

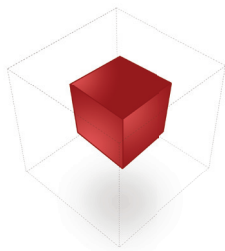
NETASQ V50, V100, V200 & V500

VIRTUAL APPLIANCES FOR SMB AND NETWORK SEGMENTATION

Small and medium businesses should bear in mind that all networks within their IT infrastructure, be they virtual or physical, require the same level of protection against current and emerging threats.

HIGHLIGHTS

- VMware VSphere and Citrix XenServer Ready
- No Initial Costs
- Portability
- Zero-Day Intrusion Prevention
- Automatic Updates



The benefits provided by virtualization, particularly for SMBs are clear: cost reduction, resource optimization and easier service deployment and management, in addition to faster data recovery. However virtualization enables multiple services, many with different trust levels, to run on the same physical platform.

This is a practice that requires powerful solutions to secure traffic flowing between each of the virtual machines. As it is not possible to place a traditional firewall within a virtual network, the best way to monitor communication in a virtual environment is to deploy a virtual security appliance.

SECURING YOUR VIRTUAL NETWORK ENVIRONMENT

Virtual machines host the same Operating Systems, CRM, ERP and business critical applications as physical servers, with multiple virtual machines now sharing a single hardware platform. Email and web servers, which were traditionally located in the DMZ, can therefore be hosted in the same environment as production servers, making the latter potentially more accessible.

As you move from a physical environment to a virtual network, you need a proactive, all-in-one virtual security appliance to ensure that all your protection requirements continue to be met. A mature, IPS-based Unified Threat Management solution with an integral real-time analysis will enable you to benefit from all the advantages of virtualization, including load-balancing, portability and fast data recovery.

NETASQ's zero-day Intrusion Prevention System lies at the heart of all Virtual Appliances for SMBs. Located in the system kernel, it embeds firewall, antivirus and antispam functionality. It also includes protection for your VoIP traffic and supports both IPSec and SSL VPN tunnels ensuring full protection of your inter-site communications.

The NETASQ engine analyzes network protocols and applications to detect and block threats, delivering outmost security by dramatically reducing the risk of false alarms thanks to behavioral analysis, coupled with a range of contextual signature databases.

REDUCING COSTS

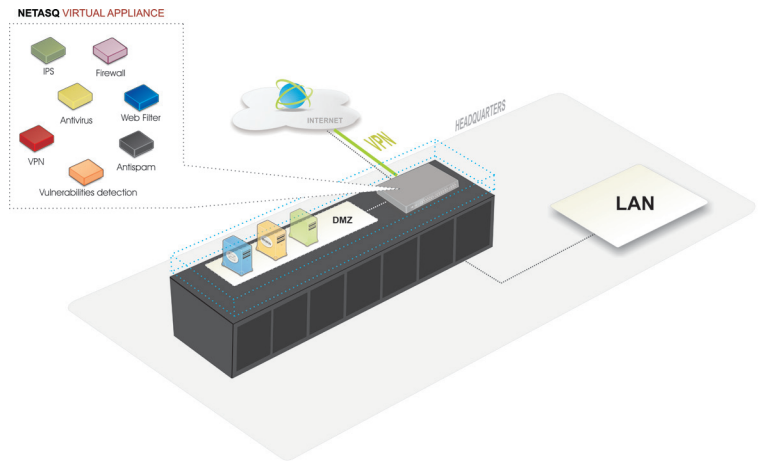
To remain competitive, small and medium businesses need to minimize the costs of their IT infrastructure, which often leads to compromises as to the quality of the deployed IT services. Taking this into account, with NETASQ Virtual Appliances for SMBs organizations can benefit from the full range of security features at no initial cost, by just subscribing for the services, which include firmware and protection updates.

The benefits of an annual subscription are clear: drastic reduction of IT security costs, full cost control, rapid return on investment on a state-of-the-art protection.

Use Case

The Virtual network needs the same protection level as the physical network

NETASQ Virtual Appliances for SMBs ensure that all virtual networks have exactly the same state-of-the-art protection as their physical counterparts through the deployment of a virtual security appliance. NETASQ V-series can protect Virtual Machine to Virtual Machine traffic as well as all virtual and physical network traffic. As virtualization can effect huge savings, there is no need to accept compromises on security. Both virtual and physical NETASQ appliances are managed by the same management suite.



MAIN CHARACTERISTICS	V50	V100	V200	V500
Protected IP addresses	50	100	200	500
Concurrent connections	100,000	200,000	400,000	600,000
802.1Q VLANs (max)	32	128	128	128
IPSEC VPN Tunnels (max)	100	500	1,000	1,000
Simultaneous SSL VPN clients	50	256	512	512

USER BASED FIREWALL

Third-party authentication - LDAP, Active Directory, Radius, NTLM

Transparent authentication - Microsoft SPNEGO - SSL Certificate

MULTIFUNCTION FIREWALL - UTM

SMTP, POP3, HTTP, FTP proxies
Embedded antivirus, antispysware
Reputation-based Antispam (DNS RBL)
Heuristic Antispam analyses
IPSEC VPN
SSL VPN

IPS - APPLICATION BASED FIREWALL

Real-time policy compliance checker
Policy scheduling
Automatic quarantining in case of attacks
Protection from flooding attacks
Protection from data evasion

Advanced management of fragmentation
Protection from SQL injections
Protection from Cross Site Scripting (XSS)
Trojan horse detection
Protection from session hijacks
Dedicated application analysis (plugins) : IP, TCP, UDP, HTTP, FTP, SIP, RTP/RTCP, H323, DNS, SMTP, POP3, IMAP4, NNTP, SSL, MGCP, Edonkey, SSH, Telnet...

NETWORK SERVICES

DHCP client and server
NTP client
DNS cache proxy

NETWORK - ROUTING - QUALITY OF SERVICE

Transparent, routed, hybrid modes
Address translation (NAT,PAT, split)
Static routing - Policy Based Routing

Dynamic routing
Bandwidth guarantee/limitation
Priority-based bandwidth management

MANAGEMENT

Role administration
NETASQ UNIFIED MANAGER
NETASQ REAL-TIME MONITOR
NETASQ EVENT REPORTER
ssh v2

MONITORING - REPORTING

Logging to Syslog servers (max 3)
E-mail alerts
Automatic report generation
SNMP v1, v2, v3 (DES, AES) agent

OPTIONS

NETASQ VULNERABILITY MANAGER: Risk management

About NETASQ

With over 75,000 unified threat management firewalls deployed to business, government and defence organisations of all sizes, NETASQ delivers solutions of unrivalled performance, protection and control and the most comprehensive EU and NATO certifications of any firewall.

For further information: www.netasq.com

FRANCE Paris +33 1 46 21 82 30 france@netasq.com	BENELUX & NORDICS Breda +31 76 8883022 benelux@netasq.com	IBERICA Madrid +34 91 761 21 76 iberia@netasq.com	ITALIA Milano +39 02 7253 7249 italia@netasq.com	UK London +44 207 092 6682 uk@netasq.com	DACH München +49 89 20 300 6320 dach@netasq.com	MIDDLE EAST & AFRICA +971 50 5573 746 INTERNATIONAL international@netasq.com
--	--	---	--	--	---	---