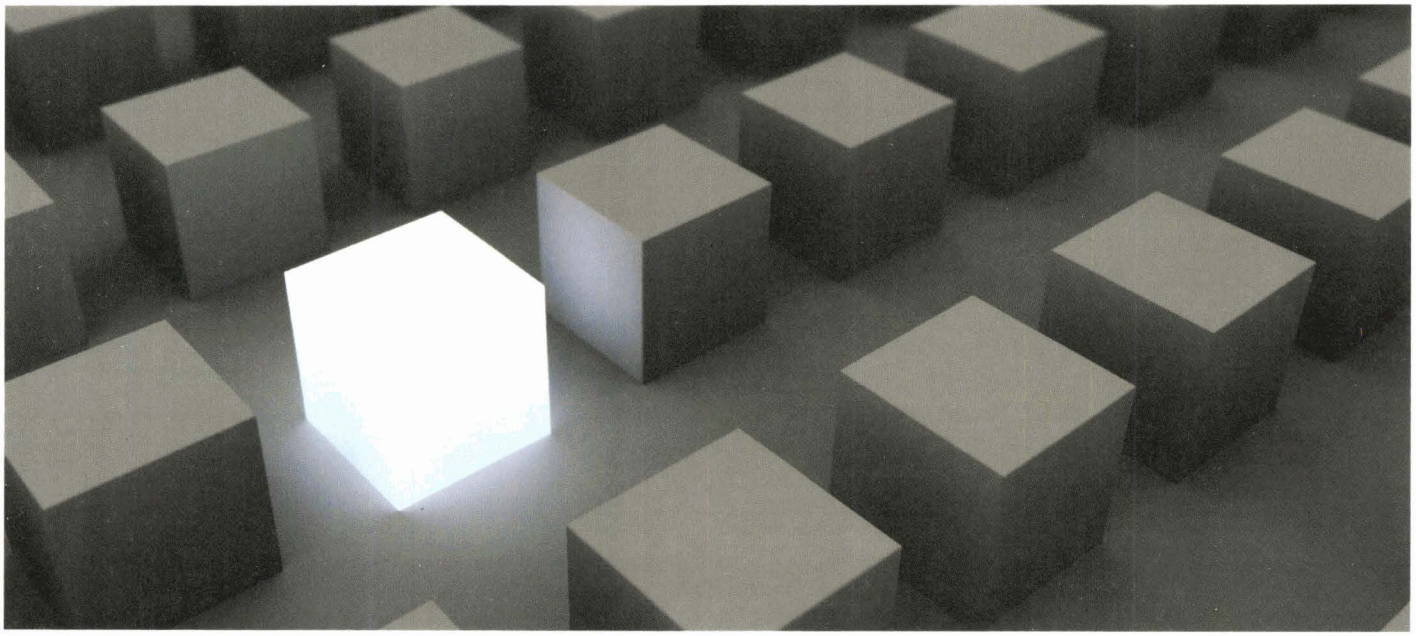
DATA SHEET

DPX NETWORK PROBE

DPX Network Probe is a passive IP probe for lawful interception, mass interception and network monitoring. It uses ipoque's deep packet inspection (DPI) technology to identify and filter network flows according to their application protocol. Target triggers comprise protocol-specific filtering criteria including network addresses, user names, protocol-specific attributes and arbitrary content keywords. This unique combination of DPI and flexible target rules delivers high quality interception data while avoiding the capturing of a large volume of unnecessary network traffic. It significantly reduces the burden on subsequent processing and mediation systems.



ADVANCED DPI ENGINE

DPX Network Probe uses PACE, ipoque's field-proven deep packet inspection (DPI) engine to enable target triggering and filtering based on communication protocol and application.

- DPI technology combining layer-7 pattern matching, behavioral, statistical and heuristic analysis
- Support for close to 200 protocols covering thousands of applications
- High classification accuracy with very low false negative rate and virtually no false positives
- Reliable detection of obfuscated and encrypted protocols such as Skype, BitTorrent, SSL and many VPN tunnels
- Support for asymmetric traffic identification
- Correlation of signaling & content data flows

POWERFUL TARGET TRIGGERING

DPX Network Probe features a powerful rules engine that combines traffic identification criteria with versatile actions specifying how matching traffic will be handled. The traffic identification criteria allow to match on specific targets and application flows and to filter out irrelevant data that would otherwise overload the post-processing chain. The string search engine enables matching on arbitrary payload keywords and virtual identities such as e-mail addresses, IM user names and SIP phone numbers.

Generic Keyword Spotting

- String search across the entire content of an application data exchange
- Capitalization and single-character wildcards
- Multi-word expressions with full Boolean expression support

HIGHLIGHTS

- IP network probe for lawful interception, mass interception and network surveillance
- DPI engine for layer-7 traffic identification and filtering with support for encrypted and obfuscated protocols
- Target triggering by protocol, application and content attributes
- Application layer metadata generation
- Raw packet and content stream forwarding
- Wire speed operation at multiple 10 Gbit/s
- Keyword spotting at wire speed
- Full IPDR and CDR generation for all network flows

- Support for up to 25,000 keywords
- Full TCP reassembly to facilitate keyword search across packet boundaries
- On-the-fly application-layer decoding for Base64 e-mail attachments, HTTP chunked transfer encoding, HTTP gzip/deflate content compression and Base64-encoded HTTP data URIs
- Generic stream search covering the full TCP or UDP flow

Layer-7 Filters

- Layer-7 protocol or application
- Protocol- and application-specific keywords covering specific parts of a transmission
  - HTTP hosts and URIs
  - HTTP request header & body, response header & body
  - Web proxy URIs
  - E-mail (POP3, IMAP4, SMTP) sender, recipients including CC, BCC, subject, body
  - VoIP: SIP caller/callee

Layer-2-4 Filters

- IP addresses, port numbers and ranges
- Black- and whitelists for IP, MAC and MPLS

All trigger criteria listed above can be combined (e.g. layer-7 protocol AND IP address AND e-mail address). DPX Network Probe supports large rule sets with up to 25,000 concurrent rules per system or per blade.

TRAFFIC PROCESSING BY RULE ACTIONS

The action part of a rule defines how to act on a match by a trigger criterion, allowing to forward the Content of Communication (CC) and Intercept Related Information (IRI) as required by ETSI.

Content Data Forwarding (CC)

- Raw packet forwarding with MAC- or GRE-based packet marking, or in PacketCable ESP 1.5 format
- Packet payload interception forwarding fully reassembled application-layer content data streams
- Integrated flow buffer for delivery of intercepted flows from the first to the last packet

Metadata Generation (IRI)

- Application- and protocol-specific metadata, or IP Detail Record (IPDR), generation
- IPDR generation for either all flows or target flows only
- Flow IPDRs indicating trigger hit and end/timeout of a flow
- IPDR delivery using syslog
- Layer-7 IPDRs for RADIUS on all protocol events
- Layer-7 IPDR generation for e-mail (POP3, IMAP4, SMTP)
- Conditional filtering of RADIUS layer-7 IPDRs (AAA Probing)

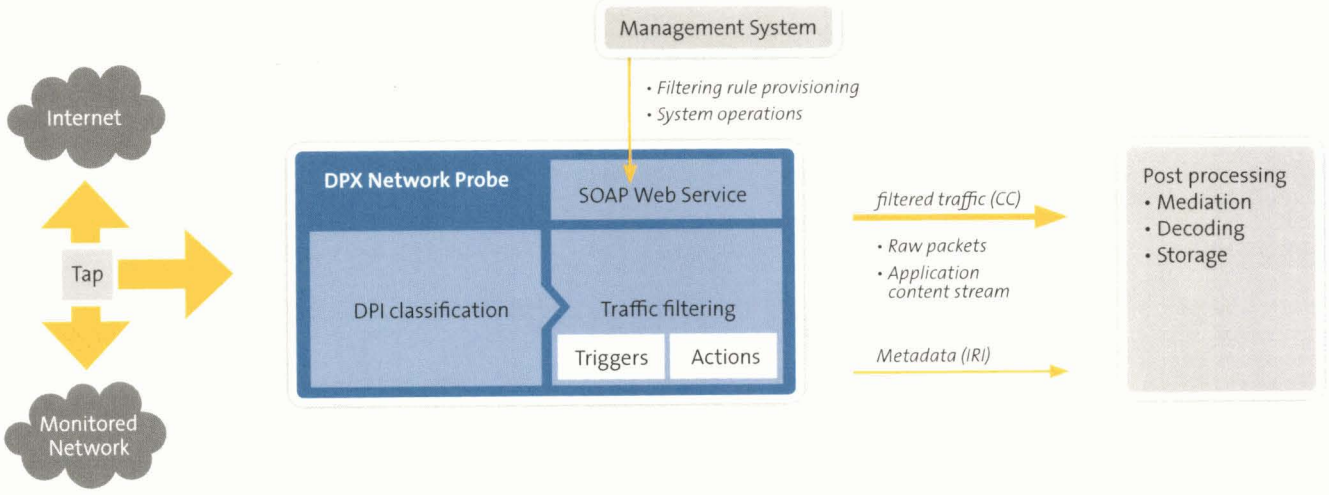
All traffic processing actions for content data forwarding and metadata generation listed above can be combined (e.g. generate flow IPDRs AND intercept raw packets).

SEAMLESS INTEGRATION & MANAGEMENT

- Flexible integration and handover interfaces
- Seamless integration in any LI infrastructure, e.g. CALEA, ETSI
- Web-based GUI for management of stand-alone systems
- SOAP Web service over HTTPS for integration with existing management and mediation systems
- Comprehensive system performance profiling information in real time
- SNMP support
- Current and historical throughput statistic (packets and bytes per direction, IPv4 and IPv6, TCP and UDP, all supported layer-7 protocols)

DPX SPECIFICATION

	DPX-1G	DPX-10G
Hardware	19" 1U appliance	19" 9U appliance based on IBM BladeCenter H
Scalability		Load-balancing cluster of up to 13 packet processing blades
Monitoring interfaces	2x 1000Base-T/LX/SX to monitor one Gigabit Ethernet link	20 XFP interfaces to monitor ten 10 Gbit/s links
Management	Dedicated 1000Base-T interface	Dedicated management blade
Performance	Full 1 Gbit/s wire speed	Full 10 Gbit/s wire speed
System throughput	2 Gbit/s	Up to 50 Gbit/s up to 30 Gbit/s for string search
Packet rate (packets per second)	1 million	1 million per blade
Concurrent flows	5.5 million	5.5 million per blade
New flows per second	400,000	400,000 per blade
Concurrent target rules	25,000	25,000 per blade
Concurrent keywords	25,000	25,000 per blade
Concurrent IP addresses	1,650,000	1,650,000



ipoque GmbH, Neumarkt 29-33, 04109 Leipzig, Germany
Phone: +49 341 59403 0 Fax: +49 341 59403 019

www.ipoque.com
info@ipoque.com