Basic Configuration

Configuration of basic NETASQ services

Last update: 13 novembre 2009 (rev. 507)

Summary

Introduction

This document has been prepared as an appendix to the document « Best Practices: Configuration solutions on NETASQ UTM appliances ». It lists the services we recommend that you implement, so as to ensure the optimal functioning of your NETASQ UTM.

We will develop items in this document that will allow building a well-based configuration so as to avoid issues relating to synchonization, or the gathering of data.

You may also visit our Knowledge Base, which contains articles dealing with issues that you might encounter. It provides quick answers to many questions and is the first step in resolving problems. Even before opening a case with NETASQ's support team, you are highly advised to visit this Knowledge Base to check if whether the issue has already been addressed in an article.

The Knowledge Base is accessible from your private client area, via the menu `Technical Support / Knowledge Base`.

Registering the UTM appliance

After receiving your NETASQ UTM, you must register it. This registration will enable you in particular to activate the license, to update firmware versions,or to read a wide variety of documents relating to NETASQ products and services.

In order to register your NETASQ product, please connect to our website www.netasq.com, in the upper menu `CLIENTS - PARTNERS`, then click on `Register your first NETASQ product`. Please ensure that you have the following information at hand before performing this action:

UTM serial number: The serial number is located on the back panel of the appliance and on the delivery note. Example: U250XA0Z0899010.

The WEB password: This password is also located on the back panel of the appliance. It is generally composed of 8 alphanumeric characters.

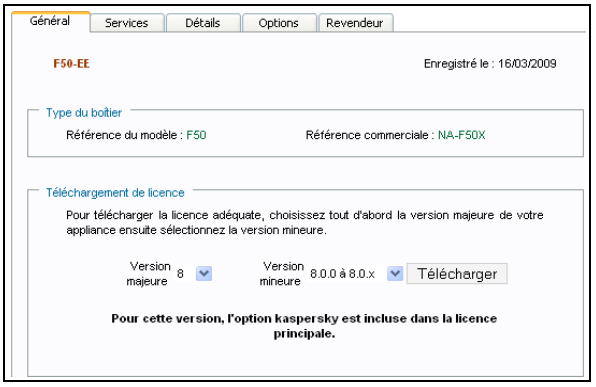
Your distributor: The name of the company from which you purchased your Firewall.

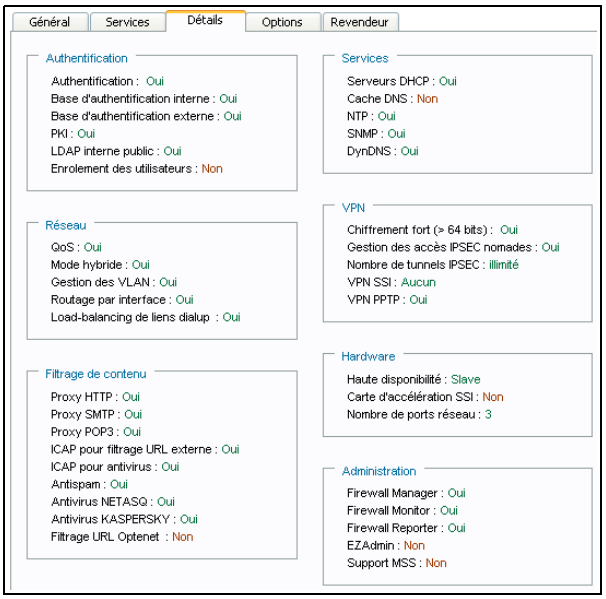
WARNING

The "factory" license of each appliance remains valid for 3 months. If you miss this deadline, you will not be able to use the UTM anymore. It is therefore necessary to register the appliance and insert the licensein the shortest possible time.

Injecting the license

Once you have registered the UTM, you will be able (it is even necessary) to inject the license into your appliance, so as to benefit from the options you have subscribed. To do so, please log in via the menu `CLIENTS - PARTNERS` on our website www.netasq.com and click on the link `Go to your private area`. Once you are authenticated, open the menu `License Management`. Here the list of UTMs registered on your account will be displayed. Click on the corresponding model, then on the serial number to obtain its license information. The panel as shown appears:





The general properties of your license are shown on this page and you will be able to download it. You are also free to check the license details (including available options) via the `Details` tab.

Depending on the options you have bought, this page will show whether the corresponding options have been activated.

Once you have downloaded the license, you will get a .licence extension file. To inject it into your UTM, you must connect to your appliance via the Unified Manager, and go to the menu `Firewall / Licenses...`. Then, click on the `License...` button. Select the license file and validate.

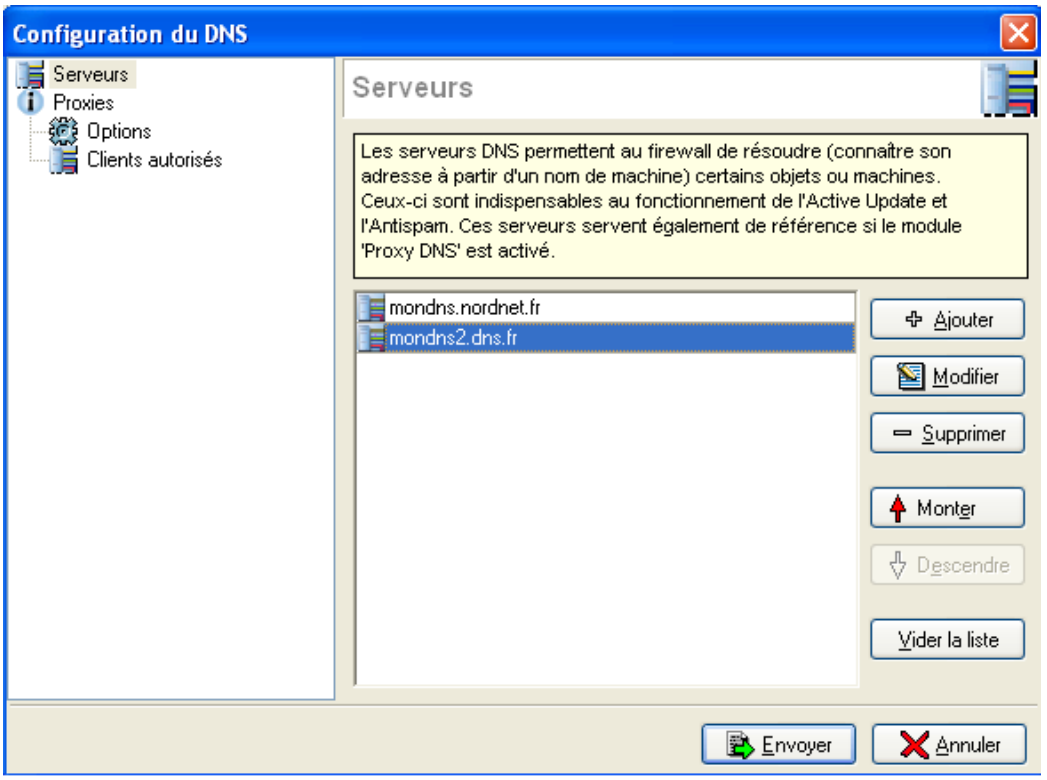
WARNING

The UTM will reboot after the license has been injected.

Once the UTM has rebooted, all the options you have subscribed will be available and ready to be used.

DNS servers information

When you connect for the first time with the Unified Manager to your UTM, a message will appear, indicating that you have not yet configured any DNS servers. DNS servers allow you to match a hostname and its IP address. This service is essential, particularly to enable the UTM to perform updates properly. So to notify your DNS servers, you must have the IP address of your server(s) (your Internet Service Provider generally provides you with this information), and go to the menu `Services / DNS`, in order to add hosts that correspond to your servers, as shown below:



By clicking on the `Add` button, you wille be asked to choose the host that corresponds to your DNS server in your objects base. If this host does not exist yet, it is possible to create it by clicking on `New / Host`.

Once you have added the DNS server, you can send the configuration to the UTM. Thus, the UTM will be able to resolve hostnames for its own needs.

NOTE

Several DNS servers may be added. Consequently, the UTM will use them randomly.

Configuring the timezone

This often-neglected feature is particularly important. If you define a timezone, you will no longer have to bother about Daylight Saving Time. It is also useful for locating an event that has been registered in log files, or for comparing logs from other appliances.

To set up this parameter, please go to the menu `Firewall / System Configuration...` then select the `Timezone` tab. The following panel will appear:

You can define the timezone thanks to all the standard designations (GMT, CET, CEST, ...) or by selecting the reference city by browsing the areas menu (for example: Europe/Paris).

If you choose a city rather than an international timezone, it will allow you to synchronize during Daylight Saving Time. We therefore advise you to choose this type of timezone.

WARNING

The UTM will reboot after the timezone has been modified.

Activating the NTP service

The NTP service (Network Time Protocol) enables an entire network to synchronize its clocks on a unique server which will act as a temporal reference.

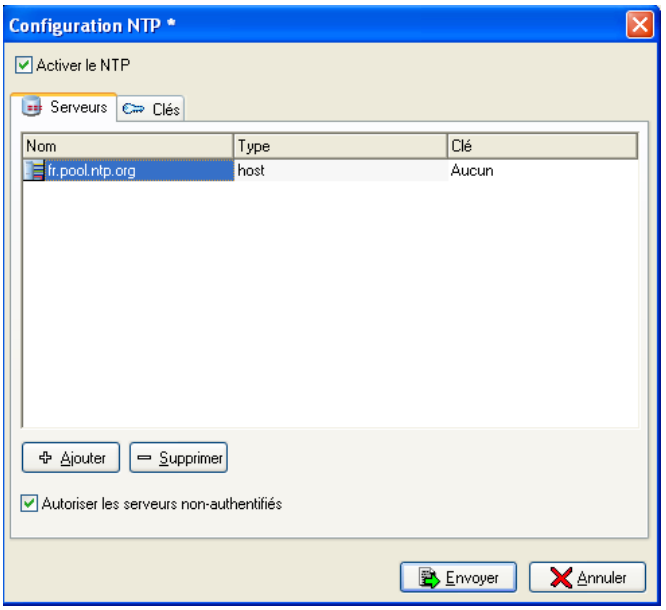
To use the NTP service, you must first activate it. You can do so in the `Services / NTP` menu. (This service is not available for F25 UTMs).

Two tabs are available: `Servers` and `Keys`.

The `Servers` tab lists all the servers (public or private) that your UTM can connect to, in order to synchronize itself.

Click on `Add` to choose in your objects list the corresponding host (create it if it does not exist yet).

The `Keys` tab enables the configuration of authentication keys for NTP servers. This key wille be visible if you connect with "modify" rights, otherwise it is hidden.



The project pool.nt.org makes an inventory of many NTP servers around the world. For France, the NTP server for this project would be: fr.pool.ntp.org.

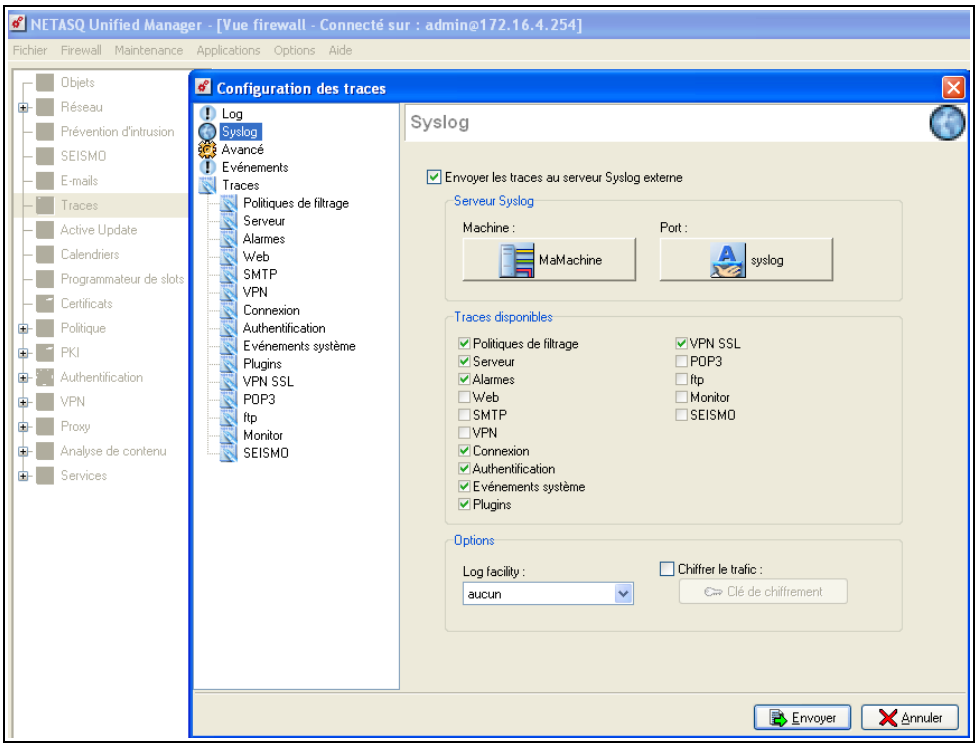
NOTE

Even if you have configured the NTP service, you must still configure your timezone. Indeed, NTP is a synchronization protocol which works in UTC mode (Coordinated Universal Time). The time lag must therefore be indicated locally.

Configuring the Syslog server

All the logs and alarms the UTM generates are stored on the UTM hard disk drive, in the /log directory. However, NETASQ "S" models (F25, F50, F60, U30 and U70) do not integrate any hard disk drives and consequently cannot store logs.

Nevertheless, it is possible to configure a very useful service that will allow exporting to a remote server the logs and alarms generated by your UTM; this service is called "syslog". To configure it, please go to the menu `Logs / Syslog` as shown below:



For the `Host`, select the workstation on which you will store your logs. By default, the port used for transmitting logs is UDP/514.

You are free to select logs you wish to store by selecting from the list of `Available logs`.

By default, the backup directory of these files is C:\Program Files\NETASQ\script\log\.

Obviously, this implies that the administration host must be running 24/7 so as to continuously receive logs that the UTM sends.

Registering your UTM registration after an exchange

Your appliance has broken down. Your warranty enables you to return the defective appliance to us. After having received your new product, you legitimately attempt to register it in your private area on www.netasq.com, but you get an error message which shows that your appliance has already been registered.

Indeed, after an exchange, the new appliance you receive will automatically be registered in your private area. As such, you do not have to do anything about the new product registration. The NETASQ Sales Administration Department will handle everything.

However, you will need to inject the corresponding license to your new appliance, and possibly update it to the latest firmware version.

Installing and activating a NETASQ VPN client

When you purchase a NETASQ VPN license, you will obtain a serial number which enables you to download the VPN NETASQ-TheGreenbow software on our website http://vpn.netasq.com.

Once you have downloaded this software, you must activate your license using the same serial number before being able to use functions on the NETASQ-TheGreenbow VPN client.

NOTE

A 30-day trial version is available by typing "demo" in the Serial ID field.

Filter policy

The filter function is the key element of a security policy, because it allows or blocks traffic passing through the UTM.

Thanks to this policy, it is possible to define hosts which are allowed to communicate with each other, or their destination interfaces, or even to define authentication rules for your users.

The priority of filter rules is easy: every rule is treated in the order it appears in the policy you have defined. It means that when a packet reaches the UTM, it checks if the packets can be applied to the rule number 1; if this rule cannot be applied, the UTM will test with the rule number 2, etc.

As soon as a rule matches the received packet, the UTM will apply the corresponding action and will exit its filter policy.

Consequently, if you wish to authorize a traffic for all users with a restriction on one or several hosts (a trainee for instance), you must first create the rule that blocks the exception before creating the rule for all the other hosts.

Do note that whatever is not authorized in the filter rules will be blocked.

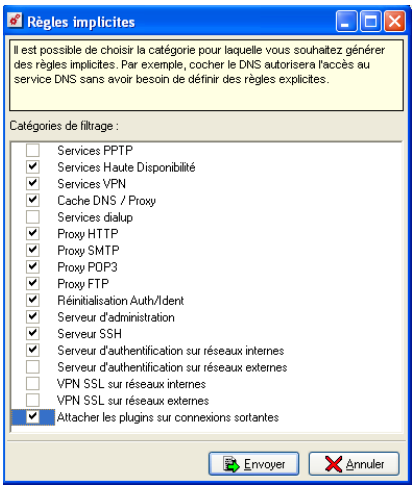
Note also that the NETASQ filter is Stateful. This means that when a packet is authorized to transit through the UTM, the filter module will also authorize every possible reply automatically (it will authorize for instance an "echo reply" ICMP packet if an "echo request" ICMP packet has previously passed through the UTM).

NOTE

The NETASQ filter is not Stateful for protocols such as GRE, ESP, ...

Lastly, some open ports for child connections are managed by ASQ plugins (FTP, SIP, H323, ...).

Implicit rule: Do note that a list of implicit rules is available via the men `Policy / Implicit Rules`. This menu enables you to validate services that NETASQ places at your disposal. If you do not select the service, you will have to create the corresponding filter rules yourself in order to authorize the traffic to pass throught. Implicit rules have the upper hand on explicit rules (that is to say that even if you block all traffic in your slot, implicit rules will always be in pass mode).



NAT policy

NAT allows (among other things) using a private address range for the local network and "hiding" all the hosts behind a single IP address for Internet connections for instance. In other words, only one public IP address will represent all the private hosts from the local network.

NAT offers two advantages:

- It hides a network's hosts from the outside,
- There is no need for a huge number of public IP addresses (only one is enough)

A few types of translations are available on NETASQ appliances:

Map: map allows hiding n IP addresses behind only one public IP address. Typically, this type of translation is used for allowing a local network to browse on Internet.

Example of a Map rule:

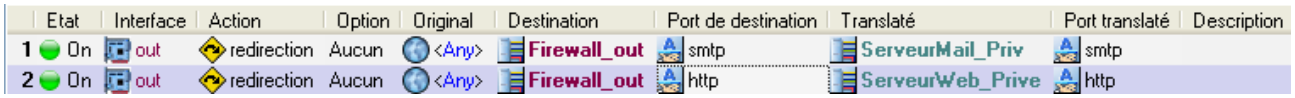
Bi-Map: This translation allows hiding a private address behind a public address. You can use it if the firm has a lot of public IP addresses. This translation consists of allocating an IP address from a public address range to a server.

Unlike the Map rule, the Bi-Map rule is bidirectional, that is to say that the server can only be reached by the public address and it connects to the Internet with this same address.

Example of a Bi-Map rule:

Redirect: Thanks to this translation, servers from our local network can be reached from the Internet. Traffic received by the UTM will be redirected to the UTM's public IP address (example Firewall_out), which will in turn redirect the traffic to the relevant server according to the requested destination.

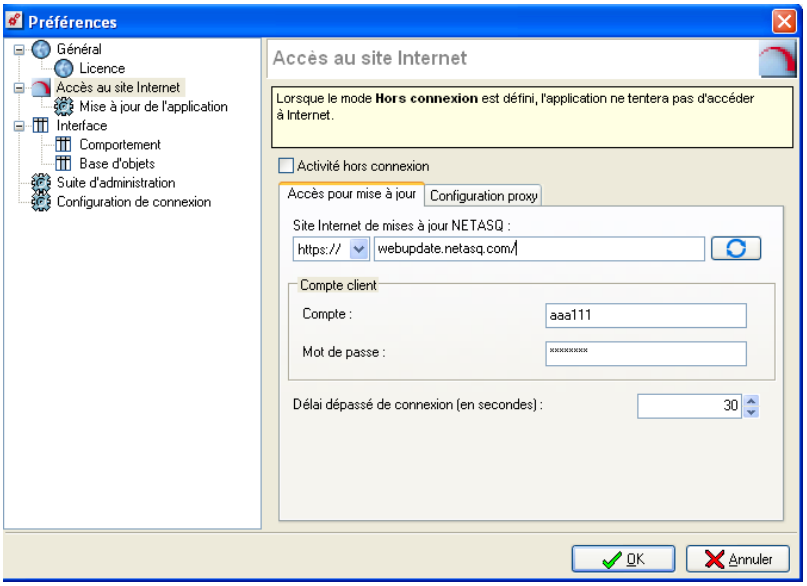
Example of a Redirect rule:



Quick search for new firmware versions

It is possible, in the Unified Manager to perform a quick search for the latest firmware version available and to install it, without having to connect manually to NETASQ's website. In a few mouse clicks you will be able to update your UTM.

To do so, you just need to configure the menu `Options / Preferences / Internet Site Access`, and to indicate the website that will allow you to update and enter your login/password, as shown below:



Then, you only need to click on `Maintenance / Search for firmware...`. The menu will appear and shows whether a new firmware version currently exists on NETASQ's website. If a version is available, you only need to click on `Update...`.