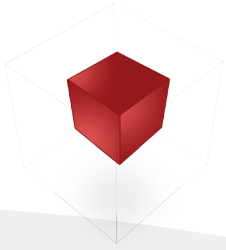
NETASQ V50, V100, V200 & V500

VIRTUAL APPLIANCES FOR ISPs 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 MSPs 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 MSPs. 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 MSPs 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.

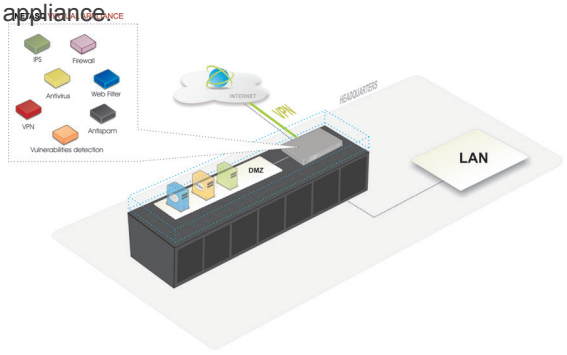
The benefits of an annual subscription are clear: drastic reduction of IT security costs, full cost control, rapid return on investment on a state-of-the-art protection.

Use Case

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

NETASQ Virtual Appliances for MSPs 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 - SSO Agent

MULTIFUNCTION FIREWALL - UTM
SMTP, POP3, HTTP, FTP proxies
Embedded antivirus, antispyware
Reputation-based Antispam (DNS RBL)
Heuristic Antispam analyses
IPSEC VPN
SSL VPN
NETASQ Extended Web Control 65 categories (Optional)

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 interactive report generation
SNMP v1, v2, v3 (DES, AES) agent

OPTIONS
NETASQ VULNERABILITY MANAGER: Risk management

About

Arkoon+Netasq, 100% subsidiaries of Airbus Defence & Space (Airbus group), offer security solutions which are particularly innovative for network protection. These trusted solutions are certified at the highest European level (EU RESTRICTED, NATO and ANSSI EAL4+), to secure strategic information. They are sold through a network of resellers, integrators and telecom operators to companies, government and defence organisations of all sizes throughout the world. www.arkoon-netasq.com

EUROPE

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

UNITED KINGDOM (London)
+44 207 092 6682
uk@netasq.com

ASIA PACIFIC

CHINA (Shanghai City)
+86 400 011 4313

INDIA (Hyderabad)
+91 99495 55806

SINGAPORE (Singapore)
+65 6333 9077

MIDDLE-EAST & AFRICA

UAE (Dubai)
+971 55 5511 337

INTERNATIONAL

international@netasq.com

NETASQ VS5 & VS10
VIRTUAL APPLIANCES FOR SERVERS

To compete on todays market, organizations deploy more and more web and application services supporting 24x7 business operations. The level of investment for this uncontrolled growth being 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.

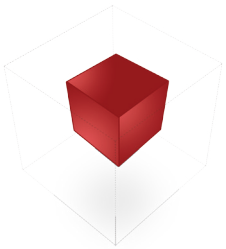
HIGHLIGHTS
- No initial cost for a fast return on investment (ROI)
- Proven IPS protection and vulnerability assessment
- Compliant with virtualization market leaders
- Evolutive solution

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.

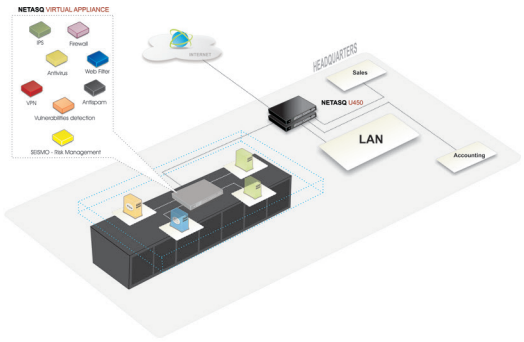
To benefit from the full range of security features and the vulnerability assessment delivered by NETASQ's Virtual Appliances for Servers, businesses just need to subscribe for the maintenance services, firmware and protection updates.The advantages of the yearly subscription approach are clear: full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

MULTIFUNCTION FIREWALL - UTM
SMTP, POP3, HTTP, FTP proxies
Embedded antivirus, antispyware
Reputation-based Antispam (DNS RBL)
Heuristic Antispam analyses
IPSEC VPN
SSL VPN
NETASQ Extended Web Control 65 categories (Optional)

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 interactive report generation
SNMP v1, v2, v3 (DES, AES) agent

About

Arkoon+Netasq, 100% subsidiaries of Airbus Defence & Space (Airbus group), offer security solutions which are particularly innovative for network protection. These trusted solutions are certified at the highest European level (EU RESTRICTED, NATO and ANSSI EAL4+), to secure strategic information. They are sold through a network of resellers, integrators and telecom operators to companies, government and defence organisations of all sizes throughout the world. www.arkoon-netasq.com

EUROPE

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

UNITED KINGDOM (London)
+44 207 092 6682
uk@netasq.com

ASIA PACIFIC

CHINA (Shanghai City)
+86 400 011 4313

INDIA (Hyderabad)
+91 99495 55806

SINGAPORE (Singapore)
+65 6333 9077

MIDDLE-EAST & AFRICA

UAE (Dubai)
+971 55 5511 337

INTERNATIONAL

international@netasq.com

NETASQ VU (UNLIMITED)

VIRTUAL APPLIANCE FOR ENTERPRISE

Many enterprises adopt virtualization as a means to consolidate their major data centers. It is crucial for them to ensure that new virtual architectures do not suffer any degradation in the level of protection afforded to them.

Enterprises adopt virtualization both to bring consistency to their IT infrastructure and to profit from a technology, which brings about a huge TCO reduction, enhanced system exploitation and manageability, load balancing, server portability and immediate recovery.

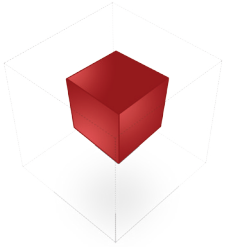
Poor security practices though, may nullify the dramatic benefits of virtualization. Its dark side is indeed the possibility to arbitrarily connect virtual hosts to network segments with different trust levels. The fact that traditional IPS/IDS appliances, once shielding the physical network, are useless in a fully virtualized environment is a further aggrieving factor.

Enterprises need to maintain the same quality of security for virtual environments hosting their business critical applications and information, as previously granted within physical networks.

KEY BENEFITS

- Proven, EAL4+ certified solution
- Unrestricted users and IP licence
- On demand security: no initial costs
- Compliant with virtualization market leaders
- Best-in-Class zero-day Intrusion Prevention
- Perfectly fits your green IT strategy

VIRTUALIZE SECURELY



By sharing the same hardware platform to host operating systems, CRM and ERP as well as all services once located in the DMZ, all affected by potential application vulnerabilities, virtualization raises new challenges for the protection of business critical information.

To adequately protect such multi-layer architectures, enterprises need a mature virtual security solution, allowing to centrally manage multiple virtual and physical security devices. They also require to support smooth migrations within meshed topologies, network segmentation and optimal protection of the inter-site communication. The NETASQ Virtual Appliance for Enterprise is the solution covering all these expectations.

Located in the system kernel, our patented intrusion prevention engine delivers real-time behavioral and protocol analysis of the data flow. It combines several technologies to proactively protect against thousands of existing and future threats. Deployed in a virtual environment, the NETASQ Virtual Appliance for Enterprise comes with an efficient and intuitive management interface. Per user security policy configuration and comprehensive network monitoring are natively supported to let the security team in control of their virtual network.

On top of the field-proven EAL 4+ certified solution, our virtual appliance integrates all functionalities you would expect from a complete all-in-one solution (UTM). An enterprise may also benefit from a real-time vulnerability assessment engine*, which drastically reduces the risks for sensitive architectures.

Last but not least, NETASQ's VU (unlimited) contributes to secure mobility by delivering a proactive analysis of the data flow coming through "secure" SSL or IPSec VPN tunnels.

ON DEMAND SECURITY

One of the principles driving virtualization being a massive cutback on infrastructure costs, NETASQ Virtual Appliance for Enterprise is delivered at no initial cost, "on demand". To benefit from the full range of security features offered by NETASQ's Virtual Appliance for Enterprise, large organizations just need to yearly subscribe for the services, firmware and protection updates. The subscription approach bears several advantages, among which full cost control on a yearly basis and fast return on investment for state-of-the-art protection are just a few.

NETASQ Virtual Appliance for Enterprise delivers future-ready, enterprise-class security, granting to large global organizations true protection against internal and external threats. It safeguards both the performance of their virtual network and the employees' productivity.

*requires subscription

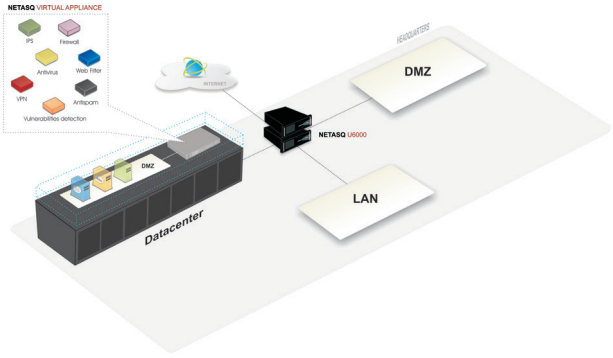
Use Case

Secure your virtual network as a second line of defence.

NETASQ Virtual Appliance for Enterprise ensures that all virtual networks have exactly the same state-of-the-art protection as their physical counterparts. Securing a virtual network with a physical firewall/IPS can be unpleasant, as virtualization features such as high availability and life migration of virtual machines need to be taken into account.

By inserting a virtual firewall / IPS directly into your virtual environment, you do not just benefit from and work with these features, but you build an ideal second line of defense for your entire network.

This ensures the same level of protection for your virtual network as for your physical environment. Both physical first line of defence and virtual second line of defence can be managed with the same NETASQ Management Suite, providing easy and cost-effective management.



MAIN CHARACTERISTICS	VU
Protected IP addresses	Unlimited
Concurrent connections	3,000,000
802.1Q VLANs (max)	512
IPSEC VPN Tunnels (max)	10,000
Simultaneous SSL VPN clients	2,048

USER BASED FIREWALL
Third-party authentication - LDAP, Active Directory, Radius, NTLM
Transparent authentication - Microsoft SPNEGO - SSL Certificate - SSO Agent

MULTIFUNCTION FIREWALL - UTM
SMTP, POP3, HTTP, FTP proxies
Embedded antivirus, antispyware
Reputation-based Antispam (DNS RBL)
Heuristic Antispam analyses
IPSec VPN
SSL VPN
NETASQ Extended Web Control 65 categories (Optional)

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 interactive report generation
SNMP v1, v2, v3 (DES, AES) agent

OPTIONS
NETASQ VULNERABILITY MANAGER: Risk management

About

Arkoon+Netasq, 100% subsidiaries of Airbus Defence & Space (Airbus group), offer security solutions which are particularly innovative for network protection. These trusted solutions are certified at the highest European level (EU RESTRICTED, NATO and ANSSI EAL4+), to secure strategic information. They are sold through a network of resellers, integrators and telecom operators to companies, government and defence organisations of all sizes throughout the world. www.arkoon-netasq.com

EUROPE

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

UNITED KINGDOM (London)
+44 207 092 6682
uk@netasq.com

ASIA PACIFIC

CHINA (Shanghai City)
+86 400 011 4313

INDIA (Hyderabad)
+91 99495 55806

SINGAPORE (Singapore)
+65 6333 9077

MIDDLE-EAST & AFRICA

UAE (Dubai)
+971 55 5511 337

INTERNATIONAL

international@netasq.com