



NETASQ Firewall Reporter

Logging and Reporting on NETASQ UTM appliances ⁽¹⁾

Firewall Reporter is a tool in the **NETASQ Administration Suite** that enables **creating reports and recording logs** obtained from NETASQ UTM appliances. Other functions such as configuration, updates and monitoring are conducted by the other tools in the suite. Firewall Reporter's **user-friendly and easy-to-use** graphical interface ensures **quick understanding of recorded events** and is helpful to define **relevant actions to take**.

Firewall Reporter exists in **two versions : Standard and Pro**. The **Pro version** contains a license that enables managing a **SQL database** that combines logs from **several UTM appliances**. Moreover, it also comes with an **automatic HTML report generator** which makes it easier to read information regarding network events.

Highlights

- Remote administration
- Proprietary communication protocol (AES+SRP)
- Free administration software
- Common Criteria-certified
- Automatic report generator (Autoreport)
- Bilingual administration software (French and English)



Proprietary communication protocol (AES+SRP) : In order to secure the remote administration of its UTM appliances, NETASQ has developed a standard-based proprietary communication protocol. Communications between UTM appliances and administration tools are based on SRP (Secure Remote Password) exchanges, which is a challenge-response protocol. These communications consist of the user proving his identity to a peer without transmitting any shared secret over the network in any form whatsoever (eg, passwords). Once peer identities have been established, all communications will be encrypted in AES (128-bit encryption key), which is currently the most powerful symmetrical encryption algorithm in terms of robustness and encryption speed).

Remote administration: The proprietary communication protocol that NETASQ uses for exchanges between its UTM appliances and their administration station provides an excellent guarantee of integrity and confidentiality, which makes remote administration of UTM appliances possible (not only connected directly to the UTM appliance) through an insecure network (local network and in particular, over the internet).



Logging and reporting : Firewall Reporter enables quick, intuitive and efficient reading of logs recorded on UTM appliances (these logs can be combined in a **SQL database delivered with the PRO version**). The following are the types of

logs that Firewall Reporter treats: Logs recorded in files (filter, alarm, connection), logs generated by application analyses (plugins, POP3, SMTP, WEB), and statistics on the use of the appliance (count, filter, translation). All the information is then displayed in the form of **tables or graphs** and can be **sorted using several methods**.

With the PRO version of Firewall Reporter, logs from several UTM appliances can be simultaneously displayed, thus allowing the administrator to view the impact of an event on other sites (for example, the creation of VPN tunnels).

Automatic HTML report generator: Autoreport (a function in Firewall Reporter PRO) can be used for generating HTML reports automatically in order to organize the presentation of certain traffic information. This will enable you to quickly obtain detailed statistics regarding network activity, alarms, visited websites, etc.

Free administration software: NETASQ Firewall Reporter, like all of NETASQ's other administration software programs (Firewall Manager, Firewall Monitor) is provided with UTM appliances at no additional charge.

Bilingual administration software: NETASQ Firewall Reporter exists in English and in French.

Common Criteria Certification: In conforming with its Common Criteria certification, NETASQ has taken steps to include the configuration software for its products in its security target (elements in the UTM appliances evaluated for Common Criteria certification). This means that when V5.1 Firewall Reporter is used for the remote configuration of an UTM appliance, the hypotheses indicated at the beginning of the certification are met, and the certification is coherent.

NETASQ UTM appliances have been built around a unique **real-time intrusion prevention** technology: **ASQ (Active Security Qualification)**. ASQ provides **context-based** intrusion prevention by analyzing traffic from network up to application layer, while applying **multiple methods** to identify and block malicious traffic. ASQ uses **classes** of attacks guaranteeing superior accuracy to protect against zero-day threats at wire speeds of up to 2 Gbps. This unique concept, linked to hardware specifically designed to provide next-generation intrusion prevention, allows NETASQ UTM appliances to provide real-time application layer intrusion prevention **without degrading system performance**.

(1) Available only for appliances in version 6.x.



Layout of log displays

Files (Filters, Alarms, Connections)
Contents (plugins, POP3, SMTP, WEB)
Graphs (displayed in graphs)
Statistics (Connection, Filter, Translation)
Services (information on the operation of different services: VPN, VPN SSL, authentication)
Miscellaneous (log management on UTM appliances and the database)

Source

Depending on the version of Firewall Reporter (STD or PRO), this field will be based on different log sources in order to display the logs.

Firewall (directly connected to the UTM appliance)
Syslog (retrieves logs from a Syslog server)
Collector (NETASQ log collector, logs are inserted into a SQL database in this case)
Archives (archiving logs from the SQL database on physical media such as CDs and DVDs is possible on Firewall Reporter)

Size of the log database (delivered with the PRO version of Firewall Reporter)

The SQL database requires approximately 20 MB of disk space for the installation, and another 20MB is needed for each log file for an average of 50,000 log lines.

Minimum hardware specifications needed for installing NETASQ Firewall Reporter

The requirements indicated below apply to a full installation of the standard NETASQ Administration Suite.

- ▶ PC Pentium III,
- ▶ 256 MB of RAM (512 MB recommended),
- ▶ 100 MB hard disk space,
- ▶ 10 or 100 Mbps Ethernet network adapter,
- ▶ Windows Internet Explorer 5,
- ▶ Windows 2000 (SP3), XP (SP1).

Compatibility with IPS-Firewalls

Unless otherwise stated, a major version of Firewall Reporter is compatible only with IPS-Firewalls in a corresponding major version. However, minor versions are compatible with each other. Therefore Firewall Reporter in V5.0.x is compatible with all 5.0.x versions of the NETASQ IPS-Firewall firmware (compatibility between minor versions).

With version V5.0.9 of Firewall Reporter, NETASQ IPS-Firewalls in version 5.0.7, version 5.0.9 and even version 5.0.11 can be managed.

However, an older version of Firewall Reporter cannot manage newer features from more recent firmware and vice-versa.

(1) Available only for appliances in version 6.x.