

NETASQ Firewall Monitor

Real-time monitoring on NETASQ UTM appliances ⁽¹⁾

Firewall Monitor is a tool in the **NETASQ Administration Suite** that enables **monitoring NETASQ UTM appliances in real time**. Other functions such as configuration, updates and reporting are conducted by the other tools in the suite. Firewall Monitor's **user-friendly and easy-to-use** graphical interface ensures **advanced monitoring of NETASQ appliances**.

Highlights

- Remote administration
- Proprietary communication protocol (AES+SRP)
- Free administration software
- Common Criteria-certified
- Highly detailed Real-Time Monitoring
- Bilingual administration software (French and English)



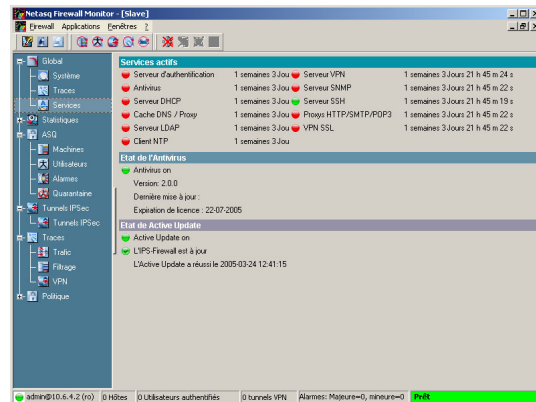
Proprietary communication protocol (AES+SRP) : In order to secure the remote administration of its UTM appliances, NETASQ has developed a standard-based proprietary communication protocol. Communications between UTM appliances and administration tools are based on SRP (Secure Remote Password) exchanges, 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).



Real-time monitoring: Firewall Monitor enables displaying in real time a wide variety of data contributing to the management of UTM appliances (HA, throughput, bandwidth, alarms, quarantine, users, VPN, Services actifs). Furthermore, Firewall Monitor allows viewing the most recently recorded logs, as such completing the panel of information that the interface generates. Firewall Monitor has also been adapted for the administrator to easily make a quick and relevant decision when he encounters an event – the application is displayed as soon as an alarm is

generated, possibility of taking quick action (quarantining, viewing fraudulent packets, etc).



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

Bilingual administration software: NETASQ Firewall Monitor 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 Monitor 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.



Global

- Systems (Operating status of modules, Active Update, high availability, and antivirus)
- Logs (size of disk space for logs)
- Services (active services on UTM appliances)

Statistics (real-time display of information)

- Bandwidth
- Throughput
- Connection
- Details (detailed display of packets passing through each interface)

ASQ (tables of data obtained from ASQ analyses)

- Hosts
- Users (list of authenticated users)
- Alarms
- Quarantine (quarantined hosts and/or users)

IPsec Tunnels

Viewing IPsec tunnels and managing the tunnel lifetime (deletion of VPN tunnels, management of orphan tunnels, etc)

Logs (viewing the latest logs recorded by the UTM appliance)

- Traffic (information on traffic passing through the UTM appliance)
- Filter (filter logs)
- VPN (VPN-related information messages and errors)

Policy

- Slots (different policies in use)
- Filter (list of all the filter rules currently applied)

Minimum hardware specifications needed for installing NETASQ Firewall Monitor

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

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

Compatibility with UTM appliances

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

With version V5.0.9 of Firewall Monitor, NETASQ UTM appliances in version 5.0.7, version 5.0.9 and even version 5.0.11 can be managed.

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

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