

# NETASQ Firewall - UTM Version 8.1.5.1

## Highlights

---

- Virtual appliance
- Real time monitoring

### Level of modification

---

|                      |       |                   |       |
|----------------------|-------|-------------------|-------|
| Filter policy        | None  | Proxy             | None  |
| SSL VPN              | None  | High availability | None  |
| Administration Suite | Minor | Operating system  | Major |
| ASQ                  | None  | Real time monitor | Major |

---

## Software compatibility

---

Minimum version required: 7.0.0

---

Minimum version required for H.A: 7.0.0

---

## Hardware compatibility

---

|               |          |
|---------------|----------|
| F25*          | U30      |
| F50*          | U70      |
| F60           | U120     |
| F200          | U250     |
| F500          | U450     |
| F800          | U1100    |
| F1200         | U1500    |
| F2000 – F2500 | U6000    |
| F5000 – F5500 | NG1000-A |
|               | NG5000-A |

\*: with restrictions (see facing column)

### Virtual Appliances

---

|      |      |
|------|------|
| V50  | VS5  |
| V100 | VS10 |
| V200 | VU   |
| V500 |      |

---

### Compatibility restrictions

---

The antivirus module will no longer be functional on F25/B, F25/C and F50/C products.

During the update procedure, the module will be disabled and the antivirus database will be deleted.

---

## Contents

---

### Version

---

|         |                          |  |                           |                              |
|---------|--------------------------|--|---------------------------|------------------------------|
| 8.1.0   | <a href="#">Features</a> | <a href="#">Resolved vulnerabilities</a> | <a href="#">Bug fixes</a> |                              |
| 8.1.1   | <a href="#">Features</a> | <a href="#">Resolved vulnerabilities</a> | <a href="#">Bug fixes</a> |                              |
| 8.1.2   | <a href="#">Features</a> | <a href="#">Resolved vulnerabilities</a> | <a href="#">Bug fixes</a> |                              |
| 8.1.3   | <a href="#">Features</a> | <a href="#">Resolved vulnerabilities</a> | <a href="#">Bug fixes</a> |                              |
| 8.1.4   | <a href="#">Features</a> | <a href="#">Resolved vulnerabilities</a> | <a href="#">Bug fixes</a> | <a href="#">Known issues</a> |
| 8.1.5   | <a href="#">Features</a> | <a href="#">Resolved vulnerabilities</a> | <a href="#">Bug fixes</a> | <a href="#">Known issues</a> |
| 8.1.5.1 |                          |  | <a href="#">Bug fixes</a> |                              |

## 8.1.0 Features

### System

#### Virtualization

The software system on NETASQ products has been upgraded in order to manage the new range of virtual equipment (NETASQ Virtual Appliance).

#### New equipment

The software system on NETASQ products has been modified to integrate new equipment from the NETASQ range – NG1000-A and NG5000-A.

### IPSEC VPN

#### IKE Protocol

The module that manages the IKE protocol has been updated. IPSec-tools are now in version 0.7.3.

### NETASQ REAL-TIME MONITOR

#### Alarm panel

Several enhancements have been made to the panel listing the alarms found on an appliance.

- The **Alarms** panel has now been named **Events**.
- The **Events** panel now displays different types of information: alarm, web, virus, mail, FTP, filter and connection.
- The default column display has been modified.
- The number of columns present has increased.
- A new “details” column allows the display of relevant information regardless of the source log file.
- A drop-down list enables the selection of a predefined filter on the information presented:
  - Filter by alarm events
  - Filter by information regarding viruses
  - Filter by connection events
  - Filter by web events
  - Filter by mail events
  - Filter by FTP events
  - Filter by filter events

The aggregation of different types of information provides a synthetic view of important events. The use of predefined filters ensures real help when monitoring the security policy.

#### Filter function

An advanced filter feature is available on most tables in the NETASQ REAL-TIME MONITOR application. As such, all information can be filtered by one or several columns using the following operators:

- Equals
- Contains
- Starts with
- Ends with

- Use of the joker character (?, \*, [...])
- Regular expression (cf <http://qt.nokia.com/doc/4.5/qregexp.html>)
- Use of a negation operator

Once a filter has been applied on a column, a specific icon will appear.

## Refreshment of information

The frequency of data refreshment has been modified. The refreshment value can now be set to 1 second in order to obtain real-time information.

## 8.1.0 Resolved vulnerabilities

### NS-BSD

The `security.bsd.map_at_zero` parameter on `sysctl` has been disabled in order to follow the recommendation `FreeBSD-EN-09:05.null`.

## NETASQ EVENT REPORTER

The NETASQ EVENT REPORTER product has been modified in order to offer a new version of the database. Version 8.3.9 of PostgreSQL includes fixes for the following vulnerabilities:

- Error in the management of the `'/'` character in the “**domain name**” field which could cause man-in-the-middle attacks in order to hijack an SSL session on the database server (CVE-2009-4034).
- Ability to obtain more privileges with a valid login (CVE-2009-4136)

## 8.1.0 Bug fixes

### ASQ Engine

#### TCP: Resending of SYN

**Support reference: 20989**

The retransmission of SYN packets is no longer blocked once the SYN/ACK exchange has taken place.

#### HTTP Plugin: “Proxy-Connection: keep-alive” field

**Support reference: 18836**

The “Proxy-Connection: keep-alive” header field of the HTTP/1.0 protocol is now managed.

#### HTTP Plugin: “Content-Length” field

**Support reference: 20058**

“Content-Length” values higher than 4 GB (full 32 bits) are now correctly managed.

#### HTTP Plugin: truncated POST query

**Support reference: 20193**

The transfer of the truncated POST query is now supported.

## SYN flooding

Protection from SYN flooding on internal networks has been improved. The ASQ engine reinitializes the connection attempts to the servers of the protected network according to the value of the “SYN timeout” parameter. This allows servers to free up their resources more quickly.

## SSL Plugin

The SSL plugin has been enhanced in order to better handle “TLS hello” messages sent by clients using a higher version of TLS than the server’s. This allows supporting in particular HTTPS negotiations of the Opera 10.50 application.

## Proxy

### HTTP Plugin: “Content-Length” field

**Support reference: 20058**

“Content-Length” values higher than 4 GB (full 32 bits) are now correctly managed.

### Explicit HTTP Proxy

The proxy will no longer shut down upon detection of a null character in a header. An error page will be presented to the end user instead.

## Memory leak

Several memory leaks concerning proxies and the PKI module have been fixed.

## SSL VPN

### Java proxy parameters

**Support reference: 19649**

The Java applet now takes into account Java proxy parameters.

### User profiles

**Support reference: 19864**

During user authentication, if the SSL VPN profile of the user is unknown, it will be loaded dynamically (in the event of the creation of a new user or a new profile on an external LDAP).

### Full access

**Support reference: 21824**

Quote marks in commands to be executed during connections are now correctly supported.

## Improved compatibility

Compatibility for accessing Google through the SSL VPN has been improved.

## PKI

### Enrolment

The selection of the encryption level of the portal was not correctly displayed by Internet Explorer 8 in Windows Vista. This anomaly has been fixed.

## System

### SNMP Module: memory leak

**Support reference: 20335**

The net-snmp module has been updated to version 5.4.2.1. This version fixes a problem with memory leaks in the snmpd daemon.

### Active Update

**Support reference: 20887**

The message “Master updates are scheduled the (...) of each month, today is the (...) => WON'T do master update today” will no longer be displayed during the execution of the autoupdate command with the force option -f.

### Serverd connection

**Support reference: 20729**

The maximum size of the DN (Distinguished name) field for the “USER” commands has been increased from 128 to 1024 bytes.

### High availability

In order to prepare for an unexpected change of equipment, the quality of the interfaces is no longer calculated during the network activation command “ennetwork”.

## NETASQ UNIFIED MANAGER

### Management of high availability

**Support reference: 18145**

Backups on the backup partition are now systematically made on the active appliance in the cluster. The appliance targeted by the system backup command no longer depends on the value of the “passive update” parameter.

### HTTP Plugin

The maximum size of the buffer for the management of cookies has been increased from 4096 to 65 536 bytes.

### PKI / LDAP

Starting up the LDAP configuration wizard from the PKI screen after having been disconnected caused the application to crash. This anomaly has been fixed.

# NETASQ EVENT REPORTER

## Migration of the Collector module

**Support reference: 17956**

A warning message has been added to the migration phase from version 7 to version 8 of the Collector module. This message will inform the user that older logs will no longer be migrated automatically. In order to perform the migration, the logs will have to be exported in version 7 then imported in version 8.

## 8.1.1 Features

### Intrusion prevention (ASQ)

#### SMB/SMB2 analysis

Analyses of the Microsoft NB-CIFS and NB-SSN protocols have been improved in order to block the exploitation of the following vulnerabilities:

- CVE-2010-0270: buffer overflow on the SMB protocol with the possibility of remote exploitation for Windows 7 and Windows 2008 R2.
- CVE-2010-0476: possible denial of service on the SMB protocol affecting Windows 2003 SP2, Windows Vista Gold, Windows Server 2008 Gold and SP2.
- CVE-2010-0269: buffer overflow on the SMB protocol with the possibility of remote exploitation on Windows 2000 SP4, Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista Gold, SP1, SP2 and Windows Server 2008 Gold, SP2 and R2 and Windows 7.
- CVE-2010-0477: remote execution of arbitrary code on the SMB2 protocol, affecting Windows Server 2008 R2 and Windows 7.

For these protections, the alarm "Invalid NBSS/SMB/SMB2 protocol" (id 157) has been split into two distinct alarms:

- **"Invalid NBSS/SMB2 protocol" (id 157):** is raised when several types of malformed NBSS/SMB2 packets are detected.
- **"Invalid NBSS/SMB protocol" (id 158):** is raised when several types of malformed NBSS/SMB packets are detected.

These alarms are "Sensitive". If configured to "Pass", their detection involves the detachment of the associated plugin. By default, these alarms are set to "Block, Minor"

#### DNS analysis

The DNS plugin blocks attempts to exploit the following vulnerability with the alarm "Invalid DNS protocol" (id 88):

- CVE-2010-0024: denial of service on the MX analysis affecting Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP2, Server 2008 Gold, SP2 and R2, and Exchange Server 2003 SP2.

## 8.1.1 Resolved vulnerabilities

### ClamAV

**Support reference: 22489**

A vulnerability relating to a denial of service through specially-forged PDF files has been fixed. (CVE-2010- 1639).

### PostgreSQL

PostgreSQL has been upgraded to 8.3.11. This version fixes the following vulnerabilities:

- CVE-2010-0442 (fixed in version 8.3.10)
- CVE-2010-1169
- CVE-2010-1170

## 8.1.1 Bug fixes

### ASQ

#### Limits for profile 00

**Support reference: 22930**

The limits defined in ConfigFileS/ASQ/00 (filter rules, hosts, users and maximum queue size) have been applied again.

### SMB2 analysis

A false positive in the SMB2 protocol analysis has been fixed.

### SEISMO

The encoding of accented characters in SEISMO messages has been repaired.

### IPSEC VPN

#### NAT Traversal (NAT-T)

**Support reference: 21483**

Improved stability for IPSec configurations that use NAT-T.

#### Memory leak

**Support reference: 21936**

A memory leak which could alter performance on certain configurations that use many anonymous IPSec peers has been fixed.

## SSL VPN

### Rewriting

**Support reference: 21808**

The rewriting of Javascript and HTML by SSL VPN has been improved.

## Proxy

### HTTP Proxy: “Content-Length” field

**Support reference: 22375**

Tabs or spaces after the “Content-Length” value are no longer blocked by the HTTP proxy.

### SMTP Proxy and Antivirus

**Support reference: 21163**

Certain large e-mails would sometimes be duplicated during their transmission to the server via the proxy

## System

### High availability

**Support reference: 22293**

An issue with the reboot of the hardware daemon that could arise with the use of Watchdog has been fixed.

### MTU of VLAN

**Support reference: 22572**

U70, U120, U250 and U450 models: to set the MTU of a VLAN to 1500, it is no longer necessary to increase the MTU of the parent interface to more than 1500.

### External LDAP

**Support reference: 21870**

Spaces in the “Distinguished Name” (DN) are now better supported.

### Authentication

**Support reference: 22424**

A more detailed message now appears on the authentication portal when the Kerberos password has expired.

### DHCP server

**Support reference: 22520**

The activation of the server no longer fails if an error occurs on a single machine (e.g.: MAC address deleted). The error will be ignored so that the DHCP service will not be shut down for other devices.

## Syslog

The size of logs sent by Syslog has been restricted to avoid exceeding 1024 bytes (limit imposed by RFC 3195). The affected logs are:

- Alarm logs: The contents of a packet will no longer be sent if it causes the limit to be exceeded.
- Web logs: If the *arg* field (containing the URL) takes too long to transmit the log, the URL will be truncated (512 bytes).

## NG1000-A, NG5000-A

The restoration of a configuration on a U or F model to an NG model now takes into account their administration ports. They will remain available after the restoration.

The wizard now handles administration ports correctly.

## Real-time Monitor

### Dashboard

**Support reference: 22250**

A problem with the display of CPU consumption graphs on the dashboard has been fixed.

### Events

**Support reference: 22331**

VPN and system events are no longer duplicated during refreshment.

## 8.1.1.1 Resolved vulnerabilities

### System

**Support reference: 23407**

The ARP request management module has been updated to fix a vulnerability. In some configurations, when the NETASQ appliance is forced to send out a large number of ARP requests without responses, a denial of service may occur.

## 8.1.1.1 Bug fixes

### System

#### Serverd connection

**Support reference: 23473**

The tracking of Active Update command statuses could cause the NETASQ REAL-TIME MONITOR application to freeze. This anomaly has been fixed.

## 8.1.2 Features

### ASQ engine

#### HTTP and DNS plugin

3 new signature contexts have been created to provide more effective and accurate protection:

- http:client:useragent
- http:client:cookie
- tcpudp:hostname

#### Important note

Some signatures from the context http:client:header have been moved to the new contexts mentioned above. Furthermore, some of the new protection methods will only be available for these contexts.

#### “hostname” context

The context “tcpudp:hostname” applies to the “hostname” fields in HTTP and DNS requests. It embeds many signatures that allow identifying various websites. As such, a hostile site will be blocked based on either the DNS request or the HTTP request. This function optimizes performance in particular as it prevents unnecessary HTTP requests by prohibiting DNS resolution towards a malicious site.

#### Alarm configuration

The protocol alarm “Packet with destination on the same interface” (ID 95) is now a “Sensitive” alarm, and can as such be configured to “Pass”. This configuration allows the exchange of packets between 2 hosts connected on the same interface and in the same network as the firewall, without having to configure the “Bypass” rule.

## System

#### Management interface

**Support reference: 22647 and 23729**

Administration connections are now allowed on the “out” interface (port 1) in the default configuration via an explicit rule. As such, the filter policy enabled by default (01 – “Block all”) will allow administration connections on all interfaces. In this case, a new group object in read-only mode, named “Firewall\_all” containing “Firewall\_\*” objects, is used.

#### Hardware supervision

The hardware supervision module (watchdog) is enabled in the default configuration (300 seconds). In earlier versions, this module was only enabled for appliances configured in high availability.

## Virtual Appliance

### Disk space

**Support reference: 22755**

The disk capacities on NETASQ Virtual Appliance models have been increased. The new values are:

| Virtual Appliance models | Disk space          |
|--------------------------|---------------------|
| V50, V100, V200 and V500 | Storage space: 10GB |
| VS5, VS10 and VU         | Storage space: 15GB |

### High availability

NETASQ Virtual Appliance models can now be configured in high availability.

## 8.1.2 Resolved vulnerabilities

### ClamAV

**Support reference: 24233**

The ClamAV engine has been upgraded to version 0.96.3 in order to fix a memory overflow vulnerability (CVE-2010-0405) that can cause a denial of service and probably the execution of code using a specially-forged compressed file.

Note: From version 6.2 onwards, the ClamAV server has been functioning without any privileges.

### PostgreSQL

The PostgreSQL database has been updated to version 8.3.12 in order to fix a vulnerability (CVE-2010-3433) that can cause a possible increase in privileges using a specially-forged script code.

## 8.1.2 Bug fixes

### ASQ engine

#### Filter rules

**Support reference: 24439**

The reloading of a filter policy with corrupt objects has been improved:

- Filter rules will no longer be purged after 2 consecutive reloads
- If the firewall is rebooted with a filter slot that cannot be loaded, all implicit rules will be loaded.

#### FTP plugin

**Support reference: 16787**

The FTP commands MLST and MLSD are no longer considered as unknown commands.

## SMTP plugin

**Support reference: 20147 and 24007**

A false positive in the SMTP analysis has been fixed. This bug would sometimes cause the alarm "Bad TCP sequence number" to be raised.

## SMB2 plugin

A potential false positive in the analysis of SESSION SETUP requests has been corrected.

## Proxy

### URL filters

**Support reference: 24227**

The possibility of bypassing URL filter rules by using specially-forged URLs has been fixed.

## SSL VPN

### Lotus Domino

**Support references: 23309, 23007 and 24926**

Version 7.0.4 of Lotus Domino Web Access is now better supported. The correction of this bug required the use of a specific configuration attribute for Zimbra mail servers. This attribute can be configured in the serverd management protocol.

### OWA 2007 and 2010

**Support reference: 23090**

Support for internet links in e-mails has been corrected.

### Zimbra

**Support reference: 23259**

Support for internet links in e-mails has been corrected.

## IPSEC VPN

### Removal of the SA

**Support reference: 21809**

The removal of the SA in a heavy traffic context could cause a system crash. This anomaly has been fixed.

## System

### Resumption of configuration synchronization in high availability

**Support reference: 19748**

The synchronization process has been enhanced with the addition of a mechanism that allows backtracking in the event of a process failure. This allows preventing the potential loss of configuration files on the passive appliance.

### Configuration synchronization in high availability

**Support reference: 22852 and 24702**

The reliability of the synchronization process has been improved in order to prevent the occurrence of either unexpected switches during treatment or the appearance of an active-active state.

### High availability status

**Support reference: 23638**

The stability of the hacheckstatus tool has been improved especially in a usage context of the encrypted syslog module.

### PPTP VPN

**Support reference: 19504**

A bug that could cause packet loss has been fixed.

### Gateway management

**Support reference: 24231**

Using the encrypted syslog feature could cause the route management module (gatemon) to crash. This anomaly has been fixed.

### ARP failure on VLANs

**Support reference: 23361**

An issue regarding the failure of ARP resolution on VLANs attached in bridge mode to the same parent interface has been fixed. This anomaly affected U70, U120, U250 and U450 products.

### Authentication portal

**Support reference: 24483**

A translation error has been fixed on the Polish version of the portal.

### Software update via USB key

The software update process via USB key has been simplified as follows:

- If the key contains a single file with a .maj extension, it will be applied regardless of the file name
- If there are several update files available on the key, they will need to comply with the nomenclature fwupd-<version>-NETASQ-<buildmodel>.maj (where <buildmodel> may take on one of the following values: S, M, L, XL)

## Kaspersky daemon

The bug that failed to apply the deactivation of the Kaspersky module has been fixed.

## Virtual Appliance

### Naming of images

**Support reference: 23051**

The file names of virtual images (.ova extension) have been modified. Models and image files are now associated as follows:

| Virtual images | Virtual Appliance models |
|----------------|--------------------------|
| VM             | V50, V100, V200 and V500 |
| VS-VU          | VS5, VS10 and VU         |

## NETASQ Unified Manager

### Updating the passive appliance

**Support reference: 22672**

Beginning in version 8.1.0, the checkbox "Update passive" did not function correctly. This bug has been fixed.

### Updating the application

**Support reference: 23296**

Despite the existence of a new version of the NETASQ UNIFIED MANAGER application, the update button remained grayed out. This bug has been fixed.

### Managing scripts

**Support reference: 24971**

The interruption of the execution of scripts on several appliances without error returns has been corrected.

## NETASQ Real Time Monitor

### Retrieving events

**Support reference: 23032**

The use of different time zones between an appliance and the application caused the retrieval of events to fail. This bug has been fixed.

### Dashboard

The time zone is now displayed with the time.

## Active Update

The status "Consecutive failures" is now supported in the download tracking panel Active Update. This status, introduced in version 8.1.1, corresponds to several consecutive failures when downloading signature databases.

## SEISMO

The list of operating systems would be incomplete after forced manual updates of a host's operating system. This bug has been fixed.

## 8.1.2.1 Resolved vulnerabilities

### ClamAV

**Support reference: 25566**

The ClamAV engine has been upgraded to version 0.96.5 in order to fix several vulnerabilities (CVE-2010-4260, CVE-2010-4261 and CVE-2010-4479) that may cause denial of service attacks and possibly the execution of arbitrary code.

Note: From version 6.2 onwards, the ClamAV server has been functioning without any privileges.

### OpenSSL

**Support reference: 25567**

The OpenSSL module has been upgraded to fix a vulnerability (CVE-2010-4180) that may lower the encryption level of SSL connections.

## 8.1.2.1 Bug fixes

### SSL VPN

#### Authentication portal

**Support reference: 25556**

Following an upgrade to version 8.1.2, the SSL portal was no longer able to run using certificates. This anomaly has been fixed.

## 8.1.3 Features

### ASQ engine

#### HTTP plugin

New protection methods have been added to the HTTP plugin in order to prevent the exploitation of the following vulnerabilities:

- Spoofing of the name of a downloaded file by overloading it with specific Unicode characters (CVE-2009-3376). These characters come from alphabets that are written from right to left. Upon detection of an overload, a new alarm ("*Suspicious unicode reading direction reversal character in URL*" - ID161) will be raised. This alarm is set by default, to "block", "major".
- Duplication of HTTP parameters (HTTP parameter pollution) to transmit an attack on several parameters that bear the same name, with the second overloading the first. This mechanism allows disregarding mechanisms that offer protection by standard signatures. The duplication of parameters in a URL is now blocked with the new alarm "*HTTP parameter pollution attempt*" (ID160) which is set by default to "block", "major" in the "High" ASQ profile and to "pass", "minor" in the other profiles.

### IPSEC VPN

#### SHA2 certificate

**Support reference: 22201**

The IPsec VPN authentication module now supports the use of certificates signed with SHA2 (SHA-256).

#### HMAC SHA2 signature

**Support reference: 18635**

The use of SHA2 (HMAC-SHA2) is now supported during the establishment of Phase 2.

### System

#### OpenSSL

The OpenSSL module has been upgraded to version 1.0.0.c

#### Syslog

**Support reference: 26192**

The configuration of the syslog module allows modifying the location of the "*logtype*" parameter in a syslog event.

## 8.1.3 Resolved vulnerabilities

### OpenSSL

**Support reference: 20740**

The OpenSSL module has been upgraded with the implementation of RFC 5746 in order to fix a data injection vulnerability during the negotiation of the TLS protocol (CVE-2009-3555).

### TCP

A new protection method has been added to counter evasion by the use of the TCP Urgent Pointer parameter. TCP packets containing an Urgent Pointer parameter are blocked by default by all plugins except the FTP and TELNET plugins and the new alarm "*Unauthorized urgent data in TCP traffic*" (ID 162) will be raised. This alarm is set by default, to "block", "major".

By disabling this alarm, these plugins remove the URG parameter before transmitting the packet and the value of the "Urgent Pointer" parameter will be checked. Whenever an invalid value beyond the size of the received packet is detected, the alarm "*Invalid TCP protocol (out of bound urg pointer)*" (ID 98) will be raised.

### ClamAV

The ClamAV engine has been upgraded to fix a vulnerability (CVE-2011-1003) that could cause a denial of service and potentially corrupt the system.

Note: From version 6.2 onwards, the ClamAV server has been functioning without any privileges.

## 8.1.3 Bug fixes

### ASQ engine

#### Protocol of service objects

**Support reference: 24439**

The protocol of a service object can no longer be modified in the graphical interface.

### DNS

The response to a DNS query can now be resent several times for 2 seconds. This behavior used to be blocked by the alarm "DNS id spoofing – ID38". A new alarm "*Duplicated DNS reply*" (ID159) has been added in order to detect multiple responses within these 2 seconds. This alarm is set by default, to "pass", "ignore".

### QoS

The traffic distribution algorithm has been enhanced.

## Proxy

### Antispam: closure of DNS sessions

**Support reference: 23613**

The closure of a connection during treatment of DNS responses could cause the proxy to shut down unexpectedly. This anomaly has been fixed.

### RBL server

**Support reference: 15582**

The SORBS RBL server has been replaced with the SPAMCOP server in the default configuration of the antispam module.

### Closure of SMTP connections

**Support reference: 24578**

The SMTP proxy no longer closes connections immediately when the size of the message is exceeded. It now waits for the QUIT command to be sent by the mail client.

## Authentication

### Space character

**Support reference: 23758**

The use of spaces is now prohibited in the authentication page.

### Updating the CRL

**Support reference: 25084**

Changes to the period for updating the list of revoked certificates have been correctly applied.

### SPNEGO

**Support reference: 25762**

The use of the same value for the main name and the domain name could cause the authentication module to shut down unexpectedly. This anomaly has been fixed.

## IPSEC VPN

### Stability of the module

The stability of the IPsec module has been improved.

### Updating the CRL

**Support reference: 24950**

The minimum period for downloading the list of revoked certificates has been increased to 15 minutes. Updates within a shorter period are sometimes not applied.

## System

### Updating URL filter files

**Support reference: 18905**

This anomaly, which could sometimes lead to the loss of files from the URL filter database, has been fixed. It would typically occur during the update of the main file.

### Updating Kaspersky signatures

**Support reference: 22162**

The mechanism for updating the Kaspersky signature database has been improved with regards to checks and follow-up messages.

### Updating the license

Loading a license after the validity date of the license's signature certificate will no longer fail.

### Expiry date of licenses

The expiry date of a license is now the closest date between the date in the "NotAfter" field and the expiry date of the certificate used for signing the license.

### Route management

**Support references: 26416 and 25504**

An alert has been added to the creation phase of a static route to reach a network that is directly connected to the NETASQ appliance. Such routes are unnecessary and may prevent routes from being listed properly.

### High availability

**Support reference: 26393**

In the event the active firewall is manually restarted, the status of the passive appliance now stays as passive until the active appliance returns.

### FTP traffic address translation

**Support reference: 25293**

The management of FTP traffic with address translation could cause the appliance to shut down unexpectedly. This anomaly has been fixed.

### Updating the firmware

Downloading an invalid firmware update file could cause memory leaks. This has been fixed.

## DHCP server

An alert has been added to the configuration phase of a very large address pool, which could lead to the saturation of the */var* partition. Limits used for raising an alert depend on the model of the appliance:

- S model: 256 addresses
- M model: 4096 addresses
- L model: 8192 addresses
- XL model: 16384 addresses

## NETASQ Unified Manager

### Managing scripts

**Support reference: 25306**

The launch of a script that attempts to download an unreadable file is no longer suspended without an explicit error message.

## NETASQ Real Time Monitor

### Refreshing statistics

**Support reference: 25306**

The refreshment of the display of TCP, UDP and ICMP packet statistics is now correctly managed.

### Stability

The stability of the NETASQ Real Time Monitor application has been improved.

## 8.1.4 Features

### ASQ engine

#### Filter rule

**Support reference: 21185**

The maximum number of objects for all groups used in the filter rules has doubled – except for S models (U30-U70). The new limits are:

- S model: 512 objects
- M model: 2048 objects
- L model: 8192 objects
- XL model: 16384 objects

#### Address translation

**Support reference: 25710**

It is now possible to create redirection rules to the same destination. This type of translation allows overriding proxy redirection rules.

## 8.1.4 Resolved vulnerabilities

### PostgreSQL

PostgreSQL has been upgraded to 8.3.14. This version fixes a memory overflow vulnerability (CVE-2010-4015), which can lead to a denial of service and potentially allow code to be executed.

### DHCP module

Correction of a vulnerability (CVE-2011-0997) that could cause the execution of arbitrary commands through the use of meta-characters transported in a DHCP message.

## 8.1.4 Bug fixes

### ASQ engine

#### Hosts detected in bridge mode

**Support reference: 26406**

Hosts detected on an unprotected interface of a bridge will no longer be added to the host table. This allows using bridges on the VS range of NETASQ Virtual Appliance products without flooding host tables.

#### Unknown host on a bridge

Packets sent to an unknown host on a bridge are no longer sent on the source interface.

#### Routing by policy and load balancing

**Support reference: 22602**

The route identifier is now kept during the retrieval of connections in the event of a switch or reboot.

#### Filtering and Dialup interface

**Support reference: 27442**

The network interface is imposed for filter rules that allow traffic going to a Dialup interface on the NETASQ UTM firewall.

### HTTP

The HTTP application context has been modified to fix an anomaly that arose after an interruption in data transfer. Some of the information in events logs was not correctly updated.

### Network interfaces

#### “Keep VLAN” option

**Support reference: 27388**

The option of keeping VLANs has been fixed. Network packets that cross a bridge will now keep the VLAN tag.

## Loop detection on VLAN interfaces

**Support reference: 27749**

An anomaly arose regularly on the mechanism that manages network loops on VLAN interfaces. The NETASQ intrusion prevention engine did not re-enable the VLAN interface that was disabled after the detection of a network loop. This anomaly has been fixed.

Furthermore, the network loop detection mechanism has been enhanced. The option allowing the intrusion prevention engine to disable the VLAN interface upon detection of a network loop is disabled by default.

## PPTP server

**Support reference: 23974**

Configuring a large address range no longer causes flooding of the `/var` partition when it is enabled.

## Static routing

**Support reference: 27801**

Static routes defined for disabled interfaces will no longer be injected.

## Shutdown appliance ARP response

**Support reference: 26073**

Following an anomaly on network interfaces, NETASQ UTM firewalls would respond to ARP requests despite having been shut down. This anomaly has been fixed by disabling the network interfaces during the shutdown. The models affected by this fix are U70, U120, U250 and U450.

## Address translation

### MAP rule to a single port

Using a MAP rule that has been configured with a single translated port as its source port would cause an unexpected shutdown. This anomaly has been fixed.

## Proxy

### SMTP error code

**Support reference: 21498**

In some cases, temporary error codes (4xx) would be sent instead of permanent error codes (5xx). This anomaly has been fixed.

## ClamAV

Proxies would occasionally block files larger than 26 MB even when the policy has been set to "Pass" in the event of a failure during the scan. This anomaly has been fixed.

## Optenet URL filtering

A potential unexpected shutdown of the proxy when listing the OPTENET URL domains has been fixed.

## System

### DHCP default gateway

**Support reference: 23044**

The NETASQ UTM firewall can now retrieve via DHCP a default gateway that does not belong to an address range that can be retrieved.

### High availability

**Support reference: 24103 et 26579**

A possible infinite loop on the treatment of administration commands relating to high availability has been fixed.

### Active Update

**Support reference: 27097**

A potential leak of file descriptors has been fixed. This anomaly could cause the update of the antivirus signature database to be suspended.

### Authentication portal

**Support reference: 27179**

The signatures of java applets on the authentication portal have been updated.

### LDAP authentication

**Support reference: 26952**

In the event of a real authentication on the LDAP server, it is now possible to authenticate users whose absolute names (DN) do not contain the root absolute name (base DN).

### USB key

**Support reference: 26943**

The startup failure following the insertion of a USB key formatted in UFS has been fixed.

## NETASQ Unified Manager

### Object group

**Support reference: 27000**

By using an object group in a static route, the display of the objects in the group would not show any elements. This anomaly has been fixed.

### Loss of inspection profiles in Global mode

**Support reference: 27119**

During the deployment of profiles, the default inspection profiles for incoming and outgoing traffic would be lost. This anomaly has been fixed.

## NETASQ Real Time Monitor

### Display of events

**Support reference: 27609**

A potential shutdown of the application during the display of events has been fixed.

## 8.1.4 Known issues

### Network interfaces

#### VLANS attached to a disabled interface

**Support reference: 14891**

VLANS attached to disabled interfaces do not function correctly if the parent interfaces have been configured in DHCP.

A solution for bypassing this restriction is to configure a static IP address on the parent interface.

#### ARP publication on a disabled bridge

**Support reference: 17719**

A problem with ARP learning may arise when the first interface of a bridge has been disabled. After the network configuration command, some hosts are deemed to belong to the inactive interface until they are seen on another interface. During this period, traffic to these hosts may be blocked.

A solution for bypassing this restriction is to enable this interface even if it is not connected or used.

### Authentication

#### Object name same as Windows domain name

**Support reference: 13734**

Configuring a "host" object with the name of a Windows domain will prevent the appliance from correctly retrieving the list of users.

### IPSEC VPN

#### Management of the "Bypass" policy

**Support reference: 17873**

Adding or deleting a "Bypass" VPN policy would require the VPN slot to be disabled then re-enabled. Merely reloading the slot would place the policy at the end of the SPD whereas for it to function properly, it should be at the start.

### SSL VPN

#### Management of browsing issues

**Support reference: 21807**

When a user clicks on "Reply" on e-mails that have been opened in a new window, an HTTP 404 error would appear. There are several ways to bypass this problem:

- “Reply” without opening a new window
- Right-click -> “reply”

## System

### Serial interface speed

**Support reference: 16806**

The system message "more tty-level Buffer Overflow" may sometimes appear on the console for U1100, U1500 and U6000 products. This means that the characters are sent more quickly than the hardware can read them.

### Damaged RAID configuration

**Support reference: 19105**

The command that displays the status of the RAID configuration reports a damaged configuration when it has only functional disks.

A solution for bypassing this anomaly is to enter a system command in order to refresh the information sent.

## 8.1.5 Features

### System

#### Kaspersky

Major upgrade to the Kaspersky antivirus engine. A complementary heuristic analysis (switch to version SDK 8) has been added.

#### Dynamic routing

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

## 8.1.5 Resolved vulnerabilities

### System

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

OpenSSL has switched to version 1.0.0e.

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

Two vulnerabilities that could cause denial of service attacks within the DHCP server have been resolved.

 **NOTE**

The DHCP server is enabled in the default configuration.

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

ClamAV has been upgraded to version 0.97.2, which corrects the vulnerability CVE-2011-2721.

 **NOTE**

The ClamAV engine is not enabled in the default configuration.

## 8.1.5 Bug fixes

### Intrusion prevention

#### SSL plugin

**Support reference: 29653**

ECDHE encryption algorithms are allowed.

#### Netbios CIFS

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

### Network

**Support reference: 28004**

Hosts from two different sub-networks (using aliases) on the same bridge are able to communicate.

### Proxies

**Support reference: 25697**

Outgoing e-mails that exceed the maximum antivirus scan size are no longer blocked.

**Support reference: 28400**

The proxy now starts up correctly even when the certificate of the SLD module is invalid.

### URL filtering

**Support reference: 28173**

An issue in the search for the categories of certain URLs has been fixed.

### Authentication

**Support reference: 28858**

An issue that could cause the authentication daemon to reboot has been fixed.

#### LDAP method

**Support reference: 28142**

In the "real authentication" mode, user authentication failures on the portal no longer switch the firewall to the backup LDAP server.

### SSL VPN

**Support reference: 27728**

The parameters of external URLs would be lost during a redirection by the SSL VPN.

## System

**Support reference: 28160**

Importing private keys in DER format is now better managed.

## Cryptography

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

## 8.1.5 Known issues

### Network

**Support reference: 14891**

VLANs attached to a disabled Ethernet interface cannot operate correctly if the parent interface has been configured in DHCP.

In order to fix this problem, a static IP address has to be attached to the parent interface.

**Support reference: 17719**

Problems with reading the ARP table may arise when the first interface of a bridge has been disabled.

After enabling the network, a substitute host may be linked to the disabled interface until it is detected by another network.

During this time, it may block the firewall from its own traffic transfer.

The solution is to enable the interface (even if it is not connected/used).

## Authentication

### Active Directory

**Support reference: 13734**

When a host registered in the objects database is represented by its domain name, the firewall does not allow the list of users to be correctly retrieved.

## IPSec VPN

**Support reference: 17873**

Before adding or deleting a bypass policy, you must first enable/disable the existing policy. Once the operation is complete, the page has to be refreshed in order to guarantee the proper operation of the policy.

## OWA Premium 2003 with Internet Explorer

**Support reference: 21807**

If "Error 404 not found" appears when you attempt to reply to an e-mail open in a new window, you have one of the two following solutions:

- Click directly on "Reply"
- Right-click and select "Reply"

## System

### Buffer overflow

**Support reference: 16806**

The message “more tty-level Buffer Overflow” may sometimes appear on the console on U1100, U1500 and U6000 models. This means that some characters have been entered too quickly for the firewall to read them.

## 8.1.5.1 Bug fixes

### Captive portal

#### Browser

**Support reference: 30980**

After updating Windows KB2585542, problems to open the captive portal occurred, with several browsers. This is caused by a change in the format of SSL packets generated by this patch of Windows.