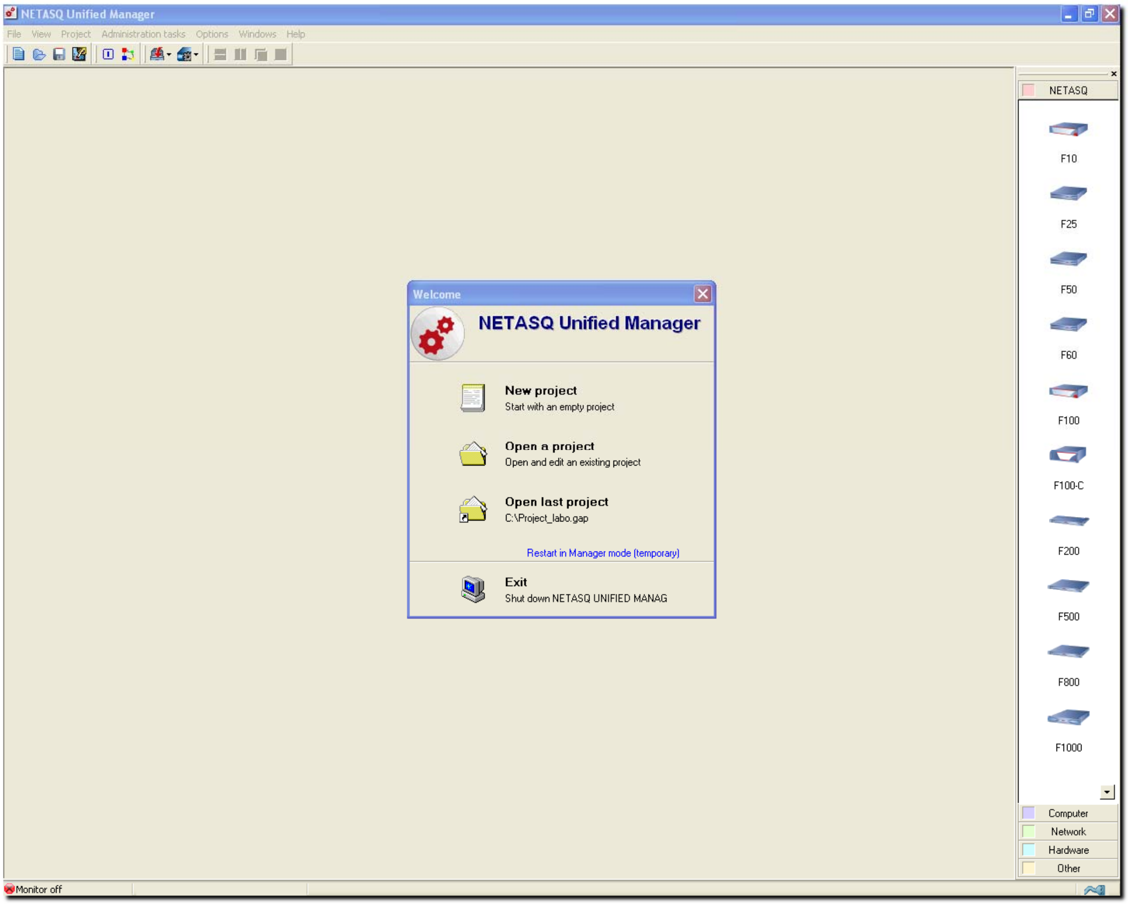
➲ To use NETASQ Global Administration, start the application using the Windows **`Start`** menu, from the following path: **`Start\Programs\Netasq\Administration Suite 7.0\NETASQ UNIFIED MANAGER.`**

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

20.1.3. Creating/opening a projet

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



Welcome

NETASQ Unified Manager

New project
Start with an empty project

Open a project
Open and edit an existing project

Open last project
C:\Project_labo.gap

Restart in Manager mode (temporary)

Exit
Shut down NETASQ UNIFIED MANAG

Figure 451: 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**.

CHAPTER 2: USING THE GLOBAL ADMINISTRATION MODE

20.2.1. User interface

20.2.1.1. Main window

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

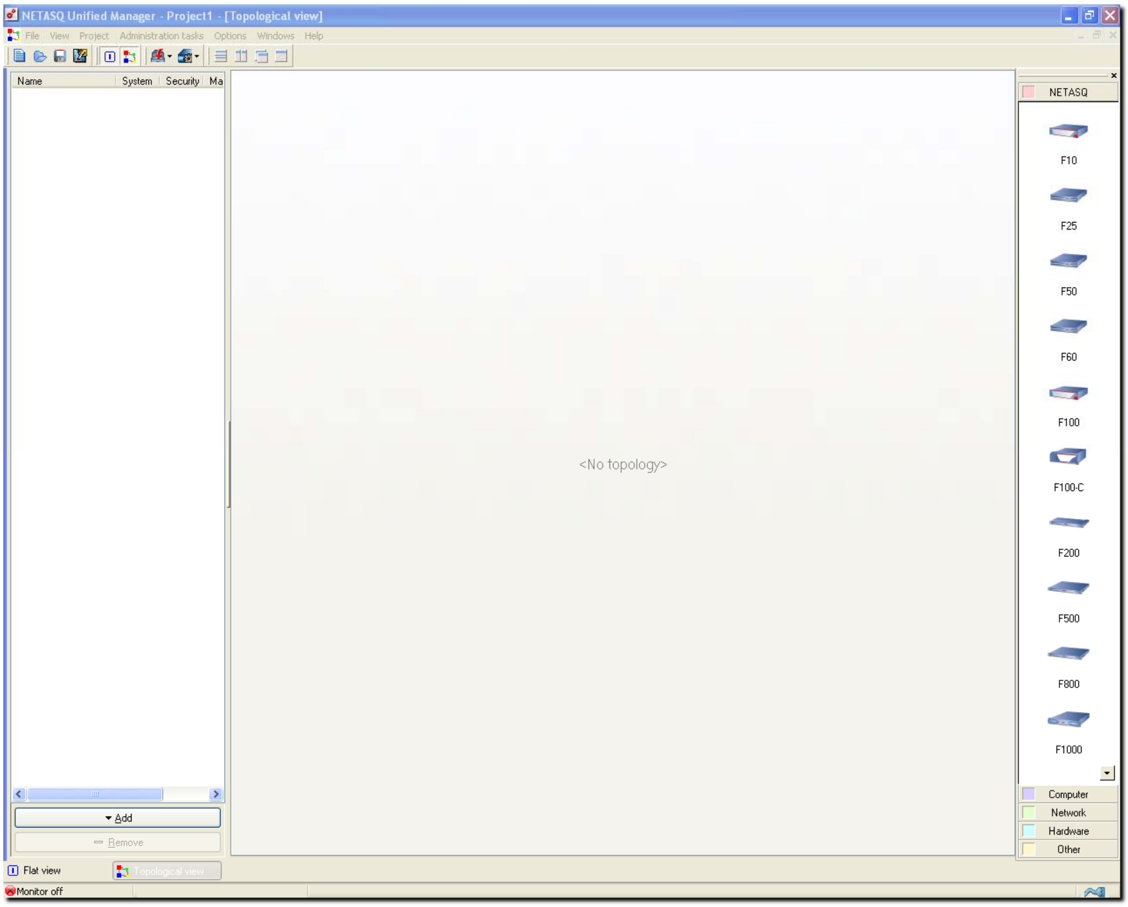


Figure 452: Main window

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.

20.2.1.2. Menu bar

This bar contains the following menus:

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

20.2.1.3. Icon and shortcut bar

The following bar contains the shortcuts for certain operations:

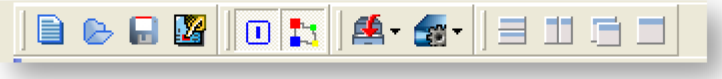


Figure 453: Icon and shortcut bar

📄	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`**).

20.2.1.4. Object bar

The object bar is organized as follows:

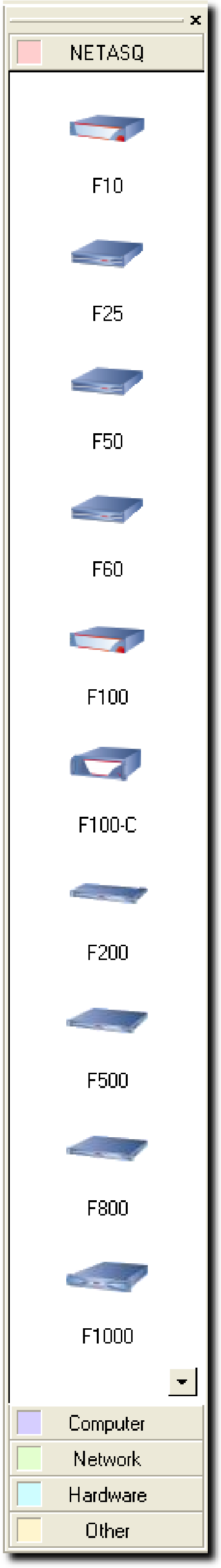


Figure 454: Object bar

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

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.

20.2.1.5. 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.

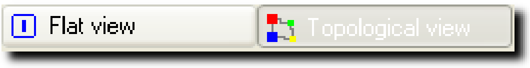


Figure 455: Switching views

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`**).

20.2.1.6. 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 456: Monitor and web mode

The monitor function is described in the section on *Part 20/Chapter 3: monitoring and supervision*. 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`**.

20.2.1.7. Topological view

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

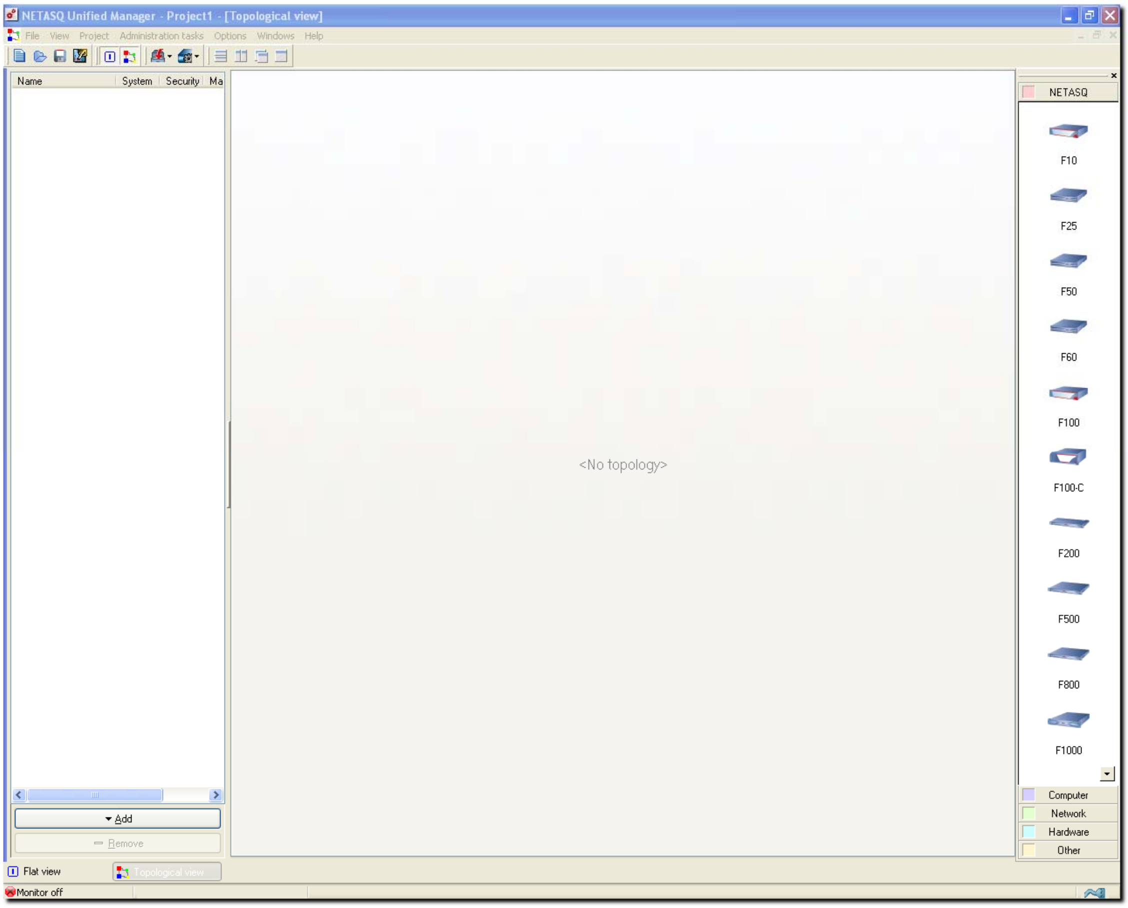


Figure 457: Topological view

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

20.2.2. Menus

20.2.2.1. 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

20.2.2.2. 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.

20.2.2.3. Project

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

20.2.2.4. 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.

20.2.2.5. Options

Preferences	For defining the NETASQ Global Administration options.

20.2.2.6. 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.

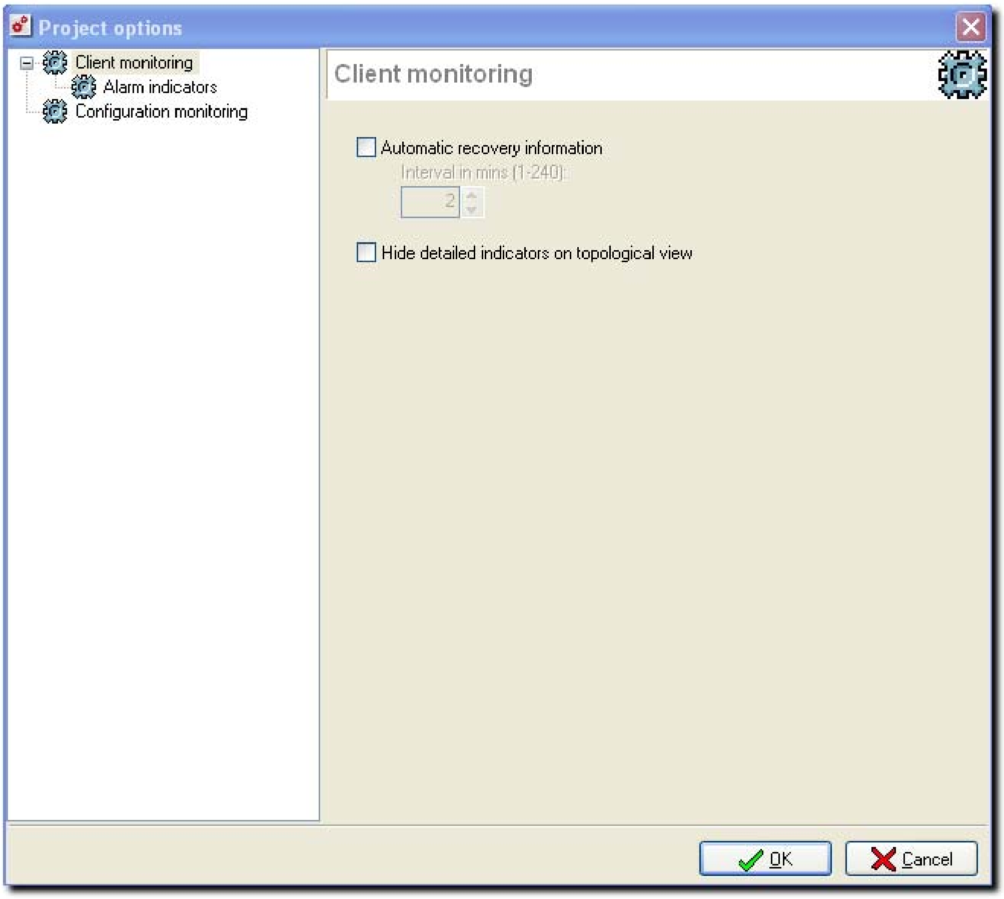
20.2.2.7. Help

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.

20.2.3. Project

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

20.2.3.1. Client monitoring



□ Automatic recovery information
Interval in mins (1-240):
2

□ Hide detailed indicators on topological view

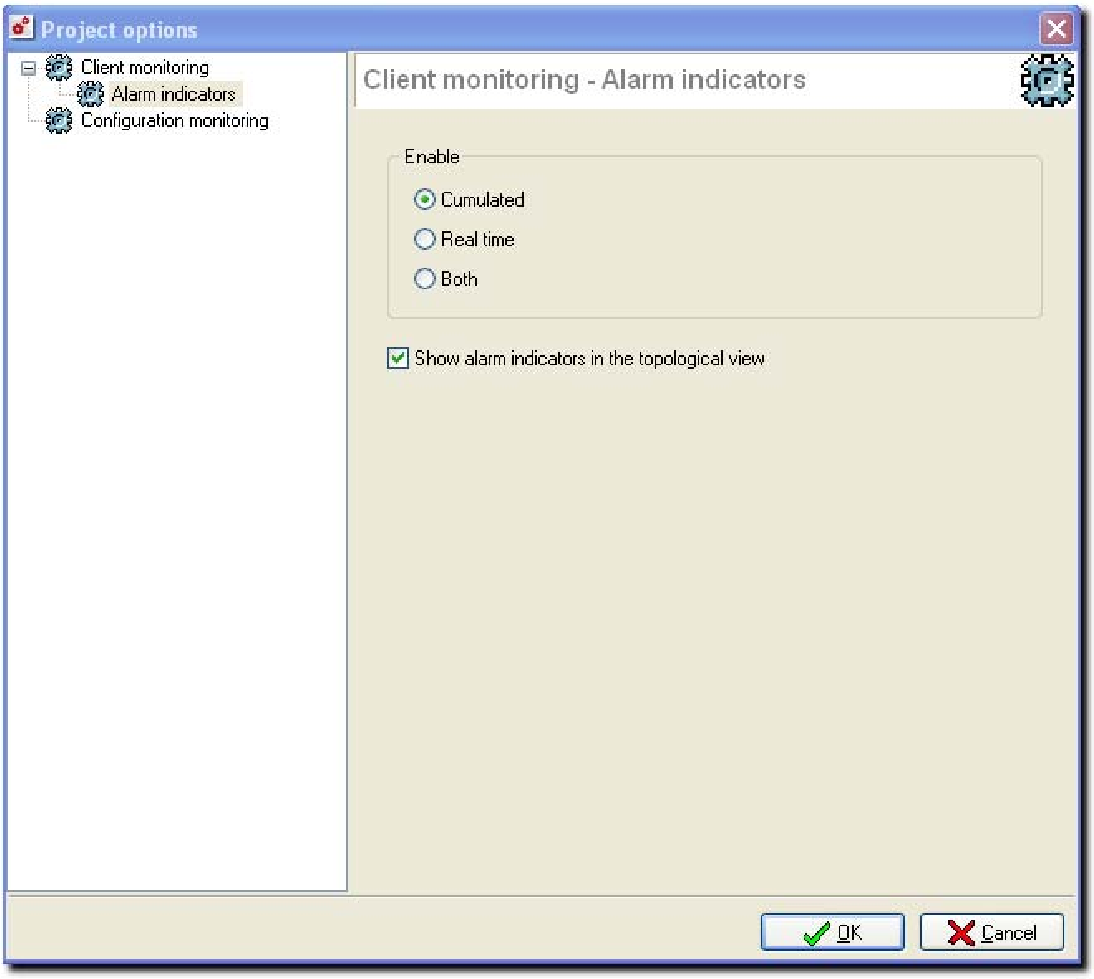
Figure 458: Project options - Client monitoring

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.

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.



Project options

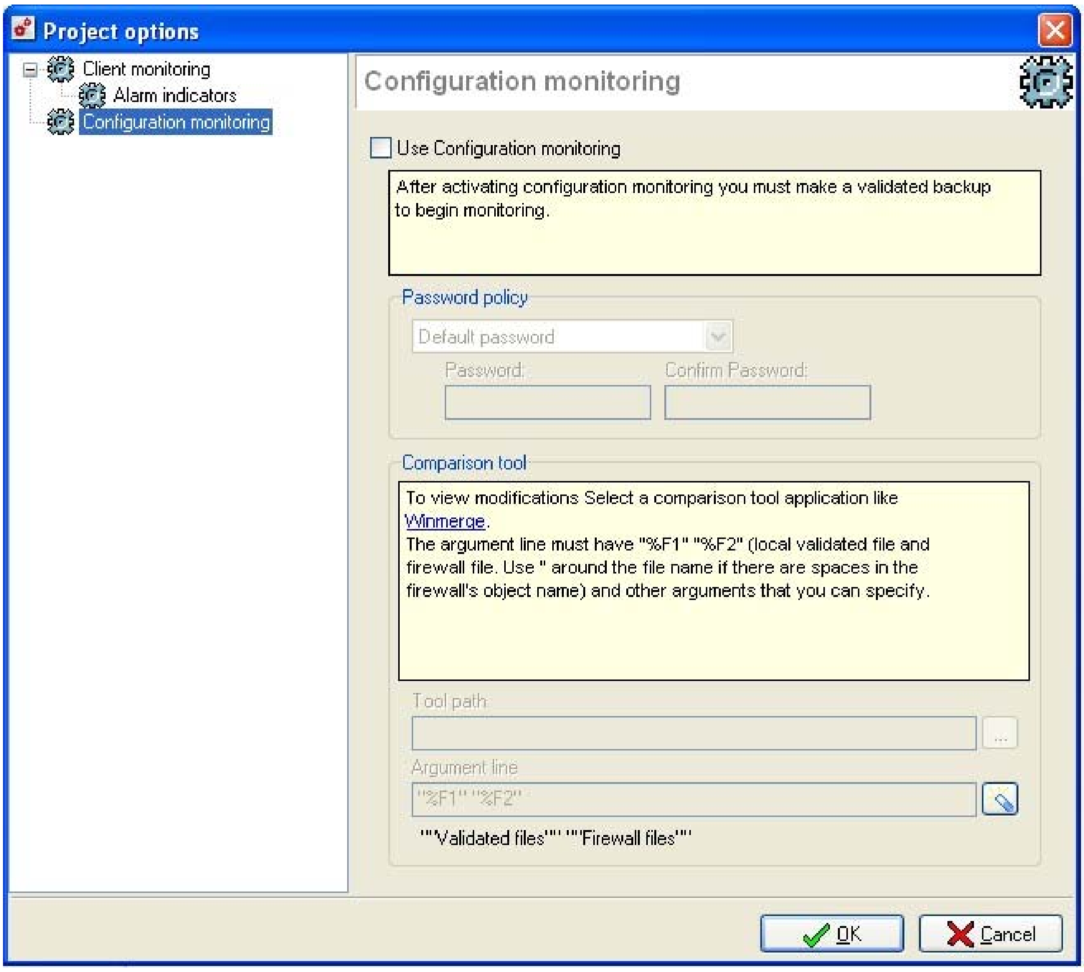
Client monitoring - Alarm indicators

Enable
- ● Cumulated
- ○ Real time
- ○ Both

☑ Show alarm indicators in the topological view

Figure 459: Project options – Alarm indicators

20.2.3.2. Configuration monitoring



☐ Use Configuration monitoring

After activating configuration monitoring you must make a validated backup to begin monitoring.

To view modifications Select a comparison tool application like Winmerge.
The argument line must have "%F1" "%F2" (local validated file and firewall file. Use " around the file name if there are spaces in the firewall's object name) and other arguments that you can specify.

"%F1" "%F2"

""Validated files"" ""Firewall files""

Figure 460: 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).

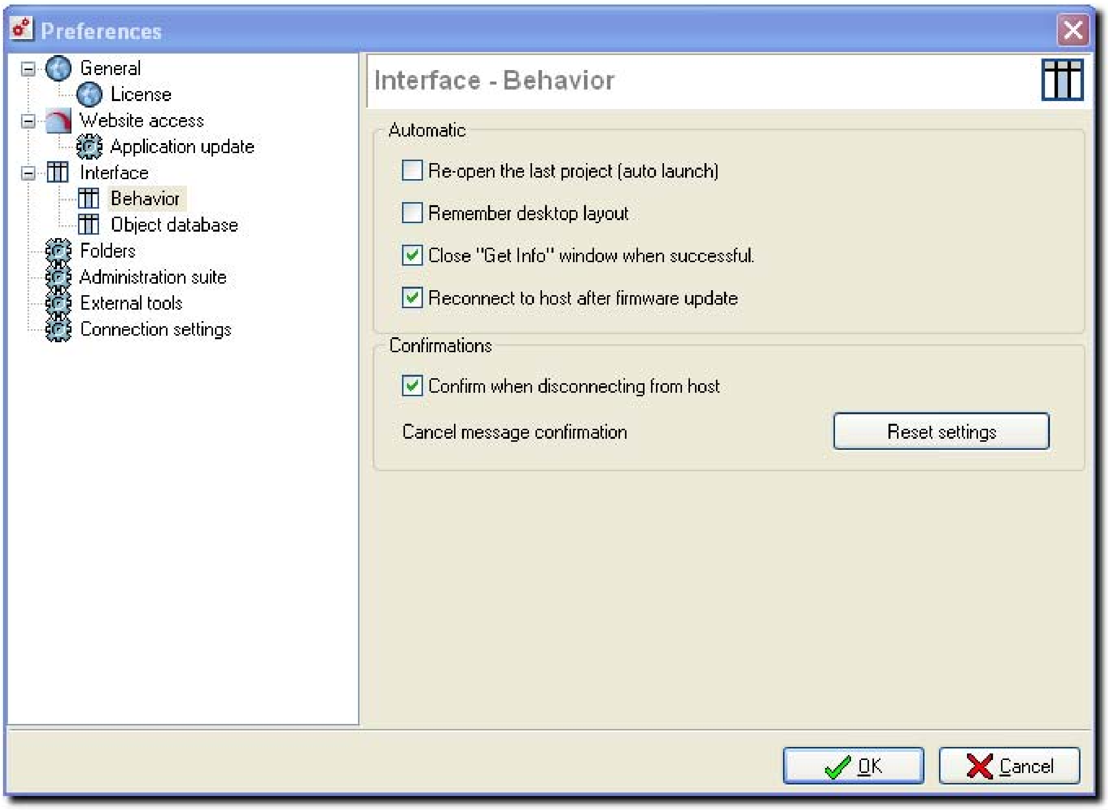
Use configuration monitoring	Option that activates configuration monitoring. The configurations of the monitored appliances have to be backed up and validated before you begin.
Password policy	By default, passwords are not needed when validating a configuration. However, passwords can be defined, either 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 poassword 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.

20.2.4. Options

This menu is explained in *Part 19: Miscellaneous actions*. However, in Global Administration mode, some windows may be different.

20.2.4.1 Behavior



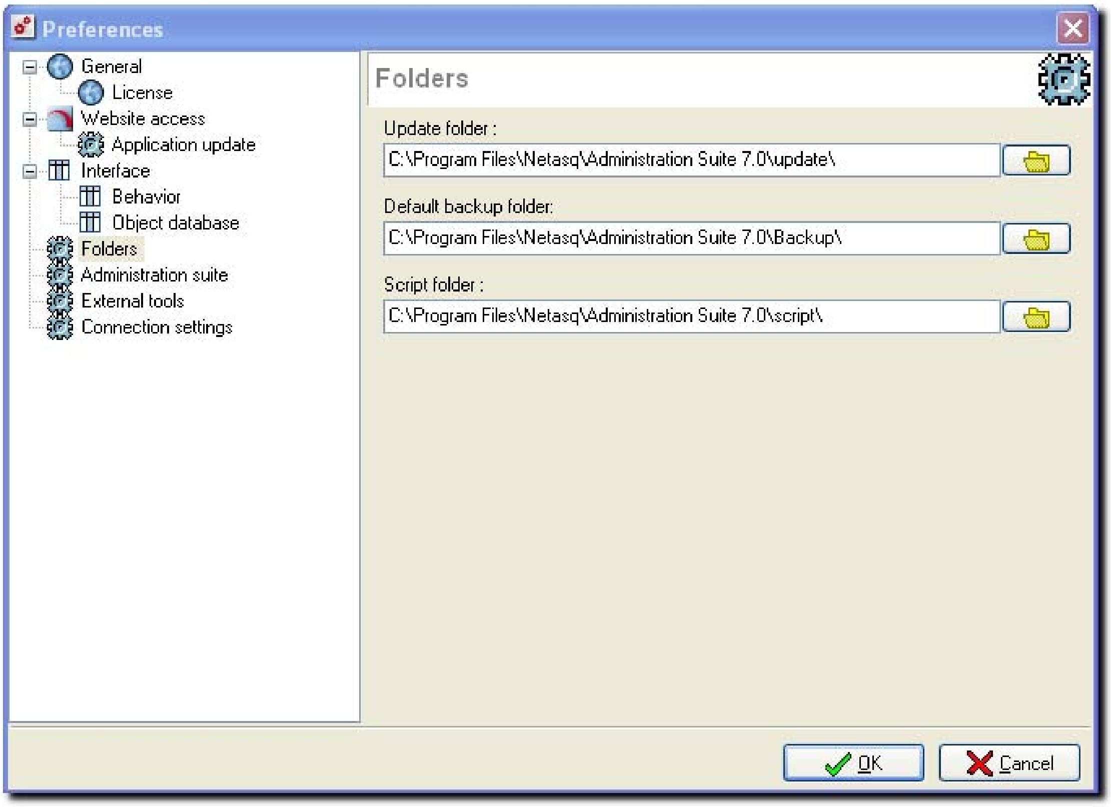
□ Re-open the last project (auto launch)
□ Remember desktop layout
☑ Close "Get Info" window when successful.
☑ Reconnect to host after firmware update
☑ Confirm when disconnecting from host
Cancel message confirmation

Figure 461: 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"	Closes this window automatically.

window when successful	
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.

20.2.4.2. Folders



Update folder :
C:\Program Files\Netasq\Administration Suite 7.0\update\

Default backup folder:
C:\Program Files\Netasq\Administration Suite 7.0\Backup\

Script folder :
C:\Program Files\Netasq\Administration Suite 7.0\script\

Figure 462: 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 cofngurations bakcup, 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\
```

20.2.4.3. 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).

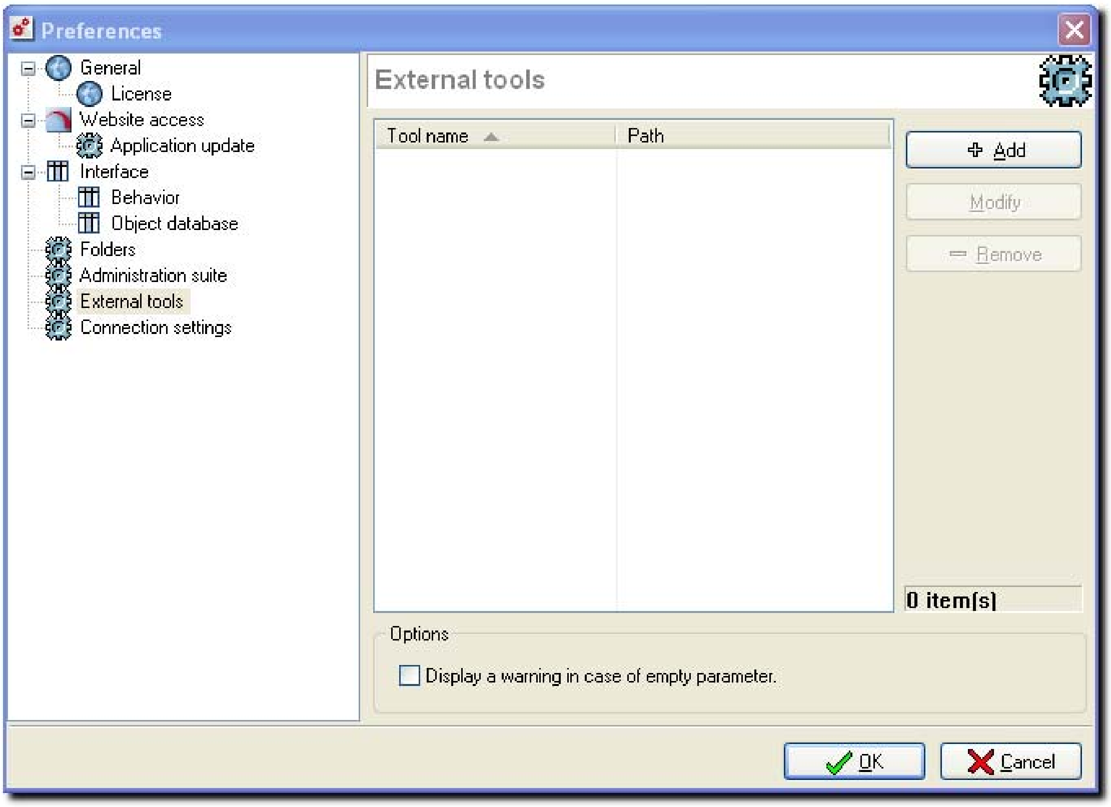


Figure 463: Preferences - External tools

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

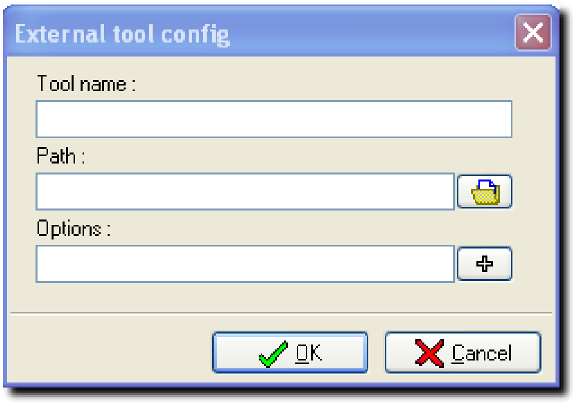


Figure 464: Configuring external tools

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.

CHAPTER 3: USING GLOBAL ADMINISTRATION

20.3.1. General

20.3.1.1. 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.

20.3.1.2. 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.

20.3.1.3. Opening and closing a project

You can open a project by starting NETASQ Global Administration (*Part 20/Chapter 1: 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.

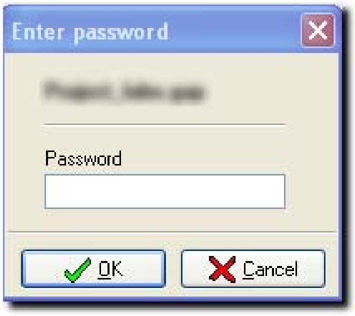


Figure 465: Password

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

20.3.1.4. 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.

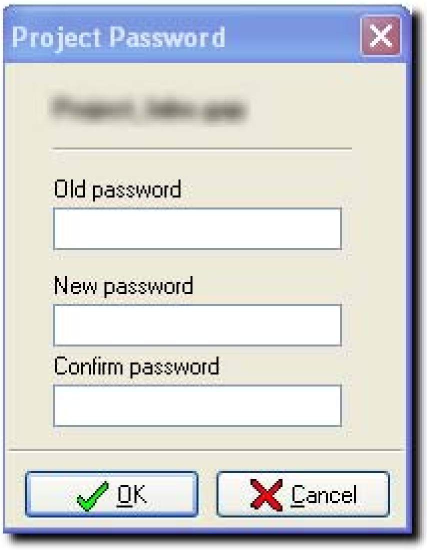


Figure 466: Project password

20.3.1.5. 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.

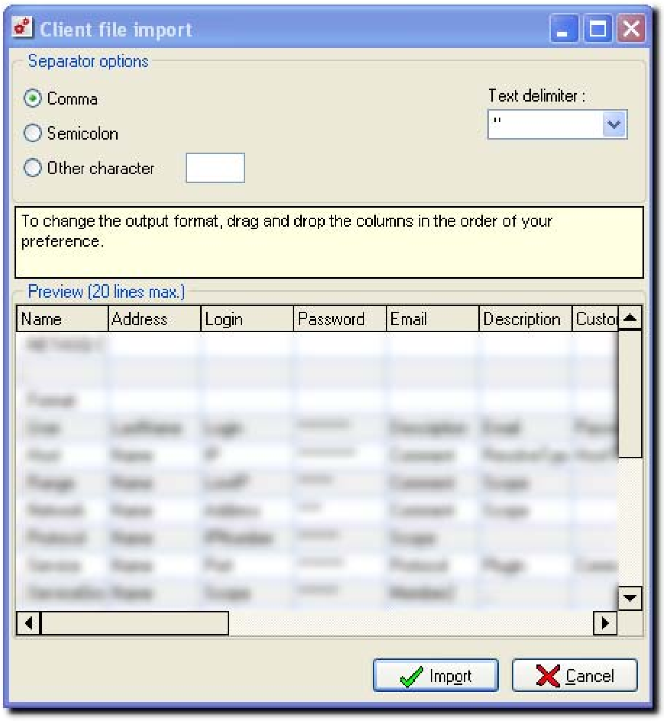
Example
FW_1,10.0.0.1,admin,FRANCE,jean.dupont@NETASQ.com
FW_2,10.0.0.2,admin,ITALY
FW_3,10.0.0.3,,BELGIUM

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.

Once the file has been selected, the following window will appear:



Client file import

Separator options

● Comma

○ Semicolon

○ Other character

Text delimiter : "

To change the output format, drag and drop the columns in the order of your preference.

Preview (20 lines max.)

Name	Address	Login	Password	Email	Description	Custo

Figure 467: Importing client 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.

20.3.1.6. Exporting firewall from a projet

All appliances in the general view of a selection of some of them can be exported to a .csv or .txt file.

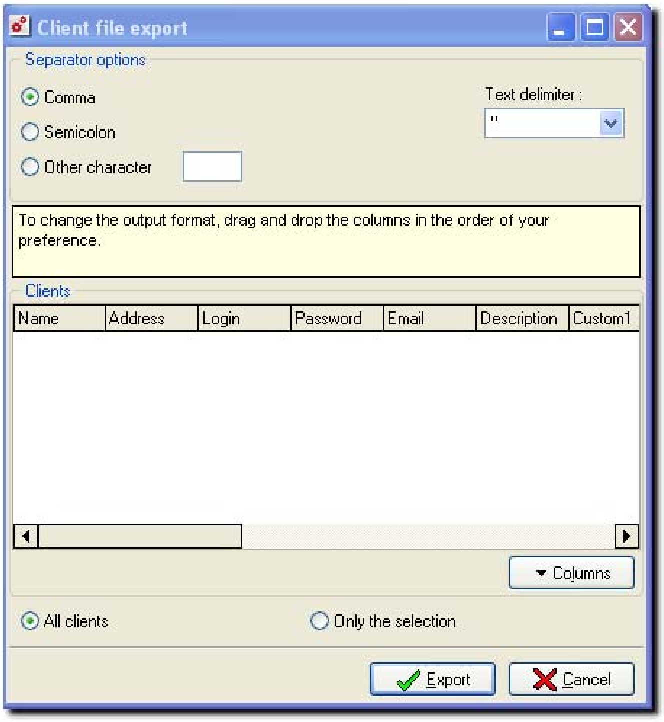
This file could contain the following information for each appliance:

- 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….`** The following window will appear:



Client file export

Separator options

● Comma

○ Semicolon

○ Other character

Text delimiter : "

To change the output format, drag and drop the columns in the order of your preference.

Clients

Name	Address	Login	Password	Email	Description	Custom1

● All clients

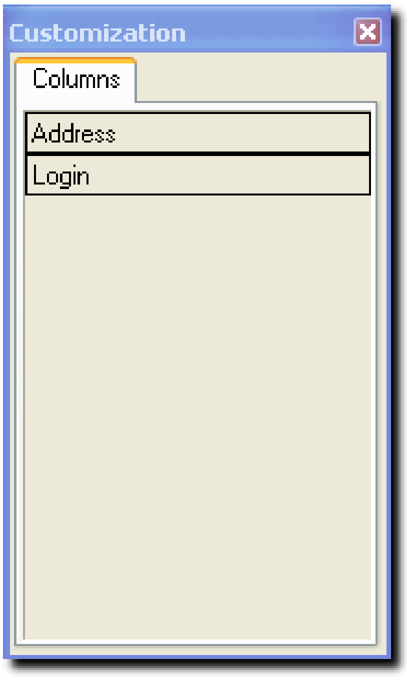
○ Only the selection

Figure 468: Exporting the client 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**.

A window similar to the following window opens:



Customization

Columns

Address

Login

Figure 469: Customization - Columns

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, 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.

20.3.1.7. Modifying the project password

It is possible to modify the password protecting the current project.

Select the menu item **`Project\Modify password`**. The following window appears:

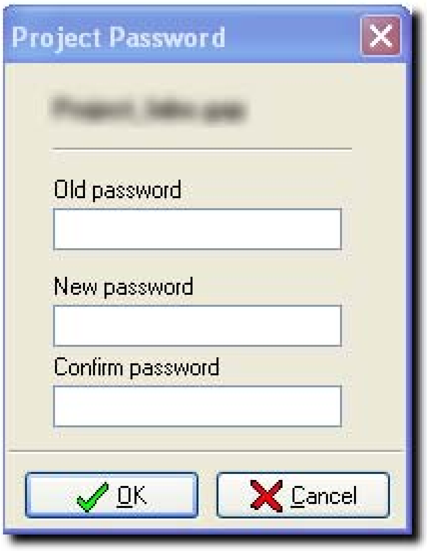


Figure 470: Project password

Enter the old project password, and then enter and confirm the new password.

20.3.2. Managing firewalls in the flat view

20.3.2.1. Flat view

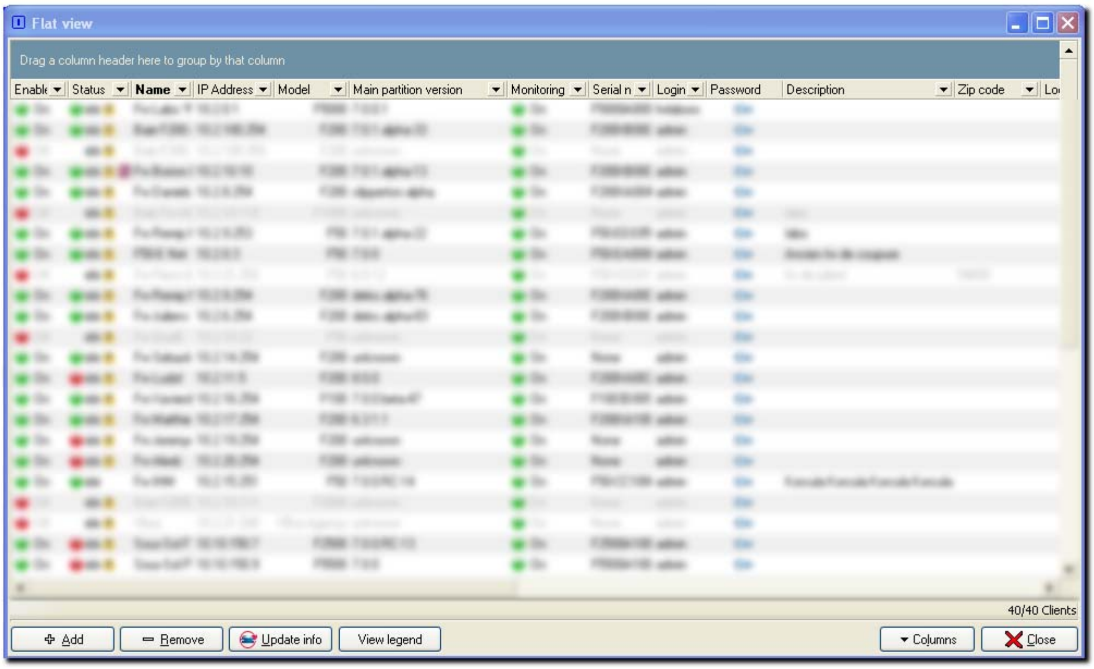


Figure 471: Flat view

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:

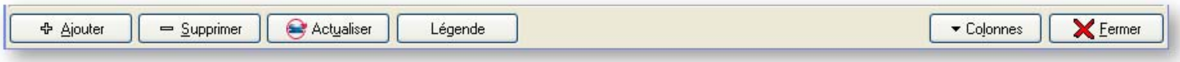


Figure 472: Action buttons

Add	Allows you to add an appliance to the table
Delete	Allows you to delete an appliance from the table
Update information	Manually refreshes the information concerning the appliances.
Legend	Displays an information window regarding the last conection, high availability, configuration tracking and the connection.
Columns	Manages the display of the table columns.
Close	Closes the view.

20.3.2.2. Managing appliances in a table

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:

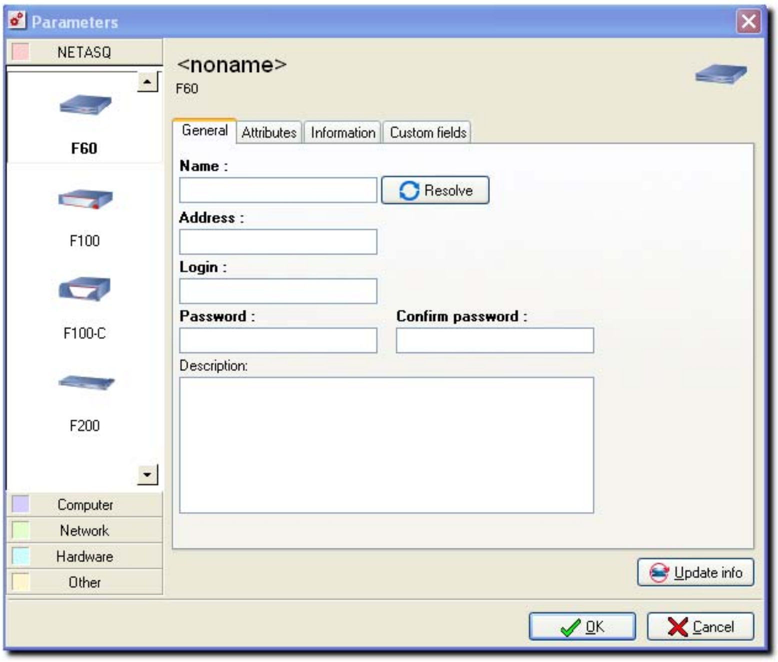


Figure 473: Parameters - General

<u>"General" tab</u>

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

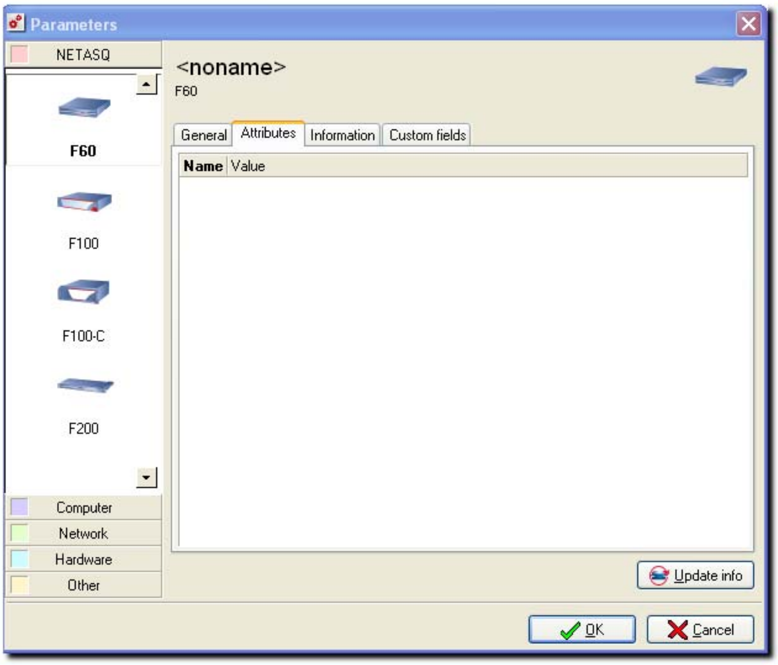


Figure 474: Parameters - Attributes

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

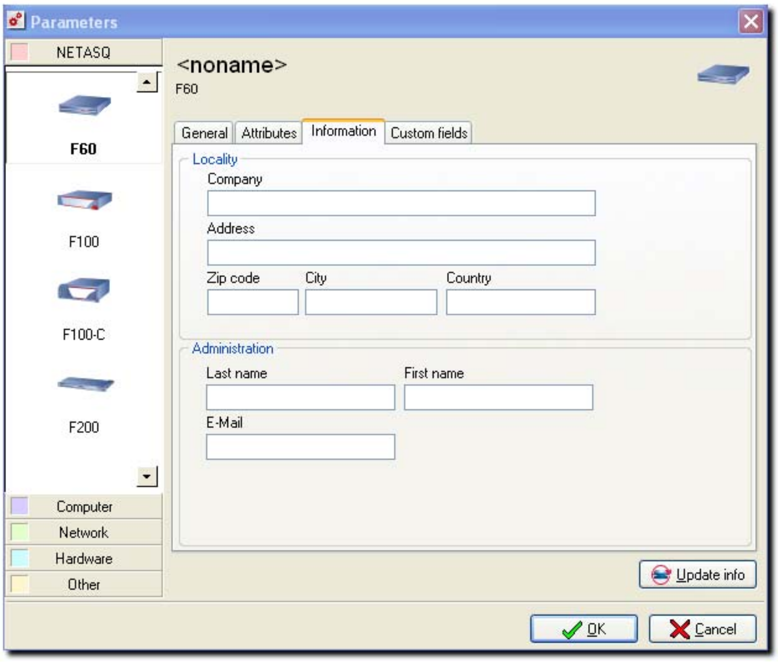
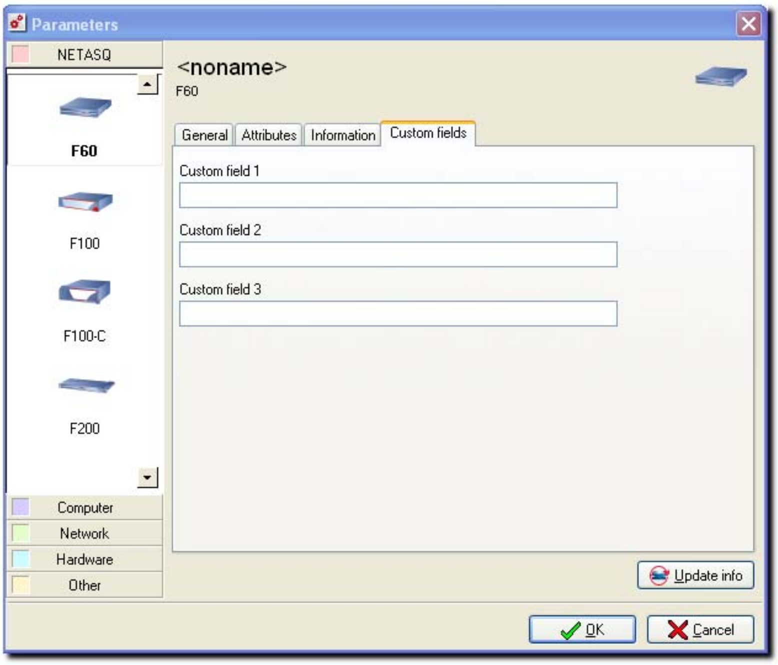


Figure 475: Parameters - Information

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



<noname>
F60

Custom field 1

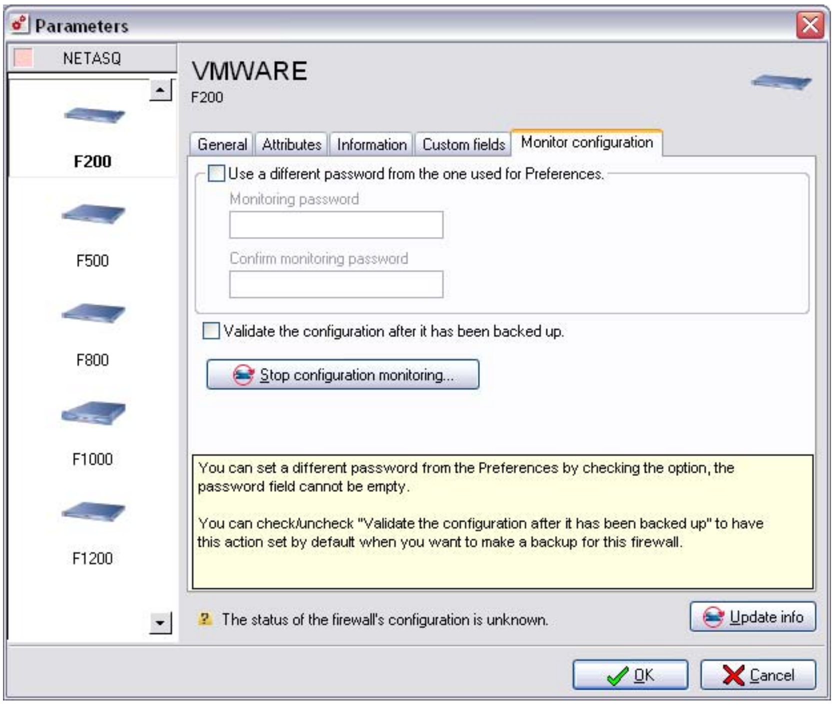
Custom field 2

Custom field 3

Figure 476: Parameters – Custom fields

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

"Configuration Monitoring" tab



VMWARE
F200

☐ Use a different password from the one used for Preferences.

Monitoring password

Confirm monitoring password

☐ Validate the configuration after it has been backed up.

You can set a different password from the Preferences by checking the option, the password field cannot be empty.

You can check/uncheck "Validate the configuration after it has been backed up" to have this action set by default when you want to make a backup for this firewall.

? The status of the firewall's configuration is unknown.

Figure 477: Parameters – Configuration monitoring

This tab only appears if the configuration monitoring features have been activated in NETASQ Global Administration (see *Part 20/Chapter 2: "Project options")* and if the appliance supports this feature (NETASQ appliances in version 6.3 or higher). The options for this tab enable defining the monitoring mode selected by the administrator.

Use a different password from the one in Preferences	To monitor the appliance's configuration, NETASQ Global Administration's comparison is based on a backup of a "validated" configuration. The password validates this backup by default. This option allows defining a specific password for monitoring.
Monitoring password	Field in which the password is entered (mandatory if the option **Use a different password from the one in Preferences** has been selected).
Confirm monitoring password	Field for confirming the monitoring password.
Validate the configuration after a backup	To monitor the appliance's configuration, NETASQ Global Administration's comparison is based on a backup of a "validated" configuration. During the backup stage, the checkbox **Validate the configuration after a backup** is automatically selected, thereby ensuring that each backup is automatically "validated".
Stop configuration monitoring	The button **Stop configuration monitoring** resets information known about the appliance's configuration. NETASQ Global Administration will no longer indicate whether the configuration has been modified until the next "Refreshment".

The model of the selected firewall can be changed, using the bar to the left of the window.

Click on **OK** once the information has been entered. The appliance is then added to the flat view list.

Then add all the appliances that you want to manage in the current project.

Deleting a firewall from the table

To delete an appliance, you must first select it in the table and then click on the **Remove** button, or press the **Del** button, or click with the right mouse button and choose the "Remove" option. The appliance is then removed from the list, and all information concerning this appliance is deleted.

Deactivating a firewall in the table

If an appliance is no longer active (after a hardware crash, or uninstallation, etc.) it can be considered as deactivated in NETASQ Global Administration. To do this, click on the appliance with the right mouse button, then select the "Disable" option. This means that the appliance is then no longer managed by NETASQ Global Administration; its status changes to **OFF**, and it will be grayed out in the different views. To reactivate this appliance click with the right mouse button, then select the "Enable" option.

Multi-Selection

It is possible to execute the same actions simultaneously on several Firewalls listed in the table. Use the **Shift** and **Ctrl** buttons to select several Firewalls.

General view contextual menu

A right click on “General 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. At any time the features accessible from the contextual menu when selecting an object integrate the features accessible when placing the pointer over empty space, therefore only this menu shall be covered.

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

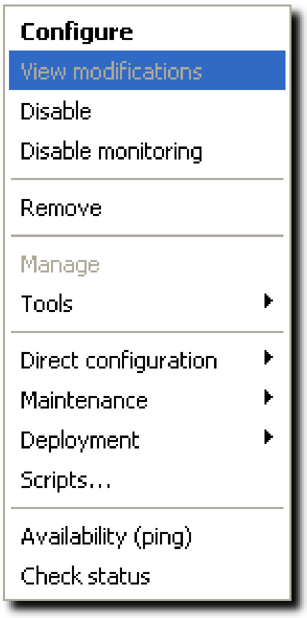


Figure 478: Contextual menu

Add	Adds a firewall to the General View
Configure	Accesses the configuration of a firewall. 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	Firewall monitoring can now be enabled or disabled. By default, monitoring is enabled as long as the license allows it.
Remove	Removes a firewall from the General View.
Manage	Opens NETASQ UNIFIED MANAGER.
Tools	Access to NETASQ configuration tools and external tools.
Direct configuration	Access to direct configuration (cf 20.3.10. Direct configuration).
Maintenance	Access to NETASQ Global Administration maintenance functions.
Deployment	For deploying the configurations in NETASQ Global Administration.
Scripts…	Enables executing NETASQ scripts on targeted appliances.
Availability (ping)	Tests the availability of an appliance (tries to connect to the servers).
Check status	Manual update of appliance status

20.3.2.4. Information listed in the table

The table lists certain types of information relating to each product.

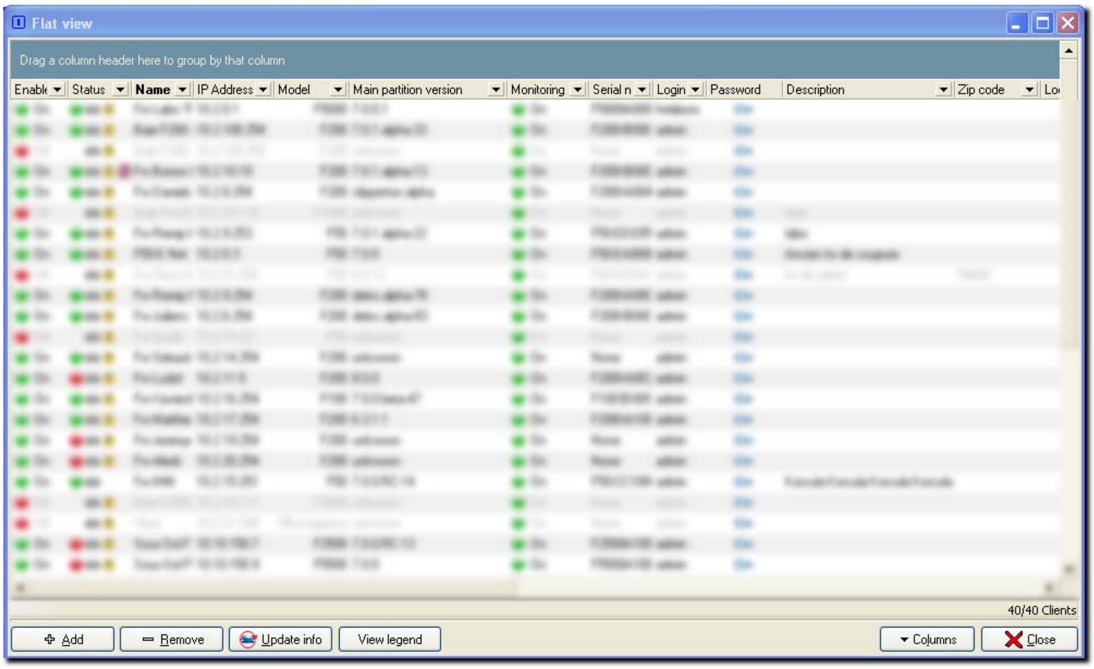


Figure 479: General view

This information includes:

Enable	This field is for specifying whether you wish to manage the appliance with NETASQ Global Administration or not. If the status is “ON”, then the appliance will be managed by NETASQ Global Administration, if the status is “OFF”, then the appliance will not be managed by NETASQ Global Administration (but the information will be retained in the project).
Name	Name chosen for the firewall.
IP address	IP address of the appliance to which NETASQ Global Administration can be connected.
Login	Administration account login for the firewall.
Password	Administration account password for the firewall.
Partition	Current version of the firewall’s firmware
Model	Model of the firewall.
Monitoring	The status of configuration monitoring is shown in the general view.
Description	Comments associated with the firewall.
Company	Company (or subsidiary, or department…) where the firewall is installed.
Country	The country where the firewall is installed.
Admin e-mail	E-mail address of the contact person who manages the firewall locally.
Admin first name	First name of the contact person who manages the firewall locally.
Admin last name	Last name of the contact person who locally manages the firewall.
Address	Address where the appliance is installed.
Zip Code	The postal code of the city where the appliance is installed.
Status	Status of the Firewall. This information is updated with the “Status Verification” function.

Serial number	Firewall's serial number.
Custom 1	First customized field containing additional information.

The "Partition" information is obtained directly on each firewall. All the other information had been entered when adding the appliance.

The password field does not appear in plain text for obvious security reasons.

To modify the information contained in the table, double-click on the appliance that you would like to edit and select the appliance, then click with the right mouse button and select **`Configure`**. Then you can modify the information concerning the Firewall in the window that opens.

20.3.2.4. Modifying the display of information

You can modify the display of information for readability and easier access to information.

Choosing the columns to display

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 **Columns\Customize**. A window similar to the following window is displayed:

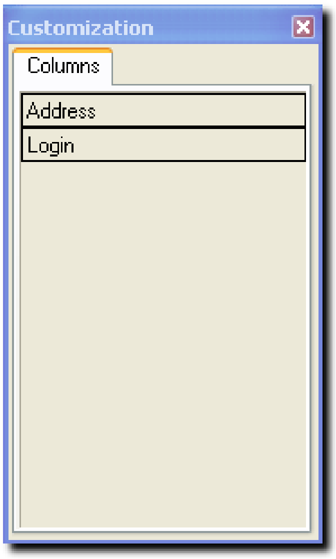


Figure 480: Customization - Columns

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 header of the column to the location where you would like to insert it in the bar of column headers, 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 you have to do to select a column and move it to the location desired.

Click on the white X in the upper right corner of the window to close the customization window.

You can revert to the initial display of the columns by clicking on Columns\Reset.

Hierarchical view

The table can be viewed as a hierarchy, which makes it easier to read information. This view is possible when creating group information.

A drop zone is positioned above the table, where you will see "Drag a column header here to group by that column". To group the information of a column, select the header of the column and move it into this zone. Then the appearance of the table changes. The column thus grouped, appears in the drop zone and the table displays the values resulting from the grouping, in node form. Clicking on the plus sign + in front of the group values expands the nodes and displays the line items that have been grouped. Thus there is no limit to grouping within groups.

> **Example**
> It is possible to group by main partition, then by model, in order to see the update status for the group of equipment by appliance type.

Sorting and filtering the information

There are two supplemental tools for managing the display of information.

Sort

You can sort the table’s lines according to the value of one of the columns, all you have to do is to click on the header of the column whose information you want to sort. Then a small gray triangle appears next to the column header ▲. The direction of the triangle determines the direction of the sort. To change the direction, just click on the column header again.

Filters

It is possible to display nothing but the lines of the table where certain fields respond to particular criteria. You will find the following small icon at the level of each column header ▼:

A drop-down list appears when you click on this icon. This list comprises all the values found in the column plus two values, “All” and “Custom”.

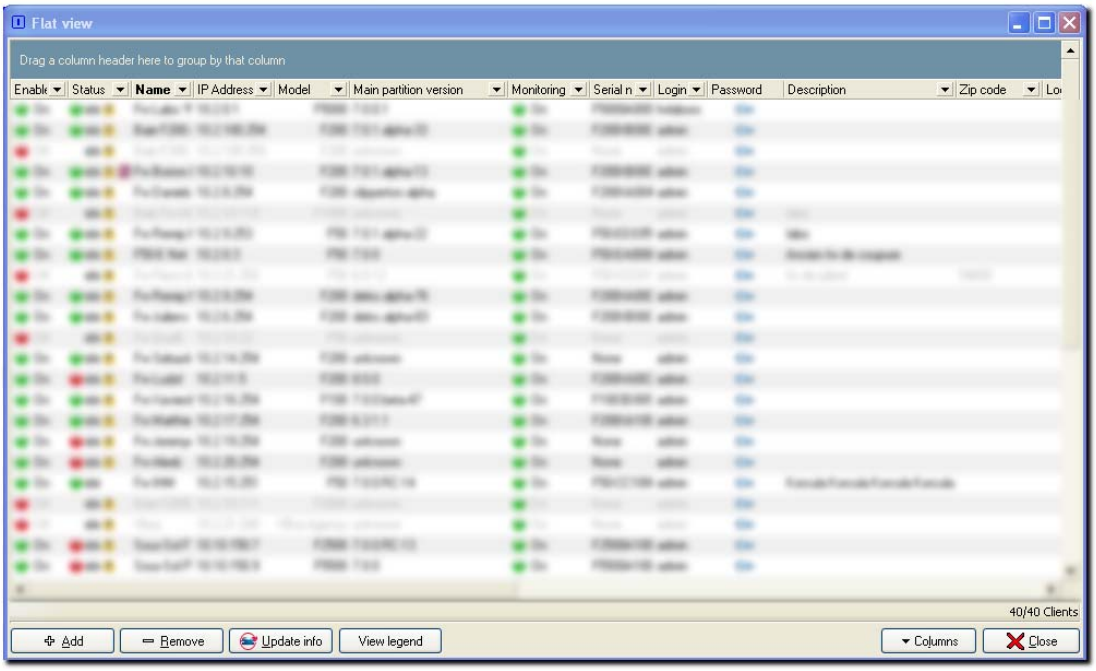
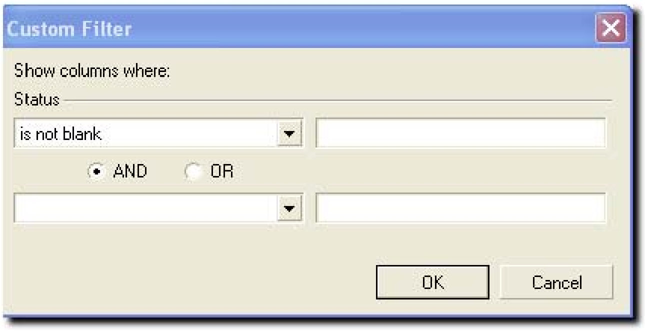


Figure 481: Drop-down list

When you choose a value from this list, only the lines whose column value equals the value selected will be displayed.

Choosing “All” displays all the line items.

Choosing “Custom” displays the following window:



Custom Filter

Show columns where:

Status

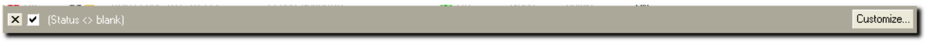
is not blank

● AND ○ OR

Figure 482: Custom filter

Use this window to define a personalized filter. You can define two criteria related by an “AND” or “OR” logical link.

When one or more filters are applied a new bar appears at the bottom of the table. This bar displays all the criteria that are applied to filter the table. The checkbox in this bar allows you to switch the filter on or off. The box containing an x allows you to delete the filter.



☒ ☑ (Status <> blank)

Figure 483: Filter bar

The **Customize** button in this same bar allows you to display a filter constructor to build higher-resolution filters.

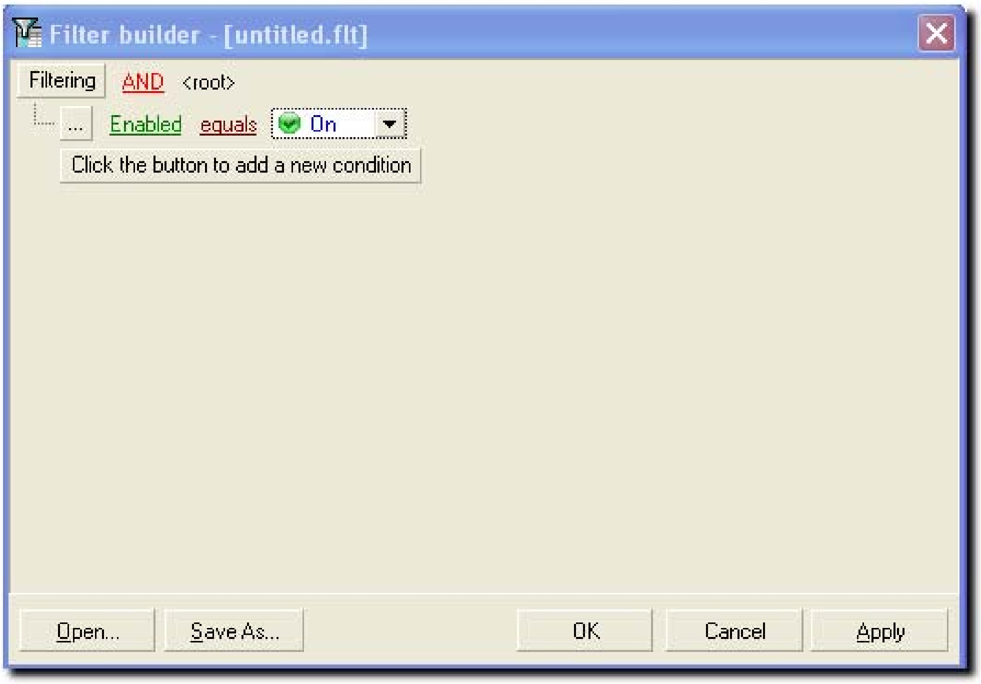

Filter builder - [untitled.flt]
Filtering
AND
<root>
...
Enabled
equals
On
Click the button to add a new condition
Open...
Save As...
OK
Cancel
Apply

Figure 484: Filter builder

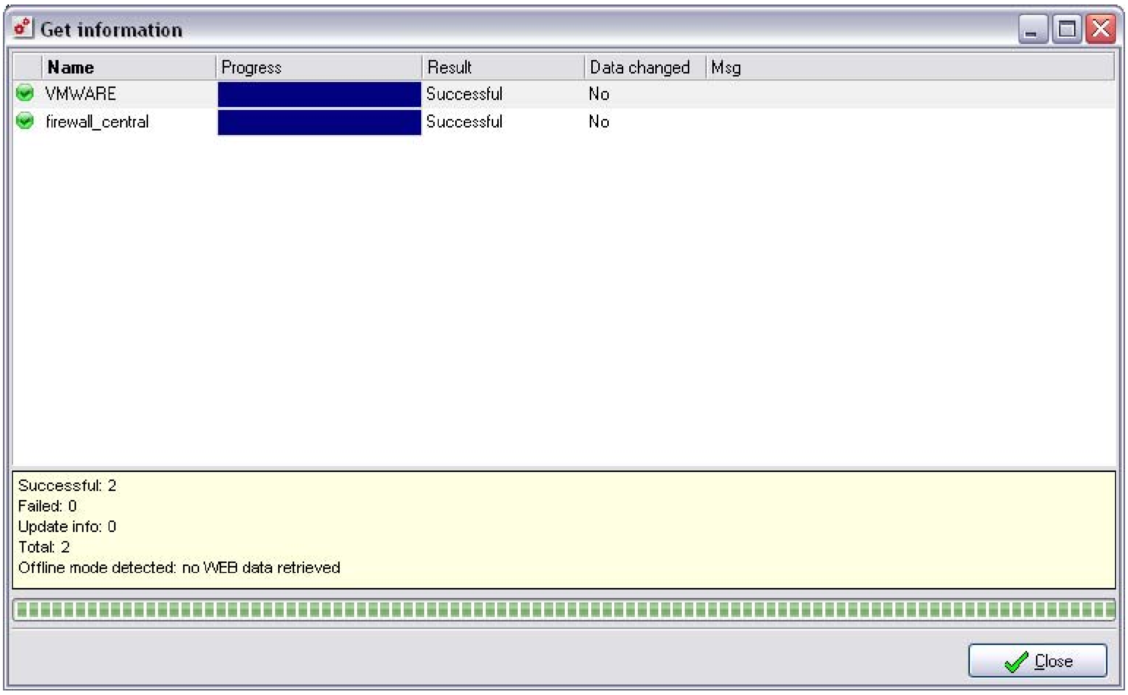
The filter constructor is displayed in a tree-structure and represents the different filter conditions. The filters can be saved for use in other projects thanks to the **Save as…** button. All you have to do is use the **Open** button to search for and open a filter that has been saved previously.

Example of a filter:

This filter means that the lines selected will be those for which the firewall has been activated.

20.3.2.5. Updating information

You can update the information concerning each appliance either automatically (**`Options/Preferences`**) or manually. To manually update the information, click on **Update info**; only those appliances with the value **ON** in the **Status** column will be taken into consideration. Then the following window is displayed:



Name	Progress	Result	Data changed	Msg
✓ VMWARE		Successful	No	
✓ firewall_central		Successful	No	

Successful: 2
Failed: 0
Update info: 0
Total: 2
Offline mode detected: no WEB data retrieved

Figure 485: Getting information

All the relevant firewalls appear in this window, a bar indicates the progress of the information update, and a signal light indicates the status of the update:

●	Information is being updated.
✗	Failure when updating information.
✓	Information was successfully updated.

Description of the different fields in this window

Name	Name of the firewall requiring an update.
In progess	Gauge of the update's progress.
Result	Result of the information update.
Modified data	Indicates whether the information has been modified since the last information update
Message	Explanatory message regarding the operation

4 items are provided at the bottom of the window: the number of successful information updates, the number of failed information updates, the number of information updates with modifications, all successful updates, all failures and the number of updates that have provided information.

The update notice will also be displayed to indicate the progress of the information update with regards to the NETASQ website:

Once the information has been updated, click on **Close**. Now the flat view information and the appliance attributes, such as the software version number, are completely updated.

20.3.3. Managing firewalls using the topological view

20.3. 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 topological view is organized as follows:

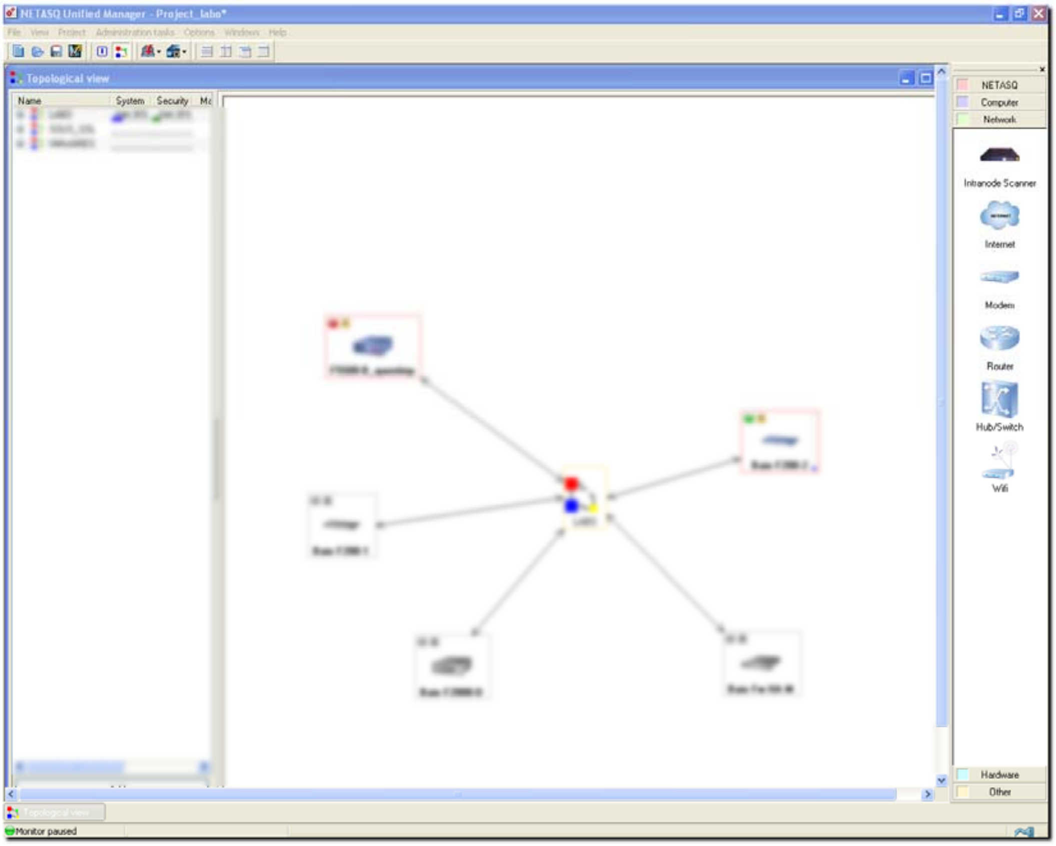


Figure 486: Topological view

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).

20.3.3.2. 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.

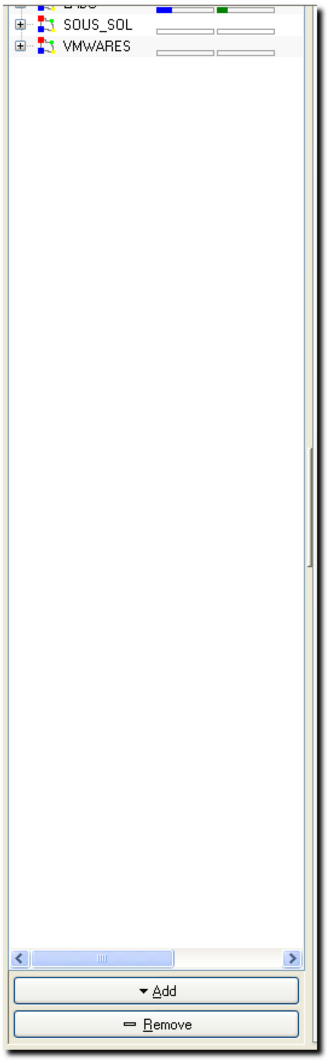


Figure 487: Topology classification

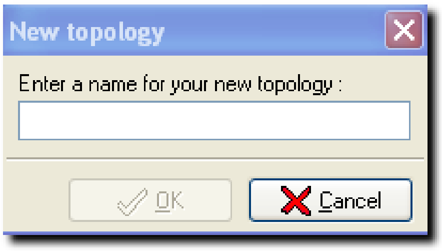


Figure 488: New Topology

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

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.

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.

20.3.3.3. Topology viewing zone

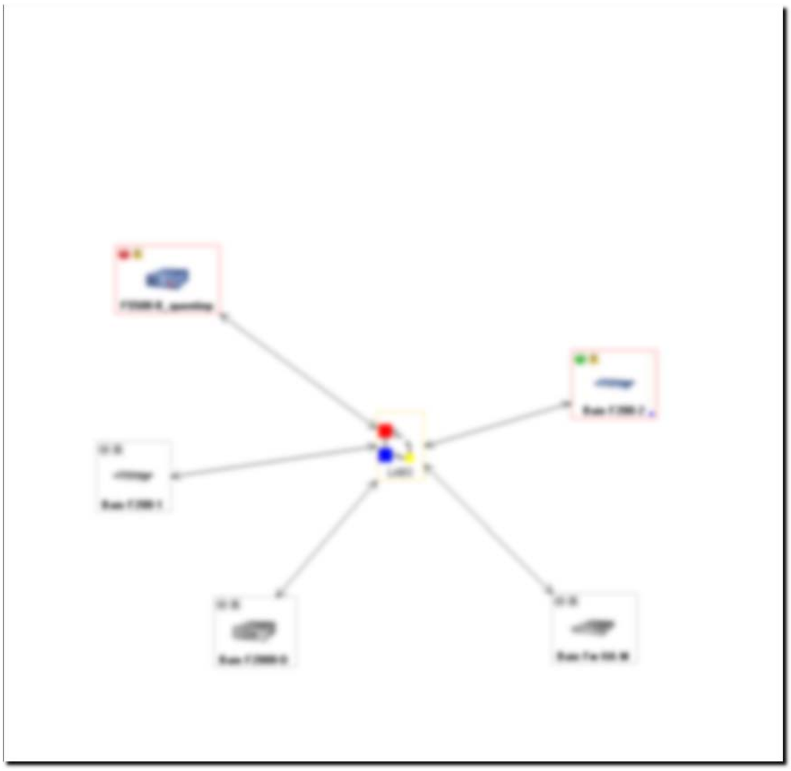


Figure 489: Topology viewing zone

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.

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:

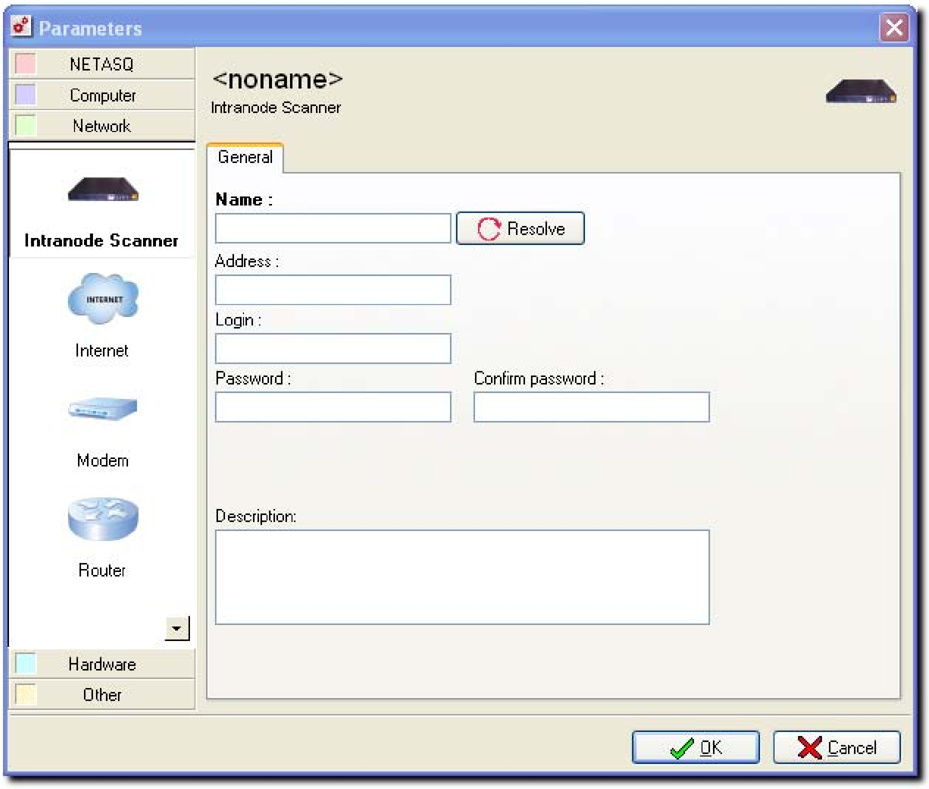


Figure 490: Parameters - General

(*See the section, 20.2.1. User interface for more about each of these object categories)*

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.

For "NETASQ" category objects

The following window is the first one displayed:

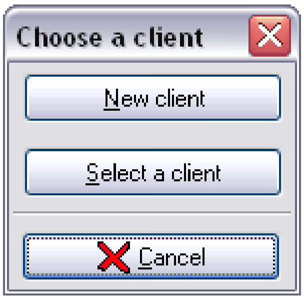


Figure 491: Choosing a client

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:

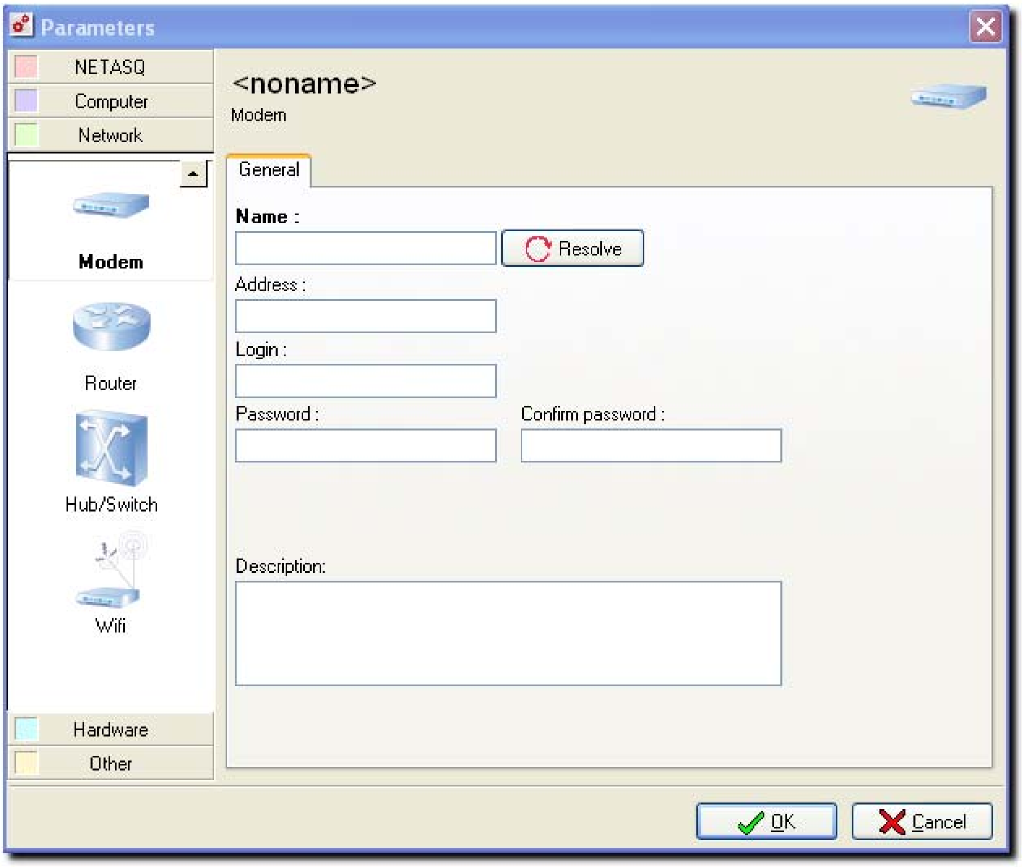


Figure 492: Parameters - General

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

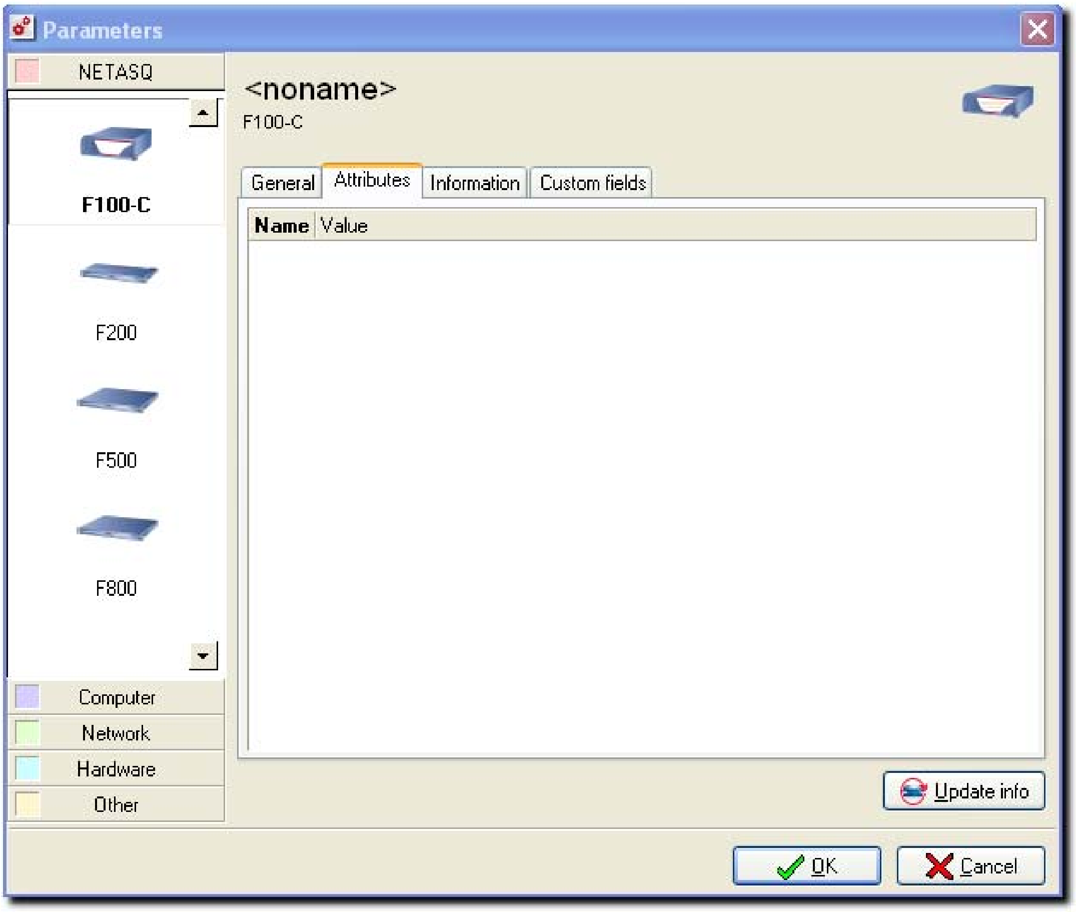


Figure 493: Parameters - Attributes

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

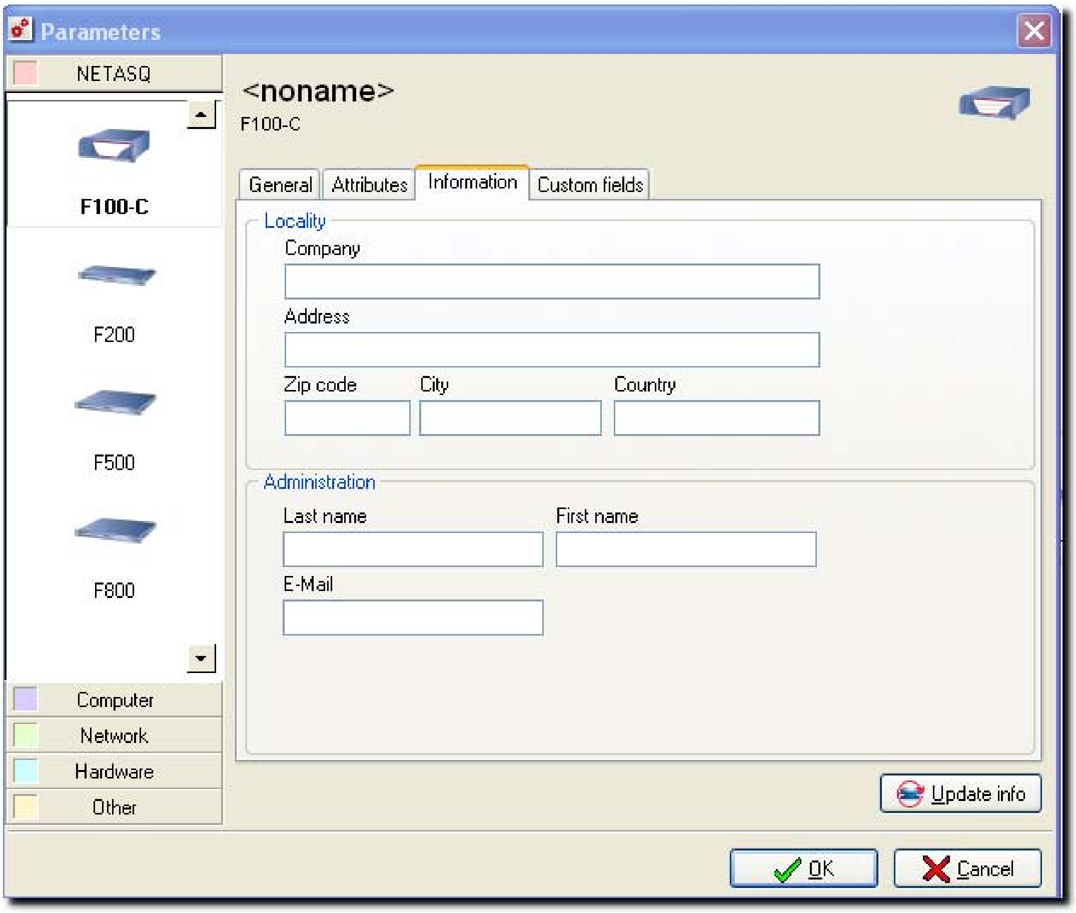


Figure 494: Parameters - Information

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.

For a “computer” category object

The following window appears:

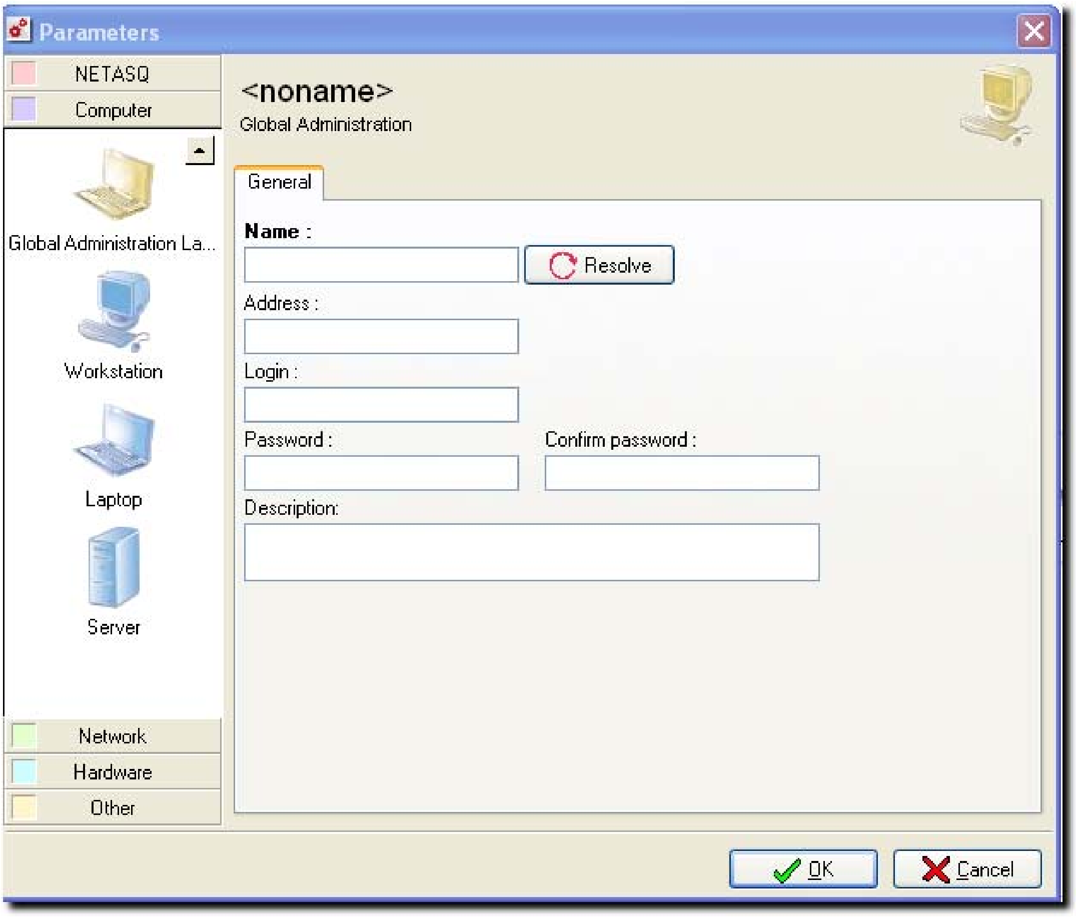


Figure 495: Parameters - General

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.

NETASQ UNIFIED MANAGER mode can launch external administration tools for certain equipment; in this case it will use the connection information provided here.

Click on **OK**. The object is then added in the preview zone.

For "Network" category objects

For example, the following window appears for modems:

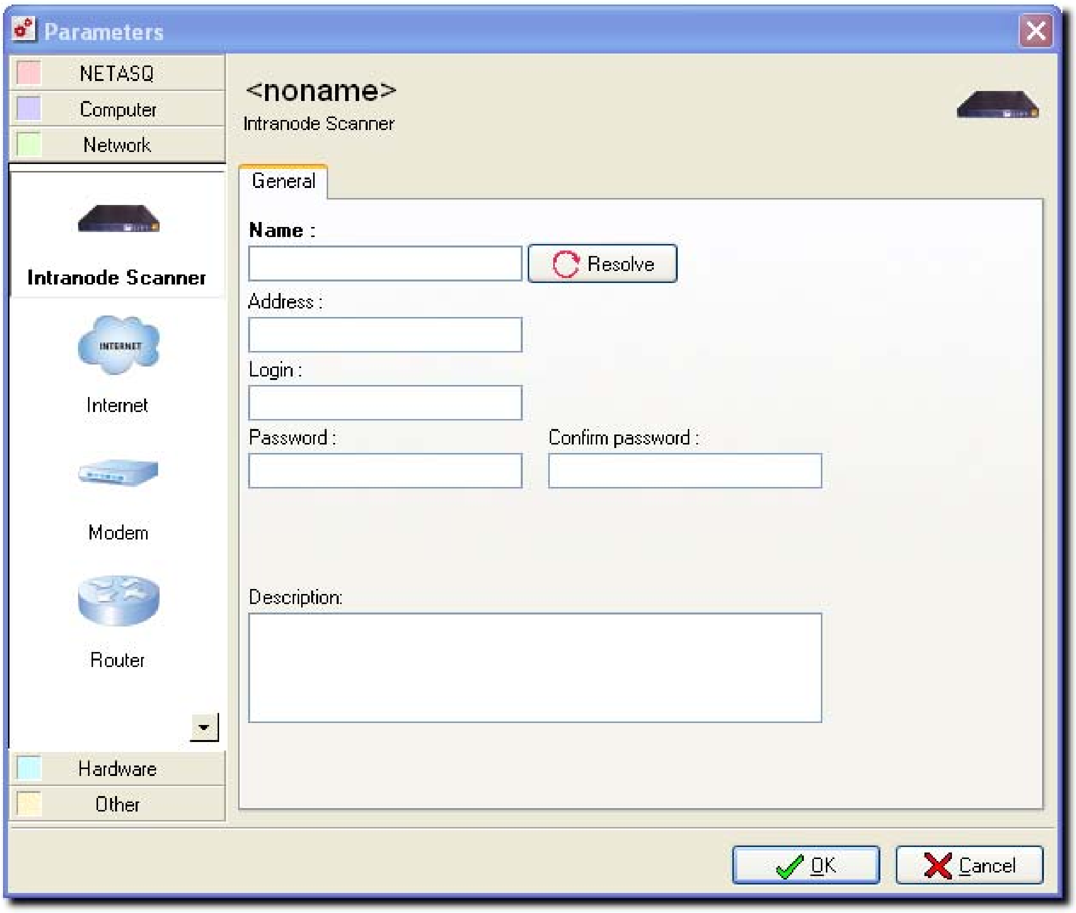


Figure 496: Parameters - General

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.

NETASQ UNIFIED MANAGER mode can launch external administration tools for certain equipment; in this case it will use the connection information provided here.

Click on **OK**. The object is then added in the preview zone.

For a "Hardware" category object

The following window will appear:

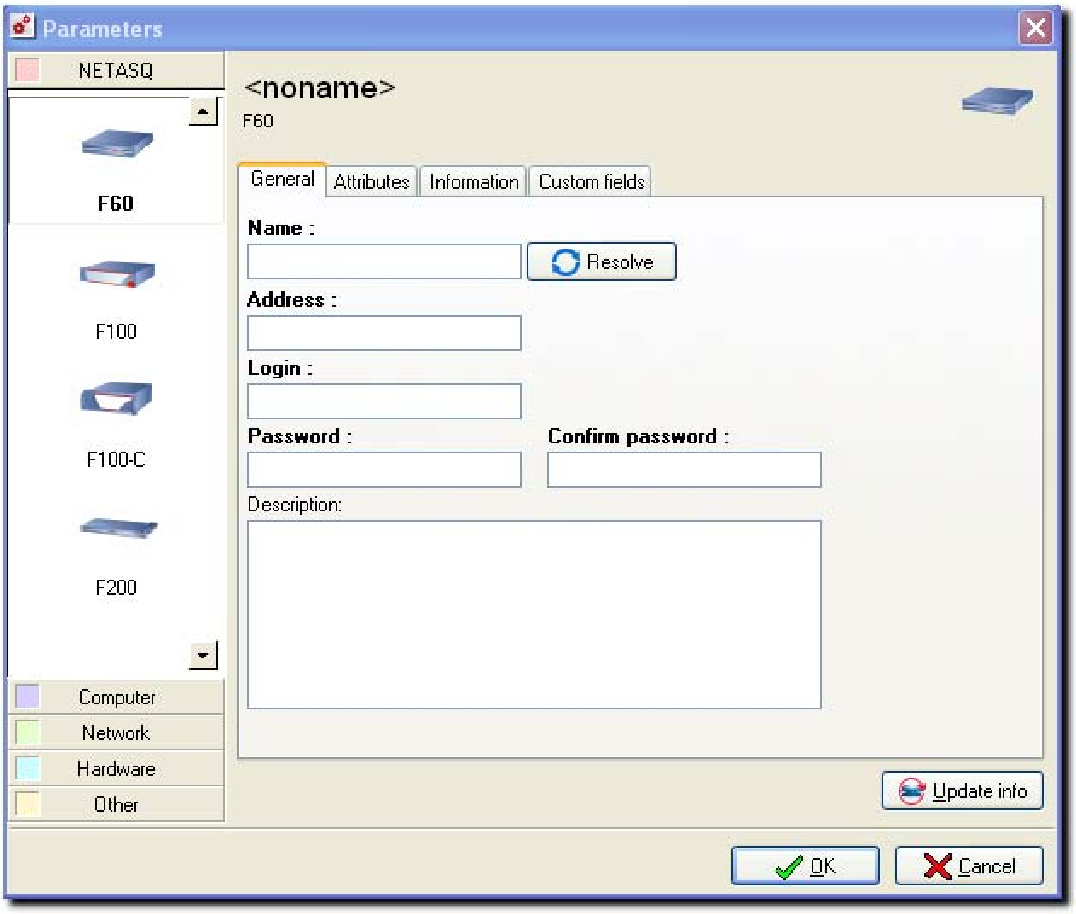


Figure 497: Parameters - General

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.

NETASQ UNIFIED MANAGER mode can launch external administration tools for certain equipment; in this case it will use the connection information provided here.

Click on **OK**. The object is then added in the preview zone.

For "Other" category objects

The following window appears:

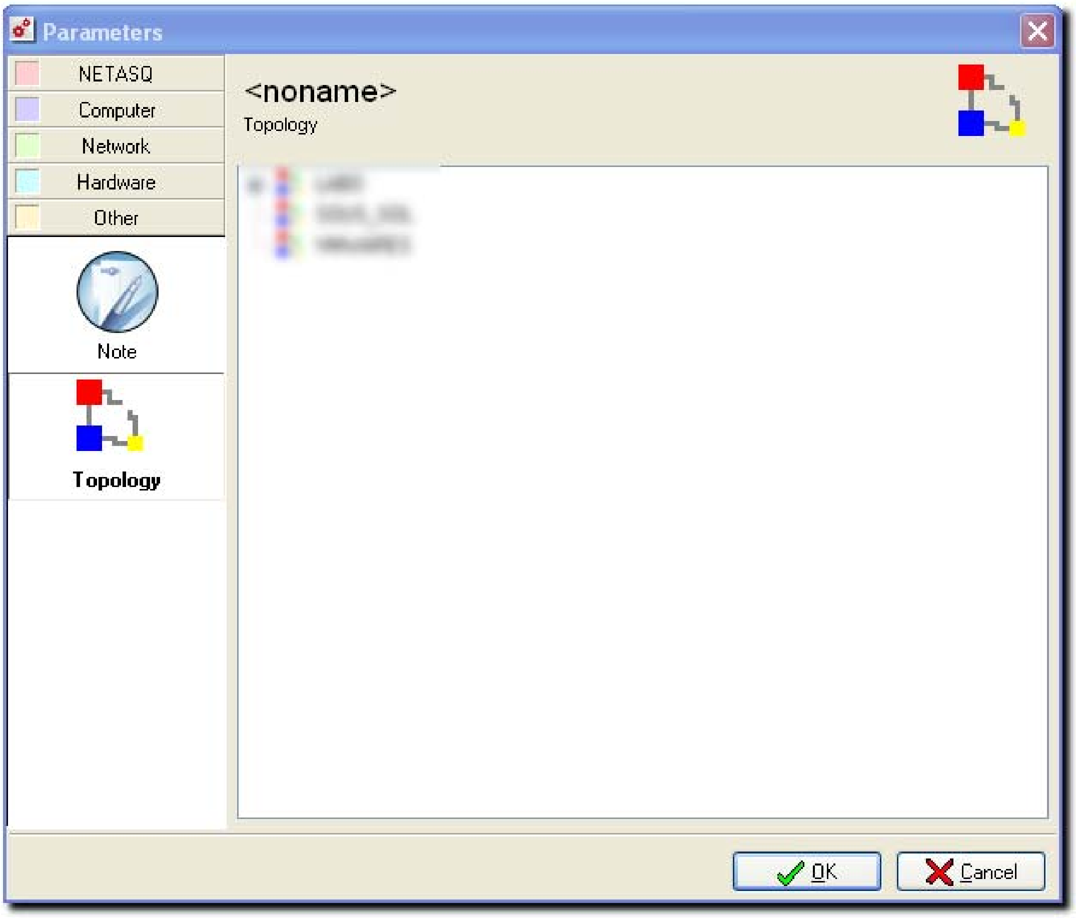


Figure 498: Parameters - Other

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.

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:

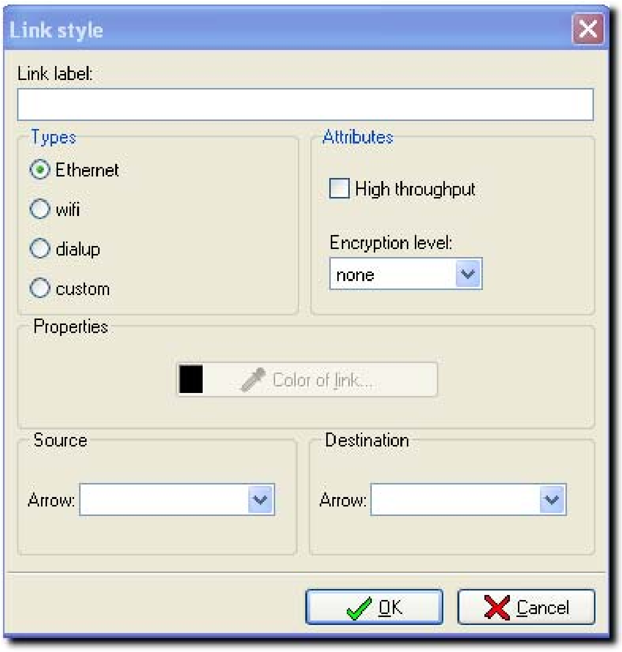
- NETASQ UTM.
- Host: NETASQ UNIFIED MANAGER workstations, servers, others.
- Network object: switch, modem, other.
- Hardware object.
- Notes.
- Topologies.

20.3.3.4. 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 the following window opens:



Link style

Link label:

Types
- ● Ethernet
- ○ wifi
- ○ dialup
- ○ custom

Attributes
- □ High throughput
- Encryption level: none

Properties

Color of link...

Source
Arrow:

Destination
Arrow:

Figure 499: Link style

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.

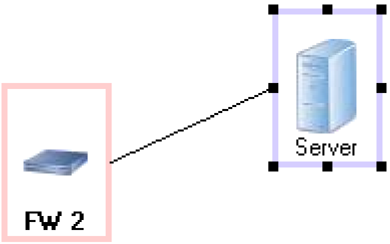


Figure 500: Link

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.

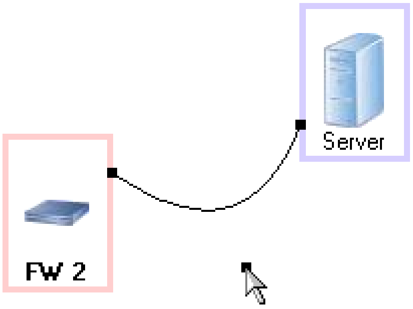


Figure 501: Link

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

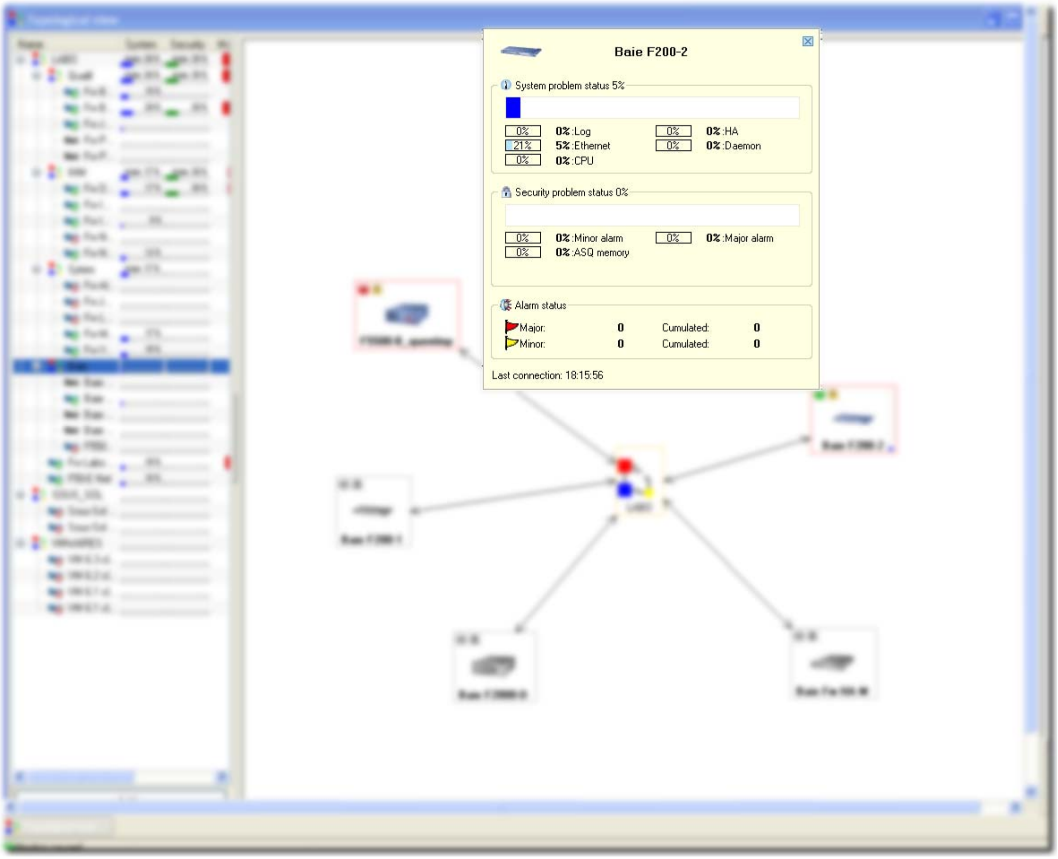
Select an object or the objects that you want to move, and then move the selection to the required location, keeping the left mouse button depressed.

20.3.4. 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.

Topological View indicator window



Baie F200-2

System problem status 5%

0%	**0%** :Log	0%	**0%** :HA
21%	**5%** :Ethernet	0%	**0%** :Daemon
0%	**0%** :CPU		

Security problem status 0%

0%	**0%** :Minor alarm	0%	**0%** :Major alarm
0%	**0%** :ASQ memory		

Alarm status

Major:	**0**	Cumulated:	**0**
Minor:	**0**	Cumulated:	**0**

Last connection: 18:15:56

Figure 502: 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.

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.

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 (see 20.2.3. Project).

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).

20.3.5. Administration tasks

20.3.5.1. 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.

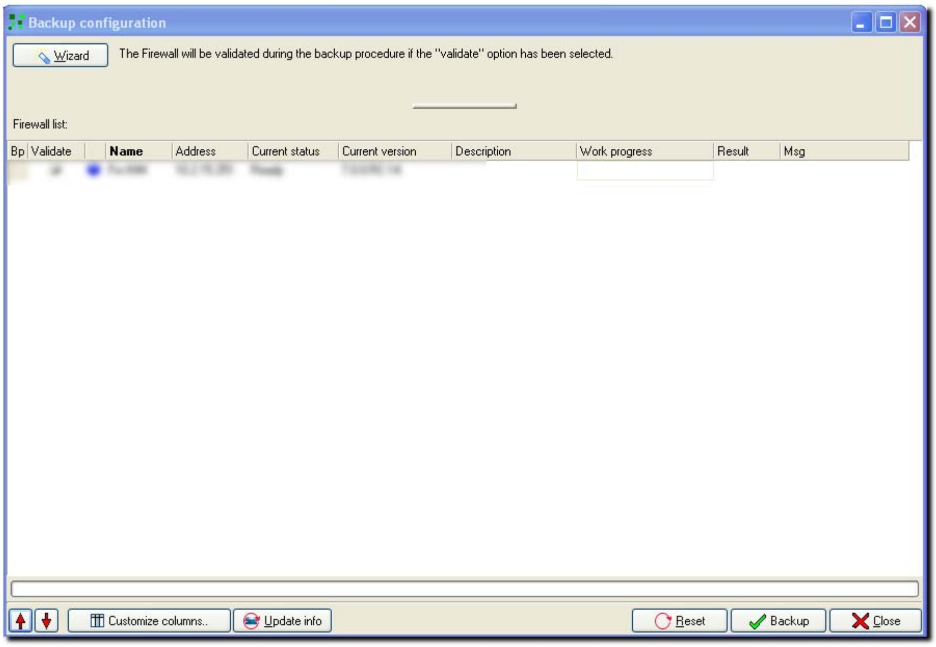
Configuration	Backs up and restores the configurations of appliances.
Update firmware	Updates the firmware of appliances.
Update license	Updates the licenses of appliances.
Back up partition	Backs up main partitions on secondary partitions (backup partitions).
Scripts	Enables the execution of NETASQ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

20.3.5.2. 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 menus in the NETASQ Global Administration mode:

- the menu **`Administrative tasks\configuration.`**
- the General View contextual menu in the “Maintenance” section,
- the Topological View contextual menu in the section **`Maintenance\Backup`** or **`Restore`**.

Configuration backup



The Firewall will be validated during the backup procedure if the "validate" option has been selected.

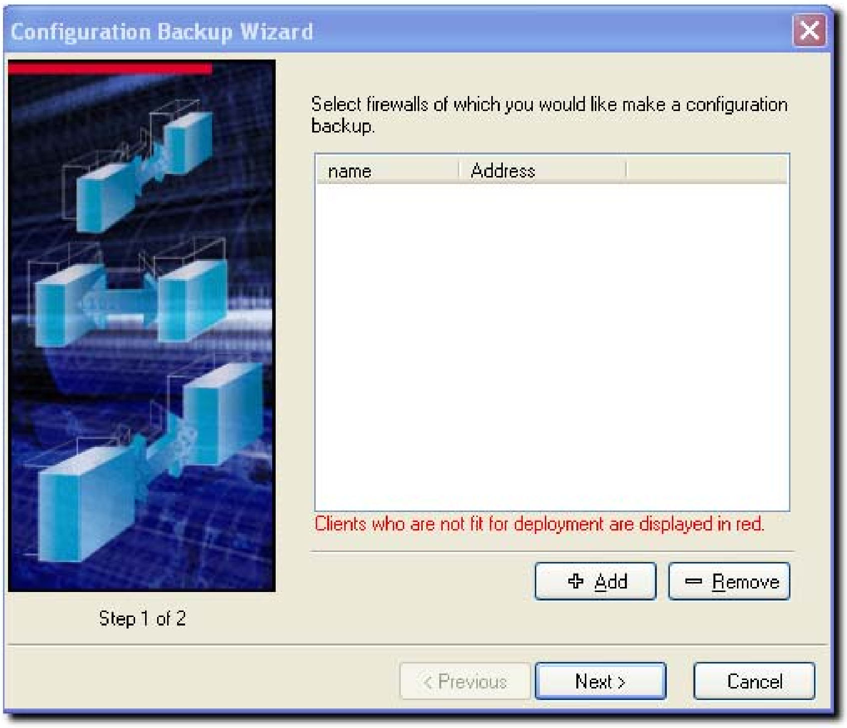
Firewall list:

Bp	Validate	Name	Address	Current status	Current version	Description	Work progress	Result	Msg

Figure 503: Configuration backup

Select **Wizard** at the top of the window to back up the configuration of an appliance, or of several appliances. Backing up the appliance configuration involves two steps.

Step 1



Select firewalls of which you would like make a configuration backup.

name	Address

Clients who are not fit for deployment are displayed in red.

Figure 504: Backup wizard - Step 1

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

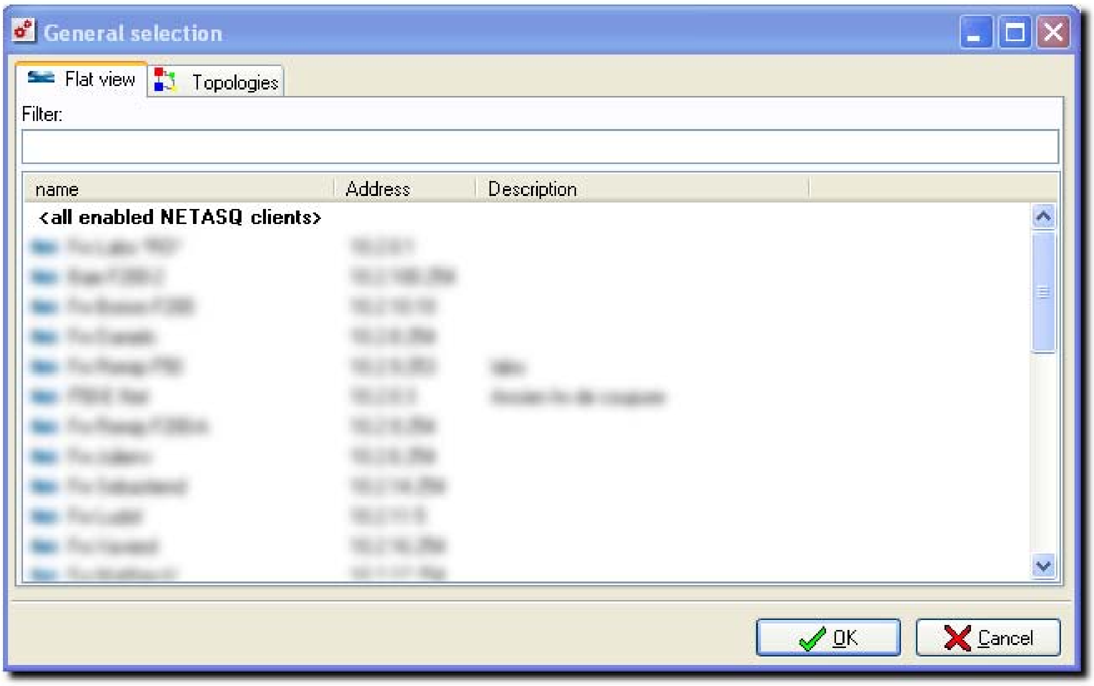
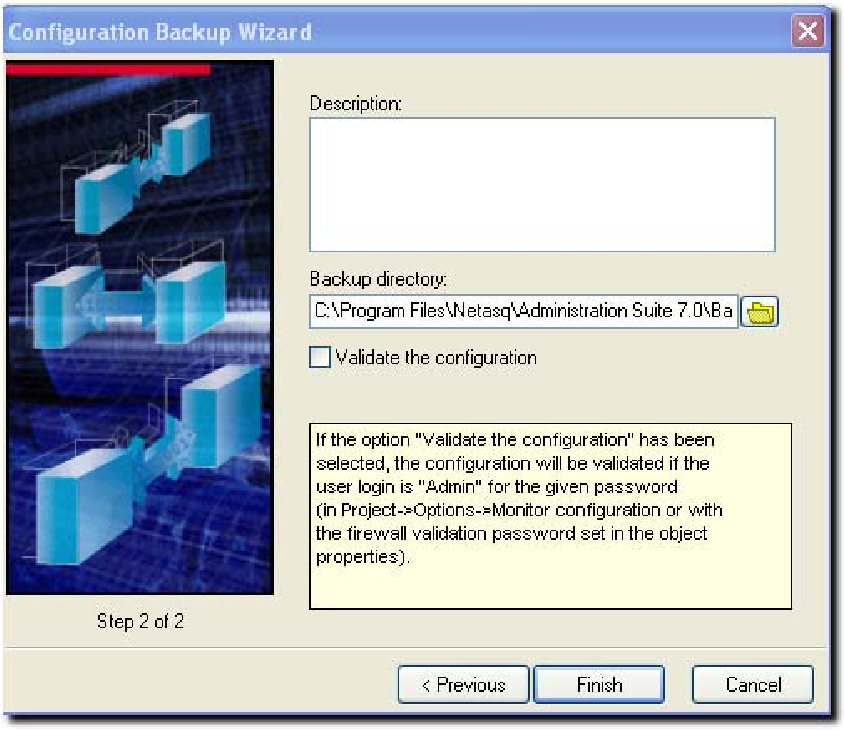


Figure 505: General selection – Flat view

Select the firewall(s) to add then click on **Next** to continue.

Step 2



Description:

Backup directory: C:\Program Files\Netasq\Administration Suite 7.0\Ba

□ Validate the configuration

If the option "Validate the configuration" has been selected, the configuration will be validated if the user login is "Admin" for the given password (in Project->Options->Monitor configuration or with the firewall validation password set in the object properties).

Figure 506: Backup wizard - Step 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. The parameters that have been defined can be modified in this window.

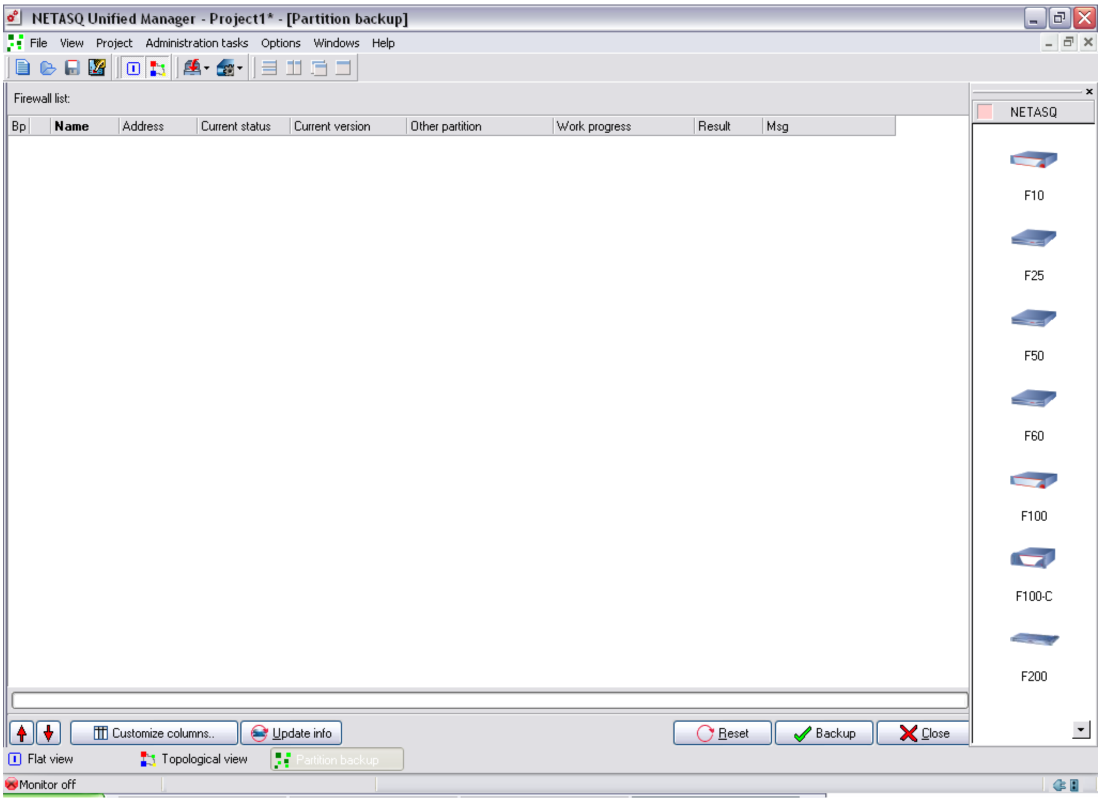


Figure 507: Partition backup

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).

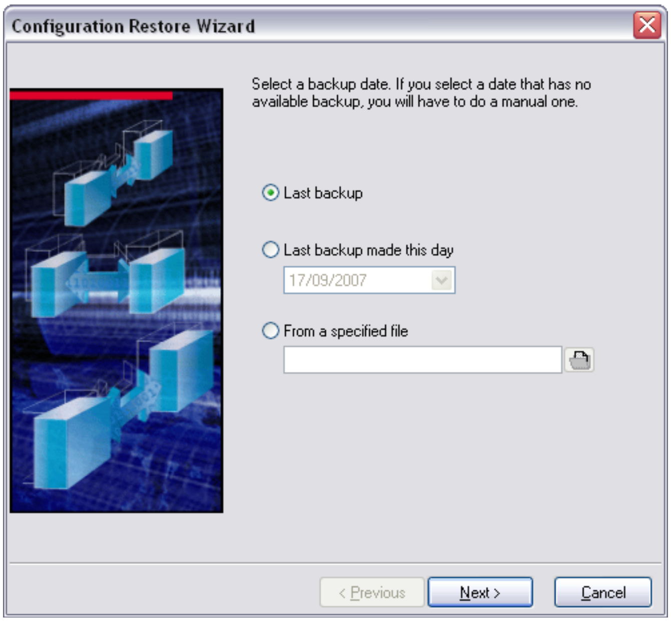
Backing up configurations

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.

Restauring 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



Configuration Restore Wizard

Select a backup date. If you select a date that has no available backup, you will have to do a manual one.

● Last backup

○ Last backup made this day

17/09/2007

○ From a specified file

Figure 508: Restoration wizard

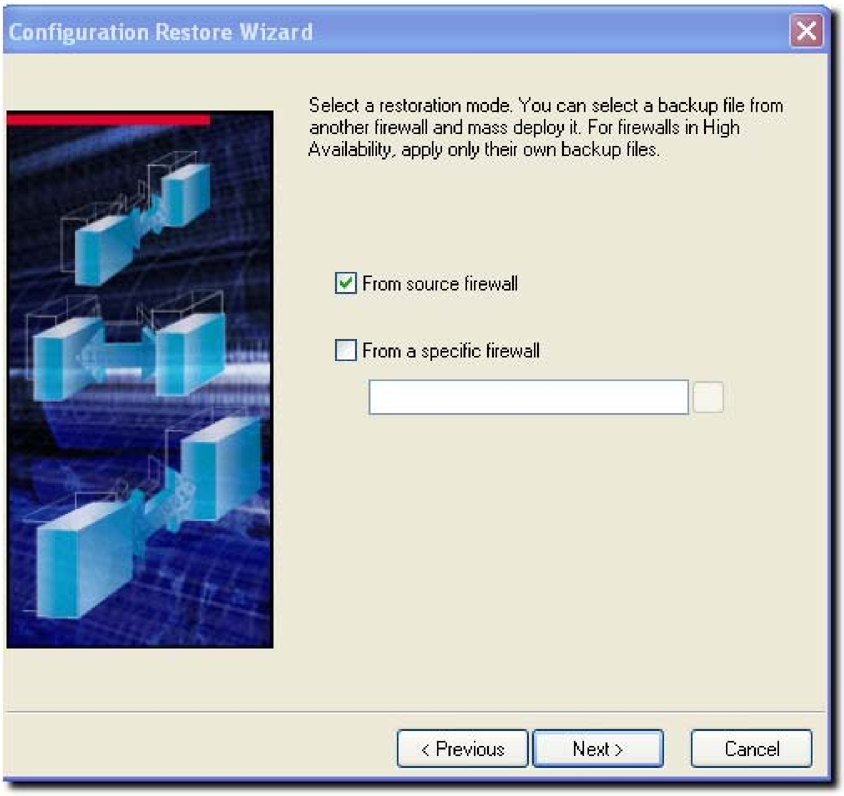
Steps 1 and 2 consist of defining the backup to be used for the restoration by defining the backup date and source.

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).

2 Step 2



Configuration Restore Wizard

Select a restoration mode. You can select a backup file from another firewall and mass deploy it. For firewalls in High Availability, apply only their own backup files.

☑ From source firewall

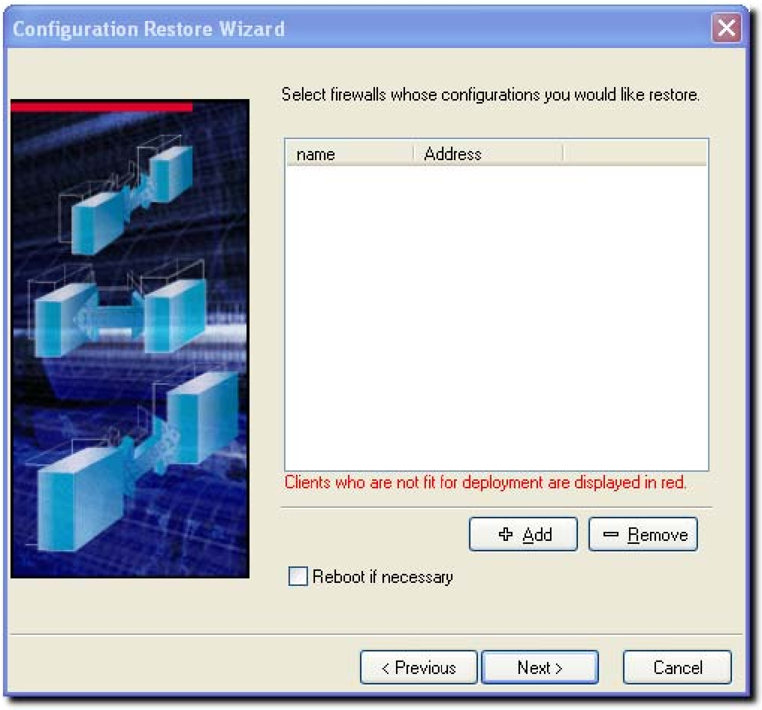
□ From a specific firewall

Figure 509: Restoration wizard

From **source Firewall**: This option is for specifying a backup located in the configuration backup directory craetred 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.

3 Step 3



Configuration Restore Wizard

Select firewalls whose configurations you would like restore.

name	Address

Clients who are not fit for deployment are displayed in red.

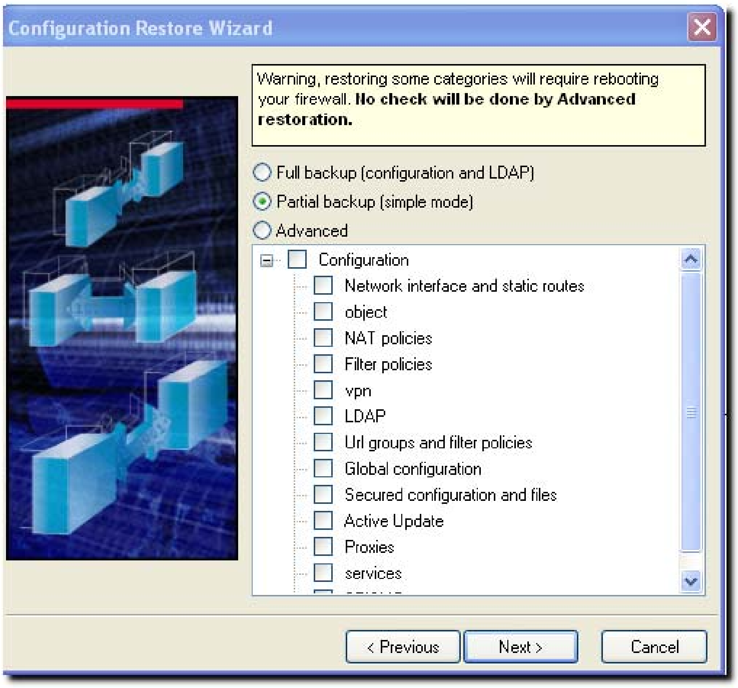
□ Reboot if necessary

Figure 510: 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.

4 Step 4



Configuration Restore Wizard

Warning, restoring some categories will require rebooting your firewall. **No check will be done by Advanced restoration.**

○ Full backup (configuration and LDAP)
● Partial backup (simple mode)
○ Advanced

- □ Configuration
  - □ Network interface and static routes
  - □ object
  - □ NAT policies
  - □ Filter policies
  - □ vpn
  - □ LDAP
  - □ Url groups and filter policies
  - □ Global configuration
  - □ Secured configuration and files
  - □ Active Update
  - □ Proxies
  - □ services

Figure 511: Restoration wizard – Simple mode

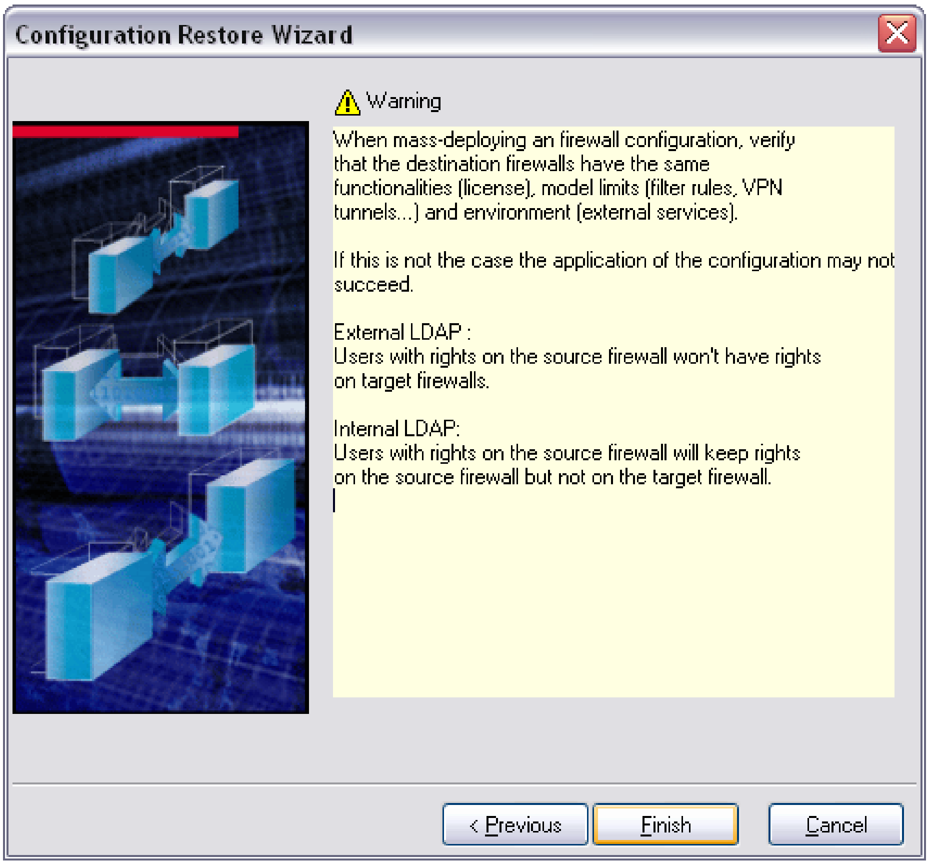
In your previous selections, if you had selection either “From the original firewall” or “From a specific firewall”, the restoration wizard will allow you to select three types of restoration:

- 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.
- Certificats and pre-shared keys: certificats 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 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.

5 **Step 5**



⚠ Warning

When mass-deploying an firewall configuration, verify that the destination firewalls have the same functionalities (license), model limits (filter rules, VPN tunnels...) and environment (external services).

If this is not the case the application of the configuration may not succeed.

External LDAP :
Users with rights on the source firewall won't have rights on target firewalls.

Internal LDAP:
Users with rights on the source firewall will keep rights on the source firewall but not on the target firewall.

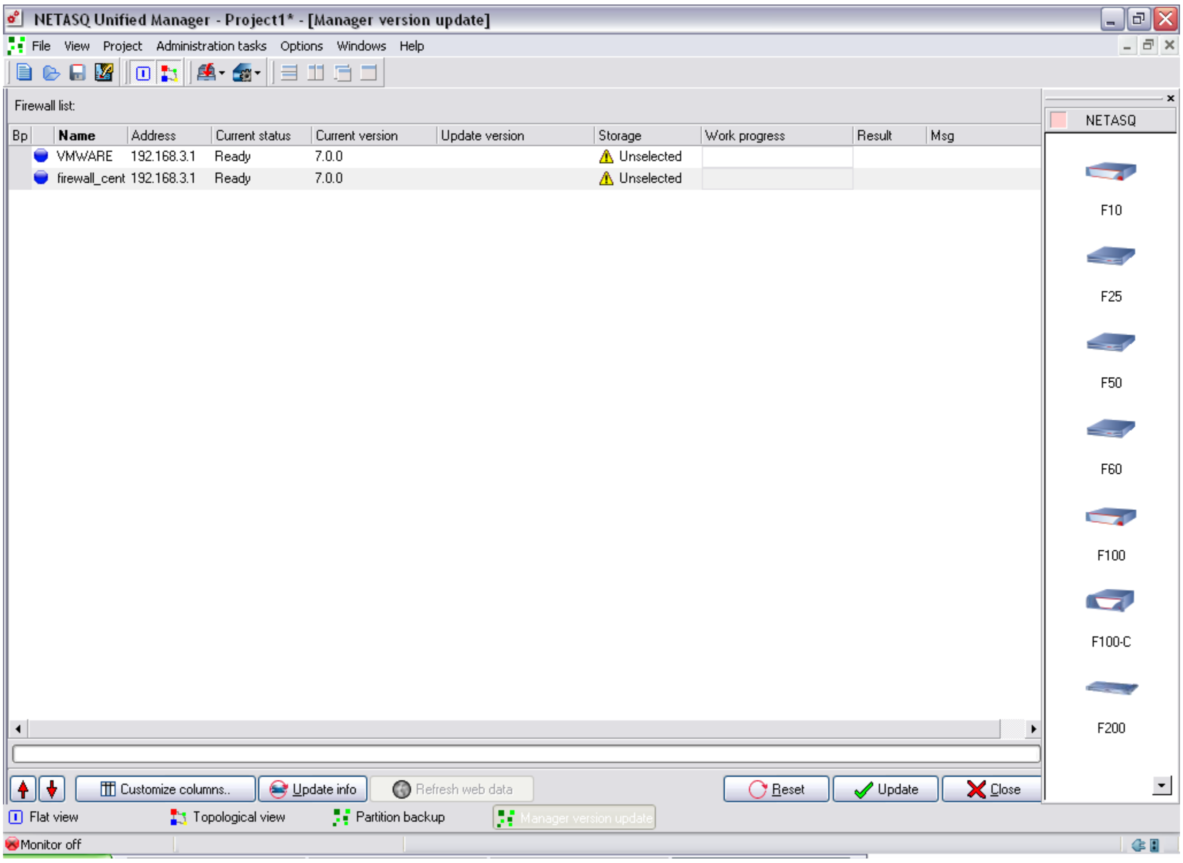
Figure 512: Restoration wizard

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.

20.3.5.3. Updating the firmware

Selecting the `Administration tasks\Update Firmware` menu item opens the following window:



Firewall list:

Bp	Name	Address	Current status	Current version	Update version	Storage	Work progress	Result	Msg
●	VMWARE	192.168.3.1	Ready	7.0.0		⚠ Unselected			
●	firewall_cent	192.168.3.1	Ready	7.0.0		⚠ Unselected			

Figure 513: Updating 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.

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 have to be updated (using the button **Update information in flat view**).

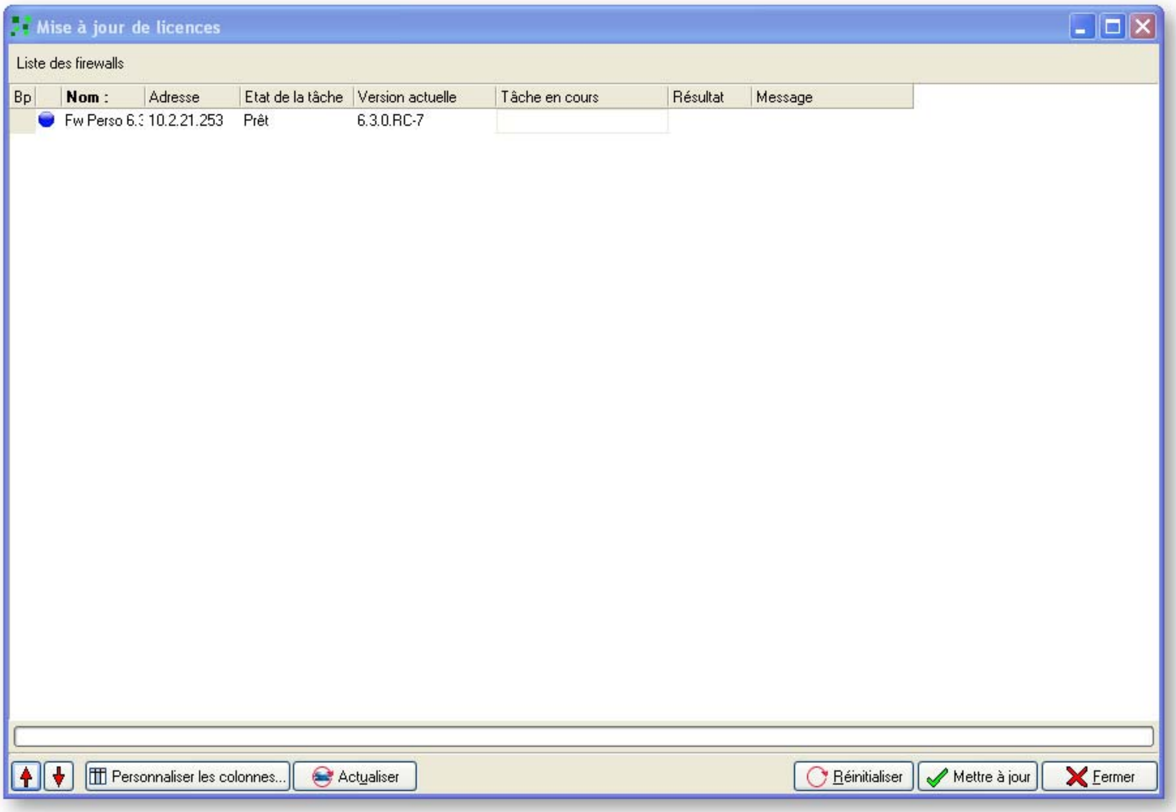
Updating NETASQ UTM appliances

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 (Cf. 20.3.5.5. backing up the partition*)*.

20.3.5.4. Updating the license

➲ When you select the **`Administration tasks\Update the license`** menu item the following window opens:



Mise à jour de licences

Liste des firewalls

Bp	Nom :	Adresse	Etat de la tâche	Version actuelle	Tâche en cours	Résultat	Message
🔵	Fw Perso 6.:	10.2.21.253	Prêt	6.3.0.RC-7			

Figure 514: Updating licenses

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 moade 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:

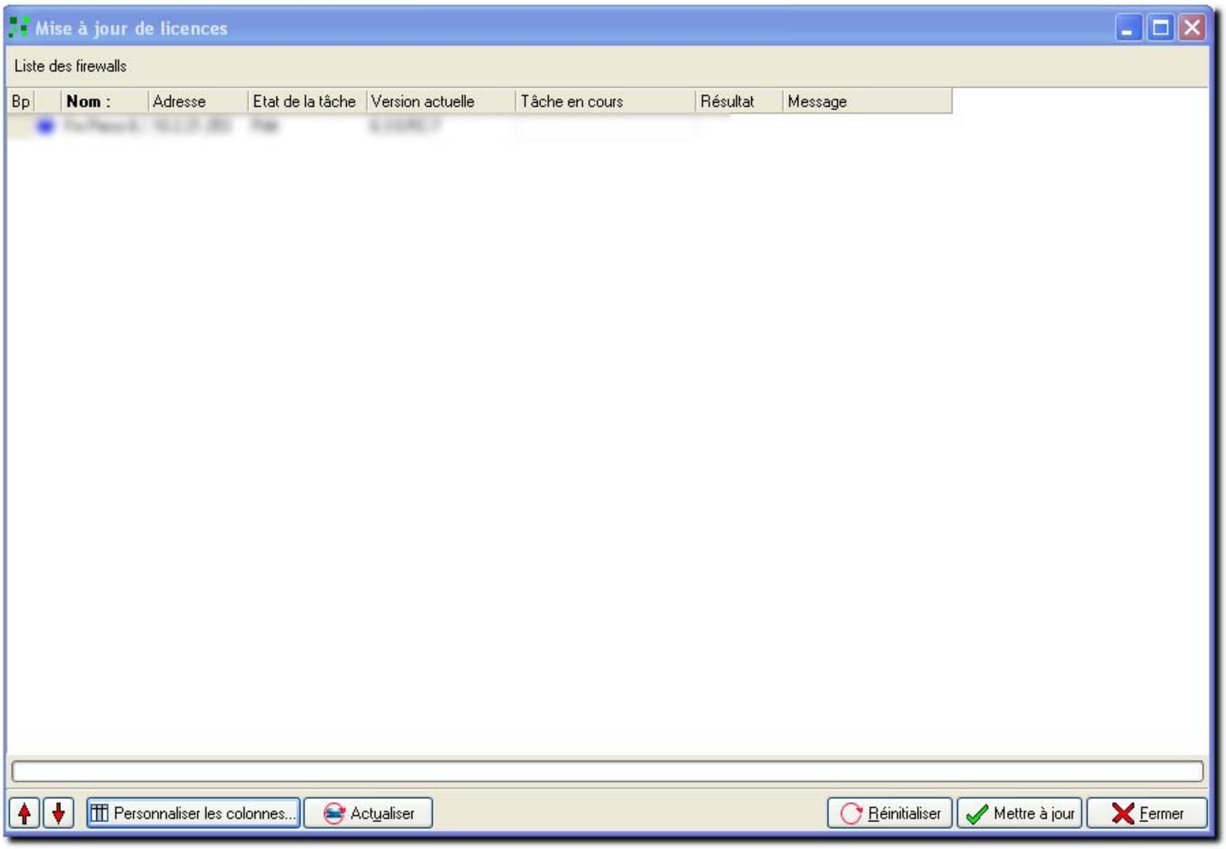
Name	Name chosen for the appliance
Address	IP address of the appliance
Status of the task	Status of the action (waiting, begun, completed, etc.)
Current version	Current version of the firmware of the appliance
License version	Current version of the license.
Task progress	Progress of current task
Result	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.

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).



Bp	Nom :	Adresse	Etat de la tâche	Version actuelle	Tâche en cours	Résultat	Message

Figure 515: Updating licenses

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).

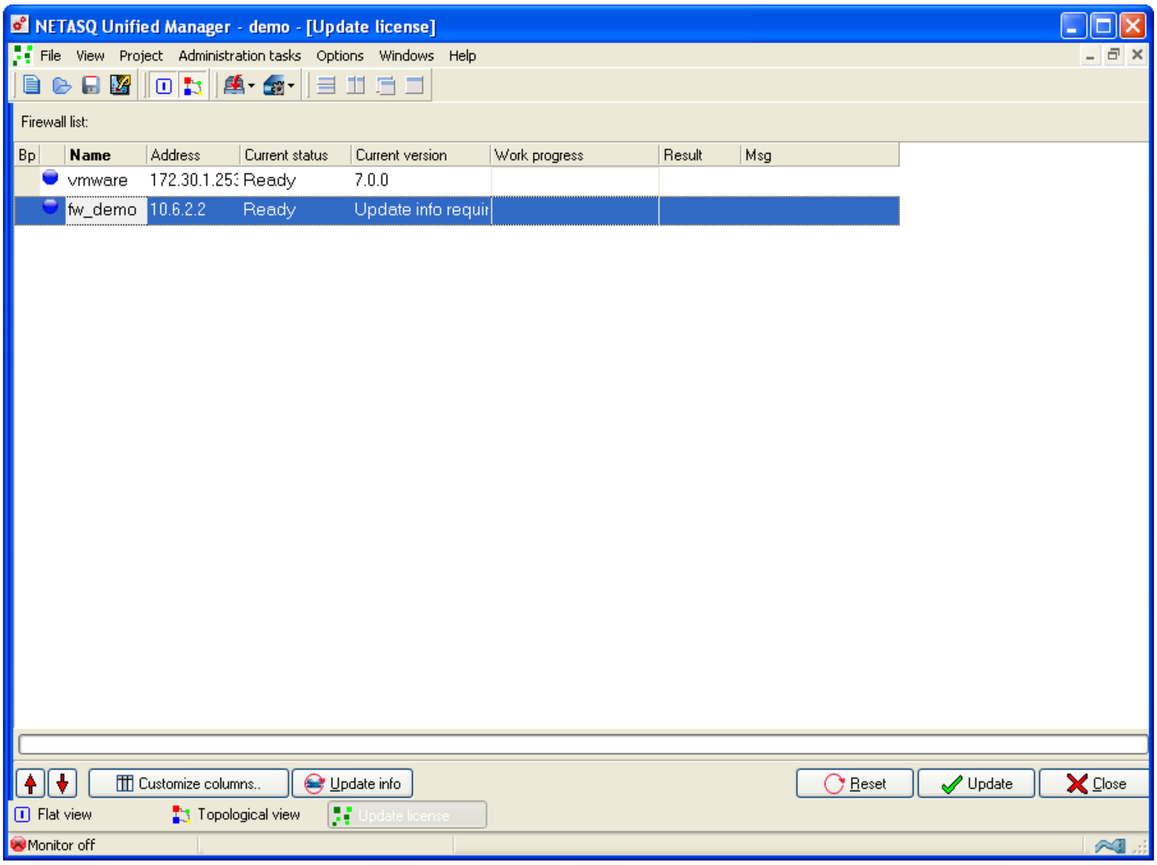
Updating the licenses of the appliances

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.

20.3.5.5. 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.

When you select the **Administration tasks\Partition backup** menu item the following window opens:



Bp	Name	Address	Current status	Current version	Work progress	Result	Msg
🔵	vmware	172.30.1.25:	Ready	7.0.0			
🔵	fw_demo	10.6.2.2	Ready	Update info requir			

Figure 516: Partition backup

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

20.3.6. 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 following window:

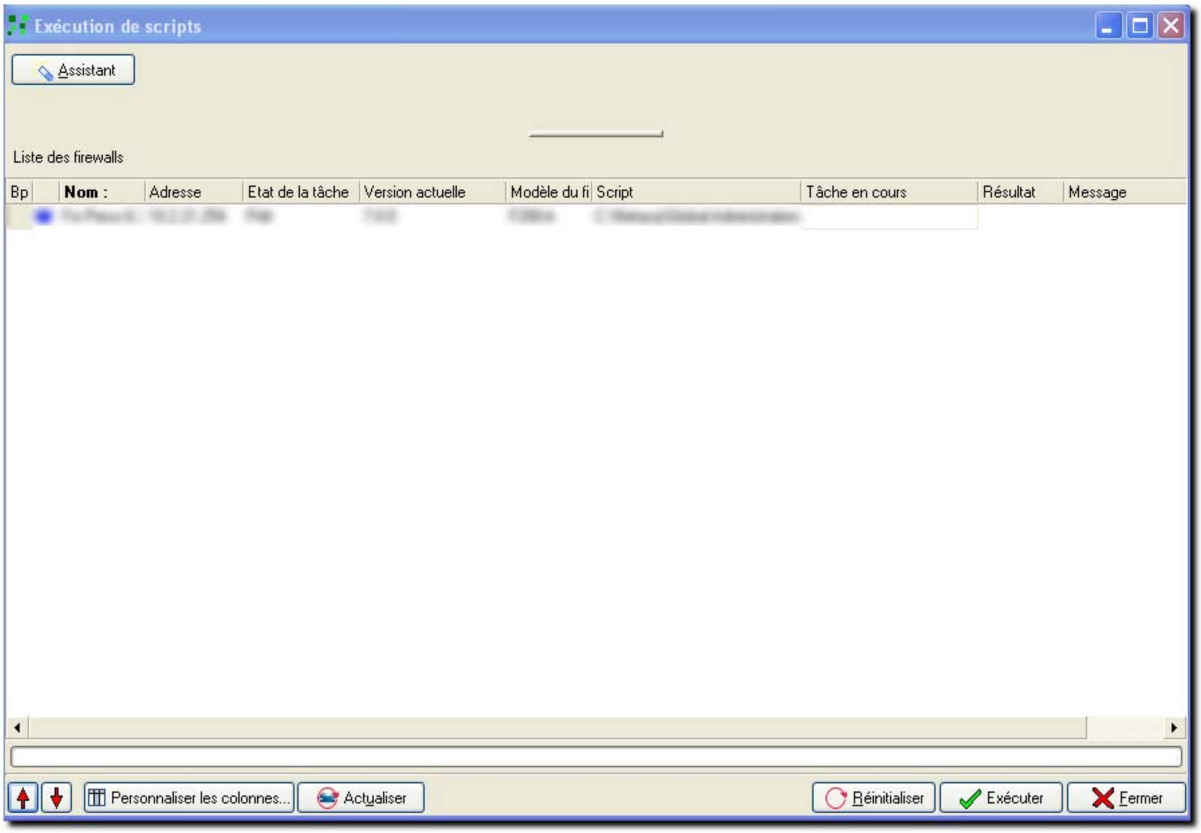
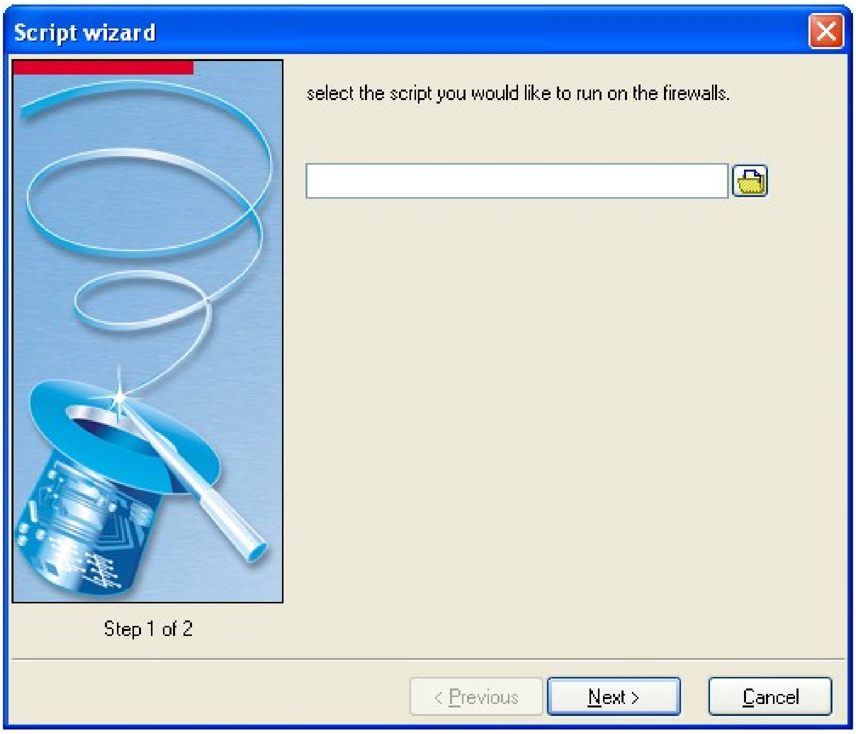


Figure 517: Executing scripts

1 Step 1

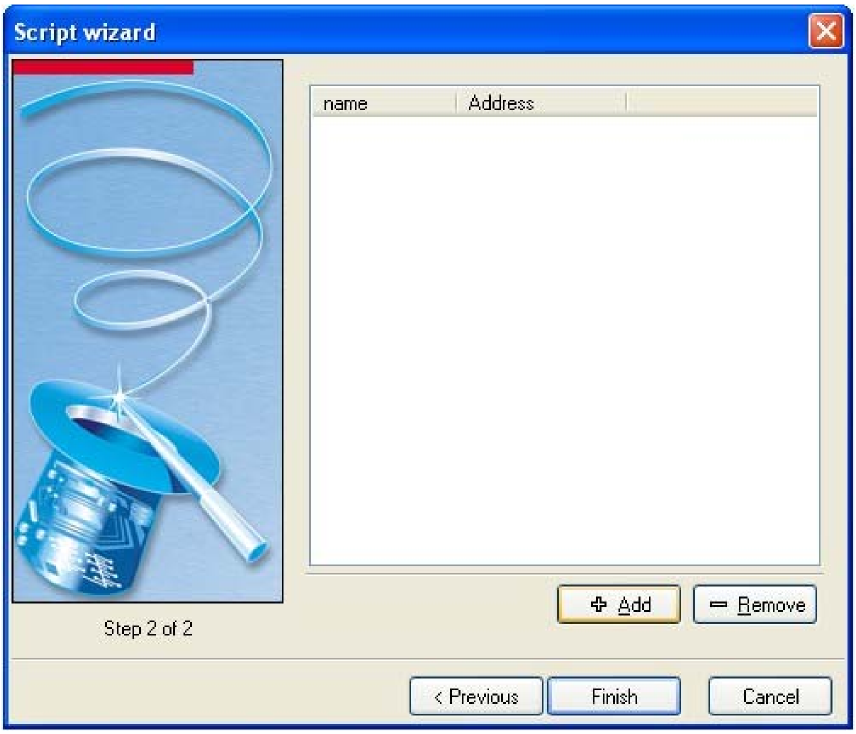

Script wizard

select the script you would like to run on the firewalls.

Figure 518: 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**.

2 Step 2


Script wizard

name	Address

Figure 519: 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:

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.

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 varaiables 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
```

20.3.6.1. 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	Deployment of the ASQ kernel.

prevention	
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 20.3.6.1. Deployment

20.3.7. 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.

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 ❌.

Checking the operational status of appliances

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

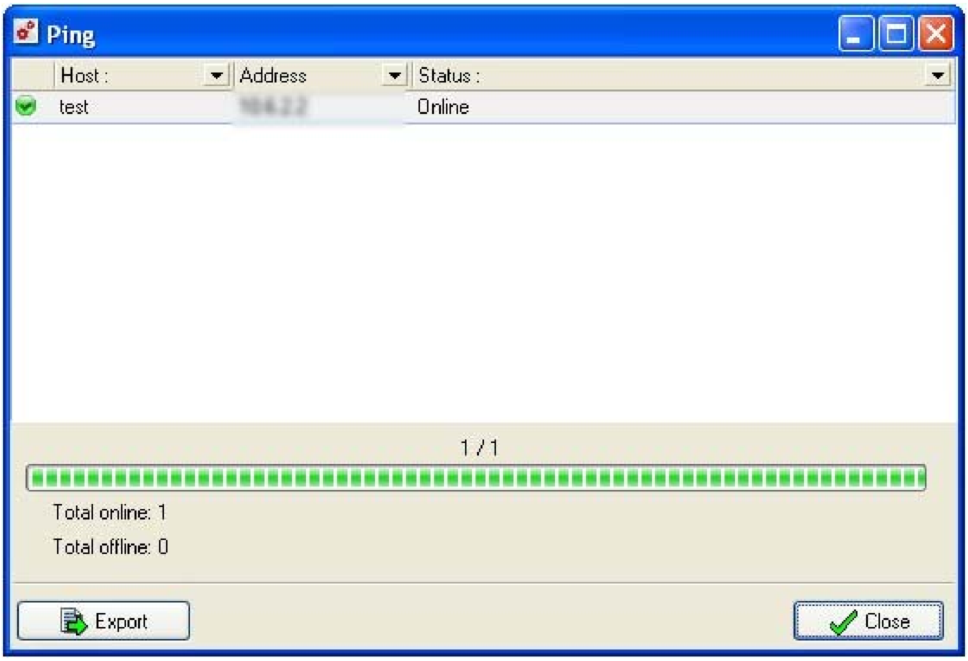
If certain appliances are filtered, the NETASQ Global Administration mode may consider them non-operational even if they may be operating perfectly fine. Likewise, if the equipment does not respond to ICMP commands, it will be considered non-operational. In order to use the NETASQ Global Administration 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.

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):



Host :	Address	Status :
test	[redacted]	Online

1 / 1

Total online: 1

Total offline: 0

Figure 520: Ping

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.

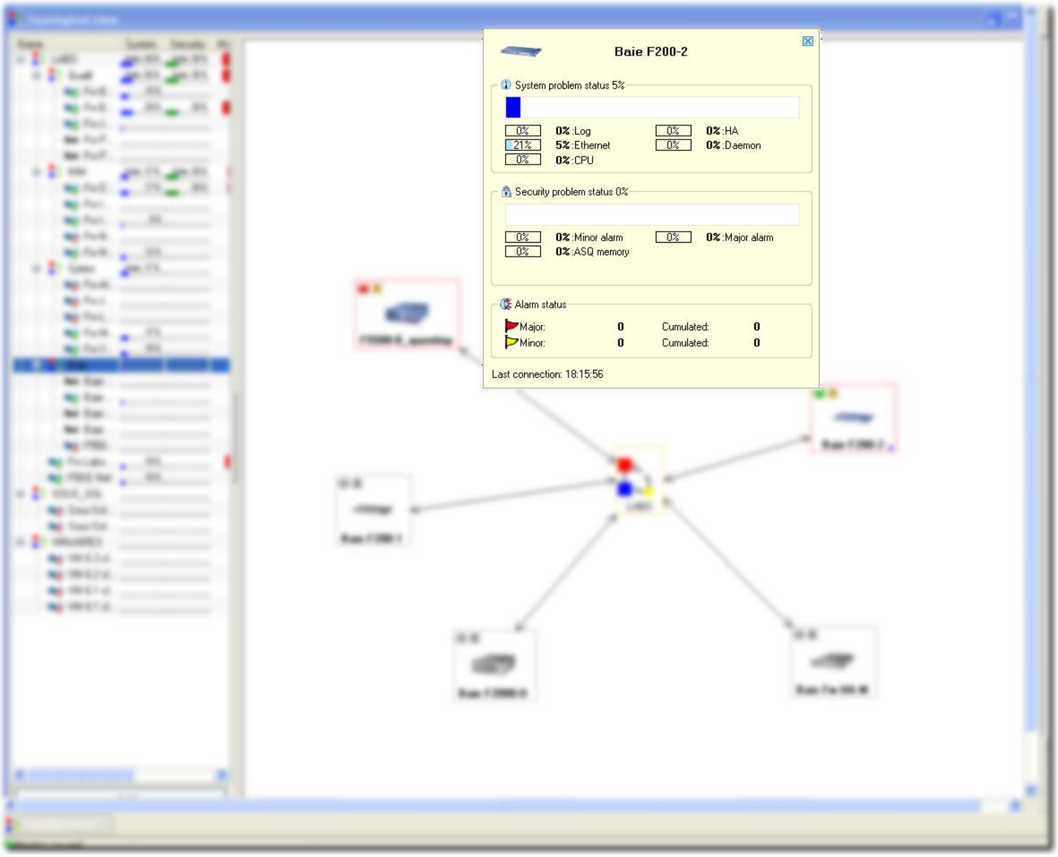
WARNING

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.

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:



Baie F200-2

System problem status 5%

0%	**0%** :Log	0%	**0%** :HA
21%	**5%** :Ethernet	0%	**0%** :Daemon
0%	**0%** :CPU		

Security problem status 0%

0%	**0%** :Minor alarm	0%	**0%** :Major alarm
0%	**0%** :ASQ memory		

Alarm status

Major:	**0**	Cumulated:	**0**
Minor:	**0**	Cumulated:	**0**

Last connection: 18:15:56

Figure 521: 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.

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

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.

20.3.8. 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.

Operating principle

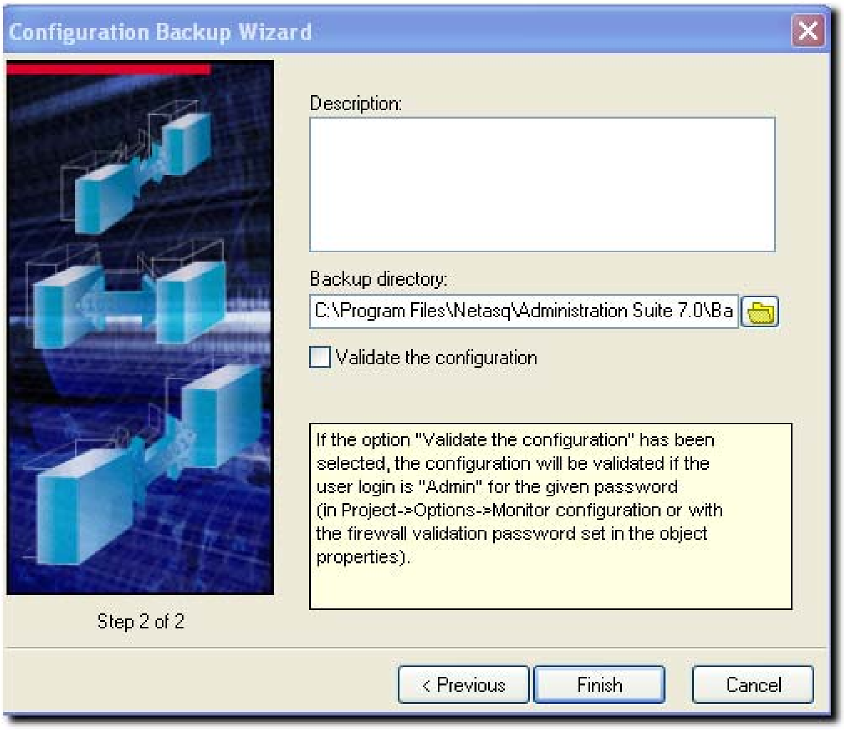
The Global Administration mode will establish a model for comparing configurations based on a "validated" configuration backup. This means that the configuration is constantly compared with the configuration currently running on the monitored appliance. As soon as a difference is detected between both 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.

Setting up configuration monitoring

1 **Step 1: Activating configuration monitoring**
Enable configuration monitoring by selecting the option **Enable configuration monitoring**. (Cf. 20.3.8. Configuration monitoring for more information on the available parameters in this menu).

2 **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. 20.3.8. Configuration monitoring)

3 **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.



Configuration Backup Wizard

Description:

Backup directory:

C:\Program Files\Netasq\Administration Suite 7.0\Ba

□ Validate the configuration

If the option "Validate the configuration" has been selected, the configuration will be validated if the user login is "Admin" for the given password (in Project->Options->Monitor configuration or with the firewall validation password set in the object properties).

Step 2 of 2

Figure 522: Backup wizard - Step 2

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.

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.

20.3.9. 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.

20.3.10. Direct configuration

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

20.3.11. Deploying configurations

20.3.11.1. 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.

Contextual menu

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

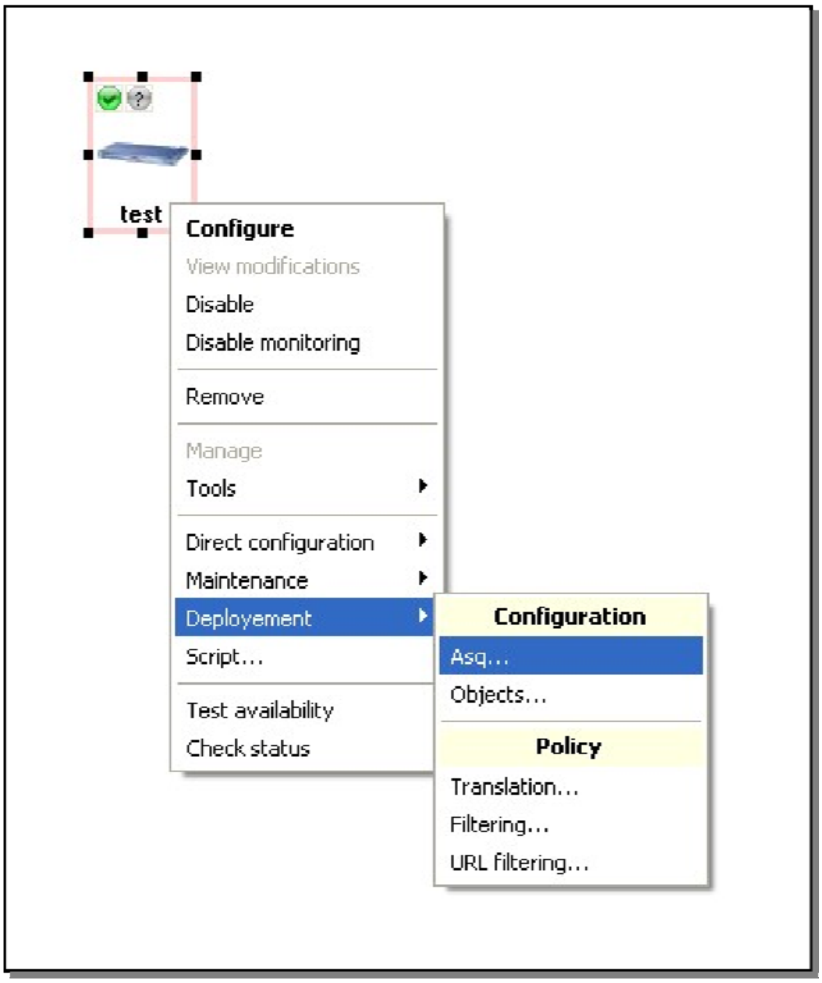


Figure 523: Contextual menu

20.3.11.2. 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.

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.

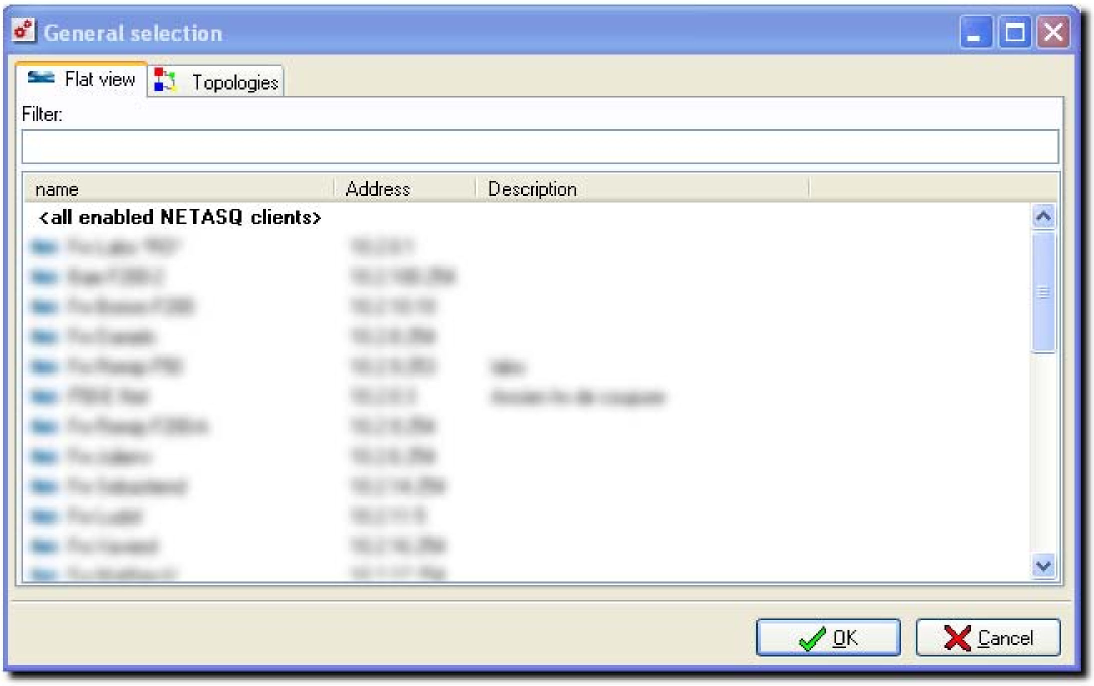


Figure 524: General selection – Flat view

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.

"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**.

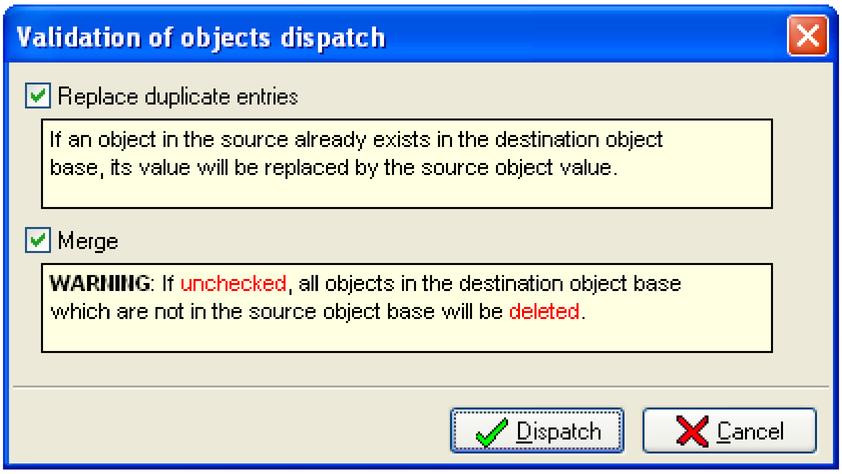
WARNING
The selected Firewall appears in red on the list of Firewalls if its version is not suitable for the source Firewall (the configuration of a firewall cannot be deployed en version 7 to a firewall in version 6 and vice-versa).

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, and the following window will appear:


Validation of objects dispatch

☑ Replace duplicate entries

If an object in the source already exists in the destination object base, its value will be replaced by the source object value.

☑ Merge

WARNING: If unchecked, all objects in the destination object base which are not in the source object base will be deleted.

Figure 525: Validating the dispatch of objects

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

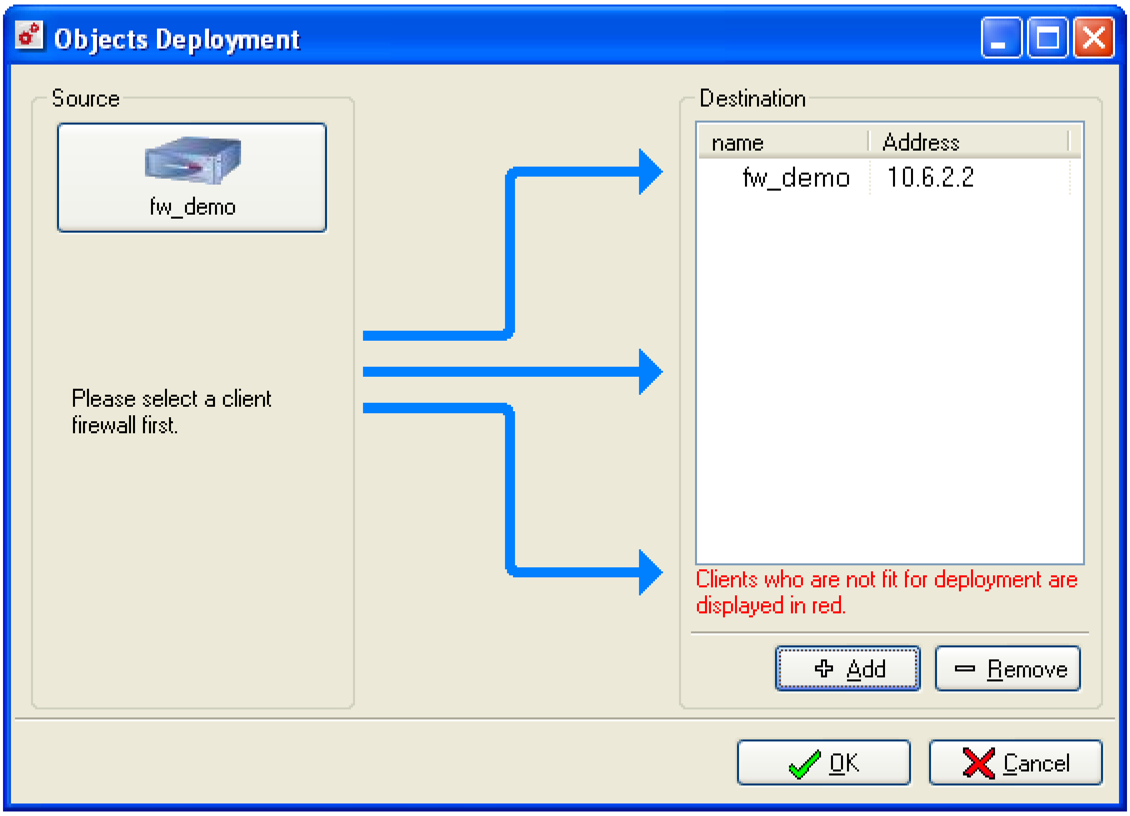
Replace duplicate entries	When this option is checked, the value of the object in the source database will replace the value of the object in the destination database if an object in the destination object database bears the same name as an object in the source object database.
Merge	WARNING If unchecked, 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.

20.3.11.3. Particularities of deployment windows

Objects categories

Categories are used in the deployment of objects.

➲ Select "Objects" if you wish to deploy an object database. The following screen will appear:



Please select a client firewall first.

name	Address
fw_demo	10.6.2.2

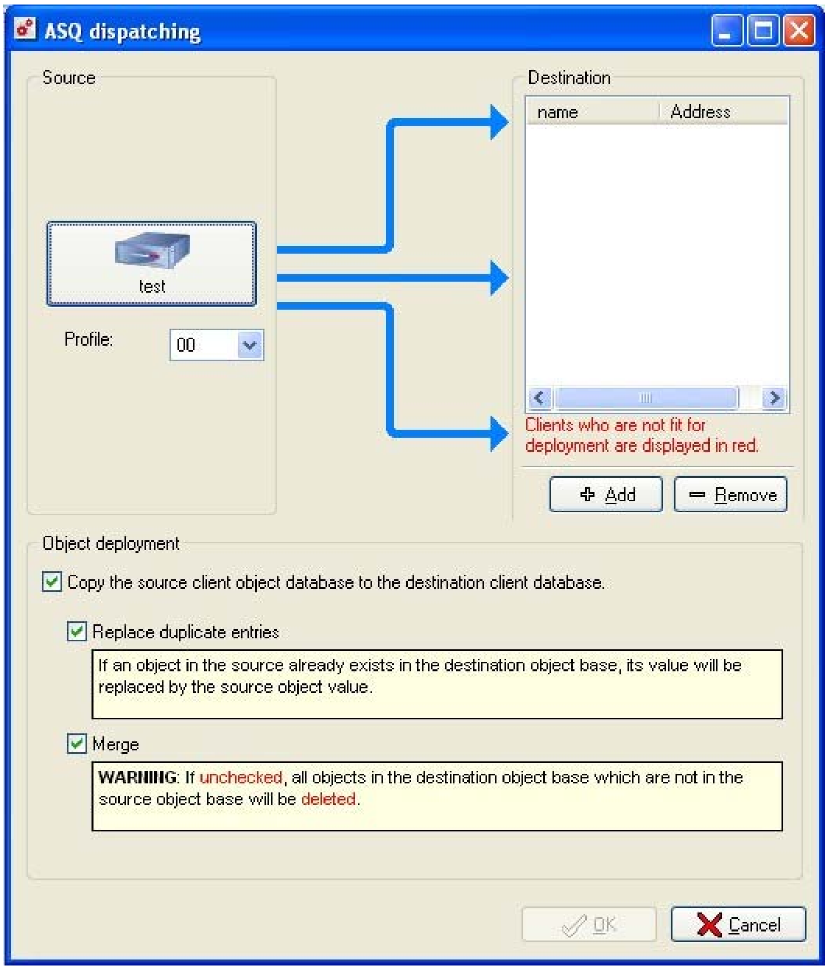
Clients who are not fit for deployment are displayed in red.

Figure 526: Deploying objects

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.**

Choosing the intrusion prevention profile

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



Profile: 00

Clients who are not fit for deployment are displayed in red.

Object deployment

☑ Copy the source client object database to the destination client database.

☑ Replace duplicate entries

If an object in the source already exists in the destination object base, its value will be replaced by the source object value.

☑ Merge

WARNING: If unchecked, all objects in the destination object base which are not in the source object base will be deleted.

Figure 527: Deploying the intrusion prevention configuration

➲ Select "Intrusion prevention " if you intend to deply 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.

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.

20.3.11.4. Deploying the object database

Copy the source object database to the destination	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).

clients	
Replace duplcate 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.

20.3.11.5. 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.

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 fo 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.

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: Session and user privileges

Session privileges:

- Base
- Other
- Log
- Filter
- VPN
- URL
- PKI
- Object
- User
- Admin
- Network
- Route
- Maintenance
- ASQ
- Globalobject
- Globalfilter
- Globalother
- SEISMO
- HA

User privileges:

- Modify
- Base
- Other
- Log
- Filter
- VPN
- URL
- PKI
- Object
- User
- Admin
- Network
- Route
- Maintenance
- ASQ
- Globalobject
- Globalfilter
- Globalother
- Seismo
- HA
- Network

RO for "Read Only"
W for "Write" – modification privileges
M for "Mon_Write" – modification privileges on Monitor only

Appendix B: 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	Protocol	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 the 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	Resource 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 Printing 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 endpoint 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
ldap	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	
ldaps	636	UDP	LDAP over TLS/SSL
Kerberos-adm	749	TCP / UDP	Kerberos administration
Kerberos-iv	750	UDP	Kerberos version IV

Appendix C: 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 D: ICMP Codes

Type	Code	Description	Request	Error
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 E: 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.

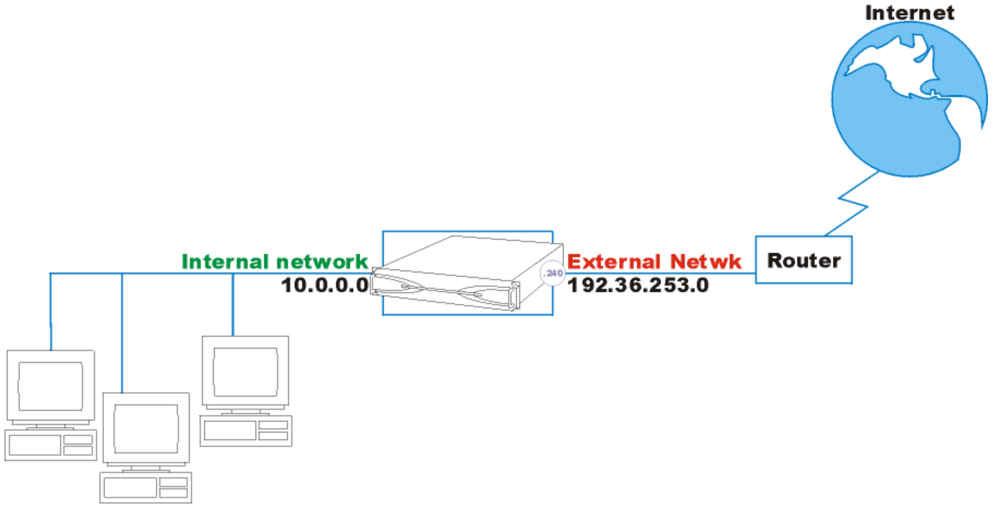


Figure 528: Unidirectional translation

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	

Example 2: Bi-directional translation

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

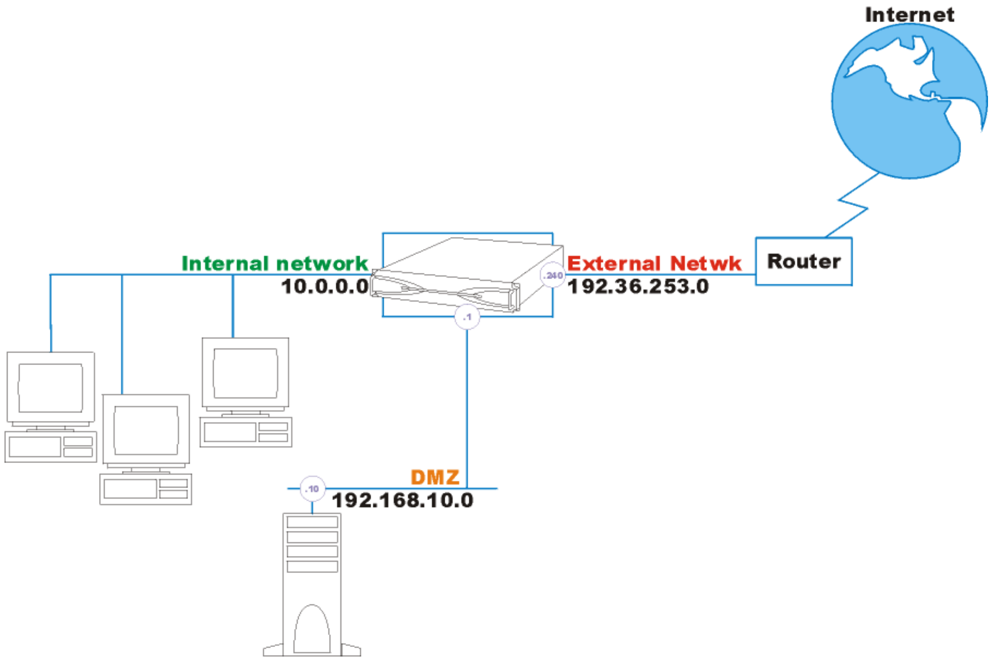


Figure 529: Bi-directional translation

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.

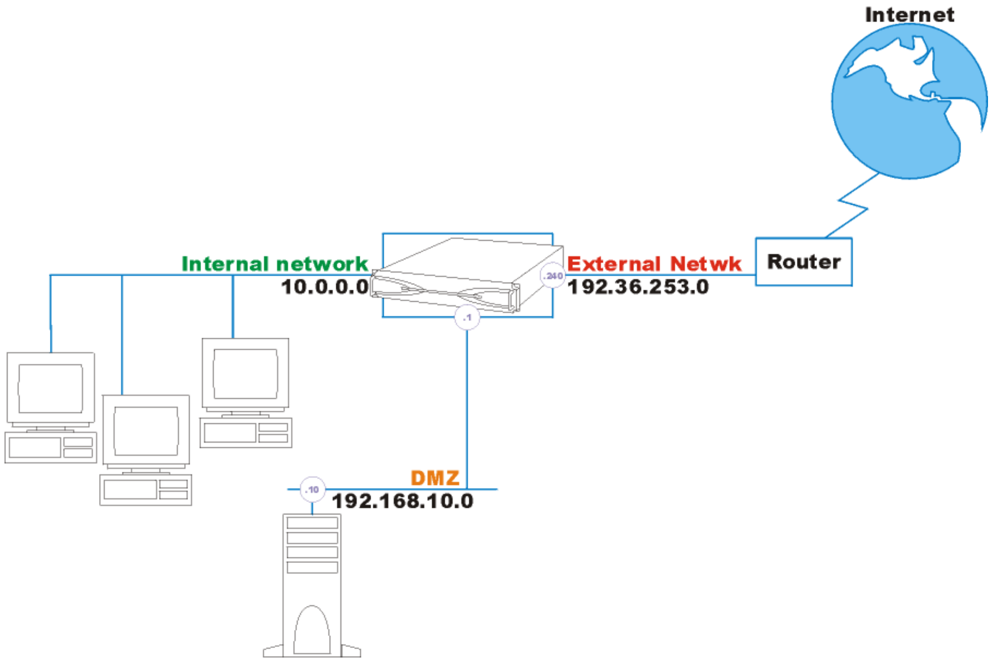


Figure 530: Web server in DMZ

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_dial up	

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.

Example

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_Serve r	http
On	out	redirect	none	<Any>	Firewall_out	smtp	Mail_Server	smtp

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

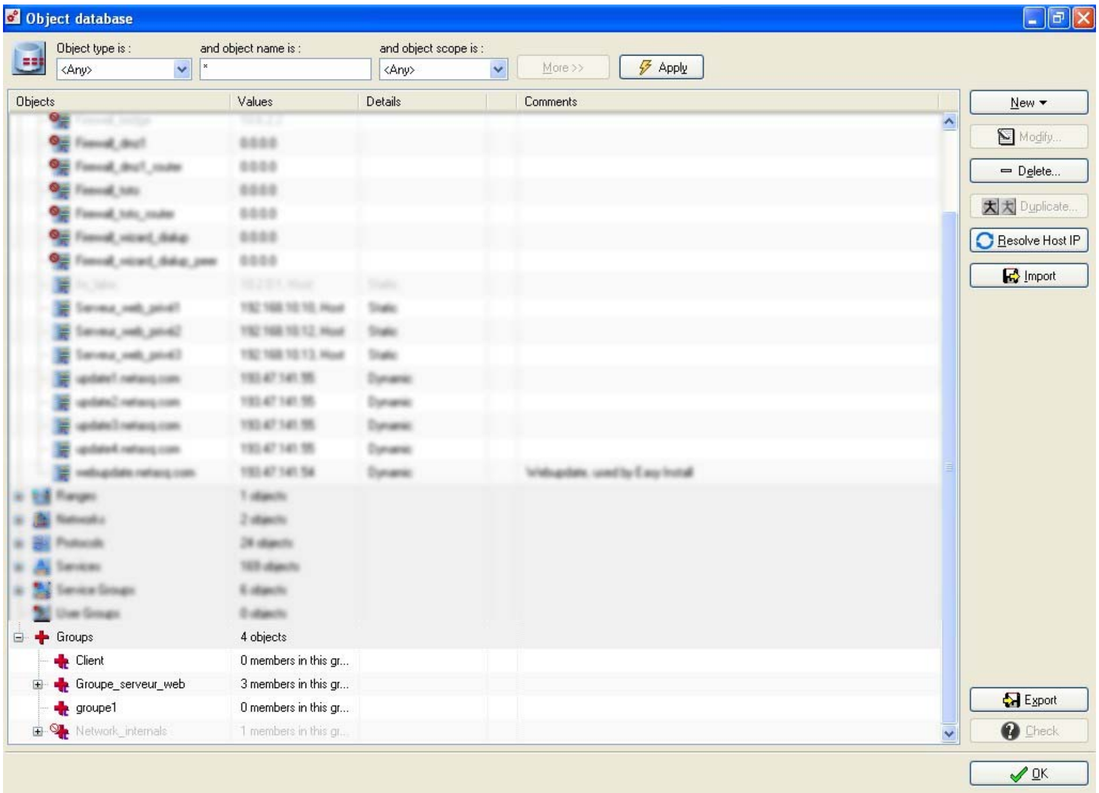
Example 6: Load balancing

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.



Objects	Values	Details	Comments
Groups	4 objects		
Client	0 members in this gr...		
Groupe_serveur_web	3 members in this gr...		
groupe1	0 members in this gr...		
Network_internals	1 members in this gr...		

Figure 531: 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 F: Examples of filter rules

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

- DNS access
- ICMP access

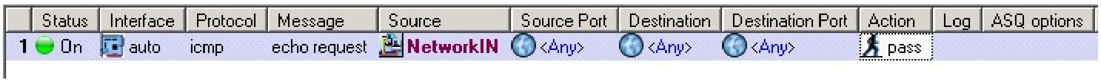
- Telnet access
- FTP access
- Access to an internal web server from the outside and from the internal network
- Internet access with or without URL filtering
- Client workstations’ access to the mail server
- Configuring a mail server
- Regulating bandwidth
- Verifying filter rules
- Authentication

WARNING
Some configurations could be unnecessary if you activate the specific implicit rules. (Cf.CHAPTER 4: 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.



	Status	Interface	Protocol	Message	Source	Source Port	Destination	Destination Port	Action	Log	ASQ options
1	On	auto	icmp	echo request	NetworkIN	<Any>	<Any>	<Any>	pass		

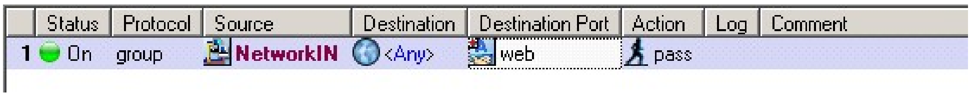
Figure 532: ICMP access

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:



	Status	Protocol	Source	Destination	Destination Port	Action	Log	Comment
1	On	group	NetworkIN	<Any>	web	pass		

Figure 533: Internet access

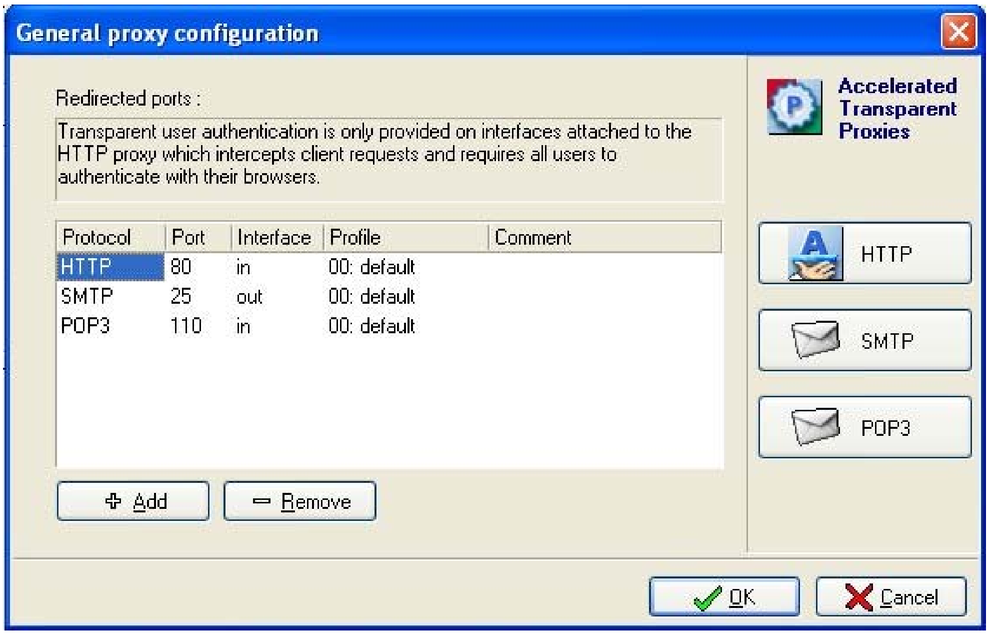
If you use URL filtering, you will indirectly pass through a web proxy located on the Firewall.

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:



Redirected ports :

Transparent user authentication is only provided on interfaces attached to the HTTP proxy which intercepts client requests and requires all users to authenticate with their browsers.

Protocol	Port	Interface	Profile	Comment
HTTP	80	in	00: default	
SMTP	25	out	00: default	
POP3	110	in	00: default	

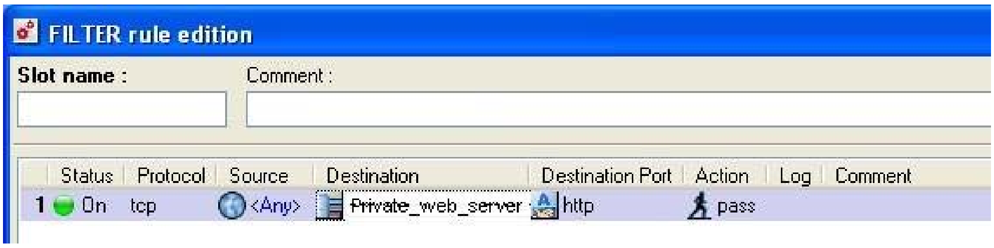
Figure 534: General proxy configuration

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":



Slot name : Comment :

	Status	Protocol	Source	Destination	Destination Port	Action	Log	Comment
1	On	tcp	<Any>	Private_web_server	http	pass		

Figure 535: Editing filter rules

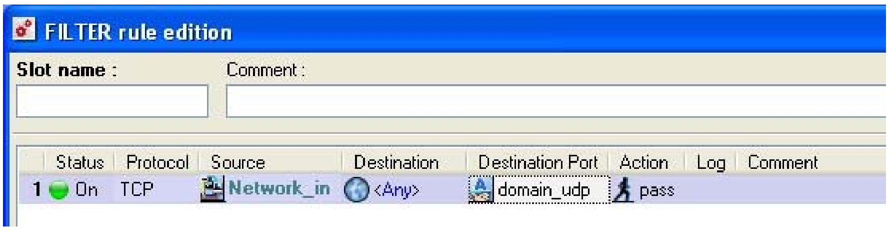
WARNING

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.



FILTER rule edition

Slot name : Comment :

	Status	Protocol	Source	Destination	Destination Port	Action	Log	Comment
1	On	TCP	Network_in	<Any>	domain_udp	pass		

Figure 536: Editing filter rules

FTP access

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

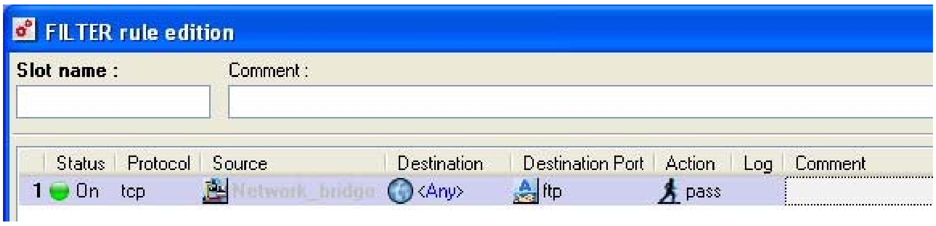
- A command connection to send and receive FTP commands
- A data connection for the transit of traffic.

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:



FILTER rule edition

Slot name : Comment :

	Status	Protocol	Source	Destination	Destination Port	Action	Log	Comment
1	On	tcp	Network_bridge	<Any>	ftp	pass		

Figure 537: 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).

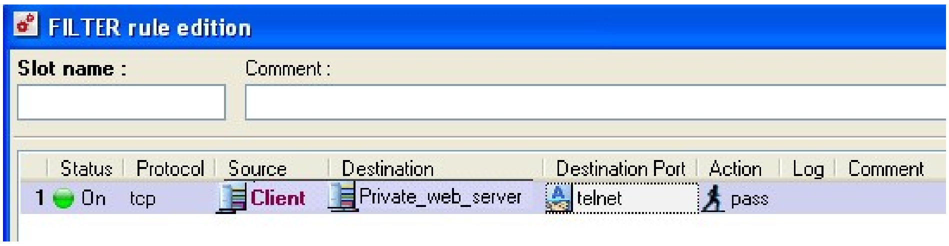
You can then create a service group called "Mail" in which you will place the POP3 and SMTP services. This will avoid the need to place two lines with the same properties in the filter rules.

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.



Slot name :

Comment :

	Status	Protocol	Source	Destination	Destination Port	Action	Log	Comment
1	On	tcp	Client	Private_web_server	telnet	pass		

Figure 538: Editing filter rules

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

IPSec connections

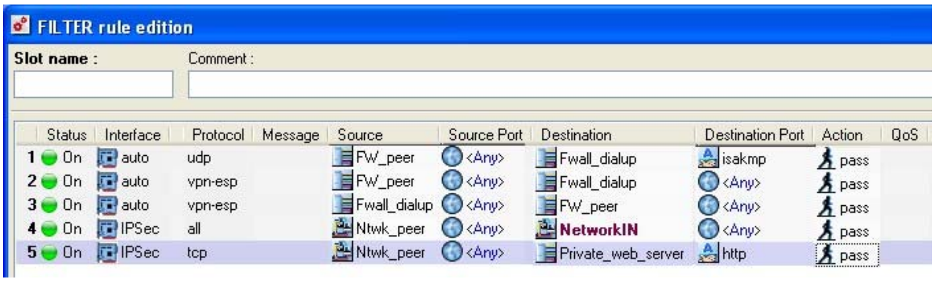
After setting the IPSEC VPN parameters on the Firewall, filter rules have to be implemented to authorize these protocols on the Firewall (except if implicit rules are activated for this traffic type).

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”.



FILTER rule edition

Slot name :

Comment :

	Status	Interface	Protocol	Message	Source	Source Port	Destination	Destination Port	Action	QoS
1	On	auto	udp		FW_peer	<Any>	Fwall_dialup	isakmp	pass	
2	On	auto	vpn-esp		FW_peer	<Any>	Fwall_dialup	<Any>	pass	
3	On	auto	vpn-esp		Fwall_dialup	<Any>	FW_peer	<Any>	pass	
4	On	IPSec	all		Ntwk_peer	<Any>	NetworkIN	<Any>	pass	
5	On	IPSec	tcp		Ntwk_peer	<Any>	Private_web_server	http	pass	

Figure 539: 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.

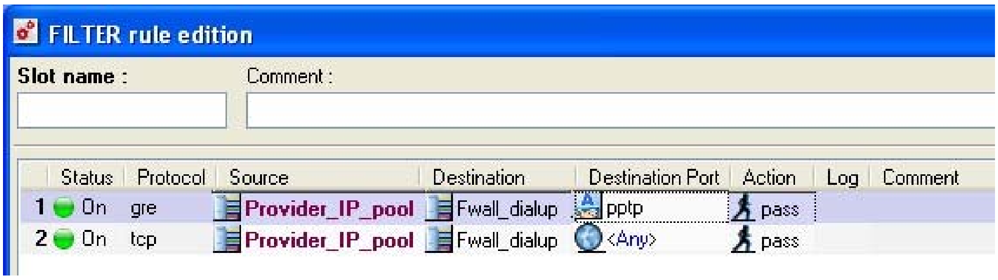
Example

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:



FILTER rule edition

Slot name :

Comment :

	Status	Protocol	Source	Destination	Destination Port	Action	Log	Comment
1	On	gre	Provider_IP_pool	Fwall_dialup	pptp	pass		
2	On	tcp	Provider_IP_pool	Fwall_dialup	<Any>	pass		

Figure 540: Editing filter rules

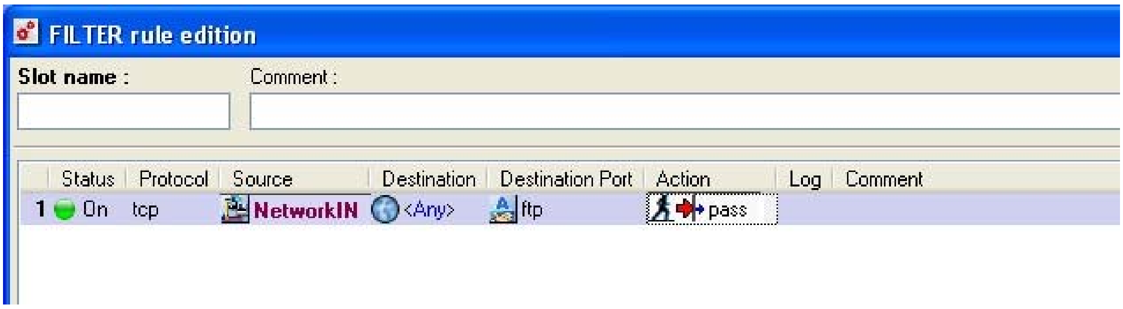
Bandwidth control

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.



FILTER rule edition

Slot name :

Comment :

	Status	Protocol	Source	Destination	Destination Port	Action	Log	Comment
1	On	tcp	NetworkIN	<Any>	ftp	pass		

Figure 541: 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 endof 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.

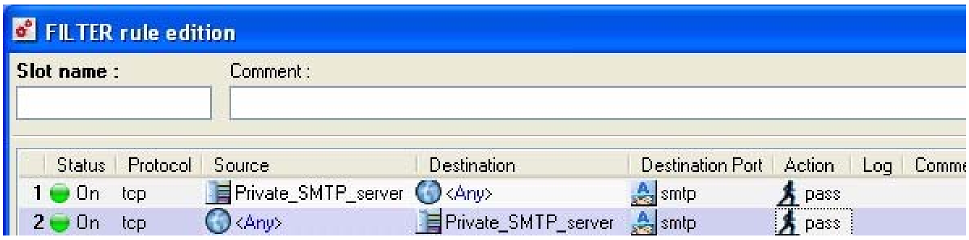
Access to the mail server

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:



FILTER rule edition

Slot name :

Comment :

	Status	Protocol	Source	Destination	Destination Port	Action	Log	Comme
1	● On	tcp	Private_SMTP_server	<Any>	smtp	pass		
2	● On	tcp	<Any>	Private_SMTP_server	smtp	pass		

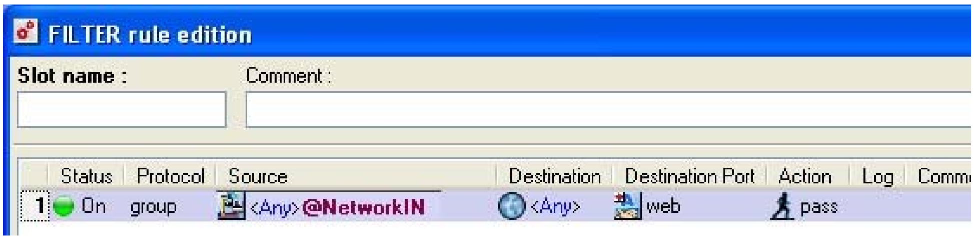
Figure 542: Editing filter rules

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:



FILTER rule edition

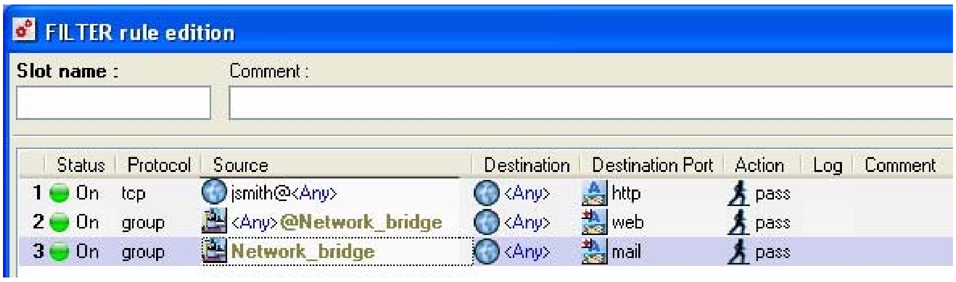
Slot name :

Comment :

	Status	Protocol	Source	Destination	Destination Port	Action	Log	Comm
1	● On	group	<Any>@NetworkIN	<Any>	web	pass		

Figure 543: 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:



FILTER rule edition

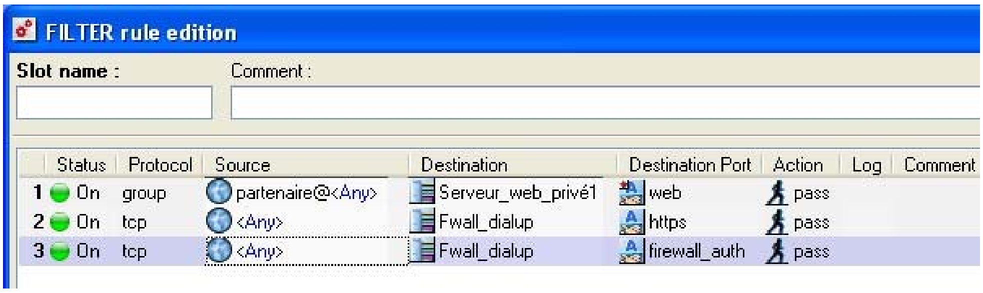
Slot name :

Comment :

	Status	Protocol	Source	Destination	Destination Port	Action	Log	Comment
1	● On	tcp	jsmith@<Any>	<Any>	http	pass		
2	● On	group	<Any>@Network_bridge	<Any>	web	pass		
3	● On	group	Network_bridge	<Any>	mail	pass		

Figure 544: 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).



FILTER rule edition

Slot name : Comment :

	Status	Protocol	Source	Destination	Destination Port	Action	Log	Comment
1	On	group	partenaire@<Any>	Serveur_web_privé1	web	pass		
2	On	tcp	<Any>	Fwall_dialup	https	pass		
3	On	tcp	<Any>	Fwall_dialup	firewall_auth	pass		

Figure 545: 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 G: Events

Below is a non-exhaustive list of the event notifications set off by the NETASQ Firewall.

Event notification

Certain events do not have to be attacks to be logged by the Firewall. These events can be viewed from in NETASQ UNIFIED MANAGER (**`Configuration\Logs`** menu).

Notification	Description
Firewall shutdown	Indicates that the Firewall has been shut down
'Authentication failed for' + user name	PPTP authentication has failed (the login or PPTP password is incorrect)
'Connection terminated for' + user name	The PPTP or dialup connection is over.
You have 20% of disk space left for the log file	The log file has exceeded 80% of its capacity (only in shutdown or security mode, which means that in this case the Firewall acts as a "block all").
'connection established for'	The PPTP or dialup connection is established correctly
'phase 1 IPsec failed'	Phase 1 of the IKE protocol has not been established correctly
'phase 2 IPsec failed'	Phase 2 of the IKE protocol has not been established correctly
'The IPsec key cannot be located for' + the VPN identifier	No pre-shared key corresponds to this VPN identifier. The key corresponding to the identifier has not been specified in the pre-shared key management.
'Firewall start-up'	Indicates a firewall start-up
HA: Active Firewall failure	Indicates a breakdown of the active Firewall. The passive Firewall then becomes active. (This event can only be detected if you possess two Firewalls configured in high availability).
HA: Passive Firewall failure	Indicates a breakdown of the passive Firewall (This incident can only be detected if you have two Firewalls configured for high availability).
'CRL invalid for the VPN tunnel'	The certificate revocation list (CRL) used for a VPN tunnel is invalid.
'certificate for the VPN tunnel invalid'	The remote VPN equipment certificate is invalid.
The log partition has	The disk partition containing the logs can no longer be detected on the same

been changed	disk as on the previous reboot. There are two possible causes - a hardware intervention (a disk has been added to the Firewall to contain the log partition), or a disk problem (the log division can no longer be detected correctly).

Appendix H: 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):

Launching the command server

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

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
- **ipnat -l:** displays the active address translation rules.
- **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 slot or an option

Deactivation

- **ennat 00:** deactivates address translation.
- **envpn 00:** deactivates the active VPN tunnel.
- **enurl 00:** deactivates URL filtering.

Activation

- **ennat xx:** activates the address translation slot bearing the number xx
- **envpn xx:** activates the VPN slot bearing the number xx.
- **enurl xx:** activates the URL filter slot bearing the number xx.
- **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.

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      :  U700XXA0Z0899020
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 I: 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:

- Firstly the LEDs on the front panel of the appliance light up (red) or flicker (yellow) to alert you.
- Then the alarms are logged in a specific file which you can consult from the graphical interface (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. Moreoever, an action can be added: sending an e-mail to the administrator or quarantining the 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 ou 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 J: 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

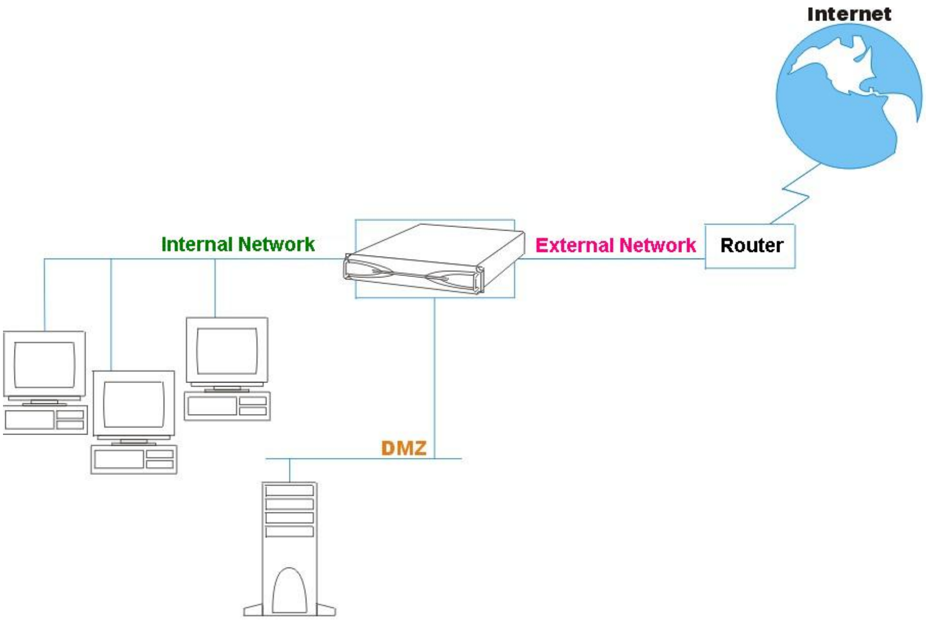


Figure 546: Setting up a DMZ

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

Appendix K: 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 ofSecure 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 L: Resetting the firewall

It is possible to restore the default factory settings of a NETASQ Firewall. This operation will bring the product into its initial state.

> **WARNING**
> Resetting a Firewall will completely remove the configuration made on the product. This operation is irreversible, so don't apply this procedure unless absolutely needed.

For a U30, U70, U120, U250 and U450

In order to reset a NETASQ U30, U70, U120, U250 or U450 Firewall, take a pointed object (a pen for example). A small switch is located on the appliance's front panel (between the USB port and the VGA port) and is accessible through a hole in the hood. Keep the button pressed for about 15 seconds, until you hear a sound. The reset procedure will be automatically launched and after a few minutes the initial settings will be recovered and the Firewall will reboot. This reboot takes about 5 minutes, so do wait until the end of the procedure (you will hear a sound) before reconnecting to the firewall. Caution: this operation will also reset the password.

For other products

For other products, resetting a NETASQ Firewall has to be done in console mode. Several methods are possible to access the Firewall in console mode. The easiest one can be done with the serial link. For this, use the serial cable provided with the Firewall in order to connect the appliance and a PC through their serial port.

Start an application like HyperTerminal (accessible through the menu **`Start\Programs\Accessories\Communication`**).

Choose a communication on the COM port and specify the following parameters:

- Bits per second: 9600
- Data bits: 8
- Parity: None
- Stop bit: 1
- Traffic control: Hardware

The following invitation appears:

```
FreeBSD (U70XXA0Z089020) (ttyd0)
login:
```

Indicate the “admin” login and the related password that you use to connect to the Firewall. Enter the following command: **defaultconfig -f** and press Enter

```
FreeBSD (U70XXA0Z0899020) (ttyd0)
login: admin
SSH Passphrase:
Copyright (c) 1980, 1983, 1986,1988, 1990, 1991, 1993, 1994
                    The Regents of the University of California. All rights reserved

U70XXA0Z0899020>defaultconfig -f
```

A beep will sound and your Firewall will reboot. The Firewall is now restored to factory defaults.

Appendix M: Prohibited names

The following is a list of object names (except for “user” objects) prohibted on the NETASQ Firewall.

Prohibited characters

These characters cannot be used in object names:

- « »
- \
- #
- @
- [
-]
- =

- <tab>
- <space>

Prohibited beginning characters

Object names cannot begin with numerals (0, 1, 2, 3, 4, 5, 6, 7, 8, 9).

Prohibited prefixes

These case-insensitive prefixes cannot be used at the beginning of an object name:

- Firewall_
- Network_
- ephemeral_
- Global_

Prohibited names

The following case-insensitve names cannot be used when creating objects on the Firewall:

- any
- anonymous
- broadcast

Appendix N: 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 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 mode	Port TCP/1300
Appliance operation check and status indicators	ICMP (PING)
NETASQ UNIFIED MANAGER, NETASQ REAL-TIME MONITOR, NETASQ EVENT REPORTER, VPN Manager	Port TCP/1300
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.

Appendix O: Vulnerability families

There are currently 20 vulnerability families:

- 3= « database »
- 4= »DNS Server »
- 7= « FTP Server »
- 13= « Peer to Peer »
- 10= « Instant Messengers »

- 2= « Web Applications »
- 1= « SSH »
- 5= « Web Server »
- 6= « Web Client »
- 8= « FTP Client »
- 9= « MISC »
- 11= « Mail Server »
- 12= « Mail Client »
- 14= « Media Players »
- 15= « Operating System »
- 16= “Security Tool”
- 17= « Malware »
- 18= « Netawork Tool »
- 19= “Office”
- 20= “System Tool”

Appendix P: List of protocol alarms

Probe alarms

- Nmap OS probe
- Queso OS probe
- Firewall policy detection
- Possible port scan
- XProbe OS probe

DNS alarms

- DNS label recursion
- DNS id spoofing
- DNS zone change
- DNS zone update
- DNS cache poisoning
- Bad pointer in packet
- Possible buffer overflow using DNS string
- Bad DNS protocol

Miscellaneous alarms

- Invalid RIP packet
- Invalid eDonkey protocol
- Blacklisted address
- Whitelisted address
- Packet for destination on the same interface
- Datatracking problem
- Quality of service drop
- Unauthorized protocol detected
- Skype protocol detected

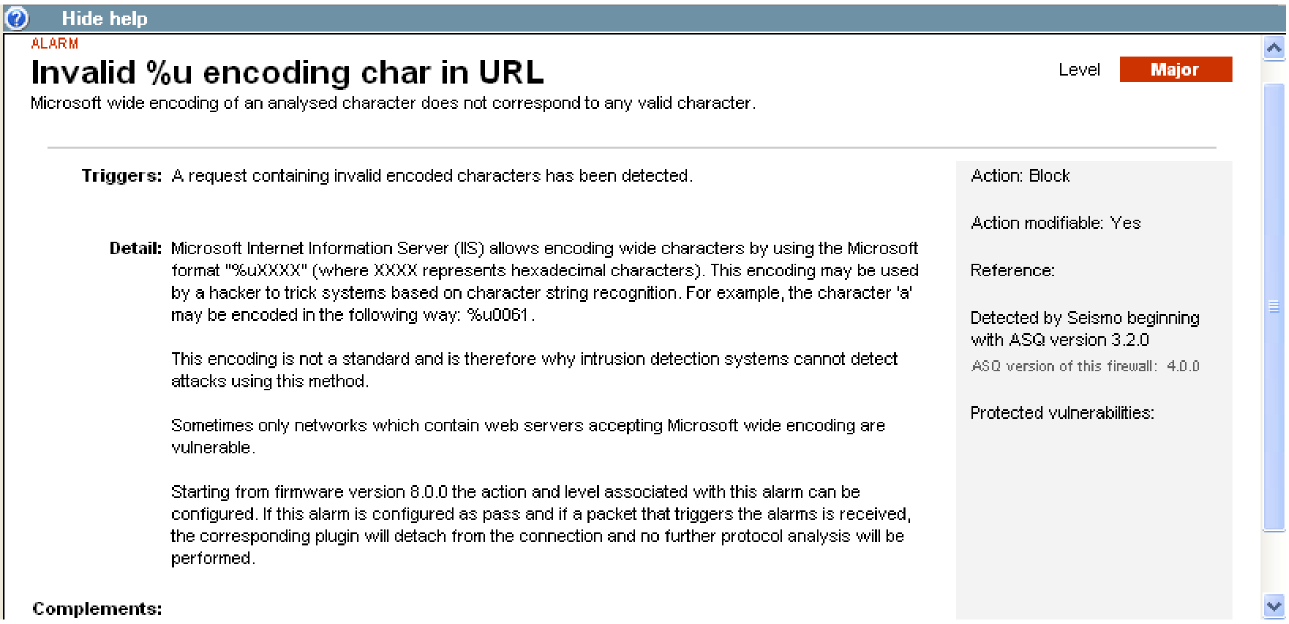
DoS alarms

- Land style attack
- Possible ICMP flooding
- Possible UDP flooding

- Possible TCP SYN flooding
- Windows OOB data bug
- Possible attack on capacity

HTTP alarms

- Invalid %u encoding char in URL. Its help file is the following:



ALARM

Invalid %u encoding char in URL

Level Major

Microsoft wide encoding of an analysed character does not correspond to any valid character.

Triggers: A request containing invalid encoded characters has been detected.

Detail: Microsoft Internet Information Server (IIS) allows encoding wide characters by using the Microsoft format "%uXXXX" (where XXXX represents hexadecimal characters). This encoding may be used by a hacker to trick systems based on character string recognition. For example, the character 'a' may be encoded in the following way: %u0061.

This encoding is not a standard and is therefore why intrusion detection systems cannot detect attacks using this method.

Sometimes only networks which contain web servers accepting Microsoft wide encoding are vulnerable.

Starting from firmware version 8.0.0 the action and level associated with this alarm can be configured. If this alarm is configured as pass and if a packet that triggers the alarms is received, the corresponding plugin will detach from the connection and no further protocol analysis will be performed.

Complements:

Action: Block

Action modifiable: Yes

Reference:

Detected by Seismo beginning with ASQ version 3.2.0

ASQ version of this firewall: 4.0.0

Protected vulnerabilities:

- Evasion using %u encoding char in URL.
- Invalid escaped char in URL
- Escaped NULL char in URL
- Escaped percent char in URL
- Evasion using UTF-8 encoding
- Invalid HTTP protocol
- Possible buffer overflow on URL
- Possible buffer overflow on HTTP request
- Tunneling using CONNECT method
- Multiple slashes in URL
- Directory self-reference
- Directory traversal
- Bad UTF-8 encoding in URL
- Possible malicious code in HTTP header
- Directory traversal backward root folder
- Site with open redirect
- 304 response with message body.
- Additional data at end of reply

IGMP alarms

- Unknown IGMP type
- Non-multicast address in IGMP query
- Invalid IGMP packet
- Wrong IGMB checksum

IP alarms

- IP loopback address spoofing
- IP address spoofing

- Broadcast packet
- Multicast packet
- Address from experimental classe
- Bad IP options
- Unknown IP options
- Unanalyzed IP protocol
- Unknown internal network host
- Oversized fragment
- Overlapped fragment
- Source routing
- Zero sized fragment received
- Port 0 used as service
- Tiny fragment
- Port probe
- Direct access to private interface
- IP address spoofing on bridge
- “Link local” addresses (RFC 3330)
- Broadcast address used in source address
- Invalid IP protocol
- Wrong IP checksum
- IP fragment analyze
- Local GRE protocol
- Local ESP IPSec protocol
- Local AH IPSec protocol
- IP address spoofing on the IPSec interface
- Local OSPF protocol

MGCP alarms

- MGCP protocol error
- MGCP without request
- Possible buffer overflow in MGCP request/reply
- Possible malicious code in MGCP parameter
- Forbidden parameter in MGCP
- Missing mandatory SDP field in MGCP
- MGCP operations limit exceeded

SMTP alarms

- Invalid SMTP protocol
- Invalid char in SMTP header

SSL alarms

- Unencrypted data detected
- Unauthorized cipher level
- SSL version mismatch
- Invalid SSL packet
- Invalid SSL Record Layer

FTP alarms

- Possible FTP bounce attack
- FTP PASV insertion attack
- Unknown FTP command
- Buffer Overflow on FTP login
- Buffer Overflow on FTP

- Brute force attack on FTP password
- Command execution using SITE EXEC
- FTP PASV DoS
- Invalid FTP protocol
- Invalid PORT command
- ICMP information request
- Allowed by ICMP analyze
- Modification of ECHO ICMP data
- Unanalyzed protocol in ICMP message

ICMP alarms

- Unknown ICMP type
- ICMP replys without request
- ICMP redirect
- Invalid ICMP message
- ICMP timestamp request
- ICMP mask request
- Invalid ICMP checksum
- Possible small MTU attack

RTCP alarms

- Invalid RTCP protocol
- Invalid RTCP version
- Invalid RCTP packet type

RTP alarms

- Invalid RTP protocol
- Invalid RTP version
- Invalid RTP payload type

SIP plugin alarms (TCP & UDP)

- Invalid SIP protocol
- Possible buffer overflow in SIP request/reply
- Possible malicious code in SIP header
- Necessary SIP header missing
- Possibly spoofed SIP request
- Missing mandatory SDP field in SIP
- Bad expires field value in SIP
- Bad UTF-8 encoding in SIP
- SIP operations limit exceeded
- Missing purpose parameter in SIP
- Bad Via header in SIP
- Binary packet in SIP

TCP alarms

- Invalid TCP option
- Unknown TCP option
- Wrong TCP sequence number
- Wrong TCP checksum
- Multicast address with TCP

- Xmas tree attack
- Possible small MSS attack
- Misplaced TCP option
- TCP data evasion
- TCP broadcast address
- TCP data queue overflow
- Possible backdoor connection detected
- Invalid TCP packet for current connection state
- Invalid TCP protocol

UDP alarms

- UDP port loopback
- Wrong UDP checksum
- Invalid UDP protocol

Appendix Q: List of generic FTP commands and details of filtering

- **ABOR**: Command that interrupts the transfer in progress. This command does not accept arguments. By default, a scan will be performed to check RFC compliance.
- **ACCT**: Command that specifies the account to be used for connecting. This command accepts only a single argument. By default, a scan will be performed to check RFC compliance.
- **ADAT**: Command that sends security data for authentication. This command accepts only a single argument. By default, a scan will be performed to check RFC compliance.
- **AUTH**: Command that selects the security mechanism for authentication. This command accepts only a single argument. By default, a scan will be performed to check RFC compliance.
- **CCC**: Command that allows unprotected messages.
- **CDUP**: Command that modifies the parent working folder. This command does not accept arguments. . By default, a scan will be performed to check RFC compliance.
- **CONF**: Command that specifies the "confidential" message used for authentication.
- **CWD**: This command modifies the working folder. This command accepts one or several arguments. By default, a scan will be performed to check RFC compliance.
- **ENC**: This command specifies the "private" message used for authentication. This command accepts only a single argument. By default, a scan will be performed to check RFC compliance.
- **EPRT**: This command enables the extended active transfer mode. This command accepts only a single argument. By default, a scan will be performed to check RFC compliance.
- **EPSV**: This command selects the extended passive transfer mode. This command has to be executed with at most one argument. This command is blocked by default.
- **FEAT**: This command displays the extensions supported by the server. It does not accept arguments. The result of this command is filtered by the proxy if filtering has been requested on the FEAT command.
- **HELP**: This command returns the details for a given command. This command has to be executed with at most one argument. By default, a scan will be performed to check RFC compliance.
- **LIST**: This command lists the contents of a data location in a friendly way.
- **MDTM**: This command displays the date of the last modification for a given file. This command accepts one or several arguments. By default, a scan will be performed to check RFC compliance.
- **MIC**: This command specifies the "safe" message used for authentication. This command accepts only a single argument. By default, a scan will be performed to check RFC compliance.
- **MLSD**: This command displays the contents of the normalized folder. By default, a scan will be performed to check RFC compliance.
- **MLST**: This command displays the information of the normalized folder. By default, a scan will be performed to check RFC compliance.
- **MODE**: This command specifies the transfer mode. By default, a scan will be performed to check RFC compliance. This command is the object of a greater filter. It is allowed only with the arguments S, B, C and Z. If the antivirus scan has been enabled, only the argument S will be allowed.
- **NLST**: This command lists the contents of a data location of the computer in a friendly way. By default, a scan will be performed to check RFC compliance.

- **NOOP**: This command does not do anything. It does not accept arguments. By default, a scan will be performed to check RFC compliance.
- **OPTS**: This command specifies the status options for the given command. This command accepts one or several arguments. By default, a scan will be performed to check RFC compliance.
- **PASS**: This command specifies the password used for the connection. This command accepts only a single argument. By default, a scan will be performed to check RFC compliance.
- **PASV**: This command selects the passive transfer mode. This command does not accept arguments. By default, a scan will be performed to check RFC compliance.
- **PBSZ**: This command specifies the size of encoded blocks. This command accepts only a single argument. By default, a scan will be performed to check RFC compliance.
- **PORT**: This command selects the active transfer mode. This command accepts only a single argument. By default, a scan will be performed to check RFC compliance.
- **PROT**: This command specifies the level of protection. By default, a scan will be performed to check RFC compliance. This command is the object of a greater filter. It is allowed only with the arguments C, S E and P.
- **PWD**: This command displays the current working folder. This command does not accept arguments. By default, a scan will be performed to check RFC compliance.
- **QUIT**: This command terminates the session in progress and the connection. By default, a scan will be performed to check RFC compliance.
- **REIN**: This command terminates the session in progress (initialized with the user). By default, a scan will be performed to check RFC compliance.
- **REST**: This command specifies the offset with which the transfer has to catch up. By default, a scan will be performed to check RFC compliance. This command is the object of a greater filter. It is prohibited if the antivirus scan is running. Otherwise, the proxy will check that a single argument is present.
- **RETR**: This command retrieves a given file. This command accepts one or several arguments. By default, a scan will be performed to check RFC compliance
- **SITE**: This command executes a command specific to the server. This command accepts only a single argument. By default, a scan will be performed to check RFC compliance.
- **SIZE**: This command displays the transfer size for a given file. This command accepts one or several arguments. By default, a scan will be performed to check RFC compliance.
- **SMNT**: This command modifies the data structure of the system in progress. This command accepts one or several arguments. By default, a scan will be performed to check RFC compliance.
- **STAT**: This command displays the current status. By default, a scan will be performed to check RFC compliance.
- **STRU**: This command specifies the structure of transferred data. By default, a scan will be performed to check RFC compliance. This command is the object of a greater filter. It is allowed only with the arguments F, R and P. If the antivirus scan has been enabled, only the argument F will be allowed.
- **SYST**: This command displays the information about the server's operating system. This command does not accept arguments. By default, a scan will be performed to check RFC compliance.
- **TYPE**: This command specifies the type of data transferred. By default, a scan will be performed to check RFC compliance. This command is the object of a greater filter. It is allowed only with the arguments ASCII, EBCDIC, IMAGE, I, A, E and L. If the antivirus scan has been enabled, only the arguments ASCII, IMAGE, I and A will be allowed. The option L may be followed by a digital argument. The options E, A, EBCDIC and ASCII accept the following arguments: N, C and T.
- **USER**: This command specifies the name of the user for connecting.
- **XCUP**: This command modifies the parent working folder. This command does not accept arguments. By default, a scan will be performed to check RFC compliance.
- **XCWD**: This command modifies the working folder. This command accepts one or several arguments. By default, a scan will be performed to check RFC compliance.
- **XPWD**: This command displays the current working folder. This command does not accept arguments. By default, a scan will be performed to check RFC compliance.

Appendix R: List of FTP modification commands and details of filtering

- **ALLO**: This command allocates the storage space on this server. It accepts one or several arguments. By default, a scan will be performed to check RFC compliance if the option “Enable modification commands” has been enabled. Otherwise, the command will be blocked.
- **APPE**: This command adds (or creates) to the data location. This command is the object of a greater filter. Indeed, this command is prohibited if the antivirus scan has been enabled (risk of bypass). Otherwise, the presence of at least one argument will be checked for.
- **DELE**: This command deletes a given file. It accepts one or several arguments. By default, a scan will be performed to check RFC compliance if the option “Enable modification commands” has been enabled. Otherwise, the command will be blocked.
- **MKD**: This command creates a new folder. It accepts one or several arguments. By default, a scan will be performed to check RFC compliance if the option “Enable modification commands” has been enabled. Otherwise, the command will be blocked.
- **RMD**: This command deletes the given folder. It accepts one or several arguments. By default, a scan will be performed to check RFC compliance if the option “Enable modification commands” has been enabled. Otherwise, the command will be blocked.
- **RNFR**: This command selects a file that has to be renamed. It accepts one or several arguments. By default, a scan will be performed to check RFC compliance if the option “Enable modification commands” has been enabled. Otherwise, the command will be blocked.
- **RNTO**: This command specifies the new name of the selected file. It accepts one or several arguments. By default, a scan will be performed to check RFC compliance if the option “Enable modification commands” has been enabled. Otherwise, the command will be blocked.
- **STOR**: This command stores a given file. It accepts one or several arguments. By default, a scan will be performed to check RFC compliance if the option “Enable modification commands” has been enabled. Otherwise, the command will be blocked.
- **STOU**: This command stores a given file with a unique name. This command does not accept arguments. By default, a scan will be performed to check RFC compliance if the option “Enable modification commands” has been enabled. Otherwise, the command will be blocked.
- **XMKD**: This command creates a new folder. It accepts one or several arguments. By default, a scan will be performed to check RFC compliance if the option “Enable modification commands” has been enabled. Otherwise, the command will be blocked.
- **XRMD**: This command deletes the given folder. It accepts one or several arguments. By default, a scan will be performed to check RFC compliance if the option “Enable modification commands” has been enabled. Otherwise, the command will be blocked.

Appendix S: List of sensitive alarms

There are 27 sensitive alarms.

- Dns (4): SFA_DNS_LABEL
  SFA_DNS_BADPOINTER
  SFA_DNS_LARGESTRING
  SFA_DNS_BADPROTO
- Edonkey (1): SFA_EDONKEY_BADPROTO
- Ftp (4): SFA_FTP_PASVINSERT
  SFA_FTP_UPOVERFLOW
  SFA_FTP_CMDOVERFLOW
  SFA_FTP_BADPROTO
- Http (7): SFA_HTTP_WIDEBAD

SFA_HTTP_WIDEEVASION
SFA_HTTP_ESCNULL
SFA_HTTP_UTF8OVERLONG
SFA_HTTP_BADPROTO
SFA_HTTP_URLOVERFLOW
SFA_HTTP_OVERFLOW

- Mgcp (2): SFA_MGCP_BADPROTO
SFA_MGCP_OVERFLOW
- Sip (2): SFA_SIP_BADPROTO
SFA_SIP_OVERFLOW
- Skype (1): SFA_SKYPE_DETECTED
- Smtp (1): SFA_SMTP_BADPROTO
- Ssl (3): SFA_SSL_BADVERSION
SFA_SSL_BADPACKET
- SFA_SSL_BADRECORDLAYER

Appendix T: List of alarms relating to protocols

HTTP

- **Invalid %u encoding char in URL**: this alarm checks the validity of %u encoding characters.
- **Evasion using %u encoding char in URL**: this alarm is raised by the %u encoding of an ASCII character (<256)
- **Possible malicious code in http header**: this alarm is raised when characters with an ASCII code > 127 are detected in the HTTP header.
- **Invalid escaped char in URL**: this alarm is raised by an invalid Unicode escaped character, for example a character %uXX or XX is not a hexadecimal value.
- **Escaped NULL char in URL:** this alarm is raised when there is the character %00 in the URL.
- **Escaped percent char in URL**: this alarm is raised when there is the character %25 (encoding of the '%') in the URL.
- **Evasion using UTF-8 encoding:** this alarm is raised when one or several characters encoded in UTF-8 (see [RFC2279]) are detected.
- **Bad UTF-8 encoding in URL:** UTF-8 encoding of an analyzed character does not correspond to any valid character.
- **Invalid HTTP protocol**: this alarm is raised when the HTTP is used improperly. A complement to the alarm message specifies the reason for the rejection.
- **Possible buffer overflow on URL**: This alarm is raised when the length of the URL exceeds the limit set in the ASQ configuration.
- **Possible buffer overflow on http request:** This alarm is raised when the length of a line in the body of the request exceeds the limit set by the ASQ configuration.
- **Tunneling using CONNECT method**: This alarm is raised when the CONNECT method is used.
- **Multiple slashes in URL:** this alarm is raised when there are several consecutive "/" in a URL.
- **Directory self-reference**: This alarm is raised when the URL contains a reference to a current directory (".")
- **Directory traversal**: this alarm is raised when the URL contains a reference to the parent directory ("..")
- **Bad UTF-8 encoding in URL**: This alarm is raised when an invalid UTF-8 field is detected.
- **Directory traversal backward root folder**: The requested URL contains a combination of dots (".") and slahes ("/").
- **Site with open redirect**: An open redirect allows bouncing to another website with checking parameters (example: www.realsite.fr/client.html?url=http://www.badsite.com.
- **304 response with message body**: An HTTP response "304 Not modified" had ben received with a message body that was not empty. HTTP 304 responses are used by a server to inform the client that a page has not been modified since its last visit as a response to a conditional GET. 304 responses must not contain a message body.
- **Additional data at end of reply**: The amount of data contained in an HTTP response (without keepalive and containing a Content-Length header field) exceeds the size announced in the Content-Length field of the HTTP header.

FTP

- **Possible FTP bounce attack:** This alarm may be raised in active or passive mode.

In active mode, the client asks the server to connect to a socket (via the PORT command). There is a bounce when the client asks the server to connect to a socket that is located on another host.
The alarm is raised by the PORT command, whose IP address given in the parameters does not correspond to the packet's source address.

In passive mode, there is a bounce when an FTP client requests from a server the address of a socket for a data connection and the server responds by specifying a socket on another host – the alarm is raised by a response to the PASV command whose IP address given in the parameters does not correspond to the packet's source address.

- **FTP PASV insertion attack**: Raised by a response to the PASV command even though it was not issued.
- **Unknown FTP command** An unknown FTP command has been detected.
- **Buffer Overflow on FTP login**: this alarm is raised by the USER command or a PASS command followed by an argument of more than 100 characters.
- **Buffer Overflow on FTP**: this alarm is raised by a command (other than USER or PASS) followed by an argument of more than 256 characters.
- **Brute force attack on FTP password**: raised after 5 successive login attempts.
- **Command execution using SITE EXEC**: Raised after a dangerous attempt to execute commands on the server.
- **FTP PASV Dos:** This alarm detects multiple open connections on the same FTP server. During the same FTP connection, if at least two PASV commands and their responses are detected and these responses correspond to the opening of two different ports, the alarm will be raised.
- **Invalid FTP protocol:** this alarm is raised by an FTP session that the ASQ can't analyze. Four events are capable of raising this alarm.
- **Invalid PORT command**: A "PORT" FTP command with invalid syntax has been detected.

EDONKEY

- **Invalid eDonkey protocol**: an eDonkey frame has the following structure (H = number in hexadecimal). The alarm is raised by an eDonkey frame with a field size that is either 0 or strictly above 500 000 bytes.

RIP

- **Invalid RIP packet**: Raised by a RIP packet whose parameters do not comply with RFC 1058 and RFC2453.

DNS

- **DNS label recursion**: to avoid repeating several occurrences of a domain name in a DNS packet, one occurrence can be replaced with a pointer to the beginning of another one.
- **DNS id spoofing**: The DNS if a DSN response is different from the id in the request. The DNS response and request are matched according to the IP address and the source port used by the sender of the request, which has to correspond to the IP address and the destination port in the response.
- **DNS zone change**: A DNS packet containing the operation Notify request.
- **DNS zone update**: DNS packet containing the operation Zone Update.
- **DNS cache poisoning**: raised by a DNS request containing one or several additional responses (RP).
- **Bad DNS protocol**: raised by improper use of the DNS protocol, a complement to the alarm message specifies the reason for the rejection.
- **Possible buffer overflow using DNS string:** a domain name in the packet exceeds 256 bytes.
- **Bad pointer in packet**: A domain name pointer points outside the packet.

SSL

- **Unencrypted data detected**: Unecnrypted data has been detected in an SSL communication.
- **Unauthorized cipher level**: The SSL negotiation ended up with an encryption level that was not allowed by the security policy.
- **SSL version mismatch**: The SSL client uses a different version of the protocol from the version used by the server.
- **Invalid SSL packet**: An invalid SSL packet has been detected.
- **Invalid SSL Record Layer**: An unknown SSL Record Layer has been transmitted (type, size, contents, etc). SSL Record Layers receive uninterpreted data from the highest protocols in blocks of arbitrary size that are not empty.
- **Skype protocol detected**: A Skype client has probably attempted to open an SSL connection. Indeed, this instant messenger can use SSL connections to bypass classic security devices.

SMTP

- **Invalid SMTP protocol**: An invalid SMTP communication has been detected.
- **invalid char in SMTP header**: A non-ASCII character has been identified in the SMTP header.

MGCP

- **MGCP protocol error**: An error was detected during the analysis of an MGCP communication. A complement to the alarm explains the problem.
- **MGCP without request**: The firewall detected an MGCP reply that does not match any request. A complement to the alarm explains the problem.
- **Possible buffer overflow in MGCP request/reply**: this alarm is raised by a request or a reply containing a line that exceeds the maximum limit (value can be configured). A complement to the alarm specifies the line concerned.
- **Possible malicious code in MGCP parameter**: Raised when characters that have an ASCII code > 127 in a parameter has been detected.
- **Forbidden parameter in MGCP**: Raised when an unauthorized MGCP parameter has been detected.
- **Missing mandatory SDP field in MGCP**: Raised when the missing field in the SIP protocol has been detected, a complement to the alarm specifies the field concerned.
- **MGCP operations limit exceeded**: Raised when the limits on MGCP operations have been exceeded (maximum 16 operations, requests without replies have a timeout of 2 seconds). A complement to the alarm indicates the reason for the rejection.

RTP

- **Invalid RTP protocol**: The RTP is invalid. A complement to the alarm indicates the reason.
- **Invalid RTP version**: The RTP version number is wrong. The first two bits are not “10”.
- **Invalid RTP payload type**: The data type detected is not in the list of types that the configuration allows. A complement to the alarm indicates the reason.

RTCP

- **Invalid RTCP protocol**: The RTP is invalid. A complement to the alarm indicates the reason.
- **Invalid RTCP version**: The RTP version number is wrong. The first two bits are not “10”.
- **Invalid RCTP packet type**: The packet type detected is not in the list of types that the configuration allows. A complement to the alarm indicates the reason for the rejection.

SIP

- **Invalid SIP protocol**: raised when improper use of the SIP protocol has been detected. A complement to the alarm indicates the reason for the rejection.

- **Possible buffer overflow in SIP request/reply**: This alarm is raised by a request or a reply containing a line that exceeds the maximum limit (value can be configured). A complement to the alarm specifies the line concerned.
- **Possible malicious code in SIP header**: Raised when characters that have an ASCII code > 127 in the SIP header has been detected.
- **Missing mandatory header in SIP**: raised when the SIP header, which is mandatory, has not been found
- **Possibly spoofed SIP request**: Raised when a SIP request which was possibly spoofed, has been detected.
- **Missing mandatory SDP field in SIP**: Raised when the missing field in the SIP protocol has been detected, a complement to the alarm specifies the field concerned.
- **Bad expires field value in SIP**: raised when there is an invalid expiry date.
- **Bad UTF-8 encoding in SIP:** raised when an invalid UTF-8 field has been detected.
- **SIP operations limit exceeded**: Raised when the limits on SIP operations have been exceeded (maximum 8 operations, requests without replies have a timeout of 60 seconds). A complement to the alarm indicates the reason for the rejection.
- **Missing purpose parameter in SIP**: Raised when the “purpose” parameter is not in the “Call info” for at least one URL.
- **Bad Via header in SIP**: raised when the “via field is invalid. A complement to the alarm indicates the reason for the rejection.
- **Binary packet in SIP:** A “0” ASCII character has been detected in the packet.

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 know 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 go, 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 contain 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 Shield

Security agent that protects Microsoft Windows® workstations and servers by integrating NETASQ’s ASQ technology.

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 Tunnelling 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 (internal name for NETASQ SEISMO *Parallel Virtual Machine*)

Software that enables using a set of UNIX workstations linked to a network much like a parallel workstation.

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.

SEISMO

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.

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 programme, 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 know 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.