



NETASQ F500

IPS-Firewall



Entry-level Gigabit Platform

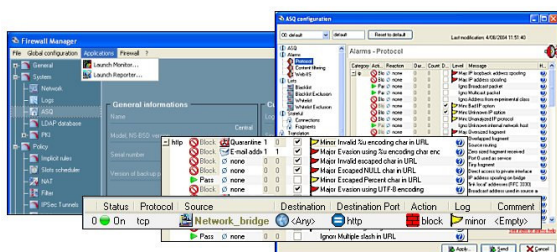
NETASQ IPS-Firewalls are purpose-built network security appliances that combine Real-Time Intrusion Prevention, Firewall, IPSEC Virtual Private Networking (VPN), Clientless SSL VPN, Advanced Content Filtering, Antispam and Kaspersky Antivirus⁽³⁾. Based on NETASQ's revolutionary 'ASQ' in-line Intrusion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



NETASQ's F500 IPS-Firewall is a flexible gigabit security appliance for medium-sized businesses offering a superior level of security at high performances. The F500 is specifically focused on high performance, redundancy and is ideal to act as central IPSEC and SSL VPN gateway.

PERFORMANCE: Ideal for multi-site VPN deployment as well as central gateway to perform real-time intrusion prevention embedded antivirus analysis, antispam and content filtering at high speeds. The F500 IPS-Firewall can handle up to 1,000 VPN tunnels, 50,000 concurrent sessions and has an IPS-Firewall throughput of 250Mbps.

REDUNDANCY & FLEXIBILITY: Designed for maximum flexibility, the NETASQ F500 IPS-Firewall offers built-in High Availability to provide fully redundant security solutions. Furthermore, four integrated and fully routable Ethernet ports can be extended with 2 onboard Gigabit interfaces and support for up to 64 VLANs make the NETASQ F500 IPS-Firewall the ideal solution to integrate into more complex networks.



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 F500 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.

F500 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:

KASPERKSY ANTIVIRUS

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

Specifications F500⁽¹⁾

IPS-Firewall performance (Incl. Intrusion Prevention)	250 Mbps
AES VPN performance (Incl. Intrusion Prevention)	65 Mbps
100 Base-T interfaces (copper) ⁽²⁾	4
Maximum n° of interfaces	6
Maximum n° of Gigabit ports	2
Concurrent connections	50,000
Filter policies	5,000
Gateway-Gateway VPN tunnels	1000 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 License



Network Features

- Routed, translated, bridged and hybrid mode
- Routing per interface
- Support for up to 64 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 8 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
- 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
- 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
- Port Upgrade (activates 2 on-board Gigabit interfaces)

Antivirus Features ⁽³⁾

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

Optional Software Suite

- NETASQ Global Administration

Performances

IPS-Firewall performance (Incl. Intrusion Prevention)	250 Mbps
AES VPN performance (Incl. Intrusion Prevention)	65 Mbps

Hardware Specifications

Max n° of interfaces	6
Max n° of Gigabit ports	2 on-board
Processor	2.0 Ghz
Storage	40 GB
Memory	256 MB
Dimensions (mm)	450 x 400 x 44
	1U / 19"
Weight	7.5 Kg
Power supply	300 W
Fan	4, lateral
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

