



# NETASQ F50

## IPS-Firewall



### Real-Time Intrusion Prevention for Small to Midsize companies

NETASQ IPS-Firewalls are purpose-built network security appliances that combine Real-Time Intrusion Prevention, Firewall, IPSEC Virtual Private Networking (VPN), Advanced Content Filtering, Antispam and Kaspersky Antivirus<sup>(2)</sup>. Based on NETASQ's revolutionary 'ASQ' in-line Intrusion Prevention Technology, all NETASQ IPS-Firewalls ensure the highest level of security.

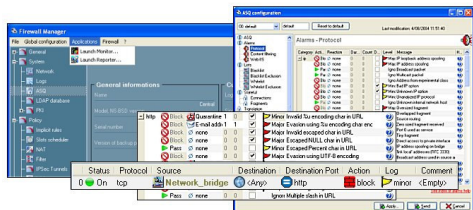


**NETASQ's F50 IPS-Firewall** is an easy-to-deploy security solution for small businesses and/or branch offices that require a DMZ port and granular management, monitoring and reporting. The F50 addresses the needs of small businesses of up to 50 employees that require complete content security and IPSEC VPN.

**IN-LINE INTRUSION PREVENTION:** NETASQ's embedded multi-layer multi-method intrusion prevention – ASQ – screens traffic in real-time, protecting against the most sophisticated network, application and blended attacks. Due to its in-line mode of operation it provides protection on all interfaces, securing local servers malicious activity from within.

**POWERFUL ANTISPAM:** identifies unsolicited e-mails (spam) before they reach the user's mailbox.

**REMOTE USER AND GATEWAY-GATEWAY VPN:** NETASQ's F25AV IPS-Firewall supports state-of-the-art IPSEC VPN for both gateway-gateway tunnels and remote users. While traffic can be encrypted up to 256-bit AES it still gets inspected by NETASQ's embedded intrusion prevention.



**ADVANCED URL FILTERING:** NETASQ's Advanced URL Filtering solution is a hosted service that provides an extensive on-line database with websites sorted in categories.

**CONTEXTUAL SIGNATURES:** The ASQ Contextual Signature integrates patterns of new applications, new attacks and updates to existing signatures. ASQ signatures support up to 12 application protocols and Peer-to-Peer applications such as Kazaa and Emule, or Instant Messaging tools like Yahoo!, AOL or MSN Messenger.

### ADMINISTRATION SUITE

Each NETASQ F50 IPS-Firewall comes with a complete Administration Suite. This suite consists of Firewall Manager, Monitor and Reporter. All these tools have an intuitive and user-friendly Windows-based GUI, which allows easy installation, configuration, monitoring, and reporting of your IPS-Firewall.

### CENTRALIZED MANAGEMENT – NETASQ GLOBAL ADMINISTRATION

NETASQ Global Administration allows companies, integrators or service providers to manage large deployments of NETASQ IPS-Firewalls from a central location. An easy to use graphical user interface enables you to centrally update, monitor and configure NETASQ IPS-Firewalls. Comprehensive log collection stores the logs of deployed IPS-Firewalls in a SQL-database, enabling high-speed trouble-shooting and generating reports.

F50 comes with a Global Administration version limited to 5 appliances. This limited version does not include log collection and storing in a SQL database. Unlimited version is also available in option.

### LICENSED OPTIONS:

#### KASPERSKY ANTIVIRUS

KASPERSKY Antivirus provides an additional layer of protection against E-mail based viruses and worms.

Specifications F50 <sup>(1)</sup>	
IPS-Firewall performance (Incl. Intrusion Prevention)	100 Mbps
AES VPN performance (Incl. Intrusion Prevention)	15 Mbps
100 Base-T interfaces (copper)	3
Maximum n° of interfaces	3
Concurrent connections	4,000
Filter policies	550
Gateway-Gateway VPN tunnels	100
Client-Gateway VPN tunnels	Yes
User License	Unlimited.

NETASQ IPS-Firewalls 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 multi-gigabit wire speeds. This unique concept, linked to hardware specifically designed to provide next-generation intrusion prevention, allows NETASQ IPS-Firewalls to provide real-time application layer intrusion prevention **without degrading system performance**.

(1) System Performances provided are the measured maximums under ideal testing conditions and may vary by deployment  
 (2) Requires a Kaspersky licence



### Network Features

- Routed, translated, bridged and hybrid mode
- Routing per interface
- Support for up to 16 VLANs
- Built-in Dialup router (PPTP, PPPoE, PPP)
- Address Translation (NAT, 1 to 1, PAT and Split)
- Time Scheduling
- xDSL High Availability and Load Balancing
- Support for up to 4 xDSL or Dialup modems
- Bandwidth Management
- Alias IP support (multiple IP addresses per interface)

### Intrusion Prevention System (ASQ)

- ASQ Real Time Intrusion Prevention
- ASQ plug-ins (HTTP, FTP, DNS, RIP, H323, EMule, SSL, SSH, Telnet, SMTP, POP3, IMAP4, NNTP, Generic...)
- Blocking attacks in VPN tunnels
- Multi-layer Inspection (Protocol, Connection, Session and Application layer attacks)
- Blocking known and unknown attacks with or without context
- Flooding protection (ICMP, UDP and TCP)
- Block Data-Evasion
- Trojan/Backdoor and protection
- Finger printing protection
- Hijacking session protection
- Contextual Signatures
- Dynamic Blacklisting
- Quarantining

### IPSEC VPN Features

- Supported VPN Protocols: IPsec & PPTP
- Supports up to 32 PPTP VPN clients
- Up to 256 bit encryption supporting DES, 3DES, AES, CAST128 and Blowfish
- ESP
- SHA-1 & MD5 Authentication
- IKE Certificate Authentication
- Pre-shared keys, PKI certificates, Static
- Hub & Spoke VPN
- Gateway – Gateway tunnels
- Client - Gateway tunnels
- VPN Keep-alive
- Dead Peer Detection
- NAT-Traversal (UDP 500 and 4500)

### Antispam

- DNS Blacklisting

### Authentication

- Single-Sign-On support
- LDAP Authentication (Internal and External)
- Windows Authentication (NT4 – NTLM and WIN2K Kerberos)
- External PKI compatibility
- Radius

### Services

- HTTP Proxy - URL filtering
- ICAP support for URL filtering
- SMTP Proxy
- POP3 Proxy
- DynDNS
- SNMP v1, v2 and v3
- Internal DHCP Server

### High Availability

- Active / Passive
- Software management
- Configuration synchronization
- Session synchronization for firewall



### Logging / Monitoring

- E-mail notification
- SNMP v1, v2 and v3
- Real Time Monitor
- Syslogging
- Internal Log Storage
- Historical Reporting
- Packet Dumping

### Management

- Firewall Manager (Windows GUI)
- Firewall Monitor (Windows GUI)
- Firewall Reporter (Windows GUI)
- Syslog, SSHv2, Console

### Options

- Kaspersky Antivirus

### Antivirus Features <sup>(2)</sup>

- SMTP Proxy forwarding
- HTTP Proxy forwarding
- Embedded Kaspersky Antivirus (SMTP, POP3)
- Maximum scannable uncompressed file-size: 10 MB

### Optional Software Suite

- NETASQ Global Administration

### Performances

IPS-Firewall performance (Incl. Intrusion Prevention)	100 Mbps
AES VPN Performance (Incl. Intrusion Prevention)	15 Mbps

### Hardware Specifications

N° of Ethernet interfaces	3
Max n° of Interfaces	3
Processor	400 Mhz
Storage	Flash 128 MB
Memory	128 MB
Dimensions (mm)	213 x 195 x 44
	1U / 0.5 x 19"
Weight	1.5 Kg
External Power supply	30 W external
Control connection	RS-232C serial port VT100 emulation

### Environment

Operational temperature	5° to 35 °C
Non-operational temp.	-30° to 65 °C

Note: Features provided on this datasheet are only applicable on last generation F50 IPS-Firewall hardware (with external power supply). Older hardware revisions (with internal power supply) might not support latest firmware features.

[www.netasq.com](http://www.netasq.com)



Non-contractual document. In order to improve the quality of its products, NETASQ reserves the right to make modifications without prior notice. All trademarks are the property of their respective companies.

(1) Requires Contextual Signature Subscription Service  
 (2) Requires Kaspersky License