



# STORMSHIELD

## STORMSHIELD NETWORK VS5 & VS10

### VIRTUAL APPLIANCES FOR SERVERS

#### VIRTUAL APPLIANCES FOR SERVERS

##### Highlights

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



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 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.

#### 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 Stormshield'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, Stormshield's Virtual Appliances for Servers come at no additional cost with Stormshield Vulnerability Manager, 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.

## ABOUT

Stormshield, a fully-owned subsidiary of Airbus Defence and Space, offers innovative end-to-end security solutions to protect networks (Stormshield Network Security), computers (Stormshield Endpoint Security) and data (Stormshield Data Security).

[WWW.STORMSHIELD.EU](http://WWW.STORMSHIELD.EU)

Phone  
+33 9 69 32 96 29

Non-contractual document. In order to improve the quality of its products, Stormshield reserves the right to make modifications without prior notice.

All trademarks are the property of their respective companies.

Stormshield'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, Stormshield 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 Stormshield'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.

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

## TECHNICAL SPECIFICATIONS

	VS5	VS10
Protected virtual machines	5	10
Vulnerability Manager	Yes	Yes
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	500	500

### USAGE CONTROL

Firewall/IPS/IDS mode, identity-based firewall, application firewall, Microsoft Services Firewall, detection and control of the use of mobile terminals, application inventory (option), vulnerability detection (option), filtering per localisation (countries, continents), URL filtering (embedded database or cloud mode), transparent authentication (Active Directory SSO Agent, SSL, SPNEGO), multi-user authentication in cookie mode (Citrix- TSE), guest mode authentication, time scheduling per rule.

### PROTECTION FROM THREATS

Intrusion prevention, protocol scan, application inspection, protection from denial of service attacks (DoS), protection from SQL injections, protection from Cross-Site Scripting (XSS), protection from malicious Web2.0 code and scripts, Trojan

detection, detection of interactive connections (botnets, Command&Control), protection from data evasion, Advanced management of fragmentation, automatic quarantining in the event of an attack, Antispam and antiphishing: reputation-based analysis — heuristic engine, embedded antivirus (HTTP, SMTP, POP3, FTP), detection of unknown malware via sandboxing, SSL decryption and inspection, VoIP protection (SIP), collaborative security: Dynamic Host Reputation, IP reputation.

### CONFIDENTIALITY

Site-to-site or nomad IPSec VPN, remote SSL VPN access in multi-OS tunnel mode (Windows, Android, iOS, etc), SSL VPN agent configurable centrally (Windows), Support for Android/iPhone IPSec VPN.

### NETWORK - INTEGRATION

IPv6, NAT, PAT, transparent

(bridge)/routed/hybrid modes, dynamic routing (RIP, OSPF, BGP), multi-level internal or external PKI management, multi-domain authentication (including internal LDAP), transparent or explicit proxy, policy-based routing (PBR), QoS management, DHCP client/relay/server, NTP client, DNS proxy-cache, HTTP proxy-cache, WAN link redundancy.

### MANAGEMENT

Web-based management interface, object-oriented security policy, real-time configuration help, firewall rule counter, more than 15 installation wizards, global/local security policy, embedded log reporting and analysis tools, interactive and customizable reports, sending to syslog server UDP/TCP/TLS, SNMP v1, v2, v3 agent, role based management, email alerting, automated configuration backup.