

FEATURES/BENEFITS

- **System supports real-time network surveillance for a wide range of applications such as:**
Lawful intercept, national security/intelligence gathering, and cyber crime detection.
- **Fast: Performs deep packet inspection at wire speeds**
Host processor with multiple packet inspection accelerators (PIXLs) supports multiple, identity-free, 1Gbps and 10Gbps interfaces.
- **Distributed architecture is scalable for even higher performance**
Multiple DeepSweeps can be combined via configurable pipelining/parallelizing to increase performance and functionality. Available in 1Gbps and 10Gbps models
- **Flexible and extensible system serves evolving surveillance needs**
Use one or more DeepSweeps as standalone appliance(s), in conjunction with other equipment, or enhanced with co-residing user applications.
- **Quick and easy to configure**
Browser-based setup screens enable fast, flexible configuration of complex surveillance logic at network/protocol level or application level.

The IP Fabric's DeepSweep™ is the first 1Gbps and 10Gbps system optimized for real-time IP network surveillance.

The DeepSweep system is a very powerful configurable appliance for performing deep packet inspection (DPI) on network traffic and acting on traffic of interest. For example, traffic can be inspected at layers 2-7 of network protocols, using complex constructs such as broad protocol filters, classification databases, white/black lists, and signature databases. Once traffic of interest has been detected, the DeepSweep provides a flexible set of actions, such as recording the traffic in a local file, encapsulating and transmitting the packet, generating SNMP alerts, transmitting to a local or remote surveillance module, or passing to a locally-residing user application.

DeepSweep has the capability to fully inspect every network packet using easily-expressed, complex surveillance logic, while also providing a flexible set of actions to take when packets, flows, and conversations of 'interest' are detected. This power and flexibility make DeepSweep ideal for detection and forensics of crimes and abuse on both public and internal networks.

DeepSweep™ 1Gbps and 10Gbps IP Network Surveillance System



IP Fabric's DeepSweep systems are the industry's only self-contained network surveillance systems for 1Gbps and 10Gbps IP networks.

1Gbps and 10Gbps Models, Scalable Architecture

Based on IP Fabric's innovative Surveillance Module™ architecture and underlying patent-pending multi-core virtualization technology, DeepSweep provides many unique advantages over PC-based or hard-wired ASIC-based surveillance systems.

DeepSweep's internal host processor and multi-core packet inspection accelerators allow it to monitor multiple 1Gbps (DeepSweep-1 Model) and 10Gbps (DeepSweep-10 Model) Ethernet links at true wirespeed with full layer 2-7 DPI capabilities.

The innovative Surveillance Module architecture enables DeepSweep to be used as a stand-alone network surveillance system, in conjunction with other security/surveillance systems (e.g., as a pre-filter) and even supports hosting user-applications on the system processor. The highly scalable architecture allows multiple DeepSweeps to be configured in parallel or pipelined, as well as enabling remote systems to share learned information (e.g., dynamic IP address assignment, VoIP call establishment information).

DeepSweep™ -1 and DeepSweep™ -10 Datasheet

PRODUCT SPECIFICATIONS

DeepSweep-1 and DeepSweep-10

Surveillance Inspection:

Payload

- Regular expressions
- Updatable signature databases
- Advanced protocol-specific and application level inspection and analysis via Surveillance Modules

Layer 2

- Ethernet, PPP, VLAN, MPLS

Layer 3/4

- Built-in IPv4 and IPv6 support
- Common protocols (e.g., TCP, UDP, HTTP, etc)
- Powerful, updatable classification database (wildcards, ranges, etc)

Surveillance Actions:

- Record to system record file (.PCAP)
- Encapsulate, optionally encrypt, and transmit recording record
- Accumulate statistics
- Pass to co-residing user application via Linux socket
- Pass to next Surveillance Module
- Reflect input out a network interface
- Generate SNMP trap
- Generate a database update message to another DeepSweep
- Monitor via web browser
- Retransmit in application-specific standardized format, such as CALEA

Surveillance Modules:

- Packet traffic: individual L3-L7 packet analysis at the network/protocol level
- Packet flow: L3-L7 flow-based analysis at the network/protocol level
- Sub IP: L2/2+ analysis (e.g. Ethernet, PPPoE, MPLS)
- DNS: protocol-specific analysis of DNS lookups
- User Connection: protocol-specific analysis of user login, authentication, IP assignment
- Future Options
 - Unusual traffic: malformed packets, improper fragments, protocol anomalies other equipment
 - SIP/RTP Intercept: protocol-specific analysis of SIP messages, packets, flows
 - Email: protocol-specific analysis of common email protocols (e.g., SMTP) and email content

POWERFUL BROWSER-BASED INTERFACE



DeepSweep-1 and DeepSweep-10 share the same browser interface which provides an easy way to express complex surveillance logic.

DeepSweep-1

Performance and Capacities:

- Dual 3.6GHZ Xeon host with 2 or 4 packet inspection accelerators
- Up to 500GB (usable) of RAID1 disk space
- Up to 1,000,000 flows, 5,000 signatures, 8Gbps wire-speed surveillance

I/O:

- 4 or 8 10/100/1000 identity-free Ethernet surveillance interfaces
- Flexible physical interfaces on surveillance ports via pluggable SFPs
- 2 Gb Ethernet system ports

Power:

- Hot-swappable, redundant, auto-sensing 100-240 VAC

Physical/Mechanical:

- Rack mountable, 2U appliance
- Dimensions: 3.45" (H) x 17.14" (W) x 20" (D)
- Weight: 33lbs

Environmental (preliminary):

- Temp: 10 c to 35 c (operating), -40 c to 70 c (non-operating)
- Non-operating humidity: 95% non-condensing

Safety/Emissions (preliminary):

- UL 1950, CSA 950, IEC 950, TUV/GS EN60950
- FCC Class A certified. Tested to CISPR 22, EN55022, VCCI ITE, AS/NZS 3548 Class A

Regulatory Markings (preliminary):

- CE, FCC, VCCI, RoHS/WEEE

DeepSweep-10

Performance and Capacities:

- Dual-Core Intel® Xeon host processor (4 total cores) with Dual OCTEON™ CN58xx packet inspection acceleration (32 MIPS CPUs)
- 73 GB (usable) of disk space, expandable via external storage
- Wire-speed surveillance on typically-loaded 10Gbps Ethernet links

I/O:

- 4 10Gbps and 6 10/100/1000 bps identity free Ethernet surveillance interfaces,
- Flexible interfaces on surveillance ports via pluggable SFP/SFP+
- 2 Gb Ethernet system ports

Power:

- Dual -48/-60 VDC inputs with 15 Amp fuse protection
- Rear pluggable 850W AC

Physical/Mechanical:

- 2U 2-slot ATCA
- Height: 86.6mm (2U)
- Width: 19 inches
- Depth: 20 inches
- Weight (preliminary): 21lbs

Environmental

- Operating temp: 5 c to 40 c
- Non-operating temp: -40 c to 70 c

ORDERING INFORMATION

For more information, including pricing, availability, and ordering, please contact IP Fabrics by email at info@ipfabrics.com or at the phone number at right.



IP Fabrics, Inc.
14976 NW Greenbrier Pkwy
Beaverton, OR 97006

Tel: 503-444-2400
Fax: 503-444-2401

www.ipfabrics.com