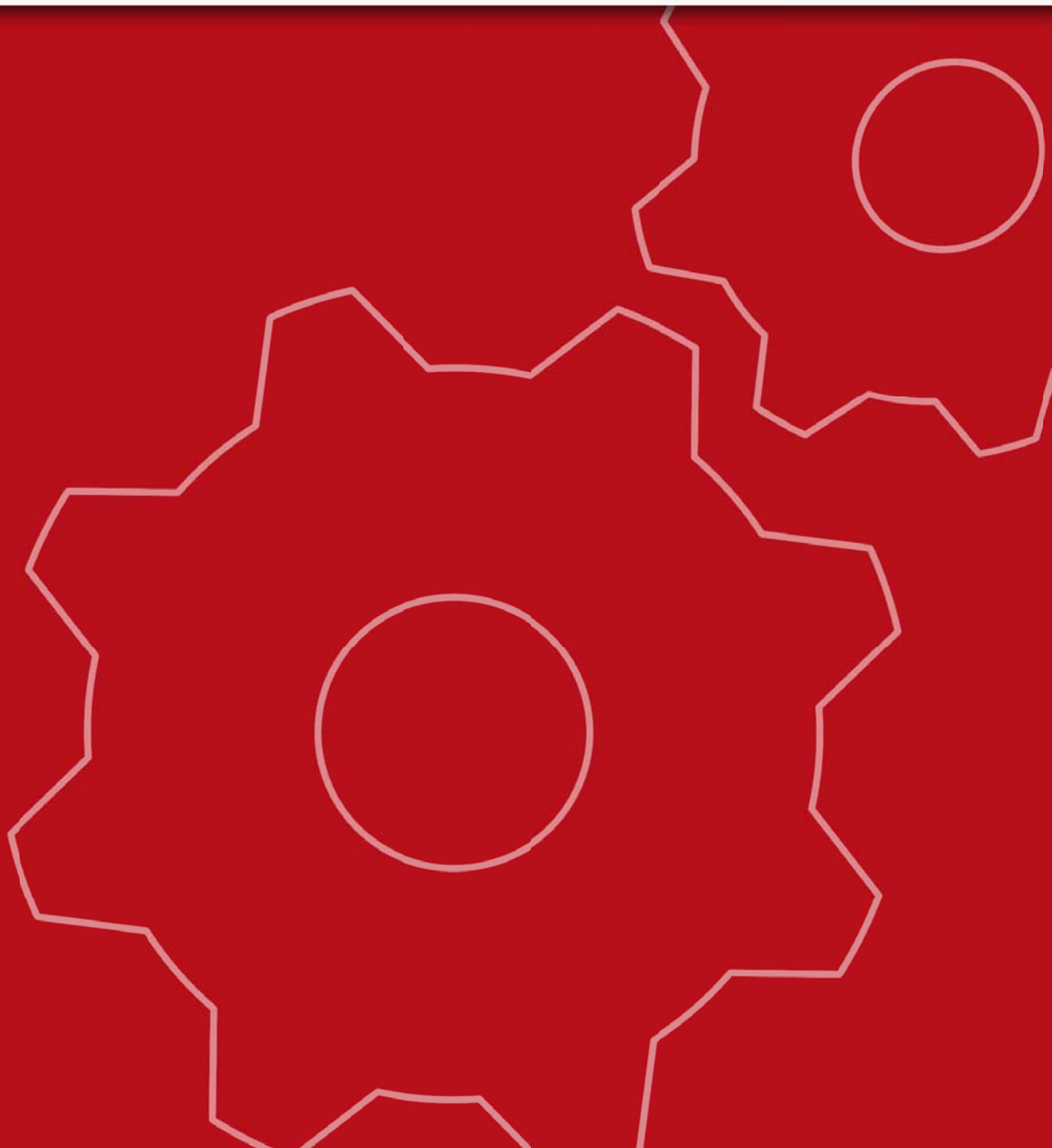




NETASQ
UNIFIED MANAGER



NETASQ UNIFIED MANAGER

V. 7.0.2

USER CONFIGURATION MANUAL

(DNS)

Reference : ENCH0803_DNS-V7.0.2
Created: March 2008
Modified: March 2008

DNS

Introduction

In this section, we intend go back on a few principles of how DNS operates

DNS functions in client-server mode. The client part is called the *resolver*, which is a library. The server part is called the *name server*.

Three types of name servers exist:

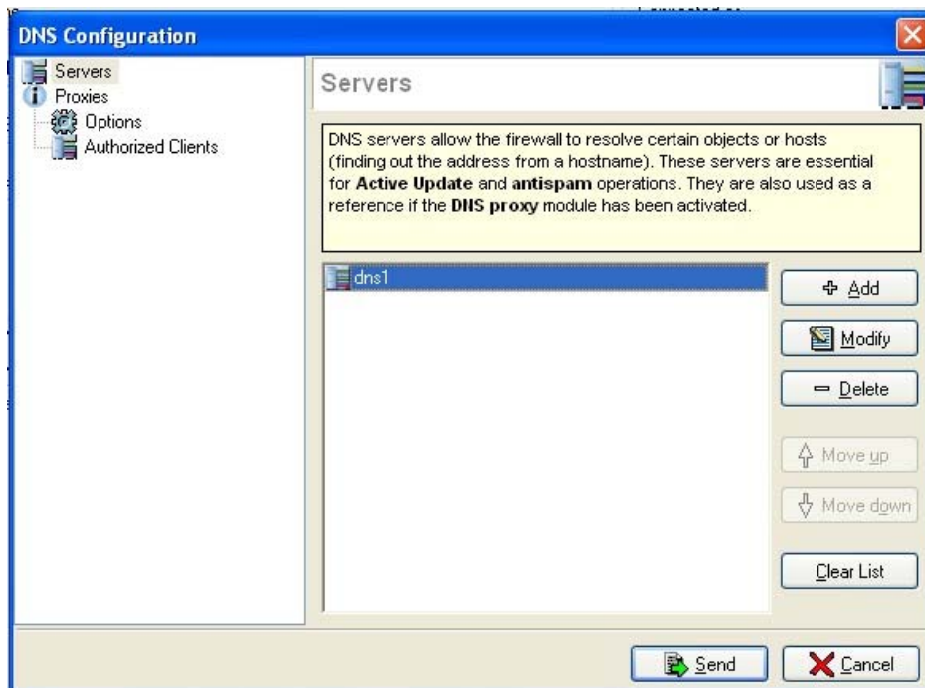
- **Primary**: possesses up-to-date tables on a domain.
- **Secondary**: possesses tables from another server.
- **Cache**: possesses tables formed from processed information.

Using the NETASQ UTM Firewall's DNS service

NETASQ's DNS service is a cache. A DNS request is sent through the Firewall, the Firewall stores (in the **DNS** cache) the response and this guarantees better response time during the next similar DNS request. Furthermore, the Firewall intercepts and receives the requests, thereby ensuring optimal security.

Operation

➤ The DNS service has to be activated in order to be used, via the menu **Services**\DNS.



The **DNS** service configuration screen consists of two sections:

- On the left, a directory displaying the various features of the **DNS** service menu
- On the right, the options that can be configured

The **DNS** service proposed by the NETASQ Firewall is a **DNS** cache, which serves to store **DNS** responses matching domain names and IP addresses.

Servers

Servers enable the Firewall to resolve (find out a host's IP address from its name) certain objects or hosts. These servers are essential for Active Update and Antispam to function and are also used as a reference if the DNS proxy has been activated.

When servers are configured, antispam, antivirus and object resolution modules send their queries to these servers without necessarily activating the Firewall's DNS proxy (DNS cache). In this case, if a user sends a DNS request on an unconfigured server, the Firewall will transmit the request to the said server and the user sending a DNS query to the Firewall will see his query being refused.

If the option **Enable DNS** has been selected in the **Proxies** menu, antispam, antivirus and object resolution modules will send their queries to configured servers without having to consult the DNS cache. If a user sends a DNS query to an unconfigured server, the Firewall will transmit the query to the said server, and when a user sends a DNS query to the Firewall, the DNS cache will treat his query.

Finally, if the DNS proxy has been activated and the transparent mode configured (see transparent mode configuration above) antispam, antivirus and object resolution modules send their queries to configured servers using the DNS cache. If a user sends a DNS query to an unconfigured server, the Firewall will transparently redirect the query to the configured servers in this module, and when a user sends a DNS query to the Firewall, the DNS cache will treat his query.

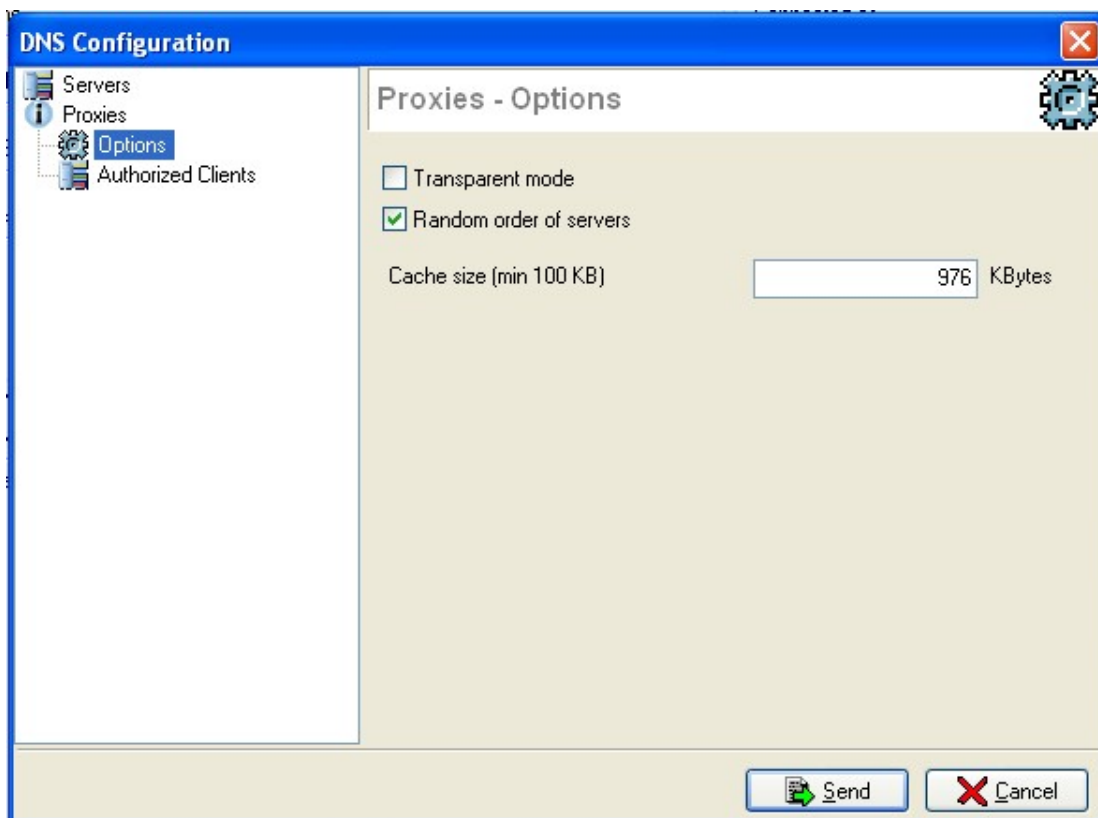
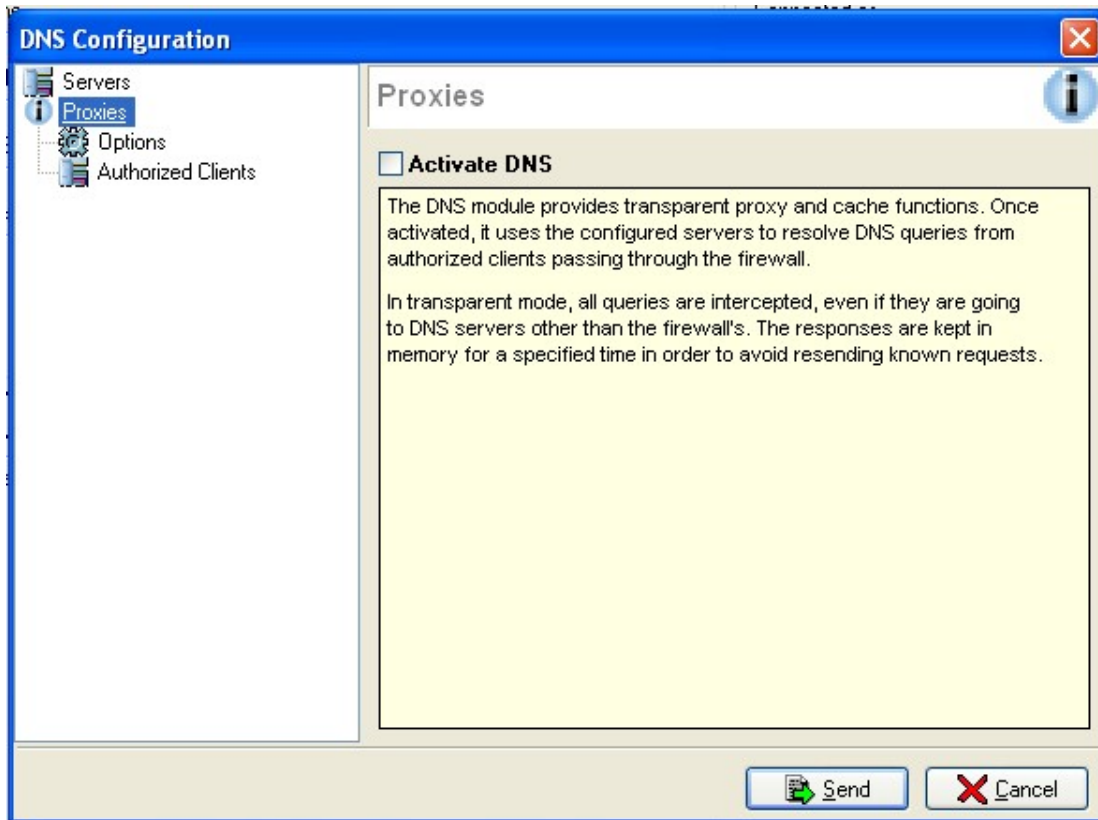
Action bar

Add	Adds a DNS server. The objects database will appear so that Hosts, Address Ranges and Groups can be selected.
Edit	Modifies the selected DNS server.
Delete	Removes the selected DNS server.
Move up	Places the selected row before the row directly above it.
Move down	Places the selected row after the row directly below it.
Clear list	Deletes the whole list of servers.

Proxies

The DNS module offers cache and transparent proxy functions. Once it is enabled, DNS queries from authorized clients passing through the firewall will be resolved by the module, using the configured servers.

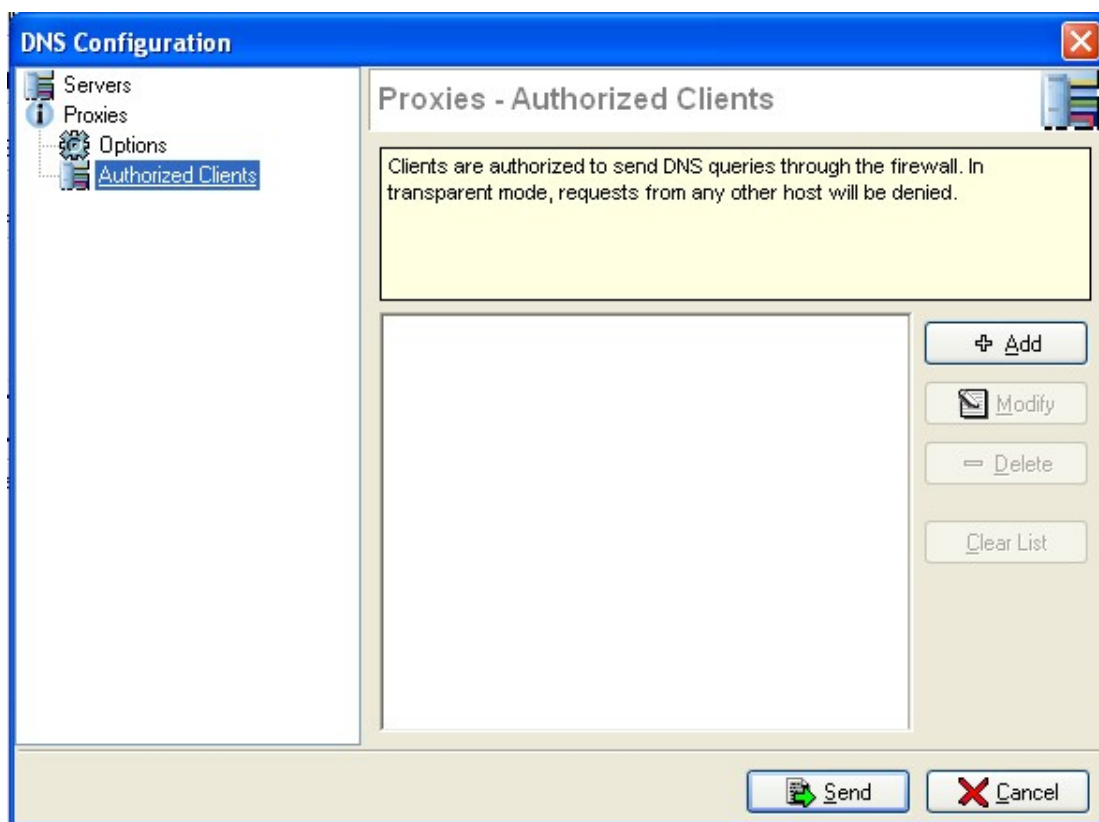
In transparent mode, all queries will be intercepted, even if they are headed to DNS servers other than the firewall. Responses are kept in memory for a certain period in order to avoid re-sending requests that have already been sent.



Options

Transparent mode	As its name implies, this option aims at making the NETASQ Firewall DNS service transparent. As such, when this option is activated, the redirection of DNS flows to the DNS cache will be invisible to users who think they are accessing their DNS server.
Random order of servers	Allows the firewall to select a DNS server at random from the list.
Cache size	Size allocated to the DNS cache

Authorized clients



Authorized Clients: List of clients authorized to send DNS requests. This list may contain networks. In transparent mode, requests from any other machines will not be treated.