

DPX Network Probe

Comprehensive Lawful Interception and Monitoring in Broadband Networks

Highlights

- Wire speed lawful interception and network surveillance
- Full layer-7 traffic classification with support for encrypted protocols
- Flow-based interception with TCP reassembly and application-specific decoding
- Powerful protocol and keyword-based interception rules
- Stream buffer for complete session interception
- Intelligent data reduction at interception point
- Seamless integration in any LI infrastructures, e.g. CALEA, ETSI
- Protocol-specific CDR/IPDR generation



DPX Network Probe is a passive probe system for lawful interception and network monitoring. It uses ipoque's deep packet inspection (DPI) technology to classify network flows according to their application protocol. Based on user-definable rules, content and signaling data of these flows can be recorded and forwarded to external devices such as mediation systems for further processing. These rules comprise target information including IP addresses, user names, protocol-specific filtering criteria, 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 the subsequent processing and mediation systems.

In addition to the interception functions, DPX generates comprehensive application-aware statistics data on the network usage providing an additional benefit for networks operators.

The Bandwidth and Performance Challenge

Network probes today face many challenges. The network bandwidth is growing more rapidly than the performance of most computer technologies including processors and memory, making it hard to keep up with the proportionally growing data processing requirements. Much of this bandwidth surge is due to the continually rising proportion of multimedia content. Such content is mostly exchanged through peer-to-peer file sharing networks (P2P), but also through Web-based services such as YouTube and large-scale file hosting services such as Rapid-

Share. Keyword search and traffic interception usually do not make any sense for this multimedia content. Instead, an application-aware metadata generation providing information such as file names and confirmed content type has become the new challenge for LI solutions.

Another issue for LI systems is the rising number of different, often proprietary and quickly evolving protocols used to transmit application data. Protocol obfuscation and encryption becomes more and more prevalent which makes both header and content data difficult and sometimes impossible to scrutinize.

The ipoque DPX Solution

DPX Network Probe utilizes ipoque's leading deep packet inspection technology to detect and classify all application traffic prior to any search and interception operations. ipoque's DPI engine uses layer-7 pattern matching and behavior analysis technology to detect even the most elusive protocols, no matter if they use advanced obfuscation, port hopping, encryption, and other techniques to hide from detection.

Independent tests have proven that ipoque's highly parallelized DPI technology easily scales to gigabit links and beyond. The overall performance of a DPX system depends on the kind and number of deployed rules. The full protocol classification prior to any search operations, that are necessary to check the active rules' trigger criteria, allows to exclude all uninteresting applications where, for instance, a keyword search is useless. This approach further improves the overall probe performance.

High-Quality Search and Interception Data

DPX Network Probe's protocol awareness enables the deployment of powerful application-specific interception rules such as the dedicated search for e-mail addresses, instant messenger user names or SIP phone numbers within relevant flows. DPX also provides general keyword trigger criteria taking into account the various application-specific encoding schemes such as MIME Base64 encoding for e-mails or gzip compression for Web content. All keyword-based interception trigger criteria are evaluated on fully reassembled TCP streams.

The reliable protocol classification of DPX ensures that all intercepted network sessions only contain packets belonging to them. It provides clean interception data to subsequent mediation and reconstruction systems, improving their accuracy and performance.

Full Session Buffering

Many interception trigger criteria produce a match late in a network session when previous packets have already passed. For many LI applications it is key that complete sessions starting with the very first data packet are intercepted, even if, for instance, a keyword match only happens in the second attachment of an e-mail message. DPX includes a full stream buffer that stores all sessions that are being monitored and have not yet produced a search hit. The maximum buffering period depends on the number of concurrently monitored sessions, the hit-miss ratio, and the stream buffer capacity in each DPX probe.

Network Statistics – Added Value for ISPs

DPX Network Probe records detailed traffic statistics that provide operators with in-depth network visibility. Current and historical bit and packet rates for all protocols are available directly on the DPX system in graphical and tabular form. Detailed application statistics can be generated and exported to external database or analysis systems.

The application metadata generated by the DPI engine is also used to create rich IP detail records (IPDR) that include all infor-

mation available about a recorded network session. The IPDRs can be forwarded to an external system using the syslog protocol.

Scalability and High Availability

The DPX server platform can be configured so that most components (e.g. power supply, disk drives) are redundant and hot-pluggable. Several such systems can be deployed to monitor the same link using one-to-many taps. The measurement card's integrated filter engine can be used to implement various load balancing schemes, for instance based on IP addresses. A DPX LI installation scales up to multiple 10 Gigabit links. With one-to-many taps it is also possible to deploy a second hot-standby system that permanently monitors the primary systems and takes over its operation in case of a failure.

Features

- Full gigabit wire speed, scalability to 10 Gbit/s and beyond
- Proven ipoque DPI engine using layer-7 pattern matching and behavioral analysis
- Classification rate >90%
- Detection of obfuscated and encrypted protocols such as Skype, BitTorrent, VPN, and SSL
- Regular detection signature updates
- Protocol-specific IPDR/CDR generation
- Session interception based on:
 - Layer-7 protocol
 - Protocol-specific keywords, e.g. e-mail addresses, IM user names, SIP phone numbers
 - Arbitrary payload keywords
 - IP addresses, port numbers and ranges
 - Radius attributes such as subscriber names
- Packet or payload interception
- Comprehensive VoIP support
 - H.323, SIP, IAX, Skype
 - Signaling and call correlation
- Support of protocol-specific encodings
 - Gzip in HTTP transfers
 - MIME Base64 encoding in e-mail attachments
- Integrated stream buffer for complete session interception
- Up to 500,000 packets per second
- Over 5 million concurrent sessions
- Up to 400,000 new sessions per second
- 50,000 concurrent target rules
- 10,000 concurrent keywords
- Current and historical throughput statistics per protocol
- Generation and export of protocol-aware statistics