

StoneGate™ Intrusion Prevention System Appliance Comparison Datasheet

October 2010



Next Generation Security

- Vulnerability-centric and zero-day protection with regular expression-based fingerprinting and protocol validation
- Threat protection – DoS/DDoS, buffer overflow, worm, spyware, malware, adware, backdoor, trojan, reconnaissance, Microsoft /Linux/Unix vulnerabilities on client- and server-side and other suspicious traffic
- Web 2.0 protection and content filtering
- More than 3 500 detected situations for more than 170 protocols and applications
- Transparent (layer-2) deep inspection firewall capabilities prevent unauthorized access between security zones
- SSL inspection of encrypted Web traffic for both client- & server side protection
- Minimized false positives with event correlation and context sensitive fingerprinting
- IDS and/or IPS simultaneously
- DLP library of signatures
- Network application identification and control – P2P, IM, streaming and tunneling protocols
- Full protocol decode and analysis – Ethernet, IPv4, IPv6, ICMP, UDP, TCP, DNS, FTP, HTTP, IMAP, SMTP, SSH, NBT, SMB, MSRPC, POP3, SIP

Next Generation Availability & Scalability

- Built-in patented High Availability technologies
- IPS clustering in a serial or parallel configuration
- Built-in bypass functionality

- Back-up analyzer for fast alert, log and data recovery
- Network status and traffic optimization tools
- Flexible deployments even in the most demanding environments
- No special network configurations required

Next Generation Management

- Single console – complete visibility and proactive control of physical and virtual networks
- Third-party event management – monitoring, logging and reporting of switches, routers and security appliances from other vendors
- One-step management – automatic “blacklisting,” automatic policy/rule execution, create once, deploy everywhere policy/rule execution
- Accelerated incident management – correlated view of all network activity, powerful data mining engine and sophisticated incident case management tools
- Central repository – shared rules for Firewall and IPS, repository backup for disaster recovery, customizable role-based access, domains for managing different environment with one management server
- Real-time monitoring and alerting – customizable dashboards and alerting, geographic pinpointing of IP addresses, Web portal for monitoring security from any device
- Interactive reporting and compliance with PCI, HIPPA, SOX and Basel II and other regulations – customizable reports, automated report generation and distribution, system auditing and audit trails, comparative analysis of security policies

STONESOFT

Secure Information Flow



StoneGate™ IPS for Demanding Environments

The StoneGate IPS uniquely integrates the most advanced security techniques with our patented high availability technologies and sophisticated next generation management so your business will never miss a beat... no matter what threat comes your way.

In fact, according to industry experts like NSS Labs and ICSA Labs, the StoneGate IPS offers one of the highest levels of protection, performance and manageability at the lowest total cost of ownership on the market today – as much as 30-70% than other products. From the largest data centers and enterprise networks to your remote offices, we offer solutions to fit your specific needs.



Appliance Specifications	IPS-1030	-Z	IPS-1060	-P	IPS-1205	IPS-3201	IPS-3205
Software	Sensor	Analyzer	Sensor		Sensor	Sensor	Sensor
Inspected throughput	200 Mbps		350 Mbps	600 Mbps	2 Gbps	5 Gbps	13 Gbps
Latency	< 150 µs		< 150 µs		< 150 µs	< 150 µs	< 150 µs
Connections/s	15 000		30 000		50 000	240 000	750 000
Concurrent connections	300 000		400 000		1 300 000	5 000 000	15 000 000
SSL inspection client/server side	40 Mbps / 40 Mbps		60 Mbps / 60 Mbps		350 Mbps / 350 Mbps	yes / yes	yes / yes
Network Interfaces	6 x 10/100/1000	2 x 10/100/1000	6 x 10/100/1000		6 x 10/100/1000	2 x 10/100/1000	2 x 10/100/1000
Bypass interface pairs	2	-	2		2	*max 6	*max 6
Layer-2 firewall	yes	-	yes		yes	yes	yes
Analyzer	option	yes	option		option	yes	yes
Web filtering	option	-	option		option	option	option
Number of detection signatures	3 500+		3 500+		3 500+	3 500+	3 500+
Inline serial clustering /HA	yes		yes		yes	yes	yes
VLAN inspection	4 094		4 094		4 094	4 094	4 094
Dynamic overload handling	yes	-	yes		yes	yes	yes
Form factor	1U rack		1U rack		1U rack	2U rack	2U rack
Dimensions (W x H x D)	425 x 44 x 362 mm 16.73" x 1.73" x 14.25"		425 x 44 x 362 mm 16.73" x 1.73" x 14.25"		426 x 44 x 400 mm 16.77" x 1.73" x 15.7"	437 x 89 x 450 mm 17.2" x 3.5" x 17.7"	437 x 89 x 450 mm 17.2" x 3.5" x 17.7"
Module slots	-		-		-	3	3
Redundant power supply	-		-		-	yes	yes