NETASQ F800
UTM Appliance

F800 : SEGMENTATION AND SPEED

F800, the latest addition to the NETASQ UTM appliance range, contains 8 gigabit interfaces! These interfaces translate to greater speed capacities and more significant bandwidth and throughput. The first product in NETASQ's range to have only Gigabit interfaces, the F800 appliance is ideal for organizations that seek optimum protection while benefiting from a high-performance architectures.

Studies point to the internal network as the source of most threats, so being able to segment a network into trusted zones (zones can be segmented by department, by server or by the floor in the building) becomes the next logical step, in which traffic has to pass through the UTM appliance when moving between zones. By offering maximum protection for each zone in the network at Gigabit speed, the F800 appliance is the perfect solution for mid-sized and large structures seeking to segment their networks without compromising on performance.

MID-SIZED STRUCTURE range

NETASQ products for mid-sized structures meet security imperatives as well as the need for the integration of medium enterprise networks. The number of interfaces on these appliances can be upgraded in order to keep up with changes in the network infrastructure and all the security functions necessary for this structure type are built in. F200, F500 and F800 models are ideal platforms for use as IPSec VPN or SSL VPN hubs.

Main advantages of NETASQ solutions

Characteristics	Advantages	Benefits
NETASQ provides a real UTM approach	NETASQ products include numerous features in a single appliance, such as firewall, IPS, VPN, Quality of service, Antivirus, Antispam, URL filtering, and many more.	The integration of all these features within a single appliance enables the setup of a global security solution without the additional high installation and management costs while ensuring the proper installation of all features.
NETASQ is THE leading solution in the IPS field	The ASQ technology developed by NETASQ since 1998, based on the concepts of using vulnerability signatures and securing protocols, is a combination of techniques that provide protection from known and unknown attacks, also known as zero-day attacks.	This technology, developed in kernel mode, guarantees high-end performance while ensuring quality protection.
NETASQ offers a straightforward and simple product range	Every NETASQ product is delivered with the highest security. All features are already built-in by default. Performance figures given indicate performance with intrusion prevention activated.	NETASQ's clients have full control over the cost of ownership.
Intuitive and comprehensive administration suite	A suite of administration tools is provided with any product in the NETASQ range. This intuitive software suite allows the installation, configuration, maintenance and supervision of any NETASQ product.	Easy to install and to use! These easy-to-handle and intuitive graphical interfaces enable installing products easily, thereby increasing the relevance of the implemented policy.
An evolutionary range	NETASQ offers a range of evolutionary appliances that allow adding new DMZs or ports in order to segment the network.	NETASQ keeps abreast of its clients' changing needs.

NETASQ – 3 rue Archimède 59650 Villeneuve d'Ascq – Tel : 03 20 61 96 30 – Fax : 03 20 61 96 39

Features supported on the NETASQ F800 UTM appliance

Network and Filtering Features

• Routed, translated, bridged and hybrid mode
• Routing by interface
• Support for up to 128 VLANs
• Built-in Dialup router (PPTP, PPPoE, PPP)
• Address Translation (NAT, 1 to 1, PAT and Split)
• Time Scheduling
• Policy rule (NAT, filter, URL) compliance checker
• xDSL High Availability and Load Balancing
• Support for up to 12 xDSL or Dialup modems
• Dynamic Bandwidth Management
• Quality of Service management (Stateful QoS)
• Alias IP support (multiple IP addresses per interface)

Intrusion Prevention System (ASQ)

• ASQ Real Time Intrusion Prevention
• Protocols managed by ASQ : HTTP, FTP, DNS, RIP, H323, EMule, SSL, SSH, Telnet, SMTP, POP3, IMAP4, NNTP, etc.
• Protocol and application analyses
• Blocks known and unknown attacks
• Flooding protection (ICMP, UDP and TCP)
• Blocks data evasion via traffic reconstitution and decoding
• Detection of Trojan horses
• Session hijack protection
• Contextual Signatures with automatic updates
• Permanent and temporary quarantining
• P2P and Instant Messaging application filters
• Anti-spyware protection
• Protection from vulnerability scanners

IPSEC VPN and PPTP 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

• Clientless SSL VPN acess supported
• WEB Mode: access to web servers
• Full Mode: access to applications via JAVA applets
• User profile management

High Availability

• Active / Passive
• Configuration synchronization
• Session replication
• Detection of technical failures

Antivirus Features

• Embedded Kaspersky Antivirus (SMTP, POP3)
• SMTP Proxy forwarding
• HTTP Proxy forwarding
• Automatic updates

Antispam

• DNS Blacklisting

Authentication

• Single-Sign-On supported
• LDAP Authentication (Internal and External)
• Windows Authentication (NT4 – NTLM and WIN2K Kerberos)
• Radius
• Internal PKI CA & CRL
• External PKI compatibility
• 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
• Automatic update of the firmware and administration software
• Secure configuration [1]

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 PRO (Windows GUI)
• Global Administration for 5 appliances
• Syslog, SSHv2, Console

Options

• Kaspersky Antivirus according to maintenance contract
• Port upgrade

Optional software suite

• NETASQ Global Administration unlimited version

[1] Depending on the appliance's generation. Requires a USB port on the appliance and a compatible USB key.

NETASQ – 3 rue Archimède 59650 Villeneuve d'Ascq – Tel : 03 20 61 96 30 – Fax : 03 20 61 96 39

Specifications and performance for the NETASQ F800 UTM appliance

IPS-Firewall performance (incl. Intrusion prevention)	600 Mbits
AES VPN performance	136 Mbits
100 Base T Interface (copper)	n/a
1000 Base T Interface (copper)	4, 6 or 8
Simultaneous connections	400 000
Max. no. of filter rules	4096
Max no. of IPSec VPN tunnels	4000
Client-Gateway IPSec VPN Tunnels	Yes
SSL VPN Tunnels	Yes
Max. no. of users	Unlimited

Hardware Specifications

Max no. of Ethernet ports	n/a
Max no. of Gigabit ports	2 on motherboard + 6 on PCI card
Max no. of interfaces	8
Processor (MHz)	2400
Storage	40 GB HDD (SATA)
Memory (MB)	512
Dimensions (mm)	490 x 400 x 44, 1U / 19''
Weight (kg)	xx
Power supply (W)	300
Cooling Subsystem	4 internal 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

Certifications

Common Criteria	EAL 2+
ICSA Labs	v4.0

NETASQ – 3 rue Archimède 59650 Villeneuve d'Ascq – Tel : 03 20 61 96 30 – Fax : 03 20 61 96 39