

NETASQ VS5 & VS10

VIRTUAL APPLIANCES FOR SERVERS

To compete on today's market, organizations deploy more and more web and application services supporting 24x7 business operations. The level of investment for this uncontrolled growth is no longer acceptable, IT managers see in virtualization a viable means to highly reduce the costs of their server infrastructure.

From a security perspective though, virtualization is not a synonym for benefits. By fully overthrowing the traditional physical separation in different trust zones for back-end and front-end servers, virtualization is a two-edged sword. In the strive towards simpler, more consistent and agile hardware utilization, businesses often neglect, that virtual assets are exactly as vulnerable as their physical counterparts.

The most efficient solution to monitor communication between virtual servers running on the same physical hardware is a virtual appliance with Firewall and IPS capabilities. NETASQ Virtual Appliance for Servers is the solution to protect virtual DMZ.

HIGHLIGHTS

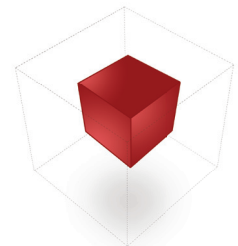
- No initial cost for a fast return on investment (ROI)
- Proven IPS protection and vulnerability assessment
- Compliant with virtualization market leaders
- Evolutive solution

PROTECT YOUR VIRTUAL DMZ

Like physical environments, virtual networks can suffer from bandwidth abuse, Denial-of-Service (DoS) attacks, viruses and vulnerability exploits. These threats jeopardize the network availability as well as the productivity of the employees.

To fully take advantage of virtualization by nullifying its risks, businesses do not just need real time protection against current and future threats, but also to regain complete visibility and control of applications flaws on the different virtual servers.

Located in the system kernel, our patented intrusion prevention engine delivers real time behavioral and protocol analysis of the data flow. Our unique architecture embeds both IPS and all functionalities of a complete all-in-one solution (UTM), a further added value enterprises can benefit from, if needed. Furthermore NETASQ's VS5 and VS10 support transparent network segmentation, intuitive user-based security policy, and protect data coming through "secure" IPsec or SSL VPN tunnels by proactively scanning the traffic generated via remote connections.



On top of the field-proven, EAL 4+ certified protection for your data and voice traffic, NETASQ's Virtual Appliances for Servers come at no additional cost with NETASQ SEISMO, a real time vulnerability management system. It delivers real-time assessment of the threats affecting your virtual servers as well as efficient information on the location of patches and updates for their correction.

NETASQ's Virtual Appliances for Servers are compatible with VMware vSphere™ and Citrix XenServer™. Thanks to the virtual appliance format, the installation/restoring process is extremely simple, granting a high degree of portability.

BUDGET UNDER CONTROL

As all organizations need to consider the price / quality ratio of IT security, NETASQ wished to contribute to protecting virtual servers by giving access to both VS5 and VS10 at no initial cost.

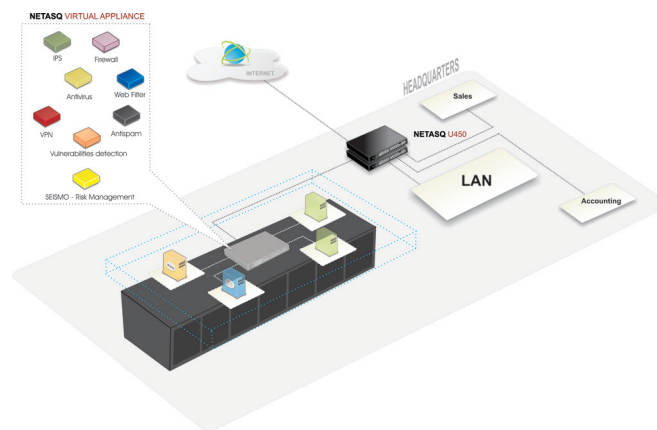
To benefit from the full range of security features and the vulnerability assessment delivered by NETASQ's Virtual Appliances for Servers, businesses just need to subscribe for the maintenance services, firmware and protection updates. The advantages of the yearly subscription approach are clear: full cost control and fast return on investment for state-of-the-art protection.

NETASQ's Virtual Appliances for Servers deliver dedicated "future ready" protection, safeguarding your network, productivity, and budget.

Use Case

Secure the Virtual DMZ by monitoring and blocking VM-to-VM communication threats.

NETASQ Virtual Appliances for Servers are placed at the core of the virtual environment. With up to 10 virtual network interfaces, each virtual server can be isolated in a dedicated security zone, with no change to the network configurations thanks to the transparent bridge feature. Thanks to NETASQ's innovative risk assessment solution (NETASQ VULNERABILITY MANAGER), not only is the inter VM communication secured but possible server vulnerabilities are immediately identified.



MAIN CHARACTERISTICS	VS5	VS10
Protected virtual machines	5	10
NETASQ VULNERABILITY MANAGER	✓	✓
Concurrent connections	1,000,000	2,000,000
802.1Q VLANs (max)	512	512
IPSEC VPN Tunnels (max)	10,000	10,000
Simultaneous SSL VPN clients	2,048	2,048

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

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