CUBRO
NETWORK VISIBILITY
SIMPLE | SCALABLE | SUSTAINABLE

DATA SHEET

# Cubro FlowVista Series

## PRODUCT REVIEW



The Cubro FlowVista provides flexible signature syntax and identification while focusing on high performance and real time DPI processing.

The engine to support ACL and load balancing rules are based on IP 5-tuple application protocols. In addition, FlowVista can identify and tag the raw data and output the flow log based on IP 5-tuple in NetFlow V9 standard.

### Functions / Benefits:

- Built-in logical signature processing engine, supporting rule priority and output identification results of the highest priority.
- Flexible rule syntax description: users can define the protocol rules based on PDL* syntax
- Supporting cross-packet search
- Supporting rule hot swapping, achieving rule upgrading without interrupting traffic processing.
- Correlate-identification: correlating multi-session protocol and unifying the identification result.
- Packet filtering load balancing: FlowVista can process the packets based on IP 5-tuple and application protocol rules and support combined ACL rules and multi-dimensional load balancing (preserving session/subscriber integrity).

* (The PDL syntax is the language of the Cubro Regex Compiler to generate new Fingerprints)

## Network Probe
### At a glance

### Definition

A probe is a passive device which receives network traffic from TAPs and Packet Brokers and extracts metadata .

### Advantages of FlowVista

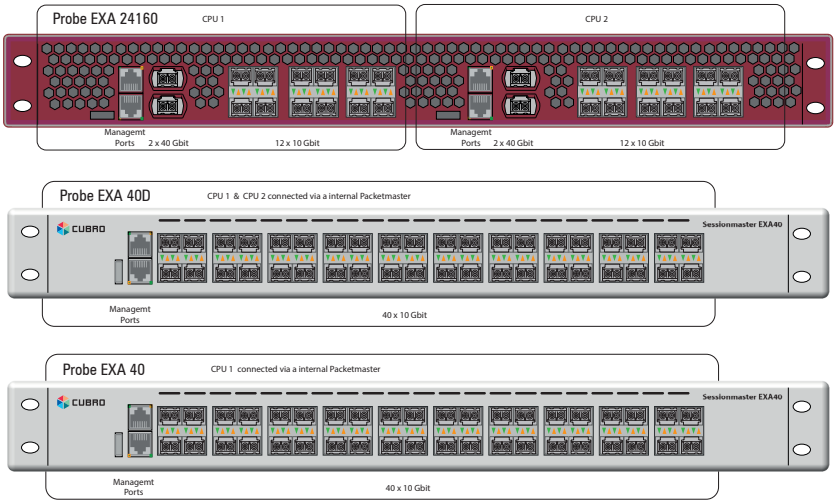
- Small foot print & low power design
- L7 application detection
- Embedded Network Processor design
- Can be customized to customer's requirement
- NetFlow V9
- Support of any kind of SFP and SFP+ (also 10 Gbit BASE_T), and QSFP
- 24 x 10 Gbit and 4 x 40 Gbit

# PRODUCT CAPABILITIES / FEATURES

| | |
|---|---|
| **Identification Feature** | Identification based on port, signature, and traffic type<br>Cross-packet matching<br>Correlate-identification (FTP/DNS/bbc-iPlayer/afreecavideo)<br>HTTP identification for non-standard ports |
| **Protocol Identification Rule** | Protocol identification engine: finding the app id of the highest priority<br>Rule compiler: generating graph with PDL*, 8K rules (maximum)<br>User-defined rules with PCRE |
| **Other DPI Features** | Hot-swappable rule upgrading<br>Tagging signature information on packet Ethernet header |
| **Packet Preprocessing** | Jumbo frame, IP - reassembly<br>TCP-reassembly such as out-of-order packets, TCP state tracking<br>Tunnel identification such as GTP/GRE, supporting protocol processing inside the tunnel |
| **Classification** | 6-tuple ACL rule (IP 5-tuple + app id, maximum: 4K)<br>Redefining app id with actions to classify applications<br>Load balancing (preserving session/subscriber integrity) |
| **Flow Detail Record** | Generating flow log in Netflow V9 standard |
| **Ports EXA24160** | 24 X 10 Gbps / 1 Gbps and<br>4 X QSFP 40 Gbps |
| **Configuration / Communication** | Serial/SSH/Telnet/FTP |
| **Performance EXA24160** | Throughput 160 Gbps<br>DPI Performance 60 Gbps<br>Session 20 million online (max) |
| **CPU** | Mips 64 96 Core |
| **MTBF** | 178,125 hours |

* (The PDL syntax is the language of the Cubro Regex Compiler to generate new Fingerprints)

# TECHNICAL DATA / SPECIFICATIONS




## Operating specifications:

Operating Temperature: 0°C to 45°C
Storage Temperature: -10°C to 70°C
Relative Humidity: 10% min, 95% max
Non-condensing

## Mechanical specifications:

Dimension (HxWxD): W=440.00 mm, L=660 mm, H=44,4 mm
Weight: 9.4 kg

## Electrical specifications:

Input Power: 100-240V, 2A, 47-63 Hz
Maximum Power Consumption: 400W

## Certifications:

Fully RoHS compliant
CE compliant
Safety - UL 60950-1 / CSA C22.2 60950-1-07 / IEC 60950-1 (2005)
EN 60950-1 (2006)

## INPUTS*

Several 1, 10 , 40 Gbit interfaces can be used as inputs from TAPs or NPB.

On EXA40 and EXA40D a NPB is build in the probe.

On EXA24160 an external NPB can be used for load balancing the traffic.

## OUTPUTS*

Any port can be used as metadata streaming output. The Netflow CDR can also send load balanced traffic over several ports to reduce the load on the servers.

## PERFORMANCE

Nearly more than 1000 pre-configured fingerprint applications id available.

Advanced multi-core CPU design

Lowest power usage per Gbit traffic processing in the industry.

### MANAGEMENT

Management Port: (1)
RJ45 10/100/1000 Mbit

Configuration (CLI) Port: (1) RS-232 DB9

USB 3.0 for software update

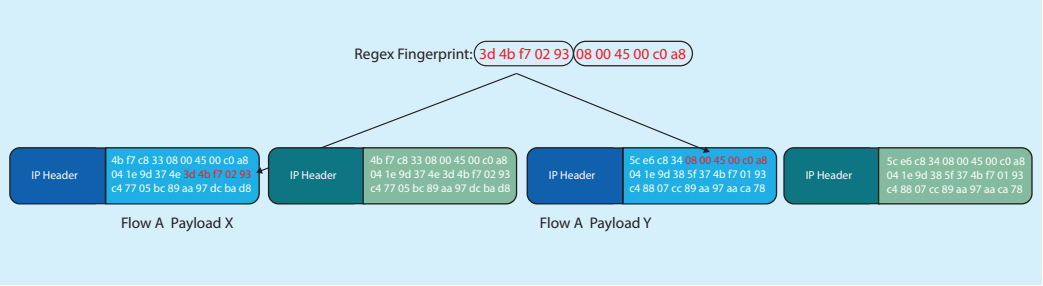
### INDICATORS

Per RJ45 port: Speed, Link/ Activity

Per SFP+ port: Status, Rx, Tx, Link

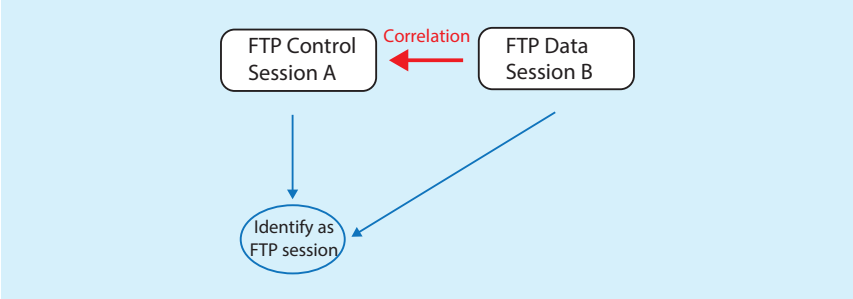
Per Device: Power, Status

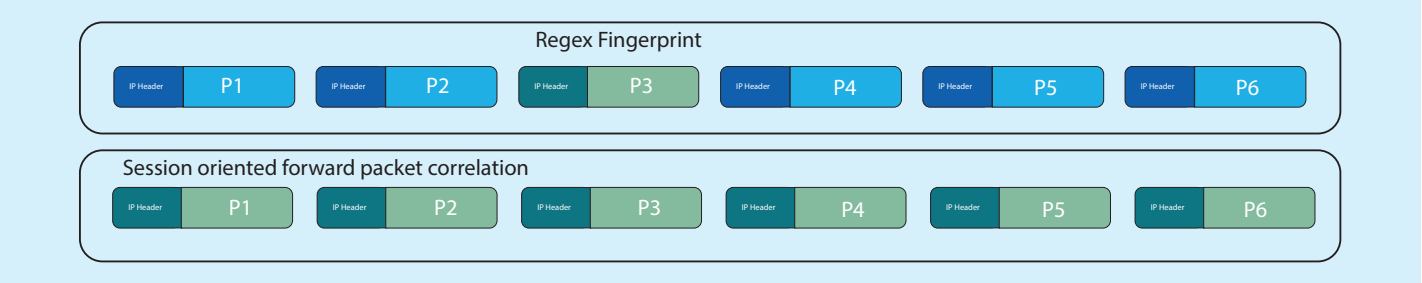
# ADVANCED FUNCTION DESCRIPTION




**Supporting cross-packet search:** For example, signature S is separated into S1 and S2. S1 and S2 are in two adjacent packets and FlowVista can still identify signature S.

**Correlate-identification:** Correlating multi-session protocol and unifying the identification result.

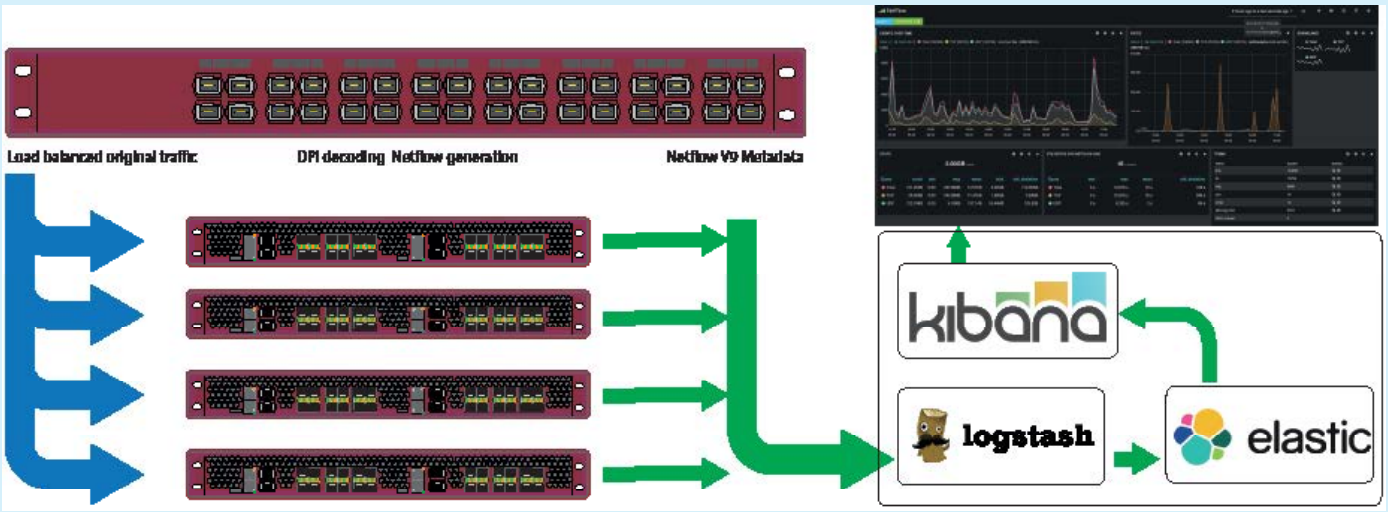



**Raw packet tagging:** Tagging the identification information in the "MAC" field of raw packet header. FlowVista supports tagging buffering feature. For example: packet A is in front of packet B in the same session and packet B carries the signature. When FlowVista identifies the signature carried by packet B, it can still tag packet A with the signature information.

**FDR:** FlowVista can make statistics of the session up link/down link traffic, session status, starting/ending time, and protocol identification information. FlowVista outputs the statistics information in NetFlow V9 standard.

# TYPICAL APPLICATION: BIG DATA OPEN SOURCE



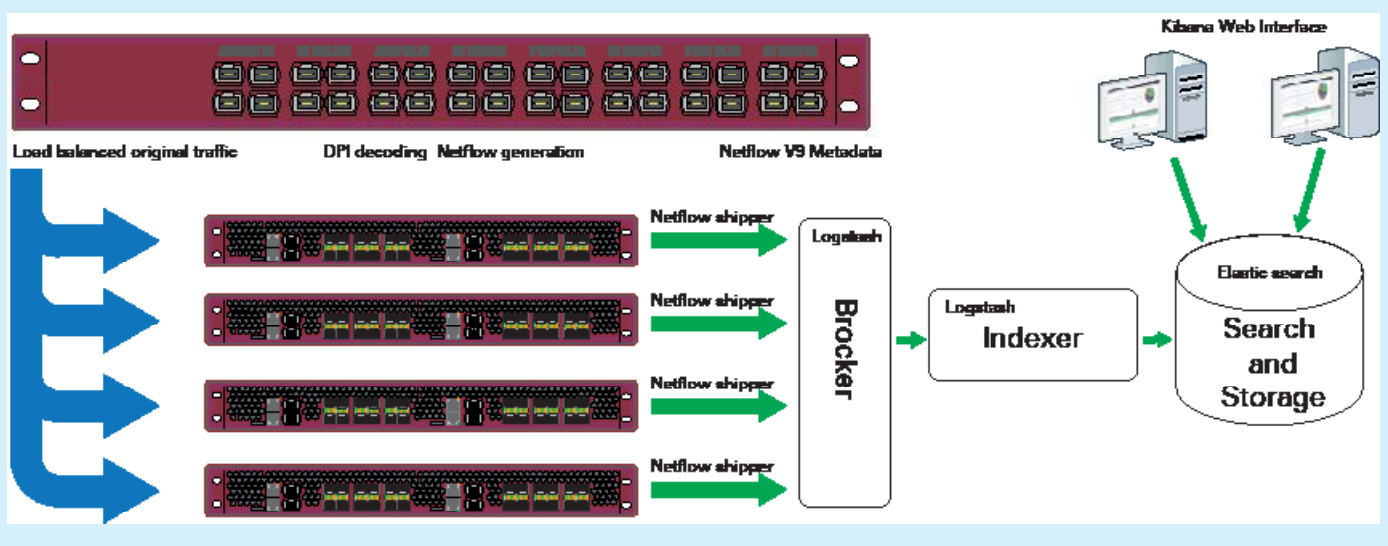

The Cubro FlowVista probe can be also used to generate metadata from the network and feed a big data application. As one example of such an installationthe picture shows 3 open source applications (ELK ore kibana stack) which can be used to build a powerful and flexible collector.

**Logstash** offers centralized log aggregation of many types, such as server logs, and also Netflow. It is a very simple message based architecture. Logstash has a single agent that is configured to perform different functions in combination with the other ELK components.

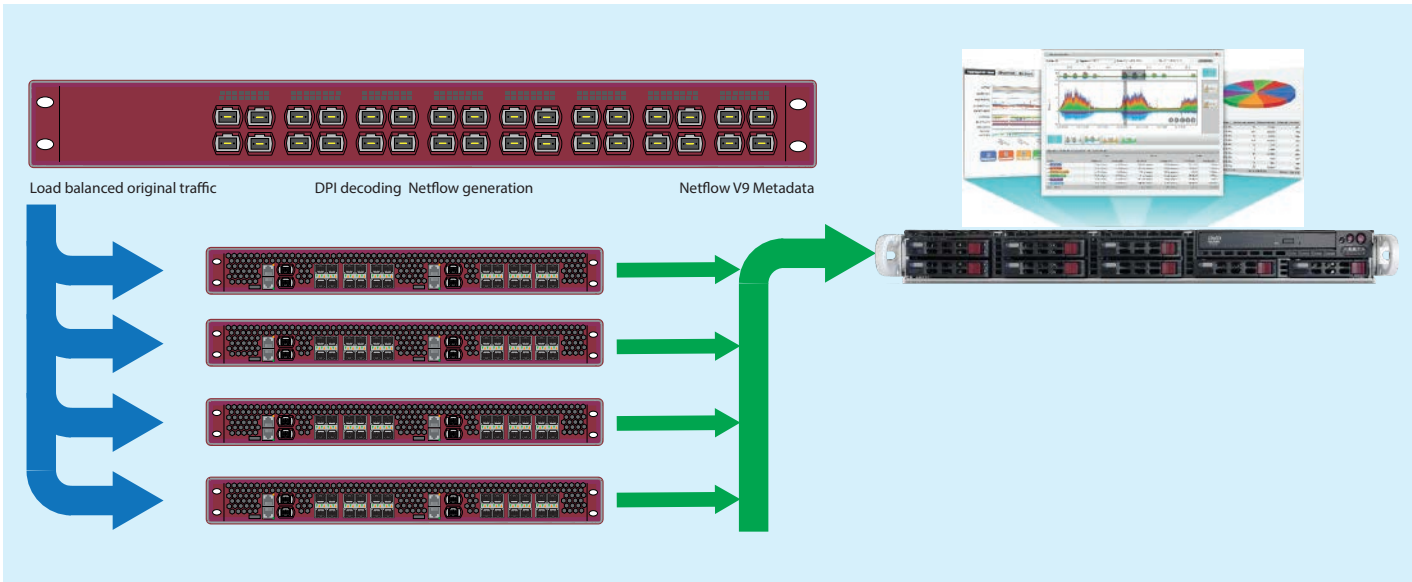
**Elasticsearch** is a distributed search and analytics engine. It is a schema-free, full text search engine with multi language support. It provides support for geo location, suggestive search, auto complementation and search snippets.

**Kibana** is analytics and visualization platform architectured for Elasticsearch. It provides real-time summary and charting of streaming data with the ability to share and embed dashboards.

Two more components should be mentioned **Marvel** to monitor the full system itself and **Shield** which takes care of security features to ELK such as role-based access control and much more.



# TYPICAL APPLICATION STANDARD COLLECTOR




This drawing shows a typical solution to monitor a huge amount of traffic, in this case more than 250 Gpbs. The traffic is received via TAPs to the EX32100 from various interfaces. The EX32100 is aggregating, filtering and load balancing the traffic to 4 FlowVista Probes, each handling 60 - 70 Gbps traffic.

The probes are sending the Flow CDR to a flow collector. The collector is a 3rd party product. The Netflow V9 is a generic format, which can be handled by many 3rd parties and open source products.

# ORDERING INFORMATION

**Product Components:**

- Cubro FlowVista Probe
- AC/DC power supply
- European power cord
- (no SFPs included)

| Part Number | Description |
|---|---|
| CUB.FVP-S | FlowVista Probe, single CPU, AC power |
| CUB.FVP-D | FlowVista Probe, dual CPU, AC power |
| CUB.FVP-Q | FlowVista Probe, quad CPU, AC power |
| CUB.FVP-S-DC | FlowVista Probe, single CPU, DC power |
| CUB.FVP-D-DC | FlowVista Probe, dual CPU, DC power |
| CUB.FVP-Q-DC | FlowVista Probe, quad CPU, DC power |

For more information please check our website **www.cubro.com**