NETASQ FIREWALL MULTIFUNCTION

USER CONFIGURATION MANUAL

Date	Version	Author	Details
April 2012	V1.2 - Firmware V9.0.3	NETASQ	Update

Reference : naengde_FirewallUserGuide.doc

WELCOME

Welcome NETASQ version 9's online help.

This guide details functionalities of the web administration interface modules, and provide information on how to configure your NETASQ firewall into your network.

For any questions, if you wish to report an error or suggest an improvement, feel free to contact us on **documentation@netasq.com**.

ACCESS PRIVILEGES

This module consists of 3 tabs:

- **Default options**: This tab allows you to define **IPSec and SSL VPN** access parameters as well as the default **Authentication** method.
- **User configuration**: Table of rules corresponding to **IPSec and SSL VPN** access parameters and **Authentication** of users and user groups.
- **PPTP**: Allows adding and listing users who have access to PPTP VPN via their logins, and creating passwords to enable them to log on.

"Default options" tab

Authentication

Default authentication method	In this field, you will be able to define the default authentication method for users or **Deny access** so that they will be unable to log on. In the drop-down list, you will see the authentication methods that you have previously added or enabled in the menu **Users\Authentication\Available methods** tab (**SSL Certificate, LDAP, Radius, SPNEGO, Kerberos**).

Click on **Apply** to confirm your configuration.

SSL VPN

SSL VPN profiles (see menu VPN\SSL VPN module) represent the set of web and application servers that you wish to list in order to assign them to your users or user groups.

Default SSL VPN profile	In this field, the default SSL VPN profile can be defined for users. Prior to this, ensure that you have already restricted access to servers defined in the configuration of the SSL VPN in the menu VPN\SSL VPN\User profiles tab (see *SSL VPN* document*).* The drop-down list will display the following options: **No profile:** Users will not have access to the SSL VPN. **Access to all profiles:** The user will have access to all SSL VPN profiles created previously. ---------- <**Name of user1 profile**>: the user will have access only to this SSL VPN profile. <**Name of user2 profile**>: the user will have access only to this other SSL VPN profile.

Click on Apply to confirm your configuration.

IPSEC

IPSec VPN enables the establishment of secure tunnels (peer authentication, data encryption and/or integrity checking) between two hosts, between a host and a network, or between two networks

.

Default IPSec policy	In this field, it is possible to **Deny** or **Allow** users the privilege of negotiating IPSec VPN tunnels by default. Depending on your selection, users and user groups will or will not be able to

	communicate internally on your private and protected IP networks, thereby allowing their data to be transmitted securely.

Click on Apply to confirm your configuration.

"User configuration" tab

Possible operations

Add button: Inserts a line to be configured after the selected line.
Delete button: Deletes the selected line.
Up button: Places the selected line before the line just above it.
Down button: Places the selected line after the line just below it.

From version 9.0.1 onwards, a search field by keywords/letters allows accessing the relevant users.

Configuration table

This table allows assigning access privileges to your users or user groups. You may customize them with regards to Authentication, SSL VPN and IPSec VPN parameters.

The table contains the following columns:

Status	Status of the access privilege configuration for the user or user group: **Enabled**: Double-click anywhere in the column to enable the created rule. **Disabled:** The rule is not in operation. The whole line will be grayed out to indicate that it has been disabled. **REMARK** The firewall will assess rules in their order of appearance on the screen: one by one from the top down. They are numbered likewise on the left side of the column. If Rule 1 affects a user group, all users involved in the rules that follow and which are part of this same group will be subject to its configuration. **Example**: If in **Rule 1,** you deny a user group authentication and/or access to the SSL VPN and if the user in **Rule 2** can authenticate via the LDAP and has a particular SSL VPN profile but is part of the group, this user will be blocked, and will have neither access to authentication nor to the SSL VPN.
User-user group	When a new line is added to the table, you can select the user of the user group you wish to configure. To do so, click on the arrow to the right of the column, which will display a drop-down list offering you a choice of several CNs created earlier, in the menu Users\Users module. **NOTE** It is also possible to add users who are not in the LDAP database, for example, for the KERBEROS and RADIUS methods.
Authentication	This column expands to show the list of possible authentication options for your user or

	user group. You will only be able to view the authentication methods that you have allowed in the menu **Users\Authentication** module\Available methods tab (*cf document on Authentication*). **NOTE** If you have not configured any authentication methods earlier, only "**Default**" and "**Deny**" will be available when you click on the arrow to the right of the column. By selecting "**Default**" the method selected automatically will be the method that you have defined in the previous tab Default options\Authentication- Default method field. By selecting "**Deny**", the selected user or user group will not be able to authenticate.
SSL VPN	This column allows you to assign a particular SSL VPN profile to a user or user group, configured beforehand in the menu VPN\SSL VPN module\User profiles tab. You may also select the **Default** option, which will take into account the default SSL VPN profile entered in the previous tab (Default options). If you select **Deny**, the user or user group will not have access to any SSL VPN profiles, contrary to the option **All profiles**, which will provide access to all web and application servers that have been enabled in the user profiles.
IPSEC	In this field, it is possible to **Deny** or **Allow** users the privilege of negotiating IPSec VPN tunnels. Depending on your selection, users and user groups will or will not be able to communicate internally on your private and protected IP networks, thereby allowing their data to be transmitted securely. **REMARK** The IPSec privilege only concerns tunnels: – with pre-shared key authentication and e-mail address logins, or – with authentication by certificate.
Description	Comments describing the user, user group or the rule.

REMARK

When you add lines to the table without having set up any rules, the columns **Authentication**, **SSL VPN** and **IPSEC** will be set to "**Deny**" by default, even if you have configured them differently in the Default options tab.

You therefore need to click on the option "**Default**" using the arrow to the right of each column if you wish to retrieve changes made earlier.

"PPTP" tab

This tab allows listing users who have access to the PPTP VPN, providing them with a secure and encrypted connection for their login.

The following actions can be performed:

Add	When you click on this button, a new line will be added to the table and will display the drop-down list of users created earlier in the menu Users\Users module:

	To ensure that the operation is valid, you will need to enter the user's password in the window that appears. **NOTE** It is possible to enter a user that does not exist in the firewall's user database, as the PPTP is separate from the LDAP module.
Delete	To delete a user, select the line containing the user to be removed from the list of PPTP logins, then click on **Delete**.
Modify user password	Select the line containing the user whose password you wish to modify and enter the new data in the window that appears.

From version 9.0.3 onwards, logins can now be entered in uppercase letters.

ACTIVE UPDATE

The Active Update configuration window consists of a single screen:

This screen is divided into two sections

- **Automatic updates**: allows activating an update module.
- **Advanced properties – Update servers**: allows defining update servers.

Automatic updates

Enabled	Enables or disables (Enabled/ Disabled buttons), by a simple click, updates via Active Update for the type of update selected.
Module	Type of update. (The list of modules varies according to the license purchased).

NOTES
In the event of a failed update, the system will automatically backtrack.
Simply double-click to allow (**"Allow all"** button) or prohibit (**"Block all"**) all updates.

Update servers

URL	Update files are retrieved on one of the servers defined by the user. (Update servers are common to all update types.) 4 URLs are defined by default. To add a URL, click on **Add**: the following URL will be added by default: http://update.netasq.com/1. Replace this with your URL and click on **Apply**. To delete a URL from the list, select it and click on **Delete**.

You can add URLs by clicking on the icon , and on to **Delete** them.

Update frequency	Indicates the frequency with which dynamic URL lists, ASQ contextual signatures and the antispam configuration are updated. The frequency is indicated as 3 hours, and can be modified in console mode.

ADMINISTRATORS

This module consists of 2 tabs:
- Administrators: allows creating administrators by granting administration privileges to users using one of the following authentication methods: LDAP RADIUS, KERBEROS or SSL.
- Administrator account: allows defining the authentication password of the administrator account by exporting the public or private key.

“Administrators” tab

The window for this tab is divided into 3 sections:
- A taskbar (top): displays the various possible operations that can be performed (**Add an administrator**, **Delete**, **Copy privileges** etc.).
- The list of users and user groups identified as admin (left).
- The table of administrator privileges (right).

Possible operations

You will be able to create your table of administrators from your LDAP database as well as their respective privileges.

Adding an administrator

Add an administrator without any privileges	This type of administrator has all the basic privileges such as access to the **Dashboard** and to the following modules: **License, Maintenance, Active Update, High availability** and its wizard, **CLI** console**, Network, Routing, Dynamic DNS, DHCP, DNS cache proxy**, Objects, URL groups, **Certificates and PKI**, **Authentication** and its wizard, **URL filtering, SSL** and **SMTP, Alarms, Inspection profiles, Antivirus, Antispam, Vulnerability detection, Block messages,** and Preferences**.**
Add an administrator with read-only access	This type of administrator has the same basic access privileges as the administrator "without privileges" with the following additional privileges: reading of **SNMP** logs, **E-mail alerts**, **System events** as well as reading privileges for **Filtering** and **VPN**.
Add an administrator with all privileges	This type of administrator has access to all modules except Configuration, Administrators, and Directory configuration (LDAP). **REMARK** There can only be one "superadministrator" with the following characteristics: • The only administrator authorized to log on via the local console on NETASQ appliances, and only during the installation of the firewall or for maintenance operations outside of normal production use. • Tasked with defining the profiles of the other administrators. • Full access to the premises on which the firewall appliances are stored, and all interventions are performed under his supervision,

Once you have imported your administrator, he will appear in the list "**User-user group**" to the left of the screen.
The following operations can be performed on this administrator.

Delete	Select the administrator to be removed from the list and click on **Delete**.
Up	Places the administrator above the administrator before him in the list.
Down	Places the administrator below the administrator after him in the list.
Copy privileges	Select the administrator whose privileges you wish to copy and click on this button.
Paste privileges	Select the administrator to whom you wish to assign the same privileges as the administrator from whom the privileges have been copied and click on this button.
Grant all privileges	Regardless of the privileges assigned to the selected administrator, by clicking on this button.

Table of privileges

Your interface is in "**simple view**" by default. The table displays 5 columns, which represent 5 categories of privileges to which an administrator may or may not be affiliated: **System, Network, Users, Firewall** and **Monitoring**.
The icons in the table mean:

: All privileges have been assigned.

: All privileges have not been assigned.

: Some of the privileges have been assigned.

By switching to "**advanced view**" using the icons or (depending on the length of your screen), the table will display the details of the privileges by category. To find out the exact privileges corresponding to each column, see the bubble that appears when the mouse passes over each column header.

Example
If you are at the top of the **System** column, you will see the access privileges it includes, in this case, *"Maintenance"* and *"Objects"*.

NOTES

Double-clicking on the represented icons changes the status of privileges (from "assigned" to "not assigned" for example).

Double-clicking on this icon  will assign the privileges, and this icon  will be displayed instead.

The list of privileges that can be assigned in simple view are:

Privileges in simple view

System	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) Privilege to modify Object database
Network	Privilege to modify filtering policy configuration and routing configuration (default route, static routes and trusted networks)
Users	Privilege to modify Users and PKI
Firewall	Privilege to modify VPN configuration, Intrusion prevention (IPS) configuration et vulnerabilitymanagement
Monitoring	Privilege to modify configuration from NETASQ Realtime Monitor and logs configuration

Privileges in advanced view

Logs (R)	Logs consultation
Filter (R)	Filtering policy consultation
VPN (R)	VPN configuration consultation
Logs (W)	Privilege to modify logs configuration
Filter (W)	Privilege to modify filtering policy configuration
VPN (W)	Privilege to modify VPN configuration
Monitoring	Privilege to modify configuration from NETASQ Realtime Monitor
Content filtering	Privilege for URL filtering, Mail, SSL and antivirus management
PKI	Privilege to modify PKI
Objects	Privilege to modify Object database
Users	Privilege to modify Users
Network	Privilege to modify network configuration (interfaces, bridges, dialups, VLANs and dynamic DNS configuration)
Routing	Privilege to modify routing (default route, static routes and trusted networks)
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)
Intrusion prevention	Privilege to modify Intrusion prevention (IPS) configuration
Vulnerability Manager	Privilege to consult or modify vulnerabilities
Objects global	Privilege to access to global objets
Filter global	Privilege to access to global filtering policy

“Administrator account” tab

This screen allows the definition of authentication data for the administrator account.

Password	Defines the password for the admin account. **REMARK** Must not contain the character **''**.
Confirm password	Confirms the password of the admin account which you have just entered in the previous field.
Password strength	This field indicates the security level of your password: “Very weak”, “Weak”, “Medium”, “Strong” or “Excellent”. The use of uppercase and special characters is strongly advised.

NOTE
NETASQ uses asymmetrical encryption, meaning that it uses a key pair consisting of a public key, used for encrypting data, and a private key, used for decryption. The advantage of using this system is that it removes the problem of securely transmitting the key and allows electronic signatures.

Export private key	By clicking on this button, you will save the private key associated with the admin account on your workstation.
Export public key	By clicking on this button, you will save the public key associated with the admin account on your workstation.

ALARMS

In this module, you will be able to manage the configuration of your alarms.
It is divided into two views:

- “view by inspection profile” (also called “ view by configuration”)
- ”view by context” (also called “view by protocol”)

View by inspection profile

This screen represents the view of the alarms by configuration or by inspection profile.

NOTE
A configuration is a set of protocol profiles. They are defined in the “Inspection profiles” module.
Alarms can be sorted, filtered by criteria (DoS, IM, etc...) or filtered by keywords. The results are paginated.

Selecting the configuration profile

You can configure up to 10 profiles, bearing by default the names “Config”, “Config 1” etc.
These names cannot be modified in the Alarms module but in the menu Application protection\Inspection profile:

1. Select a configuration from the drop-down list.
2. Click on “Edit” and select “Rename”.
3. Change the name of the profile in the field and add a comment if necessary.
4. Click on “Update”.

You will see your modified profile in the drop-down list of configurations in the Alarms module.
You can perform several actions in the profile:

Apply a model

Internet	By applying this model, most alarm levels will be set to “Ignore”
Low	By applying this model, most alarm levels will be set to “Minor”
Medium	By applying this model, alarm levels will be modified according to the selected profile.
High	By applying this model, most alarm levels will be set to “Major”

New alarms

Approve all	If this option is selected, all new alarms represented by the icon will be accepted: the icon will disappear and the action in the column relating to these alarms will be set to “Allow”.

Search

This field allows displaying only the alarm(s) containing the letter or word entered.

Filter

This list contains several protocols and services covered by the alarms. You can sort them and display only the alarms that belong to the following categories:

None	All categories of alarms will be displayed.
New alarms	Only new alarms, represented by the icon will be displayed (as a general rule, ftp or http alarms).
VoIP	Only alarms relating to VoIP will be displayed (mgcp, rtcp or SIP).
Denial of service	Only alarms relating to Denial of Service attacks (DoS) will be displayed.
Instant messaging	Only alarms indicating an anomaly with regards to instant messaging services (MSN, Yahoo Messenger etc.) will appear on the screen.
Peer to peer	Only alarms relating to peer-to-peer systems will be displayed.

The various columns

Context: id	Alarm name
Message	Text describing the alarm and its characteristics.
Action	When an alarm is raised, the associated action will be applied to the packet that caused the alarm. You can choose to **Allow** or **Block** traffic that causes this alarm.
Level	Three alarm levels are available: "Ignore", "Minor" et "Major".
New	Allows viewing new alarms, represented by the icon .
Advanced	This column displays the selected reaction when the alarm is raised (in addition to **Block** or **Allow**). When you click in this column, a window appears and offers these options: **None:** nothing will be done for this alarm. **Send an e-mail:** an e-mail will be sent when this alarm is raised. **Quarantine:** the packet that caused the alarm will be blocked. You can also choose to capture the packet that caused the alarm by selecting the corresponding checkbox. The capture can then be viewed using a network analyzer (sniffer). Next, click on **Apply**.

For each of the 10 profiles, you can configure them any way you wish by modifying the parameters described above.

View by context

This view sets out alarms by protocol profiles. The first drop-down list, on the left, allows selecting the protocol context.

For each protocol, you can configure up to 10 configuration profiles, which can be selected from the second drop-down list (which displays “default”)
You can change the name of the file by going to the menu Application protection\ Protocols and applications:

1. Select a configuration from the drop-down list.
2. Click on “Edit” and select “Rename”.
3. Change the name of the profile in the field and add a comment if necessary.
4. Click on “Update”.

You will see your modified profile in the drop-down list of configurations in the Alarms module.
You can perform several actions in the profile:

Edit policy

Internet	By applying this model, most alarm levels will be set to “Ignore”
Low	By applying this model, most alarm levels will be set to “Minor”
Medium	By applying this model, alarm levels will be modified according to the selected profile.
High	By applying this model, most alarm levels will be set to “Major”

REMARK
The selected policy will appear in brackets beside the button.

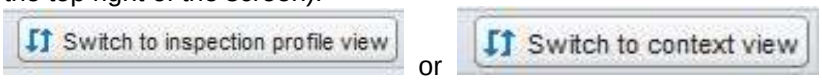
New alarms

Approve all	If this option is selected, all new alarms represented by the icon will be accepted: the icon will disappear.

Search

This field allows displaying only the alarm(s) containing the letter or word entered.

GENERAL NOTE
You can at any time, switch from one view to the other by clicking on the following buttons (at the top right of the screen):



From version 9.0.1 onwards, an instant search field appears in both views of the module, in order to more easily filter profiles and contexts without having to press “Enter”.
A new alarm has been added for the detection of Cisco WAN Optimizer traffic. This alarm blocks this traffic by default, but it can be allowed (tcpudp : 247).

WARNING
Once it is authorized, this type of traffic will not undergo protocol scans.

ANTISPAM

The antispam configuration screen consists of 3 tabs:

- General: Basic configuration of the Antispam module (activation, SMTP parameters, Reputation-based analysis, etc).
- Whitelisted domains: contains the list of domains that must be systematically considered legitimate.
- Blacklisted domains: contains the list of domains that must be systematically considered as spam senders.

"General" tab

The antispam module can be enabled by determining the analyses to be enabled. Two options are available on the firewall:

Enable reputation-based analysis (DNS blacklists - RBL)	This option allows validating the sender by comparing against a public list of known spam senders (DNSBL).
Enable heuristic analysis	This option allows examining the contents of the e-mail to determine its impact.

SMTP parameters

The trusted server concerns the SMTP server. By filling in this field, which is optional, e-mails will be analyzed more thoroughly by the **Antispam** module.

SMTP server domain name (FQDN)	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.
Action	There are 4 possible actions that will allow the SMTP proxy to respond to the remote SMTP server by indicating that the message has been rejected as it is spam. • **Tag as spam**: e-mails will not be blocked but will be tagged as spam. • **Block all spam messages:** the e-mail will be rejected regardless of the level of confidence. • **Block all spam messages at Level 2 or higher**: this option allows defining that beyond the confidence threshold of Level 2, an e-mail will be rejected. The thresholds are: "1 – Low", "2 – Medium", "3 – High". • **Block only Level 3 spam messages**: this option allows defining that beyond the confidence threshold of Level 3 (High), the e-mail will be rejected.

For example, if you set a limit of 500 for the heuristic analysis, e-mails with a score higher than 500 will be considered spam. From 500 to 2000, the level of confidence will be low, from 2000 to 3500 it will be moderate and from 3500 to 5000, 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 2000 to 5000) will be rejected whereas those from 500 to 2000 will be kept.

REMARK
When several methods of analysis are used simultaneously, the highest score will be assigned.

Advanced properties

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:

Add spam tag to subject fields (prefix)	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 provide for 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** Double quote characters are not allowed.
Insert X-Spam headers	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 "spam assassin" format, to perform the necessary actions on the tagged message.

Reputation-based analysis

The **DNS blacklist analysis** or **RBL** (*Realtime Blackhole List*) enables identifying the message as spam through RBL servers. The following menus allow configuring the list of RBL servers which will be used for this analysis as well as the level of trust assigned to each of the servers.

List of DNS blacklist severs (RBL)

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 disabled by clicking on the checkbox at the start of each line (in the **Enabled** column).
The levels indicated in the columns of the table refer to the levels of confidence assigned to the server.
You can also configure the RBL servers to which you would like your Firewall to connect. To add a server, click on **Add**. A new line will appear.
Specify a name for this server (a unique name for the RBL server list), a DNS target (Field: **Domain name** only, which should be a valid domain name), a level of confidence (Low, Medium and High) and comments (optional). Click on **Apply.**
To delete configured server, select it in the list and click on **Delete**.

NOTE
RBL servers in NETASQ's native configuration are differentiated from customized servers by a padlock symbol (), which indicates **RBL** servers in NETASQ's native configuration.

Reminder: **Active Update** only updates the list of these servers.

Heuristic analysis

The heuristic analysis is based on GOTO Software's VadeRetro antispam. Using a set of calculations, this antispam will derive a message's degree of legitimacy.
The antispam module calculates a value that defines a message's "unwantedness". E-mails that obtain a value exceeding or equal to the threshold set will be considered as spam.

Minimum score for spam definition [1-5000] :	The heuristic analysis performed by the **Antispam** module calculates a value that defines a message's "unwantedness". 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. By modifying the score, the minimum value of the 3 confidence thresholds will be modified. Furthermore, the higher the calculated value, the higher will be the level of confidence that the antispam module assigns to the analysis. Thresholds for the levels of confidence cannot be configured in the web administration interface.

"Whitelisted domains" tab

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 name (generic characters accepted: * and ?)	Specify 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**.

NOTE
The antispam module will NEVER treat messages from whitelisted domains as spam.

"Blacklisted domains" tab

This section enables the definition of domains from which analyzed messages will be systematically treated as **spam**. The procedure for adding a domain to be blocked is as follows:

Domain name (generic characters accepted: * and ?)	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**.

GENERAL REMARKS
The antispam module will treat as spam all messages from blacklisted 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. A domain name can appear in either the whitelist or the blacklist.
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.

ANTIVIRUS

The configuration screen for the Antivirus service consists of 2 zones:

- Selection of the antivirus engine
- Parameters

Antivirus engine

The drop-down list allows migrating between antivirus solutions (ClamAV or Kaspersky). When the choice of an antivirus is made, the following message will appear:
« The antivirus database has to be fully downloaded before the antivirus can be changed. During this interval, the antivirus scan will fail." Click on **Switch engines** pour to confirm your selection.
Once the database has been downloaded, the antivirus will be enabled.

Parameters

Analysis of ClamAV files

In this menu, the types of files that need to be scanned by the NETASQ firewall antivirus service are configured.

Analyze compressed executable files	This option enables the decompression engine (Diet,Pkite, Lzexe, Exepack…).
Analyze archives	This option enables the extraction engine and allows scanning archives (zip, arj, lha, rar, cab…)
Block password-protected files	This option allows blocking files that are protected by passwords.
Block unsupported file formats	This option allows blocking file formats that the antivirus is unable to scan.

Analysis of Kaspersky files

Inspect archives	This option enables the extraction engine and allows scanning archives (zip, arj, lha, rar, cab…)
Block password-protected files	This option allows blocking files that are protected by passwords.

AUTHENTICATION

The authentication feature allows users to enter their logins and to identify themselves by entering a password that only they would know and which protects their personal data.
It uses an LDAP (*Lightweight Directory Access Protocol*) database that stores user accounts and occasionally the user's X509 digital certificate as well.
When authentication is successful, the user's login will be associated with the host from which he identified himself and with all IP packets that originate from it, for a duration specified by the user.

The **Authentication** module consists of a configuration wizard, which appears by clicking on the icon  and involves several steps that vary according to the directory that you select.
It is divided into 4 tabs:

- General: Enables configuration of access to the captive portal from various interfaces, as well as the different information relating to it (SSL access, authentication, proxy).
- Available methods: This tab offers you the choice of one or several authentication methods and the possibility of configuring them, by indicating if you wish to allow them on internal and/or external interfaces.
- Internal interfaces: Enables management of user passwords, authorized authentication durations and enrolment at the internal interface level.
- External interfaces: Enables management of user passwords, authorized authentication durations and enrolment at the external interface level.

Authentication wizard

In this section, you will be able to select your authentication method:

- Authentication on an Active Directory (Kerberos)
- Authentication on the internal directory (LDAP)
- Authentication on a RADIUS base

From version 9.0.1 onwards, links added to the authentication portal in version 9 have been translated into all the supported languages.
ISO-8859-15 characters (including "€") are allowed for administrator passwords.

Authenticating on an Active Directory (Kerberos)

Kerberos is different from other authentication methods. Instead of letting authentication take place between each client host and each server, Kerberos uses symmetrical encryption, KDC (Key Distribution Center) to authenticate users on a network.
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 the same, in order to pass through the Firewall.

Step 1: Interfaces

Authentication on the firewalls differs according to the interface on which traffic arrives.
The authentication feature can be enabled from internal or external interfaces, or both.

Allowing users to authenticate

From internal networks (protected interfaces)	If this option has been selected, identification on protected interfaces (represented by the icon) inside the company network is possible.
From public networks (external interfaces) (needed for SSL VPN)	Users can identify themselves on firewalls from unprotected interfaces. They may, for example, connect to a firewall from home, by going through the SSL VPN (See module VPN\SSL VPN).
From internal and public networks	If this option is selected, authentication will be possible from any interface.

Step 2: Authentication methods

If you wish to authenticate on an Active Directory, select the relevant option and click on **Next**.

Step 3: Kerberos method

Access to the Active Directory server (Kerberos method)

Domain name (Kerberos)	Domain name assigned to the Active Directory server for the Kerberos authentication method.
Server	You need to select an object corresponding to your Active Directory server from the drop-down list.

REMARK
You will skip **Step 4** of the configuration, relating to **Password management**, as the Kerberos authentication method does not require any specific configuration.

Step 5: Summary

Authentication configuration

This screen will allow you to finalize the configuration you have just completed for authentication.
For Kerberos, the summary will contain:
- The name(s) of the interface(s) from which authentication is allowed.
- The authentication method used
- The Kerberos domain name
- The name of the assigned server

If all the information is correct, click on **Finish.**

Authenticating on the internal directory (LDAP)

Step 1: Interfaces

Allowing users to authenticate:

From internal networks (protected interfaces)	If this option has been selected, identification on protected interfaces (represented by the icon) inside the company network is possible. These interfaces appear in the LAN, defining the local network or a host group belonging to the same organization ("In", "Dmz", etc.).
From public networks (external interfaces) (needed for SSL VPN)	Users can identify themselves on firewalls from unprotected interfaces. They may, for example, connect to a firewall from home, by going through the SSL VPN (See module VPN\SSL VPN).
From internal and public networks	If this option is selected, authentication will be possible from any interface.

Step 2: Authentication methods

If you wish to authenticate on an internal directory (LDAP method), select the relevant option and click on **Next**.

Step 3: User enrolment

Allow access to the captive portal and enrolment from protected networks (internal interfaces)	By selecting this option, you will enable authentication on internal interfaces, and you will allow unknown users to access your directory, to register and to fill in account creation request forms. **NOTE** During the creation of a new user, SHA will be used by default for storing passwords.

Step 4: Password management

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. The field **Lifetime** appears below, allowing you to indicate the number of days the password will remain valid.

Step 5: Summary

Authentication configuration

This screen will allow you to finalize the configuration you have just completed for authentication.
For the internal directory, the summary will contain:
- The name(s) of the interface(s) from which authentication is allowed.
- The authentication method used
- The status of the enrolment option (**Enabled** or **Disabled**)
- The type of password management selected (See *Step 4*)

If all the information is correct, click on **Finish.**

Authenticating on a RADIUS base

RADIUS is a standard authentication protocol functioning in client-server mode which allows defining remote users' network access. This protocol is equipped with a server linked to an identification database (e.g. LDAP directory). The NETASQ Firewall can act as a RADIUS client and 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.

Step 1: Interfaces

Allowing users to authenticate:

From internal networks (protected interfaces)	If this option has been selected, identification on protected interfaces (represented by the icon) inside the company network is possible.
From public networks (external interfaces) (needed for SSL VPN)	Users can identify themselves on firewalls from unprotected interfaces. They may, for example, connect to a firewall from home, by going through the SSL VPN (See module VPN\SSL VPN).
From internal and public networks	If this option is selected, authentication will be possible from any interface.

Step 2: Authentication methods

If you wish to authenticate on a RADIUS base, select the relevant option and click on **Next**.

Step 3: Radius server

Access to the RADIUS base:

Server	Select an object corresponding to your RADIUS server from the drop-down list.
Pre-shared key	Password that enables access to the server of your RADIUS base.

Step 5: Summary

Authentication configuration

This screen will allow you to finalize the configuration you have just completed for authentication.
For the RADIUS base, the summary will contain:
- The name(s) of the interface(s) from which authentication is allowed.
- The authentication method used
- The name of the server
- The pre-shared key displayed in plaintext

If all the information is correct, click on **Finish.**

"General" tab

Enabling the captive portal

By selecting this option, you will enable the Authentication module and allow authentication via a web form from protected and/or public interfaces.
You may specify from which interface(s) you wish to allow access by selecting one of the following options:

Only from internal (protected) interfaces	If this option has been selected, identification only on protected interfaces (represented by the icon) inside the company network is possible.
Only from external (public) interfaces	Users can only identify themselves on firewalls from unprotected interfaces. They may, for example, connect to a firewall from home, by going through the SSL VPN (See module VPN\SSL VPN).
From internal and external interfaces	If this option is selected, authentication will be possible from any interface.

REMARK
If the option **Enable the captive portal** has not been selected, the fields above would be grayed out.

Captive portal: SSL access

Certificate (private key)	By default, the CA that the firewall's authentication module uses is the firewall's own CA, and the name associated with this CA is the product's serial number. Thus, when a user attempts to contact the firewall other than by its serial number, it will receive a warning message indicating incoherence between what the user is trying to contact and the certificate it is receiving. By clicking on the icon , the CA configuration screen will appear (server certificate).

Advanced properties

User authentication

This section will allow customizing the identification process with the selection of several options:

Interrupt connections once the authentication period expires	As soon as the authentication duration expires, connections will be interrupted, even if the user is in the middle of a download.
Use the firewall account to check user authentication on the directory	If this option is selected, the firewall will connect to the internal LDAP base in order to check user data.
Authenticate directly on the directory with the user account	The user will connect to the directory on his own by going through the firewall, entering his login and password.
Use firewall name or certificate CN as FQDN	This option allows redirecting to the authentication portal by using the name of the firewalls if it has been defined or the CN of a certificate if it has been configured. As a last resort, you may use the product's serial number.

Proxy configuration file (.pac)

This field allows sending to the firewall the .pac file, which represents the proxy's automatic configuration file (Proxy Auto-Config), to be distributed. Users can retrieve .pac files or check their contents by clicking on the button to the right of the field.
Users can indicate in their web browsers the automatic configuration script located at https://if_firewall>/config/wpad.dat.

Captive portal

Hide the NETASQ logo	This option makes it possible to hide the NETASQ banner when the user authenticates on the captive portal, for confidentiality reasons.

"Available methods" tab

This tab comprises 3 sections:

- The column on the left listing the authentication methods, including the allowed interfaces.
- The column on the right displaying configuration options for the selected authentication method.
- The redirection method for the HTTP proxy.

Authentication methods

The button **Add and authentication method** opens a drop-down list that offers a choice of 5 authentication methods, which you can **Delete** when necessary:

LDAP

The configuration of this method is automatic and requires the implementation of an LDAP base, in the menu Users\Directory configuration.

Certificate (SSL)

After having selected your authentication method from the left column, you may enter information about it in the right column, which sets out the following elements:

Certificate authorities (C.A)

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 create 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 root authority on the Firewall.

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 the CAs. (See *Certificates and PKI*) 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 root authorities, so if the certificate of the user to be authenticated 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 root authority. 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.
Delete	Deletes the selected certification authority.

Certificate authority (C.A): This field displays the certificates you wish to trust and which you will use.

RADIUS

After having selected your authentication method from the left column, you may enter information about it in the right column, which sets out the following elements:

Access to the server

When the RADIUS method is selected, RADIUS authentication will be enabled. This menu will allow you to specify information relating to the external RADIUS server used and a backup RADIUS server. For each of them, the configuration requires the following information:

Server	IP address of the RADIUS server.
Port	Port used by the RADIUS server, in the event the main server fails.
Pre-shared key	Key used for encrypting exchanges between the firewall and the RADIUS server.

Backup server

Server	IP address of the backup server.
Port	Port used by the backup server, in the event the main server fails.
Pre-shared key	Key used for encrypting exchanges between the firewall and the backup server.

REMARK

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.

Kerberos

After having selected your authentication method from the left column, you may enter information about it in the right column, which sets out the following elements:

Domain name (FQDN)	Domain name assigned to the Active Directory server for the Kerberos authentication method. Defining this domain name allows masking the server's IP address and simplifying the search for it. Example: ***www.netasq.com***: ***netasq.com*** represents the domain name, which is more legible than its corresponding IP address: 91.212.116.100.

Access to the server

Server	IP address of the server for the Kerberos authentication method (*Active Directory* for example)
Port	Port used by the server.

Backup server

Server	IP address of the backup server for the Kerberos authentication method
Port	Port used by the backup server.

Transparent authentication (SPNEGO)

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 he accesses the internet (requiring authentication in the filter policy on the Firewall) with a web browser (Internet Explorer, Firefox, Mozilla).
SPNEGO can be configured on the firewall with the options explained in the table below:

Service name	The firewall's serial number is recommended instead of its name for the authentication (this name corresponds to the name indicated in the NETASQ script that comes with the installation instructions). The serial number will be prefixed by "HTTP/". **Example** HTTP/U70XXAZ0899020
Domain name	Kerberos server's domain name. This domain name corresponds to the full name of the Active Directory domain. It has to be entered in uppercase.
KEYTAB	This field represents the shared secret, generated when the script is used on Active Directory. This secret has to be provided to the firewall so that it can communicate with Active Directory. You must execute the KEYTAB generation script: ***spnego.bat*** with strict case sensitivity. This script is available on NETASQ's website or in your firewall's administration CD-ROM.

Interfaces allowed

Internal	Allows enabling or disabling the authentication method selected on the internal interface.
External	Allows enabling or disabling the authentication method selected on the external interface.

REMARK

Enabling these fields will add the selected authentication method to the drop-down list in the **Authentication** column in the menu Users\Access privileges\User configuration tab.

Redirection method for the HTTP proxy

When a default redirection method (SRP, Certificate or SPNEGO) is enabled for the HTTP proxy, the SSO feature for this method will also be enabled. This means that once you have entered your login/password, you no longer need to identify yourself the next time you connect, as they will be stored and automatically applied.

Internal interfaces	This field requires the definition of an SSL and SPNEGO authentication method, and the selection of the method to apply for the HTTP proxy to the internal interfaces.
External interfaces	This field requires the definition of an SSL and SPNEGO authentication method, and the selection of the method to apply for the HTTP proxy to the external interfaces.

"Internal interfaces" tab

User passwords

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. The field **Lifetime** appears below, allowing you to indicate the number of days the password will remain valid. **NOTE** 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 25 November 2010, the password has to be changed from 12.00 midnight on 26 November 2010 and not 24 hours later.

Authentication periods allowed

Minimum duration	Minimum duration for which the user can be authenticated, in minutes or in hours (up to 24 hours).
Maximum duration	Maximum duration for which the user can be authenticated, in minutes or in hours (up to 24 hours).
For transparent authentication	This SSO-based (Single Sign-On) authentication method allows defining the duration for which the firewall will not request any transparent re-authentication.

Advanced properties

Allow access to the .PAC file from internal interfaces	By selecting this option, you will be authorizing the publication of the .pac file on the internal interfaces. The publication of the .pac file is also possible on external interfaces.

User enrolment

NETASQ offers web-based user enrolment. If the user attempting to connect does not exist in the user database, he may request the creation of his account via web enrolment.

Do not allow user enrolment	If this option is selected, no “unknown” users will be able to register or create accounts with the LDAP directory.
Allow web enrolment for users	A user account has to be created in order for this option to be functional. If this option is selected, any user who attempts to connect and who does not exist in the user database will be able to request the creation of his account by filling in a web form. The administrator will then be able to confirm or deny his request.
Allow web enrolment for users and create their certificates	If this option is selected, users will not only be able to request the creation of their accounts if they do not exist in the user database, but they will also be able to request the creation of a certificate.

Notification of a new enrolment

This option allows new enrolled users to be informed of the creation of their accounts in the user database.

Do not send any e-mail	By default, the drop-down list will show that no e-mails will be sent to the administrator to inform him of enrolment requests. You can also define a group of users to whom enrolment requests will be sent in the menu Notifications\E-mail alerts\Recipients. Once this group has been created, it will automatically be included in the drop-down list and will be able to receive requests if you select it.

Map user/IP address

Allow multiple users to authenticate from the same IP address	If this option has been selected, several logins can be saved on the same IP address. The users’ actual addresses are hidden by a single IP address. (see **Security Policy \Filtering and NAT**).
Prohibit simultaneous authentication of a user on multiple hosts	This option makes it possible to prevent a user from authenticating on several computers at the same time. By enabling this option, his multiple requests will automatically be denied.

Expiry of the HTTP cookie

Managing cookies for user authentication on the firewalls allows securing authentication by preventing replay attacks for example, given that the connection cookie is necessary in order to be considered authenticated.

Cookies are essential for the option **Allow multiple users to authenticate from the same IP address**.
The web browser negotiates cookies, therefore if authentication is carried out with Internet Explorer, it will not be effective with Firefox or other web browsers.

At the end of the authentication period	The HTTP cookie expires by default **At the end of the authentication period**, meaning that it is negotiated only once throughout the whole duration of the authentication.
When a session is shut down	The cookie will be negotiated every time a request is sent to your web browser.
Do not use (not recommended)	It is possible to function without using the HTTP cookie, but this option is not recommended as it compromises the security of the authentication.

"External interfaces" tab

User passwords

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. The field **Lifetime** appears below, allowing you to indicate the number of days the password will remain valid.

Authentication periods allowed

Minimum duration	Minimum duration for which the user can be authenticated, in minutes or in hours (up to 24 hours).
Maximum duration	Maximum duration for which the user can be authenticated, in minutes or in hours (up to 24 hours).
For transparent authentication	This SSO-based (Single Sign-On) authentication method allows defining the duration for which the firewall will not request any transparent re-authentication.

Advanced properties

Allow access to the .PAC file from external interfaces	By selecting this option, you will be authorizing the publication of the .pac file on the external interfaces. The publication of the .pac file is also possible on internal interfaces.

User enrolment

Do not allow user enrolment	If this option is selected, no “unknown” users will be able to register or create accounts with the LDAP directory.
Allow web enrolment for users	A user account has to be created in order for this option to be functional. If this option is selected, any user who attempts to connect and who does not exist in the user database will be able to request the creation of his account by filling in a web form. The administrator will then be able to confirm or deny his request.
Allow web enrolment for users and create their certificates	If this option is selected, users will not only be able to request the creation of their accounts if they do not exist in the user database, but they will also be able to request the creation of a certificate.

Notification of a new enrolment

Do not send any e-mail	By default, the drop-down list will show that no e-mails will be sent to the administrator to inform him of enrolment requests. You can also define a group of users to whom enrolment requests will be sent in the menu Notifications\E-mail alerts\Recipients. Once this group has been created, it will automatically be included in the drop-down list and will be able to receive requests if you select it.

Map user/IP address

Allow multiple users to authenticate from the same IP address	If this option has been selected, several logins can be saved on the same IP address. The users’ actual addresses are hidden by a single IP address. (see **Security Policy \Filtering and NAT**).
Prohibit simultaneous authentication of a user on multiple hosts	This option makes it possible to prevent a user from authenticating on several computers at the same time. By enabling this option, his multiple requests will automatically be denied.

Expiry of the HTTP cookie

At the end of the authentication period	The HTTP cookie expires by default **At the end of the authentication period**, meaning that it is negotiated only once throughout the whole duration of the authentication.
When a session is shut down	The cookie will be negotiated every time a request is sent to your web browser.
Do not use (not recommended)	It is possible to function without using the HTTP cookie, but this option is not recommended as it compromises the security of the authentication.

BLOCK MESSAGES

The configuration screen for the **Block messages** module comprises 2 sections:

- The **Antivirus** tab: detection of viruses attached to documents, which may arise when sending or receiving e-mails (POP3, SMTP) or through file transfers (FTP).
- The **HTTP block page** tab: page that appears during an attempt to access a website that has not been allowed by the filter rules.

Antivirus tab

POP3 protocol

Contents of the e-mail	This field allows modifying the text of the message received when a virus is detected in an e-mail. **Example:** *Your NETASQ Firewall has detected a virus in this e-mail, it has been cleaned by the embedded antivirus. Infected attachments might have been removed.*

SMTP protocol

SMTP error code	Restricted to 3 digits, this field allows defining the error code that the SMTP server will receive when a virus is detected in a sent e-mail. **Example:** *554*
Accompanying message	This field contains the message that will be sent to the SMTP server when a virus is detected. **Example:** *5.7.1 Virus detected*.

FTP protocol

FTP error code	Restricted to 3 digits, this field contains the error code that the user or the FTP server will receive when a virus is detected in a transferred file. **Example:** *425*
Accompanying message	This spot is reserved for the message that will be sent with the error code when a virus is detected while sending/receiving a file to/from an FTP server. **Example:** *Virus detected. Transfer aborted.*

"HTTP block page" tab

This window displays by default the HTTP block page during attempts to access a website blocked by the URL filter rules.
The default block page consists of an icon and a sentence explaining why the page has been blocked, as well as the URL group category that the unauthorized website falls under. As all aspects of this page can be modified, an icon, a sentence, or both, can be displayed.
Example:
The company's policy does not allow access to this page. It falls under the category: "Games".

Edit	This button allows customizing the HTTP block page by modifying the HTML code. By clicking on this button, a sheet appears below the default block window. This sheet allows, for example, changing the icon, text, font, color or size.

REMARK
Variables can be used to make the categories of the blocked sites dynamic:

- $rule: name of the category
- $host: name of the HTTP destination host (ex: **www.google.com**).
- $url: blocked URL

CERTIFICATES AND PKI

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.
NETASQ's PKI allows generating and issuing certificate authorities (CAs) as well as certificates. These contain a bi-key associated with information that may belong to a user, a server, etc. The aim of NETASQ's PKI is to authenticate these elements.

The window of the Certificates and PKI module consists of 3 sections:
- At the top of the screen, the different operations possible in the form of a search bar and buttons.
- On the left, the list of authorities and certificates.
- On the right, details concerning the authority or certificate selected earlier in the list on the left, as well as the information concerning the CRL and the configuration of the CA or sub-CA.

Possible operations

Search bar

Enter the name of the particular certificate or CA you are looking for if it exists.
The search field will list all certificates and CAs with names that correspond to the keywords entered.
Example:
If you type "a" in the search bar, the list below it will show all certificates containing an "a".

Filter

This button allows you to select the type of certificate to display and to view only items that are relevant to you. A drop-down menu will offer the following choices:

All	Represented by the icon  , this option allows displaying all existing authorities and certificates in the list on the left.
Certificate authorities	Represented by the icon  , this option allows displaying all existing authorities and sub-authorities in the list on the left.
User certificates	Represented by the icon  , this option allows displaying only user certificates and the CA that they depend on.
Server certificates	Represented by the icon  , this option allows displaying only server certificates and the CA that they depend on.
Smartcard certificates	Represented by the icon  , this option allows displaying only Smartcard certificates and the CA that they depend on.

Add

The Certificates and PKI module window makes it possible to **Add** several types of authorities:

For each of them, a wizard will appear so that the authority's properties can be defined.

From version 9.0.1 onwards, You can now add CRLDP (CRL distribution points) for CAs imported via the GUI..

Delete

This button relates to the left column. Select the item from the list of CAs, sub-CAs or certificates that you wish to remove and click on **Delete**.

Download

This button allows you to download CAs, sub-CAs and certificates, by selecting them from the list on the left.

1) A window will open offering you the following options:

"**Open with – Browse**"
or
"**Save file**"

An certificate import wizard will then appear, if you have selected "Open with". It helps to copy certificates, list of trusted certificates and CRLs from your hard disk to the certificate library.

A certificate sent by a CA is a confirmation of your identity and contains information used in protecting your data and establishing secure network connections.

2) Click on **Next** and select the file to import.

3) Next, enter the password. Two options are available:

- Enable increased protection for private keys. You will be asked to enter the private key each time an application uses it, if you enable this option.
- Tag this key as exportable. This will allow you to save and send your keys later.

4) Click on **Next**, and you will access the certificate library. Windows may automatically select the certificate library, or you can specify the location of the certificate.

Two options are available:

- Automatically select the certificate library according to the type of certificate.
- Add all certificates to the following library: select the location by clicking on **"Browse"**.

5) Click on **Next**, you will reach the end of the certificate import wizard which summarizes the parameters that you have configured.

6) Click on **Finish**. A "Security warning" screen may appear and ask you to confirm the installation of your certificate (this will depend on your Windows configuration or your OS).

From version 9.0.3 onwards, the 'downloads' menu will also offer the export of a certificate revocation list (CRL) in PEM or DER format.

NOTE

Any issues encountered during this procedure are beyond NETASQ's competence.

LDAP publication

This button allows you to publish a CA, sub-CA or certificate in a directory by selecting it from the list on the left.

Create a CRL

This button allows you to create a CRL for a CA, sub-CA or certificate in the list on the left.
You will need to enter the password protecting the CA, then click on **Create a CRL**.
If you wish to check that a CRL is up to date, enter the command "checkcrl –d".
For a CRL to be correctly entered, remember to indicate "http//" + FQDN + /ca.crl

NOTE

This icon on the top right side of the screen allows you to define one of the CAs as the "default" authority via a confirmation window: to do this, select the desired CA and select "default". You can also "Check usage" for your CA.

If it is already in use in a module, you will see it appear in the directory of modules on the left.

Set as default

This button allows defining the default certificate authority that the firewall should use.

Check usage

You can look for the features or modules that use the selected certificate.

Adding authorities and certificates

The **Add** button has a drop-down list offering 6 options that will enable the creation of an authority or a certificate, via a wizard.

Adding a root authority

A root authority or “root CA” is an entity that signs, sends and maintains certificates and CRLs (*Certificate Revocation Lists*).
You will need to define the properties of the authority you wish to add:

WARNING
This information cannot be modified after the creation of the authority is confirmed.

CN	Enter a name that would allow you to identify your root authority, limited to a maximum of 64 characters. This name may refer to an organization, a user, a server, a host, etc. **Example** *NETASQ* **NOTE** This field has to be entered in order to continue the configuration.
ID	Even though this field is not mandatory, you can indicate here a shortcut to your CN, which will come in handy for your command lines. **Example** If you had selected a first name and last name for your CN, the ID may indicate just the initials.

Select the parent CA (if necessary)

Selecting a parent authority involves first entering the authority’s attributes in the fields below.

Parent CA	Even though a CA is made up of certificates, it can also involve sub-CAs that depend on it. A sub-CA can only be used after the identification of its “**Parent authority**” or CA.
Password for the parent CA	Define a password if you wish to indicate that you are indeed in charge of the parent CA.

Certificate authority attributes

During this step, you will need to enter general information regarding the authority that you wish to implement. The information entered will be found in your CA’s certificate and in your users’ certificates.

NOTE

For sub-CAs, these data are already pre-entered. And unless you modify the configuration, not all of this information can be modified later.

Organization (O)	Name of your company (e.g.: NETASQ).
Organizational Unit (OU)	"Branch" of your company (e.g.: INTERNAL).
Locality (L)	City in which your company is located (e.g.: Villeneuve d'Ascq).
State or province (ST)	State or province in which your company is located (e.g.: Nord).
Country (C)	Select from the list the country in which your company is located (e.g.: France).

Click on **Next**.

Next, you will need to secure access to your authority.
In this step of the PKI configuration wizard, you will need to enter a password that will allow you to protect your certificate authority's private key.

WARNING

You are advised against choosing passwords that are too easy. We recommend that you mix uppercase and lowercase letters with numbers and special characters.

Certificate authority password

Password (min. 8 char)	Enter a password of at least 8 characters in order to protect access to your CA. **NOTE** The firewall will not save this password. If you forget your password, you will need to reinitialize the PKI and as such, you will lose the configuration parameters that you had defined for it.
Confirm password	Type your password again in this field in order to confirm it.
Password strength	This field indicates your password's level of security: "Very weak", "Weak", "Moderate", "Good" or "Excellent". You are strongly advised to use uppercase letters and special characters.

E-mail address

Entering your e-mail address in this field will allow you to receive a message confirming that your authority has been created.

Key size (bytes)

When you create a CA, you need to provide a key in the form of a password in order to allow traffic to be encrypted. The larger the key, the more secure it is.
4 key sizes (in bytes) are available:

1024	If you select this key size, the password generated for your authority will be 1024 bytes. **NOTE** This number corresponds to 1024 characters visible in the console on your workstation.
1536	If you select this key size, the password generated for your authority will be 1536 bytes.
2048	If you select this key size, the password generated for your authority will be 2048 bytes.
4096	If you select this key size, the password for your authority should not exceed 4096 bytes. **WARNING** Even though large keys are more effective, you are advised against using this key with entry-level appliances such as the U30 as this will mean the key will take a long time to be generated.

NOTE

The computation of big keys may slow down your NETASQ appliance.

Validity (days)

This field corresponds to the number of days for which your certificate authority and consequently your PKI, will be valid. The date affects all aspects of your PKI as indeed, once this certificate expires, all user certificates will also expire. This value cannot be modified later.

NOTE

The value of this field must not exceed 3650 days.

Click on **Next**.

In this step of the wizard, you will need to enter the configuration regarding the distribution of the CRL (*Certification Revocation List*). This information will be embedded in the generated CAs and will allow applications that use the certificate to automatically retrieve the CRL in order to check the certificate's validity.

You can now manage your certificate revocations in the table that appears on the screen and enter the URLs that act as distribution points for revoked (invalid) certificates.

Add	When you click on this button, a new line will appear allowing you to enter a URL as a distribution point for certificate revocation lists. The first URL you enter will be numbered "1" and so on for the URLs that follow. The firewall will process items in the CRL according to their order of appearance on the screen.
Delete	Select the line to delete and click on this button to remove it from the list.
Up	Move your URL up one line in the order of priority in the table by clicking on this button. Repeat this operation until your URL reaches the number you wish to assign to it.
Down	Bring down your URL one or several places in the list using this button.

The following window sets out a summary of the information in your certificate.
Click on **Finish**.

You will now see in the left column of the Certificates and PKI screen the CA that you have just created, represented by the icon (which represents the default CA).
By clicking on the relevant CA, detailed information about it will be displayed on the right side of the screen in 3 tabs:

"Details" tab

This tab contains 4 sections setting out data concerning the "**Validity**" of the authority, its recipient ("**Issued for**"), its "**Issuer"** and its "**Fingerprint**" (information about the CA and its version).

"CRL" tab

Rounds up information regarding the CRL: its la validity including the last and next update, the table of distribution points and the table of revoked certificates which should contain a serial number, a revocation date and a reason for the revocation (optional).

From version 9.0.1 onwards, the maximum lifetime of certificates has been increased to ten years.

"Properties" tab

This tab presents the **Key size (bytes)** and the **Validity (days)** for the certification authority (including the **CRL validity (days)** for the CA, limited to a maximum of 3650 days), user certificates, Smartcard certificates and server certificates.

Adding a sub-CA

During the creation of a sub-CA, the windows are similar to those for the root CA. The configuration wizard for a sub-CA requires a "parent" reference from which it will copy information.
The CA selected as a reference for the sub-CA will be the default CA, or the last CA selected before clicking on "**Add a sub-CA**".

You will need to enter a CN and an ID to begin with. Next, enter the password of the parent authority in the field "**Password for the parent CA**". The icon  allows you to see the password in plaintext to check that it is correct.
Click on **Next**.

The screen that follows will ask for the password of your CA and a confirmation.
You can also enter your **E-mail address**, **Key size (in bytes)**, as well as the duration of your sub-CA's **Validity (in days)**.
You will then see a summary of the information entered.

NOTE

To view your sub-CA in the list to the left, expand the parent CA to which it is attached.
Click on **Finish**.

By clicking on the relevant sub-CA, detailed information about it will be displayed on the right side of the screen in 3 tabs:

"Details" tab

These 4 sections will contain the same data concerning the "**Validity**" of the authority, its recipient ("**Issued for**"), its "**Issuer"** and its "**Fingerprint**" (information about the product and its version).

"CRL" tab

Displays the same information regarding the CRL: its la validity including the last and next update, the table of distribution points and the table of revoked certificates which should contain a serial number, a revocation date and a reason for the revocation.

"Properties" tab

This tab presents the **Key size (bytes)** and the **Validity (days)** for the certification authority (including the **CRL validity (days)** for the CA, limited to a maximum of 3650 days), user certificates, Smartcard certificates and server certificates

Adding a user certificate

In the configuration wizard, the administrator will specify information relating to the user for whom he wishes to create a certificate, by entering the user's e-mail address.
Once the certificate has been generated and published by the administrator, the user will receive a confirmation e-mail that his certificate has been created and will be able to use it for logging on (if the e-mail sending option has been enabled).

NOTE

The user certificate also depends on a parent CA, and will therefore select the default CA. Click on the button **Add a user certificate**.

Name (CN) (mandatory)	Enter your user's name, limited to a maximum of 64 characters. **NOTE** This field has to be entered in order to continue the configuration.
ID	Even though this field is not mandatory, you can indicate here a shortcut to your CN, which will come in handy for your command lines. **Example** If you had selected a first name and last name for your CN, the ID may indicate just the initials.
E-mail address (mandatory)	In this field, enter the e-mail address of the user for whom you wish to create a certificate.

Next, you will need to specify various options for your user certificate.
The field "**Validity"** is set by default to 365 days, and the field **Key size** to 2048 bytes.

NOTE

To view your certificate created in the list to the left, expand the parent CA to which it is attached.

Publication in LDAP directory

You can choose to associate the user certificate with your LDAP database by selecting the option "**Publish this certificate in the LDAP directory"**.
If this option is selected, the certificate can be directly linked to its user if this user exists in the LDAP database and consequently make the Authentication process easier.

For this, the e-mail address specified during the creation of the user certificate in the wizard has to be the same as the address used in the user profile in the firewall's user database.

Password of the published PKCS#12	The PKCS#12 container is a certificate format. It contains the private key and the user certificate as well as the CA's certificate.

container (min. 8 char)	Enter a password in order to protect the data for the 3 items mentioned above.
Confirm password	Type your password again in this field in order to confirm it.
Password strength	This field indicates your password's level of security: "Very weak", "Weak", "Moderate", "Good" or "Excellent". You are strongly advised to use uppercase letters and special characters.

Click on **Next**.
The following windows set out the information about the pre-selected parent CA as well as a summary of the data in the user certificate.
Click on **Finish**.
By clicking on the relevant certificate, detailed information about it will be displayed on the right side of the screen in a single tab:

"Details" tab

These 4 sections will contain the same data concerning the "**Validity**" of the authority, its recipient ("**Issued for**"), its "**Issuer"** and its "**Fingerprint**" (information about the product and its version).

Adding a Smartcard certificate

The Smartcard certificate is linked to a *Microsoft Windows* account associated with a user and a certificate. It allows signing and issuing certificates that allow the authentication of registered users in the Active Directory (see document on Directory configuration (LDAP)\Connection to a Microsoft Active Directory), and also in your LDAP database.

NOTE

Each user will be assigned a Windows account. Consequently, each user is assigned a Smartcard certificate. The CA used must have defined CRLDPs.

Name (CN) (mandatory)	Enter a name for the Smartcard certificate, limited to a maximum of 64 characters.
ID	Even though this field is not mandatory, you can indicate here a shortcut to your CN, which will come in handy for your command lines. **Example** If you had selected a first name and last name for your CN, the ID may indicate just the initials.
E-mail address (mandatory)	In this field, enter the e-mail address of the user for whom you wish to create a certificate.
Main user name (Windows)	Enter the name of the owner of the Windows account for whom you wish to create a Smartcard certificate.

Proceed in the same way as for adding a user certificate:
Specify the various options for your Smartcard certificate. The field "**Validity"** is set by default to 365 days, and the field **Key size** to 1024 bytes.

You can then "**Publish this certificate in the LDAP directory**" by selecting the relevant option, and define a password that you will confirm for the PKCS#12 container.
After having clicked on **Next**, select a parent CA for your certificate and enter its password. You will see a summary of the data that was entered.
Click on **Finish**.
By clicking on the relevant certificate, detailed information about it will be displayed on the right side of the screen in a single tab:

"Details" tab

These 4 sections will contain the same data concerning the "**Validity**" of the authority, its recipient ("**Issued for**"), its "**Issuer"** and its "**Fingerprint**" (information about the product and its version).

Adding a server certificate

The server certificate is installed on a web server and allows providing a link between them.
In the case of a website, it allows checking that the URL and its DN (domain name) belong to the stated company.
Define the properties of the server certificate through the wizard.

Fully Qualified Domain Name (FQDN)	The FQDN represents the full name of a host in a URL, such as HOST (e.g. *www*) and a domain name (such as *netasq.com*). **Example** ***www.netasq.com***
ID	Even though this field is not mandatory, you can indicate here a shortcut to your FQDN, which will come in handy for your command lines. **Example** *NETASQ* (owner of the FQDN)

Proceed in the same way as for adding a user certificate or a Smartcard certificate:
Specify the various options for your server certificate. The field "**Validity"** is set by default to 365 days, and the field **Key size** to 2048 bytes.
You can then "**Publish this certificate in the LDAP directory**" by selecting the relevant option, and define a password that you will confirm for the PKCS#12 container.
After having clicked on **Next**, select a parent CA for your certificate and enter its password. You will see a summary of the data that was entered.
Click on **Finish**.
By clicking on the relevant certificate, detailed information about it will be displayed on the right side of the screen in a single tab:

"Details" tab

These 4 sections will contain the same data concerning the "**Validity**" of the authority, its recipient ("**Issued for**"), its "**Issuer"** and its "**Fingerprint**" (information about the product and its version).

Importing a file

By clicking on this button, you will import a file (containing your certificate) through the configuration wizard.
This will save you the hassle of having to go through the steps of creating the CA, sub-CA or certificates.

File to import	By clicking on the icon  , to the right of the field, you will be able to browser your computer or your web browser to look for a certificate (if you have created one earlier).
File format	3 file formats are suggested: • **Base64 format** (**PEM** - *Privacy Enhanced Mail*), It allows encoding X509 certificates in Base64. A PEM-type certificate may look like this: -----BEGIN CERTIFICATE----- MIIDdzCCAuCgAwIBAgIBBzANBgkqhkiG9w0BAQQFADCBpDELMAkGA1UEBhMCQ0gxCzAJBgNVBAgTAkdFMQ8wDQYD VQQHEwZHZW5ldmExHTAbBgNVBAoTFFVuaXZlcnNpdHkgb2YgR2VuZXZhMSQwIgYDVQQLExtVTklHRSBDZXJ0aWZpY 2F0ZSBBdXRob3JpdHkxETAPBgNVBAMTCFVuaUdlIENBMR8wHQYJKoZIhvcNAQkBFhB1bmlnZWNhQHVuaWdlLmNoMB 4XDTk5MTAwNDE2MjI1N1oXDTAwMTAwMzE2MjI1N1owgbExCzAJBgNVBAYTAkNIMQswCQYDVQQIEwJHRTEPMA0GA1 UEBxMGR2VuZXZhMR0wGwYDVQQKExRVbml2ZXJzaXR5IG9mIEdlbmV2YTEeMBwGA1UECxMVRGl2aXNpb24gSW5mb

	3JtYXRpcXVlMRowGAYDVQQDExFBbGFpbiBldWdlbnRvYmxlcjEpMCcGCSqGSIb3DQEJARYaQWxhaW4uSHVnZW50b2JsZXJAdW5pZ2UuY2gwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBALIL5oX/FR9ioQHM0aXxfDELkhPKkw8jc6I7BtSYJk4sfqvQYqvOMt1uugQGkyIuGhP2djLj6Ju4+KyKKQVvDJIu/R1zFX1kkqOPt/A2pCLkisuH7nDsMbWbep0hDTVNELoKVoVIAazwWMFlno2JuHJgUcs5hWskg/azqI4d9zy5AgMBAAGjgakwgaYwJQYDVR0RBB4wHIEaQWxhaW4uSHVnZW50b2JsZXJAdW5pZ2UuY2gwDAYDVR0T200BAUwAwIBADBcBglghkgBhvhCAQ0ETxZNVU5JR0VDQSBjbGllbnQgY2VydGlmaWNhdGUsIHNlZSBodHRwOi8vdW5pZ2VjYS51bmlnZS5jaCBmb3IgbW9yZSBpbmZvcm1hdGlvbnMwEQYJYIZIAYb4QgEBBAQDAgSwMA0GCSqGSIb3DQEBBAUAA4GBACQ9Eo67A3UUa6QBBNJYbGhC7zSjXiWySvj6k4az2UqTOCT9mCNnmPR5I3Kxr1GpWToH68LvA30inskP9rkZAksPyaZzjT7aL//phV3ViJfreGbVs5tiT/cmigwFLeUWFRvNyT9VUPUov9hGVbCc9x+v05uY7t3UMeZejj8zHHM+ -----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 Base64 framed by markers like "-----BEGIN X509 CRL-----" and "-----END X509 CRL-----". As for the private key file, it contains chains of coded characters in Base64 framed by markers like "-----BEGIN RSA PRIVATE KEY-----" and "-----END RSA PRIVATE KEY-----". • **Binary format** (**DER** - *Distinguished Encoding Rules),* containing the user's certificate in binary format. • **Container** (**PKCS#12**), containing the private key and the user certificate as well as the CA's certificate. Furthermore, it is encrypted.
File password (if PKCS#12)	Define a password for the PKCS#12 file, if this is the format you have chosen (the same as for publishing the user certificate in the LDAP). The icon  allows you to view the password in plaintext to check that it is correct.
Items to import	Given that each file format contains different items, you can choose to import a file or part of it through the following choices. **All:** Imports all items contained in your files. Or select only the following: **Certificate(s)** **Private key (s)** **CRL** **Certification authority (CA)** **Request(s)**
Overwrite existing content in the PKI	If you select this option, contents similar to the items above will be overwritten in the PKI, in favor of new certificates/private keys/CAs and requests.

Click on **Next**. You will see a summary of the data regarding the import of your file (its name, format and items to import).
Click on **Finish**.

CLI CONSOLE

This module will allow you to view executable commands on your appliance's CLI (Command Line Interface) console.
You can access it from the menu System\CLI.
This module consists of two sections:

- the list of commands in the upper part of the window, which is a text zone
- a data entry zone at the bottom of the window

List of commands

The window displays by default the 16 main executable commands that are part of the "HELP" category.

NOTE
By entering the "HELP" command in the data entry zone that we will see later, the list that summarizes the main commands will appear again.

The following are the visible commands:

AUTH	Used with the aim of avoiding spoofing, this command allows the user or the administrator to authenticate in total security.
CHPWD	Allows redefining the password if necessary.
CONFIG	Allows accessing the firewall's configuration features, which group 38 implicit commands (ACTIVATE CONFIG, ANTISPAM CONFIG etc., cf "Data entry zone").
GLOBALADMIN	Allows obtaining information about the system and consists of two implicit commands: GETINFOS and GETSTATUS.
HA	Allows accessing high availability features, grouping 8 commands.
HELP	This command, as indicated earlier, allows displaying the list of main executable commands.
LIST	Displays the list of connected users, by showing user privileges (by level) and privileges for the session in progress (SessionLevel).
LOG	Allows viewing the NETASQ multifunction firewall's activity logs, groups 6 commands.
MODIFY	This command is a specific privilege that allows the user to modify the configuration of a module, in addition to reading privileges.
MONITOR	Allows accessing features relating to MONITOR, contains 20 commands.
NOP	Does not perform any action and avoids disconnection from the server.
PKI	Allows displaying or downloading the PKI, groups 7 commands.
QUIT	Allows logging off.
SYSTEM	Groups 20 commands relating to the system.
USER	Groups 12 commands relating to the user.
VERSION	Allows displaying the version of the server.

Data entry zone

When you go to the CLI module, the focus is on the command entry field.
To the right of it, there are two buttons and a checkbox, which allow modifying certain actions:

Launch	This button allows launching the command that was entered manually. The command will also be launched when the user presses “Enter”. **NOTE** In the field for editing commands, you can browse through the various commands that have already been launched, using the Up/Down buttons. Command history is stored and re-used each time the web application is launched.
Clear display	This button allows erasing the list of commands displayed above it (cf “List of commands”). To view them again, enter the HELP command in the data entry zone and click on “Launch”.
Raw output	If this option is selected, the launch of the command will display the line of code in its raw form between markers.

NOTE
Most commands displayed in the list at the top of the page involve others. To view all these commands, proceed as follows:

1. Enter the command of your choice in the text entry zone.
2. Click on “Launch”.
3. Depending on the command you have selected, the list will display the additional commands included in it.

Example
If you enter the CONFIG command, all commands relating to it will appear on the screen.
To use one of these commands, enter “CONFIG” in the data entry zone, followed by a space and the desired command, such as: “CONFIG HA”.

CONFIGURATION

The configuration-administration screen consists of 3 tabs:

- General configuration: definition of the firewall's settings (name, language, keyboard), date and time settings and NTP servers.
- Firewall administration: configuration of access to the firewall's administration interface (listening port, SSH etc.)
- Network settings: configuration of the proxy server, VLAN restrictions and DNS resolution.

"General configuration" tab

The General configuration tab allows the modification of the following parameters:

General configuration

Firewall name	This name is used in alarm e-mails sent to the administrator and is displayed in the firewall's main window. Anything can be indicated for this name.
Firewall language (logs)	Choice of language, limited to **French** and **English**. This language is used for logs, syslog and the CLI configuration.
Keyboard (console)	Type of keyboard that the firewall supports. 5 layouts are available: **English, French, Italian, Polish, Swiss**.

Time configuration

Date	Firewall's date. Select the date from the calendar. This field will be grayed out if NTP configuration has been enabled.
Time	Firewall's time. This field will be grayed out if NTP configuration has been enabled.
Synchronize with your machine	By clicking on this button, the firewall will synchronize its time with your computer's time. This field will be grayed out if NTP configuration has been enabled.
Time zone	Time zone defined for the firewall (GMT by default). **WARNING** The firewall has to be restarted if the time zone is changed.
Synchronize firewall time (NTP)	NTP (*Network Time Protocol*) is a protocol that allows synchronizing the local clock on your computers with a time reference via your network. If this option is selected, your firewall will automatically be synchronized with the local time.

REMARK
The date and time to which your NETASQ firewall is set are important – they allow you to locate events in the log files. They are also useful in the scheduling of configurations.

List of NTP servers

This table can only be accessed if you have selected the option **Synchronize firewall time (NTP)**. If you have not done so, the list of NTP servers will be grayed out.

NTP servers (host or group-address range) (max 15)	The NTP server represents the remote clock with which your firewall will be synchronized. You can **Add** or **Delete** servers by clicking on the relevant buttons. When you click on **Add**, a new line will be added to the list of NTP servers. You may select an object from the drop-down list or create one by clicking on . It will then be possible to create a host, an IP address range or a group. Click on **Apply** after you have entered the data for the new object.
Password (ASCII)	Even though this is optional, you can enter a password for your NTP server which you can use for authentication.

"Firewall administration" tab

Access to the firewall's administration interface

Allow the 'admin' account to log in	The 'admin' account is the only account with all privileges. It can connect without using certificates and as such, force a connection. This option has to be selected if you wish to keep this privileged access. **WARNING** This account is to be considered "dangerous", in view of the extent of its configuration possibilities and the access privileges granted to it.
Listening port	This field represents the port on which you can access the administration interface (https, tcp/443 by default). **NOTE** You can create an additional listening port by clicking on . **WARNING** The object can only be of "TCP" type (not "UDP").
Enable protection from brute force attacks	Brute force attacks are defined by the repeated attempts to connect to the firewall, by testing all password combinations possible If this option is selected, you will prevent such attacks and enable the configuration of the two fields that follow, in order to restrict connection attempts.
Number of authentication attempts allowed	Number of authentication attempts allowed in the event of a connection failure (login/password error or case sensitivity, for example). By default, the number of attempts allowed is limited to 3.
Freeze time (minutes)	Duration for which you will not be able to authenticate or log on after the number of failed attempts specified above. The duration of the freeze may not exceed 60 minutes.

Access to firewall administration pages

Add a server	Select a server from the drop-down list of objects. This server will be treated as an **Authorized administration host** that will be able to log on to the administration interface. This object may be a host, host group, network or address range.
Delete	Select the line to be removed from the list and click on **Delete**.

Remote SSH access

Enable SSH access	SSH (*Secure Shell*) is a protocol that allows logging on to a remote host via a secure link. Data from host to host are encrypted. SSH also allows the execution of commands on a remote server. Select this option if you wish to connect remotely and securely in console mode. **NOTE** By selecting this option, you will enable the configuration of the two fields below it.
Enable password access	The password in question corresponds to the password for the "admin" account, as it is the only account that is able to connect in SSH. The "admin" will need to enter it in order to access the firewall via a remote host. You may also use a private/public key pair to authenticate.
Listening port	This field represents the port on which you will be able to access the administration interface (ssh tcp/22 by default). **NOTE** You can create an additional listening port by clicking on . **WARNING** The object can only be of "TCP" type (not "UDP").

"Network settings" tab

Proxy server

The firewall uses a proxy to access the internet	Select this option to enable the fields below it and to allow the firewall to use a proxy in order to access the internet securely. This field is used by ActiveUpdate and LicenceUpdate.
Server	This field allows specifying the object corresponding to the server that the firewall will use as a proxy.
Port	This field allows specifying the port used by the firewall to contact the proxy.
ID	This field allows defining an ID that the firewall will use to authenticate with a proxy.
Password	Define a password that you will need to enter in order to access the proxy server.

Limits

Available VLANs (max: 128)	Restriction on the number of VLANs available in the network configuration. The default number of available VLANs is 64, changing this number will cause your

	appliance to reboot.

DNS resolution

List of DNS servers used by the firewall

DNS servers allow the firewall to resolve (find out IP addresses based on a host name) objects or hosts configured in “Automatic” DNS resolution.

Add	Clicking on this button will add a new line to the table and will allow you to select a DNS server from the drop-down list.
Delete	Select the line to be removed from the table and click on **Delete**.
Up	Moves the selected line above the previous line.
Down	Moves the selected line below the next line.

DASHBOARD

The dashboard provides an overview of the information concerning your firewall. It is represented by this icon  and is divided into 2 sections:

- The module configuration menu on the left, containing 4 collapsible tabs that can be personalized according to your needs: “My favorites”, “Configuration”, “Objects”, “Users and groups”. A search bar is available for the last 3 modules.
- A dynamic area at the center, containing 9 modules or widgets:

Network
Alarms
Resources
License
Hardware
Properties
Active Update
Service
Interfaces

By default, each one of these windows is updated dynamically. The most recent components are downloaded automatically and are displayed on the screen.

The module configuration menu

This retractable column (button) is divided into 4 collapsible sections. They will allow you to personalize your interface and configure your modules.

My favorites

This section is closely linked to the “pin” icon: .
When you come across this icon at the top right of each module, select it if you want it to be added to your favorites.

Configuration

This section is presented as a directory of the menus and their modules, with a keyword search bar.
9 sub-menus are available (click on them to expand):

- Dashboard
- System (containing 7 modules: Configuration, Administrators, License, Maintenance, Active Update, High availability, CLI console)
- Network (containing 5 modules: Interfaces, Routing, Dynamic DNS, DHCP, DNS cache proxy)
- Objects (containing 4 modules: Network objects, Web objects, Certificates and PKI, Time objects)
- Users (containing 5 modules: Users, Access privileges, Directory configuration, Authentication, Enrolment)

- Security policy (containing 6 modules: Filtering and NAT, URL filtering, SSL filtering, SMTP filtering, Quality of service, Implicit rules)
- Application protection (containing 6 modules: Alarms, Protocols and Applications, Inspection profiles, Vulnerability detection, Antivirus, Antispam)
- VPN (containing 3 modules: IPSec VPN, SSL VPN, PPTP server)
- Notifications (containing 5 modules: Logs - syslog, SNMP agent, E-mail alerts, System events, Block messages)

NOTE

If certain modules are grayed out, this means that you have not subscribed to the required license and therefore cannot access them.

This can also mean that the connected user does not have the necessary privileges for accessing these menus

The icon allows personalizing the display of your directory:

This provides a partial view of your directory, displaying only the menus.

This provides a full view of your directory, displaying the menus and their modules.

The dynamic area: widgets

In this area, you will be able to view certain updates on your firewall such as the latest alarms raised or the expiry dates of your licenses.
9 windows are shown, each with a toolbar at the top right corner, including the full dashboard module.
The possible actions that can be performed with these tools are:

Enlarge	Represented by the icon , this tool allows adding a column to the dashboard module and enlarging the window for widgets.
Reduce	Represented by the icon , this tool allows deleting a column from the dashboard module and minimizing the window for widgets.
Close	Represented by the icon , this tool allows closing your widget.
Refresh	Represented by the icon , this tool allows you to refresh the data on the dashboard or the widget concerned.
Open	Represented by the icon , this tool opens the module associated with the widget you are browsing and as such, closes the dashboard.
Dashboard configuration	Represented by the icon , this tool allows you to select the **Components** you wish to display on the dashboard, through a series of checkboxes. You can also configure the **Update frequency** of the widgets: “Manual only” (you will need to click on the “Refresh” ( ) icon systematically) , “Every minute” or “Every 5 minutes”.
Add to favorites	Represented by the icon , this tool allows you to add the Dashboard module to “**My favorites**” in the directory on the left (see section *The module configuration menu*).

Network

This window displays the model of your NETASQ multifunction firewall as well as the number of interfaces available on it (32 maximum).
The used interface(s) appears in green and a tooltip containing information about each interface is available.
The following information is given:

Name	Name of the interface used (“in”, “out” or “dmz”), accompanied by its IP address and subnet mask.
Network packets	The number of Accepted, Blocked, Fragmented, TCP, UDP and ICMP packets.
Traffic received	The total and individual breakdown of TCP, UDP and ICMP packets received.
Traffic sent	The total and individual breakdown of TCP, UDP and ICMP packets sent.
Throughput	Current incoming and outgoing throughput.

Alarms

This window contains the list of the last 50 alarms raised by the firewall.

Date	Date and time of the last alarms raised, arranged from the most recent to least recent.
Priority	3 levels of priority are possible and can be configured in the module Application Protection /Alarms.
Source	IP packet or connection that raised the alarm.
Destination	Address of the intended destination before the alarm was raised.
Message	Comment associated with the selected alarm. **Examples of possible messages** “Invalid *ICMP message (no TCP/UDPlinked entry)*” (minor priority). “*IP address spoofing (type=1)*” (major priority).
Online help	Select the desired alarm and click on this link, which will lead you to a help page relating to the message (see above).
Action	When an alarm is raised, the packet that caused the alarm will receive the specified action. The actions are “Block” or “Pass”.

From version 9.0.1 onwards, this section of the dashboard will contain a new button ( ) allowing you to “Clear screen”, or delete information logs.

Resources

This window provides a graphic view of hardware resources relating to your firewall.

Space used	Percentage of space used for the firewall’s logs.
CPU	Percentage of your processor’s use.
Temperature	Temperature of your appliance. This information is not available on virtual machines.
Memory	Memory used by your appliance: **Host**: percentage of memory allocated by hosts (bytes). **Fragmented**: percentage of memory allocated by fragments (or folders that are too big

	and fragmented – in bytes). **Connection**: percentage of memory allocated for various connections (bytes). **ICMP:** percentage of memory allocated for ICMP (bytes). **Logs:** percentage of memory used for DataTracking. **Dynamic**: memory in which a computer puts its data while they are processed.

License

This window displays the various values of your license and their update deadlines.

Update	Deadline for updating the appliance.
Pattern	Expiry date for ASQ templates.
Antivirus	Deadline for updating ClamAV and Kaspersky antivirus databases.
VulnBase	Deadline for updating NVM (NETASQ Vulnerability Manager) vulnerabilities.
VirusVendor	Deadline for updating Kaspersky antivirus databases.
URLFiltering	Enables or disables URL filtering via the NETASQ database in the proxy. (Default value: 1).
AntiSPAM	Enables or disables spam filtering via DNSBL in the proxy. (Default value: 1).

From version 9.0.2 onwards, the License widget offers a view by expiry date.

Hardware

This window sets out the various hardware data of your appliance.

High availability	Checks the integrity of the high availability cluster (licenses, configuration, synchronization, active member).
Hardware	Presence or absence of a USB key on the system (secure configuration for the module System\Maintenance).
RAID	Status of the RAID (redundant set of independent or low-value hard disks) and of its disks, if the option is available on the hardware. ***From version 9.0.1 onwards,*** an alarm will appear if a disk is defective or missing.

Properties

This window shows the data essential to the configuration of your firewall.

Properties

Serial number	Your NETASQ firewall's reference.
Date	Date and time in real time.
Backup partition	Absence or presence of a backup partition on your system (cf Menu System\module Maintenance\tab Configuration).
Uptime	Duration for which the firewall has been running uninterrupted.

LDAP configuration	Status of the connection with the LDAP.

Policy

Filter	Profile applied for the filter and NAT policy.
VPN	Status of the von on your network.

Active Update

Object name	Name of the listed module.
Status	Whether the module is up to date.
Last update	Date and time of the last update.

Services

Services	List of the various services available on the appliance.
Uptime	Duration for which the service has been running uninterrupted.
% CPU	Status of the service.

Interfaces

Object name	Name of the in, out or dmz interface.
Type	This may be a physical interface (ethernet), VLAN, or modem (dialup)
Address	IP address and subnet mask of the interface.
Incoming throughput	Incoming traffic in KB.
Outgoing throughput	Outgoing traffic in KB.

From version 9.0.1 onwards, disabled interfaces will be displayed in the Dashboard.

DHCP

The configuration screen for the DHCP service comprises 5 tabs:

- **General**: Enables the DHCP service in 2 specific modes: server or relay.
- **Server settings** (followed by “inactive” if the option **Enable service** has not been selected in the **General** tab or if the Relay mode was selected in the **General** tab). This menu is reserved for the configuration of the addresses of various servers: “Gateway”, "DNS", "E-mail" (**SMTP** and **POP**), "Time" (**NTP**), News and TFTP server. These addresses are automatically sent to the stations so that they can contact the corresponding servers.
- **Address range** (followed by “inactive” if the Relay mode was selected in the **General** tab). For each range, you will need to specify a group of addresses that will be assigned to users. The address will be allocated for the duration determined in the global configuration.
- **Host** (followed by “inactive” if the Relay mode was selected in the **General** tab). For each host, the address assigned by the service will always be the same: the address indicated in the **Host** menu. This is in fact a “static” address range but which allows releasing the client workstation from its network configuration.
- **Relay settings** (followed by “inactive” if the Relay mode was not selected in the **General** tab).

The “General” tab

Enable service: Enables or disables the fields in either “Server” or “Relay” mode.

DHCP server	Sends various server configurations to DHCP clients. These servers will be used only if the DHCP software program requests for it. If this option is selected, the Relay settings tab will switch to “inactive” mode.
DHCP relay	The DHCP relay should be used when client requests are to be redirected to an external DHCP server. If this option is selected, the Server settings, Address range and Host tabs will switch to “inactive” mode.

“Server settings” tab

In this section, global settings such as the **domain name** that hosts will use, **DNS servers**, etc can be configured.

Domain name	Domain name used for the definition of users.
Default gateway	The default gateway is the default route used if no other route has been specified for the client’s or network’s address.
Primary and secondary DNS	Sends the addresses of the primary and secondary DNS servers to DHCP clients. These servers are mandatory in almost every DHCP configuration. If the firewall obtains the IP address of one of its interfaces via DHCP, DNS servers obtained by the firewall can be defined with the access provider. To do so, enable the option **Request domain name servers from the DHCP server and create host**

	objects in the module Network\Interfaces\Advanced configuration for the relevant interface. Next, use the objects “Firewall_<interface_name>_dns1” and “Firewall_<interface_name>_dns2” in these fields.

Advanced properties

WINS server	Sends the WINS server’s address to DHCP clients. WINS is a Microsoft NETBIOS name server (NBNS). WINS eliminates the need to broadcast data in order to resolve host names according to their IP addresses.
SMTP server	The SMTP server is used for sending e-mails. Right-clicking on this field selects the server.
POP3 server	The POP3 server is used for receiving e-mails. Right-clicking on this field selects the server.
NTP server	This field allows sending the NTP server’s address to DHCP clients. If clients have been configured to synchronize their NTP clocks, this server has to be used as a time reference.
News server (NNTP)	This field allows sending the news server’s address to DHCP clients. This server provides the NNTP service, which allows clients to read Usenet news.
TFTP server	The TFTP server is used for booting hosts remotely. This field can be used for starting up network appliances such as routers, X-terminals or workstations without hard disks.
Distribute the web proxy autodiscovery (WPAD) file	Allows the server to distribute the proxy configuration through the .pac file to DHCP clients who request addresses. The .pac file is sent in the DHCP response (option 252: WPAD-URL). If this option is selected, the user will be informed that he will need to enable sharing on internal and/or external interfaces in the authentication window. *(Cf. Authentication).*
Update DNS server entries	Selected by default. Dynamic update of the DNS. When information contained by the DHCP server is modified, the primary DNS server is updated dynamically.

Assigned lease time

Default (Hour)	In order to optimize network resources, IP addresses are assigned for a limited period. The default duration for which stations will keep the same IP addresses has to be defined here.
Minimum (Hour)	Minimum duration for which stations will keep the same IP address.
Maximum (Hour)	Maximum duration for which stations will keep the same IP address.

“Address range” tab

GENERAL NOTE

In this tab, you will see the icon  that will allow you to **Add** items to your tables, and this icon  to **Delete** them.
In order for a DHCP server to provide IP addresses, a pool of addresses has to be defined, from which the DHCP server can take addresses.

Address range	It is possible to instruct the server to provide IP addresses only in the address ranges defined by the lines “dhcp_range” in this column. To do so, select a “range” in the object database in the drop-down list, by clicking on the arrow to the right of the cell.
Gateway	If the gateway associated with the defined address range is “auto”, the default gateway will be used. You can define another gateway by selecting it in the object database, which will appear by clicking on the arrow on the right side of the cell.

WARNINGS

Ranges cannot overlap. An address range belongs to a single bridge/interface. A host cannot be defined in a range. The gateway defined for a network belongs to this network.

“Host” tab

The **Host** tab allows declaring hosts that the DHCP needs to know and applying a particular configuration to them.
In this tab, a default IP address and gateway can be defined. This configuration resembles a static address range but nothing is indicated on the client workstation. This simplifies the management of allocated addresses and the configuration of client workstations.
The table shows the host and gateway. Click on the arrow to the right of each cell to select the object from the base.

WARNINGS

You need to select objects that already have a configured MAC address.

The IP address must not fall within the address range defined in the Address range tab.
The IP address has to be in the address range of the interface(s) belonging to the firewall that assigns IP addresses in DHCP.

“Relay settings” tab

The DHCP relay is used when you wish to redirect client requests to an external DHCP server.

DHCP server(s)	Enter the IP address of the DHCP relay.
DHCP relay queries for all interfaces.	The relay listens on all interfaces.

Listening interfaces on the DHCP relay service

Add and delete interfaces involved in the relay.

WARNINGS

Listening interfaces must include interfaces for listening on requests on the client’s side as well as listening interfaces for the response on the server’s side.
The DHCP server has to be configured in such a way that it can distribute IP addresses to clients that pass through the relay.

DIRECTORY CONFIGURATION (LDAP)

LDAP is a standard protocol that allows managing directories, i.e., accessing user databases on a network through the TCP/IP protocols.
NETASQ firewalls embed an internal LDAP database, which stores information relating to users who need to authenticate in order to go through the firewall. However, it is also possible to connect the firewall to an external LDAP database located on a remote host.
The Directory configuration module (accessible through the menu Users\Directory configuration) contains a wizard in the first page, offering you the choice of a directory and initializing it.

- Connection to a Microsoft Active Directory
- Connection to an external LDAP directory
- Connection to an internal LDAP directory

Depending on your selection, the next step will vary, as the configuration of the external LDAP requires more information.
The configuration of each of these directories consists of 3 steps. Select the LDAP database you wish to create by clicking on the relevant option.

Creating an internal LDAP

This type of directory is hosted by your NETASQ multi-function firewall, and your information is stored in it once the LDAP directory is created.

Step 1: Selecting the directory

As indicated above, the LDAP database option has to be selected in order to confirm your choice. This is the first step in the configuration of a directory.
Select the option **Connect to an internal LDAP directory** and click on **Next.**

Step 2: Accessing the directory

In this second step, you will need to enter general information concerning the LDAP database that you wish to create. The information entered here will reappear in your firewall's LDAP directory schema.

Organization	Name of your company (e.g.: NETASQ).
Domain	The country in which your company is located (e.g.: fr).
Password	Definition of the NetasqAdmin password.
Confirm	Confirmation of the LDAP administration password that you have just entered in the previous field.
Password strength	This field indicates your password's level of security: "Very weak", "Weak", "Moderate", "Good" or "Excellent". You are strongly advised to use uppercase letters and special characters.

NOTE
Only the password can be modified later, after you have configured your internal LDAP.

Click on **Next** to go on to Step 3.

Step 3: Authentication

Now that your internal directory has been defined, this screen will allow you to authorize access to the LDAP database and to enable options relating to authentication. 3 services are offered:

Allow access to the LDAP database	This option allows making the LDAP directory public.
Allow access to the captive portal from protected networks (internal interfaces)	While this is restricted to internal interfaces, if this option is selected, you will enable authentication on the captive portal. This is the "internal interface" equivalent of the option **Enable the captive portal** in the Authentication module (in the menu Users\Authentication).
Enable user enrolment through the web portal	If this option is selected, users who do not have accounts to authenticate on the firewall may fill in an enrolment request form on the captive portal. **NOTE** The enrolment request must be endorsed by the administrator before the account can be activated. Requests may be accepted or denied by the administrator.

Click on **Finish**.

Internal LDAP directory screen

Once the configuration of the LDAP directory is complete, you will arrive at the internal LDAP screen which sets out the following items:

Enable user directory	This option allows starting the LDAP service. If this option is not selected, the module will be inactive.

Internal LDAP directory

Organization	This field will contain the name of your company, entered earlier.
Domain	This field will contain your company's domain.
ID	The login that will allow you to connect to the internal LDAP base.
Password	The password allowing the firewall to connect to the directory. This password can be modified.
Confirm password	Confirmation of the LDAP administration password that you have just entered in the previous field.
Password strength	This field indicates your password's level of security: "Very weak", "Weak", "Moderate", "Good" or "Excellent". You are strongly advised to use uppercase letters and special characters.

Access to the internal LDAP

Enable unencrypted access (PLAIN)	Data entered will not be encrypted, but displayed in plaintext.
Enable SSL access (SSL certificate issued by the server)	In order to set up SSL access, you will need to select a certificate server already generated by your root CA, or an imported certificate.

Advanced properties

Password hash: The password encryption method for new users.
Some authentication methods (such as LDAP) have to store the user's password in the form of a hash (result of a hash function applied to the password) which will avoid having to store the password in plaintext.
You have to select your desired hash method from the following:

SHA	"Secure Hash Algorithm". This encryption method allows establishing a 160-bit or 160-byte character string (called a "key") which will be used as a reference for identification.
MD5	"Message Digest". This algorithm allows checking the integrity of data entered, by generating a 128-bit MD5 key. **REMARK** As this method uses fewer bytes and as such has a lower level of security, it is less robust against attacks.
SSHA	"Salt Secure Hash Algorithm". Based on the same principle as SHA, but contains a password salting function in addition, which consists of adding a bit sequence to the data entered in order to make them less legible. **NOTE** This variant of SHA uses a random value to diversify the password's fingerprint. Two identical passwords will therefore have two different fingerprints. The encryption method is the most secure and you are strongly advised to use it.
SMD5	"Salt Message Digest". Based on the same principle as MD5, with the addition of the password salting function.
CRYPT	The password is protected by the CRYPT algorithm, derived from the DES algorithm which allows block encryption using 56-bit keys. This method is not highly advised, as it has a relatively low level of security.
None	No password encryption, meaning it is stored in plaintext. **WARNING** This method is not recommended, as your data will not be protected.

After you have finished your configuration, click on **Apply** to activate it.

NOTE
To connect to another directory and return to the configuration wizard at any time, click on the magic wand ( ) at the top right side of the screen.

WARNING
Selecting the icon will reinitialize the LDAP database and as such, permanently delete the previous configuration of the directory and its components.

Connecting to an external LDAP directory

The external LDAP is a directory to which your NETASQ multi-function firewall will connect.

Step 1: Selecting the directory

Select the LDAP base of your choice. This is the first step in the configuration of this directory.
Select the option **Connect to an external LDAP directory** and click on **Next.**

Step 2: Accessing the directory

Server	Select an object corresponding to your LDAP server from the drop-down list. This object has to be created prior to this step and must reference the IP address of your LDAP server.
Port	Enter the listening port of your LDAP server. The default port is: 389.
Root domain (Base DN)	Enter the root domain (DN) of your directory. The DN represents the name of an entry, in the form of a path to it, from the top to the bottom of the tree structure. **Example of a DN** o=NETASQ,dc=COM
ID	An administrator account allowing the firewall to connect to your LDAP server and make changes (reading and writing privileges) to certain fields. We recommend that you create a specific account for the firewall and assign privileges to it only in the necessary fields. **Example** cn=id.
Password	The password associated with the ID for you to connect to the LDAP server. **NOTE** The key icon ( ) allows you to view the password in plaintext to check that it is correct.

Click on **Next** to go on to Step 3.

Step 3: Authentication

Allow access to the captive portal from protected networks (internal interfaces)	While this is restricted to internal interfaces, if this option is selected, you will enable authentication on the captive portal. This is the “internal interface” equivalent of the option **Enable the captive portal** in the Authentication module (in the menu Users\Authentication).

NOTE
When creating a new user, the SHA hash function will be used by default for storing passwords.

External LDAP directory screen

Once the configuration of the LDAP directory is complete, you will arrive at the external LDAP screen which sets out the following items:

"EXTERNAL DIRECTORY" TAB

The page that appears presents a window that summarizes the information entered for your external LDAP and various services concerning access to your directory.

Enable user directory	This option allows starting the LDAP service.. If this option is not selected, the module will be inactive.

Remote directory

Server	This field contains the name of the server that you had entered in the previous page.
Port	This field contains the listening port that you had selected in the previous page.
Root domain (Base DN)	Your directory's root domain.
ID	The login name allowing the firewall to connect to your LDAP server.
Password	The password created in the firewall for connecting to the LDAP server.

Secure connection (SSL)

Enable SSL access	This option allows checking your digital certificate generated by the firewall's root CA. The information will be encrypted in SSL, which uses port 636. Public access to the LDAP is protected by the SSL protocol. **NOTE** If this option is not selected, access will not be encrypted.
Check that the name of the server matches the FQDN in the SSL certificate	The FQDN represents the full name of a host in a URL, such as HOST (e.g. *www*) and a domain name (such as *netasq.com*). **Example** ***www.netasq.com*** If this option is selected, the verification of the server certificate will be enabled. The SSL certificate contains an FQDN, which the name of the server must match in order for the data to be correctly protected.
Certificate authority	This option allows selecting the CA against which the server certificate issued by the LDAP server will be compared, in order to ensure the authenticity of the connection to the LDAP server. Click on the magnifying glass icon ( ) to search for the corresponding CA. **NOTE** This option will be grayed out by default if the previous option **Check that the name of the server matches the FQDN in the SSL certificate** was not selected.

Advanced properties

Backup server	This field allows defining a replacement server in the event the main server fails. You can select it from the list of objects suggested in the drop-down list. By clicking on the button **Test access to the directory** below it, a window will inform you that your main server is functional. Click on **OK**.

Click on **Apply** to confirm your configuration.

"Structure" tab

Read-only access

User selection filter	When using the firewall in interaction with an external database, only users that correspond to the filter will be used. By default this filter corresponds to *ObjectClass = InetOrgPerson*.
User group selection filter	When using the firewall in interaction with an external database, only user groups that correspond to the filter will be used. By default this filter corresponds to *ObjectClass = GroupOfNames*.
Certification authority branch	This field defines the location of the CA on the external LDAP base. This location is used in particular when searching for the CA used for the SSL authentication method. **NOTE** Configuring this field is not absolutely necessary but in this case, in order for the SSL authentication method to work the CA has to be specified in the list of trusted CAs in the configuration of the SSL method. (See menu Users\Authentication module\Available methods tab: the authentication method **Certificate (SSL)** has to be added and the CA indicated in the right column "Certificate authorities (C.A)")

Mapped attributes

Apply a model: This button offers you 3 choices of LDAP servers, which you will apply to define your attributes:

- OpenLDAP: LDAP server.
- Microsoft Active Directory (AD): LDAP directory services for Windows operating systems.
- Open Directory: directory of websites under license of *Open Directory*

External directory attributes	This column represents the value given to the attribute in the external directory. **Examples:** *Cn= NETASQ* *telephoneNumber= +33 (0)3 61 96 30* *mail = salesadmin@netasq.com*

You are accessing the directory in read-only mode. The creation of users and groups is not allowed: if this option has been selected, you will not have writing privileges.

Write access

User branch	Enter the name of the LDAP branch for storing users. **Example** ou=users.
Group branch	Enter the name of the LDAP branch for storing user groups. **Example** ou=groups.

Advanced properties

Protected characters	For some external severs, a \ has to be added so that LDAP requests will be taken into account.

Password hash: The password encryption method for new users.
Some authentication methods (such as LDAP) have to store the user's password in the form of a hash (result of a hash function applied to the password) which will avoid having to store the password in plaintext.
You have to select your desired hash method from the following:

SHA	"Secure Hash Algorithm". This encryption method allows establishing a 160-bit or 160-byte character string (called a "key") which will be used as a reference for identification.
MD5	"Message Digest". This algorithm allows checking the integrity of data entered, by generating a 128-bit MD5 key. **REMARK** As this method uses fewer bytes and as such has a lower level of security, it is less robust against attacks.
SSHA	"Salt Secure Hash Algorithm". Based on the same principle as SHA, but contains a password salting function in addition, which consists of adding a bit sequence to the data entered in order to make them less legible. **NOTE** This variant of SHA uses a random value to diversify the password's fingerprint. Two identical passwords will therefore have two different fingerprints. The encryption method is the most secure and you are strongly advised to use it.
SMD5	"Salt Message Digest". Based on the same principle as MD5, with the addition of the password salting function
CRYPT	The password is protected by the CRYPT algorithm, derived from the DES algorithm which allows block encryption using 56-bit keys. This method is not highly advised, as it has a relatively low level of security.
None	No password encryption, meaning it is stored in plaintext. **WARNING** This method is not recommended, as your data will not be protected.

After you have selected your algorithm, click on **Apply** to confirm your configuration.

Connecting to a Microsoft Active Directory

Like the internal and external directories, Active Directory offers the same user management features that have been developed by Microsoft, using a *Windows* OS.

Step 1: Selecting the directory

Select the directory of your choice. This is the first step in the configuration of this directory.
Select the option **Connect to a Microsoft Active Directory** and click on **Next.**

Step 2: Accessing the directory

Server	Select an object corresponding to your LDAP server from the drop-down list. This object has to be created prior to this step and must reference the IP address of your LDAP server.
Port	Enter the listening port of your LDAP server. The default port is: 389.
Root domain (Base DN)	Enter the root domain (DN) of your directory. The DN represents the name of an entry, in the form of a path to it, from the top to the bottom of the tree structure. The field with the name of the AD domain can be entered using the name of the Root Domain (DN). **Example of a DN** AD domain is “netasq.com” so my Root domain (Base DN) should be “dc=netasq,dc=com”
ID	An administrator account allowing the firewall to connect to your LDAP server and make changes (reading and writing privileges) to certain fields. We recommend that you create a specific account for the firewall and assign privileges to it only in the necessary fields. **Example** cn=id.
Password	The password associated with the ID for you to connect to the LDAP server. **NOTE** The key icon ( ) allows you to view the password in plaintext to check that it is correct.

Click on **Next** to go on to Step 3.

Step 3: Authentication

Allow access to the captive portal from protected networks (internal interfaces)	While this is restricted to internal interfaces, if this option is selected, you will enable authentication on the captive portal. This is the “internal interface” equivalent of the option **Enable the captive portal** in the Authentication module (in the menu Users\Authentication).

NOTE
When creating a new user, the SHA hash function will be used for storing passwords.

Microsoft Active Directory screen

“Active Directory” tab

Once you have completed the configuration of the directory, you will arrive at the Active Directory which sets out the following items:

Enable user directory	This option allows starting the LDAP service. If this option is not selected, the module will be inactive.

Directory distant

Server	This field contains the name of the server that you had entered in the previous page.
Port	This field contains the listening port that you had selected in the previous page.
Root domain (Base DN)	Your directory's root domain.
ID	The login name allowing the firewall to connect to your LDAP server.
Password	The password created in the firewall for connecting to the LDAP server.

Secure connection (SSL)

Enable SSL access	This option allows checking your digital certificate generated by the firewall's root CA. The information will be encrypted in SSL, which uses port 636. Public access to the LDAP is protected by the SSL protocol. **NOTE** If this option is not selected, access will not be encrypted.
Check that the name of the server matches the FQDN in the SSL certificate	The FQDN represents the full name of a host in a URL, such as HOST (e.g. *www*) and a domain name (such as *netasq.com*). **Example** ***www.netasq.com*** If this option is selected, the verification of the server certificate will be enabled. The SSL certificate contains an FQDN, which the name of the server must match in order for the data to be correctly protected.
Certificate authority	This option allows selecting the CA against which the server certificate issued by the LDAP server will be compared, in order to ensure the authenticity of the connection to the LDAP server. Click on the magnifying glass icon ( ) to search for the corresponding CA. **NOTE** This option will be grayed out by default if the two options above were not selected.

Advanced properties

Backup server	This field allows defining a replacement server in the event the main server fails. You can select it from the list of objects suggested in the drop-down list. By clicking on the button **Test access to the directory** below it, a window will inform you that your main server is functional. Click on **OK**.

Click on **Apply** to confirm your configuration.

“Structure” tab

Read-only access

User selection filter	When using the firewall in interaction with an external database, only users that correspond to the filter will be used. By default this filter corresponds to *ObjectClass = InetOrgPerson*.
User group selection filter	When using the firewall in interaction with an external database, only user groups that correspond to the filter will be used. By default this filter corresponds to *ObjectClass = GroupOfNames*.
Certification authority branch	This field defines the location of the CA on the external LDAP base. This location is used in particular when searching for the CA used for the SSL authentication method. **NOTE** Configuring this field is not absolutely necessary but in this case, in order for the SSL authentication method to work the CA has to be specified in the list of trusted CAs in the configuration of the SSL method. (See menu Users\Authentication module\Available methods tab: the authentication method **Certificate (SSL)** has to be added and the CA indicated in the right column “Certificate authorities (C.A)”)

Mapped attributes

Apply a model: This button offers you 3 choices of LDAP servers, which you will apply to define your attributes:

- OpenLDAP
- Microsoft Active Directory (AD)
- Open Directory

External directory attributes	This column represents the value given to the attribute in the external directory. **Examples:** *Cn= NETASQ* *telephoneNumber= +33 (0)3 61 96 30* *mail = salesadmin@netasq.com*

You are accessing the directory in read-only mode. The creation of users and groups is not allowed: if this option has been selected, you will not have writing privileges.

Write access

User branch	Enter the name of the LDAP branch for storing users. **Example** ou=users.
Group branch	Enter the name of the LDAP branch for storing user groups. **Example** ou=groups.

Advanced properties

Protected characters	For some external severs, a \ has to be added so that LDAP requests will be taken into account.

Password hash: The password encryption method for new users.
Some authentication methods (such as LDAP) have to store the user's password in the form of a hash (result of a hash function applied to the password) which will avoid having to store the password in plaintext.
You have to select your desired hash method from the following:

SHA	"Secure Hash Algorithm". This encryption method allows establishing a 160-bit or 160-byte character string (called a "key") which will be used as a reference for identification.
MD5	"Message Digest". This algorithm allows checking the integrity of data entered, by generating a 128-bit MD5 key. **REMARK** As this method uses fewer bytes and as such has a lower level of security, it is less robust against attacks.
SSHA	"Salt Secure Hash Algorithm". Based on the same principle as SHA, but contains a password salting function in addition, which consists of adding a bit sequence to the data entered in order to make them less legible. **NOTE** This variant of SHA uses a random value to diversify the password's fingerprint. Two identical passwords will therefore have two different fingerprints. The encryption method is the most secure and you are strongly advised to use it.
SMD5	"Salt Message Digest". Based on the same principle as MD5, with the addition of the password salting function
CRYPT	The password is protected by the CRYPT algorithm, derived from the DES algorithm which allows block encryption using 56-bit keys. This method is not highly advised, as it has a relatively low level of security.
None	No password encryption, meaning it is stored in plaintext. **WARNING** This method is not recommended, as your data will not be protected.

Click on **Apply** to confirm your configuration.

DNS CACHE PROXY

When you send a DNS query to your browser or to an e-mail address, the DNS server will convert the known domain name (e.g. *www.netasq.com* or *smtp.netasq.com*) into an IP address and communicate it to you.
The DNS cache proxy allows storing the response and IP address communicated earlier by the server in the firewall's memory. As such, whenever a similar query is sent, the firewall will respond more quickly on behalf of the server and will provide the saved IP address.
The **DNS cache proxy** window consists of a single screen, divided into two sections:

- A table listing the DNS clients allowed to use the cache.
- A drop-down menu allowing the definition of advanced properties.

Enable DNS cache

This option allows the DNS cache proxy to run: when a DNS query is sent to the firewall, it will be processed by the DNS cache.

List of clients allowed to used the DNS cache

DNS client [host, network, range, group]:

The clients that appear in the list can send DNS queries through the firewall.

Add	By clicking on this button, a new line will be added to the top of the table. The arrow to the right of the empty field allows adding a DNS client. You may select this client from the object database that appears. This may be a host, network, address range or even a group.
Delete	First, select the DNS client you wish to remove from the list. A window will appear with the following message: "**Remove selected DNS client?**" You can confirm the deletion or **Cancel** the operation.

NOTE
In transparent mode, the selected clients will benefit from the DNS cache proxy, while other requests will be subject to filtering.

Advanced properties

Cache size (in bytes):

The maximum size allocated to the DNS cache depends on your firewall's model.

Transparent mode (intercepts all DNS queries sent by authorized clients)	As its name implies, the purpose of this option is to make the NETASQ firewall's DNS service transparent. As such, when this option is enabled, the redirection of DNS traffic to the DNS cache will be invisible to users who will get the impression they are accessing their DNS servers. In transparent mode, all queries will be intercepted, even if they are going to DNS servers others than the firewall. The responses will be saved in memory for a certain duration to avoid resending known requests.
Random querying of domain name servers	If this option is selected, the firewall will select the DNS server at random from the list. (see menu System/Configuration module/Network settings tab/DNS Resolution panel).

DYNAMIC DNS

The configuration screen for the Dynamic DNS client consists of 2 sections:
- On the left, the “List of Dynamic DNS profiles”.
- On the right, “DNS resolution”, or the configuration of the profile selected earlier.

List of Dynamic DNS profiles

The table that presents the profiles consists of 2 columns:

Status	Double-clicking on this allows enabling or disabling the profile.
Preview	Indicates the domain name, interface and status of the resolution with regards to the profile.

The **Add** button allows adding a profile.
The **Delete** button allows deleting a selected profile.

From version 9.0.3 onwards the status of the Dynamic DNS profile can now be reinitialized using the **"Reset"** button via the web administration interface’s configuration module.

Configuring a profile

DNS resolution

Domain name (mandatory)	Domain name assigned to the Dynamic DNS client. For example: *myfirewall.dyndns.org*. By using the option **Resolve domain names for all sub-domains (wildcard management),** you will be able to cover all sub-domains. For example, if you specify **netasq.dyndns.org** in the “Domain name” field and the option **Resolve domain names for all sub-domains (wildcard management)** has been selected, all sub-domains (commerce.netasq.dyndns.org, labo.netasq.dyndns.org, etc.) will be associated with the client.
Interface associated with the domain name	Name of the network interface whose IP address is associated with the domain name. **NOTE** - An interface can use only one profile. - A profile can only be used by one interface. - The profile cannot be active if an interface has not been indicated
Resolve domain names for all sub-domains (wildcard management)	Enables or disables the inclusion of sub-domains linked to the domain name. **NOTE** Subscribing to the Wildcard range is necessary in order to benefit from this feature.

Dynamic DNS service provider

This zone allows you to enter the access information for your Dynamic DNS service provider.

Dynamic DNS provider (mandatory)	DNS service provider. Currently, only one DNS service provider is supported: **DynDNS**.
Login (mandatory)	User indicated by the DNS service provider for the authentication of the Dynamic DNS client.
Password (mandatory)	Password indicated by the DNS service provider for the authentication of the Dynamic DNS client.
Dynamic DNS server (mandatory)	Server of the DNS service provider. The object to specify in this field must be named: "members.dyndns.org" or "members.dyndns.com" in order to run with DynDNS.
Dynamic DNS service (mandatory)	This option allows you to indicate the service you have subscribed with the DNS service provider from among the following: "dynamic DNS", "custom", and "static DNS".

Advanced properties

Access the settings for advanced properties by clicking on the button **Advanced properties**. These allow in particular, renewing registrations and changing addresses.

Renewal frequency (days)	Renewal period of the Dynamic DNS service. NETASQ has set this period to 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 used for the update	Protocol used during the dynamic DNS service renewal phase. You can choose between HTTPS and HTTP.
Notify provider	This service, which **DynDNS** charges at a fee, enables redirecting traffic headed for your network to a specific page when your connection is inactive.

E-MAIL ALERTS

The screen consists of three sections:

- Configuration tab: allows proceeding to the basic settings of module, such as SMTP server settings, e-mail sending frequency (in minutes), intrusion prevention alarms and system events.
- Recipients tab: allows defining groups that will be used in the mailing policies but also in other configuration modules in which e-mails need to be sent.
- Templates tab: allows viewing and modifying e-mail formats, used when sending notifications to users and administrators.

"Configuration" tab

This tab contains all the necessary parameters for configuring e-mail alerts.
It consists of the following elements:

Enable e-mail notifications

This option enables the configuration of alerts. If it is disabled, none of the configuration items will be accessible as the firewall will not send ay e-mails. This option is disabled by default.

REMARK
The e-mail notification feature requires a mail server that can receive e-mails from the firewall.

SMTP server

Server	This field determines the host (SMTP server) to which the firewall will send e-mails, by selecting it from the object database. This field is empty by default.
Port	Port on the SMTP server to which e-mails will be sent. A list allows selecting an object, whose default value will be "SMTP".
Authentication *From version 9.0.2 onwards*	A login and password can now be defined for sending e-mail via the firewall. This checkbox allows you to enable the authentication of the firewalls when sending e-mail alerts.
ID	This entry is disabled if the Authentication option is disabled. This field allows entering the SMTP username (this entry has to be provided if authentication has been enabled).
Password	This entry is disabled if the Authentication option is disabled. This field allows entering the SMTP username (this entry has to be provided if authentication has been enabled).
DNS domain	This is useful for indicating the domain name of the e-mail sender. The e-mail address of the sender will therefore be expressed as follows: <firewall_name>@<domain_name>.

E-mail sending frequency (in minutes)

Sending frequency	This option allows you to specify the frequency with which reports will be sent. A report contains all the alarms detected from the previous report. As such, e-mails will be received during certain time slots and not each time an alarm is raised. The default value is 15.

Intrusion prevention alarms

Here, you may select a group to notify of intrusion prevention alarms.
The list of alarms will be sent in the body of the e-mail to the specified group.
The frequency for sending alarm reports can be modified in the field “Sending frequency” in the menu **E-mail sending frequency (in minutes)**

Example

If you define a frequency of 15 minutes in the field “Sending frequency”, you will be informed by e-mail every 15 minutes of alarms that were raised on the firewall during this period.

Do not send	No intrusion prevention alarm reports will be sent. This radio button is selected by default.
Send only major alarms	If this option is selected, the group that you will select in the next field will receive major alarms.
Message recipient	Selection of the group that will receive major intrusion prevention alarms.
Send major and minor alarms	If this option is selected, the group that you will select in the next field will receive major and minor intrusion prevention alarms.
Message recipient	Selection of the group that will receive major and minor intrusion prevention alarms.

System events

Like the previous field, a group can also be notified of system events.
The frequency for sending system events can be modified, likewise, in the field “Sending frequency” in the menu **E-mail sending frequency (in minutes).**

Do not send	No system events will be sent. This radio button is selected by default.
Send only major alarms	If this option is selected, the group that you will select in the next field will receive major system events.
Message recipient	Selection of the group that will receive major system events.
Send major and minor alarms	If this option is selected, the group that you will select in the next field will receive major and minor system events.
Message recipient	Selection of the group that will receive major and minor system events.

REMARK
The status of system events can be viewed in a module of the same name: In the menu, go to Notifications\System events.

"Recipients" tab

This screen consists of 2 views:

- Recipient groups
- Select a group

Each group contains a certain number of e-mail addresses
Up to 50 groups can be created.
There are no pre-configured groups. You may add new groups and comments, and delete groups.
Each group must contain at least one e-mail address. There is no restriction to the number of e-mail addresses in a group.

Next, you will be able to select a group to which detailed or simplified vulnerability reports can be sent, in the menu Application protection => Vulnerability detection.

Creating a group

1. Click on the button **New recipient group.** A new line will appear in the list and you will be asked to enter the name that you wish to give the group.
2. You can add comments regarding this group, by filling in the field in "Comments" column.

To add a recipient, go to the selected group. Its name will appear on the right in the field **Recipients of group: <groupname>**. Next, click on **Add new recipient to group**. A screen will appear, allowing you to indicate either the recipient's e-mail address or the user or the group he belongs to if it exists in the object database. Any e-mail address can be entered, but the format of the address will be checked.

Deleting a group

1. Select the line to delete.
2. Click on the button **Remove**. The message "**Delete the group "group name"?**" will appear. By clicking on "Yes", the group will be deleted from the list.

> **REMARK**
> Groups can be deleted only if the group is not being used in another configuration on the firewall.
> If you wish to delete a group that is active in another module, a pop-up window will appear with the following options: force deletion, check where the group is being used, or cancel.

Check use

The **Check use** button allows checking if a group of e-mail is used in the different modules of the firewall's configuration.

1. Select the line to check.
2. Click on the button **Check use** in order to check.

"Templates" tab

This section allows you to use a customized message for sending out e-mails. Six templates are available, each of them containing a body that differs according to the message that you wish to send out.

Editing the template (HTML)

Each template has some content called the "body" (like in an HTML page). This consists of unformatted text that may contain simple HTML markers that may finalize the formatting.

These templates can be modified and may contain keywords which will later be replaced with values. For example, a keyword may automatically display the user's name.
To modify contents, click on the button **Edit**.
The screen will be split into two parts:

- Top: preview of the e-mail template
- Bottom: Editing window

2 buttons allows you to modify the message's body:

Insert a variable	This button allows you to select variables that will later be replaced with real values when the message is sent.
Apply default template	Allows resetting the template to its initial presentation. When you click on this button, the following message will appear: "*Reset the contents of this template to its default values?"*

Vulnerability detection

- Vulnerability detection (detailed): detailed vulnerability report template, applied by default.
- Vulnerability detection (summary): simple vulnerability report template, applied by default.

Certificate request

- Accept the certificate request: e-mail template specifying that the certificate request has been approved by the administrator.
- Reject the certificate request: e-mail template specifying that the certificate request has been rejected by the administrator.

User enrolment

- Accept the user request: e-mail template specifying that the enrolment request has been approved by the administrator.
- Reject the user request: e-mail template specifying that the enrolment request has been rejected by the administrator.

List of variables

E-mail templates dedicated to vulnerability detection:

- Mail subject ($Title)
- Subtitle ($SubTitle)
- Message summary ($MailSummary)
- Vulnerability summary ($VulnSummary)
- Affected hosts ($HostsByVuln)
- Vulnerable applications ($VulnByProduct)

- Message footer ($Footer)

E-mail templates used for certificate requests and user enrolment requests.

- User's last name ($LastName)
- User's first name ($FirstName)
- Date of the enrolment request ($Date)
- User ID ($UID)
- URL for downloading the certificate ($URL)

Example of a report received by e-mail regarding alarms

Type	Minor
Action	Block
Date	2010-10-11 15:08:32
Interface	dmz2
Protocol	tcp
Source	10.2.18.5:55987 (ed:ephemeral_fw_tcp)
Destination	66.249.92.104:80 (**www.google.com**)
Description	SQL injection prevention: suspicious instruction OR in the URL

ENROLMENT

NETASQ's web enrolment service allows "unknown" users in the user database to request the creation of their access accounts (internet, mail server, all services that require authentication) and their certificates.

This module requires at least the use of an LDAP database for user requests and a root CA (internal PKI) for user certificate requests.
The Enrolment module consists of 3 zones:

- The table containing user enrolment requests and certificate requests on the left
- Information relating to the user or to the selected certificate on the right
- Advanced properties

The enrolment table

Possible operations

Validate	When a user sends an enrolment or a certificate request, the request will appear in this table. To validate a user's request, go to the relevant line and click on **Validate**.
Reject	You can also reject users' requests for enrolment or for certificates by selecting the corresponding line and clicking on **Reject**.
Ignore	This button allows you to cancel an approval or a rejection. This avoids having to use the **Cancel** button and erasing operations in progress.
Refresh	This button allows refreshing the list of enrolment and certificate requests. As such, recent requests will be added automatically to the table pending approval or rejection.

User enrolment and certificate requests

Type	This column indicates the type of request the user has created: an enrolment request is represented by "**User**" while certificate requests are represented by "**Certificate**".
CN User	Name that allows identifying the user or the certificate.
E-mail address	E-mail address of the user, which will allow him to receive an approval or a rejection of his enrolment or certificate request.

Summary

Information regarding the selected user/certificate is displayed here.

ID	User's login
Last name	User's last name
First name	User's first name
E-mail address	User's e-mail address, which will be useful for sending him a response regarding his enrolment or certificate request.
Description	Description of the user
Telephone number	User's telephone number

Password	User's password
Certificate request	Indicates whether the user requested a certificate during his enrolment request.

NOTE
For certificate requests, only the e-mail address will appear in the field on the right.

Advanced properties

Automatically approve certificate requests

This option allows you to automatically approve certificate requests. When the administrator approves the user account creation request, the application will automatically approve the creation of the certificate associated with this user.

User identifier format for empty ID fields

Identifier format	Define a default character string for connection IDs. **Example:** %F.%L
Example	Illustrated example of a user ID. **Example:** JOHN.SMITH

NOTE
The desired number of characters for the first name and/or last name can be defined by indicating the number after the F and/or the L.

%F1%L
JSMITH

E-mail notification

Send an e-mail to the user:
when approving/rejecting user's enrolment request
This option allows sending an e-mail to the user to inform him that his enrolment request has been approved or rejected.

when approving/rejecting user's certificate request
This option allows sending an e-mail to the user to inform him that his certificate request has been approved or rejected.

FILTERING AND NAT

Filtering and NAT are now condensed in a single module and are part of the Security policy menu.
This new module consists of 2 tabs, each containing an area reserved for filter policies and NAT policies, and their configuration:

- Filtering: this is a set of rules that allow or block certain types of network traffic according to the defined criteria.
- NAT: these allow rewriting (or translating) source and destination addresses and ports.

Policies

This section allows you to select and manipulate Filter policies and NAT policies.

Selecting the filter policy

The drop-down menu offers 10 pre-configured filter policies, number from 1 to 10:

"Block all (1)"	By selecting this policy, you will have access only to the firewall's administration screen, regardless of the interface on which you are connected. All other connections will be blocked.
"High (2)"	If you select this filter policy, only web, e-mail and FTP traffic and ICMP requests will be allowed from internal interfaces to the outside.
"Medium (3)"	By selecting this policy, intrusion prevention will be applied to outgoing connections, to the extent that the protocol can be automatically detected by the threat prevention engine: For example, port 80 is generally used for HTTP traffic. The firewall will therefore consider all traffic on port 80 as HTTP traffic, as this port is defined as the default port for the HTTP protocol (default ports for each protocol are defined in the menu Application protection\Protocols and applications)**.** However, if another protocol is used (e.g. an SSH tunnel) for traffic going to port 80, the connection will be considered illegitimate and will be blocked as the only protocol allowed is HTTP. **REMARK** All outgoing TCP connections that cannot be scanned (for which no protocol can be recognized) will be accepted.
"Low (4)"	A protocol scan will be forced for outgoing connections. **REMARK** All outgoing connections that cannot be scanned will be allowed.
"Filter 05, 06, 07, 08, 09"	Apart from the 5 pre-configured policies (**Block all, High, Medium, Low, Pass all,** which can be edited where necessary), there are 5 blank policies that you can customize.
"Pass all (10)"	This policy allows all traffic to pass through. It should only be used for testing.

NOTE

You can **Rename** these policies and modify their configuration whenever you wish (see below).

Possible operations

Activate this policy	Immediately activates the policy being edited. Parameters saved in this slot will overwrite current parameters in force and the policy will be applied immediately on the firewall.
Edit	This function allows performing 3 operations on profiles: • **Rename:** by clicking on this option, a window comprising two fields will appear. It will allow you to modify the name of the filter policy and add comments. Once the operation has been performed, click on "Update". This operation can also be cancelled. • **Reinitialize**: allows resetting the profile to its initial configuration, thereby deleting all changes made to the profile. • **Copy to:** This option allows copying a profile to another, with all the information from the copied profile transmitted to the receiving profile. It will also have the same name.
Last modification	This icon allows finding out the exact date and time of the last modification.

From version 9.0.1 onwards, filter and NAT rules can be moved by dragging and dropping.

Drag & drop

Throughout the creation and edition of rules, you will be able to drag and drop objects and actions.

You can move any object to wherever you wish in the table, or insert objects from the browser bar on the left (Objects field), if they have been created earlier (you can also create them directly in the fields that accept objects).

REMARK

Two icons indicate whether the selected object or action can be moved within a particular cell:

Means that the operation is possible,

Means that the object cannot be added to the chosen cell.

"Filtering" tab

NETASQ's intrusion prevention technology includes a dynamic packet filtering engine ("stateful inspection") with rule optimization that allows the application of filter policies safely and effectively.

The implementation of filter functions is based on the comparison of the attributes of each IP packet received against the criteria of each rule in the active filter policy. Filtering applies to all packets without any exceptions.

The selection criteria of the traffic for a filter rule 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,

DSCP in order to define traffic differentiation.

- 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 are taken from 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 (see Action column).

Filtering consists of two parts. The strip at the top of the screen allows choosing the filter policy, activating it, editing it and seeing its last modification. The filter table is dedicated to the creation and configuration of rules.

Actions on filter policy rules

Search	This field allows performing searches by occurrence, letter or word. **Example:** If you enter "Network_internal" in the field, all filter rules containing "Network_internal" will be displayed in the table.
New rule	Inserts a predefined line or a blank line after the selected line. 3 choices are available: authentication, SSL inspection and explicit HTTP proxy rules will be defined via a wizard in a separate window: • **Standard rule:** This option allows creating a blank rule that will leave the administrator the possibility of entering different fields in the filter table. • **Separator – rule grouping**: This option allows inserting a separator above the selected line and helps to improve the filter policy's readability and visibility. It can, for example, allow the administrator to create a hierarchy for his rules or group those that apply to traffic going to different servers. ***From version 9.0.1 onwards,*** you can copy/paste separators from one location to another. • **Authentication rule:** The aim of this is to redirect unauthenticated users to the captive portal. By selecting it, an authentication wizard will appear. You will need to select the **Source** (displays "Network_internal" by default) and the **Destination** (displays "Internet" by default) of your traffic from the drop-down list of objects, and then click on **Finish.**

	◦ **SSL inspection rule:** The aim of this rule creation wizard is to inspect encrypted SSL traffic. You will need to define the **Profile of traffic to be encrypted** by indicating the **Source hosts** ("Network_internal" by default), **Incoming interface** ("any" by default), the Destination ("Internet" by default) and the destination port ("ssl" by default) from the drop-down list of objects. In order to **Inspect encrypted traffic** through the second zone in the wizard window, you will need to define the configuration of the **Inspection profile**, by selecting one of those you have defined earlier in Application protection/Inspection profile, or leave it in "Auto" mode. You will also be able to select an **SSL filter policy** (SSL certificate content filtering) and the **Antivirus** and to enable them (**On**/**Off** buttons). ◦ **Explicit HTTP proxy rule:** This option allows enabling the explicit HTTP proxy and defining who can access it. You will need to choose a **Host** object and an **Incoming interface** in the "**Source**" field. Next, define the **Inspection of transmitted traffic** by indicating whether you wish to assign a default configuration to the URL filter and the Antivirus, and enable them (**On**/**Off** buttons). Click on **Finish**.
Delete	Deletes the selected line. **NOTE** Several lines can be deleted at the same time, by selecting them with the "Ctrl" key and pressing on **Delete**.
Up	Places the selected line before the line just above it.
Down	Places the selected line after the line just below it.
Collapse all	This button allows collapsing all folders in the filtering directory.
Expand all	This button allows expanding all folders in the filtering directory.
Copy	This button allows you to copy a filter rule in order to duplicate it.
Paste	This button allows you to duplicate a filtering rule after having copied it.
Reset columns	When you click on the arrow on the right in the field containing a column's name (example: **Status**), you will be able to display additional columns or remove columns so that they will not be visible on the screen, by ticking or unticking them. **Example:** Tick the options "**Nom**" and "**Src port**" which are not displayed by default. By clicking on **reset columns**, your columns will be reset to their original settings, before you selected any additional columns. As such, "**Nom"** and "**Src port**" will be hidden again.

Filter table

This table allows 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 (Rule No. 1, 2 and so on) and stops as soon as it finds a rule that applies to the IP packet.

It is therefore advisable that you define the rules from **most detailed to most general**.

GENERAL NOTE:

Each time you come across a drop-down list of objects in the columns (except “Status” and “Action”) a mathematical operator icon will appear ( ). It can only be used if an object other than “**Any**” has been selected.

You can therefore customize the parameters of your traffic using the following icon in 4 different ways:

- “=" (or): the value of the attribute corresponds to what is selected.
- “!=" (or) the value of the attribute is different from what has been selected.
- “<“ (or ; used for source and destination ports only): the port number of the traffic is lower than what is selected.
- “>“ (or ; used for source and destination ports only): the port number of the traffic is higher than what is selected.

From version 9.0.1 onwards, if you click quickly 10 times on the “Up” button, you will see that the rule moves up but the waiting window will only appear when you leave the button for 2 or 3 seconds. And at the end, only a single command will be executed.

NOTE

Rules can be moved more much fluidly as such.

The filter table sets out the following columns:

Status

This column shows the status of the rule: **On**/**Off**. Double-click on it to change its status. By doing this once, you will enable the filter rule. Repeat the operation to disable it.

Action

This zone refers to the action applied to the packet that meets the selection criteria of the filter rule.
To define the various parameters of the action, double-click in the column. A window containing the following elements will appear:

“General” tab

General	
Action	5 different actions can be performed: **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. **Decrypt:** This action allows decrypting the encrypted traffic. Decrypted traffic will continue to move down the list of rules. It will be encrypted again after the scan (if it is not blocked by any rule). **Log:** The NETASQ firewall does not do anything. This is useful when you only want to logs certain types of traffic without applying any particular actions. **Reset TCP/UDP**: This option mainly concerns TCP and UDP traffic: For TCP traffic, a “TCP reset” packet will be sent to its sender. For UDP traffic, a “port unreachable” ICMP packet will be sent to its sender. As for other IP protocols, the NETASQ firewall will simply block the packet corresponding to this filter rule.

	If you are editing the global filter policy, a 6th option will appear: **Delegate**. This option makes it possible to stop comparing the traffic against the rest of the global policy, but to compare it directly with the local policy.
Log level	4 choices are available: **None**: No logs will be kept if the packet corresponds to this filter rule. **NOTE** This option is not available if you have selected the "Log" action in the previous field. **Log:** If you select this option, a log will be added to the filter logs. **Minor alarm:** As soon as this filter rule is applied to a connection, a minor alarm will be generated. This alarm is transferred to the logs, and can be sent by Syslog (Logs – Syslog) or by e-mail (see module E-mail alerts). **Major alarm:** As soon as this filter rule is applied to a connection, a major alarm will be generated. This alarm is transferred to the logs, and can be sent by Syslog (Logs – Syslog) or by e-mail (see module E-mail alerts).
Scheduling	In order to use this field, you must first create a Time Object in the menu Objects\Time Objects. You will then be able to define the **period/ day of the year / day of the week / time/ recurrence** of rule validity.

Routing

Gateway – router	This option is useful when specifying a particular router that will allow directing traffic that corresponds to the rule to the defined router. **NOTE** During packet treatment, NETASQ's intrusion prevention engine will assess rules in the order in which they have been defined in the table.

Click on **Ok** to confirm your configuration.

"Quality of service" tab

The QoS module, integrated into NETASQ's intrusion prevention engine, is associated with the Filtering module in order to provide Quality of Service features.
As soon as it is received, the packet will be treated by a filter rule then the intrusion prevention engine will assign it to the right queue according to the configuration of the QoS field in this filter rule.

QoS

Queue	This field offers you the choice of several queues that you have defined earlier in the module Quality of service, in the menu Security policy.
Fairness	**No fairness:** If you select this option, no particular amount of bandwidth will be assigned and each user/host/connection will use it according its needs. **User fairness:** bandwidth will be distributed evenly between users. **Host fairness:** bandwidth will be distributed evenly between hosts. **Connection fairness**: bandwidth will be distributed evenly between connections.

Connection threshold
The NETASQ firewall may limit the maximum number of connections accepted per second for a filter rule. For the protocols 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 per second 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).

If threshold is reached	**Do not do anything:** the number of connections per second (c/s) will not be restricted. **Enable the SYN proxy:** This option allows protecting servers from TCP SYN packet flooding ("SYN flooding") attacks. The SYN proxy instead of the server will respond and will assess the reliability of the TCP request before transmitting it. You can limit the number of TCP connections per second for this filter rule in the field below. **Block traffic:** Depending on the maximum number of connections per second that you define for the protocols below, the traffic will be blocked once the defined number is exceeded.
TCP (c/s)	Maximum number of connections per second allowed for the TCP protocol.
UDP (c/s)	Maximum number of connections per second allowed for the UDP protocol.
ICMP (c/s)	Maximum number of connections per second allowed for the ICMP protocol.
Requêtes applicatives (r/s) *From version 9.0.2 onwards*	Maximum number of Application requests per second allowed for the HTTP and DNS protocol.

Click on **Ok** to confirm your configuration.

DSCP

DSCP (*Differentiated Services Code Point)* is a field in the IP packet header. The purpose of this field is to allowing differentiating services contained in a network architecture. It will specify a mechanism for classifying and controlling traffic while providing quality of service (QoS).

Impose value	By selecting this option, you will enable the field below and allow access to the DSCP service. This option allows rewriting the packet with the given value, so that the next router will know the priority to apply to this packet.
New DSCP value	This field allows defining traffic differentiation. Through this field, it is possible to determine which service a type of traffic belongs to, thanks to a pre-established code. This DSCP service, used in the context of Quality of Service, allows the administrator to apply QoS rules according to the service differentiation that he has defined.

Click on **Ok** to confirm your configuration.

Advanced properties

Service	**None**: This option means that none of the following services will be used: the user will not go through the HTTP proxy and will not be redirected to the authentication page. **HTTP proxy:** If you select this option, the HTTP proxy will intercept user connections and scan traffic transparently. **Authentication:** If you select this option, unauthenticated users will be redirected to

	the captive portal when they connect.
Count	If you select this option, the NETASQ firewall will count the number of packets that correspond to this filter rule and will generate a report. It will therefore be possible to obtain volume information on a desired traffic type.

Click on **Ok** to confirm your configuration.

Source

This field refers to the source of the treated packet, and is used as a selection criterion for the rule.
Double-click in this zone to select the associated value in a dedicated window.
This window contains two tabs:

"General" tab

General

User	The rule will apply to the user that you select in this field. There are two choices by default: **"Any user":** refers to any authenticated user. **"Unknown users":** refers to any unknown or unauthenticated user. **NOTE** In order for unauthenticated users to be automatically redirected to the captive portal, at least one rule must be defined, applying to the object "**unknown users"**. This rule will also apply when an authentication expires.
Source hosts	The rule will apply to the object or the user (created beforehand in the dedicated menu: Objects\Network objects or Users\ Users) that you select in this field. The source host is the host from which the connection originated. You can **Add** or **Delete** one or several objects by clicking on ✚
On the interface	Interface on which the filter rule applies, presented in the form of a drop-down list. By default, the firewall selects it automatically according to the operation and source IP addresses. It can be modified to apply the rule to another interface. This also allows specifying a particular interface if "Any" has been selected as the source host.

Click on **Ok** to confirm your configuration.

"Advanced properties" tab

Advanced properties

Source port	This field allows specifying the port used by the source host, if it has a particular value. By default, the "Stateful" module memorizes the source port used and only this port will then be allowed for return packets.
Via	**Any**: This option means that none of the following services will be used: the connection will not go through the HTTP proxy, will not be redirected to an authentication page and will not go through an IPsec VPN tunnel. **Explicit HTTP proxy:** the traffic comes from the HTTP proxy. **SSL proxy:** the traffic comes from the SSL proxy. **IPsec VPN tunnel:** the traffic comes from an IPsec VPN tunnel.
Source DSCP	This field allows filtering according to the value of the DSCP field of the packet received.

Click on **Ok** to confirm your configuration.

Destination

Destination object used as a selection criterion for the rule. Double-click in this zone to select the associated value in a dedicated window.
This window contains two tabs:

"General" tab

General

Destination hosts	Select the destination host of the traffic from the object database in the drop-down list. You can **Add** or **Delete** one or several objects by clicking on ✚

Click on **Ok** to confirm your configuration.

"Advanced properties" tab

Advanced properties

From the interface	This option allows choosing the packet's outgoing interface, to which the filter rule applies. By default, the firewall selects it automatically according to the operation and destination IP addresses. Filtering by a packet's outgoing interface is possible.

NAT on the destination

Destination	If you wish to translate the traffic's destination IP address, select one from the objects in the drop-down list. Otherwise, leave the field empty, i.e. "**None**" by default.
ARP Publication *From version 9.0.2 onwards*	this option has been added so that an ARP publication can be specified when a filter rule with a NAT operation is used on the destination.

Click on **Ok** to confirm your configuration.

Dest. port

The destination port represents the port on which the "source" host opens a connection to the "destination" host.
It must be defined in the protocol editing window.

Protocol

This field refers to the protocol on which the filter rule will apply.

Port

Destination port	Service or service group used as a selection criterion for this rule. Double-click on this zone to select the associated object. **Examples:** Port 80: HTTP service Port 25: SMTP service You can **Add** or **Delete** one or several objects by clicking on ✚

Protocol type

Depending on the protocol type that you choose here, the following field that appears will vary:

Automatic protocol detection (default)	If this option is selected, a field with the same name will appear below with the following data: Application protocol: Auto IP protocol: All

Application protocol	If this option is selected, a field with the same name will ask you to choose: Application protocol: Select the desired protocol from the drop-down list. IP protocol: All
IP protocol	If you select this option, the field will offer a drop-down list of the various IP protocols.

From version 9.0.2 onwards, the status of IP connections can now be tracked for protocols other than TCP, UDP or ICMP.

Status tracking (stateful)	If you select “IP Protocol”, a “stateful” option will be available.

NOTE
For example, connection status tracking (stateful mode) can be enabled for the GRE protocol, which is used in PPTP tunnels. Thanks to this tracking tool, the source (map), destination (redirection) or both (bimap) can be translated.
However, it will be impossible to differentiate 2 connections that share the same source and destination addresses. In concrete terms, this means that when the firewall translates a source N -> 1 (map), only one simultaneous connection to a PPTP server can be made.

From version 9.0.1 onwards, for the translation of a selected destination, an additional option is available:

Translated port

Translated destination port	Translated port to which packets are going. Network packets received will be redirected from a given port on a host or a network device to another host or network device. If you wish to translate the traffic’s destination port, select one from the objects in the drop-down list. Otherwise, leave the field empty, i.e. “None” by default.

Security inspection

Inspection type

General
Inspection level

IPS (Detect and block)	If this option is selected, NETASQ’s IPS (*Intrusion Prevention System*) will detect and block intrusion attempts, from the Network level to the Application level in the OSI model.
IDS (Detect)	If this option is selected, NETASQ’s IDS (*Intrusion Detection System*) will detect intrusion attempts on your traffic, without blocking them.
Firewall (Do not inspect)	This option only provides access to basic security functions and will merely filter your traffic without inspecting it.

Configuration

Auto, Config 00 to 09 [by default]	You can customize the configuration of your security inspection by assigning a predefined policy to it, which will appear in the filter table. Numbered configurations can be renamed in the menu Application protection\Inspection profiles.

Application inspection	
Antivirus	The **On**/**Off** buttons allow you to enable or disable the antivirus in your filter rule.
Antispam	The **On**/**Off** buttons allow you to enable or disable the antispam in your filter rule.
URL Filtering	Select a URL filter policy from the policies offered. You can choose whether to enable it (**On**/**Off** buttons).
SMTP Filtering	Select an SMTP filter policy from the policies offered. You can choose whether to enable it (**On**/**Off** buttons). **NOTE** Selecting the SMTP filter policy also enables the POP3 proxy in the event the filter rule allows the POP3 protocol.
FTP Filtering	The **On**/**Off** buttons allow you to enable or disable FTP filtering in your filter rule.
SSL Filtering	Select an SSL filter policy from the policies offered. You can choose whether to enable it (**On**/**Off** buttons).

Comments

You can add a description that will allow distinguishing your filter rule and its characteristics more easily.

Checking the policy in real time

The firewall's filter 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 filter policy is in avoiding the creation of rules that inhibit other rules. When a filter policy is voluminous, the administrator's task becomes even more crucial as the risk increases. Furthermore, during the advanced configuration of very specific filter rules, the multiplicity of options may give rise to the creation of a wrong rule that does not meet the administrator's needs.

To prevent this from happening, the editing screen for filter rules has a "**Check policy**" field (located under the filter table), which warns the administrator whenever a rule inhibits another or an error has been created on one of the rules.

Example
If you "**pass**" all types of traffic ("**Any**") in Rule 1, any attempt to block other traffic in Rule 2 will be denied.

The following message will appear:

[Rule 2] This rule will never be applied as it is covered by Rule 1.

NOTE
Before version 9.0.1, in the ***Destination*** column and the "Advanced properties" tab, the filter table allowed setting the destination port as the port to which packets are translated.
This setting has been moved ***from version 9.0.1 onwards,*** to the ***Protocol*** column for translations of the selected ***Destination***.

"NAT" tab

The principle of NAT (*Network Address Translation)* is to convert an IP address to another when passing through the firewall, regardless of the source of the connection. It is also possible to translation ports through NAT.

GENERAL NOTE:

Each time you come across a drop-down list of objects in the columns (except "Status" and "Action**"**) a mathematical operator icon will appear ( ). It can only be used if an object other than "**Any**" has been selected.

You can therefore customize the parameters of your traffic using the following icon in 4 different ways:

- "**=**" (or): the value of the attribute corresponds to what is selected.
- "!=" (or) the value of the attribute is different from what has been selected.
- "<" (or ; used for source and destination ports only): the port number of the traffic is lower than what is selected.
- ">" (or ; used for source and destination ports only): the port number of the traffic is higher than what is selected.

From version 9.0.1 onwards, if you click quickly 10 times on the "Up" button, you will see that the rule moves up but the waiting window will only appear when you leave the button for 2 or 3 seconds. And at the end, only a single command will be executed.

NOTE

Rules can be moved more much fluidly as such..

Actions on NAT policy rules

Search	This field allows performing searches by occurrence, letter or word. **Example:** If you enter "Any" in the field, all NAT rules containing "Any" will be displayed in the table.
New rule	Inserts a blank line after the selected line, 3 choices are available: • **Standard rule:** This option allows creating a dynamic NAT rule. This type of rule allows converting multiple IP addresses into one or N IP addresses (a public IP address, for example). • M**asquerading rule**: This option allows creating a PAT (Port Address Translation) dynamic NAT rule. This type of rule allows converting multiple IP addresses into one or N IP addresses. The source port is also rewritten. • **Separator – rule grouping**: This option allows inserting a separator above the selected rule in order to add a comment on a line to edit the NAT, for example. The aim of this option is to group rules until the next separator. You can collapse or expand the node of the separator in order to show or hide the rule grouping. • **Static NAT rule:** The principle of static address translation is to convert an IP address (or N public IP addresses) to another (or N private IP addresses) when going through Firewall, whatever the origin of the connection. A wizard window will allow you to map a private IP address to a public (virtual) IP address by defining their parameters. You must also choose from the drop-down lists the **Private**

	and **virtual hosts** for your IPs, as well as the interface on which you wish to apply them. The **Advanced properties** field allows restricting the application to a port or port group, and enabling ARP publication, which may make the IP to be published available via the firewall's MAC address. Click on **Finish** to confirm your configuration. **NOTE** 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.
Delete	Deletes the selected line. **NOTE** Several lines can be deleted at the same time, by selecting them with the "Ctrl" key and pressing on **Delete**.
Up	Places the selected line before the line just above it.
Down	Places the selected line after the line just below it.
Collapse all	This button allows collapsing all folders in the filtering directory.
Expand all	This button allows expanding all folders in the filtering directory.
Copy	This button allows you to copy a filter rule in order to duplicate it.
Paste	This button allows you to duplicate a filtering rule after having copied it.
Reset columns	When you click on the arrow on the right in the field containing a column's name (example: **Status**), you will be able to display additional columns or remove columns so that they will not be visible on the screen, by ticking or unticking them. **Example:** Tick the options "**Nom**" and "**Src port**" which are not displayed by default. By clicking on **reset columns**, your columns will be reset to their original settings, before you selected any additional columns. As such, "**Nom"** and "**Src port**" will be hidden again.

NAT table

The NAT table is divided into two part: **Original traffic (before translation)**, and **Traffic after translation.**

Status	Status of the rule: **On**, the rule has been enabled and will be used by the NETASQ firewall. **Off**, the rule has been disabled: double-click the field to enable or disable the rule. **REMARK** The firewall will assess rules in their order of appearance on the screen: one by one from the top down. Once it comes upon a rule that corresponds to the request, the will perform the specified action and stop there.

From version 9.0.1 onwards, source address translation manages stateless IP protocols (GRE) but with the following restriction:

If two clients go through the same firewall, they will not be able to connect to the same server at the same time.
NETASQ'S intrusion prevention engine will block packets received by the second client.
After 5 minutes, the intrusion prevention engine will deem the session too old and will allow the second client to take over.

Original traffic (before translation)

By clicking in the column "Source" a configuration window will appear:

Traffic source before translation

"General" tab
General

User	The rule will apply to the user that you select in this field. There are three choices by default: **"No user":** This option allows clearing the user field and to no longer apply any criteria for the rule. **"Any user":** refers to any authenticated user. **"Unknown users":** refers to any unknown or unauthenticated user.
Source hosts	The rule will apply to the object that you select in this field. The source host is the host from which the treated packet originated: it is the sender of the packet. **NOTE** Several objects can be specified at the same time.
On the interface	Interface on which the translation rule applies, presented in the form of a drop-down list. By default, the firewall selects it automatically according to the operation and source and destination IP addresses. It can be modified to apply the rule to another interface.

Click on **Ok** to confirm your configuration.

"Advanced properties" tab
Advanced properties

Source port	This field allows specifying the port used by the source host. By default, the "Stateful" module memorizes the source port used and only this port will then be allowed for return packets.
Source DSCP	This field refers to the DSCP code of the received packet.

Click on **Ok** to confirm your configuration.

Next, the outgoing interface of the traffic has to be defined:

Traffic destination before translation

"General" tab
General

Destination hosts	Select the destination host of the traffic from the object database in the drop-down list.
Destination port	If you wish to translate the destination port of the traffic, select one from the objects in the drop-down list. The object "Any" is selected by default.

From version 9.0.1 onwards, types of load balancing other than connection hashing can now be selected with a range of destination ports.

Click on **Ok** to confirm your configuration.

"Advanced properties" tab
Advanced properties

From the interface	Interface from which the traffic will leave the firewall before translation. By default, the firewall selects it automatically according to the operation and source and destination IP addresses. It can be modified to restrict the rule to a particular interface.

Traffic after translation

Source of the traffic after translation

"General" tab

Translated source host	The rule will apply to the object that you select in this field. The translated source host refers to the new IP address of the source host, after its translation by NAT.
Translated source port	This field allows specifying the source port used by the source host after translation. By default, "Stateful" mode memorizes the source port used and it will be the only port allows for return packets.
Select a random translated source port	By selecting this option, the firewall will randomly select the translated source port from the list.

Click on **Ok** to confirm your configuration.

"Advanced properties" tab

Load balancing	This option allows distributing IP addresses of sources that sent the packet after translation. The load distribution method depends on the algorithm used. Several load balancing algorithms are available: **None:** No load balancing will be carried out. **Round-robin:** This algorithm allows fairly distributing the load among the various IPs of the selected address range. Each of these source IP addresses will be rotated. **Source IP hash:** The source address will be hashed in order to choose the address to use from the range. This method allows guaranteeing that a given source address will always be mapped to the same address range. **Connection hash: :** Users can now choose the hash by connection (source port + source IP address) as a load balancing method in their NAT rules. This allows connections from one source to the same server to be distributed according to the source port and source IP address. **Random:** The firewall randomly selects an address from the selected address range
ARP publication	This option makes the IP address to be published available via the firewall's MAC address.

Click on **Ok** to confirm your configuration.

Traffic destination after translation

"General" tab

Translated destination host	This field allows selecting the destination host of the translated packet from the drop-down list of objects.
Translated dest. port	This field allows specifying the port used by the destination host.

Click on **Ok** to confirm your configuration.

"Advanced properties" tab

Load balancing	This option allows distributing the transmission of packets among several destination IP addresses. The load distribution method depends on the algorithm used. Several load balancing algorithms are available: **None**: No load balancing will be carried out. **Round-robin**: This algorithm allows fairly distributing the load among the various IPs of the selected address range. Each of these source IP addresses will be rotated. **Source IP hash**: The source address will be hashed in order to choose the address to use from the range. This method allows guaranteeing that a given source address will always be mapped to the same address range. **Connection hash:** Users can now choose the hash by connection (source port + source IP address) as a load balancing method in their NAT rules. This allows connections from one source to the same server to be distributed according to the source port and source IP address. **Random**: The firewall randomly selects an address from the selected address range
Ports	This option allows distributing the transmission of packets among several destination ports. The load distribution method depends on the algorithm used. The load balancing algorithms are the same as the ones described earlier.
ARP publication	This option makes the IP address to be published available via the firewall's MAC address.

Click on **Ok** to confirm your configuration.

Options

NAT inside IPSec tunnel (before encryption, after decryption)	If the option has been selected, the encryption policy will be applied to the translated traffic. The NAT operation is performed just before encryption by the IPSec module when packets are sent and after decryption when packets are received.

Comments

You can add a description that will make it possible to refine your NAT rule and its characteristics.

Example of a NAT rule

Original traffic (before translation)	Traffic after translation

Source	Destination	Dest port	Destination
Internet on	**Virtual_mail server**	**smtp**	**Internal_mail server**
			ARP

Checking the policy in real time

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 the creation of a wrong rule that does not meet the administrator's needs.

To prevent this from happening, the editing screen for filter rules has a "**Check policy**" field (located under the filter table), which warns the administrator whenever a rule inhibits another or an error has been created on one of the rules.

Example
If you "**pass**" all types of traffic ("**Any**") in Rule 1, any attempt to block other traffic in Rule 2 will be denied.

The following message will appear:

[Rule 2] This rule will never be applied as it is covered by Rule 1.

HIGH AVAILABILITY

This module will allow you to create first of all, a cluster or a group of firewalls. Once this is done, another firewall can be added to join the cluster that you have just initialized.
NETASQ's high availability operates in "Active/passive" mode: Consider a cluster containing 2 firewalls. If the firewall considered "active" fails, or if a cable has been disconnected, the second firewall considered "passive" will transparently take over. As such, the "passive" firewall becomes "active".
The configuration of high availability takes place in 4 steps:

- Step 1: Creating a cluster/joining an existing cluster
- Step 2: Configuring network interfaces: the main link and the secondary link (optional)
- Step 3: Defining the cluster's pre-shared key
- Step 4: Summary of the steps and application of configured settings

Once you are done with these 4 steps, a new screen will appear suggesting new configurations within the high availability module.

Step 1: Creating or joining a high availability cluster

Create a cluster	If this option is selected, the firewall will be prepared to receive other firewalls and will add itself to the cluster.
Join a cluster	If this option is selected, the appliance will attempt to connect to the firewall with the IP address defined during the creation of the cluster. As such, this second firewall will retrieve information from the first and synchronize with it. The cluster therefore comprises two firewalls: when the first firewall fails, the second will take over transparently. **NOTE** At the end of the wizard, the appliance will be rebooted. Once the reboot is complete, the appliance will be part of the cluster, and therefore no longer exists as an entity, but as a member of the cluster. **WARNING** If you choose to "join" a cluster, it implies that you have already created one beforehand, and have selected the option "**Create a cluster**)" and have performed the necessary configuration to set it up on the first firewall.

WARNING
It is important to avoid creating a cluster twice, as this would mean that you would be setting up two high availability clusters, each containing a firewall, and not a high availability cluster containing 2 firewalls.

From version 9.0.2 onwards, a member of a cluster can be forced to be the active firewall, even if members of the group have differing firmware versions.

Step 2: Configuring network interfaces

If you have chosen to create a cluster

Main link

Interface	Main interface used for linking two firewalls that make up the cluster. Select it from the list of objects in the drop-down list.
Define the IP address	Enter the IP address to which your firewall cluster will need to connect in order to function.
Define the network mask	Enter the network mask for you firewall cluster.

Secondary link (optional)

If the firewall does not receive responses on the main link, it will attempt to connect to this secondary link. This will prevent both firewalls from switching to active/active mode if a problem arises on the main link.

Use a second communication link	Select this option in order to enable the fields below it and to define a secondary link for your cluster.
Interface	Secondary interface used for linking both firewalls that make up a cluster. Select it from the list of objects in the drop-down list.
Define the IP address	Enter the IP address for your secondary link.
Define the network mask	Enter the network mask for you secondary link.

NOTE

In order for a link to work, both members of the cluster have to use the same interface.

If you have chosen to join a cluster

This option assumes that a cluster has already been created beforehand, in order for a firewall to be able to join it.
As such, some of the information from the first firewall created will be copied.

Main link

Interface	Main interface used for linking two firewalls that make up the cluster. This has to be the same interface that you had selected during the creation of the cluster on the first firewall.
Define the IP address	The IP address to which your firewall cluster will need to connect in order to function. This address has to belong to the same sub-network as the one defined during the creation of the cluster on the first firewall.
Define the network mask	The network mask for you firewall cluster. This has to be the same mask that you had used during the creation of the cluster on the first firewall.

Secondary link (optional)

If the firewall does not receive responses on the main link, it will attempt to connect to this secondary link. This will prevent both firewalls from switching to active/active mode if a problem arises on the main link.

Use a second communication link	Select this option in order to enable the fields below it and to define a secondary link for your cluster. This option must only be selected if it was also selected during the creation of the cluster on the first firewall.
Interface	Secondary interface used for linking both firewalls that make up a cluster. This has to be the same interface that you had selected during the creation of the cluster on the first firewall.
Define the IP address	IP address for your secondary link. This address has to belong to the same sub-network as the one defined during the creation of the cluster on the first firewall.
Define the network mask	Network mask for you secondary link. This has to be the same mask that you had used during the creation of the cluster on the first firewall.

NOTE

In order for a link to work, both members of the cluster have to use the same interface.

Step 3: Cluster's pre-shared key

If a cluster is being created

To secure the connection between members of the cluster, you will need to define a pre-shared key. This key will only be used by firewalls that are joining the cluster for the first time.

New pre-shared key	Define a password/pre-shared key for your cluster.
Confirm	Confirm the password/pre-shared key that you have just entered in the previous field.
Password strength	This field indicates the security level of your password: "Very weak", "Weak", "Medium", "Strong" or "Excellent". The use of uppercase and special characters is strongly advised.

Click on **Next**.

If a cluster exists

IP address of the firewall to contact	Enter the IP address that you had defined in the wizard during the creation of the cluster (IP address of the main or secondary link).
Pre-shared key	Enter the password/pre-shared key that you had defined in the wizard during the creation of the cluster. This icon allows you to view the password in plaintext to check that it is correct.

Step 4: Summary

If a cluster is being created

After having viewed the summary of your configurations, click on **Finish.** The following message will appear:
This firewall is ready to run in high availability. You may now configure another firewall to add it to the cluster.
Now that your cluster has been created, a new screen will appear when you attempt to access this module.

If a cluster exists

After having viewed the summary of your configurations, click on **Finish.** The following message will appear:
This firewall has to be rebooted in order to add a firewall to the cluster. Join the cluster?
To confirm the configuration, this firewall will join the cluster and synchronize the initial configuration. It will then restart in order to apply the configuration. To access this cluster, you need to connect to the active firewall.

NOTE
This step may take a long time on entry-level models (U30, U70). Do not unplug the firewall.

High availability screen

Communication between firewalls in the high availability cluster

Configure the main link	Main interface used for linking both firewalls that make up the cluster. Select it from the list of objects in the drop-down list.
Use a second communication link	Select this option in order to enable the fields below it and to define a secondary link for your cluster.
Secondary link	Secondary interface used for linking both firewalls that make up the cluster. Select it from the list of objects in the drop-down list.

WARNING
You are advised to use a secondary link when you wish to change the interface used as the main link. Indeed, changing the link may cause interruptions to communications between members of the cluster, which may lead to a nonoperational cluster.

Advanced properties

Modifying the pre-shared key between firewalls in a high availability cluster

New pre-shared key	This field allows modifying the pre-shared key or the password defined during the creation of the cluster.
Confirm	Confirm the password/pre-shared key that you have just entered in the

	previous field.
Password strength	This field indicates the security level of your password: “Very weak”, “Weak”, “Medium”, “Strong” or “Excellent”. The use of uppercase and special characters is strongly advised.

Quality indicator

Active firewall if equal

This option allows favoring one firewall as the active firewall in the event both firewalls have the same quality.
The aim of favoring an active firewall is to keep as many logs as possible on the same firewall or to favor traffic on a specific firewall. If the active firewall fails, or if a cable is accidentally unplugged, the other firewall will take over as the active firewall.

Automatic	If you select this option, no priority will be assigned.
This firewall (<its serial number >)	By selecting this option, you will set this firewall as the active firewall and the second firewall will take over from it if it malfunctions or is unplugged.
The other firewall (remote) (<its serial number >)	By selecting this option, you will set this firewall as the active firewall and the second firewall will take over from it if it malfunctions or is unplugged. **WARNING** Selecting this option will cause the firewalls to swap immediately, or switch from this firewall as the active firewall, causing a disconnection from the administration interface.

Communication between the firewalls in the high availability cluster

Encrypt communication between firewalls	By default, communication between the firewalls is not encrypted, based on the principle that the link used by high availability is a dedicated link. In some architectures, the high availability link is not dedicated, and if you wish to prevent inter-cluster communications from being read, they can be encrypted (in AES, for example). **WARNINGS** 1) Selecting this option can degrade the performance of your high availability cluster. 2) Only connections, and not their contents, pass through the high availability link.

Optimize swap for network bridges

From version 9.0.3 onwards

An option has been added so that when surrounding appliances change from a cluster to bridge mode, the change is applied faster.

Reboot interfaces in a bridge during the swap	If this option is enabled, interfaces on the bridge are reinitialized at the time of the switch in order to force switches connected to the firewall to renew their ARP tables.

Gracious ARP

Periodically send gracious ARP requests	If this option is selected, you will send ARP announcements at regular intervals so that the different devices on the network (switch, routers, etc) can update their own ARP tables. **NOTE** Even during the passive stage, the firewall will still send an ARP announcement, regardless of this option.
Frequency (in seconds)	This field enables defining the frequency of ARP requests in seconds, to a maximum of 9999 seconds.

Impact of the unavailability of an interface in a firewall's quality indicator

Interface	This column lists all of your firewall's Ethernet interfaces.
Weight [0-9999]	The weight allows giving the interface a relative value. "100" has been set by default for the listed interfaces. They all therefore have the same weighting. This criterion can be modified by selecting the relevant checkbox. E.g. specifying that the "in" interface is more important than the "out" interface and the other interfaces by assigning it a value of 150. **NOTE** It may be useful to set all unused interfaces to 0 so that they will not affect the quality calculation.

From version 9.0.2 onwards, disabled network interfaces no longer appear in the high availability quality calculations.

Next, click on **Apply.**

IDENTIFICATION PORTAL

Logging on

In order to configure your NETASQ firewall, you need to log onto the web administration interface.

Configuration of a firewall is only accessible to administrators of the product. The “super admin” user or the administrator who holds all privileges can assign privileges to users and/or user groups in the menu System\Administrators.

Presentation

The connection module consists of 2 sections:

- A static section
- A collapsible section: options

The information required depends on whether it is the administrator’s first connection to the firewall.

Username	This field is reserved for users who have at least basic privileges.
Password	User’s password, which he will be asked to enter upon his initial connection. For a default configuration, no passwords need to be entered (empty field).
Authentication with SSL certificate	If this option is selected, the fields **Username** and **Password** will no longer be necessary, and therefore grayed out. The following message will appear: *“Using a certificate will allow you to authenticate automatically. Enable automatic authentication?”*. Select **Manual authentication** or **Automatic authentication**. **REMARK** The automatic connection option can be enabled automatically in the section Preferences\Connection settings\ *Connect automatically with an SSL certificate.*
Log in	Clicking on this button or pressing “Enter” will allow sending connection information to the firewall.

WARNING

The NETASQ firewall is case-sensitive and distinguishes uppercase and lowercase letters, both for the username as well as for the password.

Options

Language	Language of the web-based graphical interface. When the user chooses a new language for the web interface, the authentication page will reload in the selected language. English, Spanish, French, Italian and Polish are available.
Read only	Allows connecting in “read-only” mode. As such, you will be able to log onto the firewall without modification privileges using an account that ordinarily has such privileges. This allows the user to refrain from using modification privileges if they are not necessary.

REMARK

- Options are contained in a cookie. The user therefore stores his connection preferences on his browser.
- If the “read only” option has been enabled in a cookie during the connection to the authentication page, to avoid confusion, part of the options will be presented to the user as deployed options.

Error notifications

When a field is empty

If a user attempts to authenticate without having entered the **User** or **Password** field, authentication will not be launched and the message “This field should not be empty” will appear.

When “Caps lock” has been enabled

If this button has been enabled when the user enters his password, a warning icon will indicate that “Caps Lock has been enabled”.

Authentication failure

When authentication fails, the message “*Authentication has failed*” will appear in red.

REMARK

Protection from brute force attacks:
When too many requests are sent with the wrong password, the following message will appear: “*Protection of authentication from brute force attacks has been enabled. The next authentication attempt will be possible in* ***<number of seconds>***”.

The “admin” account, super administrator

By default, only one user has all administration privileges on NETASQ products – the “admin” account (whose login is “admin”). This administrator holds all privileges and can perform certain operations such as the modification of a user’s authentication method, for example.

WARNING

The administrator account has the value “admin” as login **and** password by default.

REMARK

Given the privileges assigned to the “admin” account, NETASQ recommends that you use this account only for tests or maintenance operations.

Only the “admin: user can assign administration privileges to other users.

Logging off

The procedure for logging off the firewall is as follows:

1. Click on  at the top right side of the interface. The window “Quit?” will appear with the following message: “**You are about to be disconnected**”. Click on “**Quit**” or on “Cancel if you do not wish to log off.
2. By clicking on **Quit**, the interface will return to the connection window. Cancelling will return the user to the main screen, without any effect to the execution of the program.

IMPLICIT RULES

Implicit filter rules

This screen shows that it is possible to automatically generate various IP filter rules in order to allow the use of some of the firewall's services. If a service is enabled, the firewall will automatically create the necessary filter rules, without having to create "explicit" rules in the filter policy.

Rule table

This table sets out the following columns:

Enabled	Status of the rule: **Enabled**/**Disabled**: Click on the field to enable/disable the creation of one or several implicit riles. The rule **Allow external (unprotected) interfaces (Authd_ext) to access the authentication portal and the SSL VPN** has been disabled by default.
Name	Name of the implicit rule: this name cannot be modified.

The following rules appear in the "**Name**" column:

- **Allow external (unprotected) interfaces (Authd_ext) to access the authentication portal and the SSL VPN**: a rule allowing access to the https service (port 443) will be created for each external (public) interface. Users can then authenticate and access the SSL VPN from external networks.
- **Allow protected interfaces (Authd_int) to access the authentication portal and the SSL VPN:** a rule allowing access to the https service (port 443) will be created for each internal (protected) interface. Users can then authenticate and access the SSL VPN from internal networks.
- **Block and reinitialize ident requests (port 113) for modem interfaces (dialup).**
- **Block and reinitialize ident requests (port 113) for ethernet interfaces**.
- **Allow protected interfaces to access the firewall's DNS service (port 53)**: users can contact the DNS service and therefore use the DNS cache proxy if it has been enabled.
- **Allow mutual access to the administration server (port 1300) between the members of a firewall cluster (HA)**: this allows the different members of the HA cluster to communicate with each other.
- **Allow access to the PPTP server**: users can contact the firewall via PPTP to access the server, if it has been enabled.
- **Allow protected interfaces (serverd) to access the firewall's administration server (port 1300):** administrators will be able to log on via their internal networks to port 1300 on the firewall. This service is used especially by NETASQ Real-Time Monitor.
- **Allow protected interfaces to access the firewall's SSH port**: allows opening access to the firewall via SSH in order to log on using command lines from a host located on the internal networks.
- **Allow ISAKMP (UDP port 500) and the ESP protocol for IPSec VPN peers:** IPSec VPN peers will be able to contact the firewall via these two protocols, thereby allowing data on the IP traffic to be secured.
- **Allow protected interfaces (WebAdmin) to access the firewall's web administration server (port 443):** administrators will be able to log on via internal networks to port 443, used by the web administration interface.

  NOTE
  This rule allows access to the captive portal, and therefore the web administration interface for all users connected from a protected interface. To restrict access to web

administration (“/admin/” directory), define one or several hosts in the menu System\ Configuration\ Firewall administration tab. A table will allow you to restrict access to these pages at the web application level.

WARNING

The following action may be dangerous:

- **Disabling the “Serverd” rule**: in the absence of an explicit rule, may cause users to no longer have access to tools using port 1300, namely NETASQ RealTime Monitor, GlobalAdmin, NETASQ Event Reporter, NETASQ Centralized Management and NETASQ Event Analyzer.
- **Disabling the “WebAdmin” rule:** you will no longer have access to the web administration interface, unless an explicit rule allows it.

INSPECTION PROFILES

The inspection profile module consists of 2 screens:
- A zone dedicated to the default configuration and a collapsible menu for advanced properties.
- A zone for associating application profiles, accessible by clicking on “**Go to profiles**”.

Security inspection

Global configuration for each profile

Default configuration

Configuration for incoming traffic	Define the profile to apply for incoming traffic on the network via the NETASQ firewall. Incoming traffic represents the traffic of an unprotected interface (such as the internet) to a protected interface (your local/internal network).
Configuration for outgoing traffic	Define the profile to apply for outgoing traffic on the network via the NETASQ firewall. Outgoing traffic represents the traffic of a protected interface (such as the internet) to an unprotected interface.

New alarms

Apply default model to new alarms	This option is related to the Application protection\Alarms module. By enabling it, new alarms will be updated automatically and will be issue with the NETASQ signature. The three options that follow will be grayed out if you have chosen an automatic configuration. If you wish to apply them yourself, unselect the option and define the parameters in the fields that follow.
Action	When an alarm is raised, the packet that set off the alarm will be subject to the action configured. You can choose to **Pass** or **Block** new alarms. You will notice the status you have applied to the Application protection\Alarms module. New alarms can be found in the column “**New**”.
Level	Three levels of alarms are available: "Ignore", "Minor" and "Major".
Packet capture	By selecting this option, the packet that set off the alarm will be captured.

Advanced properties

Apply translation operations (NAT) before IPSec VPN	This option means that the IP addresses will be modified before the encryption performed by the IPSec VPN.
Treat IPSec interfaces as internal interfaces	When a host attempts to access a protected interface via an IPSec VPN tunnel, its data will be decrypted and saved. The host will therefore change from a remote network (or have a status of an external interface) to a local network (or to the status of an internal interface).

Configuring profiles

This screen consists of 2 sections:

- A zone for editing various possible profile configurations
- A zone for associating protocol profiles

Select the application profile associated with the protocol from the drop-down list by clicking on the arrow to the right of the field.
To return to the previous menu, click on “**Go to global configuration”**.

IPSEC VPN

A standard protocol, IPSec (IP Security) enables the creation of VPN tunnels between two hosts, between a host and a network, between two networks and any type of object that supports the protocol.

The services that NETASQ's IPSec offers provide access control, integrity in offline mode, authentication of data source, protection against replay, confidentiality in encryption and on traffic.

You can for example, create a tunnel between two firewalls, or between the firewall and mobile clients on which VPN clients would be installed.

The IPSec VPN module consists of 4 tabs:

- Encryption policy – Tunnels: this tab allows creating your IPSec tunnels between two firewalls (**Site to site – Gateway- Gateway**) or between a NETASQ multi-function firewall and a mobile user (**Anonymous – Mobile users**). 10 blank encryption policies can be configured, activated and edited. The anonymous policy also allows configuring tunnels with another firewall, but which does not have a fixed IP address. It will therefore have the same problem as a "classic" mobile workstation: an unpredictable IP address
- Peers: here, you can create new peers (remote site or anonymous mobile peer) by entering their **IKE profiles**, their negotiation method, as well as the specific parameters for each negotiation method.
- Identification: this tab allows listing your approved certificate authorities in the tunnels using PKI methods as well as the pre-shared keys (PSK) of your mobile tunnels in two tables.
- Encryption profiles: here, define your IKE (phase 1) and IPsec (phase 2) encryption profiles, add new ones or set their maximum lifetime (in seconds). You can also define negotiation proposals for authentication and encryption algorithms.

"Encryption policy – Tunnels" tab

Profile bar	The drop-down menu offers 10 IPSec profiles numbered from (1) to (10). To select a profile in order to configure it, click on the arrow to the right of the field.
Activate this policy	Immediately activates the selected IPSec policy: parameters saved in this slot will overwrite current parameters in force.
Edit	This function allows performing 3 operations on profiles: • **Rename:** by clicking on this option, a window comprising two fields will appear. It will allow you to modify the name and add comments. Once the operation has been performed, click on "Update". This operation can also be cancelled. • **Reinitialize**: Deletes all changes made to the profile • **Copy to:** This option allows copying a profile to another, with all the information from the copied profile transmitted to the receiving profile. It will also have the same name.
Last modification	This icon allows finding out the date and time of the last modification.

Disable policy	This button allows immediately deactivating the selected IPSec policy.

From version 9.0.2 onwards, static routes can now be added on an IPSec interface..

Site to site (Gateway-Gateway)

This tab will allow creating a VPN tunnel between two compatible network devices.
This process is also called a *Gateway to Gateway VPN tunnel*.

Search	Searches will be performed on the name of the object and its various properties, unless you have specified in the preferences of the application that you would like to restrict this search to object names only.
Delete	Select the IPSec VPN tunnel to be removed from the table and click on this button. **WARNING** No confirmation window will appear and your rule will be deleted directly.
Up	Places the selected line before the line just above it.
Down	Places the selected line after the line just below it.

Add

In order to configure the tunnel, select the VPN policy in which you wish to set it up. The IPSec VPN policy wizard will guide you through the configuration.

Site to site tunnel

Here, you will define each of the endpoints for your tunnel as well as for your peer.

Peer selection	This is the object that corresponds to the public IP address of the tunnel endpoint, or of the remote VPN peer. The drop-down list displays “None” by default. You can create peers in the following option or select an existing peer from the list.
Create a peer	Define the parameters for your peer. Several steps are necessary: 1 Selecting the gateway: ***Remote gateway:*** select the object corresponding to the IP address of the tunnel endpoint from the drop-down list. You can also add gateways using the + button. ***Name*:** you can specify a name for your gateway or keep the peer’s original name, which will be prefixed with “Site_” (“Site_<name of object>“). Click on **Next**. 2 Identifying the peer: 2 choices are possible, identification via **Certificate** or by **Pre-shared key (PSK)**. Select the desired option. 1) If you have selected **Certificate**, you will need to select it from those you have previously created in the Certificates and PKI module.

2) If you have selected **Pre-shared key (PSK),** you will need to define the secret that both peers of the IPSec VPN tunnel will share, in the form of a password to be confirmed in a second field.

You can **Enter the key in ASCII characters** (every character in ASCII text is stored in a byte whose 8th is 0) by selecting the relevant option.

Unselect the option to view the key in hexadecimal characters (which is based on 16 digits: the letters A to F and numbers 0 to 9).

Click on **Next.**

3 Finish creating the peer:

The screen will show you a window summarizing the configuration that was made, the **Parameters of the remote site** and the **Pre-shared key**.

You can also add a backup peer by clicking on the link provided. You will need to define a remote gateway.

Click on **Finish**.

Local network	Host, host group, address range, network or network group that will be accessible via the IPSec VPN tunnel.
Remote network	Host, host group, address range, network or network group that references the VPN peer as the counterpart of your firewall and vice versa. Both peers must be able to negotiate traffic from either side.

Star configuration

This procedure consists of directing several VPN tunnels to a single point. It allows, for example, linking agencies to a central site.

Local network	Select your host, host group, address range, network or network group that will be accessible via the IPSec VPN tunnel, from the drop-down list of objects.
Remote sites	Define the parameters for your remote sites: select your peer from the list of those already created or click on the icon » to create a new one and select the remote networks from the objects in the drop-down list. You can **Add** or **Delete** peers by clicking on the relevant buttons.
Treat remote networks as internal networks	By default, the IPSec interface is considered an external interface. By selecting this option, the interface will switch to “protected” mode.

Click on **Finish**.

Separator – rule grouping

This option allows inserting a separator above the selected line. This allows the administrator to create a hierarchy for his tunnels according to his needs.

The table

Line	This column indicates the number of the line treated in order of appearance on the

	screen.
Status	This column shows the status **On**/**Off** of the tunnel. When you create tunnels, they are active by default. Click once to disable them.
Local network	Select the host, host group, address range, network or network group that will be accessible via the IPSec VPN tunnel, from the drop-down list of objects.
Peer	Configuration of the peer, which can be viewed in the tab of the same name in the IPSec VPN module.
Remote network	Select from the drop-down list of objects, the host, host group, address range, network or network group that references the VPN peer as the counterpart of your firewall; for example the known public IP address of your peer.
Encryption profile	This option allows selecting the protection model associated with your VPN policy, from the choice of 3 preconfigured profiles: **StrongEncryption, GoodEncryption and FastEncryption.** Other profiles can be created or modified in the tab "Encryption profiles".
Comments	Description given of the VPN policy.

Anonymous – Mobile users

The IPSec VPN has two endpoints: the tunnel endpoint and the traffic endpoint. For anonymous or mobile users, the IP address of the tunnel's endpoint is not known in advance.
As for the IP address of the traffic endpoint, it can either be chosen by the peer ("classic" case) or given by the gateway ("Config mode").

Name of the mobile configuration

By default, the drop-down list will display the message "no peer found", but this can be fixed by following the procedure below in **" Mobile peer creation"** part.

VPN clients parameters (Config Mode) *- From version 9.0.2 onwards -*

For mobile users, a DNS server can now be defined and areas in which this server is used can be specified. These indications are indispensable, for example, in the event an Apple® mobile client is used (iPhone, iPad). This feature is tied up with the config mode, and is not used by all VPN clients on the market.

DNS Server	This field determines the host (DNS server) that will be used by mobile clients in order to perform DNS resolutions. You can select it or create it in the objects database. This field is empty by default.

Table of domains used by the DNS server (depends on the VPN client)

The client will use the DNS server selected earlier, only for domains specified in this table. For other domains, the client will continue to use his system DNS server(s). These will generally be internal domains.

Example

If the domain "netasq.com" is selected, an iPhone for example will use the DNS server specified above by contacting "www.netasq.com" or "intranet.netasq.com". However, if it attempts to contact "www.google.fr", it will continue to use its former DNS servers.

Add	Domain names can be added to the list.

Delete	Select the name of the domain to be removed from the list and click on **Delete**.

Mobile Peer Creation

The procedure for creating a mobile peer is as follows:

1 Click on the button "**Add**" a "**New policy**" (VPN), then on "**Create a mobile peer**" via the mobile IPSec VPN policy wizard.

2 Name your mobile configuration, and click on **Next**.

3 Select the authentication method of the peer.

Certificate	If you select this authentication method, you will need to select the **Certificate** (server) to be presented to the peer, from the list of those you have already created previously (Certificates and PKI module). You can also enter details about the **Certificate authority** (CA) that signed your peer's certificate.
Hybrid	If you select this hybrid method, you will need to provide the **Certificate** (server) to be presented to the peer and probably its CA. It is used with IKE and is different from the various authentication methods, which combine the use of certificates and a pre-shared key.
Certificate and XAuth (iPhone)	This option allows mobile users to connect to your company's VPN gateway via their mobile phones, using a certificate. **NOTE** This is the only mode compatible with iPhones.
Pre-shared key (PSK)	If you have chosen this authentication method, you will need to edit your key in a table, by providing its ID and its value to be confirmed. To do so, click on **Add**. The ID may be in an IP address (X.Y.Z.W), FQDN (monserver.domain.com), or e-mail address format (toto.dupont@domain.com). It will then occupy the "Identity" column in the table and the pre-shared key will occupy a column of the same name with its value displayed in hexadecimal.

Click on **Next**.

4 Check the summary of you mobile configuration and click on **Finish**.

5 Next, enter the local resource, or "**local network**" to which your mobile user will be directed.

Other operations can also be performed:

Search	Searches will be performed on the name of the object and its various properties, unless you have specified in the preferences of the application that you would like to restrict this search to object names only.
Delete	Select the IPSec VPN tunnel to be removed from the table and click on this button. **WARNING** No confirmation window will appear and your rule will be deleted directly.
Up	Places the selected line before the line just above it.
Down	Places the selected line after the line just below it.

The table

Line	This column indicates the number of the line treated in order of appearance on the screen.
Status	This column shows the status **On**/**Off** of the tunnel. When you create tunnels, they are active by default. Click once to disable them.
Local network	Select the host, host group, address range, network or network group that will be accessible via the IPSec VPN tunnel, from the drop-down list of objects.
Peer	Configuration of the peer, which can be viewed in the tab of the same name in the IPSec VPN module.
Remote network	Select from the drop-down list of objects, the host, host group, address range, network or network group that references the VPN peer as the counterpart of your firewall. **NOTE** When creating a new mobile IPSec VPN policy via the wizard, you will be asked to enter details about the local network, and not the remote network, since the IP address is unknown. The object “Any” will therefore be selected by default.
Encryption profile	This option allows selecting the protection model associated with your VPN policy, from the choice of 3 preconfigured profiles: **StrongEncryption, GoodEncryption and FastEncryption.** Other profiles can be created or modified in the tab “Encryption profiles”.
Config mode	This column makes it possible to activate “Config mode”, which is disabled by default. This allows distributing the traffic endpoint IP address to the peer **NOTES** 1) If you choose to activate this mode, you will need to select an object other than “Any” as the remote network. 2) With config mode, only one policy can be applied per profile.
Comments	Description given of the VPN policy.

REMARK
Only one mobile (“roadwarrior”) user can be used and created for each IPSec profile.
Peers can be applied to all profiles.

“Peers” tab

This tab consists of two sections:
- Left: the list of IPSec VPN and mobile IPSec VPN peers.
- Right: Information about the selected peer.

List of peers

Search in peers	This field allows performing searches on the name of the object and its various properties, by occurrence, letter or word.

Filter	3 choices are possible: You can view "**All peers**" in the lists, including gateways and mobile users. You can also choose to view only "**Gateways**" or only "**Mobile peers**".
Add	Peers can be added to this area. To do so, select the type of peer to create from the drop-down list: a "**New remote site**" or a "**New anonymous (mobile) peer**". You can also "**Copy from the selection**" – the copied peer will be duplicated. To do this, click on the peer to be copied and enter its new name in the window that appears.
Delete	Select the peer to be deleted from the list and click on **Delete**.
Name	Name given to the peer during the creation phase.

Peer information

"Gateway" peer

Comments	Description given of the local peer.
Remote gateway	Object selected as the remote gateway during the creation of the peer via the wizard.
Backup configuration	This field indicates whether you have defined a backup configuration during the creation of the peer. "None" will appear by default if you have not created any. However, you can define one by selecting it in the drop-down list containing your other remote peer.
IKE profile	This option allows selecting the protection model associated with your VPN policy, from the choice of 3 preconfigured profiles: **StrongEncryption, GoodEncryption and FastEncryption.** Other profiles can be created or modified in the tab "Encryption profiles".

Identification

Authentication method	This field will show the authentication method selected during the creation of your peer via the wizard. You may modify your choice by selecting another method from the drop-down list. **NOTE** For a "gateway" peer, you have the choice of **Certificate** or **Pre-shared key (PSK)**.
Certificate	If you have chosen the certificate authentication method, this field will display your certificate. If you had opted for the pre-shared key method, this field will be grayed out.
Local ID (Optional)	This field represents an IPSec VPN tunnel endpoint, sharing the "secret" or the PSK with the "Peer ID", the other endpoint.You are represented by the "Local ID".
Peer ID	This field represents an IPSec VPN tunnel endpoint, sharing the "secret" or the PSK with the "Local ID", the other endpoint. The "Peer ID" represents your peer.

Pre-shared key (ASCII)	In this field your PSK appears in the format you had selected earlier when creating the peer via the wizard: ASCII or hexadecimal characters (the format can be selected in the checkboxes below the field if you wish to change formats).
Confirm	Confirmation of you pre-shared key (PSK).

Advanced properties

Negotiation mode	In IPSec, 2 negotiation modes are possible: main mode and aggressive mode. They have particular influence over Phase 1 of the IKE protocol (authentication phase). **Main mode**: In this 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**: In this 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.
Backup mode	The backup mode is the switch mode for the IPSec failover – if a server fails, another will take over transparently. Two choices are possible: "**temporary**" mode: the main peer will be contacted as soon as possible. "**permanent**" mode: if the peer cannot be contacted, you will switch to another peer. **NOTE** This field can only be edited in expert mode (CLI).
Local gateway	Object selected as the local gateway. This field is set to "Any" by default.
Do not initiate the tunnel (Responder only)	If this option is selected, the IPSEC server will be put on standby. It won't initiate tunnel negotiation. This option is used in the case where the peer is a mobile host.
DPD	This field enables configuring the VPN feature called DPD *(Dead Peer Detection)*, which allows checking whether a peer is still active. When DPD has been enabled on a peer, the peer will regularly send packets or messages to the other peer, to which the latter peer will respond by signaling its presence. These exchanges are secured via ISAKMP (*Internet Security Association and Key Management Protocol*) SAs. If it is detected that a peer is no longer responding, the negotiated SAs will be destroyed. **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**: **Inactive:** DPD requests from the peer are ignored. **Passive**: DPD requests sent by the peer get a response from the firewall. However, the firewall does not send any.**Low:** the frequency of DPD packets being sent is low and the number of failures tolerated is higher. **High**: the frequency of DPD packets being sent is high and the number of failures relatively low.

NOTE

For each field that contains “Gateway” and the icon +, you can add an object to the existing database by specifying its name, DNS resolution, IP address and then clicking on **Apply**.

From version 9.0.1 onwards, when the authentication duration expires or access to the SSL VPN is denied, the user will be redirected to the transparent authentication page (SSO) if this method is available.

“Mobile” peer

Comments	Description given of the remote peer.
Remote gateway	This field is grayed out for mobile peers.
Backup configuration	This field is grayed out for mobile peers.
Encryption profile	This option allows selecting the protection model associated with your VPN policy, from the choice of 3 preconfigured profiles: **StrongEncryption, GoodEncryption and FastEncryption.** Other profiles can be created or modified in the tab “Encryption profiles”.

Identification

Authentication method	This field will show the authentication method selected during the creation of your peer via the wizard. You may modify your choice by selecting another method from the drop-down list. **NOTE** For “mobile” peers, you have a choice between **Certificate**, **Pre-shared key (PSK)**, **Hybrid, Certificate and XAuth (iPhone).**
Certificate	If you have chosen the **Certificate**, **Hybrid** or **Certificate** and **XAuth** authentication method, this field will display your certificate or will suggest that you select it from the drop-down list. If you had opted for the pre-shared key method, this field will be grayed out.
Local ID (Optional)	This field represents an IPSec VPN tunnel endpoint, sharing the “secret” or the PSK with the “Peer ID”, the other endpoint. You are represented by the “Local ID” **NOTE** This field can only be accessed if you have selected the **Pre-shared key** authentication method.

Click here to edit the PSK list	By clicking on this link, you will switch to the "**Identification**" tab in the IPSec VPN module. You can add you **Approved certificate authorities** as well as your M**obile tunnels: pre-shared keys**.

Advanced properties

Negotiation mode	In IPSec, 2 negotiation modes are possible: main mode and aggressive mode. They have particular influence over Phase 1 of the IKE protocol (authentication phase). **Main mode**: In this 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**: In this 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. **NOTE** NETASQ recommends the use of certificate, hybrid or XAuth authentication methods with the main mode. If the client wishes to use the PSK, he has to use the aggressive mode. **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.
Backup mode	The backup mode is the switch mode for the IPSec failover – if a server fails, another will take over transparently. Nonetheless, the field is grayed out here as the backup configuration cannot be applied to a mobile configuration. **NOTE** This field can only be edited in expert mode (CLI).
Local gateway	Object selected as the local gateway. This field is set to "Any" by default.
Do not initiate the tunnel (Responder only)	If this option is selected, the IPSEC server will be put on standby. It won't initiate tunnel negotiation. This option is used in the case where the peer is a mobile host.
DPD	This field enables configuring the VPN feature called DPD *(Dead Peer Detection)*, which allows checking whether a peer is still active. When DPD has been enabled on a peer, the peer will regularly send packets or messages to the other peer, to which the latter peer will respond by signaling its presence. These exchanges are secured via ISAKMP (*Internet Security Association and Key Management Protocol*) SAs. If it is detected that a peer is no longer responding, the negotiated SAs will be destroyed.

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**:

Inactive: DPD requests from the peer are ignored.

Passive: DPD requests sent by the peer get a response from the firewall. However, the firewall does not send any. **Low:** the frequency of DPD packets being sent is low and the number of failures tolerated is higher.**High**: the frequency of DPD packets being sent is high and the number of failures relatively low.

"Identification" tab

Approved certificate authorities

This table will allow you to list the authorities in order to identify your peers within the IPSec VPN module.

Add	When you click on this button, a window will open showing the CAs and sub-CAs that you have created earlier. Select the authorities that will enable you to check the identities of your peers, by clicking on **Select**. The CA or sub-CA selected will be added to the table.
Delete	Select the CA to be removed from the list and click on **Delete**.

CA

Below this field, the added and approved certificate authorities will be displayed.

Mobile tunnels: pre-shared keys

If you had created a mobile peer using the **Pre-shared key (PSK)** authentication method, this table will be pre-entered.
You would have edited a key by assigning it an ID and a value (in hexadecimal or ASCII characters).

Search	Even though the table displays all the pre-shared keys of your mobile tunnels by default, you can search by occurrence, letter or word, so that only the desired keys are displayed.
Add	When you click on this button, a key editor window will appear: you need to provide it with an ID, a value and confirm it. You can choose to edit characters in hexadecimal or ASCII.
Delete	Select the key to be removed from the list and click on **Delete**.

Identity

This column displays the IDs of your pre-shared keys, which may be represented by a domain name (FQDN), an e-mail address (USER_FQDN) or an IP address.

Key

This column displays the values of your pre-shared keys in hexadecimal characters.

REMARKS

An unlimited number of pre-shared keys can be created.

Deleting a pre-shared key that belongs to an IPSec VPN tunnel will cause this tunnel to malfunction.

"Encryption profiles" tab

Default encryption profiles

The mass deployment and use of IPSec requires an extendable and automated protocol for managing standard SAs on the internet. By default, the automated key management protocol selected for IPSec is IKE.
IKE takes place in 2 negotiation phases:

IKE (Phase 1) encryption profile

Phase 1 of the IKE protocol aims to set up an encrypted and authenticated communication channel between both VPN peers. This "channel" is called ISAKMP SA (different from the IPSec SA). Two negotiation modes are possible: main mode and aggressive mode.

The drop-down list allows choosing the protection model associated with your VPN policy, from 3 pre-configured profiles: **StrongEncryption, GoodEncryption,** and **FastEncryption**. Others may also be created.

IPSec (Phase 2) encryption profile

Phase 2 of the IKE protocol securely negotiates (through the ISAKMP SA communication channel negotiated in the first phase) the parameters of future IPSec SAs (one incoming, one outgoing).

The drop-down list allows choosing the protection model associated with your VPN policy, from 3 pre-configured profiles: **StrongEncryption**, **GoodEncryption**, and **FastEncryption**. Others may also be created.

Table of profiles

This table offers a series of predefined Phase 1 and Phase 2 encryption profiles. For each selected profile, you will see its characteristics to the right of the screen ("**General**", "**Authentication proposals**" and "**Encryption proposals**" fields).

Add	By clicking on this button, you will be able to add a **Phase 1 profile (IKE)** or **Phase 2 profile (IPSec)**, which will be displayed in the "Type" column. You can give it any "Name" you wish. It is also possible to copy a profile and its characteristics: to do so, select the desired profile and click on the option **Copy selection**, and give it a name.
Delete	Select the encryption profile to be deleted from the list and click on **Delete**.

General

Comments	Description given to your encryption profile.
Diffie Hellman/Perfect Forward Secrecy (PFS)	This field represents two types of key exchange: if you have selected an **IKE** encryption profile, the **Diffie-Hellman** option will appear. **Diffie-Hellman** allows 2 peers to generate a common secret on each side, without sending sensitive information over the network. On the other hand, if you have chosen an **IPSec** profile, **PFS** will be offered. **Perfect Forward Secrecy** allows guaranteeing that there are no links between the various keys of each session. Keys are recalculated by the selected Diffie-Hellman algorithm. The higher the number, the higher the level of security Regardless of what you choose, a drop-down list will suggest that you define the number of bits that allow strengthening security during the transmission of the common secret or password from one peer to another. Several choices (in bytes) are possible: **768, 1024, 1536, 2048, 3072** and **4096**. **REMARK** The longer the password (or "key"), the higher the level of security, but at the same time consumes more resources.
Maximum lifetime (in seconds)	Period beyond which leys will be renegotiated. The default duration of an **IKE** profile is 21600 seconds, and 3600 seconds for an **IPSec** profile.

Authentication proposals

This table allows you to modify or add authentication algorithms to the pre-entered list of the selected profile.

Add	The authentication algorithm that appears by default when you click on this button is **hmac_sha1,** with a "Strength**"** of 160 bits and a priority of "1". Click on the arrow to the right of the "Algorithm" column if you wish to modify it. Each time you add a new line to the table, it will be of the priority level that follows.
Delete	Select the line to be deleted from the list and click on **Delete**.
Algorithm	6 choices are offered: **sha1, md5, sha256, sha384, sha512** or **non_auth**.
Strength	Number of bits defined for the selected algorithm.

Encryption proposals

This table allows you to modify or add encryption algorithms to the pre-entered list of the selected profile.

Add	The encryption algorithm that appears by default when you click on this button is **des,** with a "Strength**"** of 64 bits. Click on the arrow to the right of the "Algorithm" column if you wish to modify it. Each time you add a new line to the table, it will be of the priority level that follows.
Delete	Select the line to be deleted from the list and click on **Delete**.
Algorithm	5 choices are offered: **des**, **3des**, **blowfish, cast128** and **aes**.
Strength	Number of bits defined for the selected algorithm.

REMARKS

These two tables appear only if you have selected an **IPSec** profile.

For **IKE** profiles, only the "**Proposals**" table will appear, divided into two columns: "Authentication" and "Encryption", with their respective algorithms.
You can **Add** or **Delete** lines, by modifying the order of priority using the **Up** and **Down** buttons.

Click on **Apply** once you have completed the configuration.

INTERFACES

The Interfaces module allows you to manage, add and delete network elements called network interfaces that represent physical or virtual communication devices between the various networks that pass through the appliance.

Bridges comprise 3 tabs, interfaces consist of 2 tabs (Ethernet and VLANs) and modems take up only 1 tab.

WARNING
Object names cannot contain the words “vlan“, “serial“ and “ethernet“ if they are immediately followed by numbers.

From version 9.0.3 onward, Interface names may contain more special characters including “/” and “-”.

Operating mode between interfaces

How interfaces on the firewall interact can be configured according to three different modes:

- Advanced mode
- Bridge mode (or transparent mode)
- Hybrid mode

Advanced mode

In advanced mode: each interface has a different IP address and the network that has been assigned to it is in the same address class. This enables the configuration of translation rules for accessing other zones in the firewall.
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.

Bridge mode or transparent mode

In transparent (bridge) mode: interfaces are part of the address range declared on the bridge.
The transparent or "bridge" mode, allows keeping the same address range between interfaces.
It simulates a filtering bridge: in other words, all the network traffic crosses it.
However, you can subsequently filter traffic across by using interface objects or address ranges according to your needs and therefore 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.

Hybrid mode

In hybrid mode: some interfaces have the same IP address and others have a distinct address.

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

Internal zone and DMZ (or external zone and DMZ) and certain interfaces in a different address range. As such, you have greater flexibility when integrating the product.

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.

Presentation of the configuration screen

The interface configuration window consists of 3 sections:

- **The directory of interfaces**: the appliance's interfaces are presented sorted in the following order: Bridge, Interface, VLAN, Modem according to the selected view. Clicking on an interface allows viewing its configuration. It is also possible to use the search engine to look for a specific interface. (Example: by typing "br", all bridges will be displayed).
- **The configuration panel** (central panel): by clicking on an interface in the directory, its configuration will appear in this panel.
- **The toolbar**: this bar allows:
  - Adding or deleting interfaces (bridge, modem),
  - Expanding or collapsing the folders in the interface directory,
  - Selecting one of 3 views: "Mixed view" which is the default view and which corresponds to a logical representation of the interfaces (that is, bridges first (they make up the root node), interfaces, VLANs (attached to the interface or the bridge), then modems). "Group by physical port" and "Group by address range" allow filtering according to the desired interface and checking its use.

Directory of interfaces

The appliance's interfaces are indicated in the directory.

Drag & Drop

Dragging and dropping an interface modifies its configuration (its relationships and address range). If a drag & drop operation is authorized, a green tick will appear. Otherwise, if the move is prohibited, a red circle will be indicated.
When an interface is detached from a bridge, a window will appear, allowing the address range to be entered.

The following moves are allowed:

Bridge/Interface	From	To
Ethernet Interface	Bridge	Root
Ethernet Interface	Bridge	Another bridge
Ethernet Interface	Racine	Bridge
VLAN	Ethernet Interface	Another Ethernet interface
VLAN	Ethernet Interface	Bridge
VLAN	Bridge	Another bridge
VLAN	Bridge	Ethernet Interface
Modem (PPPoE)	Interface	Another interface

Searching for interfaces

An interface can be found more easily with the search field.
Searches are possible in the following fields of the interfaces: Name, Address, Type, Comments, Hostname (DHCP), Physical MAC address, Gateway (routing by interface).

Example: You can search for an interface by indicating its name or even the address of its gateway.
To validate a search, simply click on **Enter**. To delete a search, click on the cross to the right of the search field.

Identifying interfaces

Each interface has its own icon for quicker visual identification. This icon also allows identifying whether the interface has been enabled or disabled. If it has been disabled, the icon and the name of the interface will be grayed out.
Ethernet interfaces have a real name (ex: "Out") and a technical name (ex: "0"). The physical port is displayed in brackets after the name of the interfaces.

Toolbar

Add	This button allows you to open the bridge, VLAN or modem creation wizard.
Delete	This button allows you to delete an interface that was previously selected in the interface directory. Ethernet interfaces cannot be deleted.
Collapse	This button allows collapsing all folders in the interface directory.
Expand	This button allows expanding all folders in the interface directory.
Mixed view	3 views are suggested: **Mixed view**, **Group by physical port** (interfaces are grouped by port. For each port, interfaces and VLANs are indicated), **Group by address range** (interfaces are separated according to their address range. If the interface contains an address + an alias, in this case, it will appear twice in the directory).

Show all	5 filter options are available: **Bridge**, **Interface**, **VLAN**, **Modem (Dialup)**, **Show all**.
Check usage	If you click on this button after having selected an interface, the results will appear in the directory of modules. If you delete an interface, a check will be performed in order to warn the user about configurations that use the interface he wishes to delete. If the interface is in use, the following message will appear: "***Warning**, this interface/bridge is being used by one or several modules. Removing it will make the firewall unstable*." You can either force the deletion, check its usage or cancel. If the check does not turn up any results, the message will be: "Delete this interface?".

From version 9.0.1 onwards, an external 3G modem can now be connected to the USB port. A warning message will appear when an interface is renamed.

NOTE
Renaming an interface does not migrate references to it especially in configuration items that use generated objects such as "Network_in".

Modifying a Bridge

To modify the parameters of a bridge, click on its name in the left side of the window. Three tabs allow the modification of the bridge's parameters.

"General" tab

Name (mandatory)	Name of the interface. (See warning in the introduction to the chapter on **Interfaces**)
Comments	Allows you to enter comments regarding the interface.

Bridge members

Physical ports	List of Ethernet ports in the bridge (Example: (Port2)
Interfaces (physical and logical)	List of interfaces contained in the bridge (Example: in)

Address range

Dynamic IP (obtained by DHCP)	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 (**dyndns.org** for example) in order to contact this firewall without having to know its IP address. This feature can be enabled by selecting a dynamic DNS account that you would have configured earlier. *The configuration of dynamic DNS clients is explained further in the document Dynamic DNS module*. This field allows specifying to the firewall that the configuration of the bridge (IP address and mask) is defined by DHCP. In this case, the "DHCP" zone in the

	Advanced properties tab will be enabled.
Fixed IP (static)	Your firewall has a static (fixed) IP address.

List of the bridge's IP addresses

This table appears if the option **Fixed IP (static)** has been selected.

IP address	IP address assigned to the bridge. (All the interfaces contained in the bridge have the same IP address).
Network mask	Network mask of the sub-network to which the bridge belongs. The various interfaces that are part of the bridge have the same IP address so all networks connected to the firewall are part of the same address range. The network mask provides the firewall with information about the network that it belongs to.
Comments	Allows entering comments regarding the address range of the bridge.

Here, several associated IP addresses and network masks may be defined for the same bridge (the need to create aliases, for example). These aliases may allow you to use this 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 **Add** or **Delete** buttons under the IP address and Netmask fields.

"Advanced configuration" tab

MTU	Maximum length (in bytes) of frames transmitted on the physical support (Ethernet) so that they are sent at one go (without fragmentation).
Physical (MAC) address	**WARNING** This option is not accessible 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). When the MAC address is assigned to the bridge, all interfaces contained in this bridge will then have the same MAC address. This address consists of 6 bytes in hexadecimal separated by :

DHCP

NOTE

This field will be indicated as “disabled” if the option **Dynamic IP (obtained by DHCP)** was not selected in the **General** tab, and options will be grayed out.

DNS name (optional)	Name of the DNS server (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. This name consists of 6 bytes in hexadecimal separated by :
Requested lease time (seconds)	Period during which the IP address is kept before renegotiation.
Request domain name servers from the DHCP server and create host objects	If 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.

“Bridge members” tab

Another way to include interfaces in a bridge, apart from dragging and dropping, is to use the panel in this tab. (bridge members).
To move an available interface to the bridge, drag and drop it or use the red arrow in between both tables or double-click on the interface you wish to move.
To remove an interface from a bridge, do the exact opposite.

Creating a bridge

Bridges can be created using a wizard that allows you to create the interface easily.
Click on **Add** in the toolbar and select “Add a Bridge”. The bridge creation wizard will then appear.

NOTE

The number of bridges to create depends on your firewall model.

Identifying the bridge

Name	Name of the interface. (See warning in the introduction to the chapter on **Interfaces**)

Comments	Allows you to enter comments regarding the interface.

Address range

Fixed IP (static)	By selecting this option, the bridge will have a static address range. In this case, its IP address and the mask of the sub-network to which the bridge belongs, have to be indicated.
Dynamic IP (obtained by DHCP)	By selecting this option, the interface will be defined by DHCP. In this case, a DHCP hostname that is the name of a server for the connection (FQDN) must be indicated. 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 as well as the allocated time (mandatory). This name consists of 6 bytes in hexadecimal separated by : The period during which the IP address is kept before renegotiation must also be indicated.

Click on **Next** at the bottom of the screen. The bridge creation screen will appear (Step 2).
Select the interfaces for which you wish to create a bridge. The list of "Available interfaces" shows all the Ethernet and VLAN interfaces already in the configuration. At least two interfaces have to be selected in order to make a bridge, either by using arrows or by dragging and dropping between both lists or by double-clicking on the interface. Click on **Finish** to confirm the creation.

Deleting a bridge

To delete a bridge, select it in the interface directory, then click on **Delete** in the toolbar. The message "*Delete this bridge?*" will appear.
Confirm or cancel the deletion.
If you confirm the deletion, a check will be performed to see if the interface is in use.

NOTE
Deleting a bridge disables the interfaces that it contained and also disables their switch to a configuration in DHCP.

Modifying an Ethernet interface (in bridge mode)

If an interface is in a bridge, it will be represented as a child node in relation to the bridge. Thus, a bridge may contain several child nodes.
You can change the parameters of each interface, whether or not it belongs to the bridge. To do so, select an interface located inside or outside a bridge on the left-hand side of the window. Two tabs will then appear:

NOTE
Ethernet interfaces cannot be added or deleted.

"Configuration of the interface" tab

Name (mandatory)	Name given to the bridge interface. (See warning in the introduction to the chapter on **Interfaces**)
Comments	Allows you to enter comments regarding the interface.
Physical port	Name of the physical port (example: in (port 2)).
VLANs attached to the interface	List of VLANs attached to the selected interface. ***From version 9.0.1 onwards,*** the appliance no longer needs to be systematically rebooted whenever a VLAN is deleted.
Color	Color assigned to the interface.
This interface is	If "internal (protected)" is selected, this indicates that the interface is private. Addresses of **internal** interfaces cannot be used as destinations for packets coming from unprotected interfaces, except if they have been translated. **NOTE** You will notice that "internal (protected)" implies being on a protected interface. Therefore the options "internal (protected)" and "external (public)" are incompatible. If you select "external (public)" this indicates 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, represented by a shield (), disappears when this option is checked.

Address range

None (interface disabled)	By selecting/unselecting this option, the interface will be enabled/disabled. By disabling 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 which is not active. An interface which has been disabled because it is not in use is an example of an additional security measure against intrusions.
Dynamic IP (obtained by DHCP)	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 (**dyndns.org** for example) in order to contact this firewall without having to know its IP address. This feature can be enabled by selecting a dynamic DNS account that you would have configured earlier. *The configuration of dynamic DNS clients is explained further in the document Dynamic DNS module.* This field allows specifying to the firewall that the configuration of the bridge (IP address and mask) is defined by DHCP. In this case, the "DHCP" zone in the Advanced properties tab will be enabled.
Address range inherited from the bridge	If the interface is part of a bridge, the address range of the bridge can be retrieved.
Fixed IP (static)	By selecting this option, the interface will have a static address range. In this case, its IP address and the mask of the sub-network to which the interface belongs, have to be indicated.

"Advanced configuration" tab

MTU	Maximum length (in bytes) of frames transmitted on the physical support (Ethernet) so that they are sent at one go (without fragmentation). This option is not available for interfaces contained in a bridge.
Physical (MAC) address	**WARNING** This option is not accessible 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). If the interface is contained in a bridge, it will have the same MAC address as the bridge. **NOTE** This field is grayed out when the interface belongs to a bridge. It can neither be modified nor deleted.

DHCP

NOTE

This option will be indicated as “disabled” if the option **Dynamic IP (obtained by DHCP)** was not selected in the **Configuration of the interface** tab and the options will be grayed out.

DNS name (optional)	Name of the DNS server (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. This name consists of 6 bytes in hexadecimal separated by :
Requested lease time (seconds)	Period during which the IP address is kept before renegotiation.
Request domain name servers from the DHCP server and create host objects	If 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. **NOTE** This option will be disabled if the option **Dynamic IP (obtained by DHCP)** was not selected in the Configuration of the interface tab.

Bridge – Routing without analysis

NOTE

This option will be indicated as “disabled” if the option **Address range inherited from the bridge** was not selected in the **Configuration of the interface** tab and the options will be grayed out.

Authorize without analyzing	Allows letting IPX (Novell network), Netbios (on NETBEUI), AppleTalk (for Macintosh), PPPoE or Ipv6 packets pass between the bridge’s interfaces. No high-level analysis or filtering will be applied to these protocols (the firewall will block or pass).

Bridge – Routing by interface

NOTE

This option will be indicated as “disabled” if the option **Address range inherited from the bridge** was not selected in the **Configuration of the interface** tab and the options will be grayed out.

Keep initial routing	As its name indicates, this option allows keeping the initial routing for hosts connected on this interface. You can therefore specify a default gateway for certain hosts while specifying a gateway on the firewall for hosts that do not have one. This option eases the integration of the firewall into an architecture made up of many different gateways.
Keep VLAN IDs	This option enables the transmission of tagged frames without the firewall having to be the VLAN endpoint. The VLAN tag on these frames is 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.
Gateway address	This field is used for routing by interface. All packets that arrive on this interface will be routed via a gateway.

Media

Media	Connection speed of the 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.

Interface’s throughput (for information only)

Throughput	Defines the debit on an interface. This is an automatic entry that is not compulsory: it is used for monitoring in the calculation of bandwidth.

Modifying an Ethernet 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 directory using the mouse. You may then configure the interface parameters.
During detachment, the address range window will appear.

Fixed IP (static)	By selecting this option, the interface will have a static address range. In this case, its IP address and network mask must be indicated.
Dynamic IP (obtained by DHCP)	By selecting this option, the interface will be defined by DHCP. In this case, a DHCP hostname and a lease time must be indicated.

Once the interface is outside the bridge, you will have access to the interface settings described in the chapter **"Modifying an Ethernet interface (in Bridge mode)".**

Modifying a VLAN

"Configuration of the interface" tab

Name (mandatory)	Name given to the VLAN. (See warning in the introduction to the chapter on **Interfaces**)
Comments	Allows you to enter comments regarding the VLAN.
Parent interface	Physical name of the interface to which the VLAN is attached.
Color	Color assigned to the VLAN.
VLAN ID	Identifier for the VLAN which may be any value between 1 and 4094 inclusive and must be unique (unless it is a VLAN associated with another bridge in a crossing VLAN).
This interface is	If "internal (protected)" is selected, this indicates that the interface is private. Addresses of **internal** interfaces cannot be used as destinations for packets coming from unprotected interfaces, except if they have been translated. **NOTE** You will notice that "internal (protected)" implies being on a protected interface. Therefore the options "internal (protected)" and "external (public)" are incompatible. If you select "external (public)" this indicates 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, represented by a shield (), disappears when this option is checked.

Address range

None (interface disabled)	By selecting/unselecting this option, the interface will be enabled/disabled. By disabling 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 which is not active. An interface which has been disabled because it is not in use is an example of an additional security measure against intrusions.
Dynamic IP (obtained by DHCP)	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 (**dyndns.org** for example) in order to contact this firewall without having to know its IP address. This feature can be enabled by selecting a dynamic DNS account that you would have configured earlier. *The configuration of dynamic DNS clients is explained further in the document Dynamic DNS module.* This field allows specifying to the firewall that the configuration of the bridge (IP address and mask) is defined by DHCP. In this case, the "DHCP" zone in the Advanced properties tab will be enabled.
Address range inherited from the bridge	If the interface is part of a bridge, the address range of the bridge can be retrieved. This zone will be grayed out if the interface does not belong to a bridge.
Fixed IP (static)	By selecting this option, the interface will have a static address range. In this case, its IP address and the mask of the sub-network to which the interface belongs, have to be indicated.

"Advanced configuration" tab

MTU	Maximum length (in bytes) of frames transmitted on the physical support (Ethernet) so that they are sent at one go (without fragmentation). This option is not available for interfaces contained in a bridge.
Physical (MAC) address	**WARNING** This option is not accessible 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). If the interface is contained in a bridge, it will have the same MAC address as the bridge. **NOTE** This field is grayed out when the interface belongs to a bridge.

DHCP

NOTE

This option will be indicated as “disabled” if the option **Dynamic IP (obtained by DHCP)** was not selected in the **Configuration of the interface** tab and the options will be grayed out.

DNS name (optional)	Name of the DNS server (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. This name consists of 6 bytes in hexadecimal separated by :
Requested lease time (seconds)	Period during which the IP address is kept before renegotiation.
Request domain name servers from the DHCP server and create host objects	If 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. **NOTE** This option will be disabled if the option **Dynamic IP (obtained by DHCP)** was not selected in the Configuration of the interface tab.

Bridge – Routing without analysis

NOTE

This option will be indicated as “disabled” if the option **Address range inherited from the bridge** was not selected in the **Configuration of the interface** tab and the options will be grayed out.

Authorize without analyzing	Allows letting IPX (Novell network), Netbios (on NETBEUI), AppleTalk (for Macintosh), PPPoE or Ipv6 packets pass between the bridge’s interfaces. No high-level analysis or filtering will be applied to these protocols (the firewall will block or pass).

Bridge – Routing by interface

NOTE

This option will be indicated as “disabled” if the option **Address range inherited from the bridge** was not selected in the **Configuration of the interface** tab and the options will be grayed out.

Keep initial routing	As its name indicates, this option allows keeping the initial routing for hosts connected on this interface. You can therefore specify a default gateway for certain hosts while specifying a gateway on the firewall for hosts that do not have one. This option eases the integration of the firewall into an architecture made up of many different gateways.
Gateway address	This field is used for routing by interface. All packets that arrive on this interface will be routed via a gateway.

Interface’s throughput (for information only)

Throughput Defines the debit on an interface. This is an automatic entry that is not compulsory: it is used for monitoring in the calculation of bandwidth.

Creating a VLAN

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

Select the interface or the bridge for which you wish to associate a VLAN. Then click on **Add** and **Add a VLAN**. The screen for Step 1 appears:

Step 1

VLAN attached to a single interface (VLAN endpoint)	NETASQ firewalls can be placed at the end of VLANs to add or remove a VLAN tag. The firewall carries out the filtering and takes care of communications 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. If you select this option, by clicking on **Next**, the screen for Step 2 will appear. The creation process takes place in 2 steps.
VLAN attached to 2 interfaces (crossing VLAN)	This option allows creating a crossing VLAN, meaning a bridge containing 2 VLANs with the same ID. If you select this option, by clicking on **Next**, the screen for Step 3 will appear

Step 2: VLAN attached to a single interface (VLAN endpoint)

VLAN identification

Parent interface	Select the interface to which the VLAN will be attached.
Name	Enter a unique name for your VLAN *(Cf. Appendix M: Prohibited names*).
Comments	You may also enter a description.
Color	Color assigned to the VLAN.
VLAN ID	This field allows specifying the value to be associated with the VLAN in packets passing through the network. This tag identifies the VLAN and is used at the Ethernet level. It must be unique and be any value between 1 and 4094 inclusive.
This VLAN is	Indicate if you wish to have an external or internal interface.

Address range

Dynamic IP (obtained by DHCP)	Select this option to give the VLAN a dynamic address.
Fixed IP (static)	By selecting this option, the interface will have a static address range. In this case, its IP address and network mask have to be indicated.

Step 3: VLAN attached to 2 interfaces (crossing VLAN)

When configuring VLANs for bridges, the same tag can be used for two VLAN interfaces, making the Firewall appear transparently on the network. This method requires the use of one VLAN interface per physical interface.
Unlike the option **Keep VLAN IDs** (*cf. in the advanced properties of an Ethernet interface*) 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.

VLAN identification

Name	Enter a unique name for your VLAN
VLAN ID	This field allows specifying the value to be associated with the VLAN in packets passing through the network. This tag identifies the VLAN and is used at the Ethernet level.
Color	Color assigned to the VLAN.

VLAN address range

Use an existing bridge	By selecting this option, you will need to select from the drop=down list the bridge to which VLANs will be attached.
Create a new bridge	If this option is selected, a wizard will allow creating a new bridge which will contain both interfaces.
Dynamic IP (obtained by	This option is used when your firewall does not have a static IP address

DHCP)	(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 (**dyndns.org** for example) in order to contact this firewall without having to know its IP address. This feature can be enabled by selecting a dynamic DNS account that you would have configured earlier. *The configuration of dynamic DNS clients is explained further in the document Dynamic DNS module.* This field allows specifying to the firewall that the configuration of the bridge (IP address and mask) is defined by DHCP. In this case, the "DHCP" zone in the Advanced properties tab will be enabled.
Fixed IP (static)	By selecting this option, the bridge will have a static address range. In this case, its IP address and the mask of the sub-network to which the bridge belongs, have to be indicated.

Step 4: VLAN attached to 2 interfaces (crossing VLAN)

Identification of the incoming VLAN

Name (mandatory)	Unique name for your VLAN. This field is pre-entered with the name indicated in the Name field in Step 3 suffixed with "1".
Interface (mandatory)	Select the interface on which the VLAN will be attached.
This VLAN is	If "internal (protected)" is selected, this indicates that the interface is private. Addresses of **internal** interfaces cannot be used as destinations for packets coming from unprotected interfaces, except if they have been translated. **NOTE** You will notice that "internal (protected)" implies being on a protected interface. Therefore the options "internal (protected)" and "external (public)" are incompatible. **If you select "external (public)"** this indicates 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, represented by a shield (), disappears when this option is checked.

Identification of the outgoing VLAN

Name (mandatory)	Unique name for your VLAN. This field is pre-entered with the name indicated in the Name field in Step 3 suffixed with "2".
Interface	Enter a unique name for your VLAN.

This VLAN is	If “internal (protected)” is selected, this indicates that the interface is private. Addresses of **internal** interfaces cannot be used as destinations for packets coming from unprotected interfaces, except if they have been translated. **NOTE** You will notice that “internal (protected)” implies being on a protected interface. Therefore the options “internal (protected)” and “external (public)” are incompatible. **If you select “external (public)”** this indicates 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, represented by a shield (), disappears when this option is checked.

Step 5: VLAN attached to 2 interfaces (crossing VLAN)

This step summarizes the configuration that you have just performed.

Adding a VLAN

If you wish to create a new VLAN and you have reached the maximum number of dynamic VLANs possible, a pop-up window will appear to allow you to add others. This number can also be modified manually by going to System\Configuration\Network\Available VLANs (max 128)\.

Deleting a VLAN

To delete a VLAN, select it in the interface directory, then click on **Delete** in the toolbar. The message “*Delete this interface?*” will appear.
Confirm or cancel the deletion.
If you confirm the deletion, a check will be performed to see if the interface is in use.

Modifying a modem

PPPoE modem

Use this modem	By selecting this option, you will enable the modem.
Name (mandatory)	Name given to the modem. (See warning in the introduction to the chapter on **Interfaces**)
Comments	Allows you to enter comments regarding the modem.
Modem type	Indicates the type of modem chosen in the creation phase.
Color	Color assigned to the modem.

Authentication

Login	Name used for authentication

Password	Password used for authentication. If you click on the key icon to the right of the field, the password will appear in plaintext for 5 seconds.

Connectivity

The modem is connected to the interface	Indicates the modem's connection interface.
Query domain name servers and create associated host objects	If 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.

Advanced properties

Service	Type of PPPoE service used. This option allows distinguishing between several ADSL modems. Leave this field empty by default.
Connection	Connection **when there is traffic (on demand)** establishes a connection with the internet only when a connection request is made by the internal network (this is more economical than in the case of a link that is charged by duration). The **Permanent** connection keeps the connection to the internet permanently active.

PPTP Modem

Use this modem	By selecting this option, you will enable the modem.
Name (mandatory)	Name given to the modem. (See warning in the introduction to the chapter on **Interfaces**)
Comments	Allows you to enter comments regarding the modem.
Modem type	Indicates the type of modem chosen in the creation phase.
Color	Color assigned to the modem.

Authentication

Login	Name used for authentication
Password	Password used for authentication. If you click on the key icon to the right of the field, the password will appear in plaintext for 5 seconds.

Connectivity

PPTP address	Internal IP address of the ADSL modem.
Query domain name servers and create associated host	If 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.

objects	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.

Advanced properties

Connection	Connection **when there is traffic (on demand)** establishes a connection with the internet only when a connection request is made by the internal network (this is more economical than in the case of a link that is charged by duration). The **Permanent** connection keeps the connection to the internet permanently active.

PPP Modem

Use this modem	By selecting this option, you will enable the modem.
Name (mandatory)	Name given to the modem. (See warning in the introduction to the chapter on **Interfaces**)
Comments	Allows you to enter comments regarding the modem.
Modem type	Indicates the type of modem chosen in the creation phase.
Color	Color assigned to the modem.

Authentication

Login	Name used for authentication
Password	Password used for authentication. If you click on the key icon to the right of the field, the password will appear in plaintext for 5 seconds.

Connectivity

Number to dial	Phone number of the access provider.
Query domain name servers and create associated host objects	If 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.

Advanced properties

Initialization strong	String of characters used optionally for initializing the connection.
Connection	Connection **when there is traffic (on demand)** establishes a connection with the internet only when a connection request is made by the internal network (this is more economical than in the case of a link that is charged by duration). The **Permanent** connection keeps the connection to the internet permanently active.

Creating a modem

Modem interfaces are used in remote connections when your modem is directly connected to the firewall (serial port or Ethernet). The firewall accepts all modem types (ADSL, ISDN, RTC, ...). New modem interfaces can be created thanks to the wizard. The maximum number of available modems on your firewall depends on the model.

In the menu **Network\Interfaces** click on **Add** and select "**Add un modem**"

Step 1

Identification du modem

Name	Enter a name (mandatory).
Comments	Description to identify the Dialup connection.
Color	Color assigned to the remote connection.
Query domain name servers and create associated host objects	If 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.

Configuring the modem

Select the type of dialup from PPPoE, PPTP, PPP or L2TP. The configuration window varies according to the selected dialup.

PPPoE	Select the network interface used for the modem
PPTP	Enter the IP address of the modem.
PPP	Enter the telephone number used for dialing.

Authentication

Login	Enter the user's ID (mandatory).
Password	Enter the password (mandatory).
Confirm password	Confirm the password in the previous field

Once Step 1 has been configured, click on **Next**.

Step 2

Routing: use the gateway obtained by the modem

Select whether you wish to define the modem as a gateway.

To the list of main gateways	The host Firewall_ <name of modem>_peer will be added to the main gateways. If there is no main gateway, a window will appear asking if you wish to define a main gateway (default router).
To the list of backup gateways	The host Firewall_ <name of modem>_peer will be added to the secondary gateways.
Do not add (configure later)	The modem has not been defined as a gateway.

Deleting a modem

To delete a modem, select it in the interface directory, then click on **Delete** in the toolbar. The message "*Delete this modem?*" will appear.
Confirm or cancel the deletion.
If you confirm the deletion, a check will be performed to see if the interface is in use.

General remarks on configuring modems

The firewall automatically negotiates the opening of a line and reinitializes the connection in the event of an interruption. In the event the connection is impossible (problem with the line), the firewall will raise an alarm.

LICENSE

The License screen consists of several sections:

- The General tab: manual or automatic installation of a license and display of main information.
- The License details tab (or in the case of high availability, a serial number such as Local License U70XXADA913500 to distinguish the active firewall from the passive firewall): details of all options in the license and their active value on the firewall.
- An additional tab per passive appliance in the case of high availability.

"General" tab

This tab will allow you to automatically or manually install a license.
There are 2 ways to install a license manually:

1) By inserting the **License file** in the relevant field. Automatic configuration possible.
2) By looking for a new license.

Buttons

Search for a new license: this button is used for finding new licenses or for updating the date of the last check for a license.
By clicking on this button, a request to search for licenses will be sent to the appliance. If a license is found, a notification will appear in the General tab and the user will then have access to the button **Install the new license**. Searches for licenses are conducted manually. If you prefer an automatic license search, you will need to change the settings in the advanced properties section in this tab.
Install the new license: If the firewall has found a license through the button **Search for a new license**, the button **Install the new license** will be enabled. By clicking on it, a download will be launched. Confirm or cancel the download.

Dates

Local firewall date: this date allows ensuring that the firewall's date is correct. Expiry dates are calculated based on this date.
Last check for license updates performed on: date of the last time a request was made manually or automatically to search for licenses.
The NETASQ firewall is sold by default with all features enabled. However, some features (URL filtering, high availability, among others) are optional and not enabled. Certain options, such as updates, are valid for a limited period. If the expiry date has lapsed, some options will be disabled on the firewall.

Important information about the license

The license configuration window shows you the version of your firewall, information on the hardware and the various options with their expiry dates, if any.
Icons and colors will indicate if an option is approaching its expiry date or has expired.

Installing from a file

You can install your first license here if you do not have internet access or if you wish to manage licenses yourself.
If you choose to use new features or renew certain options, please contact your reseller. A new encrypted file will then be given to you through your private area on NETASQ's website.

License file	This field allows you to insert a license that you have retrieved earlier from NETASQ's website and activate the configuration on your firewall. The button **Install the license file** will validate the installation of the license file on the appliance. Information concerning your firewall will be modified and the new options will be enabled on the firewall.

REMARK
The options that require rebooting the firewall are changes to encryption strength and the addition or removal of network interface cards.
In order to be accessible, these modules, even if they are physically installed, require the installation of the appropriate license following a reboot.

Advanced properties

Here, you can define how frequently the firewall will look for updates as well as the type of installation (manual or automatic).

Look for license updates	Indicates how frequently searches will be conducted. If a license is found, a notification will appear in the information panel of the General tab, which may look like this: "! A new license is available for U30XXA32100950".
Install license after it has been downloaded	If you select **always manual** (using the button *install a new license*), the button **Install the new license** will appear whenever a license is suggested. The new license can therefore be compared against the current license in the License details tab. If the license is suitable, click on **Install the new license**. A notification will appear, informing you that the current license is up to date. If you select **automatic when possible (no reboot necessary)**, the appliance will install the license. Note: There are several different notifications: "*License Update: a new license is available*" will appear when this is clearly the case. Every message is associated with an alarm (*68* in this case). It is also possible to find: *69= "License Update: Temporary license, registration is necessary*" or even *71= "License Update: A new license has been installed"* These messages can be seen in SNMP, syslog and RealTime Monitor alerts as well as in NETASQ Event Analyzer logs. To enable the sending of these messages, go to the menu Notifications, Logs-Syslog or SNMP Agent.

“License details” tab

This tab displays the current valid license of the appliance to which you are connected.

Buttons

Search for a new license	This button is used for finding new licenses or for updating the date of the last check for a license. **NOTE** In this tab, the button allows searching for licenses for all firewalls in the high availability cluster.
Install the new license	If the firewall has found a license through the button **Search for a new license**, the button **Install the new license** will be enabled. By clicking on it, a download will be launched. Confirm or cancel the download. **NOTE** In this tab, the button allows installing the license for the firewall indicated.
Collapse	This button allows collapsing all the features in the license.
Expand	This button allows expanding all the features in the license.

The table

Feature	Indicates the features and options of each feature found on the firewall. The features are: “Administration”, “Date”, “Flags”, “Global”, “Hardware”, “Limit”, “Network”, “Proxy”, “Service” and “VPN”. The options relating to the features are explained in detail in the next section.
In progress (current license)	Indicates, for each license installed, which options have been enabled for each feature, or the expiry status. A symbol indicates whether a feature is enabled, and another symbol shows that an option has been disabled. Symbols and colors show the difference between an option that is close to expiry (less than 90 days to the expiry date), an expired option and a valid option.
New license	This column appears only if a new license is available but has not yet been installed, and that a reboot would be necessary (in other words, this column will never appear if you have selected in the advanced properties of the General tab the option **Install license after it has been downloaded - automatic when possible (no reboot necessary)**. When a new license is available, this column will set out the new values in comparison with the values of the current license indicated in the column “In progress (current license)”. Symbols and colors indicate improvements or declines in value compared to the values of the current license. If the option has not changes, nothing will be indicated.

Administration

GlobalAdmin	Global administration possible via GlobalAdmin. (Default value: 1)
Manager	Administration possible via the web interface. (Default value: 1).
Monitor	Monitoring possible via NETASQ REALTIME MONITOR (Default value: 1).
Reporter	Reporting possible via NETASQ EVENT REPORTER. (Default value: 1).

Date

Antispam	Deadline for updating DNSRBL spam databases
Antivirus	Deadline for updating ClamAV antivirus databases
ExpressWarranty	Deadline for the ExpressWarranty. This allows limiting the client's waiting time during the repair of his product.
NotAfter	Expiry date of the license.
NotBefore	Earliest date for using the license
Pattern	Deadline for updating ASQ patterns.
SPAMVendor	Deadline for updating the spam filter heuristic engine.
URLFiltering	Deadline for updating NETASQ's URL filter databases.
URLVendor	Deadline for updating OPTENET's URL filter databases.
Update	Deadline for updating the appliance.
VirusVendor	Deadline for updating Kaspersky antivirus databases.
VulnBase	Deadline for updating SEISMO vulnerabilities.
Warranty	Deadline for the warranty.

Flags

Clone	Enables/disables management/presence of the backup partition. (Default value: 1).
CustomPattern	Allows customizing ASQ models.
ExpressWarranty	Express warranty that allows limiting the client's waiting time during the repair of his product.
ExternalLDAP	Enables or disables the use of an LDAP directory (Default value: 1*)
HAState	Allows defining an active and passive appliance in a high availability cluster. (Master/Slave/None).
PKI	Enables or disables the internal PKI. (Default value: 1)
PVS	Enables or disables SEISMO. (Default value: 0)

Global

Comment	Comments.
Id	Unique identifier
Temporary	Temporary license (as long as the appliance has not been registered). Default value: 1 (factory settings), 0 once the product has been registered.
Version	Version of the license (checks the compatibility of the format for the license/version of the Firmware). The default value is 9.

Hardware

CryptCard	Presence of an optional cryptographic card. (Default value: depends on the model).
Networkif	Maximum number of physical interfaces. (Default value: depends on the model).
Raid	Allows channeling date from one hard disk to another when one of them fails.

Limit

Conn	Maximum number of connections passing through ASQ. (Default value: 0 (= unlimited)).
Network	Maximum number of networks managed by ASQ. (Default value: 0 (=unlimited)).
User	Maximum number of users who can authenticate on the appliance. (Default value: 0 (=unlimited)).

Network

HADialup	Enables or disables the possibility of using dialups to establish high availability links. (Default value: 1).
HybridMode	Enables or disables hybrid mode on interfaces (mix of interfaces, bridges, VLANs, etc). (Default value: 1*).
InterfaceRoute	Allows routing by interface. This option is enabled by default. See the Menu: Configuration→Network→Interfaces/ Advanced properties tab/ Bridge: routing by interface" (Default value: 1).
LBDialup	Enables or disables load-balancing on dialups. (Default value: 1).
QoS	Enables or disables QoS. (Default value: 1).
VLAN	Enables or disables VLANs (Default value: 1).

Proxy

Antispam	Enables or disables spam filtering via DNSRBL in the proxy. (Default value: 1).
Antivirus	Enables or disables the ClamAV antivirus in the proxy. (Default value: 1).
FTPProxy	Enables or disables the FTP proxy. (Default value: 1**).
HTTPProxy	Enables or disables the http proxy (Default value: 1).
ICAPURL	Enables or disables the ICAP ReqMod. (Default value: 1).
ICAPVirus	Enables or disables the ICAP RespMod. (Default value: 1).
IMAPProxy	Enables or disables the IMAP proxy (which does not exist on UTMs). (Default value: 1).
POP3Proxy	Enables or disables the POP3 proxy. (Default value: 1).
SMTPProxy	Enables or disables the SMTP proxy. (Default value: 1).
SpamVendor	Enables or disables the spam filter heuristic engine. (Default value: 0).
URLFiltering	Enables or disables URL filtering via NETASQ's database in the proxy. (Default value: 1).
URLVendor	Enables or disables URL filtering via Optenet's database in the proxy. (Default value: 0).
VirusVendor	Enables or disables the Kaspersky antivirus in the proxy. (Default value: 0).

Service

Authentication	Enables or disables the user authentication interface.
DHCP	Enables or disables DHCP server/relay service (Default value: 1).
DNS	Enables or disables DNS cache service. (Default value: 1).
DynDNS	Enables or disables the DynDNS client of the DNS update server.
Enrolment	Enables or disables enrolment. (Default value: 1).
LDAPBase	Enables or disables the internal LDAP database (Default value: 1).
NTP	Enables or disables NTP synchronization (Default value: 1).
PublicLDAP	Enables or disables public access to the internal LDAP (Default value: 1*).
SNMP	Enables or disables the SNMP agent. (Default value: 1*).

VPN

Anonymous	Enables or disables the possibility of setting up anonymous tunnels. (Default value: 1*).
PPTP	Enables or disables PPTP tunnels. (Default value: 1*).
SSL	Enables or disables SSL VPN.
StrongEnc	Enables or disables support for strong algorithms for the encryption of IPSec tunnels. (Default value: 1*).
Tunnels	Maximum number of IPSec tunnels. (Default value: 0 (=unlimited)).

This tab works in the same way as the local license tab.

LOGS- SYSLOG

The log configuration screen consists of 2 tabs:

- Local storage
- Syslog

“Local storage” tab

The configuration of logs allows allocating disk space for each type of log on the firewall. This menu also allows modifying the firewall’s behavior when saving these logs.
This screen is divided into 2 sections:

- Top: a menu setting out the various options
- Bottom: Table

NOTE: This tab is grayed out if the model of the firewall does not have a hard disk. In this case, the Syslog tab will appear directly when this module is opened.

If the disk space quota is full

You can select the action to take when the disk reaches it space quota. The options are:

- **Erase the oldest logs (rotation)**: the most recent logs will erase the oldest logs.
- **Pause log writing:** logs will no longer be recorded on the firewall.

Configuration of the space reserved for logs

The firewall manages a certain number of log files intended for collecting events detected by the log functions. Files that are concerned with security events are:

- **Alarms**: events relating to the application of intrusion prevention features (l_alarm),
- **Authentication**: events relating to user authentication (l_auth),
- **Network connections:** events relating to connections through and to the firewall (l_connection),
- **Filter policy:** events relating to the application of filter functions (l_filter),
- **FTP proxy**: events relating to FTP traffic (l_ftp),
- **Statistics:** events relating to real-time monitoring (l_monitor),
- **Application connections (plugin)**: events relating to the treatment of ASQ plugins (l_plugin),
- **POP3 proxy:** events relating to message sending (l_pop3),
- **Applications and vulnerabilities (SEISMO):** events relating to the application for consulting vulnerabilities on the NETASQ SEISMO network (l_pvm),
- **Administration (Serverd):** events relating to the firewall administration server: "serverd" (l_server),
- **SMTP proxy:** events relating to SMTP traffic (l_smtp),
- **System events:** this is the log in which events directly relating to the system are logged: shutdown/startup of the firewall, system error, etc. Shutting down and starting log functions correspond to shutting down and starting the daemons that generate logs (l_system),
- **IPSec VPN**: events relating to the establishment of SAs (l_vpn),
- **HTTP proxy**: events relating to HTTP traffic (l_web),

- **SSL VPN:** events relating to the establishment of the SSL VPN (l_xvpn),

The files share a common storage area with other log files.

For each log menu (Alarms, Authentication, Network connections, Filter policy, FTP proxy, Statistics, Application connections (plugin), POP3 proxy, Applications and vulnerabilities (SEISMO), Server, SMTP proxy, System events, IPSec VPN, HTTP proxy, SSL VPN), you can restrict the size of the log file by selecting the size of the file as a percentage of the total space reserved for log files.

The table sets out the following columns:

Enabled	Allows enabling/disabling the log file. If this line is unselected, the percentage will be 0. In this case, the type of log will not be stored on the disk. If the line is selected, the default percentage indicated will be 1%.
Family	Name of the log file
Percentage	Current percentage of space occupied. By clicking in a box, the percentage can be modified.
Disk space quota	Proportion of the disk space that each file occupies on the disk, which varies according to the percentage specified.

The total percentage is shown at the bottom right side of the table. If the total exceeds 100%, a warning line will be indicated in red at the bottom of the table. (*Example: "Warning, incorrect distribution: 113% of the available space has been reserved)*. Modifications are however allowed.
By clicking on **Apply**, the following message will appear: "The total disk space reserved for logs exceeds this model's capacity. Apply this configuration?". You can force the save or cancel,.

NOTE
These files can be copied on the NETASQ EVENT ANALYZER solution in order to create reports or archive them.

"Syslog" tab

The Syslog tab allows configuring the sending of logs by Syslog.

Enable sending logs by Syslog	The NETASQ firewall will allow you to automatically send logs to a dedicated server. Logs are sent in WELF format. The server could be a server hosting the NETASQ LOG ANALYZER solution or any Syslog server. When the Syslog is enabled, the firewall will send UDP packets (port 514 by default) containing the log lines (one line per packet).
Destination server(s)	Indicates the IP address or the host object on which the NETASQ Event Analyzer solution or a Syslog server has been installed.

Port	Indicates the communication port associated with the Syslog server.

Families of sent logs

Enabled	Enables the activation of log files.
Family	Category of the file to be sent (Alarm, Connection, Web, Filter…).

Advanced configuration

Category (facility)	**Number added to the beginning of a log line. It can be used to differentiate several appliances when they sent their logs to the same Syslog server.**

Sending logs to a SYSLOG server

1. Select the option **Enable sending logs by Syslog**,
2. Indicate the name of the destination server,
3. Indicate the communication port associated with the destination server.

Logs can also be kept on the firewall (except on U30 and U70 models).

MAINTENANCE

The Maintenance module will allow you to modify settings and perform the necessary checks to ensure that your appliance runs smoothly.
It is possible, via the interface, to set up a secure configuration of your firewall, to back up and update your system, as the 5 following tabs show:

- Configuration
- Backup
- Restore
- Secure configuration
- System update

"Configuration" tab

System disk

This refers to the system disk of your NETASQ multifunction firewall.
You are currently using this partition: your firewall's system disk is divided into two partitions, which allow you to back up your data.
This section indicates the partition on which the product started up.

Upon startup, use the: select the product's startup partition – the main or backup partition.

Main partition	If this option is selected, your firewall will use this partition at startup.
Backup partition	The backup partition represents your last backed up partition. Select this option if you wish to use it when your firewall starts up.
Back up the active partition	This button allows you to back up the active partition (the one indicated by **You are currently using this partition**) on the other partition.

Maintenance

Reboot the firewall	Click on this button to restart your firewall directly.
Shut down the firewall	Click on this button if you wish to shut down your firewall.

System report (sysinfo)

Download the system report: This button will allow you to obtain various types of information about your firewall in "sysinfo" format.
Using this feature, you will be able to find out, for example, the model of the firewall, its serial number, its current status and the status of its memory.

"Backup" tab

Configuration backup

Through this screen, you will be able to create a comprehensive backup of your firewall's configuration in the form of files, and protect access to it.

Backup filename: By default, the name of the backup will correspond to "<firewall serial number>_day_month_year.na".

Download	The file will be saved in .na format (NETASQ ARCHIVES). Click on this button to save it.

Advanced properties

Password	Define a password to protect your backup.
Confirm	Confirm the password of your backup, entered in the previous field.
Password strength	This field indicates your password's level of security: "Very Weak", "Weak", "Medium", "Good" or "Excellent". You are strongly advised to use a combination of upper and lowercase letters, numbers as well as special characters.

"Restore" tab

Password

This window allows you to restore a backup that was made earlier.

Select a backup to restore:

Select a backup file	Click on the button to the right of the field (…) in order to insert the backup file to be restored in .na format.
Restore the configuration from the backup file	Next, click on this button in order to proceed to the restoration of the firewall's configuration, using the file selected above. You may be asked to reboot your firewall depending on the restored backup. If a reboot is necessary, you will have the choice of rebooting immediately or later.

Advanced properties

Backup password: If you have protected the selected backup with a password in the previous tab, Backup, enter it in this field.

Modules to be restored: it is possible to perform a partial or full restoration of your firewall's configuration.

Restore all modules of the backup file	This option is selected by default. If you choose to keep it that way, all modules contained in the backup file will be restored.

If you wish to restore only some of the modules of the backup file, unselect the option above in order to enable the following fields.
Select the configurations you wish to restore from:

- Network (interface, routing and dynamic DNS)
- SMTP filtering
- URL filtering
- SSL filtering
- Web objects
- Global modules
- Secure configuration
- Active Update
- Services (SNMP, DHCP server)
- Inspection profiles IPS
- Network objects
- Filtering and NAT
- IPSec VPN
- LDAP directory

“Secure configuration” tab

Secure configuration

In this window, you will be able to protect access to your firewall.

Enable "secure configuration" mode	The principle of this mode is to dissociate the “encrypted configuration” and “decryption key” on two different supports – one on a USB key, the other on your firewall’s hard disk, so that only the administrator in possession of the USB key can access the firewall’s configuration by starting it up.
USB key status	This field indicates the status of your USB key: when your backup has been encrypted, the field will indicate the status “initialized”. As an administrator, you will be able to remove the key. Anyone who attempts to reboot the appliance without the key will only obtain an unreadable configuration and will not be able to perform any operations. In order to retrieve the desired configuration, insert your USB key in the appliance, reboot your firewall and remove it once the appliance starts running.

Restore from the USB key

Restore the configuration on the key: By inserting your USB key in your firewall, you will be able to restore the configuration file stored on the key.

Select a backup file	Select the backup file to be retrieved using the button  .
Restore the configuration	Click on this button in order to proceed to the restoration of your configuration.

“System update” tab

Available updates:

Check for new updates	The firewall will conduct a search for new system updates on update servers (Objects/Network objects) and will display them on the screen.

Select the update:

Select an update file	Select the firewall update to be installed and insert it in the field using the button ... .
Save the active partition on the backup partition before updating the firewall	If this option is selected, you will back up your system's main partition on the backup partition, in order to keep a record of it. The appliance will reboot and update the firewall version
Update firmware	Apply the selected update on your appliance by clicking on this button.

Advanced properties

Action

Download the firmware update and install it	This option allows you to send the update file (.maj) and activate it.
Download the firmware update only	This option allows you to send the update file (.maj) without activating it. The file can be activated later using the option below "Install the uploaded firmware".
Install the uploaded firmware	If a file is located on the firewall, this option will allow you to activate it. **NOTE** If a file is present, the version indicated will be present in the field "Update present on the firewall".

Current version of the system

This field shows the current software version of your product.

Update uploaded on this firewall

This field displays the update that you had selected earlier at the top of this screen.

NETWORK OBJECTS

This module is divided into two sections:
- The action bar at the top, allowing you to sort and handle objects.
- Two columns dedicated to objects: one column listing them, the other displaying their properties.

Possible actions

Search	If you are looking for a particular object, enter its name. The search field allows you to list all the network objects whose properties match the keyword(s) or letter(s) entered. **Example** If you type the letter “a” in the search bar, the list below it will display all objects containing an “a” in their names or descriptions. You can also refine the search by using the “filter” that lists the various types of objects (see the section on the “Filter” button hereafter). **NOTE** The cross icon in the search field allows deleting the entry and listing all objects according to the current filter. ***From version 9.0.1 onwards***, when you go to the “Objects” tab in the menu directory on the left, the focus will now be on the search field.
Add	When you click on this button, a dialog box will appear, offering to create an object, by indicating its type and the information relating to it in the relevant fields. **REMARK** The object can be defined as a “global” object at the moment of its creation if you select the option *“This object is global”* in the dialog box. It will then appear when you select the “All objects” or “Network” filter (see below) and will be represented by the following icon .
Delete	Select the object to remove from the list and click on **Delete**.
Check usage	If you click on this button after having selected an event, the results will appear in the module directory.

Filter

This button allows you to select the type of objects to show. A drop-down menu will offer you the following choices:

All objects	Represented by the icon , this option allows displaying all types of network objects in the list of objects on the left.
Host	Represented by the icon , this option allows displaying only “host” objects in the

	column on the left.
Network	Represented by the icon, this option allows displaying only “network” objects.
IP address range	Represented by the icon, this option allows displaying only IP address ranges.
Port – port range	Represented by the icon , this option allows displaying ports and port ranges.
IP protocol	Represented by the icon , this option allows displaying only IP protocols.
Group	Represented by the icon, this option allows displaying only network groups.
Port group	Represented by the icon, this option allows displaying only port groups.

The different types of objects

Host

Select a host in order to view or edit its properties. Each one of them has by default a name, an IP address and a DNS resolution (“Automatic” or “None (static IP)”).

Object name	Name given to the object during its creation. This field can be modified, and to save changes, you need to click on “**Apply”** and “**Save**”. ***From version 9.0.1 onwards,*** the icon to the right of the checkbox allows obtaining the object’s IP address, which can be seen in the “IP address” field. To do so, the object’s full URL must be entered.
Comments	Description of the selected host.
DNS resolution	The DNS (*Domain Name System*) resolution matches IP addresses with a domain name. Two choices are possible: An **Automatic** (or “dynamic”) IP: If you select this option, the selected object will periodically receive an IP address. **None (static IP):** The selected object has a fixed IP address that will be used systematically.
IP address	IP address of the selected host.
MAC address	*Media Access control address*. This address corresponds to the physical address of a network interface or of a network card, allowing the identification of a host on a local network. **Example** *5E:FF:56:A2:AF:15.*

Network

Select a network in order to view or edit its properties. Each network has a name, IP address and a network mask.

Object name	Name given to the object during its creation. This field can be modified, and to save changes, you need to click on "**Apply"** and "**Save**".
Comments	Description of the selected network.
IP address	IP address of the selected network.
Network mask	Network mask or sub-network mask.

IP address range

Select an IP address range in order to view or edit its properties.

Object name	Name given to the object during its creation. This field can be modified, and to save changes, you need to click on "**Apply"** and "**Save**".
Comments	Description of the selected IP address range.
Start	First IP address of the range.
End	Last IP address of the range.

Port – port range

Select a port or port range in order to view or edit its properties.

Object name	Name of the service used. This field is grayed out and cannot be modified.
Comments	Description of the selected port or port range.
Port	Number of the port associated with the selected service.
Port range	By selecting this option, you will assign a port range to the selected service and enable the option below it.
From/To	If the previous option was selected, this field will be enabled and the end of the range will correspond to the number after the number of the selected port. **Example** If you select the object "cmd" that appears on port "514", the end of the range will be indicated as "515".
TCP/UDP	Select the IP protocol that your service uses: **TCP:** *Transmission Control Protocol*. Transport protocol operating in connected mode and made up of three phases: establishment of the connection, data transfer, end of the connection. **UDP:** *User Datagram Protocol.* This protocol allows transferring data simply between two entities, each of them having been defined by an IP address and a port number. **Any protocol**: The selected service can use any IP protocol (TCP, UDP or others).

IP protocol

Object name	Name of the selected IP protocol. This field is grayed out and cannot be modified.
Comments	Description of the selected IP protocol.
Protocol number	Number of the selected IP protocol.

Group

In this screen, you will be able to aggregate your objects according to your network topology, for example.

Object name	Name given to the object group during its creation. Objects in “read only” mode will be grayed out and cannot be modified.
Comments	Description of the object group.
Edit this group	This button contains a dialog box for adding objects to the group. Two columns will appear: The left column contains the list of all the network objects that you may add to your group. The right column contains the objects that are already in the group. To add an object to the group, you need to move it from one column to the other: 1 Select the item(s) to add. 2 Click on this arrow ➡. The object will move to the right column and become a part of your group (at the top of the list). To remove an object from the group, select it in the right column and click on this arrow ⬅. **NOTE** By clicking on the button “Edit this group”, you will be able to change the name of the group and add comments to it and also search for objects and include new objects in the group.
Objects in this group	The network objects in your group will be shown in a table. To add or modify objects, refer to the previous field.

Port group

This screen will allow you to aggregate your ports by category.
Example
A “**mail**” group that groups “imap”, “pop3” and “smtp” ports.

Object name	Name given to the port group during its creation.
Comments	Description of the port group.
Edit this group	This button contains a dialog box for adding ports to the group. By clicking on it, you will be able to change the name of the group and add comments to it and also search for ports and include new ports in the group. Two columns will appear: The left column contains the list of all the ports that you may add to your group. The right column contains the ports that are already in the group. To add a port to the group, you need to move it from one column to the other: 1 Select the item(s) to add. 2 Click on this arrow ➡. The object will move to the right column and become a part of your group (at the top of the list). To remove an object from the group, select it in the right column and click on this arrow ⬅. **NOTE** By clicking on the button “Edit this group”, you will be able to change the name

	of the group and add comments to it and also search for objects and include new objects in the group.
Objects in this group	The ports in your group will be shown in a table. To add or modify objects, refer to the previous field.

PPTP SERVER

The screen for configuring the **PPTP server** consists of 2 zones:

- **General configuration:** Activation of the PPTP server, selection of the address pool.
- **Advanced properties:** Selection of the number of PPTP connections.

Setting up the server is very quick and simple, and takes place in three steps:
This screen allows the configuration of the following parameters:

- The IP addresses of PPTP clients (object).
- Encryption parameters.
- The DNS server and WINS server.

General configuration

Enable PPTP server	Enables the configuration of the PPTP server on the firewall. This can be done by selecting the option **Enable PPTP server**.
IP addresses of PPTP clients (object) (mandatory)	Once the PPTP server has been enabled, a pool of private IP addresses must be created. The firewall will then assign available IP addresses from the pool to clients who connect in PPTP. A host group must be created, containing reserved addresses or an address range from the object database.

Parameters sent to PPTP clients

DNS server	The field **DNS server** allows sending the IP address of the DNS server to the client.
WINS server	The field **WINS server** allows sending the IP address of the WINS server to the client.

From version 9.0.1 onwards, the characters "_", "-", and "." are allowed for PPTP user names.

Advanced properties

Number of reserved PPTP connections [0-96] (number varies according to the model installed): If you wish to create a new PPTP server but have reached the maximum number of dynamic PPTP connections possible, you can still increase the number.

REMARK
Once the number of PPTP connections is modified (regardless of whether it is an increase or a decrease), the firewall has to be rebooted in order to apply changes.

Traffic encryption

The possible encryption parameters are:

Do not encrypt	This will disable the field **Accept only encrypted traffic and allow the following algorithms** as well as the MPPE offered.
Accept only encrypted traffic and allow the following algorithms	Allows the connection only if the client encrypts data.
40-bit MPPE	Allows the use of the 40-bit MPPE encryption protocol.
56-bit MPPE	Allows the use of the 56-bit MPPE encryption protocol.
128-bit MPPE	Allows the use of the 128-bit MPPE encryption protocol.

PREFERENCES

This module is accessible via the button  in the top row of the interface.
It will allow you to manage the parameters of your web interface.
Depending on your selection of options, you will be able to save time and browse more easily.

Access NETASQ's website

ID	Your NETASQ login (in general, lastname.firstname or your e-mail address)
Password	Enter your password. The icon  allows you to display the password in plaintext in order to avoid errors.
Access your private NETASQ area	Click on this button to directly access your secure NETASQ area (also accessible on **www.netasq.com**).

Connection settings

Connect automatically with an SSL certificate	If this option is selected, you will no longer need to identify yourself, as you will be recognized directly thanks to your SSL certificate.
Log out when idle	A duration can be set for the disconnection from your web interface: 5 minutes 15 minutes 30 minutes 1 hour You can also choose to "Always remain connected".
Systematically display the last active module at startup	If this option is selected, every time you log on, you will be redirected to the last module displayed before you were disconnected.

Application settings

Always display advanced properties	The elements of advanced properties can be expanded in every module that has them, but are collapsed by default. By selecting this option, you will make them visible on the screen without having to expand them.
Display users at startup of module	If this option is selected, all users will be displayed in the directory on the left.
Display network objects at startup of module	If this option is selected, all network objects will be displayed in the directory on the left.
Display the global security policy (filtering and NAT)	If this option is selected, the screen will display the local security policy in force whenever you connect to the menu Security policy \Filtering and NAT.

Display the security policy	Depending on the number of existing rules, you can choose to display: 30 rules per page 50 rules per page 100 rules per page 200 rules per page 500 rules per page By selecting “Automatic”, the NETASQ engine will try to deduce the number of rules per page, according to your configuration.

Management interface behavior

Search every field of an object	When you perform a search by letter or by word in the dedicated fields, the engine will check both the names and the comments, to find anything that matches the object of the search.
Disable real-time diagnoses of the security policy	When you create a rule in the security policy, the diagnosis engine will automatically check if rules overlap and if errors have been detected. If this option is selected, a manual search for these possible errors will be implied.
Week starts on Sunday	If this option is selected, Time objects that appear in the menu Objects will begin their weeks on Sunday.
Confirm before applying changes	This option allows cancelling your actions if you have made a wrong move or if you decide not to continue with your configuration. A confirmation window will appear, allowing you to confirm or cancel your action.

External links

Online help URL	This URL indicates the address to access NETASQ’s online help: you will find the directory of the modules in alphabetical order. Click on the module of your choice in order to view the corresponding page.
Alarm online description URL	This address allows you to access a help document that will help you to understand the Alarms module, which appears in the NETASQ knowledge base.
Administration suite URL	This URL allows you to download the NETASQ administration suite: Monitor, Reporter, and GlobalAdmin.

PROTOCOLS AND APPLICATIONS

This module contains the list of the various protocols and applications that can be configured from your web interface.
It is divided into 2 distinct zones:

- Protocols (left column)
- Profiles that can be assigned to the protocols and their parameters (right column)

The zone for profiles is empty by default and allows you to select a protocol in the left column.

Protocols

Search

The search bar allows locating the protocol to be configured by entering the first few letters of its name. Clicking on the desired protocol allows working directly with it.

List of protocols

Select the protocol that you wish to configure in the list displayed.
Once the protocol has been selected, you can start configuring it.

Profiles

Selecting a profile

The drop-down list offers 10 profiles, numbered from 00 to 09.
Each profile is named “Default” by default, accompanied by its number.
Examples:

- (0) Defaut00
- (1) Default01…

Buttons

Edit	This function allows performing 3 operations on profiles: • **Rename:** by clicking on this option, a window comprising two fields will appear. It will allow you to modify the name and add comments. Once the operation has been performed, click on “Update”. This operation can also be cancelled. • **Reinitialize**: allows resetting the profile to its initial configuration, thereby deleting all changes made to the profile. • **Copy to:** This option allows copying a profile to another, with all the information from the copied profile transmitted to the receiving profile. It will also have the same name.
Last modification	This icon allows finding out the exact date and time of the last modification. If the

	selected profile has comments, they will be displayed in the tooltip.
Go to global configuration	This option contains the list of default TCP ports. This option is accessible in each protocol except: IP, ICMP, RTP, RTCP. You can **Add** or **Delete** ports by clicking on the respective buttons.

HTTP

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.

"IPS" tab

Automatically detect and inspect the protocol	If this protocol has been enabled, it will automatically be used for discovering corresponding packets in filter rules. This option is not available for IP, ICMP TCPUDP, RTP, RTCP, MSN, and YMSG.

HTTP protocol extensions

Allow Shoutcast support	This option allows transporting sound over HTTP. **Examples:** Webradio, webtv.
Allow WebDAV connections (reading and writing)	This option allows adding writing and locking features to HTTP, and also allows securing HTTPS connections more easily.

Allowed HTTP commands

List of allowed HTTP commands (in CSV format). All commands included may not exceed 126 characters.
It is possible to **Add** or **Delete** commands using the respective buttons.

Prohibited HTTP commands

List of prohibited HTTP commands (in CSV format). All commands included may not exceed 126 characters.
It is possible to **Add** or **Delete** commands using the respective buttons.

URL: maximum size of elements (in bytes)

Defining a maximum size for the elements (in bytes) allows countering buffer overflow attacks.

URL (domain+path)	Maximum size of a URL, domain name and path inclusive [128 – 4096 bytes]
Per parameter (after the '?' [argument])	Maximum size of a parameter in a URL [128 – 4096 (bytes)]

Full query (URL + parameters)	Maximum number of bytes for the full query: http://URLBuffer ?QueryBuffer [128 – 4096] (bytes)]

URL

Max. nb of parameters (after '?')	Maximum number of parameters in a URL (Min :0 ; Max : 512).

HTTP headers: maximum size of elements (in bytes)

Number of lines per client request	Maximum number of lines (or headers) that a request can contain, from the client to the server (Min:16; Max: 512).
Number of ranges per client request	Maximum number of ranges that a response can contain, from the server to the client (Min:0 ; Max: 1024).
Number of lines per server response	Maximum number of lines (or headers) that a response can contain, from the server to the client (Min:16; Max: 512).

Taille maximale des champs http (en octets)

AUTHORIZATION field	Maximum number of bytes for the AUTHORIZATION field, including formatting attributes. (Min: 128; Max: 4096).
CONTENTTYPE field	Maximum number of bytes for the CONTENTTYPE field, including formatting attributes. (Min: 128; Max: 4096).
HOST field	Maximum number of bytes for the HOST field, including formatting attributes. (Min: 128; Max: 4096).
COOKIE field	Maximum number of bytes for the COOKIE field, including formatting attributes. (Min: 128; Max: 4096).
Other fields	Maximum number of bytes for others field, including formatting attributes. (Min: 128; Max: 4096).

HTML/JavaScript analyses

Inspect HTML code	Instead of prohibiting the TCP connection, the scan will erase the malicious attributes that may be contained in the HTML code, by letting the rest of the response pass through.

Max. length for a HTML tag (Bytes)	Maximum number of bytes for an attribute of a HTML tag (Min : 128 ; Max : 65536).

Inspect JavaScript code	In order to prevent malicious content from damaging dynamic and interactive web pages that use JavaScript programming, a scan will be conducted in order to detect them. Likewise for the option **Inspect HTML code**, if this option is selected, the scan will be conducted by erasing malicious content without blocking the packet.
Automatically delete malicious content	If this option is selected, any malicious code that makes its way into HTML or JavaScript code will automatically be deleted.

	Example of malicious behavior: Redirection without your knowledge, to a website other than the site you had intended to visit.

List of exceptions to the automatic deletion of malicious code (User-Agent)

This list displays the browsers and their data, which will not be automatically deleted by the earlier option mentioned above. It is possible to **Add** or **Delete** elements to or from this list by clicking on the relevant buttons.

HTTP session parameters (in seconds)

Maximum request duration	Set to 30 seconds by default (Max: 600 seconds).

Support

Disable intrusion prevention	By selecting this option, the URL filter will automatically be set to “Pass”.
Log each HTTP request	Enables or disables the logging of HTTP requests.

“Proxy” tab

Connection

Keep original source IP address	When a request is made by a web client (browser) to the server, the firewall will intercept it and check that the request complies with URL filter rules and then relays the request. If this option is selected, the new request will use the original source IP address of the web client that sent the packet. Otherwise, the firewall’s address will be used.

HTTP protocol extensions

Allow WebDAV connections (reading and writing)	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.
Allow TCP tunnels (CONNECT method)	The **CONNECT** method allows building secure tunnels through proxy servers. If this option has been selected, the **CONNECT** method will be authorized in the NETASQ Firewall.

TCP tunnels: List of allowed destination ports

In this zone, specify the types of service that can use the **CONNECT method**.

Destination port (service object)	The **Add** button allows you to add services objects database. To **modify** a service, select the line to be modified and make changes. Use the **Delete** button to delete the selected service.

Advanced properties

Explicit proxy

The explicit proxy allows referencing the proxy in a browser and sending HTTP requests directly to it.

Allow several users per IP address	This option allows assigning a common IP address to several users

Protection quality

Check URL encoding	By selecting this option, the filter policy cannot be bypassed.

Traffic sent to the server

Add authenticated user to HTTP header	If the external HTTP proxy requires user authentication, the administrator can select this option to send data regarding the user (collected by the firewall's authentication module) to the external proxy.

"ICAP" tab

Web and mail contents are the main targets of the ICAP protocol, which provides an interface to HTTP proxies (for the web) and to SMTP relays (for mail).

HTTP request (reqmod)

Send HTTP requests to the ICAP server	Each client request to a website is sent to the ICAP server.

ICAP Server

Server	Indicates the ICAP server.
Port	Indicates the ICAP port.
Name of ICAP service	Indicates the name of the service to set up. This information varies according to the solution used, the ICAP server as well as the port used.

Authentication on the ICAP server

Information available on the firewall can be used for performing ICAP services.
Example

It is possible to define in an ICAP server that a certain site is intended for a certain user. In this case, you will be able to filter according to an LDAP ID or an IP address.

Send the username/group name	This option allows using information relating to the LDAP base (especially the logins of authenticated users).
Send client's IP address	This option allows using IP addresses of HTTP clients who send requests to Adapter (object used for translating between the ICAP format and the requested format).

HTTP response (respmod)

Send HTTP responses to the ICAP server	Each response from the HTTP server to the client is sent to the ICAP server

ICAP Server

Server	Indicates the ICAP server.
Port	Indicates the ICAP port.
Name of ICAP service	Indicates the name of the service to set up. This information varies according to the solution used, the ICAP server as well as the port used.

Authentication on the ICAP server

Information available on the firewall can be used for performing ICAP services.

Example

It is possible to define in an ICAP server that a certain site is intended for a certain user. In this case, you will be able to filter according to an LDAP ID or an IP address.

Send the username/group name	This option allows using information relating to the LDAP base (especially the logins of authenticated users).
Send client's IP address	This option allows using IP addresses of HTTP clients who send requests to Adapter.

Advanced properties

Whitelist (will not be sent to the ICAP server)

HTTP server (Host – Network – Address range)	Adds hosts, networks or address ranges whose details will not be sent to the ICAP server. These items can be deleted from the list at any time.

"Analyzing files" tab

Transferring files

Partial download	When a download is incomplete, for example, due to a connection failure during a file download via HTTP, the user can continue to download from where the error occurred, 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 **Partial download** allows defining the behavior of the firewall's HTTP proxy towards this type of download. • **Block**: partial downloads are prohibited • **Block if antivirus has been enabled**: partial downloads are authorized and the antivirus module filters the traffic. • **Pass**: partial downloads are authorized but there will not be any antivirus scan.
File size limit [0-2147483647(KB)]	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, indicate the maximum size (in KB) that can be downloaded by HTTP.

File filter (MIME type)

Status	Indicates whether a file is active or inactive. 2 positions are available: "Enabled" or "Disabled".

Action	Indicates the action to be taken for the file in question, out of 3 possibilities: • **Detect and block viruses**: The file will be scanned in order to detect viruses that may have infected the files. These viruses will be blocked. • **Pass without antivirus scan**: The file can be downloaded freely without any antivirus scans being performed. • **Block:** The download is prohibited.
MIME type	Indicates the file content type. This could be text, an image or a video, to be defined in this field. **Examples**: "text/plain*" "text/*" "application/*"
Maximum size for antivirus scan (KB)	This field corresponds to the maximum size of files that will be scanned. This limit has been set to 1000 KB by default.

Actions on files

When a virus is detected	This field contains 2 options. By selecting "Block", the analyzed file will not be sent. By selecting "Pass", the antivirus will send the file in its original form.
When the antivirus scan fails	This option defines the behavior of the antivirus module if the analysis of the file it is scanning fails. **Example:** The file could not be scanned as it has been locked. If **Block** has been specified, the file being scanned will not be sent. If **Pass without scanning** has been specified, the file being scanned will be sent.
When data collection fails	This option defines the behavior of the antivirus module when certain events occur. It is possible to **Block** traffic when information retrieval fails, or **Pass without scanning**. **Example:** If the hard disk has reached its capacity, information will not be downloaded.

SMTP

The aim of the SMTP protocol is to detect connection between a client and an e-mail server or between two e-mail servers using SMTP. It allows sending e-mails and is used by SEISMO to detect the version of the client and/or e-mail server in order to report possible vulnerabilities.

"IPS" tab

Automatically detect and inspect the protocol	If this protocol has been enabled, it will automatically be used for discovering corresponding packets in filter rules. This option is not

	available for IP, ICMP TCPUDP, RTP, RTCP, MSN, and YMSG.

SMTP protocol extensions

Filter the CHUNKING extension	Allows filtering data transferred from one e-mail address to another. **Example:** Attachments in e-mails.
Filter Microsoft Exchange Server extensions	Allows filtering additional commands from the Microsoft Exchange Server.
Filter request to change connection direction (ATRN, ETRN)	Allows filtering data contained in the request to change connection direction, from the client to the server, or from the server to the client. During an SMTP communication, the use of ATRN and ETRN commands allows exchanging the client/server roles.

Maximum size of elements (KB)

Defining a maximum size for the elements (in KB) allows countering buffer overflow attacks.

Message header [64 – 4096]	Maximum number of characters that an e-mail header can contain (e-mail address of the sender, date, type of encoding used, etc.)
Server response line [64 – 4096]	Maximum number of characters that the response line from the SMTP server can contain.
Exchange data (XEXCH50) [102400 – 1073741824]	Maximum volume of data when transferring files in MBDEF format (Message Database Encoding Format).
BDAT extension header [102400 – 10485760]	Maximum volume of data sent using the BDAT command.
Command line [64 – 4096]	Maximum volume of data that a command line can contain (excluding the DATA command).

Support

Disable intrusion prevention	By selecting this option, the configuration of the various fields in the tab will not be applied.
Log each SMTP request	Enables or disables the logging of SMTP requests.

“Proxy” tab

Filter the welcome banner	When this option is selected, the server’s banner will become anonymous during an SMTP connection.

HELO Command

Replace the client's domain name with its IP address	During a basic identification, the client enters its domain name by executing the HELO command. By selecting this option, the domain name will be replaced by the IP address.

Connection

Keep original source IP address	When a request is made by a web client (browser) to the server, the firewall will intercept it and check that the request complies with URL filter rules and then relays the request. If this option is selected, the new request will use the original source IP address of the web client that sent the packet. Otherwise, the firewall's address will be used.

Limits when sending an e-mail

Message line [1000-2048 (KB)]	This field indicates the maximum length of a line when sending a message. **REMARK** Imposing a maximum size for elements (in bytes) allows countering buffer overflow attacks.
Maximum number of recipients [0 – 2147483647 (KB)]	Indicates the maximum number of recipients that a message can contain. The firewall will refuse messages with too many recipients (the refusal will be indicated by an SMTP error). This allows restricting spam.
Maximum size of the message [0 – 2147483647 (KB)]	Indicates the maximum size of messages passing through the NETASQ firewall. Messages exceeding the defined size will be refused by the firewall.

"SMTP Commands" tab

This menu allows you to authorize or reject SMTP commands defined in the RFCs. You can let commands pass, block them or analyze the syntax and check that the command complies with the current RFCs in force.

Proxy

Main commands

The button **Modify all commands** allows authorizing, rejecting or checking all commands.

Command	Indicates the name of the command.
Action	Indicates the action performed.

Other commands allowed

Command	By default, all commands not defined in the RFCs are prohibited. However, some mail systems use additional non-standard commands. You can therefore add these commands in order to let them pass through the firewall. The buttons **Add** and **Delete** allow you to modify the list of commands.

IPS

Allowed SMTP commands

List of additional authorized SMTP commands. It is possible to **Add** or **Delete** commands.

Prohibited SMTP commands

List of prohibited SMTP commands. It is possible to **Add** or **Delete** commands.

"Analyzing files" tab

Maximum size for antivirus scan [0 – 1000 (KB)]	This option depends on the hardware capacities of each firewall model but may be adapted according to the needs of the company.

WARNING

When manually defining a size limit for analyzed data, ensure that all values are coherent. The total memory space 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.

Action on messages

This zone defines the behavior of the antivirus module when certain events occur.

When a virus is detected	This field contains 2 options. By selecting "Block", the analyzed file will not be sent. By selecting "Pass", the antivirus will send the file event it has been found to be infected.
When the antivirus scan fails	This option defines the behavior of the antivirus module if the analysis of the file it is scanning fails. If **Block** has been specified, the file being scanned will not be sent. If **Pass without scanning** has been specified, the file being scanned will be sent.
When data collection fails	This option defines the behavior of the antivirus module when certain events occur. **Examples:** If the hard disk has reached its capacity, information will not be downloaded. The maximum size that the file can reach for the antivirus scan is restricted (1000KB).

POP3

The aim of the POP3 protocol is to detect connections between a client and e-mail server using the POP3 protocol.

"IPS - PROXY" tab

Both of these features have been condensed in a single tab for ease of use.

IPS

Automatically detect and inspect the protocol	If this protocol has been enabled, it will automatically be used for discovering corresponding packets in filter rules. This option is not available for IP, ICMP TCPUDP, RTP, RTCP, MSN, and YMSG.

Proxy

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 program. 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.

Filter the welcome banner sent by the server	When this option is selected, your mail server's banner will no longer be sent during a POP3 connection. This banner contains information that may be exploited by hackers (server type, software version, etc).

Connection

Keep original source IP address	When a request is made by a web client (browser) to the server, the firewall will intercept it and check that the request complies with URL filter rules and then relays the request. If this option is selected, the new request will use the original source IP address of the web client that sent the packet. Otherwise, the firewall's address will be used.

Support

Disable intrusion prevention	By selecting this option, the configuration of the various fields in the tab will not be applied.
Log each POP3 request	Enables or disables the logging of POP3 requests.

"POP3 Commands" tab

Proxy

Main commands

This menu allows you to authorize or reject POP3 commands defined in the RFCs. You can let commands pass, block them or analyze the syntax and check that the command complies with the current RFCs in force.
The button **Modify all commands** allows authorizing, rejecting or checking all commands.

Command	Indicates the name of the command.
Action	Allows defining the behavior of the command out of 3 possibilities. Click on the command's action to modify it: • **Scan**: data relating to the command will be scanned in compliance with the RFCs and blocked where necessary. **Example:** If the name of the USER command does not comply with the RFCs, the packet will not be sent to the server. • **Pass without scanning**: the command will be authorized, without being checked. • **Block:** the command will be blocked automatically, and an alarm will be raised to indicate it.

Other commands allowed

Command	This field allows adding additional personal commands.

"Analyzing files" tab

Maximum size for antivirus scan (KB)	This option depends on the hardware capacities of each firewall model. It corresponds to the maximum size of files that will be scanned. This limit has been set to 1000 KB by default.

WARNING
When manually defining a size limit for analyzed data, ensure that all values are coherent. The total memory space corresponds to a common space for all the 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.

Action on messages

This zone defines the behavior of the antivirus module when certain events occur.

When a virus is detected	This field contains 2 options. By selecting "Block", the analyzed file will not be sent. By selecting "Pass", the antivirus will send the file in its original form.
When the antivirus scan fails	This option defines the behavior of the antivirus module if the analysis of the file it is scanning fails. **Example:** The file could not be scanned as it has been locked. If **Block** has been specified, the file being scanned will not be sent. If **Pass without scanning** has been specified, the file being scanned will be sent without being checked.
When data collection fails	This option defines the behavior of the antivirus module when certain events occur. It is possible to **Block** traffic when information retrieval fails, or **Pass without scanning**.

FTP

"IPS" tab

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.

Automatically detect and inspect the protocol	If this protocol has been enabled, it will automatically be used for discovering corresponding packets in filter rules. This option is not available for IP, ICMP TCPUDP, RTP, RTCP, MSN, and YMSG.

Authentication

Allow SSL authentication	Enables SSL authentication for the protocol (FTP only). By selecting this option, personal data such as the login and password may be encrypted and therefore, protected.
Do not scan the FTP authentication phase	No data scans will be performed

Size of elements (in bytes)

Defining a maximum size for the elements (in bytes) allows countering buffer overflow attacks.

User name	Maximum number of characters that a user name can contain. This value must be between 10 and 2048 bytes.
User password	Maximum number of characters for the FTP password. This value must be between 10 and 2048 bytes.
Path (directory + filename)	Maximum number of characters of the path taken by the program execution, or the path taken in the directory to reach the FTP file. This value must be between 10 and 2048 bytes.
SITE command	Maximum number of characters that the SITE command can contain (between 10 and 2048 bytes).
Other commands	Maximum number of characters that additional commands can contain (between 10 and 2048 bytes)

Support

Disable intrusion prevention	By selecting this option, the profile that has just been created will not be applied.
Log each FTP request	Enables or disables the logging of FTP requests.

"Proxy" tab

Filter the welcome banner sent by the FTP server	If this option is selected, the server's banner will no longer be sent during an FTP connection.
Block FTP bounce	Allows the prevention of IP address spoofing. By executing the PORT command and by specifying an internal IP address, an external host may access confidential data by exploiting vulnerabilities in an FTP server or a host that is vulnerable to bounces.

Connection

Keep original source IP address	When a request is made by a web client (browser) to the server, the firewall will intercept it and check that the request complies with URL filter rules and then relays the request. If this option is selected, the new request will use the original source IP address of the web client that sent the packet. Otherwise, the firewall's address will be used.

Authorized transfer modes

Between the client and the proxy	When the FTP client sends a request to the server, the proxy will first intercept the request in order to analyze it. From the FTP "client"'s point of view, the proxy corresponds to the server. This option allows defining the authorized transfer mode. If **Active only** is specified, the FTP client will determine the connection port to use for transferring data. The FTP server will then initialize the connection from its data port (port 20) to the port specified by the client. If **Passive only** is specified, the FTP server will determine the connection port to use for transferring data (data connection) and will transmit it to the client. If **Active and passive** is specified, the FTP client will be able to choose between both transfer modes when configuring the firewall.
Between the proxy and the server	When the proxy has finished scanning the client request, it will transfer it to the FTP server, which will then interpret the proxy as the FTP client. Since the proxy has an intermediary role, it is transparent. The authorized transfer modes are the same as for the previous option.

"Commands" tab

Proxy

Main commands

Modify all commands button. This button allows you to **Pass without scanning**, **Block** or **Scan** the syntax and check that the command complies with the RFCs in force, for generic commands as well as modification commands.

Command	Name of the command.
Action	3 authorizations possible from "Pass without scanning", "Scan" and "Block".
Command type	Indicates the type of command. "Writing" FTP commands defined in the RFCs can cause 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.

Other commands allowed

Additional commands, limited to 21 characters, can be added and deleted when necessary.

IPS

Authorized FTP commands

FTP commands, limited to 115 characters, can be defined in the intrusion prevention module, by clicking on **Add**. They can also be deleted.

Prohibited FTP commands

FTP commands, limited to 115 characters, can be prohibited in the intrusion prevention module.

"Analyzing files" tab

Maximum size for antivirus scan [0 – 1000] (KB)	In this field, the maximum size used for scanning files can be determined. Move the scale to do so. You can also configure the action to perform if the file exceeds the authorized size. **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.
Analyzing files	This option allows choosing the type of file that needs to be scanned: "downloaded and sent" files; "downloaded only" or "sent only" files.

Actions on files

When a virus is detected	This field contains 2 options. By selecting "Block", the analyzed file will not be sent. By selecting "Pass", the antivirus will send the file in its original form.
When the antivirus scan fails	This option defines the behavior of the antivirus module if the analysis of the file it is scanning fails. **Example:** The file could not be scanned as it has been locked. If **Block** has been specified, the file being scanned will not be sent. If **Pass without scanning** has been specified, the file being scanned will be sent.
When data collection fails	This option defines the behavior of the antivirus module when certain events occur. It is possible to **Block** traffic when information retrieval fails, or **Pass without scanning**.

SSL

"IPS" tab

This screen will allow you to confirm the activation of the SSL protocol through the firewall.
Certain options allow reinforcing this protocol's security. For example, negotiations of cryptographic 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).

Automatically detect and inspect the protocol	If this protocol has been enabled, it will automatically be used for discovering corresponding packets in filter rules. This option is not available for IP, ICMP TCPUDP, RTP, RTCP, MSN, and YMSG.

SSL negotiation

Allow unsupported encryption methods	Select this option if the encryption algorithm that you wish to use is not supported by the SSL protocol.
Allow unencrypted data after an SSL negotiation	This option allows sending data in plaintext after an SSL negotiation. **WARNING** Allowing data transmission in plaintext poses a security risk.
Encryption levels allowed	The stronger the encryption algorithm used and the more complex the password, the higher the level of security. **Example** The AES encryption algorithm with a strength of 256 bits, associated with a password of about ten characters made up of letters, numbers and special characters. Three choices of encryption levels can be authorized: **Low, medium, high:** for example, DES (64 bits), CAST128 (128 bits) and AES. Regardless of the password's security level, the encryption level will be allowed. **Medium and high**: Only medium-security and high-security algorithms will be tolerated. **Only high:** Only strong algorithms and passwords with a high level of security will be tolerated.

Unencrypted data detection (plaintext traffic)

Detection method	**Do not detect:** unencrypted data will not be scanned. **Inspect all traffic**: all packets received will be scanned by the SSL protocol in order to detect plaintext traffic. **Sampling (7168 bytes):** only the first 7168 bytes of the traffic will be analyzed in order to detect plaintext traffic.

Support

Disable intrusion prevention	By selecting this option, the configuration of the various fields in the tab will not be applied.
Log every SSL query	Enables or disables the logging of SSL requests.
Disable Skype detection	The Skype application uses port 443 and a protocol that resembles a valid SSL session. However, several competitors may block the use of Skype. This option when selected, allows the user to unblock Skype traffic without stopping the analysis of SSL traffic. Check this option to block Skype traffic.

"Proxy" tab

Connection

Keep original source IP address	When a request is made by a web client (browser) to the server, the firewall will intercept it and check that the request complies with URL filter rules and then relays the request. If this option is selected, the new request will use the original source IP

	address of the web client that sent the packet. Otherwise, the firewall's address will be used.

Content inspection

Self-signed certificates	This option will determine the action to perform when self-signed certificates are presented: you can either **Block them** or **Continue analysis** by accepting them. These certificates are used internally and signed by your local server. They allow guaranteeing the security of your exchanges and authenticating users, among other functions.
Expired certificates	This option will determine the action to perform when self-signed certificates are presented: you can either **Block** them or **Continue analysis** by ignoring them. Expired certificates have validity dates that have lapsed and are therefore not valid. To fix this problem, they must be renewed by a certificate authority **WARNING** Expired certificates may pose a security risk. After the expiry of a certificate, the CA that issued it will no longer be responsible for it if it is used maliciously.
Unknown certificates	This option will determine the action to perform when self-signed certificates are presented: you can either **Block** them or **Continue analysis** by ignoring them.
Certificate with incorrect FQDN *From version 9.0.3 onward*	This option will determine the action to perform when certificates with an invalid domain name are encountered: you may choose to **Block the traffic** or to **Continue analysis** and ignoring the error.

Support

If decryption fails	This option will determine the action to perform when decryption fails: you can choose to **Block traffic** or **Pass without decrypting**. Traffic will not be inspected if the second option is selected.

TCP-UDP

TCP ensures control of data during their transfer. Its role is to check that IP packets sent are received in good order, without any loss of changes integrity-wise.
UDP may replace TCP in the event of minor problems, as it ensures a more fluid transfer since it does not control each of the transmission stages. For example, it is suitable for streaming applications (audio/video broadcast) for which packet loss is not vital. Indeed, during these transmissions, lost packets are ignored.
By selecting TCP-UDP from the list, you can access two screens:

- Global configuration
- Access to profiles

Profiles screen

"IPS-Connection"

Inspection

Impose MSS limit	This option allows you to set an MSS (*Maximum Segment Size*) limit for the inspection of the profile. **NOTE** MSS refers to the amount of data in bytes that a computer or any other communication device can contain in a single unfragmented packet. If this option is selected, you will enable the following field, which would allow you to set your limit.
MSS limit (in bytes)	Define your MSS limit, between 100 and 65535 bytes.
Rewrite TCP sequences with strong random values (arc4).	If this option is selected, TCP sequence numbers generated by the client and server will be overwritten and replaced with the NETASQ intrusion prevention engine, which will produce random sequence numbers.
Enable protection from repeated sending of ACK packets	If this option is selected, you are protecting yourself from session hijacking or "ACK" attacks.

Timeout (in seconds)

Connection opening timeout (SYN)	Define an opening timeout for a connection, between 10 and 60 seconds.
TCP connection	Define a lifetime for your TCP connection, between 30 and 604800 seconds.

UDP pseudo-connection	Define a lifetime for your UDP connection, between 30 and 3600 seconds.
Connection closing timeout (FIN)	Define the period after which the connection has to be shut down, between 10 and 3600 seconds.
Closed connection timeout	Define when the connection has to be shut down, between 10 and 60 seconds.
Small TCP window	Define the lifetime of a small TCP window, between 5 and 604800 seconds.

Support

Disable the SYN proxy	If this option is selected, you will no longer be protected from “SYN” attacks, as the proxy will no longer filter packets.

Global configuration screen

“IPS” tab

Denial of service (DoS)

Max no. of ports per second	This number has to be between 1 and 16 ports per second.
Purge session table every (seconds)	Define the duration after which session tables have to be purged, between 10 and 172800 seconds.

Connection

Allow half-open connections (RFC 793, section 3.4)	This option allows avoiding denial of service attacks that may operate within apparently “normal” connections.

IP

"IPS" tab

MTU

Impose MTU limit (force fragmentation)	MTU (*Maximum Transmission Unit*) represents the maximum size of an IP packet. If this option is selected, you will enable the next field and can define your limit.
Maximum MTU value	Define the maximum value of the IP datagram, between 140 and 65535 bytes.

Fragmentation

Minimum fragment size (bytes)	The fragment has to be between 140 and 65535 bytes.
Session will expire in (seconds)	This period has to be between 2 and 30 seconds.

NOTE
The IP protocol does not have a profile.

ICMP

"IPS" tab

Session parameters (in seconds)

Session expiry	This value has to be between 2 and 60 seconds.

Support

Ignore ICMP notifications (stateful TCP/UDP)	If this option is selected, you will no longer take into account error messages that could arise in the protocols, such as the accessibility of a service or a host, for example.

DNS

Profiles screen

"IPS" tab

Automatically detect and inspect the protocol	If this protocol has been enabled, it will automatically be used for discovering corresponding packets in filter rules. This option is not available for IP, ICMP TCPUDP, RTP, RTCP, MSN, and YMSG.

Maximum size of DNS fields (in bytes)

DNS name (query)	This field has to be between 10 and 2048 bytes.

Whitelist of DNS domains (DNS rebinding)
This list contains the allowed domain names (<*www.ofdomain.fr*>, for example) to be resolved by a server located on an unprotected interface.
You can add domains by clicking on the appropriate button or remove it from the list by selecting it and clicking on "Delete".

Support

Disable intrusion prevention	By selecting this option, the URL filter will automatically be set to "Pass".

Global configuration screen

DNS: list of default UDP ports

This list contains the UDP ports allowed by default.
You can add ports by clicking on the appropriate button or remove them from the list by selecting them and clicking on "Delete".

Yahoo Messenger (YMSG)

Profiles screen

"IPS" tab

Automatically detect and inspect the protocol	If this protocol has been enabled, it will automatically be used for discovering corresponding packets in filter rules. This option is not available for IP, ICMP TCPUDP, RTP, RTCP, MSN, and YMSG.

Support

Disable intrusion prevention	By selecting this option, the URL filter will automatically be set to "Pass".
Log every Yahoo Messenger (YMSG) query	Enables or disables the generation of logs relating to the Yahoo Messenger protocol.

Global configuration screen

YMSG: list of default TCP ports

This list contains the TCP ports allowed by default.
You can add ports by clicking on the appropriate button or remove them from the list by selecting them and clicking on "Delete".

ICQ – AOL IM (OSCAR)

Profiles screen

"IPS" tab

Automatically detect and inspect the protocol	If this protocol has been enabled, it will automatically be used for discovering corresponding packets in filter rules. This option is not available for IP, ICMP TCPUDP, RTP, RTCP, MSN, and YMSG.

Support

Disable intrusion prevention	By selecting this option, the URL filter will automatically be set to "Pass".
Log every OSCAR query	Enables or disables the generation of logs relating to OSCAR queries.

Global configuration screen

OSCAR: list of default TCP ports

This list contains the TCP ports allowed by default for the OSCAR protocol.
You can add ports by clicking on the appropriate button or remove them from the list by selecting them and clicking on "Delete".

OSCAR over SSL: list of default TCP ports

This list contains the TCP ports using SSL allowed by default for the OSCAR protocol.
You can add ports by clicking on the appropriate button or remove them from the list by selecting them and clicking on “Delete”.

Live Messenger (MSN)

Profiles screen

“IPS” tab

Automatically detect and inspect the protocol	If this protocol has been enabled, it will automatically be used for discovering corresponding packets in filter rules. This option is not available for IP, ICMP TCPUDP, RTP, RTCP, MSN, and YMSG.

Support

Disable intrusion prevention	By selecting this option, the URL filter will automatically be set to “Pass”.
Log every Live Messenger query	Enables or disables the generation of logs relating to Live Messenger queries.

Global configuration screen

MSN: list of default TCP ports

This list contains the TCP ports allowed by default for MSN.
You can add ports by clicking on the appropriate button or remove them from the list by selecting them and clicking on “Delete”.

TFTP

Profiles screen

“IPS” tab

Automatically detect and inspect the protocol	If this protocol has been enabled, it will automatically be used for discovering corresponding packets in filter rules. This option is not available for IP, ICMP TCPUDP, RTP, RTCP, MSN, and YMSG.

Size of elements (in bytes)

File name	This number has to be between 64 and 512 bytes.

Support

Disable intrusion prevention	By selecting this option, the URL filter will automatically be set to “Pass”.
Log every TFTP query	Enables or disables the generation of logs relating to TFTP queries.

Global configuration screen

TFTP: list of default TCP ports

This list contains the TCP ports allowed by default for TFTP.
You can add ports by clicking on the appropriate button or remove them from the list by selecting them and clicking on “Delete”.

NetBios CIFS

NetBios is a protocol that is used for sharing files/printers, generally by Microsoft systems.

Profiles screen

“IPS” tab

Automatically detect and inspect the protocol	If this protocol has been enabled, it will automatically be used for discovering corresponding packets in filter rules. This option is not available for IP, ICMP TCPUDP, RTP, RTCP, MSN, and YMSG.

Size of elements (in bytes)

Name of files (SMB2 format)	This number has to be between 1 and 65536 bytes.

Support

Disable intrusion prevention	By selecting this option, the URL filter will automatically be set to “Pass”.

Global configuration screen

NetBios CIFS: list of default TCP ports

This list contains the TCP ports allowed by default for NetBios CIFS.
You can add ports by clicking on the appropriate button or remove them from the list by selecting them and clicking on “Delete”.

NetBios CIFS: list of default UDP ports

This list contains the UDP ports allowed by default for NetBios CIFS.
You can add ports by clicking on the appropriate button or remove them from the list by selecting them and clicking on “Delete”.

NetBios CIFS over SSL: list of default TCP ports

This list contains the TCP ports using SSL allowed by default for the NetBios CIFS protocol.
You can add ports by clicking on the appropriate button or remove them from the list by selecting them and clicking on “Delete”.

NetBios SSN

The screens are the same as for the previous protocol, except that they allow configuring the NetBios SSN protocol, making it possible to exchange messages in connected mode.

MGCP

Profiles screen

"IPS" tab

Automatically detect and inspect the protocol	If this protocol has been enabled, it will automatically be used for discovering corresponding packets in filter rules. This option is not available for IP, ICMP TCPUDP, RTP, RTCP, MSN, and YMSG.

MGCP session parameters

Maximum command size (bytes)	A command can contain between 32 and 1024 bytes.
Max no. of parameters per command	The number of parameters that can appear in a command has to be between 32 and 1024 bytes.
Maximum SDP parameter size (bytes)	The SDP parameter automatically validates the launch of applications in a session from the client's *www* or by mail. Its size has to be between 32 and 1024 bytes.
Maximum idle time (seconds)	The maximum idle duration for a session has to be between 60 and 604800 bytes.

Support

Disable intrusion prevention	By selecting this option, the URL filter will automatically be set to "Pass".

Global configuration screen

MGCP: list of default ports

This list contains the ports allowed by default for MGCP.
You can add ports by clicking on the appropriate button or remove them from the list by selecting them and clicking on "Delete".

RTP

"IPS" tab

List of supported RTP codecs

This list contains the RTP codecs supported by default.
You can add codecs by clicking on the appropriate button or remove them from the list by selecting them and clicking on "Delete".

Support

Disable intrusion prevention	By selecting this option, the URL filter will automatically be set to "Pass".

Log every RTP query	Enables or disables the generation of logs relating to the RTP queries.

RTCP

"IPS" tab

Allowed RTCP commands

RTCP commands can be defined in the intrusion prevention module, by clicking on **Add.** They are limited to 115 characters and can be deleted when needed.

Prohibited RTCP commands

RTCP commands can be prohibited in the intrusion prevention module, limited to 115 characters.

Support

Disable intrusion prevention	By selecting this option, the URL filter will automatically be set to "Pass".
Log every RTCP query	Enables or disables the generation of logs relating to RTCP queries.

SIP

The SIP protocol 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:
  Verification of the SIP version and the operation, validation of the URI that must 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).

Automatically detect and inspect the protocol	If this protocol has been enabled, it will automatically be used for discovering corresponding packets in filter rules. This option is not available for IP, ICMP TCPUDP, RTP, RTCP, MSN, and YMSG.

SIP Commands

Allowed SIP commands

Add	Inserts a command in the list of additional commands that require authorization.
Delete	Select the command to remove from the list and click on **Delete**.

Prohibited SIP commands

Add	Inserts a command to the list of additional prohibited commands.
Delete	Select the command to remove from the list and click on **Delete**.

Maximum size of elements (in bytes)

SIP query [64-4096]	Maximum size of the request and the response. Allows managing memory overflow.
SIP header [64-4096]	Maximum size of the header. Allows managing memory overflow.
SDP protocol [64-604800]	Maximum size of an SDP line. Allows managing memory overflow.

SIP session parameters

Max no. of pending requests [1-512]	Maximum number of requests without responses in a single SIP session.
Session timeout (seconds) [60-604800]	Duration of a SIP session in seconds.

SIP protocol extensions

Enable extension INFO (RFC2976)	The INFO extension allows exchanging information during a call in progress. **Example** The strength of a peer's Wi-Fi signal. Select this option to enable the extension.
Enable extension PRACK (RFC3262)	Two types of responses are defined by SIP: temporary and permanent. The PRACK extension allows providing a reliable recognition system and guaranteeing a sequenced delivery of temporary responses in SIP. Select this option to enable the extension.
Enable extensions SUBSCRIBE, NOTIFY (RFC3265)	The SIP protocol includes a normalized mechanism to allow any client (a telephone in VoIP being an example of a SIP client) to monitor the status of another device. If Device A client wishes to be informed of changes to the status of Device B, it will send a SUBSCRIBE request directly to Device B or to a server that is aware of Device B's status. If the SUBSCRIBE request is successful, each time Device B's status changes, Device A will receive a SIP NOTIFY, a message indicating the change in status or presenting information about the event. When one device subscribes to another, it will be informed when an event occurs. **Example** Onlining of contacts that it is looking for. Select this option to enable the extension.
Enable extension UPDATE (RFC3311)	The UPDATE extension allows a client to update session parameters even before the session has been set up, such as all media traffic and their codecs. Select this option to enable the extension.
Enable extension MESSAGE (RFC3428)	The MESSAGE extension is an extension of the SIP protocol, allowing the transfer of instant messages. Since the MESSAGE request is an extension of SIP, it inherits all the security and progress features included in this protocol. The contents of MESSAGE requests are in MIME format. Select this option to enable the extension.
Enable extension REFER (RFC3515)	The REFER extension is used in particular for the transfer or redirection of calls. If Peer A tries to contact Peer B who is not available, A will be redirected to Peer C, who will act as B's "referrer". Select this option to enable the extension.
Enable extension PUBLISH (RFC3903)	The PUBLISH extension allows publishing the status of events to a recipient. Select this option to enable the extension.
Enable support for PINT protocol	This extension allows SIP telephones to coexist with non-IP services (fax, etc.). Select this option to enable the extension.
Enable support for Microsoft Messenger (MSN)	This option allows enabling support for Microsoft Windows Messenger.

Support

Disable intrusion prevention	By selecting this option, the URL filter will automatically be set to “Pass”.
Log every SIP query	Enables or disables the logging of SIP requests.

Others

This section is dedicated to the rest of the protocols that you may encounter but which have not been covered above.
This screen is divided into five columns:

Protocol name	Name given to the protocol
Default port	The name of the port assigned by default: A new port can be created by clicking on  to the right of the column.
Default SSL port	Name of the port assigned to the default protocol.
Automatic detection	You can choose to enable or disable automatic protocol detection: As all protocols are enabled by default, double-click on the column to disable the automatic detection of the relevant protocol.
Status	You can choose to enable or disable the selected protocol. As all protocols are enabled by default, double-click on the column to disable the automatic detection of the relevant protocol. Repeat the operation when you wish to re-enable it.

Click on “Apply” to save your changes.

QUALITY OF SERVICE (QoS)

The configuration window for quality of service consists of a single screen.

Network traffic

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 for managing congestion.

Treatment when full	This option enables the definition of the congestion management algorithm, which aims to avoid slowdowns.
Default queue	This option allows selecting the default queue from the choice of defined queues. More precisely, this option allows choosing how the default traffic (which does not correspond to any queue) will be treated in relation to the rest of the traffic. By default, this traffic type has priority over traffic treated by QoS ("Top priority"), but it is possible to subject the traffic to a certain queue by selecting it from this drop-down list.

Bandwidth reservation or limitation (CBQ)

Total bandwidth	The reference value in Kbits/s or en Mbits/s allows indicating a reference on which bandwidth restrictions, indicated in percentage in the configuration of queues, will be based.

From version 9.0.1 onwards, "ACK" and "low delay" packets are now treated with a higher default priority (in order to speed up the transfer of data through limited bandwidth).

Queues

The QoS module embedded in NETASQ's intrusion prevention engine 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 the intrusion prevention engine 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 the firewall, two of which are directly associated with the QoS algorithms mentioned above – PRIQ (Priority Queuing) and CBQ (Class-Based Queuing). The third enables traffic monitoring.

Class-based queue (CBQ)

A scheduling class can be chosen for each filter rule and a bandwidth guarantee or restriction can be assigned to it.
For example: you can associate a scheduling class with HTTP traffic by associating a CBQ to the corresponding filter rule.
Class-based queuing determines the way in which traffic assigned to QoS rules will be managed on the network. Bandwidth reservation mechanisms for this queue type guarantee a minimum service while bandwidth restriction mechanisms enable the preservation of bandwidth when dealing with applications that consume a large amount of resources.

Adding a class-based queue

To add a class-based queue, click on the button **Add a queue**, then select **Class-based queue (CBQ).** A line will be added to the table in which you will be able to make your changes.

Modifying a class-based queue

Name	Name of the queue to be configured.
Type	Type of queue (from **CBQ**, **PRIQ** or **MONQ**).
Priority	Allows selecting the priority level of the traffic assigned to the queue. The cells in this column can only be edited for PRIQs. It is possible to select a value from 1 (highest priority) to 7 (lowest priority).
Minimum bandwidth	Acting as a service guarantee, this option allows guaranteeing a given throughput and a maximum transfer time. Configured in Kbits/s or as a percentage of the reference value, this value is shared between all traffic assigned to this QoS rule. As such, if HTTP and FTP traffic is associated with a queue with a guaranteed minimum of 10Kbits/s, the HTTP+FTP bandwidth will be at a minimum of 10Kbits/s. However, there is no restriction on the HTTP bandwidth being 9Kbits/s and the FTP bandwidth being only 1Kbits/s. **REMARK** This option is synchronized by default with the option **Min rev**. By modifying the value of this option, this value will be replicated in **Min rev**. By modifying the value of **Min rev**, the values will be different and therefore desynchronized.
Maximum bandwidth	Acting as a restriction, this option prohibits bandwidth for the traffic assigned to these queues from being exceeded. Configured in Kbits/s, Mbits/s, Gbit/s or as

	a percentage of the reference value, this value is shared between all traffic assigned to this QoS rule. As such, if HTTP and FTP traffic is associated with a queue with an authorized maximum of 500Kbits/s the HTTP+FTP bandwidth must not exceed 500Kbits/s. **REMARK** This option is synchronized by default with the option **Max rev**. By modifying the value of this option, this value will be replicated in **Max rev**. By modifying the value of **Max rev**, the values will be different and therefore desynchronized
Min rev.	Acting as a service guarantee, this option allows guaranteeing a given throughput and a maximum transfer time. Configured in Kbits/s or as a percentage of the reference value, this value is shared between all traffic assigned to this QoS rule. As such, if HTTP and FTP traffic is associated with a queue with a guaranteed minimum of 10Kbits/s, the HTTP+FTP bandwidth will be at a minimum of 10Kbits/s. However, there is no restriction on the HTTP bandwidth being 9Kbits/s and the FTP bandwidth being only 1Kbits/s. **REMARK** If you enter a value higher than the **Max rev.**, the following message will appear: *"downward traffic: the minimum guaranteed bandwidth should be lower than or equal to the maximum bandwidth"*.
Max rev.	Acting as a restriction, this option prohibits bandwidth for the downward traffic, assigned to these queues, from being exceeded. Configured in Kbits/s, Mbits/s, Gbit/s or as a percentage of the reference value, this value is shared between all traffic assigned to this QoS rule. As such, if HTTP and FTP traffic is associated with a queue with an authorized maximum of 500Kbits/s the HTTP+FTP bandwidth must not exceed 500Kbits/s.
Color	Color to differentiate the queue.
Comments	Related comments.

REMARK
If you select "0" in the "Minimum bandwidth" column and "Unlimited" in the "Maximum bandwidth" column, no restrictions will be placed on the traffic. In this case, a message will appear, suggesting that you change your queue to a monitoring queue.

The table in the menu **Class-based queuing** displays the various queues that have been configured. Clicking on **Check usage** allows you to view (in the browser bar on the left) the list of filter rules in which the selected queue is being used.

Deleting a class-based queue

Select the line of the class-based queue to be deleted and click on **Delete**. A message will appear asking you to confirm that you wish to delete the queue.

Monitoring queue

Monitoring queues do not affect how traffic associated with QoS rules is treated. Throughput and bandwidth information can be saved and viewed in the **Graph** tab of NETASQ EVENT REPORTER.

Configuration options for Monitoring queues are as follows:

Adding a monitoring queue

To add a monitoring queue, click on **Add a queue**, then select **Monitoring queue (MONQ).**

Modifying a monitoring queue

Name	Name of the queue to be configured.
Type	Type of queue from **CBQ**, **PRIQ** or **MONQ**).
Color	Color to differentiate the queue.
Comments	Related comments.

Deleting a monitoring queue

Select the line of the monitoring queue to be deleted and click on **Delete**. A message will appear asking you to confirm that you wish to delete the queue.

Priority queue

There are 7 priority levels and packets are treated according to the configured priorities.

High priority can be assigned to DNS queries by creating a filter rule and associating it with a PRIQ.

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 1 to 7. Priority 1 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 (it cannot be configured) – these traffic flows will be treated after all **PRIQ** queues notwithstanding other rules.

Configuration options for PRIQ queues are as follows:

Adding a priority queue

To add a class-based queue click on the button **Add a queue**, then select **Priority queue (PRIQ).**
A line will be added to the table in which you will be able to make your changes.

Modifying a priority queue

The table displays the various queues that have been configured. Clicking on **Check usage** allows you to check whether these rules are being used in a filter rule. If this is the case, a menu will appear in the browser bar, showing the rules.

Name	Name of the queue to be configured.
Type	Type of queue from **CBQ**, **PRIQ** or **MONQ**).
Priority	Defines the priority level of the traffic assigned to the queue. The cells in this column can only be edited for PRIQs. It is possible to select a value from 1 (highest priority) to 7 (lowest priority).
Color	Color to differentiate the queue.
Comments	Related comments.

Deleting a priority queue

Select the relevant line in the table of priority queues and click on **Delete**. A message will appear asking you to confirm that you wish to delete the queue.

Available queues

At the end of the queue table, the available number of queues will be indicated for a given firewall model (20 for U30 U70 models, 100 for U120, U250 and U450 models, 200 for U1100, U1500 and NG1000-A models, 255 for U6000 and NG5000-A models).

Examples of application and usage recommendations

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

Nom	Type	Priority	Bp min	Bp max	Min rev.	Max rev.	Color	Comments
Priority queue (1 item)								
QoS_DNS		**1**						**Prioritization of DNS traffic**

Using the QoS rule in the filter policy

To view QoS in the Filtering tab, in the Filtering and NAT module, double-click on the **Action** column once you have set up your filter rule (see the document on *Filtering and NAT* or go to the menu Security Policy\Filtering and NAT module\Action column).

Effects on traffic

- Decreases the number of lost packets if the rule has level 1 priority (and is the only such rule).
- Reduces latency.

Example 2: Restricting 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 rule for http

Nom	Type	Priority	Bp min	Bp max	Min rev.	Max rev.	Color	Comments
Class-based queue (1 item)								
QoS_HTTP			**0kb**	**512kb**	**0kb**	**512kb**		**Restriction on HTTP traffic**

Using the QoS rule in the filter policy

To view QoS in the Filtering tab, in the Filtering and NAT module, double-click on the **Action** column once you have set up your filter rule (see the document on *Filtering and NAT* or go to the menu Security Policy\Filtering and NAT module\Action column).

Effects on traffic

- Lowers the risk of network congestion.
- Reduces the impact of traffic on the network's overall performance.

Example 3: Guaranteeing a minimum level of 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 QoS 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 restriction for these other types of traffic.

Defining the QoS rule for VoIP

Nom	Type	Priority	Bp min	Bp max	Min rev.	Max rev.	Color	Comments
Class-based queue (1 item)								
QoS_VoIP			**1kb**	**0kb**	**100kb**	**0kb**		**Guarantee of a minimum level of service**

Using the QoS rule in the filter policy

To view QoS in the Filtering tab, in the Filtering and NAT module, double-click on the **Action** column once you have set up your filter rule (see the document on *Filtering and NAT* or go to the menu Security Policy\Filtering and NAT module\Action column).

Effects on traffic

- Guarantees bandwidth for a specified traffic type.
- Introduces a maximum data transfer time for the service.

ROUTING

Routing can be configured in two sections:

- Gateway: 2 configurations are possible here. A simple configuration in which you only need to indicate a default gateway; to use several gateways, go to advanced configuration.
  This tab therefore allows defining the default route, main and backup gateways as well as the configuration of load balancing. The **Gateway** 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 **Gateway** tab operates with a backup system.
- Static route: Enables the definition of static routes. Static routing represents a set of rules defined by the administrator as well as a default route

Both of these segments operate simultaneously, static routing having priority over all the rest during the transmission of a packet over the network.

"Gateway" tab

Default gateway (router)	The default router is generally the equipment which allows your network to access the Internet. 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. 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 those directly linked to the NETASQ Firewall. You will be able to communicate between hosts on the internal, external or DMZ networks, but not with any other network (including 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. This option may be grayed out in several main gateways have been defined.

Advanced configuration

The firewall allows distributed or balanced routing between several main gateways with fault tolerance. To select the type of distribution, select from the options below:

Load balancing	3 options are available:" A**ccording to source address** ", " **According to source and destination (connection)**", and "**No load balancing**". • A**ccording to source address:** All the routes defined in the table "List of gateways used" will be used. An algorithm allows distributing the load according to the source of the routed traffic. If too many main routes are down, the batch of backup routes will take over, on the condition that high availability has been enabled. • **According to source and destination (connection)**: This is almost the same as load balancing by source except that the load balancing algorithm also relies on the destination of the traffic. In brief, depending on the host and its connections, packets may not necessary pass through the same route. • **No load balancing**: The first route defined in the tables "list of gateways

	used" and "List of 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). **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.

With version 9.0.2, a default routing gateway has to be entered in order to allow intrusion prevention (ASQ) to send packets correctly when it desynchronizes connections.

Buttons

To add or delete routes, click on **Add** or **Delete**.

Add	Allows adding a main or backup gateway. Clicking on this button will add a line to the end of the table.
Delete	Allows deleting one or several gateways simultaneously.
Move to the list of backups/ Move to the list of main gateways	Allows moving a route from the main table to the backup table or vice versa.
Up	Allows moving the selected gateway up the table in order for it to have priority.
Down	Allows moving the selected gateway down the table in order for it to have lower priority.

Main and backup gateways

The tables for main and backup gateways contain the following columns:

Gateway (host object) (Mandatory)	Host object that uses its IP address as a route. This can be any host or dialup gateway (Firewall_<name_dialup_interface>_peer). The maximum number of main and backup gateways is 16 (8 for each). If more than one main gateway has been defined, the option **Default gateway (router)** will be disabled .
Device(s) for testing availability	Host or host group to ping in order to check the gateway's connectivity. This test works only if the option **Enable link high availability** has been selected.
Comments	Comments concerning the gateway.

Enable link high availability	When this option is selected, high availability of routes will be enabled. Example: Imagine that you have configured 5 main routes and a switchover threshold of 4. If the 4 main routes can no longer be used, the backup routes will be used. This option also allows enabling the test **Device(s) for testing availability.**
Switchover threshold	If high availability is enabled, backup gateways will only be used if the number of main gateways is lower than the minimum number of gateways defined in the field **Switchover threshold**. This number must be at least 1.

Sending the configuration

Changes made in this screen will be validated when you click on **Apply**. You must first check that the static routes are coherent before doing so.
If the configuration made in this tab shows two main gateway, the "Default gateway (router)" button in the **Gateway** tab will be grayed out.

"Static route" tab

This tab corresponds to the list of static routes, the maximum number of which varies according to the model of the appliance:

U30	U70	U120	U250	U450	U1100	U1500	U6000	NG1000-A	NG5000-A
512	512	2048	2048	2048	5120	5120	10240	5120	10240

Button bar

Search	Search that covers host, network and group objects.
Add	Adds an "empty" static route. An added route (sending of a command) is effective only if its fields **Destination network (host, network or group object)** and **Interface** have been entered.
Delete	Deletes one or several selected routes. Use the keys **Ctrl**/**Shift** + **Delete** to delete several routes.

Apply	Sends the configuration of the static routes.
Cancel	Cancels the configuration of the static routes.

Presentation of the table

The table sets out six fields of information:

Destination network (host, network or group object) (Mandatory)	Clicking on this column will open the objects database in order to select a host, network or group.
Address range	IP address or group of addresses linked to the items in the column “Destination network (host, network or group object)”.
Interface (Mandatory)	Drop-down list that allows selecting an interface from Ethernet, VLAN and dialup.
Protected	This column indicates whether the route is protected. A protected route will be added to the object “Network internal”. The behavior of the security configuration will take this parameter into account. Hosts that can be contacted via this route will be remembered in the intrusion prevention engine.
Gateway (Optional)	Clicking on this column will open the objects database in order to select a host (router).
Color (Optional)	A window will appear, allowing the selection of an interface color (used in NETASQ REALTIME MONITOR and NETASQ EVENT REPORTER).
Comments (Optional)	Any text.

SMTP FILTERING

This module consists of 2 zones:

- A zone for profiles,
- A zone for SMTP filter rules.

Profiles

The buttons in this strip allow you to configure the profiles associated with SMTP filtering.

Selecting a profile

The drop-down list offers 10 profiles, numbered from 00 to 09.
Each profile is named “Default” by default, accompanied by its number.
Examples:

- (0) Defaut00
- (1) Default01…

To select a profile, click on the arrow to the right of the field in which “Default00” is displayed by default, and select the desired profile.

Each profile is configured as follows by default:

Status	Action	Sender	Recipient (to,cc,cci)	Comments
Enabled	Pass	*@*	*@*	default rule (pass all)

Buttons

Edit	This function allows performing 3 operations on profiles: • **Rename:** by clicking on this option, a window comprising two fields will appear. It will allow you to modify the name and add comments. Once the operation has been performed, click on “Update”. This operation can also be cancelled. • **Reinitialize**: allows resetting the profile to its initial configuration, thereby deleting all changes made to the profile. • **Copy to:** This option allows copying a profile to another, with all the information from the copied profile transmitted to the receiving profile. It will also have the same name.
Last modification	This icon allows finding out the exact date and time of the last modification. Comments can also be added.

Rules

The procedure for editing an SMTP filter profile is as follows:

1 Select a profile from the list of SMTP filter profiles.

2 The table of filters will then appear as well as a screen indicating errors.

Possible operations

Add button: Inserts a line after the selected line.
Delete button: Deletes the selected line.
Up button: Places the selected line before the line just above it.
Down button: Places the selected line after the line just below it.

Table

The table contains the following columns:

Status	Status of the rule: **Enabled**, the rule is used for filtering. **Disabled**, the rule is not used for filtering. If this rule is disabled, the line will be grayed out in order to reflect this. **REMARK** The firewall will assess rules in their order of appearance on the screen: one by one from the top down. As soon as it comes across a rule that corresponds to the request, it will perform the specified action and stop there. This means that if the action specified in the rule corresponds to **Block**, all rules below it will also be set to **Block**.
Action	Allows specifying the result of the rule: **Pass** to allow sending and receiving e-mails, **Block** to prohibit them
Sender	Defines the sender of the e-mail.
Recipient (to, cc, cci)	Defines the intended recipient of the e-mail. *From version 9.0.1 onwards,* "none" can be selected as a sender.
Comments	Comments relating to the rule.

An e-mail mask may contain the following syntax:

- *: replaces a character string.

Example

*@netasq.com allows defining all e-mails from the internet domain of the company called NETASQ.

The following can also be seen:

- ?: Replaces a character.
- <none>: This value can only be obtained when the **Sender** 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 **Sender** field in this error message will be empty.

A rule with the action “Block” can be created to prevent the e-mail from being sent if the sender is unknown.

Errors found in the SMTP filter policy

The screen for editing SMTP filter rules on the firewall has a rule compliance and coherence analyzer which warns the administrator when a rule inhibits another rule or if an error has been created on one of the rules.

This analyzer shows rule creation errors and coherence errors.

Errors are displayed in the form of a list. By clicking on an error, the rule concerned will automatically be selected.

SNMP AGENT

The screen for configuring the SNMP service consists of three tabs:

- **General**: tab that is displayed by default when users click on the SNMP menu in the directory on the left and which allows enabling the module and alarm and system notifications which will be integrated into the available(lookup and sending of traps).
- **SNMPv3:** Recommended version as it is equipped with more secure tools (security tools such as authentication, encryption, timing control, etc.).
- **SNMPv1 – SNMPv2c:** Version for which the SNMP request contains a name called "Community", which is used as an ID and transmitted over the network in plaintext.

"General" tab

This tab allows configuring the system, meaning the host and its administrator. It contains notifications (alarms and system events) which will be integrated into the available MIBs.
The option **Enable the agent** allows enabling the module. It is however possible to configure the data for this screen even if the module has not been enabled.

SNMPv3 (recommended)	Enables version 3 of SNMP, the recommended version as it is equipped with more secure tools (security tools such as authentication, encryption, timing control, etc.) Since December 2002, a new standard has been introduced for SNMP, providing a significant advance in security. The configuration requires the following parameters: SNMPv3 offers authentication and encryption methods and resolves certain security issues from earlier versions.
SNMPv1/v2c	Enables versions v1/v2C of SNMP. V1 is the first version of the protocol. The only check made by this version concerns the "Community" character string. Version v2C is a version that improves the types of operations in SNMPv2p and uses "community" character string security from SNMPv1.
SNMPv1/v2c et SNMPv3	Enables all three versions of SNMP.

Configuration of MIB-II information

Location (sysLocation)	Alphanumeric information regarding the location of the monitored item. This location can be a country, city, server room, etc. *Example: France.*
Contact (sysContact)	E-mail address, telephone number, etc of the contact person in case problems arise. *Example: admin@netasq.com*

Sending of SNMP alerts (traps)

Intrusion prevention alarms	**Do not send**: by selecting this option, you will not receive ASQ alarms. By selecting **send only major alarms**, you will be able to receive major ASQ alarms. By selecting **send major and minor alarms**, major and minor ASQ alarms will be sent.
System events	**Do not send**: by selecting this option, you will not receive system alarms. By selecting **send only major alarms**, you will be able to receive major system alarms. By selecting **send major and minor alarms**, major and minor system alarms will be sent.

From version 9.0.2 onwards, SNMP can now be configured so that the name of the firewall instead of its serial number is used for SysName.

"SNMPv3" tab

The options **Enable the agent SNMPv3 (recommended)** or **SNMPv1/v2c et SNMPv3** allow enabling the SNMP v3 module.

Connection to the SNMP agent

Username	Username used for the connection and for looking up MIBs on the firewall.

Authentication

Password	Password of the user who will look up MIBs.
Algorithm	Two authentication methods are available, MD5 (hash algorithm that calculates a 128-bit digest) and SHA1 (hash algorithm that calculates a 160-bit digest). By default MD5 will be used for authentication.

Encryption (optional)

Password	SNMP packets are encrypted in DES or AES, and an encryption key can be defined. By default the authentication key will be used. **WARNING** **You are strongly advised to use a specific key**.
Algorithm	The two encryption methods possible are DES and AES. By default DES is used for encryption.

Sending of SNMPv3 alerts (traps)

Sending traps to hosts consists of 2 parts, with the list of hosts on the left and details of a selected host on the right.

List of SNMP servers

In this screen, you can configure the stations that need to contact the firewall when it needs to send an SNMP Trap (event). If no stations (hosts) are specified, the firewall will not send any messages.
A wizard will guide you through the configuration of the hosts.
By clicking to the right of a host name, the objects database will appear, allowing you to select a host.

Server [Name of destination server (object)]

The parameters in the configuration of SNMP V3 events are as follows:

Port	Port used for sending data to the host (snmptrap by default).
Username (securityName)	Name of the user allowed to send traps on the management station.
ID (engineID)	Hexadecimal string created by the management station in order to give the user a unique identification such as 0x0011223344. The engine ID has to be made up of a minimum of 5 bytes and a maximum of 32 bytes.
Security level	Several levels of security are available for the version of the SNMP protocol: • **None:** no security. The sections “Security Level: authentication” and “Security level: Encryption” are grayed out. • **Authentication, no encryption**: authentication of traps without encryption. • **Authentication and encryption**: if the encryption password is not defined, the authentication password will be used for encryption.

Authentication settings

Password	User password
Algorithm	Two authentication methods are available, MD5 (hash algorithm that calculates a 128-bit digest) and SHA1 (hash algorithm that calculates a 160-bit digest). By default MD5 will be used for authentication.

Encryption settings

Password	SNMP packets are encrypted in DES or AES, and an encryption key can be defined. By default the authentication key will be used. **WARNING** **You are strongly advised to use a specific key**.
Algorithm	The two encryption methods possible are DES and AES. By default AES is used for encryption.

“SNMPv1 - SNMPv2c” tab

The option **Enable SNMPv1/v2c** or **SNMPv1/v2c and SNMPv3** allows enabling the SNMP V1 and V2c modules.

Connection to the SNMP agent

Community	The first versions of the **SNMP** protocol are not secured. The only field necessary is the community name. By default rpv suggests the name "public". **WARNING**

We advise against using it for security reasons. If you wish to indicate several communities, separate them with commas.

Sending of SNMPv2c alerts (traps)

List of SNMP servers

Destination server (object)	Host that receives traps, (“Host” object).
Port	Port used for sending traps to this host (object type: service). By default, snmptrap.
Community	Indicates the community.

Sending of SNMPv1 alerts (traps)

By default, the list of hosts that receive V1 traps will be minimized to point the user to version V2c.

List of SNMP servers

Destination server (object)	Host that receives traps, (“Host” object).
Port	Port used for sending traps to this host (object type: service). By default, snmptrap.
Community	Indicates the community.

MIBS and Traps SNMP

The Simple Network Management Protocol (SNMP) allows you to monitor all hosts installed on your network. SNMP alerts (traps) and data listening (MIB) can be configured using the SNMP Agent module in your firewall’s web administration interface.
In this module, you will be able to configure the workstations to which the firewall has to send SNMP events and alerts (traps) or to configure access to those that gather data. This manager allows you to communicate with the SNMP agent on a firewall and to obtain, manage and monitor data from any firewall through the network. The SNMP agent authorizes read-only access to supervisors that comply with SNMP versions v1, v2c, and v3.
To configure data tracking and to receive NETASQ traps, you must first group data from NETASQ’s information base (these MIBs are available on NETASQ’s website, at the address indicated in the chapter on NETASQ MIBs). MIB data are files in text format that describe a list of SNMP objects used by the supervisor. These MIBs therefore provision data that the supervisor would need in order to interpret SNMP traps, events and query messages sent to the firewall.
The values of NETASQ MIB traps are described in the chapter below.

NETASQ SNMP event and alert (traps) format

SNMPv2-MIB traps

http://www.net-snmp.org/docs/mibs/snmpMIB.html#notifications

coldStart NOTIFICATION-TYPE

STATUS current
DESCRIPTION "A coldStart trap signifies that the SNMP entity, supporting a notification originator application, is reinitializing itself and that its configuration may have been altered."
::= { snmpTraps 1 }

warmStart NOTIFICATION-TYPE

STATUS current
DESCRIPTION "A warmStart trap signifies that the SNMP entity, supporting a notification originator application, is reinitializing itself such that its configuration is unaltered."
::= { snmpTraps 2 }

authenticationFailure NOTIFICATION-TYPE

STATUS current
DESCRIPTION "An authenticationFailure trap signifies that the SNMP entity has received a protocol message that is not properly authenticated. While all implementations of SNMP entities MAY be capable of generating this trap, the snmpEnableAuthenTraps object indicates whether this trap will be generated."
::= { snmpTraps 5 }

Traps managed by DISMAN-EVENT-MIB

To obtain the list of traps that are sent, you will need to use the MIB **DISMAN-EVENT-MIB.**
http://www.net-snmp.org/docs/mibs/dismanEventMIB.html
The tables mteTriggerTable and mteEventNotificationTable are the most useful.

Example of how to use an SNMP MIB lookup tool:
snmpwalk -v 2c -c public -M +/usr/local/share/snmp/mibs/ -m ALL 192.168.4.250 mteEventNotificationTable
....
DISMAN-EVENT-MIB::mteEventNotification."_snmpd"._linkDown' = OID: IF-MIB::linkDown
DISMAN-EVENT-MIB::mteEventNotification."_snmpd"._linkUp' = OID: IF-MIB::linkUp
....
To find out the conditions that trigger a trap, use **mteTriggerTable**
(based on IF-MIB::ifOperStatus)
...
The following are the most useful traps:
IF-MIB::linkDown
IF-MIB::linkUp

You will find the descriptions of **IF-MIB::linkDown** and **IF-MIB::linkUp** at:
http://www.net-snmp.org/docs/mibs/IF-MIB.txt

linkDown NOTIFICATION-TYPE

OBJECTS { ifIndex, ifAdminStatus, ifOperStatus }
STATUS current
DESCRIPTION "A linkDown trap signifies that the SNMP entity, acting in an agent role, has detected that the ifOperStatus object for one of its communication links is about to enter the down state from some other state (but not from the notPresent state). This other state is indicated by the included value of ifOperStatus."
::= { snmpTraps 3 }

linkUp NOTIFICATION-TYPE

OBJECTS { ifIndex, ifAdminStatus, ifOperStatus }
STATUS current

DESCRIPTION "A linkUp trap signifies that the SNMP entity, acting in an agent role, has detected that the ifOperStatus object for one of its communication links left the down state and transitioned into some other state (but not into the notPresent state). This other state is indicated by the included value of ifOperStatus."
::= { snmpTraps 4 }

ntqNotification NOTIFICATION-TYPE

OBJECTS

- ntqATime : Date of the Trap in YYYY-MM-DD HH:MM:SS format
- ntqASif : Source interface of the pakcet that had generated the Trap
- ntqASaddr : Source IP adress of the pakcet
- ntqADaddr : Destination IP adress of the pakcet
- ntqAMessage : Alarm message

STATUS current
DESCRIPTION "notification"
::= { ntqNotifications 1 }

NETASQ Traps

.1.3.6.1.4.1.11256.1.5

NETASQ traps are defined in the file **MIB NETASQ-ALARM-MIB.txt**

time	.0.1.1
srcif	.0.1.2
src	.0.1.5
dst	.0.1.6
msg	.0.1.11

time	.1.1.1
srcif	.1.1.2
src	.1.1.4
dst	.1.1.5
msg	.1.1.10

Management information bases (MIBs)

NETASQ MIBs

Here is the list if fields of NETASQ MIBs, CLI commands corresponding and console commands.
The links can be downloaded from: http://www.netasq.com/mibs-netasq

In versions 7 and 8, all of these MIBs are valid except for NETASQ-HA-MIB.

- NETASQ-SMI-MIB: Mib as a whole

- NETASQ-ALARM-MIB: Table of alarms

.1.3.6.1.4.1.11256.1.5
==> Contents of logs
Contains 2 tables :

Alarms	
time	.0.X.1
srcif	.0.X.2
dstif	.0.X.3
proto	.0.X.4
src	.0.X.5
dst	.0.X.6
srcport	.0.X.7
dstport	.0.X.8
srcname	.0.X.9
dstname	.0.X.10
msg	.0.X.11

ICMP alarms	
time	.1.X.1
srcif	.1.X.2
dstif	.1.X.3
src	.1.X.4
dst	.1.X.5
type	.1.X.6
code	.1.X.7
srcname	.1.X.8
dstname	.1.X.9
msg	.1.X.10

- NETASQ-HA-MIB: Information on high availability

.1.3.6.1.4.1.11256.1.11
==> (CLI) HA INFO
==> (console) hainfo

General informations	
NbNode	.1.0
NbDeadNode	.2.0
NbActiveNode	.3.0
NbHALinks	.5.0
NbFaultyHALinks	.6.0

Table of HA members	
FwSerial	.7.X.2
Online	.7.X.3
Model	.7.X.4

Version	.7.X.5
HALicence	.7.X.6
HAQuality	.7.X.7
HAPriority	.7.X.8
HAStatusForced	.7.X.9
HAActive	.7.X.10
Uptime	.7.X.11

- NETASQ-POLICY-MIB: Filter policy

.1.3.6.1.4.1.11256.1.8.1
==> (CLI) MONITOR POLICY
==> (console) slotinfo

Name	.X.2
Slot_Name	.X.3
Active	.X.4
Sync	.X.5

- NETASQ-AUTHUSERS-MIB: Table of authenticated users

.1.3.6.1.4.1.11256.1.2.1
==> (CLI) MONITOR USER
==> (console) sfctl -s user

IpAddr	.X.1
Timeout	.X.2
UserName :	.X.3

- NETASQ-HOSTS-MIB: Tables of protected hosts

.1.3.6.1.4.1.11256.1.3.1
==> (CLI) MONITOR HOST
==> (console) sfctl -s host

IpAddr	.X.1
Name	.X.2
Interface	.X.3
Packet	.X.4
Byte	.X.5
Curr_throughput	.X.7
Max_throughput	.X.8
InBytes	.X.9
OutBytes	.X.10
In_curr_throughput	.X.11
Out_curr_throughput	.X.12
In_max_throughput	.X.13
Out_max_throughput	.X.14

- NETASQ-PROPERTY-MIB: Information returned by the "SYSTEM PROPERTY" command

.1.3.6.1.4.1.11256.1.0
==> (CLI) SYSTEM PROPERTY, SYSTEM IDENT, SYSTEM LANGUAGE

Model	.1.0
Version	.2.0
SerialNumber	.3.0
SystemName	.4.0
SystemLanguage	.5.0
NbEther	.6.0
NbVlan	.7.0
NbDialup	.8.0
NbPPTP	.9.0
NbSerial	.10.0
NbLoopback	.11.0
Watchdog	.12.0
Led	.13.0
Clone	.14.0
HADialup	.15.0

- NETASQ-SYSTEM-MONITOR-MIB: ASQ resource usage counters

.1.3.6.1.4.1.11256.1.10
==> (CLI) MONITOR STAT

Date	.1.0
UpTime	.2.0
Mem	.3.0
StatTime	.4.0

- NETASQ-AUTOUPDATE-MIB: Status of various modules updated by Active Update

.1.3.6.1.4.1.11256.1.9.1
==> (CLI) MONITOR AUTOUPDATE

System	.X.2
State	.X.3
Date	.X.4

- NETASQ-IF-MIB: Status of interfaces seen by ASQ

.1.3.6.1.4.1.11256.1.4.1
==> (CLI) MONITOR INTERFACE

IfName	.X.2
Name	.X.3
Addr	.X.4

Mask	.X.5
Type	.X.6
Color	.X.7
MacThroughput	.X.8
CurThroughput	.X.9
MaxThroughput	.X.10
PktAccepted	.X.11
PktBlocked	.X.12
PktFragmented	.X.13
PktTcp	.X.14
PktUdp	.X.15
PktIcmp	.X.16
TotalBytes	.X.17
TcpBytes	.X.18
UdpBytes	.X.19
IcmpBytes	.X.20
TcpConn	.X.21
UdpConn	.X.22
TcpConnCount	.X.23
UdpConnCount	.X.24
InCurThroughput	.X.25
OutCurThroughput	.X.26
InMaxThroughput	.X.27
OutMaxThroughput	.X.28
InTotalBytes	.X.29
OutTotalBytes	.X.30
InTcpBytes	.X.31
OutTcpBytes	.X.32
InUdpBytes	.X.33
OutUdpBytes	.X.34
InIcmpBytes	.X.35
OutIcmpBytes	.X.36
Protected	.X.37

- NETASQ-SERVICES-MIB: Status of firmware services

.1.3.6.1.4.1.11256.1.7.1
==> (CLI) MONITOR SERVICE
==> (console) dstat

Name	.X.2
State	.X.3
UpTime	.X.4

- NETASQ-VPNSA-MIB: Table of negotiated IPSEC SA

.1.3.6.1.4.1.11256.1.1.1
==> (CLI) MONITOR GETSA
==> (console) showSAD

SAIndex	.X.1
IPSrc	.X.2
IPDst	.X.3
Type	.X.4
Mode	.X.5
SPI	.X.6
PeerSPI	.X.7
ReqID	.X.8
Enc	.X.9
Auth	.X.10
State	.X.11
LifeTime	.X.12
Bytes	.X.13
MaxLifeTime	.X.14
MaxBytes	.X.15

MIBs

You will find the links for accessing various MIBs.
The SNMP agent only supports listed fields and sub-sets.

SNMPv2-MIB

mibfile=**http://www.net-snmp.org/docs/mibs/SNMPv2-MIB.txt**
desc=**http://www.net-snmp.org/docs/mibs/snmpMIB.html**
rfc=**http://www.ietf.org/rfc/rfc3418.txt**

system.*.0
sysORTable
snmp.*.0
setSerialNo.0

SNMP-FRAMEWORK-MIB

mibfile=**http://www.net-snmp.org/docs/mibs/SNMP-FRAMEWORK-MIB.txt**
desc=**http://www.net-snmp.org/docs/mibs/snmpFrameworkMIB.html**
rfc=**http://www.ietf.org/rfc/rfc3411.txt**

snmpEngine.*.0

SNMP-TARGET-MIB

mibfile=**http://www.net-snmp.org/docs/mibs/SNMP-TARGET-MIB.txt**
desc=**http://www.net-snmp.org/docs/mibs/snmpTargetMIB.html**
rfc=**http://www.ietf.org/rfc/rfc3413.txt**

snmpTargetSpinLock.0
snmpTargetAddrTable
snmpTargetParamsTable
snmpUnavailableContexts.0
snmpUnknownContexts.0

SNMP-NOTIFICATION-MIB

mibfile=**http://www.net-snmp.org/docs/mibs/SNMP-NOTIFICATION-MIB.txt**
desc=**http://www.net-snmp.org/docs/mibs/snmpNotificationMIB.html**
rfc=**http://www.ietf.org/rfc/rfc3413.txt**

snmpNotifyTable
snmpNotifyFilterProfileTable
snmpNotifyFilterTable
nlmConfig.*.0
nlmStats.*.0

NOTIFICATION-LOG-MIB

mibfile=**http://www.net-snmp.org/docs/mibs/NOTIFICATION-LOG-MIB.txt**
desc=**http://www.net-snmp.org/docs/mibs/notificationLogMIB.html**
rfc=**http://www.ietf.org/rfc/rfc3014.txt**

SNMP-USER-BASED-SM-MIB

mibfile=**http://www.net-snmp.org/docs/mibs/SNMP-USER-BASED-SM-MIB.txt**
desc=**http://www.net-snmp.org/docs/mibs/snmpUsmMIB.html**
rfc=**http://www.ietf.org/rfc/rfc3414.txt**

usmStats.*.0
usmUserTable

SNMP-VIEW-BASED-ACM-MIB

mibfile=**http://www.net-snmp.org/docs/mibs/SNMP-VIEW-BASED-ACM-MIB.txt**
desc=**http://www.net-snmp.org/docs/mibs/snmpVacmMIB.html**
rfc=**http://www.ietf.org/rfc/rfc3415.txt**

vacmContextTable
vacmSecurityToGroupTable
vacmAccessContextTable
vacmViewSpinLock.0
vacmViewTreeFamilyTable

SNMP-USM-DH-OBJECTS-MIB

mibfile=**http://www.net-snmp.org/docs/mibs/SNMP-USM-DH-OBJECTS-MIB.txt**
desc=**http://www.net-snmp.org/docs/mibs/snmpUsmDHObjectsMIB.html**
rfc=**http://www.ietf.org/rfc/rfc2786.txt**

usmDHPublicObjects.*.0
usmDHUserKeyTable

IF-MIB

mibfile=**http://www.net-snmp.org/docs/mibs/IP-MIB.txt**
desc=**http://www.net-snmp.org/docs/mibs/ip.html**
rfc=**http://www.ietf.org/rfc/rfc4293.txt**

ifNumber.0
ifTable
ifXTable

RFC1213-MIB

mibfile=**http://www.net-snmp.org/docs/mibs/RFC1213-MIB.txt**

rfc=**http://www.ietf.org/rfc/rfc1213.txt**

atTable

IP-MIB

mibfile=**http://www.net-snmp.org/docs/mibs/IP-MIB.txt**
desc=**http://www.net-snmp.org/docs/mibs/ip.html**
rfc=**http://www.ietf.org/rfc/rfc4293.txt**

ip.*.0
icmp.*.0

ipAddrTable
ipRouteTable
ipNetToMediaTable
ipNetToPhysicalTable

IPV6-MIB

mibfile=**http://www.net-snmp.org/docs/mibs/IPV6-MIB.txt**
desc=**http://www.net-snmp.org/docs/mibs/ipv6MIB.html**
rfc=**http://www.ietf.org/rfc/rfc2465.txt**

ipv6MIBObjects.?.0
ipv6Interfaces
ipv6IfTable
ipv6IfStatsTable

IPV6-TCP-MIB

mibfile=**http://www.net-snmp.org/docs/mibs/IPV6-MIB.txt**
desc=**http://www.net-snmp.org/docs/mibs/ipv6TcpMIB.html**
rfc=**http://www.ietf.org/rfc/rfc2452.txt**

ipv6TcpConnTable

IPV6-UDP-MIB

mibfile=**http://www.net-snmp.org/docs/mibs/IPV6-UDP-MIB.txt**
desc=**http://www.net-snmp.org/docs/mibs/ipv6UdpMIB.html**
rfc=**http://www.ietf.org/rfc/rfc2465.txt**

ipv6UdpTable

IPV6-ICMP-MIB

mibfile=**http://www.net-snmp.org/docs/mibs/IPV6-ICMP-MIB.txt**
desc=**http://www.net-snmp.org/docs/mibs/ipv6IcmpMIB.html**
rfc=**http://www.ietf.org/rfc/rfc2466.txt**

ipv6IfIcmpTable

TCP-MIB

mibfile=**http://www.net-snmp.org/docs/mibs/TCP-MIB.txt**
desc=**http://www.net-snmp.org/docs/mibs/tcp.html**
rfc=**http://www.ietf.org/rfc/rfc4022.txt**

tcp.*.0
tcpConnTable

UDP-MIB

mibfile=**http://www.net-snmp.org/docs/mibs/UDP-MIB.txt**
desc=**http://www.net-snmp.org/docs/mibs/udp.html**
rfc=**http://www.ietf.org/rfc/rfc4113.txt**

udp.*.0
udpTable

IF-INVERTED-STACK-MIB

mibfile=**http://www.net-snmp.org/docs/mibs/IF-INVERTED-STACK-MIB.txt**
desc=**http://www.net-snmp.org/docs/mibs/ifInvertedStackMIB.html**
rfc=**http://www.ietf.org/rfc/rfc2864.txt**

HOST-RESOURCES-MIB

mibfile=**http://www.net-snmp.org/docs/mibs/HOST-RESOURCES-MIB.txt**
desc=**http://www.net-snmp.org/docs/mibs/host.html**
rfc=**http://www.ietf.org/rfc/rfc2790.txt**

hrSystem.*.0
hrMemorySize
hrStorageTable
hrDeviceTable
hrProcessorTable
hrNetworkTable
hrPrinterTable
hrDiskStorageTable
hrPartitionTable
hrFSTable
hrSWRunTable
hrSWRunPerfTable
hrSWInstalled.*.0
hrSWInstalledTable

DISMAN-EVENT-MIB

mibfile=**http://www.net-snmp.org/docs/mibs/DISMAN-EVENT-MIB.txt**
desc=**http://www.net-snmp.org/docs/mibs/dismanEventMIB.html**
rfc=**http://www.ietf.org/rfc/rfc2981.txt**

mteTriggerTable
mteTriggerDeltaTable
mteTriggerExistenceTable
mteTriggerBooleanTable
mteTriggerThresholdTable
mteObjectsTable
mteEventTable
mteEventNotificationTable

DISMAN-SCHEDULE-MIB

mibfile=**http://www.net-snmp.org/docs/mibs/DISMAN-SCHEDULE-MIB.txt**
desc=**http://www.net-snmp.org/docs/mibs/schedMIB.html**
rfc=**http://www.ietf.org/rfc/rfc3231.txt**

schedLocalTime.0
schedTable

AGENTX-MIB

mibfile=**http://www.net-snmp.org/docs/mibs/AGENTX-MIB.txt**
desc=**http://www.net-snmp.org/docs/mibs/agentxMIB.html**
rfc=**http://www.ietf.org/rfc/rfc2742.txt**

NET-SNMP-AGENT-MIB

mibfile=**http://www.net-snmp.org/docs/mibs/NET-SNMP-AGENT-MIB.txt**
desc=**http://www.net-snmp.org/docs/mibs/netSnmpAgentMIB.html**

nsModuleTable
nsCacheTable
nsConfigDebug.*.0
nsDebugTokenTable
nsConfigLogging
nsLoggingTable
netSnmpExampleScalars
netSnmpIETFWGTable
netSnmpHostsTable
nstAgentModules

NET-SNMP-VACM-MIB

mibfile=**http://www.net-snmp.org/docs/mibs/NET-SNMP-VACM-MIB.txt**
desc=**http://www.net-snmp.org/docs/mibs/netSnmpVacmMIB.html**

nsVacmAccessTable

UCD-DISKIO-MIB

mibfile=**http://www.net-snmp.org/docs/mibs/UCD-DISKIO-MIB.txt**
desc=**http://www.net-snmp.org/docs/mibs/ucdDiskIOMIB.html**

UCD-DLMOD-MIB

mibfile=**http://www.net-snmp.org/docs/mibs/ucdDlmodMIB.html**
desc=**http://www.net-snmp.org/docs/mibs/ucdDlmodMIB.html**

SCTP-MIB

mibfile=**http://www.net-snmp.org/docs/mibs/SCTP-MIB.txt**
desc=**http://www.net-snmp.org/docs/mibs/sctpMIB.html**
rfc=**http://www.ietf.org/rfc/rfc3873.txt**

sctpStats
sctpParameters
sctpAssocTable
sctpAssocLocalAddrTable
sctpAssocRemAddrTable
sctpLookupLocalPortTable
sctpLookupRemPortTable
sctpLookupRemHostNameTable
sctpLookupRemPrimIPAddrTable
sctpLookupRemIPAddrTable

SSL FILTERING

SSL filtering is now integrated into the new security policy on NETASQ multi-function firewalls. This module allows filtering access to secure web sites. It also makes it possible to allow or prohibit web sites or certificates that pose risks.

This module consists of 2 zones:

- A zone for profiles,
- A zone for SSL filter rules.

Profiles

The buttons in this strip allow you to configure the profiles associated with SSL filtering.

Selecting a profile

The drop-down list offers 10 profiles, numbered from 00 to 09.
Each profile is named “Default” by default, accompanied by its number.
Examples:

- (0) Defaut00
- (1) Default01…

To select a profile, click on the arrow to the right of the field in which “Default00” is displayed by default, and select the desired profile.
Each profile is configured as follows by default:

Status	Action	URL-CN	Comments
Enabled	Pass without decrypting	any	default rule (decrypt all)

Buttons

Edit	This function allows performing 3 operations on profiles: • **Rename:** by clicking on this option, a window comprising two fields will appear. It will allow you to modify the name and add comments. Once the operation has been performed, click on “Update”. This operation can also be cancelled. • **Reinitialize**: allows resetting the profile to its initial configuration, thereby deleting all changes made to the profile. • **Copy to:** This option allows copying a profile to another, with all the information from the copied profile transmitted to the receiving profile. It will also have the same name.
Last modification	This icon allows finding out the exact date and time of the last modification. Comments can also be added.

Rules

The procedure for editing an SSL filter profile is as follows:

1 Select a profile from the list of SSL filter profiles.

2 The table of filters will then appear as well as a screen indicating errors.

Possible operations

Add button: Inserts a line after the selected line.
Delete button: Deletes the selected line.
Up button: Places the selected line before the line just above it.
Down button: Places the selected line after the line just below it.

Table

The table contains the following columns:

Status	Status of the rule: **Enabled**, the rule is used for filtering. **Disabled**, the rule is not used for filtering. If this rule is disabled, the line will be grayed out in order to reflect this. **REMARK** The firewall will assess rules in their order of appearance on the screen: one by one from the top down. As soon as it comes across a rule that corresponds to the request, it will perform the specified action and stop there. This means that if the action specified in the rule corresponds to **Block**, all rules below it will also be set to **Block**.
Action	Allows specifying the operation to perform: If **Pass without decrypting** is specified, access to the requested CN will be allowed without a prior SSL scan. If **Block without decrypting** is specified, access to the requested CN will be denied, without any SSL scan being applied. The connection will be shut down. If **Decrypt** is specified, the protocol scan will be applied to the decrypted traffic, as well as on the proxy, if a rule has been created for it.
URL-CN	This action applies according to the value of this column. It may contain a group or URL category, as well as a group of certificate names.
Comments	Comments relating to the rule.

Errors found in the SSL filter policy

The screen for editing SSL filter rules on the firewall has a rule compliance and coherence analyzer which warns the administrator when a rule inhibits another rule or if an error has been created on one of the rules.
This analyzer shows rule creation errors and coherence errors.
Errors are displayed in the form of a list. By clicking on an error, the rule concerned will automatically be selected.

NETASQ'S SSL VPN allows your mobile or static users to connect to your company's resources securely.
The SSL VPN configuration screen consists of 4 tabs:

- **General**: Allows enabling the module, selecting the access type and configuring advanced properties.
- **Web servers**: NETASQ'S SSL VPN allows securing access to your HTTP servers (Intranet, webmail,…) while avoiding the need to manage multiple HTTP servers. Furthermore, for mobile users, it allows masking information about your internal network, the only visible IP address being your firewall's.

  NETASQ'S SSL VPN automatically rewrites HTTP links found in web pages that your users visit. This allows browsing between your various servers, if they have been configured, or prohibiting access to certain servers. When a web link in a page points to an unconfigured server, the link will be redirected to the NETASQ SSL VPN start page.
- **Application servers:** This section shows the servers that have been configured for access to resources other than web-based resources (telnet, mail, etc)

  NETASQ's SSL VPN enables securing any protocol based on a single TCP connection (POP3, SMTP, telnet, 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.

  NETASQ'S SSL VPN does not impose any client installations on your users' workstations and natively supports operating systems that have Java installed (Windows, Linux, MAC OS-X,…).

  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. These can be used for control purposes and/or transparent authentications on the source of requests.
- **User profiles**: If you wish to restrict access to servers defined in the SSL VPN configuration, you need to define profiles that contain the list of authorized servers, then assign them to users.

"General" tab

Enable SSL VPN: Allows enabling SSL VPN and choosing from three options offers in the table below.

Access only to web servers	Use of the SSL VPN module to access web-based resources. Enables the Web servers tab.
Access only to application servers	Use of the SSL VPN module to access resources on a TCP connection. Enables the Application servers tab.

Access to both web and application servers	Use of the SSL VPN module to access web-based and TCP-based resources. Enables both the Web servers and Application servers tabs.

Advanced properties

Authenticate user upon each request (authentication by SSL certificate only)	If the option **Authenticate user upon each request (authentication by SSL certificate only)** 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.

Access to servers via SSL VPN

Prefix for the URL root directory	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 for user ID	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 workstation configuration

Command executed at startup	This command, which is executed 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.
Command executed during shutdown	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.

"Web servers" tab

This section groups the servers configured for access to web resources.

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, NG1000-A	256	128
U6000, NG5000-A	512	256

Adding a web server

To add a web access server, the procedure is as follows:

1. Click on **Add** then select one of the suggested servers. A screen containing server names will appear.
2. Enter a name for this server. (The field can be left empty. Allowed characters: numbers, letters, spaces, -, _, and dots.)
3. This server's configuration then appears. The different parameters are explained below.

Destination 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 **FQDN** name of the 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: access path	This URL enables going directly to the specified page.
URL used by SSL VPN	Link calculated based on 3 fields: **Destination server**, **Port** and **URL: access path**. (Example: http://destination server/URL: access path).
Name of the link on the user 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.

Advanced properties

Enable URL 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 not be accessible via SSL VPN. If the white list has been activated, it will enable access to URLs which have not been rewritten through the field **Do not rewrite URLs in the group.**. 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 "*". **WARNING** If the user clicks on a link in the whitelist, it will no longer be protected by the NETASQ SSL VPN module.
Don't show this server on the user portal (access via another server only)	All servers configured in SSL VPN are listed on the NETASQ authentication portal by default. However, it may be necessary for servers to be accessible only through another server, so in this case, the option **Don't show this server on the user 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.
Deactivate NTLM	Some web servers may request authentication before the transfer of data between the server and the user. This method can be disabled for servers that do not support this authentication method for traffic passing through the firewall.
Rewrite \"User-Agent\" field (force OWA compatibility mode)	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 on 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 automatically operates in basic mode when it encounters the "User-Agent" on these browsers.
Rewrite OWA Premium mode specific code	If this option has been selected, you will enable the specific rewriting rules that allow supporting Outlook Web Access in premium mode.

From version 9.0.3 onwards, Lotus Domino Web Access version 7.0.4 now runs through SSL VPN tunnels. Therefore, it is no longer necessary to enable the specific rewriting rules that allow supporting Lotus domino web applications.

Alternative URLs for this server (alias)

Server alias	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 **Add** will display a line that will allow you to add a new alias.

Adding an OWA web server

The **SSL VPN** module on NETASQ firewalls supports OWA (Outlook Web Access) Exchange 2003, 2007 and 2010 servers.

“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, such as “http://www.netasq.com/index.htm”.

It is therefore possible to add HTTP servers (with specific preset options for perfect compatibility with OWA) to the list of web-access servers.

To add an HTTP server-OWA, the procedure is as follows:

1. Click on **Add** then select OWA Web server 2003 (Premium mode) or OWA Web server 2007 – 2010 (premium mode)**.**
2. Enter a name for this server. (The field can be left empty. Allowed characters: numbers, letters, spaces, -, _, and dots.)
3. The preset options for an OWA 2003 premium server are: HTTP port, the field **URL: access path** with "exchange" indicated, the field **Enable URL whitelist** enabled, the field **Do not rewrite URLs in the group** with the URL group “vpnssl_owa” indicated, the field **Deactivate NTLM** and the field **Rewrite OWA Premium mode specific code**.

For an OWA 2007-2010 server, the pre-entered fields are: HTTP port, the field **URL: access path** with "owa" indicated, the field **Enable URL whitelist** with the URL group “vpnssl_owa” indicated, and the field **Rewrite OWA Premium mode specific code**.
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 web server

The **SSL VPN** module on NETASQ firewalls supports Lotus domino servers.

An HTTP server can be added to the list of web access servers with certain options specifically pre-entered for compatibility with Lotus Domino.

The procedure for adding an HTTP-Lotus Domino server is as follows:

1. Click on **Add** then select **Lotus Domino web server**.
2. Enter a name for this server. (The field can be left empty. Allowed characters: numbers, letters, spaces, -, _, and dots.)

The following field is pre-entered option for Lotus domino servers: “http” port

---

From version 9.0.3 onwards, Lotus Domino Web Access version 7.0.4 now runs through SSL VPN tunnels, without having to enable the compatibility option « Rewrite Lotus Domino specific code ».

"Application servers" tab

Configuration with an application server

The procedure for adding a server to access resources other than web-based resources is as follows:

1 Click on **Add** then select **Application server.**

2 Enter a name for this server. (The field can be left empty. Allowed characters: numbers, letters, spaces, -, _, and dots.)

3 This server's configuration then appears. The different parameters are explained below.

Destination server	This field allows specifying the object corresponding to the server that the user will be able to access.
Port	The port on the server accessible to the user can be specified in this field.

User workstation settings

Listening IP address (local)	Local address of the client.
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 privileges 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.

Advanced properties

Enable 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.
Command executed at startup	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.

Configuration with a Citrix server

1 Step 1: Creating an object for the Citrix server
Go to the object database in order to create a host and select a host.

2 Step 2: Configuring an application server
In the SSL VPN module, select the tab Application servers. Click on **Add** then select Citrix server. Give your server a name. The Citrix configuration screen will then appear.

Select the Citrix server created earlier in the objects database. *(Cf. Step1)*

3 Step 3: Configuring a web server
Select the tab Web servers.

Click on **Add** then select "web server ". Enter a name for the server. The web server configuration window will then appear:

As for the URL: access path, indicate CitrixAccess/auth/login.aspx (if it is the version Presentation Server 4.0).

4 Sending the configuration

Click on **Apply**.

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.
Next, select **Portal access\Portal** then enter your username, password and domain.

Deleting a server

To delete a server, the procedure is as follows:

1 Select the server to remove

2 Click on **Delete**.

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.

"User profiles" tab

Operating principle

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

The procedure for adding a profile to the list of available SSL VPN profiles is as follows:

1 Click on **Add**, then specify the name of the profile.

2 From the list of "Accessible web servers" and "Accessible application servers", select the servers that will be accessible to users that belong to this profile.

3 Click on **Apply** 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. Create a profile in SSL VPN\User profiles,
2. Define the profile to be used as the default profile (name of the profile and associated servers) in the configuration menu Users\Access privileges \Default options \SSL VPN.

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 specific profile (name of the profile and associated servers) in User profiles in the SSL VPN module, then click on **Apply** to apply the changes.
2. In the module Users\Access privileges\User configuration, select the user from the “SSL VPN” column, select the profile defined earlier and click on **Apply**.

SSL VPN services on the NETASQ web portal

When authentication is enabled on the firewall (module Users\Authentication\General, select “Enable the captive portal”), the NETASQ you will be able 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; you need to log in.
4. If the you have the privileges to use VPN features, the **Secure access** menu will appear, enabling access to SSL VPN features.

From version 9.0.1 onwards, when the authentication duration expires or access to the SSL VPN is denied, the user will be redirected to the transparent authentication page (SSO) if this method is available.

Accessing your company'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 other methods of secure access enable accessing other secure sites configured by the administrator.

Accessing your company'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 on the NETASQ web portal page.

SYSTEM EVENTS

In this module, you will be able to define in your configurations the alarm level of the various system events that may occur (attacks, update failures, invalid CRLs, etc).
It consists of a single screen, listing events by number and in alphabetical order, with the possibility of searching for a particular event.

Possible actions

There are two actions you can perform in this section.

Search

This field allows you to search by occurrence, letter or word. You can as such filter elements in the list in order to view only those you need.

Example

If you enter “CRL” in the field, all messages containing this term will be displayed in the table.

Restore the default configuration

This button will allow you to cancel all changes you have made earlier in the system event configuration.
When you click on this button, a confirmation message will appear, allowing you to confirm or cancel the action.

List of events

The screen consists of three columns, as well as a help page at the end of the line for each event type.

ID	This field shows the number that identifies the event. It cannot be edited.
Level	This column shows the default alarm levels assigned to events. There are 4 levels, which you can modify by selecting the desired level from the drop-down list. This list appears when you click on the downward arrow on the right: **Ignore**: No logs on the event will be kept. **Minor:** As soon as the event concerned occurs, a minor alarm will be generated. This alarm is reported in the logs and can be sent by Syslog, (section Logs - Syslog) or by e-mail (see the module E-mail alerts). **Major:** As soon as the event concerned occurs, a major alarm will be generated. This alarm is reported in the logs and can be sent by Syslog, (section Logs - Syslog) or by e-mail (see the module E-mail alerts). **Log:** The NETASQ firewall does not do anything. This is useful when you wish to log only certain types of traffic without applying any particular action.
Message (language depends on	This field shows the name of the system event and its characteristics (cannot be edited).

the firewall language)	**NOTE** By clicking on the arrow on the right side of the column header, you can invert the order in which events appear.
Show help	When you select an event from the list by clicking on it, a “Show help” link appears. Clicking on this link will take you to the NETASQ knowledge base, providing more details on the information relating to the event.

GENERAL NOTE
When you modify the alarm level of an event, don’t forget to click on “Apply” at the bottom of the page, in order to confirm your action.

TIME OBJECTS

The Time objects module consists of two screens:
- On the left: an area for creating time objects.
- On the right: an area displaying the details of the created objects.

Possible actions

Add	Two types of time objects can be created: **Add a fixed event**: This type of event has a limited duration – it has a start date and an end date. It will be named "**fixed_event**" in the list before another name is given to it. **Add a periodic event:** This type of event is not time-limited – it may arise everyday and have a time slot. No end date is defined. It will be named "**recurring_event**" in the list before another name is given to it.
Delete	Select the event to be removed from the list and click on **Delete**.
Check usage	If you click on this button after having selected an event, the results will appear in the module directory. You can also find existing time objects by going to the "Objects" area in the module directory and going to either the keyword search bar to look for them or by clicking on the icon  and selecting "Time objects" from the drop-down list that appears.
Copy	Select an existing object and click on this button. It will be named <name of event_type of event_0).
Name	You cannot change the name of your object in this column. First, select it and define it in the screen on the right, dedicated to event details *(see next section).*
Comments	You cannot include a description of the object in this column. First, select it and define it in the screen on the right, dedicated to event details *(see next section).*
Advanced configuration	This button allows you to add options to the selected time object: **Fixed event** **Day of the year** **Day of the week** **Time slot** The selected options will appear in your screen on the right.

Information regarding objects

By default, the weekly event is described as taking place *"from Monday to Friday. From 9 a.m. to 5 p.m."*
The fixed event is described by default as taking place *"from <date> to <date> at <time>. Every week from Monday to Friday"* at a specified time.
The annual event is described by default as taking place on *1 January from 9 a.m. to 5 p.m.*

Fixed event

This field allows defining “From” when the event takes place and until when it will continue. A day has to be defined from the calendar presented.
You will also need to define a time by entering the empty “to” field.

Day of the year

By default, this field indicates the date 01: 01. You can click on **Add a date range** and enter a start date and an end date for your event, by selecting the month and the day.

Day(s) of the week

The days affected by the event are marked with this icon . If you wish to remove a day, click once on it. If you wish to apply an additional day, such as a Saturday, for example, click once on the checkbox “Sat”. It will then be marked by the same icon described above and your event will affect this day.

Time slots

You can define time slots using these buttons:

Add a time slot, to add a time slot and to define the start and end time of your event.

To delete it.
New information regarding the time slot(s) will appear in the field **Description**.

URL FILTERING

This module consists of 2 zones:

- A zone for profiles,
- A zone for URL filter rules.

Profiles

The buttons in this strip allow you to configure the profiles associated with URL filtering.

Selecting a profile

The drop-down list offers 10 profiles, numbered from 00 to 09.
Each profile is named “Default” by default, accompanied by its number.
Examples:

- (0) Defaut00
- (1) Default01…

To select a profile, click on the arrow to the right of the field in which “Default00” is displayed by default, and select the desired profile.
Each profile is configured as follows by default:

Status	Action	URL group	Comments
Enabled	Passer	any	default rule (pass all)

Buttons

Edit	This function allows performing 3 operations on profiles: • **Rename:** by clicking on this option, a window comprising two fields will appear. It will allow you to modify the name and add comments. Once the operation has been performed, click on “Update”. This operation can also be cancelled. • **Reinitialize**: allows resetting the profile to its initial configuration, thereby deleting all changes made to the profile. The profile becomes “active” again thanks to the **Pass** action applied to all URL groups. • **Copy to:** This option allows copying a profile to another, with all the information from the copied profile transmitted to the receiving profile. It will also have the same name.
Last modification	This icon allows finding out the exact date and time of the last modification. Comments can also be added.

Rules

The procedure for editing a URL filter profile is as follows:

1 Select a profile from the list of URL filter profiles.

2 The table of filters will then appear as well as a screen indicating errors.

Possible operations

Add button: Inserts a line after the selected line.
Delete button: Deletes the selected line.
Up button: Places the selected line before the line just above it.
Down button: Places the selected line after the line just below it.

Table

The table contains the following columns:

Status	Status of the rule: ● **Enabled**, the rule will be active when this filter policy is selected. ● **Disabled**, the rule will not be operational. The line will be grayed out in order to reflect this. **REMARK** The firewall will assess rules in their order of appearance on the screen: one by one from the top down. As soon as it comes across a rule that corresponds to the request, it will perform the specified action and stop there. This means that if the action specified in the rule corresponds to **Block**, all rules below it will also be set to **Block**.
URL group	The name of a URL group created earlier. By clicking on this field, a drop-down list will prompt you to select a URL group, taken from the objects database. The group <Any> corresponds to any URL, even if it does not belong to any URL group.
Action	Allows specifying the result of the rule: **Pass** to allow the site, **Block** to prohibit access and directly shut down the connection without displaying a block message, **Redirect to the block page** to prohibit access and display the block page.
Comments	Comments relating to the rule.

REMARK
Dragging and dropping only applies to URL groups here.

From version 9.0.1 onwards, the characters “[ ]” and “{}” are no longer allowed in URLs (Internet Explorer 7 and 8).

Errors detected

The screen for editing URL filter rules on the firewall has a rule compliance and coherence analyzer which warns the administrator when a rule inhibits another rule or if an error has been created on one of the rules.
This analyzer shows rule creation errors and coherence errors.
Errors are displayed in the form of a list. By clicking on an error, the rule concerned will automatically be selected.

USERS

The user authentication service requires the creation of user accounts at the firewall level. To access the features of this module, you must first create or configure your LDAP base (see document *Directory configuration* or module Users\Directory configuration).
The accounts contain all the information relating to these users:

- ID
- Last name
- First name
- E-mail address (optional)
- Phone number (optional)
- Description (optional)

The Users screen consists of 2 parts:

- A banner showing the various options
- The list of **CNs** (or users) in the left column, accompanied by information about them in the right column.

Possible operations

Search bar

Enter the name of the particular user or user group you are looking for.
The search field will list all users and/or user groups with first names, last names and/or logins that correspond to the keywords entered.
Example:
If you type “a” in the search bar, the list below it will show all users and/or user groups with first names and/or last names containing an “a”.

Filter

This button allows you to select the type of CN to display. A drop-down menu will offer the following choices:

Groups and users	Represented by the icon, this option allows displaying all users and user groups in the list of CNs on the left.
Users	Represented by the icon, this option allows displaying only users in the left column.
Groups	Represented by the icon, this option allows displaying only user groups in the left column.

Creating a group

The Users module allows you to enter information about the group you wish to create in the right column.

Name	Give your group a name in order to identify it in the list of CNs. **REMARK**

	You will not be able to change the name of the group after you have created it.
Description	You can provide a description of the group and modify the contents of the description whenever necessary. This field is optional but you are advised to fill it in.

CN

Filter (search bar)	You can enter a character string in order to filter the list of members, or clear the field to see the whole list.
Add	Users can be added to a group in 2 ways: When you click on **Add**, a new line will appear at the top of the table. Expand the list of existing users with the help of the arrow on the right and select the user you wish to add to the group. You can also drag and drop users by importing them from the list of CNs in the left column.
Delete	To remove a member of the group, select it and click on **Delete**. ***From version 9.0.1 onwards,*** when a user is deleted, the administrator will be prompted to revoke his certificate.

To confirm the creation of your group and to save changes made, click on **Apply**.

Creating a user

To create a user, enter at least a login and a name. To associate a certificate with this user, you will need to indicate a valid e-mail address.

ID	User's connection ID
Last name	User's last name
First name	User's first name
E-mail address	User's e-mail address. This will be useful for creating certificates.
Phone number	User's telephone number
Description	Description of the user.

REMARK
The fields "ID", "First name" and "Last name" cannot be modified after the user is created.

To confirm the creation of your user and to save changes made, click on **Apply**.

Delete

This button allows deleting a user or a group:

1 Select the user or group to be deleted.

2 Click on **Delete.** A window will appear with the message "*Delete the user <**name of user**>?*". Click on **Yes**.

Check usage

Represented by the icon , this button will show you which groups users belong to, as well as where the user or group is used in the rest of the configuration.
Example:
Filtering.

1 Select the user or group for which you wish to check usage.
2 Click on **Check usage**. The menu directory on the left will show you the user/group (via its ID) in the tab Users and groups, and displays the list of groups to which this user belongs, as well as its use in the configuration of the firewall.

List of users (CN)

If you wish to access a user's data, select the user in the list of CNs on the left. The information concerning this user will appear in the right column.

"Account" tab

Modify the password	By clicking on this link, you will be able to create the user's authentication password in a specific window, which also displays the level of security. **NOTE** To allow the user to modify his password himself, go to the menu Users\ Authentication module\Internal (or external) interfaces tab\User passwords and select the option **Users can change their passwords**.
ID (cannot be modified)	Connection ID of the selected user.
Last name (cannot be modified)	Last name of the selected user
First name (cannot be modified)	First name of the selected user
E-mail address	E-mail address of the selected user.
Phone number	Telephone number of the selected user
Description	Description of the selected user.

"Certificate" tab

This tab will allow you to manage the user's x509 certificate.
Since the PKI does not have a certificate authority by default, you will need to create one in order to manage user's certificates: go to the menu Network objects\ Certificates and PKI\ **Add\Add a root authority**.
This certificate will be useful in two cases: SSL authentication and VPN access to the firewall with a mobile IPSec client. This certificate can also be used by other applications.

"Member of these groups" tab

This tab allows including the user in one or several groups:

1 Click on **Add**, a new line will appear at the top of the table.

2 Select the arrow to the right of the field. A drop-down menu will display the list of existing groups. Click on the group of your choice. It will be added to your table.
To remove a group, select it and click on **Delete**.

VULNERABILITY MANAGEMENT

In this menu, you will be able to configure your policy for managing vulnerabilities that may appear on your network.
You can assign a detection profile to a host, network, group or address range. There are 12 pre-configured profiles by default.
The configuration of vulnerability management therefore simply consists of:

- Linking network objects to detection profiles and
- Deciding which recipients will receive vulnerability reports.

The Vulnerability management configuration screen comprises 2 zones:

- A **General configuration** zone: it contains a checkbox for enabling the module and various items for the general configuration.
- **Advanced properties:** an area for determining data lifetime and excluded objects.

General configuration

Enable application and vulnerability detection	If this option is selected, vulnerability detection will be enabled and the relevant information will be visible in NETASQ REALTIME MONITOR. **REMARK** During the update (if you have purchased the license), the Vulnerability management module will be enabled by default. Alarms will be raised according to the default configuration: monitor all vulnerabilities for all internal hosts. **WARNING** Remember to update the vulnerability database in System\Active Update. Without a database that is up to date, the service may not run correctly. Vulnerability detection relies on the analysis of network traffic. This allows detecting an application and/or a flaw, from the moment the user first uses the network.
Send simple reports to	Group of e-mail addresses to which summary reports will be sent. These reports are brief and contain a summary of the vulnerabilities by product and the hosts affected.
Send detailed reports to	Group of e-mail addresses to which comprehensive reports will be sent. Detailed reports contain a summary of vulnerabilities, as well as their detailed descriptions (family, client, possibility of remote exploitation) and a link to their references in the NETASQ knowledge base, which generally includes instructions regarding the bug fix to apply.

REMARK
E-mail address groups can be configured in the menu: Notifications\E-mail alerts\ Recipients tab.

List of monitored network objects

The list of monitored objects is displayed in the table together with the detection profiles assigned to them.

Network object (host or group – network – address range)	Selects the network object to which monitoring applies. This object will be scanned by the NETASQ Vulnerability Manager engine which will rely on the rules contained in the associated detection profile. The type of object linked to the profile can only be a host, host group, network or address range. **WARNING** The list of monitored objects will be applied in order. This means that if a network object appears several times in this list, only the first detection profile will be applied. **REMARK** Objects can be created within the column using the button on the far right of the field in a new line.
Detection profile	Allows selecting a profile to restrict the applications to be monitored. The profile can be selected in the drop-down list of the column, which appears by clicking on the arrow on the right, when you add a new line to the table. (See **Add** button below)

Several actions can be performed in this table:

Add	This button allows you to add a network object and a profile associated with this object in the list of monitored objects. By clicking on this button, a blank line will appear in the table.
Delete	Select the object-profile pair to be deleted, then click on this button. **WARNING** You will not be asked to confirm the deletion of the profile.
Up	Allows raising the priority of the association between a network object and a profile.
Down	Allows lowering the priority of the association between a network object and a profile.

Below is the list of profiles and vulnerability families that will be detected and reported:

SERVERS	CLIENT APPLICATIONS AND OPERATING SYSTEMS	CLIENTS	TOOLS
Servers: SSH Servers – HTTP Servers / Web – Database Servers – FTP Server – Mail Servers and Operating Systems **Servers – critical flaws:** SSH-Web-Apps-DB-DNS-Web Server-FTP Server-Misc-Mail Server-P2P-OS	**Client applications and operating systems (OS)** **Client applications and operating systems (OS) – critical flaws**	**Mail client**: Client, Mail (Thunderbird, Outlook, e-mail …)	**Security tools:** Antivirus, Security tools and Vulnerability scanner or Network scanner
FTP Servers		**Browsers and other web**	**Administration tools:**

		clients: web clients, RSS traffic readers	Administration client FTP, SSH etc.
Mail servers			
Web servers: web/HTTP content servers			
Database servers (SQL)			

"All known applications" profile

This profile allows assigning to an object (host, group, network or address range), the detection of all client/server and operating system vulnerabilities detected by the NETASQ Vulnerability Manager.

Advanced properties

Data lifetime (days) [1 – 30]: Duration for which data (application, vulnerability) will be kept without traffic or updates detected.

Exclusion list (unmonitored objects)

Network object (host or group – network – address range)	Once objects have been associated with their profiles, one or several objects can be excluded from the analysis. As such, regardless of the configuration of the monitored objects, the members of this exclusion list will not be monitored. Objects to be excluded can be selected in this table by clicking on **Add**.

WEB OBJECTS

This module consists of 3 tabs:

- **URL**: Allows categorizing URLs, by creating groups (examples: “shopping”, “pornography”, “videogames”). Each of these groups contains a certain number of URLs of websites which can be blocked or allowed, depending on the desired action.
- **Certificate name (CN)**: Allows recognizing certificates assigned to secure websites and operating with SSL filtering, and categorizing them by creating groups.
- **URL database**: Depending on the maintenance service subscribed, the available URL lists are updated by different providers (NETASQ or OPTENET). NETASQ’s URL lists are offered by default, when the “standard” maintenance service is subscribed.

“URL” tab

This tab provides an overview of URLs arranged by category and by group.
For a given group, e.g. “banks”, which contains the most frequently visited URLs of banks, a rule can be created in URL filtering (Security policy\URL filtering) to block access.
Therefore, when you attempt to connect to your bank’s website, a block page will appear, with an error message. (See the module Notifications\Block messages\HTTP block page).

URL group table

The URL group screen consists of 2 parts: a first part for URL groups and a second part for the URLs. When configuring these groups, you can perform the following actions:

Add a URL group	Creates a new group. By clicking on this button, a new line will appear, allowing you to indicate the name of the group and comments if necessary.
Delete	Deletes an existing group or URL. Select the line to be deleted and click on this button. The following message will appear: ”Delete group xxx ?”. If the group is in use, the message will inform you and ask you what you wish to do.
Check usage	Allows checking if the selected group is used in a configuration. When you click on this button, a panel will appear in the module directory to indicate the modules that use this group.

The table sets out the elements indicated below:

URL	Name of the URL group.
Comments	Description of the URL group.

Format

The description of this field is valid only for URLs. URL groups are not affected by format restrictions.
The URL mask may have the following syntax:

*	replaces a character string. **Example** *.netasq.com allows defining the internet domain of the company called 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 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 URL mask '*.exe' will filter executable files.

REMARK
The description of this field is valid only for URLs. URL groups are not affected by format restrictions.
However, the number of characters for a URL group is restricted to 255.

URL table (“URL group: All”)

The following actions may be carried out in the configuration of URL groups:

Add	Adds a URL to a group. First, select the group to which you wish to add a URL in the left column, then click on this button.
Remove	Deletes a URL from a group. First, select the group from which you wish to delete a URL in the left column, then click on this button.
The table contains the elements indicates below:	
URL	Name of the URL. Wildcards may be used.

REMARK
There are two types of URL groups: static (manually entered by the administrator) and dynamic URL groups (Cf. Dynamic URL filtering below).
The provider requested is the dynamic URL group provider, which is NETASQ by default.

Static URL groups depends on the web filter provider selected.
If you select another provider, you need to ensure that the active URL filter slot does not use static URL groups from the older list, as it may invalidate this configuration during and after changing the provider.

“Certificate name (CN)” tab

This screen, which contains certificate name groups, may be useful for SSL filtering (see the module Security policy\SSL filtering). It consists of 2 parts: one for groups, one for URLs.

The screen is set out like the **URL group** tab except that the list on the right contains certificate authorities (CA).

NOTE
The number of characters for CN groups is restricted to 255.

"URL database" tab

This tab allows changing the URL group provider/certificate name.

URL database	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). By default, when a "standard" maintenance service has been subscribed, NETASQ URL lists will be proposed. If you have subscribed to the maintenance service, to activate the URL filter feature on OPTENET URL lists, select "OPTENET" from the list of proposed providers. When modifying the provider, the following message will appear: "The current URL database **will be deleted**, and the database from the provider Optenet will be downloaded. In the meantime, any URL filter policy that uses a category from the current provider **will stop working**. During the migration, you are advised to apply a URL filter policy that does not need to use URL categories. Confirm change of provider?" When shutting down the URL groups menu, the appliance will apply the request and will download new URL lists through the **Active Update** module.

A frame below the drop-down list shows information concerning the URL groups of the provider currently in use.

GLOSSARY

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 Qualificatio*n)

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, i.e., 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 entrusted channels.

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, e.g., 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.

NETASQ VULNERABILITY MANAGER

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

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

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

Packet analyzer

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

Partition

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

PAT (*Port Address Translation*)

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

Peer-to-peer

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

Ping (*Packet Internet Groper*)

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

PKI (*Public Key Infrastructure*)

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

Plugin

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

Port redirection (REDIRECT)

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

Port scanning

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

PPP (*Point-to-Point Protocol*)

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

PPPoE (*Point-to-Point Protocol over Ethernet*)

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

PPTP (*Point-to-Point Tunneling Protocol*)

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

Private IP Address

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

172.16.0.0 to 172.31.255.255
192.168.0.0 to 192.168.255.255
10.0.0.0 to 10.255.255.255

Private Key

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

Protocol analysis

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

Protocols

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

Proxy

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

Proxy server

(See *Proxy*).

Public key

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

PVM (*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, i.e., in terms of availability and throughput. Network resources are as such optimized and performance is guaranteed on critical applications.

R

RADIUS (*Remote Authentication Dial-In User Service*)

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

RAID (*Redundant array of independent disks*)

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

Replay

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

RFC (*Request for Comments*)

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

Router

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

Routing protocol

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

S

SA (*Security Association*)
VPN tunnel endpoint.

SCSI (*Small computer system interface*)
Standard that defines an interface between a computer and it(s) storage peripherals, known for its reliability and performance.

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

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

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

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

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

SMTP (*Simple Mail Transfer Protocol*)
TCP/IP communication protocol used for electronic mail exchange over the internet.

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

SNMP (*Simple Network Management Protocol)*
Communication protocol that allows network administrators to manage network devices and to diagnose network incidents remotely.

SSH (*Secure Shell*)
Software providing secure logon for Windows and UNIX clients and servers.

SSL (*Secure Socket Layer*)

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

Star topology / Network

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

Stateful Inspection

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

Static quarantine

A quarantine that the administrator sets when configuring the firewall.

Symmetrical key cryptography

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

T

TCP (*Transmission Control Protocol*)

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

Throughput

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

Trace route

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

Trojan horse

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

TTL (*Time-to-Live*)

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

U

UDP (*User Datagram Protocol*)

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

Unidirectional translation (MAP)

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

URL filter

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

URL (*Uniform Resource Locator*)

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

User enrolment

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

UTM (*Unified Threat Management*)

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

V

VLAN (*Virtual Local Area Network*)

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

VPN (*Virtual Private Network*)

The interconnection of networks in a secure and transparent manner for participating applications and protocols – generally used to link private networks to each other through the internet.

VPN keep alive

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

VPN Tunnel

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

W

WAN (*Wireless Area Network*)

Local wireless network.

Wi-Fi (*Wireless Fidelity*)

Technology allowing wireless access to a network.

documentation@netasq.com