



January 2008

StoneGate™ Intrusion Prevention System Appliance Datasheet

StoneGate™ IPS-2000

The StoneGate™ IPS-2000 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.

With the capacity of 600 Mbit/s StoneGate IPS-2000 is designed for branch offices, DMZ's, extranet or internal network segments. Appliance features both sensor and analyzer functionalities, giving flexible protection for environments requiring ultimate ease of usage. For most capacity demanding environments StoneGate IPS-2000 can be configured to feature separate sensor or analyzer mode, combining several appliances into one virtual security engine.

All StoneGate IPS-2000 sensor appliances can protect up to two inline segments. They have a bypass interface pair for each inline segment and four standard Ethernet interfaces. Standard interfaces can be used as capture interfaces for intrusion detection and one of them is needed for StoneGate management traffic.

Combined with StoneGate Firewall, IPS-2000 with transparent access control forms a multi-dimensional defense system where several security layers communicate seamlessly together. This field-proven technology provides comprehensive protection of the whole network, raising network security to a previously unseen level.

The StoneGate IPS-2000 and all other StoneGate appliances offer comprehensive network security with easy deployment and unified management. This also guarantees an optimized solution for any geographically dispersed enterprise deployment.

StoneGate™ IPS-2000 Specifications

No False Positives

Efficient network attack detection using sensor and analyser
Extended protocol validation
Over thousand fingerprints
Efficient access control

Detects spyware, DoS attacks, port scans, worms, Microsoft/Linux/Unix vulnerabilities on client and server side
Ethernet, IP, ICMP, UDP, TCP, DNS, FTP, HTTP, SMTP, SSH, NBT, SMB, MSRPC, SIP
IMAP, LDAP, MSSQL, MYSQL, Oracle, TFTP, PPTP, POP3, X11 etc.
Stateful access control for all Ethernet traffic with Transparent Access Control Module

Effective Prevention

Inline terminate, Blacklist/Whitelist, TCP Connection Termination

Flexible Deployment

Appliance supports both IPS and IDS modes and the combination of these. Inline mode sensor can protect two physical inline segments (more segments possible if VLAN tagging is used). IDS mode uses span port monitoring or Full-Duplex TAP monitoring. Installation without any network configuration changes with TAC module. Clustering for flexible performance expansion in IDS and inline-IPS*.

Efficient Management

Remote, centralized enterprise management with StoneGate Management Center, Java-based GUI, encrypted and authenticated connections

Automatic Upgrades & Updates
Extensive Logging Methods
Multiple Alert Methods
Efficient Administration

Software upgrades and dynamic updates
Direct file archive, advanced filters, traffic recording
E-Mail, SMS (text message), SNMP trap, User-defined scripts
Multiple administration accounts, simultaneous administration, three different administrator levels

Additional Modules

Transparent Access Control (TAC)

Certification

StoneGate IPS is certified by ICSA Labs

Configuration

IPS-2000S Sensor Appliance
IPS-2000ANZ Analyzer Appliance
IPS-2000C Combined Sensor/Analyzer Appliance
IPS-2000N Appliance with no bypass interfaces, can be used with external bypass device

Network interfaces

IPS-2000S/C - full copper version 4 x bypass interfaces 10/100/1000 copper,
4 x standard interfaces 10/100/1000 copper

IPS-2000S/C - fiber version 4 x bypass interfaces 1000 Base-SX fiber,
4 x standard interfaces 10/100/1000 copper

Analyzer 4 x standard interfaces 10/100/1000 copper

IPS-2000N 8 x standard interfaces 10/100/1000 copper

Performance

Throughput 600 Mbit/s, latency < 200µs. Smooth performance expansion with inline IPS serial clustering*.

Features

High Availability Back-up analyzer* for fast alert, log and monitoring data recovery. Inbuilt bypass functionality.

Mechanics

Dimensions (W x H x D) 1U-19" rack unit, 427 x 43 x 356 mm/16.8" x 1.7" x 14"
Weight 6,2 kg/13,7 lbs
Power Supply 260W, 4A
Connectors 2 x USB ports, 1 x serial port, 1x VGA. Fiber Connection type 1000 Base-SX, LC connector

Safety/EMC Certification

FCC, CE, CB

Support

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

* Available for sensor appliances