STORMSHIELD

NETWORK SECURITY

STORMSHIELD
ELASTIC VIRTUAL APPLIANCE

Re-engaging with the virtual world

63 Gbps
FIREWALL
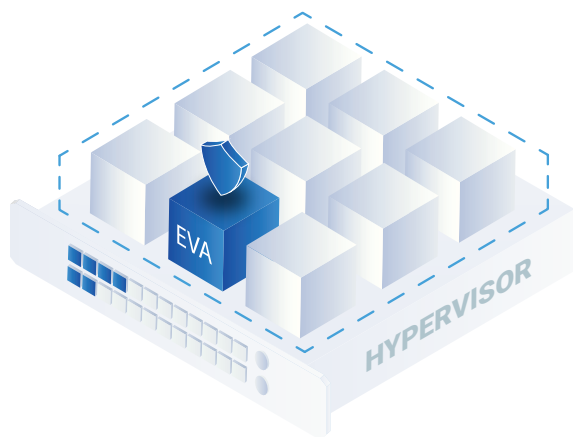PERFORMANCE

33 Gbps
IPS
PERFORMANCE

10.6 Gbps
IPSEC VPN
PERFORMANCE

Flexibility
AUTOMATIC
SIZING

Adapted to your needs
Elastic Virtual Appliance solutions adapt their capacities to the resources allocated on the hypervisor. Deploy a virtual image, it will track changes in your infrastructure.

Protection of virtual environments
- Segmentation of virtual networks
- Secure site-to-site communications
- Protection of mobile accesses

$ Cost reductions
- Adaptation to the hypervisor's resources
- Optimum RAM and vCPU consumption

Portability
- Migration from one Cloud platform to another
- Wide range of environments supported (Citrix, Microsoft Hyper-V, VMWare, KVM, Microsoft Azure, Amazon Web Services)
- Back up, roll out, restore, enjoy

CITRIX   vmware   Microsoft Hyper-V   KVM

Windows Azure   aws   OUTSCALE

SIZING

SYSTEM	EVA1	EVA2	EVA3	EVA4	EVAU
Memory (min - max, GB)	1-2	2-3	3-6	6-8	8-64
Max. number of vCPUs	1	2	4	4	16
Max. number of filtering rules	1,024	2,048	4,096	8,192	8,192
Max. number of objects	5,000	5,000	5,000	5,000	20,000
Max. size of user database	2,048	2,048	5,120	5,120	10,240

NUMBER OF USERS	EVA1	EVA2	EVA3	EVA4	EVAU
Firewall usage	30	50	150	500	4,000
NGFW usage (all features enabled)	15	25	100	300	2,000

NETWORK CONNECTIVITY	EVA1	EVA2	EVA3	EVA4	EVAU
Max. number of concurrent sessions	200,000	400,000	1,000,000	1,500,000	5,000,000
Max. number of static routes	512	2,048	5,120	5,120	10,240
Max. number of dynamic routes	10,000	350,000	350,000	350,000	700,000
802.1Q VLAN	128	256	512	512	1,024

VPN	EVA1	EVA2	EVA3	EVA4	EVAU
Max. number of IPSec VPN tunnels	200	500	750	5,000	10,000
Max. number of SSL VPN clients in portal mode	50	512	512	1,024	4,096
Max. number of simultaneous SSL VPN clients	100	150	200	250	500

The design values presented are the maximum limits of each model depending on the size of memory allocated to the Elastic Virtual Appliance product. Reduction of the allocated memory can affect the resources configured.

TECHNICAL SPECIFICATIONS

PERFORMANCE*	EVA1	EVA2	EVA3	EVA4	EVAU
Firewall throughput (1,518 byte UDP)	16.4 Gbps	27 Gbps	45 Gbps	45 Gbps	63 Gbps
IPS throughput (1,518 byte UDP)	8.6 Gbps	12.7 Gbps	20 Gbps	20 Gbps	33 Gbps
IPS throughput (1 MB HTTP)	5 Gbps	8.5 Gbps	12.7 Gbps	12.7 Gbps	14.5 Gbps
Antivirus throughput	0.9 Gbps	1.7 Gbps	3.1 Gbps	3.1 Gbps	7.1 Gpbs
IPSec throughput - AESGCM/SHA2	2.5 Gbps	3.7 Gbps	6.7 Gbps	6.7 Gbps	10.6 Gbps
New sessions per second	44,000	74,000	93,000	93,000	112,000

REDUNDANCY	EVA1	EVA2	EVA3	EVA4	EVAU
High availability (Active/Passive)	✔	✔	✔	✔	✔

*: The technical specifications of the virtual environment measured are: Intel Platinum 8168 24C@2.7GHz CPU and Intel XL710 network adapters - VMware vSphere 6.7 - SR-IOV enabled.

PLATFORMS SUPPORTED

VMware ESX/ESXi
Version 6.5, 6.7 and 7.0

Linux KVM
Red Hat Enterprise 7.9

Citrix Xen Server
Version 7.6

Microsoft Hyper-V
Windows Server 2012 R2 and 2019

FEATURES

USAGE CONTROL
Firewall/IPS/IDS mode - Identity-based firewall - Application detection and management - Microsoft Services Firewall - Industrial firewall/IPS/IDS - Industrial application control - Detection and control of the use of mobile terminals - Application inventory (option) - Vulnerability detection (option) - Geolocation (countries, continents) - Dynamic Host Reputation - URL filtering (embedded database or cloud mode) - Transparent authentication (Active Directory, SSO Agent, SSL, SPNEGO) - Agent based multi-user VDI authentication (Citrix-TSE) - Guest and sponsorship mode authentication, webservices.

PROTECTION FROM THREATS
Intrusion detection and prevention - Protocol autodetection and compliance check - Application inspection - Protection from denial of service (DoS) attacks - 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 reaction to attack (notification, quarantine, block, QOS, dump) - Antispam and antiphishing: reputation-based analysis, heuristic engine - Embedded antivirus (HTTP, SMTP, POP3, FTP) - SSL decryption and inspection - VoIP protection (SIP) - Collaborative security: IP reputation, Cloud-based Sandbox in Europe (option).

CONFIDENTIALITY OF EXCHANGES
Site-to-site or nomad IPSec VPN - Remote SSL VPN access in multi-OS tunnel mode (Windows, Android, iOS, etc.) - SSL VPN agent with automatic configuration (Windows) - IPSec VPN support for Android/iPhone.

NETWORK - INTEGRATION
IPv6 - NAT, PAT, transparent (bridge)/routed/hybrid modes - Dynamic routing (RIP, OSPF, BGP) - Multicast - Multiple link management (balancing, failover) - Multi-level internal or external PKI management - Multi-domain directories (including internal LDAP) - Explicit proxy - Policy-based routing (PBR) - QoS management - DHCP client/relay/server - NTP client - DNS proxy-cache - HTTP proxy - SD-WAN, Multifactor Authentication (MFA).

MANAGEMENT
Web-based management interface with privacy mode (GDPR compliance) - Object-oriented security policy - Contextual security policy - Realtime configuration helper - Rule counter - Connected or disconnected security updates - Global/local security policy - Embedded log reporting and analysis tools - Interactive and customisable reports - Support for multiple syslog servers UDP/TCP/TLS - SNMP v1, v2c, v3 agent - IPFIX - Automated configuration backup - Open API - Script recording.

Document not contractually binding. The features mentioned are those of version 4.x.