

Stonesoft™ IPS-1030

December 2011

Stonesoft™ High Availability IPS Appliance Datasheet

Stonesoft™ Intrusion Prevention System is a proactive defense system designed to detect malicious packets within regular network traffic and prevent intrusions by blocking the offending traffic automatically before any damage occurs.

Stonesoft IPS-1030 is designed for small enterprises, branch offices and internal network segments. The appliance features sensor and analyzer functionalities, giving flexible protection for environments requiring ultimate ease of usage.

Stonesoft IPS-1030 sensor appliance can protect up to two inline segments. The sensor has in-built bypass interface pairs for each inline segment and two standard Ethernet interfaces. Standard interfaces can be used as capture interfaces for intrusion detection and one of them is needed for Stonesoft management traffic.

Combined with Stonesoft Firewall, IPS-1030 forms a multidimensional defense system where several security layers communicate seamlessly together. Utilizing the Stonesoft's Multi-layer Traffic Normalization and inspection technology, the Stonesoft™ IPS-1030 offers the highest level of security against Advanced Evasion Techniques (AET).

Stonesoft™ IPS-1030 and all other Stonesoft appliances offer comprehensive network security with easy configuration and unified management. This ensures an optimized solution for any geographically dispersed enterprise deployment.

STONESOFT

Stonesoft™ IPS-1030 Specifications



KEY FEATURES

General

Protects	Vulnerable applications and operating systems from network attacks against client and server vulnerabilities.
Evasion protection	Stonesoft IPS with Multi-layer Traffic Normalization features provides protection against Advanced Evasion Techniques (AET). IPS decodes and normalizes network traffic for inspection on all protocol layers. Vulnerability-based fingerprints block exploits in the normalized data stream. Antievasion features are upgraded in software maintenance versions.
Web filtering	Category based Web filtering solution containing millions of URLs in 90 categories guarantees accurate visibility and control for Web browsing. Optional with additional license.

Deep Inspection

Protocol agents	Full protocol decode and analysis – Ethernet, IPv4, IPv6, ICMP, UDP, TCP, DNS, FTP, HTTP, IMAP, SMTP, SSH, NBT, SMB, MSRPC, POP3, SIP, TFTP, HTTPS (SSL/TLS)
Misuse detection	Vulnerability based regular expression fingerprints Exploit based fingerprints Protocol independent fingerprint matching for any TCP/UDP protocols
DoS/DDoS detection	Syn flood, UDP flood, Connection flood
Reconnaissance	TCP/UDP/ICMP scan, stealth and slow scan detection

Access Control

Application	Network application identification and control for P2P, IM, streaming, remote control and tunneling protocols
IPv4/IPv6	Stateful access control and logging.
Ethernet	Packet filtering and logging for any Ethernet traffic (Dix/IEEE)

FEATURES

High availability and clustering	IPS clustering (active-active)
	IDS clustering (active-active/active-passive)
	Configurable bypass/normal network interfaces
Layer-2 Firewall	Layer-2 transparent, next generation firewall protection
SSL inspection	HTTPS client stream decryption and inspection
	HTTPS server stream decryption and inspection
VLAN Inspection	Maximum number of inspected VLANs (802.1q) is 4094
Dynamic overload handling	Prioritizing continued connectivity over inspection coverage under IPS overload situation (configuration option)

Management and Monitoring

Centralized Stonesoft Management Center	Enterprise level centralized management, logging and reporting system. See more details from Stonesoft Management Center datasheet
SNMP monitoring	SNMPv1, SNMPv2c and SNMPv3

Certificates

ICSA NIPS Certified	Continuous testing by ICSA Labs, NSS Labs Certified
---------------------	---

Licensed Performance

HTTP throughput (21KB payload)	90 Mbps
New HTTP connections per second	650
UDP throughput (1514B packet size)	200 Mbps
New TCP connections per second	15 000
Concurrent TCP connections	300 000
SSL inspection	50 Mbps
Latency	< 150 microseconds
Transparent Layer-2 Firewall	Yes
Web filtering	Optional, activated with license

HARDWARE

Network Interfaces

Ethernet	6 x 10/100/1000 copper
Bypass interface pairs	2
Connectors	RS-232 serial console, 2 x USB

Measurements

Form factor	1U 19" rack unit
Dimensions (W x H x D)	425 x 44 x 362 mm / 16.73 x 1.73 x 14.25 inches
Net weight	5.5 kg / 12.13 lbs
Gross weight	8.5 kg / 18.74 lbs

Safety / EMC Certifications

CE, FCC, CB, Gost-R, RoHS

Power

Power supply	180 W, AC Input 100-240 VAC, 50-60 Hz
Typical power consumption	90 W

Other

Operating temperature/humidity	5—35°C (41—95°F) 5%—95%, non condensing humidity (RH)
Storage temperature/humidity	-20—70°C (-4—158°F) 5%—95%, non condensing humidity (RH)
MTBF	120 000 h

SUPPORT

Replacement service	15 months or 39 months replacement service for non-complying hardware
Premium support	24/7-call logging via web, email and phone, two-hour response time, software updates, hardware replacement service
Basic support	8/5-call logging via web, email and phone, next business day response time, software updates, hardware replacement service

Product codes

APP-IPS-1030-C4	Stonesoft IPS-1030 appliance
APP-IPS-1030-C1-Z	Stonesoft IPS-1030 analyzer appliance
FP-IPS-ANZ1	Analyzer module for IPS-1030 appliance
FP-1Y-WF2-151	One year Web filtering subscription for IPS-1030