

# NETASQ multi-function firewall version 9

---

## Highlights

---

Features covered	Level of modification
New configuration interface	→ Major
Filter policy	→ Major
High availability	→ Major
Operating system	→ Major
Proxy	→ Major
Intrusion prevention	→ Major

---

## Version

---

9.0.2	Features		Bug fixes
9.0.1.1		Resolved vulnerabilities	Bug fixes
9.0.1	Features	Resolved vulnerabilities	Bug fixes
9.0.0	Features		Bug fixes

Known issues

---

## Upgrade

---

Lowest version required: 8.0.3  
 Hardware compatibility: U, NG and VM ranges  
**Lowest H.A version required:** / (H.A will be disrupted during the upgrade)

**i NOTE**

Version 9 is not compatible with products in the F range.

**! WARNING**

During the update, the configuration will not be converted. Please read the document "Migration from v8-v9" for further information.

---

## 9.0.2 Features

---

### Filtering and NAT

#### Non TCP/UDP protocols

The status of IP connections can now be tracked for protocols other than TCP, UDP or ICMP. 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.

Connection status tracking on IP protocols can be enabled in the "protocol" column in the relevant filter rule.

#### NAT

An 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.

### Intrusion prevention

#### SSL scan

Detection of THC-SSL-DOS attacks with the addition of a maximum number of renegotiation attempts within the same TLS session.

#### HTTP scan

Protection from the denial of service attack CVE-2011-3192 has been added, based on the hijack of partial HTTP downloads (Partial-content / Ranges) in order to cause the excessive consumption of Apache memory resources.

The maximum number of partial download ranges has been set to 200 by default for the incoming profile (00), which protects servers, and 1024 for the outgoing profile (01).

### Installation wizard

The initial installation wizard has been enhanced, with the possibility of defining a simple security policy. In order to use this wizard, the firewall has to be in its default configuration. It can be reached at the URL: <http://10.0.0.254/admin/install.html>.

### IPsec VPN

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.

## Authentication for sending e-mail alerts

A login and password can be defined for sending e-mail via the firewall (Menu “Notifications > E-mail alerts”).

## System

SNMP can now be configured so that the name of the firewall instead of its serial number is used for SysName.

## Real Time Monitor

The latest VPN and SYSTEM events can be viewed on firewalls that have no hard disk. A window containing additional information on the 3G link has been added.

---

## 9.0.2 Bug fixes

---

### Intrusion prevention

The alarm 134 that is generated every time a telephone in SIP sends “ACK” messages will no longer be raised unexpectedly.

The scan of the option “utimeout” has been added to the TFTP protocol inspection.

**Support references 28159-30016**

Implicit PPTP rules are now correctly inserted when the PPTP server is enabled.

**Support reference 28577**

User groups containing spaces in the filter policy can now be used again.

**Support references 29342-20855**

The default values for the “Buffer Overflow” alarm in HTTP inspection have been increased.

**Support reference 29620**

FTP inspection rules containing a specific gateway (PBR) are now correctly routed in the case of data connections initiated by the firewall (passive FTP).

The SMTP scan will no longer shut down the connection if a RSET command is sent before the MAIL FROM command.

**Support reference 30216**

The source IP address used by the HTTP proxy in rules that define a specific routing gateway (PBR) is now correct with regards to the interface on which the router is located.

**Support reference 30564**

The TCP alarm for out-of-sequence packets (“outside window”) will not be raised for a TCP keepalive packet containing 1 byte.

**Support reference 30194-30738**

An error that could cause the system to unexpectedly reboot has been fixed in the SIP scan if it has been associated via a filter rule in “firewall” mode.

**Support reference 29661**

The list of default ports is now applied with the inclusion of the last element.

## **NAT**

**Support reference 29961**

NAT can be performed on TFTP when the source port is translated.

**Support reference 29214**

NAT connections will no longer be interrupted during the reinitialization of a configuration containing rules with the fields “from” or “to” in user groups, or with the operator “NOT”.

## **Network**

**Support reference 29853**

Routing by bounce on the same interface of a bridge with an alias has been fixed.

**Support reference 29583**

Static routes can now be added on an IPSec interface.

## High availability

Support reference 29738

The stability of an internal high availability process (corosync) has been enhanced.

Support reference 29954

Errors occurring when members of a cluster do not have the same software versions (firmware) have been corrected.

Support reference 30442

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

Support reference 29595

Disabled network interfaces no longer appear in the high availability quality calculations.

## Vulnerability management (NETASQ Vulnerability Manager)

Support reference 28904

Information concerning unmonitored hosts when using the explicit proxy will no longer be displayed.

## Proxies

Support reference 29852

The firewall now uses the correct IP address for outgoing packets when they use the proxy and PBR at the same time.

Support reference 29582

The CONNECT method in HTTPS using the explicit proxy has been fixed.

Support reference 29715

Problems with downloads passing through the FTP proxy have been fixed.

Support reference 29767

Users will now be entered in web logs when they use the explicit proxy and the option "several users per IP address".

An error relating to the explicit HTTP proxy has been fixed.

**Support reference 30758**

Trusted CAs have been added to the SSL proxy for GlobalSign and Verisign.

## **System**

**Support reference 28105**

The authentication portal no longer needs to be rebooted when changes are made to the SSL VPN user access policy.

**Support reference 29079**

UTF-8 characters are allowed for the authentication of LDAP users.

**Support reference 29253**

In the authentication portal, the link to the web administration interface will take into account the port if it is not 443/TCP.

**Support reference 30278**

Rules for accessing the web administration interface are kept when the software version (firmware) is upgraded.

**Support reference 15232**

The list of time zones has been updated.

**Support reference 29858**

When no IPSec interface has been defined in the network configuration file, some configuration modules may not be accessible.

**Support reference 29019**

The "Accept-Encoding" empty fields in HTTP requests are now accepted on the captive portal (sld).

**Support reference 29760**

The problem arising during the partial restoration of configurations of the categories "IPS Protection" and "Web objects" has been fixed.

## IPsec

Support reference 28793

In the event packets are lost, those corresponding to the Config Mode will be sent in order to prevent negotiation failures.

Support reference 30225

Only the first three DNSs configured in Config Mode will be taken into account from now on.

Support references 30562-30952

AES256 support with regards to hardware acceleration in the NG series has been corrected.

## Web administration interface

### Dashboard

The License widget has been enhanced to offer a view by expiry date.

### Routing

With version 9, a default routing gateway has to be entered in order to allow intrusion prevention (ASQ) to send packets correctly when it desynchronizes connections.

### Filtering

A “Collapse/Expand” button has been added for filter rules.

A Support reference 29822

The logo of version 9 is now systematically displayed when you authenticate in “read only” mode.

Support reference 28628

Users’ DNs can now be displayed, allowing a proper display for the Mac OS X LDAP server.

Support reference 29770

You will no longer be asked to delete the active URL database when you select the existing URL database.

When a user does not have writing privileges, he can neither group his filter rules nor extend his VPN.

Support reference 28850

The numbers of DH and Modp groups will be displayed for Diffie-Hellman groups in the IPsec configuration.

Support references 27890-28841-31092

Renaming an interface causes the name of objects to be changed in the whole configuration.

Support reference 29944

The option "Keep initial routing" can be defined on a bridge.

Support reference 30088

Refresh the list of peers configured in Phase 2 of creation with the peer "None".

Support reference 30546

The registration of the DynDNS server in the associated profile no longer needs to be imposed if it has not been explicitly selected.

Support reference 29459

A trusted CA can be added to the configuration when you use the IPsec installation wizard.

Support reference 29622

All hosts in a selected rule will be added when the filter suggests creating a group.

Support reference 22040

The characters '\_' are allowed in the domain name for the LDAP installation wizard.

Support reference 29749

Configuring an IPsec peer has been made easy with fields being completed during entry.

## Global Administration

**Support reference 23733**

A new option has been added to avoid deleting objects generated from groups when they are deployed on firewalls.

**Support reference 28043**

An authentication error that could arise when you attempt to connect simultaneously to several firewalls has been fixed.

**Support reference 28138**

A potential error that arises when locking/unlocking a session has been corrected.

## Real Time Monitor

**Support reference 29856**

A decryption error in the address book has been fixed.

**Support reference 28611**

QoS counters are displayed in the right order.

**Support reference 30260**

After a DHCP request, "anonymous/0.0.0.0" will no longer appear in the Host section.

**Support reference 30261**

In the logs section, "Seismo" has been replaced with "Vulnerability Manager".

**Support reference 30395**

A problem with the display of graphs has been fixed.

## Reporter

**Support reference 28397**

Connection to firewalls with the "admin" password allowed by default.

---

## 9.0.1.1 Resolved vulnerabilities

---

### System

#### **CVE-2011-4079**

The error relating to OpenLDAP has been fixed.

#### **Upgrade of ClamAV to version 0.97.3**

<http://www.clamav.net/release-info/bugs/0.97.3>

<http://www.clamav.net/release-info/changelog/0.97.3>

---

## 9.0.1.1 Bug fixes

---

### Intrusion prevention

An error that may arise when using load balancing and the IPSec VPN together has been fixed.

#### **Netbios CIFS**

A false positive triggered by implementation of SMB OSX Lion has been fixed.

### NAT

**Support references 29785-29501**

An error that may arise within the kernel after the expiry of a NAT session has been fixed.

**Support references 29520-29539**

TCP sessions no longer get lost when NAT rules are reloaded.

### System

**Support reference 29875**

The network configuration would not reload correctly when a bridge was missing from the configuration but referenced by an interface.

**Support reference 29642**

An error that may arise during the configuration of a dynamic DNS client has been fixed.

**Support reference 29601**

An issue with the rotation of filter logs (l\_filter) has been fixed.

#### **Cryptography**

A problem with RC4 encryption (ARCFOUR) on models and NG-1000 and NG-5000 has been fixed. It could impact the authentication module, the SSL proxy and SSL VPN.

---

## 9.0.1 Features

---

### New configuration interface

The web interface is now compatible with Internet Explorer 9 and is available in Polish. Many screens have changed and a wizard for the initial installation has been added in order to simplify the launch of your firewall's configuration.

#### Objects

##### DNS

A DNS resolution tool has been added to Objects: when an object is added/modified, a window appears. If the URL of an object is entered in the field "Object name" and if you click on the magnifying glass icon, you will obtain the IP address of the object, which can be seen in the "IP address" field.

##### Focus

When you go to the "Objects" tab in the menu directory on the left, the focus is now directly on the search field.

#### Alarms

An instant search field has been added to both views of the module, in order to more easily filter profiles and contexts without having to press "Enter".

##### Dashboard

The "Alarms" section in the dashboard contains a new button that allows you to "Clear screen", or in other words, erase information logs.

The "Hardware" section sets out information on the current HA version and in the event a disk is faulty or missing, it will display a warning alarm in the RAID option.

##### Cisco WAN

A new alarm has been added to detect Cisco WAN Optimizer traffic. The alarm blocks this traffic by default, but it can be allowed (tcpudp : 247).

#### **WARNING**

Once this traffic is allowed, this type of traffic will not go through protocol scans.

#### Filtering and NAT

Filter and NAT rules can now be moved by dragging and dropping.

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.

## **Users**

When a user is deleted, the administrator will be prompted to revoke his certificate.

## **HTTP**

A parameter has been added in order to allow certain HTTP headers to ignore buffer overflow protections to avoid false positives with headers that are particularly long. By default, only “Proxy-Authorization” will be on this list. The parameter “AllowOverflow” (HTTP profile) can be configured in the CLI.

## **NAT policy**

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.

## **System**

### **3G USB**

An external 3G modem can now be connected to the USB port and can be configured in the Interfaces menu.

### **Dynamic routing**

Major upgrade of dynamic routing modules (ZebOS version 7.8.2071211).

### **IPv6**

Routing of IPV6 packets is now supported by NETASQ multi-function firewall.

This option is disabled by default and can only be configured in the CLI.

### **Kaspersky**

Major upgrade of the Kaspersky antivirus engine. This engine adds a complementary heuristic analysis.

### **CRL**

You can now add CRLDP (CRL distribution points) for CAs imported via the GUI.

### **SSL authentication**

The subject field of the certificate that will be used in searching for a user in the LDAP can be modified. The LDAP field used for the search can also be modified. The e-mail address is used by default in both cases. These parameters can be set in the CLI.

## **VLAN**

The appliance no longer needs to be systematically rebooted whenever a VLAN is deleted.

## **Intrusion prevention**

Protection methods have been added for the following SCADA protocols:

- dnp3
- modbus
- realwin
- datahub
- netb
- genbroker (tcp)
- hicp (udp)

## **QoS**

“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).

---

## 9.0.1 Resolved vulnerabilities

---

### System

#### **CVE-2011-3207, CVE-2011-3210**

OpenSSL has been upgraded to version 1.0.0e.

#### **CVE-2011-2748, CVE-2011-2749**

Two flaws that could cause denial of service attacks in the DHCP server have been resolved.

 **NOTE**

The DHCP server is not enabled in the default configuration.

#### **CVE-2011-2721**

ClamAV has been upgraded to version 0.97.2. This version fixes the vulnerability CVE-2011-2721.

 **NOTE**

The ClamAV engine is not enabled in the default configuration

### SSL Proxy

The certificates provided by the Dutch company DigiNotar have been compromised, and have therefore been deleted from the list of certificate authorities supported by the NETASQ SSL proxy.

## 9.0.1 Bug fixes

---

### System

#### Web 2.0

The performance and stability of the Web 2.0 analysis engine have been enhanced.

#### Filtering and NAT

In certain configuration contexts, an expected reboot of the appliance could occur, following these modifications:

- when the filter policy is reloaded
- when the status of a filter rule is changed by a time object

#### PKI

The process of importing and deleting certificates has been enhanced.

#### General configuration

##### Modem

The addresses of DNS servers are correctly retrieved during the connection of a modem interface (predefined objects Firewall\_ <dialup>\_dnsX).

##### Daemons

Date changes are now better handled by daemons.

##### License

When a new license is available, the difference with the current license is now correctly displayed.

### Proxies

#### SSL Proxy

Several stability issues have been fixed.

HTTPS sessions decrypted by the SSL proxy were systematically logged with 127.0.0.2 as the client's IP address.

The firewall will no longer send its own certificate to the server.

Trusted authorities selected in the SSL authentication module are no longer considered "trusted" by the SSL proxy.

#### HTTP Proxy

A memory leak has been fixed.

Partial downloads are now allowed.

#### SMTP Proxy

E-mails that reach the maximum size for the antivirus scan are now correctly sent.

### **FTP Proxy**

A potential reboot of the proxy when the connection limit is reached has been fixed.

### **ClamAV**

The stability of proxies and the ClamAV antivirus has been enhanced.

### **General points**

#### Load balancing

Load balancing when proxies are enabled has been repaired.

Support reference 28496

The configuration reset button was unable to react correctly on U30 and U70 models.

Support reference 29113

Correction of a problem with the hardware acceleration of AES encryption on NG models, which could cause the corruption of packets in certain configurations.

### **Active Update**

Support reference 28421

Correct refreshment of the Active Update module when a new license is inserted.

### **PPTP**

Support reference 28853

The characters “\_”, “-”, and “.” are allowed for PPTP user names.

### **SYSLOG**

Support reference 29197

The categorization for the sending of messages via Syslog has been corrected: “kernel” becomes “user”.

Support reference 28535

The BindAddr parameter, which allows imposing the sending IP address for the Syslog module, is in working condition again.

### **Antispam**

Support reference 28387

Correction of error messages that could appear during the configuration of antispam lists following a migration from version 8 to version 9.

### **CRL**

Support reference 28289

The maximum lifetime of certificates has been increased to ten years.

## Authentication

Links added to the authentication portal in version 9 have been translated into all the supported languages.

**Support reference 29080**

The access control list (ACL) for access to the web interface is now correctly refreshed when an interface is updated in DHCP.

**Support reference 20336**

ISO-8859-15 characters (including “€”) are allowed for administrator passwords.

**Support reference 28636**

Multiple authentication with the same IP address is possible again on the explicit HTTP proxy.

## SSL VPN

### SSO

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.

**Support references 22508-24925-24639**

The JavaScript parser has been rewritten in order to correct the restrictions of the former version with regards to rewriting web links.

## IPSec VPN

The negotiation mode (main or aggressive), when it is imposed, is kept when the configuration of an IPSec peer is modified.

### X-auth

X-auth mode without Mode-Config has been fixed.

### Failover

The tunnel switching mechanism has been enhanced.

**Support reference 28937**

The parameter `cfg_domain` has been added to the configuration of IPSec peers, so that it can distribute a domain name in Mode-Config. This parameter, which can be configured in the CLI, was necessary for iPhone compatibility.

**Support reference 28793**

IPSec negotiations with X-auth have been enhanced to be better supported on less reliable networks (slowness, loss of packets).

## Network

### Load balancing

Load balancing is correctly applied on connections sent by the firewall.

### NAT/ Load balancing

Types of load balancing other than connection hashing can now be selected with a range of destination ports.

Support reference 28678

If a migration to version 9 is carried out from version 8, access to web management is allowed from any IP address so that users can reconnect remotely after the update.

Support reference 13828

The problem that arose during the reinitialization of all interfaces when modifications are made in the network screen has been fixed. Now only modified interfaces will be reconfigured.

Support reference 28350

The FTP proxy in active mode is now better supported.

## High Availability

The stability of HA has been enhanced.

### Switchover time

An option has been added to reduce the time surrounding appliances take to take into account a switch in the cluster in bridge mode. If the option has been enabled, interfaces on the bridge will be reinitialized at the moment of the switch in order to force users connected to the firewall to renew their ARP tables.

### Synchronization

The passive firewall in a HA cluster no longer needs to be rebooted when objects are synchronized.

Support reference 29330

The upgrade of the passive firewall is no longer blocked when the versions of the firewalls are different.

## Intrusion prevention

Support reference 28895

Certain TCP “keepalive” packets may be blocked by the TCP scan.

Support reference 28619

Banners of FTP servers that contain line feeds are no longer blocked.

The SSL scan's detection of unencrypted packets has been enhanced.

Support reference 28707

The stability of HTML and JavaScript context scans has been fixed.

Support reference 28322

Filter/NAT rules established with a port but without a defined protocol now only apply to TCP and UDP traffic.

Support reference 28326

The alarm "Invalid SMTP protocol (ClientInputWaitingBlankAuthLine)" raised as an alarm and which can be raised by the command SMTP "AUTH LOGIN" has been fixed.

Support reference 28528

## **NAT**

A port range can be allowed for the destination in a NAT load balancing rule, unlike a port group.

Support reference 28798

NAT rules can no longer affect the proper operation of HA and apply to the traffic between both firewalls of the same cluster.

## **MTU**

An error that arose during the refreshment of the MTU in an IP profile has been fixed.

## **Security policy**

### Routing policy / Load balancing

The ID of the router is now correctly restored when a connection is retrieved (after a HA switch or reboot of the firewall).

### SSL

Some SSL sessions did not correctly shut down after the joint use of the SSL plugin and proxy.

## New configuration interface

### General configuration

The web interface is now available in Polish.

Information on the backup partition is now correctly displayed.

A JavaScript error that appears during a request to reboot the firewall from the web interface has been fixed.

**Support reference 28113**

The stability of network configuration screens has been enhanced.

**Support reference 27488**

The characters “[ ]” and “{ }” are no longer allowed in URLs (Internet Explorer 7 and 8).

**Support reference 28848**

The quarantine duration of a host is displayed in minutes.

**Support reference 28049**

Disabled interfaces will be displayed on the dashboard.

**Support reference 28280**

The selection of a certificate imported for the authentication portal has been fixed.

**Support reference 27890**

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".

**Support reference 29058**

The error message that appears during the creation of a load balancing configuration has been fixed.

### Security policy

**Support reference 27638**

The management of colors during the creation of separators has been enhanced.

**Support reference 28513**

A Javascript error that could arise in the explicit proxy configuration wizard has been fixed.

**Support reference 28541**

“none” can be selected as a sender in the module Security policy \SMTP filtering.

**Support reference 28410**

The error that appears on certain actions in the filter rules during dragging and dropping has been fixed.

**Support reference 28262**

The value of the tooltip in the filter screen has been corrected.

**Support reference 28291**

Objects will only be displayed in the menu directory upon connection in modules that have been deemed relevant.

Filtering and NAT

You can now copy and paste the separator from one location to another. The “Down” button has been repaired.

An issue with the display of rules when the global filter policy is being edited has been fixed.

QoS

The ability to select a default queue has been removed from the web configuration interface (but is still available on the CLI console). Indeed, this rule applies to all traffic, which is seldom the desired configuration.

**High availability**

The pop-up suggesting the synchronization of a cluster in read-only mode has been removed.

**Certificates/PKI**

The pop-up informing that a change has been made to the configuration (when this is not the case) has been removed.

The JavaScript error that appears during the display of the CRL of a CA imported with its private key, has been fixed.

**Preferences**

Global objects are now correctly handled in the URLs in the SSL VPN module.

**SSL VPN**

A problem with the display of fields for entering pre-shared keys in Internet Explorer 7 has been fixed.

## IPSec VPN

**Support reference 28549**

The pre-shared key confirmation field in the IPSec installation wizard, used with Internet Explorer 7, has been fixed.

## High availability

**Support reference 28713**

The display of the firmware version on the secondary or backup partition has been fixed.

**Support reference 28600**

Access to the HA screen is possible regardless of the module's status.

## Access privileges

**Support reference 27657**

A search field has been added to the tab "Access policy".

## Unified Manager

The pop-up announcing a disconnection has been fixed (the firewall name was missing).

## 9.0.0 Features

### New configuration interface

#### Main points

The new configuration interface on NETASQ multi-function firewalls is now accessible via a web browser and benefits from the latest breakthroughs in user-friendliness and ease of use. It is compatible with the following browsers:

- Internet Explorer 7, 8
- Firefox 3.6 and +

Compatibility with Internet Explorer 9 is in the process of being finalized.

During the connection to the interface and to the various modules, the user will first have an overview of his product's configuration via the dashboard. By browsing through the modules, the basic settings will be directly accessible. The "Advanced properties" mode is collapsed for better readability.

#### The dashboard

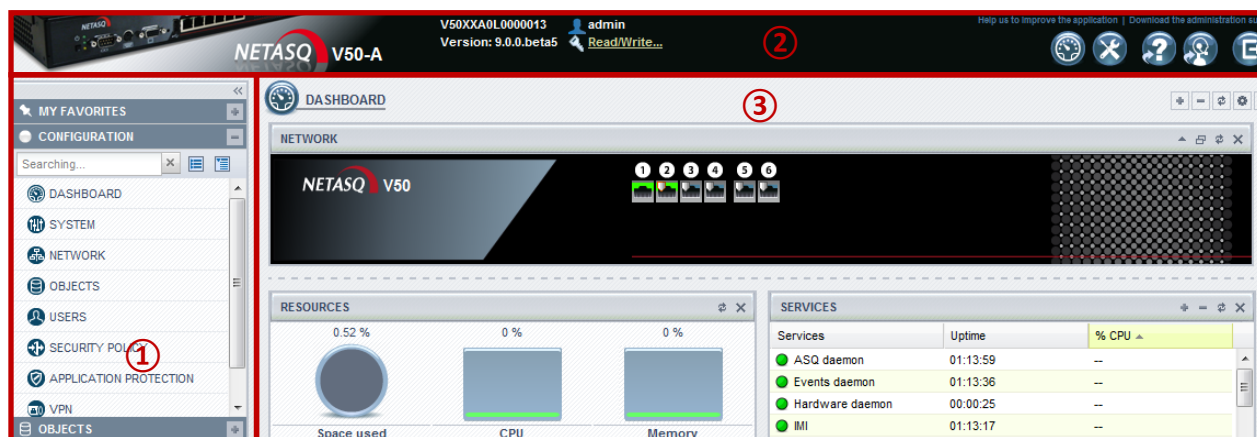
The dashboard provides an overview of the information relating to the firewall's activity and its configuration. The following modules are displayed in different tables:

- Active Update;
- Alarms;
- Interfaces;
- License;
- Hardware;
- Properties;
- Resources;
- Network;
- Services;

For example, the "Licenses" table displays the expiry dates of the various licenses currently valid on the firewall.

#### User friendliness

The web interface consists of 3 sections:



The screenshot shows the NETASQ V50-A web interface. At the top, it displays the device name 'NETASQ V50-A', version '9.0.0.beta5', and user 'admin'. The interface is divided into three main sections:

- Left Sidebar (1):** A navigation menu with categories: MY FAVORITES, CONFIGURATION, DASHBOARD, SYSTEM, NETWORK, OBJECTS, USERS, SECURITY POLICY, APPLICATION PROTECTION, and VPN.
- Top Bar (2):** A navigation bar with 'DASHBOARD' selected and a search bar.
- Main Content Area (3):**
  - NETWORK:** A section with a 'NETASQ V50' logo and a grid of icons numbered 1 through 6.
  - RESOURCES:** A section with three gauges: Space used (0.52%), CPU (0%), and Memory (0%).
  - SERVICES:** A table showing running services.

Services	Uptime	% CPU
ASQ daemon	01:13:59	--
Events daemon	01:13:36	--
Hardware daemon	00:00:25	--
IMI	01:13:17	--

- (1) The browser bar, on the left: it contains the modules arranged in the form of a directory.
- (2) The top banner: it displays the model of the firewall, the name of the user and shortcuts to the dashboard, online help, access to support and preferences.
- (3) Modules, in the center: the configuration of a module appears when it is selected in the browser bar.

### **The browser bar**

It offers several options:

A “Favorites” tab, which can be customized to the user’s needs. This allows grouping the modules most frequently used by the user;

A keyword search area: by clicking on the “Configuration” tab, the user will be able to enter the desired feature in the search field and will find everything relating to the module in question.

Example: by typing “VPN”, the following sub-modules will appear:

- Access privileges
  - Inspection profiles
  - IPsec VPN
  - SSL VPN
  - PPTP server
- 
- A shortcut to objects: allows the user to configure his firewall by dragging and dropping objects, without having to switch windows while getting a more complete view of the available objects.
  - A shortcut to users and groups.

### **The top banner**

From left to right, it sets out:

The model, name or serial number and the version of the operating system.

The logged in user;

Access privileges;

A shortcut to the dashboard;

A “Preferences” shortcut allowing the user to customize the interface’s behavior :

- Access to online help, which will describe the configuration screens of the different modules;
- Access to “Support”, sends the user directly to the support homepage in the NETASQ client and partner areas. Authentication in these areas will be necessary.
- A shortcut to log off.

### **Administration**

In version 8, administrators had to possess an LDAP account (internal or external).

In version 9, administrators of the firewall can be authenticated through several methods:

- LDAP
- SSL
- Radius
- Kerberos

The administration interface is available in 3 languages:

- English
- French
- Polish

### Certificate authentication

The administrator can choose to log on automatically using an SSL certificate, which allows the use of a token and dispenses with the need to enter and therefore transmit the password.

## Network

### Network bridges

In version 9, the maximum number of bridges that can be configured has been increased for the following models:

Product	Version 9: number of bridges	Version 8: number of bridges
U30, U70	4	2
U120, U250, U450	8	4
NG1000-A	16	16
NG5000-A, U6000	24	16

### 10Gbps connectors

The user can add 10-Gigabit fiber network ports by purchasing a new PCI-Express hardware adapter for NG1000-A and NG5000-A products.

## New security policy

### Main points

In version 8, NAT rules were defined separately from filter rules. Furthermore, content inspections (proxy) were enabled in specific modules.

In version 9, address translation is performed together with filtering. This allows assessing network packets in a single operation. However, NAT and filter policies are still displayed in separate tabs for better readability.

Content analyses (antivirus scans, for example) can be attached directly in the security policy in the new “Security inspection” column.

### Protocols

#### Protocol profiles

In version 9, administrators can use up to 10 protocol profiles for each protocol (e.g. for HTTP).

#### Inspection profiles

An inspection profile is a group of protocol profiles. Administrators can associate an inspection profile with a filter rule in the “security inspection” column. These inspection profiles are the equivalent of the 4 ASQ profiles in version 8. In version 9, up to 10 inspection profiles are available.

The combination of protocol profiles and inspection profiles provides the administrator with high flexibility, while avoiding the duplication of certain modifications.

#### Configuration grouped by protocol

In version 8, the configuration of proxies and IPS analyses (“plugin”) for a given protocol (ex: IPS and HTTP proxy) were located in separate configuration modules. In version 9, configuration elements have been grouped within the same protocol profile, accessible in the menu “Application protection - Protocols and applications”.

#### Unified view of alarms with search functions

In version 8, intrusion prevention alarms were grouped according to their protocols (http alarms) or by category. These alarms are now grouped within a single screen which offers a search function and predefined filters. It is still possible to view alarms for a given protocol.

This screen also offers specific displays of new protection methods, in order to identify changes more quickly.

#### Default SSL port

For each protocol, default SSL ports have been defined. They allow forcing the IPS engine to perform SSL inspections. Default ports are the same for all protocol profiles and can be configured by clicking on “Go to global configuration” in the configuration screen of a protocol.

#### Dynamic update of protocols

New protocol/application (“plugins”) scans can be added through automatic updates (Active Update).

### **“Security inspection” column**

A “security inspection” column now appears in the filter policy, which allows directly associating different levels of analysis to a traffic authorization rule (“pass” action).

#### Choice of inspection level

Three predefined modes are available:

- **Intrusion prevention (IPS):** Automatic traffic inspection. This is the default mode if nothing is specified in the inspection column;
- **Intrusion detection (IDS):** scans are performed and alarms are raised when suspicious traffic is detected, but traffic will not be interrupted even if the action has been set to “block”;
- **Firewall:** Level 3 filtering (TCP/IP). Traffic will not be blocked and alarms will not be raised, regardless of the configuration.

#### Content filtering

This feature allows activating the analyses performed by proxies, which takes place transparently for the user.

- **Antivirus** : antivirus scan on Http(s), SMTP(s), POP3(s), and FTP protocols;
- **Antispam** : antispam scan on SMTP(s), POP3(s) protocols;
- **URL filtering** : associates a web filter policy;
- **FTP filtering** : filters FTP exchanges;
- **E-mail filtering** : associates an SMTP and POP3 filter policy;
- **SSL filtering** : associates a filter policy with SSL decryption rules (“decrypt” action) according to the certificate (CN).

### Rule creation wizard

A wizard that allows creating standard rules, authentication rules, SSL inspection rules and explicit HTTP proxy rules, has been set up. It guides the administrator throughout the whole process of creating rules.

Example: it is possible to define a rule that allows redirecting users to the authentication portal.

### “Internet” object

The “Internet” object takes on the default value of “!Networks\_internals” (negation of the automatic object “Network\_internals” which includes all protected networks) and avoids unnecessarily using the “any” object in the security policy.

The value of the Internet object can be modified in the “Network objects” menu. The value “!rfc3330”, for example, can be assigned to it (the rfc3330 group is included in the default configuration).

### “Unknown users” object

The “Unknown users” object is linked to the use of the HTTP proxy. This will allow unauthenticated users wishing to access the internet to be redirected to the captive portal so that the user can indicate his login and password.

### Scheduling by rule

Time objects, which are making their appearance in version 9, allow scheduling when one or several filter rules will be activated. It is possible to create events of the following frequencies:

- Weekly
- Annual
- One-off

## NAT policy

### General points

NAT is now managed by the same evaluation engine used for filtering. The address translation module has been completely rewritten and now benefits from a new syntax. In version 8, a name of an action (map, bimap, rdr) was used to describe the NAT operation. In version 9, a whole table (source, destination) is now available for traffic before and after translation.

There are many advantages to this new architecture:

- Translation rules are assessed in order of their appearance, regardless of their scope.
- More combinations are available. For example, a NAT operation can be performed on both the source and the destination within the same rule.

#### Interaction with the filter policy

In version 9, the filter policy is systematically assessed on original packets, before any NAT operation. For example, when the administrator wishes to allow access to an internal server (mail server) from the internet, the public IP address of this server (before the translation operation) has to be indicated as the destination in the filter rule.

Note: in version 8, for the same filter rule, the private IP address of the server would have had to be indicated.

This change has been made in order to allow:

- Ensuring that all rules (filter and NAT) are assessed based on the original packet;
- Ensuring that a single assessment of the incoming network packet would be enough for applying NAT and associating the right filter rule;
- Managing the rewriting operations requested by NAT from the first packet onwards. This is necessary for example when rewriting IP addresses in SIP packets.

#### Load distribution by destination

Two new load balancing modes by destination appear in this version:

- **Random:** Traffic is randomly distributed between each server;
- **Source IP hashing:** the same translation operation will be applied systematically for a given source IP address.

Round-robin mode already existed in version 8 (rotation on all servers upon each new connection).

## SSL inspection

### General points

A new proxy has been added: the SSL proxy, whose objective is to decrypt and analyze data. The firewall acts as a middleman (“man in the middle”) between the client and the server in order to decrypt the SSL traffic and inspect the encapsulated traffic.

Fully transparent to the user, the encrypted request to the server is intercepted by the SSL proxy which:

Substitutes for the web browser: the SSL proxy will negotiate a connection with the web server

Takes on the role of the web server: it generates an ad hoc certificate and uses it for the negotiation with the client.

2 connections will therefore be established: between the client and the SSL proxy, but also between the SSL proxy and the server. The proxy can therefore decrypt data originating from the client and encrypt them again before sending them to the server. This decryption and encryption operation is also carried out for traffic sent by the server to the client.

Once the proxy has decrypted the traffic, the IPS as well as the HTTP, SMTP and POP3 proxies will be able to analyze the data.

### Configuration of the SSL inspection

#### Enabling SSL decryption from the filter policy

It is now possible, in the security policy, to define a rule with the “decrypt” action in order to decrypt SSL traffic and assign a specific SSL filter policy to it. This action will indicate to the firewall that:

- The SSL filter policy defined in the “Security inspection” column has to be assessed,
- The rules that follow in the security policy apply to the encapsulated traffic, once it has been decrypted.

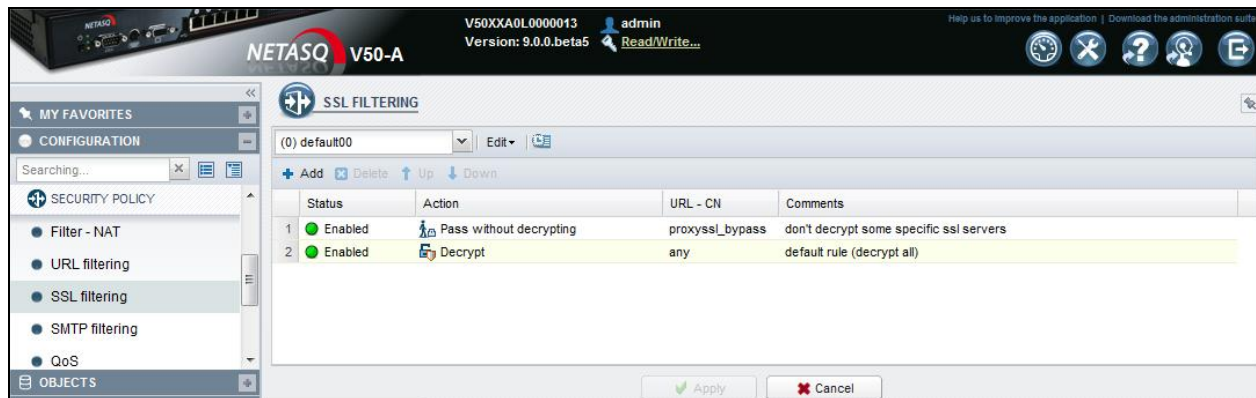
#### SSL filter policy

In the SSL filter policy, the administrator defines the behavior of the SSL proxy according to the information given by the destination server. 3 actions are possible:

- **“Block without decrypting”**: the connection will be blocked as soon as the SSL negotiation takes place, the user will not be allowed to access the site.
- **“Pass without decrypting”**: lets SSL traffic pass through without decrypting it;
- **“Decrypt”**: SSL traffic is decrypted then analyzed before being sent to server.

The “Category” column may contain a URL filter group or a certificate group.

Example:



**NOTE**

The “block without decrypting” function is a performance optimizer, but should not be considered a security feature. Indeed, it only applies if the domain name is in the category. For example, “sex.com” is in the pornography category, but “example.com/porn” would not be blocked by this action and would require traffic decryption.

## Proxies

### Keep source IP address

Connections intercepted by the various proxies can be resent with their original IP addresses. This behavior can be configured in the protocol profiles. This option is enabled by default in the inspection profile O1, assigned to incoming connections. This concept of a virtual connection enables, in particular, applying QoS on a filter rule for which content inspection has been defined.

### FTP proxy

This proxy has been upgraded in order to ensure better integration with FTP servers. It provides protection to servers during file transfers. An antivirus scan is run on downloads and/or uploads.

### Explicit HTTP proxy

The explicit HTTP proxy can be enabled directly from the filter policy, via the “action” field.

In the same way as for the SSL proxy, the rules that follow in the filter rule will apply to encapsulated traffic. A source criterion (“**via explicit HTTP proxy**”) in the source field can be associated with one of these filter rules: the rule will apply only to traffic from the explicit HTTP proxy.

### **POP3 and SMTP proxies**

By default, POP3 and SMTP proxies block partial messages in order to prevent them from bypassing antivirus scans.

## **High availability**

### **Synchronization of firewalls**

Configurations and sessions (traffic) are synchronized on average every 0.02 seconds. This synchronization is incremental in order to withstand significant network loads.

### **Reboot of backup appliance**

In version 9, the backup appliance will need to be rebooted only when the following changes are made:

- Network configuration;
- Objects;
- Time zone.

### **Switching to the backup appliance**

Failure detection now takes less than 1 second.

### **SNMP monitoring**

Specific elements in the high availability configuration can now be accessed:

- Number of hosts connected;
- Status/modes of the firewalls;
- Quality;
- Status;
- Priority;
- Status of links (in MIB-II databases).

### **Session backup**

Active session tables are the same for all sessions (translated and untranslated).

Sessions that operate with NAT will also be synchronized.

The table of authenticated users will also be transferred, so that these users will not need to re-authenticate after a switch.

## **IPSec VPN**

The IPSec VPN module has been enhanced to provide the following features:

### **X- Auth**

Extension allowing the user to authenticate with a VPN gateway using a classic login/password.

### **“Config” mode**

Automatic distribution of address ranges through the VPN tunnel and the DNS server.

### **Backup VPN tunnel**

High availability (H.A) of IPSec tunnels or “backup” configuration.

### **iPhone® compatibility**

A new type of mixed authentication allows simplifying the configuration of a mobile tunnel with iPhones.

## **System**

### **Automatic update of licenses**

The firewall will automatically search for, download and install new licenses. The user no longer needs to reboot the firewall for practically all updates (especially changes to the dates of the various services and options). This option can be configured.

### **DHCP relay**

The DHCP relay intercepts and sends the DHCP request to a server located on another network.

### **PKI: smartcard logon**

The public key infrastructure management module has been enhanced in version 9 in order to support authentication by smart cards. Indeed, the appliance generates a PKI (or a key/ server certificate infrastructure) which can now generate certificates that can be converted on specific smart cards.

In version 9, the PKI is “multi-level” (a certificate can generate certificate authorities for various applications).

### **Quality of service (QoS)**

In version 9, a “default queue” field allows assigning a default queue to traffic. If the user does not assign a queue to define priority traffic, the default traffic will have priority over all other queues.

## **Users**

### **Local storage of proprietary attributes**

In version 8, in order to use certain features on the firewall, the administrator had to modify the structure of the LDAP server or Active Directory. Now, NETASQ modules operate without the need to modify the attributes of user directories. The different attributes specific to NETASQ features are directly managed by the firewall. Connecting to the user database is therefore all it takes to benefit from all the features of the firewall.

### **Privileges for user groups**

In version 9, privileges can be assigned not only to users but also to user groups.

### **Authentication portal**

The authentication portal has been modified to include the “login” and “password” fields on the same page.

## Intrusion prevention

### **SYN proxy**

Protection from denials of service attacks has been improved to include the configuration of the SYN proxy directly in filter rules. When a connection is established, the firewall will intercept the SYN packet and respond on behalf of the server to confirm that the request is legitimate.

### **SIP: support Early Media (RFC 3960)**

“Early Media” refers to the establishment of a media channel (RTP) before the callee picks up. This allows sending an “on hold” ringtone before ending the negotiation phase. Internally, this protocol relies on NAT rules and also synchronizes during high availability.

### **Multi-packet application detection**

The identification of an application may require the reading of several network packets. To avoid sending traffic to a recipient without having identified the protocol, the attack prevention engine will desynchronize traffic until it has reconstructed enough data to identify the protocol or the application. It has an intelligent built-in session desynchronization mechanism to avoid blocks due to the exhaustion of the TCP window.

### **Application filtering for instant messaging**

File transfers via instant messengers (AIM, ICQ, Windows Live Messenger and Yahoo) can be blocked. For this, it is necessary to use different instant messaging protocols on security policy of the firewall.

Messages sent by the user to the server are now inspected. If the packet appears to be invalid, the message will be blocked.

### **SMTP protocol**

The SMTP protocol scan benefits from the following additions:

- Checks on the validity of command parameters;
- Protection from buffer overflows;
- Blocking of customizable commands;
- Ability to block Exchange extensions;
- Zero-day protection

### **TFTP protocol**

Intended especially for file transfers on VoIP telephones, this protocol is subjected to a full scan and its parameters will be checked.

## Web application IPS

In order to block multiple attacks from the web and to protect user data in the best way possible, 3 new patented technologies have been added for the HTTP protocol.

### **Html and JavaScript analysis**

The intrusion prevention engine scans html and JavaScript embedded in web pages, which benefit from dedicated protection contexts.

### **Normalization of code before inspection**

This technology has been added to normalize html as well as JavaScript in order to provide protection from application evasion attempts.

### **Real-time disinfection**

A configurable rewriting system has been set up to extract and delete any malicious code (html or JavaScript) on the fly without interrupting the connection or using the proxy.

## **Log reading**

### **NETASQ Event Reporter**

A new type of “SSL” log makes its appearance to log events relating to the decryption of SSL traffic. Additional information such as source and destination addresses on FTP and SSL VPN logs also appear.

### **End of life for Collector / Reporter Pro / Auto-Report / Syslog**

The modules for collecting logs (“collector”), the NETASQ syslog server, the report generation engine (“Autoreport”) and reading of logs from a database have been deleted in version 9.

They have been replaced with the NETASQ Event Analyzer solution.

### **Access to logs on U30/U70 models**

For U30 and U70 firewalls, it will now be possible to view the last 64 lines of logs for each category.

## 9.0.0 Bug fixes

---

### Intrusion prevention

#### Routing and anti-spoofing

Support reference 16383

“Anti-spoofing” protection mechanisms now manage the overlap of networks and static routes on different interfaces.

### Network

#### MTU value set to 1500

Support reference 17726

The default MTU value has been set to 1500 bytes for all interface types, including VLAN and bridge interfaces.

#### DHCP server

Support reference 24094

The DHCP server’s ability to assign IP addresses has been modified to impose a limit that would prevent the instability of the module in the event of an overload:

- U30 to U70: 256
- U120 to U450: 4096
- U1100, U1500 and NG1000: 8192
- U6000 and NG5000: 16384

### Proxies

#### Antispam module

Support reference 14527

Whitelists and blacklists are no longer restricted by the number of characters but by the number of entries. The limit is set to 256 lines for both lists.

### IPSEC VPN

#### Dead Peer Detection (DPD)

Support Reference 12025

When the ISAKMP SA (phase 1) expires, it will automatically be renegotiated in order to allow sending and receiving DPD messages.

### System

#### Daylight saving time

Support Reference 14785

The events manager (eventd daemon) has been fixed to take into account daylight saving time.

#### Time zone

Support Reference 18587

The events manager (eventd daemon) has been fixed to take into account changes to the time zone.

#### SNMP

Support Reference 16598

SNMP “traps” are sent even if a field is empty.

### Reporting

Support Reference 23989

To improve the readability of HTTP logs, logs for the HTTP proxy and HTTP IPS are now separated in the same way as for other proxies.

---

## Known issues

---

### Intrusion prevention

#### **Web 2.0**

The rewritten html code is not compatible with all web services (apt-get, Active Update) as the "Content-Length" header has been deleted.

#### **Instant messaging**

NAT is not supported on instant messaging protocols.

#### **Certificate revocation list (checkcrl)**

The consultation frequency or date of certificate revocation lists (CRLs) cannot be configured.

#### **High availability / routing by policy**

The ID of the connection router is not transferred to the passive firewall. As a result, a session routed by the filter policy may get lost when the cluster is switched.

#### **SSL proxy**

The IPsec VPN does not support the ICAP server's validation of HTTPS requests decrypted by the SSL proxy.

### High availability

#### **Restriction on high availability in bridge mode**

In an environment with a firewall cluster configured in bridge mode, it has been observed that the traffic switchover took about 10 seconds. This duration is related to the switchover time of 1 second, to which the time taken for switches to relearn MAC addresses will be added.

### VPN IPsec

#### **PKI**

The presence of a certificate revocation list (CRL) is not required. If no CRL has been found for the certificate authority (CA), the negotiation will be allowed.

#### **X-Auth**

Authentication module via X-Auth (IPsec) is incompatible with LDAP "realbind" connection option.

### Web administration interface

#### **Users**

The creation of several users with the same login is not prohibited, but is not compatible with user authentication.

## Network

### Routing

Support reference 28437

Load balancing does not function if the high availability link option has been disabled.

## NAT

Support reference 29286

Status management for the GRE protocol is based on source and destination addresses. Two connections to the same server at the same time, either with the same client or sharing a common source address, therefore cannot be differentiated (when "map" is used).

### H323 support

The H323 protocol's support for address translation operations is rudimentary, in particular: it does not support NAT bypass by gatekeepers (announcement of any address other than the connection's source and destination).