

NETASQ F5000

IPS-Firewall



Enterprise-class Real-Time Intrusion Prevention

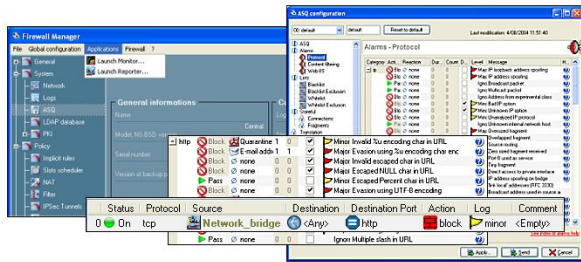
NETASQ IPS-Firewalls are purpose-built network security appliances that combine Real-Time Intrusion Prevention, Firewall, IPSEC Virtual Private Networking (VPN), Clientless SSL VPN, Advanced Content Filtering, Antispam and Kaspersky Antivirus⁽³⁾. Based on NETASQ's revolutionary 'ASQ' in-line Intrusion Prevention Technology, all NETASQ IPS-Firewalls ensure the highest level of security at the highest performance.



NETASQ's F5000 IPS-Firewall has been designed to ensure network enterprise-class security and availability under all circumstances, including hot-swappable components and redundant power supplies. This powerful security appliance is the ideal solution designed to maintain high levels of traffic in complex networks.

GIGABIT INTRUSION PREVENTION: The F5000 IPS-Firewall's performance scales up to 2 Gbps, 500,000 concurrent sessions and 15,000 VPN tunnels. Real-time intrusion prevention and content analysis are applied while maintaining these Gigabit throughputs by NETASQ's proprietary IPS: ASQ.

SCALABILITY: The F5000 IPS-Firewall supports up to 24 Gigabit Ethernet Interfaces (copper or fiber) ideal for carriers, service providers and large enterprises. Offering multiple DMZs and capable of 256 VLANs, the F5000 IPS-Firewall is the ideal solution for large enterprises and Managed Security Service Providers (MSSPs) looking for innovative technology.



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.

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**.

ADMINISTRATION SUITE

Each NETASQ F5000 IPS-Firewall comes with a complete Administration Suite. This suite consists of Firewall Manager, Monitor, **Reporter PRO** and **Auto Report Generator**. All these tools have an intuitive and user-friendly Windows-based GUI, which allows easy installation, configuration, monitoring, and auto 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.

F5000 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 F5000⁽¹⁾

IPS-Firewall performance (Incl. Intrusion Prevention)	2 Gbps
AES VPN performance (Incl. Intrusion Prevention)	180 Mbps
1000 Base-T interfaces (copper) ⁽²⁾	4
Maximum n° of interfaces	24
Maximum n° of Gigabit ports	24
Concurrent connections	500,000
Filter policies	16 650 rules
Gateway-Gateway VPN tunnels	15,000 Tunnels
Client-Gateway VPN tunnels	Yes
SSL VPN clients	Yes
Users	Unlimited

(1) System Performances provided are the measured maximums under ideal testing conditions and may vary by deployment

(2) Active with Purchase

(3) Requires Kaspersky licence



Network Features

- Routed, translated, bridged and hybrid mode
- Routing per interface
- Support for up to 256 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 12 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 64 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
- SSL VPN
- Dead Peer Detection
- NAT-Traversal (UDP 500 and 4500)

SSL VPN Features

•

High Availability

- Active / Passive
- Configuration synchronization
- Session synchronization for firewall
- Device failure detection

Antispam

- DNS Blacklisting

Authentication

- Single-Sign-On support
- LDAP Authentication (Internal and External)
- Windows Authentication (NT4 – NTLM and WIN2K Kerberos)
- Internal PKI CA & CRL
- External PKI compatibility
- Radius
- Web enrolment (creation of users and certificates)

Services

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



Logging / Monitoring

- E-mail notification
- SNMP v1, v2 and v3
- Real Time Monitor
- Syslogging
- Collecting logs in SQL database
- Internal Log Storage
- Historical Reporting
- Automatic report generation
- Packet Dumping

Management

- Firewall Manager (Windows GUI)
- Firewall Monitor (Windows GUI)
- Firewall Reporter PRO (Windows GUI)
- Auto Report Generator (Windows GUI)
- Log Collector + SQL Storage
- Syslog, SSHv2, Console

Options

- Kaspersky Antivirus

Antivirus Features ⁽³⁾

- SMTP Proxy forwarding
- HTTP Proxy forwarding
- Embedded Kaspersky Antivirus (SMTP, POP3)

Optional Software Suite

- NETASQ Global Administration

Performances

IPS-Firewall performance (Incl. Intrusion Prevention)	2 Gbps
AES VPN performance (Incl. Intrusion Prevention)	180 Mbps

Network cards supported

Copper:	2, 4 and 6-port 1000base-T cards
Fiber:	2-port 1000base-(SX or LX) cards
VPN:	SSL Accelerator Card

Hardware Specifications

Max n° of interfaces	24
Max n° of Gigabit ports	24
Processor	2 Xeon 2,8 Ghz
Storage	Raid 1 and 10 x 80 GB hot-swap SCSI drive
Controller	Ultra SCSI 320
Memory	2 GB ECC
Dimensions (mm)	452 x 610 x 178, 4U / 19"
Weight	35 Kg
Power supply	Triple Alimentation 3*300W (redundant)
Cooling Subsystem	3 Hot-plug redundant fans
Control connection	RS-232C serial port VT100 emulation Mini-din keyboard + VGA screen

Environment

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

www.netasq.com

