

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 aggravating 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.

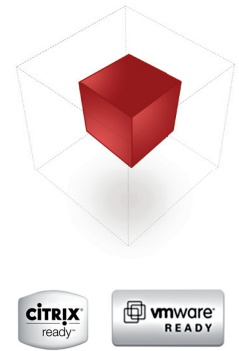
On top of the field-proven EAL 4+ certified solution, our virtual appliance integrates all functionalities you would expect from a complete all-in-one solution (UTM). An enterprise may also benefit from a real-time vulnerability assessment engine*, which drastically reduces the risks for sensitive architectures.

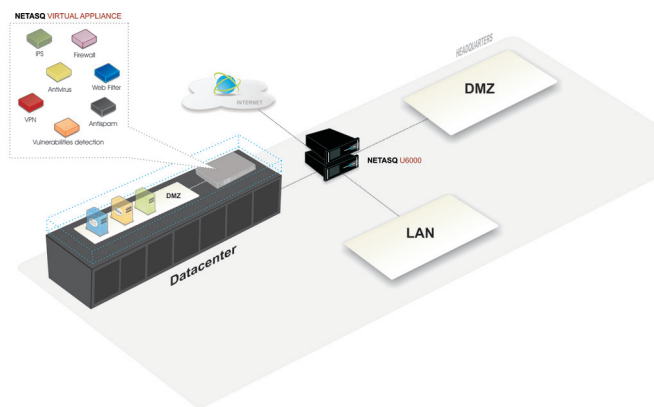
Last but not least, NETASQ's VU (unlimited) contributes to secure mobility by delivering a proactive analysis of the data flow coming through "secure" SSL or IPSec VPN tunnels.

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.





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

MULTIFUNCTION FIREWALL - UTM

SMTP, POP3, HTTP, FTP proxies
Embedded antivirus, antispymware
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

IBERIA 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