

# NETASQ Firewall - UTM Version 8.1.1.1

## 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.

---

## Version 8.1.1.1

---

Features: None

Bug fixes: Minor

Resolved vulnerabilities: Major

---

## 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>	
8.1.1.1		<a href="#">Resolved vulnerabilities</a>	<a href="#">Bug fixes</a>	<a href="#">Known issues</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 profil 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.

## 8.1.1.1 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.