



Unispeed Blue Shield Interceptor probe system

- world leading data retention and lawful interception solution

Integrated string / pattern matching and LI system

Unispeed Blue Shield interceptor is a high capacity data intelligence probe system for duplex 10 GBit network interception.

It combines a string/pattern matching capability with regulatory Data Retention (CDR and LI) and traffic analysis

The system is installed on a standard rack-mounted server and equipped with intelligent Dual port 10 GBASE Capture - Network adapters with channel merging for duplex operation.

The probe features zero-copy architecture and session based load distribution for multi-core parallel processing.

Scalability is achieved by a combination of state full offload, optical splitters and clustering of probes

¹CDR=Call Data Retention

²LI=Lawful interception



String / pattern matching module

The string/ pattern matching module compares all captured frames against a string / signature filter file.

The string / pattern match file can consist of more than 100.000 strings (e-mail addresses, login and passwords, regular numbers, words, sentences, virus and trojan signatures etc.) The file can be edited directly through the Frontend editor or by any available editor.

An advanced method – the session handler - ensures that the full context of a matching packet can be monitored and analysed.

All captured frames are assigned a hash value and buffered in the memory (back-log). When a packet is matched against the filter, all packets in the back-log, having the same hash value, are sent to the output stream. Furthermore, for a predefined (configurable) time frame - packets with the same hash value are forwarded to the output as well. Thereby it is possible to monitor the full context (the session from start to end) of a matching packet.

The session handler will forward desired packet-streams to storage or the forwarding interfaces as original Ethernet traffic or as CALEA compliant UDP/RTP encapsulated stream in connection with LEA hand off. Each session is indexed by the pattern it was matched against.

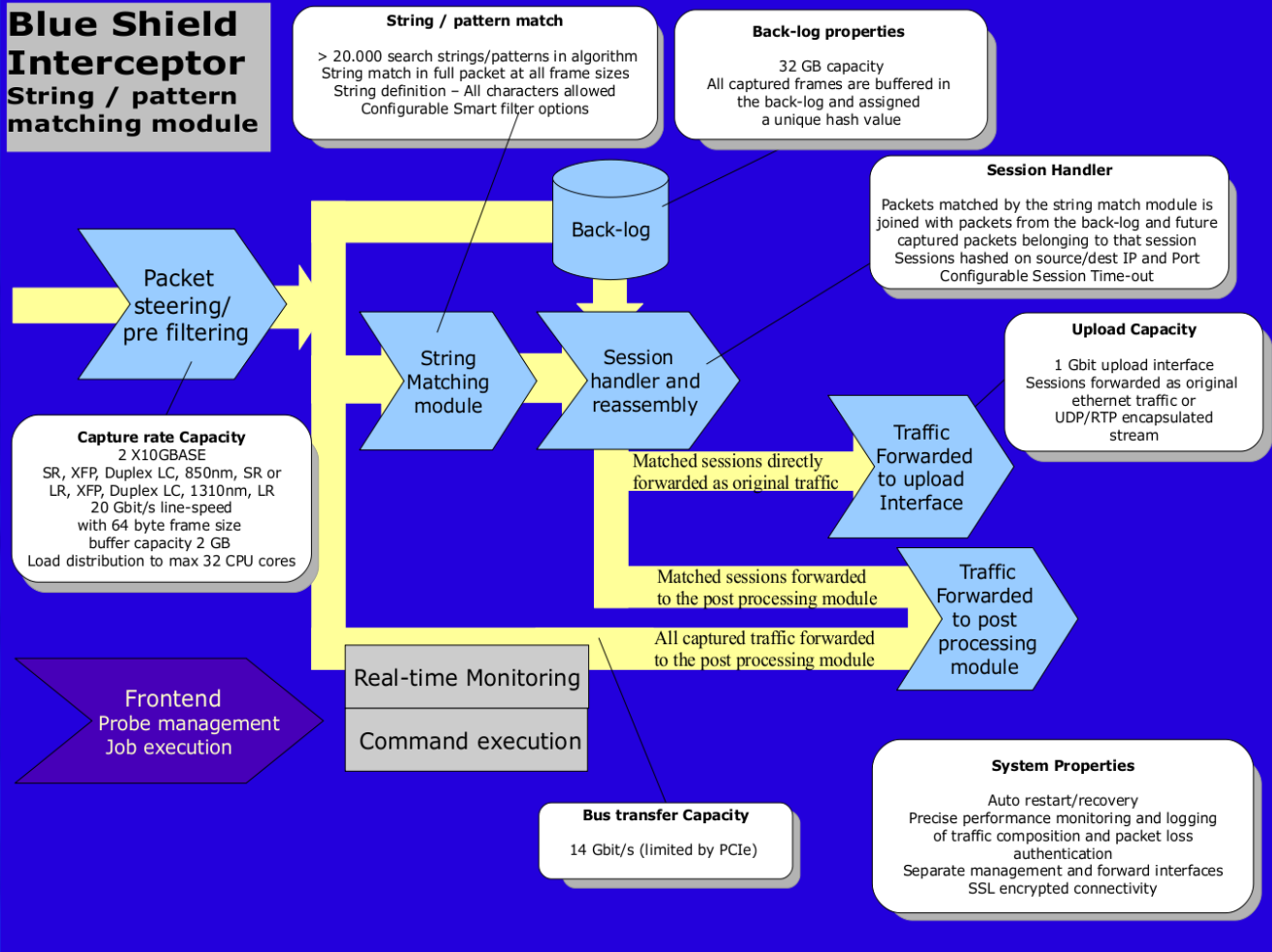
At the same time all captured traffic including the sessions matched by the string filter is made available for the post processing module for further analysis and filtering.

Packet signature filter

The architecture allows for identification of suspect traffic by matching signatures in a packet against a configurable search tree, effectively disclosing undesired traffic rare protocols or Virus and Trojans based on signatures found in the packets.

In in-line configuration the interceptor will discard infected and suspect sessions and only forward the non contaminated sessions to the transmit interfaces.

The discarded sessions are made available for the post processing module for further analysis and threat mitigation.



 unispeed

Post processing module

The architecture of the Post processing module is in many ways similar to the Unispeed blue Shield data retention probes.

However it receives two streams of data - namely the complete traffic stream captured by the network adapters and a stream containing sessions matched by the string match module.

The module also has the ability to read files and data directly from storage e.g. PCAP, TCP, text, binary and database lookups - for data-mining purpose or in order to merge data into the real-time stream e.g. Geo-Location, ODBC, static or DNS lookups.



Packet filtering

Real time Packet filtering is performed on any combination of packet headers. When ever a target is identified the preceding packets are polled from the back-log system

Again the traffic stream is divided in separated streams that can be individually analyzed or forwarded to the up-link interface or storage.

Available regulatory data collection includes.

ETSI standard - call data retention (src/dst IP and Port, transport protocol and start/end timestamps)

and Lawful interception targeted at IP-address, E-mail addresses, port and Mac-number, or any other header or content string.

Protocol extract / reassembly

Real time protocol extractors are available for a number of protocols and more is custom developed to meet customer requirement.

The protocol extractors provide high performance real-time data mining to assist criminal investigators in identifying relevant data as it passes by.

Both header information and content is made available for the record analysis modules, and captured events can be set to trigger the backbone BSM system which will generate alert messages to investigators.

Data analysis module

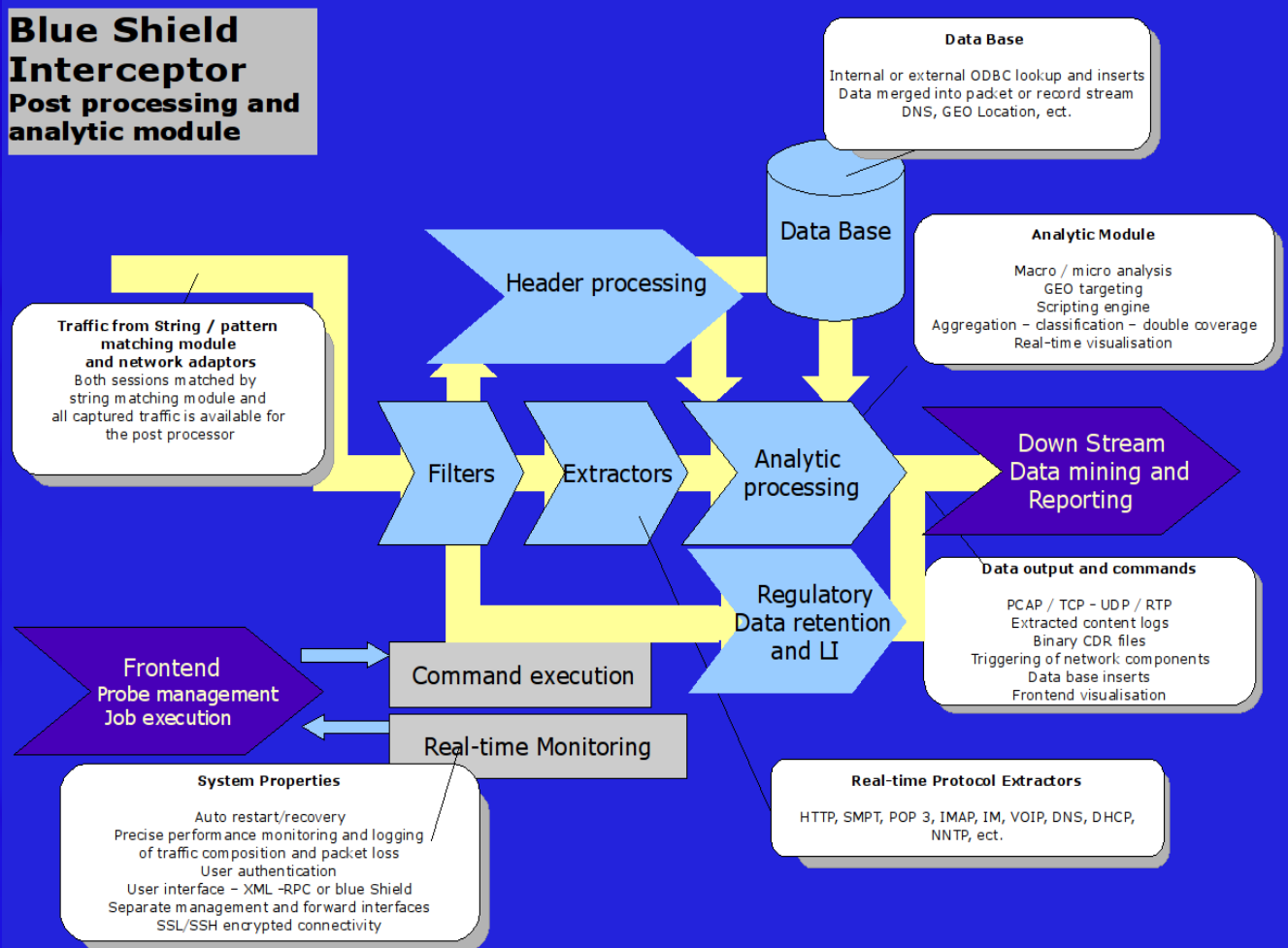
The data analysis functions of the system includes a number of aggregation, classification and double coverage components for macro analysis.

Behavioral analysis of traffic can lead to early detection of criminal activity and even DDOS attacks and mapping the impact of virus and Trojans

The output data can be inserted into internal or external databases or compared against historic data for trend and behavioral analysis.

Real-time viewers are provided for quick assessment and response to changes in the data composition.

An embedded scripting engine provides for instant alerting and generic response/triggering to events that requires immediate attention or automatic reconfiguration of the interceptor system or other network components.



 unispeed

Engvej 139 • 2300 Copenhagen S • CVR 25457412

Tlf. +45 3344 5500 • Fax +45 3344 5501 • sales@unispeed.dk