

# NETASQ F200

## IPS-Firewall



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

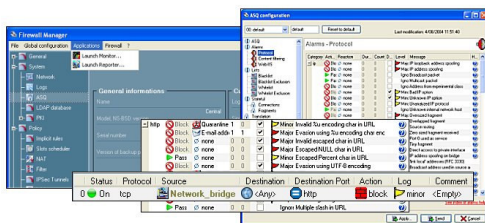
NETASQ IPS-Firewalls are purpose-built network security appliances that combine Real-Time Intrusion Prevention, Firewall, IPSEC Virtual Private Networking (VPN), Clientless SSL VPN, Advanced Content Filtering, Antispam and Kaspersky Antivirus<sup>(3)</sup>. Based on NETASQ's revolutionary 'ASQ' in-line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



**NETASQ's F200-IPS Firewall** is the ideal choice for small to midsize companies, providing a completely integrated security solution combining Firewall, IPS, IPSEC & SSL VPN, Content Filtering, Antispam and Embedded Kaspersky Antivirus with easy deployment and management, making it an ideal central gateway or VPN-concentrator.

**FLEXIBLE IPSEC AND SSL VPN** makes the F200 the industry's most versatile VPN concentrator. The F200 IPS-Firewall supports robust 256-bit AES IPSEC VPN for Gateway-Gateway and Remote User VPN. With its clientless SSL VPN features it offers a comprehensive mobile user VPN solution. Integrating Single-Sign-On with Active Directory, NT4, LDAP, PKI and Radius authentication allows users to experience transparent authentication and providing secure access through their web browser to any kind of network service.

**ALL-IN-ONE SECURITY APPLIANCE:** An all-in-one, easy to install and manage security solution offering a wide range of features such as SNMPv3, built-in DNS caching, VLAN support and xDSL router make it easy to deploy and integrate into existing 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 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 F200 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.

F200 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.

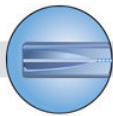
### Specifications F200<sup>(1)</sup>

IPS-Firewall performance (Incl. Intrusion Prevention)	150 Mbps
AES VPN performance (Incl. Intrusion Prevention)	30 Mbps
100 Base-T interfaces (copper) <sup>(2)</sup>	2, 3 or 4
Maximum n° of interfaces	4
Concurrent connections	35,000
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 licence



## 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 1 or 2 extra interfaces)

## Antivirus Features <sup>(3)</sup>

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

## Optional Software Suite

- NETASQ Global Administration

## Performances

IPS-Firewall performance (Incl. Intrusion Prevention)	150 Mbps
AES VPN performance (Incl. Intrusion Prevention)	30 Mbps

## Hardware Specifications

N° of Ethernet interfaces	2, 3 or 4
Max n° of Interfaces	4
Processor	733 Mhz
Storage	HD 40GB
Memory	128 MB
Dimensions (mm)	450 x 231 x 44
	1U / 19"
Weight	5 Kg
Power supply	150 W
Fan	2, lateral
Control connection	RS-232C serial port VT100 emulation

## Environment

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

[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.

(3) Requires Kaspersky License