Stonesoft IPS 5.6

Stonesoft IPS Datasheet

Stonesoft Intrusion Prevention System (IPS) detects malicious or unwanted activity within regular network traffic and prevents intrusions by blocking the offending traffic automatically before any damage occurs.

KEY BENEFITS

- **Advanced threat and evasion protection.** Utilizing our multi-layer traffic normalization and inspection technology, Stonesoft IPS offers the highest level of security against advanced attack methods and evasion techniques (AET) without compromising traffic speed or availability across the network.

- **Application and user control.** Stonesoft IPS utilizes Next-Generation IPS (NGIPS) technology, featuring port-independent application and user identification. Combined with detailed logging and reporting, this means you always have excellent visibility of network data and security events in real-time.

- **Traffic Shaping.** Prioritize business-critical applications and network communications over other network communications. Throttle bandwidth for less important network applications and protocols.

- **Flexible network deployment.** Stonesoft IPS is transparent to surrounding network components such as switches and routers, or other network security devices. Configurable fail-open/normal network interfaces and dynamic inspection overload handling guarantee uninterrupted network operation.

- **Software-based solution.** Stonesoft IPS is available as a physical appliance, software, or a virtual solution. All options are software-based and receive new features and updates automatically. The solution has been designed from the ground up to offer significant performance.

- **Powerful management.** The award-winning Security Management Center is at the core of the IPS. In addition to next-generation security and built-in high availability, administrators also have the ability to easily manage and/or monitor all security devicesacross their network – whether the devices are virtual, physical, hybrid, or from another vendor.

STONESOFT
A McAfee Group Company

IPS 5.6 Specifications

GENERAL	
Supported Platforms	
Stonesoft Appliances	1035, 1065, 1302, 3202, 3206, 5206 appliances. See more details from appliance specific datasheets.
Software Appliance	X86-based systems. See more details from software appliance datasheet.
Virtual Appliance	VMware ESX virtualization platforms. See more details from Virtual appliance datasheet.
Operating modes	IDS / IPS / Layer 2 Firewall

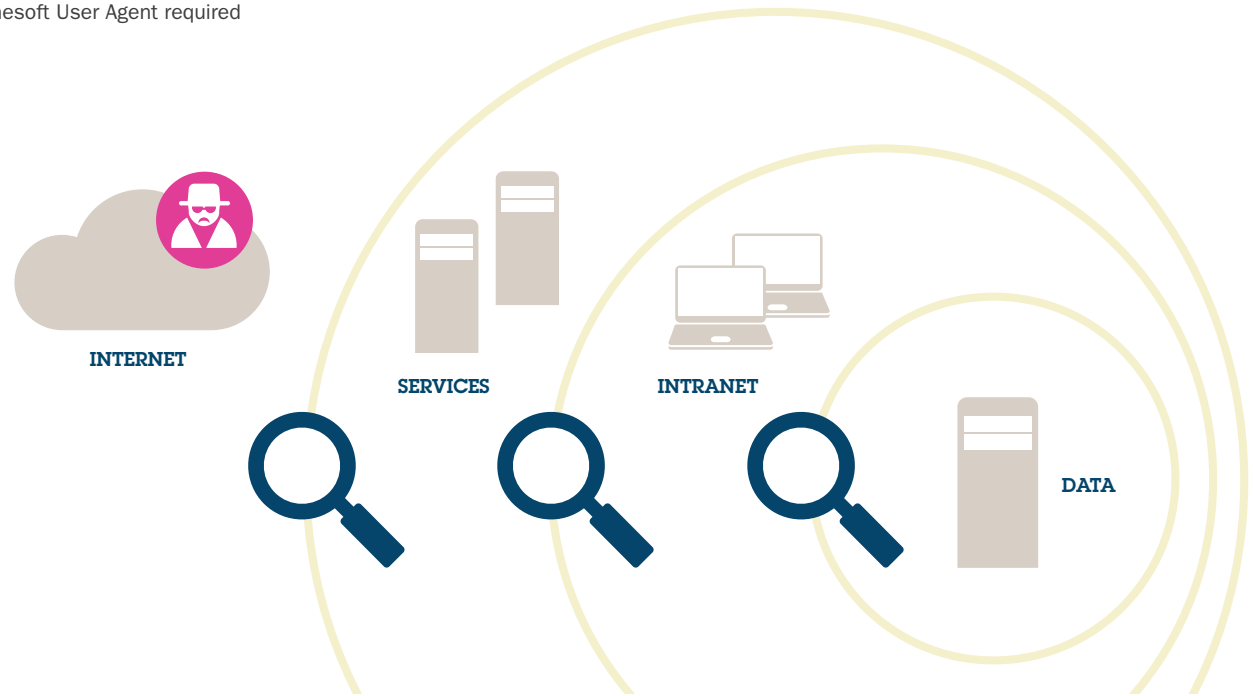
IPS AND LAYER 2 FIREWALL-SPECIFIC FUNCTIONALITY	
General	Stateless packet filtering for Ethernet protocols Stateful packet filtering for IP protocols Logical interface matching for VLANs and physical interfaces MAC address filtering
High availability	IDS clustering (active-active / active-passive) IPS serial clustering (active-active) Layer 2 Firewall clustering (active-passive) Fail-open interface support (IPS role) Dynamic overload handling (IPS role)
User identification	MS Active Directory *

GENERAL FUNCTIONALITY (ALL OPERATING MODES)	
Encapsulation	Ethernet (Dix / IEEE), 802.1q VLAN
Access control	IPv4 and IPv6 IP-in-IP IPV6 encapsulation GRE
Advanced access control	Interface zones Time TLS information Domain names User information Applications
Traffic management and QoS	Policy-based traffic shaping Guaranteed / maximum / bandwidth prioritization Differentiated Services Code Point (DSCP) matching / marking Concurrent session limiting
Inspection	
Dynamic context detection	Protocol Application File type (Flash, GIF, JPEG, MPEG, OLE, PDF, PNG, RIFF, RTF, text file, binary file)
Protocol normalization	Full protocol normalization for Ethernet, IPv4, IPv6, ICMP, UDP, TCP, DNS, FTP, HTTP, IMAP, IMAPS, SMTP, SSH, NBT, SMB, SMB2, MSRPC, POP3, POP3S, SIP, TFTP, HTTPS, GRE, IP-in-IP, IPv6 encapsulation
Protocol specific fingerprint inspection	DNS, FTP, HTTP, HTTPS, IMAP, SMTP, SSH, NBT, SMB, SMB2, MSRPC, IMAP, IMAPS, POP3, POP3S, SIP, TFTP
Protocol independent fingerprint inspection	Any TCP / UDP protocol
Evasion and anomaly detection	Multi-layer traffic normalization Vulnerability-based fingerprints Exploit-based fingerprints Fully upgradable software based inspection engine Evasion and anomaly logging
Custom fingerprint inspection	Protocol independent fingerprint matching Regular expression-based fingerprint language Snort ® signature converter Custom application fingerprinting
TLS inspection	HTTPS client and server stream decryption and inspection TLS certificate validity checks Certificate domain name based exempt list

Correlation	Local correlation, log server correlation
DoS/DDoS protection	SYN/UDP flood detection Concurrent connection limiting, interface-based log compression
Reconnaissance	TCP/UDP/ICMP scan, stealth and slow scan detection in IPv4 and IPv6
Blocking methods	Direct blocking, connection reset, blacklisting (local and distributed), HTML response, HTTP redirect
Traffic recording	Policy based traffic recordings, automatic excerpts from misuse situations
Updates	Automatic dynamic updates through Security Management Center (SMC). Current coverage over 3000 protected vulnerabilities.
Web filtering (subscription required)	
Protocols	HTTP, HTTPS
Engine	Category based URL filtering, Blacklist / exempt list
Database	Over 280 million top level domains and sub pages (total billions URLs) Support over 43 languages 82 Categories
Management and Monitoring	
Centralized Management	Enterprise level centralized management, logging and reporting system. See more details from Security Management Center datasheet
SNMP monitoring	SNMPv1, SNMPv2c and SNMPv3
Traffic capturing	Console tcpdump, remote capturing through SMC
High security management communication	256-bit security strength in engine – management communication

PLATFORM CERTIFICATIONS	
ICSA Labs	Network IPS enterprise certified
NSS Labs Tested	Network Intrusion Prevention, Next Generation Firewall, Firewall
VMware	Virtual appliance VMware ready certified
RSA	Secured by RSA certified with RSA SecureID and RSA envision
Arcsight	Common Event Log format (CEF) certified
Q1Labs	Log Event Enhanced Format (LEEF) certified

* Stonesoft User Agent required



Stonesoft Corporation International Headquarters
Itälahdenkatu 22A FI-00210 Helsinki, Finland
tel. +358 9 4767 11 | fax. +358 9 4767 1349
www.stonesoft.com

STONESOFT
A McAfee Group Company

Stonesoft Inc Americas Headquarters
1050 Crown Pointe Parkway, Suite 900
Atlanta, GA 30338, USA
tel. +1 866 869 4075 | fax. +1 770 668 1131