Cubro DPI Metadata Application

APPLICATION NOTE

CUBRO
NETWORK VISIBILITY
SIMPLE | SCALABLE | SUSTAINABLE

Introduction: DPI in Telecommunication

Deep Packet Inspection (DPI) is a technology that enables the network owner to analyze internet traffic, through the network, in real-time and to differentiate them according to their payload.

DPI is often used for understanding the performance or behavior of subscribers, which applications they use, how often etc. This helps operators to focus on improving service for the important applications. For instance, video streaming services like Netflix, YouTube, etc consume a lot of bandwidth. DPI can be used to limit this.

Why DPI

How is Omnia Metadata output used?

Deep Packet Inspection (DPI) is used extensively by both enterprises and internet service providers for the following applications.

- Policy Definition and Enforcement
- Buffer Overflow Attack Detection
- Data Leak Prevention (DLP)
- Policy Definition and Enforcement
- Targeted Advertising
- Quality of Service (QoS)
- Tiered Services Offer
- Copyright Enforcement
- Net Neutrality Prevention
- Lawful Interception
- OTT application monitoring

Why is this needed?

- Find, Identify, Classify, Reroute, and Block Packets with particular data/code payloads.
- Allocate available resources to smoothen traffic flow
- Ameliorate network performance and throughput
- Impose online privacy through sender-receiver identification
- Enable advanced network management, user service, internet data mining, internet censorship, and eavesdropping
- Ensure throttled data transfer preventing P2P (Peer-to-Peer) misuse

Overview of DPI Applications

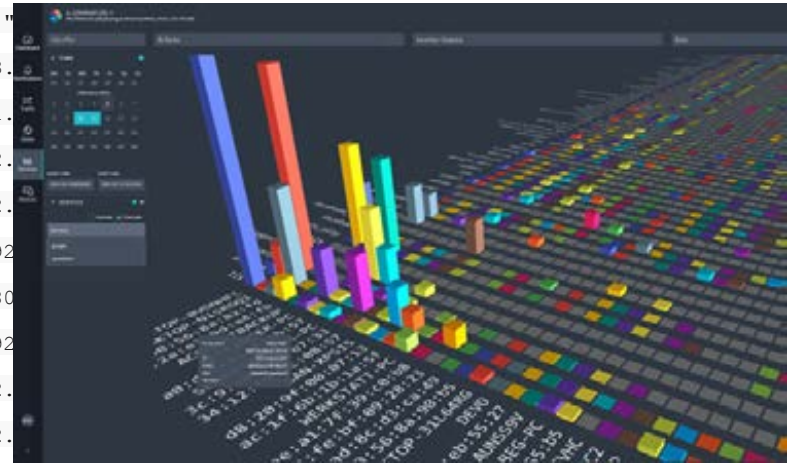
DPI facilitates analyzing and managing IP traffic and securing IP networks in real time by providing network visibility and real-time application awareness. Besides influencing bandwidth and traffic management decisions, DPI can provide insights into:

- Network Security
- Network Management
- Network and Subscriber Analysis
- Content Regulation
- Targeted Advertisement
- Application Distribution and Load Balancing

Cubro DPI

Deep Packet Inspection (DPI) is detecting traffic type by Signature; beyond port and protocol


```
{ "hash":"7461864e", "service": "whatsapp", "ip_1":"213.143.110.250", "ip_2":"
{ "hash":"7461864e", "service": "whatsapp", "ip_1":"31.13.84.49", "ip_2":"213.
{ "hash":"ce931c02", "service": "whatsapp", "ip_1":"192.168.3.83", "ip_2":"31.
{ "hash":"ce931c02", "service": "whatsapp", "ip_1":"31.13.84.51", "ip_2":"192.
{ "hash":"70d46209", "service": "whatsapp", "ip_1":"31.13.84.49", "ip_2":"192.
{ "hash":"b6cd9e62", "service": "whatsapp", "ip_1":"80.110.82.15", "ip_2":"192
{ "hash":"6fc2f8ce", "service": "whatsapp", "ip_1":"192.168.3.130", "ip_2":"80
{ "hash":"55e8f416", "service": "whatsapp", "ip_1":"192.168.3.44", "ip_2":"192
{ "hash":"113d5e32", "service": "whatsapp", "ip_1":"31.13.84.49", "ip_2":"192.
{ "hash":"a597661a", "service": "whatsapp", "ip_1":"31.13.84.49", "ip_2":"192.
```

This is the output from our DPI engine so we can find WhatsApp even when it is ciphered!
We can find up to 4000 different applications.

CUBRO NETWORK VISIBILITY
SIMPLE | SCALABLE | SUSTAINABLE

DPI applications

There are generally two different main applications for DPI

1. Analytics

A: In this application the DPI engine can decode the full traffic and produce results in DB format for analytics purpose. This is only possible on CPU based units like (Omnia10 / Omnia20 / Omnia120 / EXA24400 and so on). Since every packet has to be handled, it is a big effort in terms of CPU load and data output.

B: IPFIX with DPI enriched output. This is also a very common way of analyzing DPI data, but it is not very efficient and produce a lot of overhead. IPFIX on ISP level is very difficult because of the millions of sessions. This leads often in big issues with memory limits in the probe.

2. Tagging/filtering/blocking

This application resonates with Cubro approach - remove an unwanted application type from the monitoring. It is common to remove video streaming services.

The same application is for blocking certain applications, or sending certain traffic to a special monitoring device. In this case it is not needed to do a full decode because sampling gives a similar result but with much less effort.

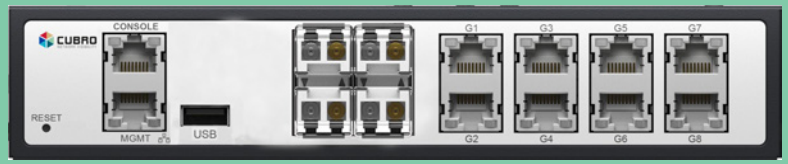
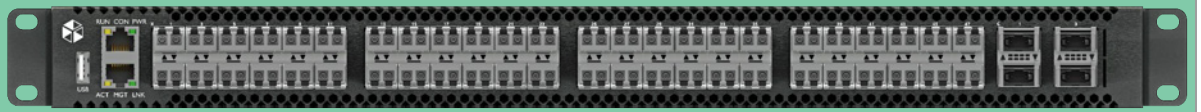
DPI Signatures (Applications & Protocols)

We support up to 4000 signatures. These signatures are divided into two parts:

- 1400 see DPI Services - these are the top signatures which are maintained manually.
- The other signatures are maintained by deep learning and AI.

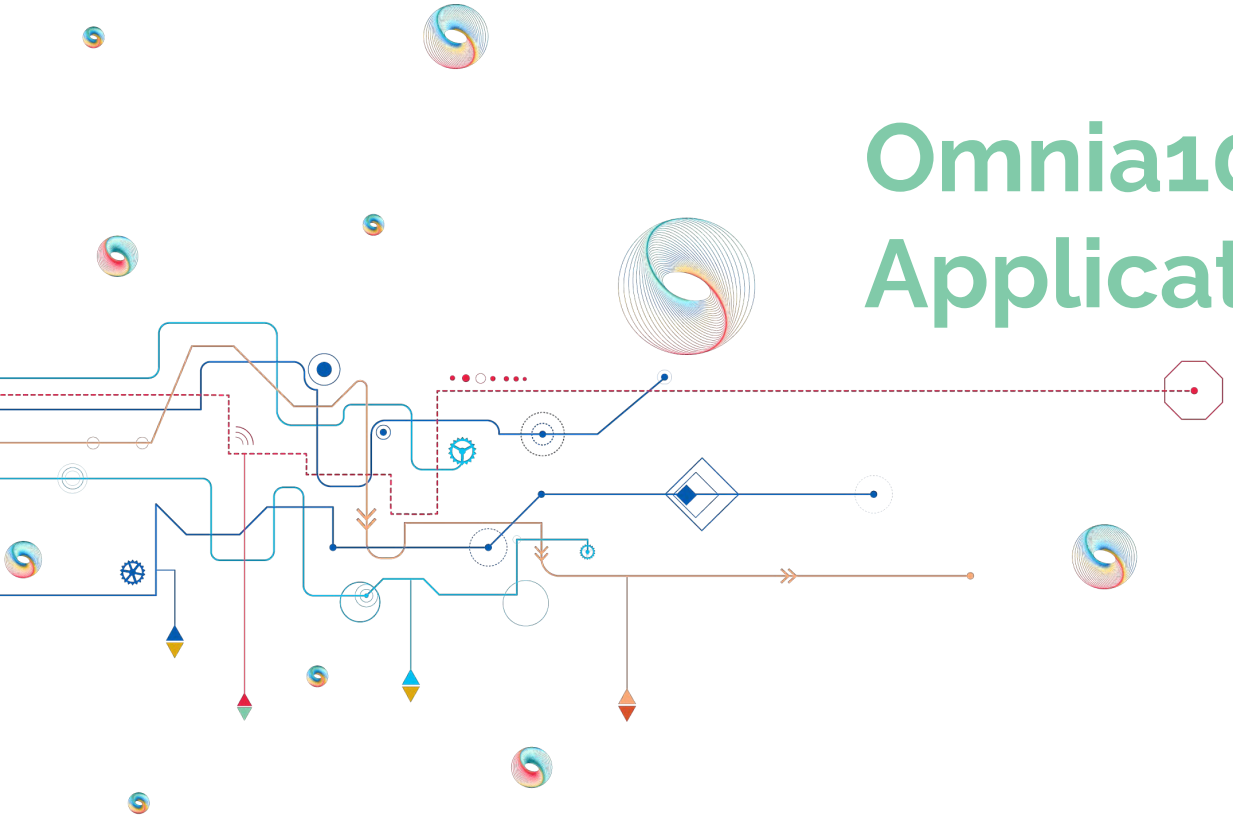
(The update cycle is between 7 and 10 Days)

CPU and Switch Omnia models overview

Omnia10	
Omnia20	
Omnia120	

CPU only Omnia models overview

Omnia200	
Omnia400	
Omnic	

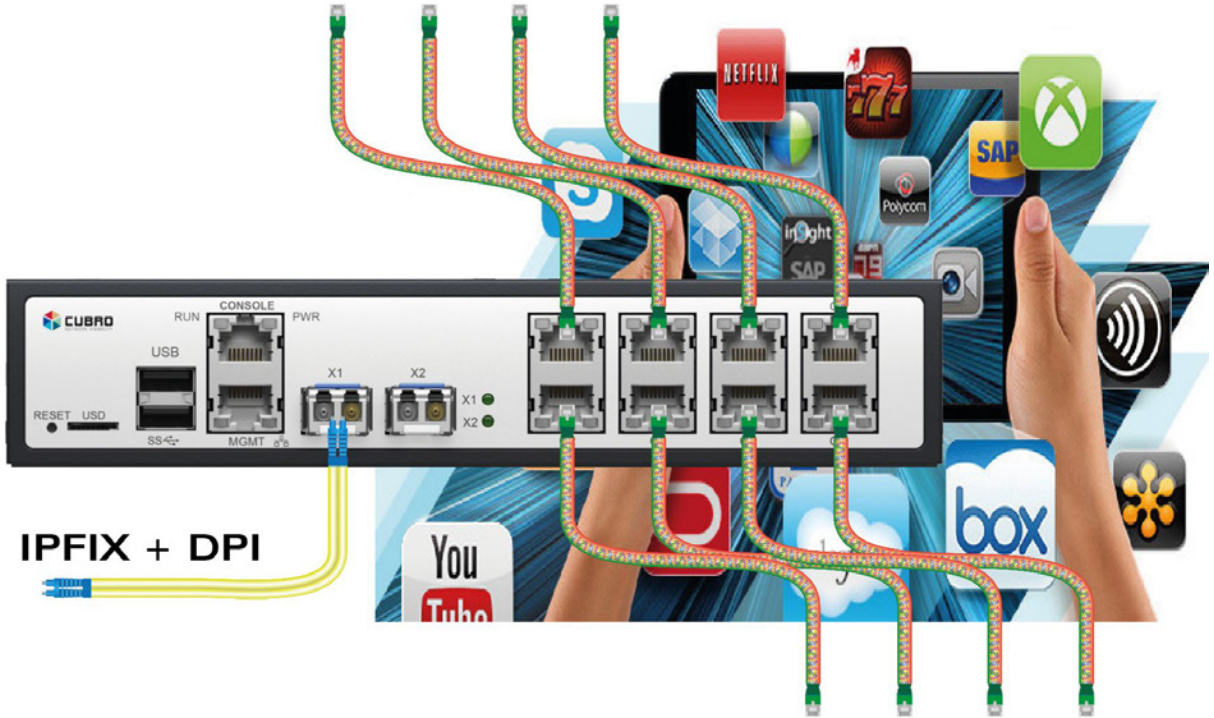


Omnia10/20 Applications

CUBRO
NETWORK VISIBILITY
SIMPLE | SCALABLE | SUSTAINABLE

OMNIA10 as IPFIX -DPI exporter

IPFIX - DPI enriched exporter



CUBRO NETWORK VISIBILITY
SIMPLE | SCALABLE | SUSTAINABLE

OMNIA10 as IPFIX -DPI exporter + Collector

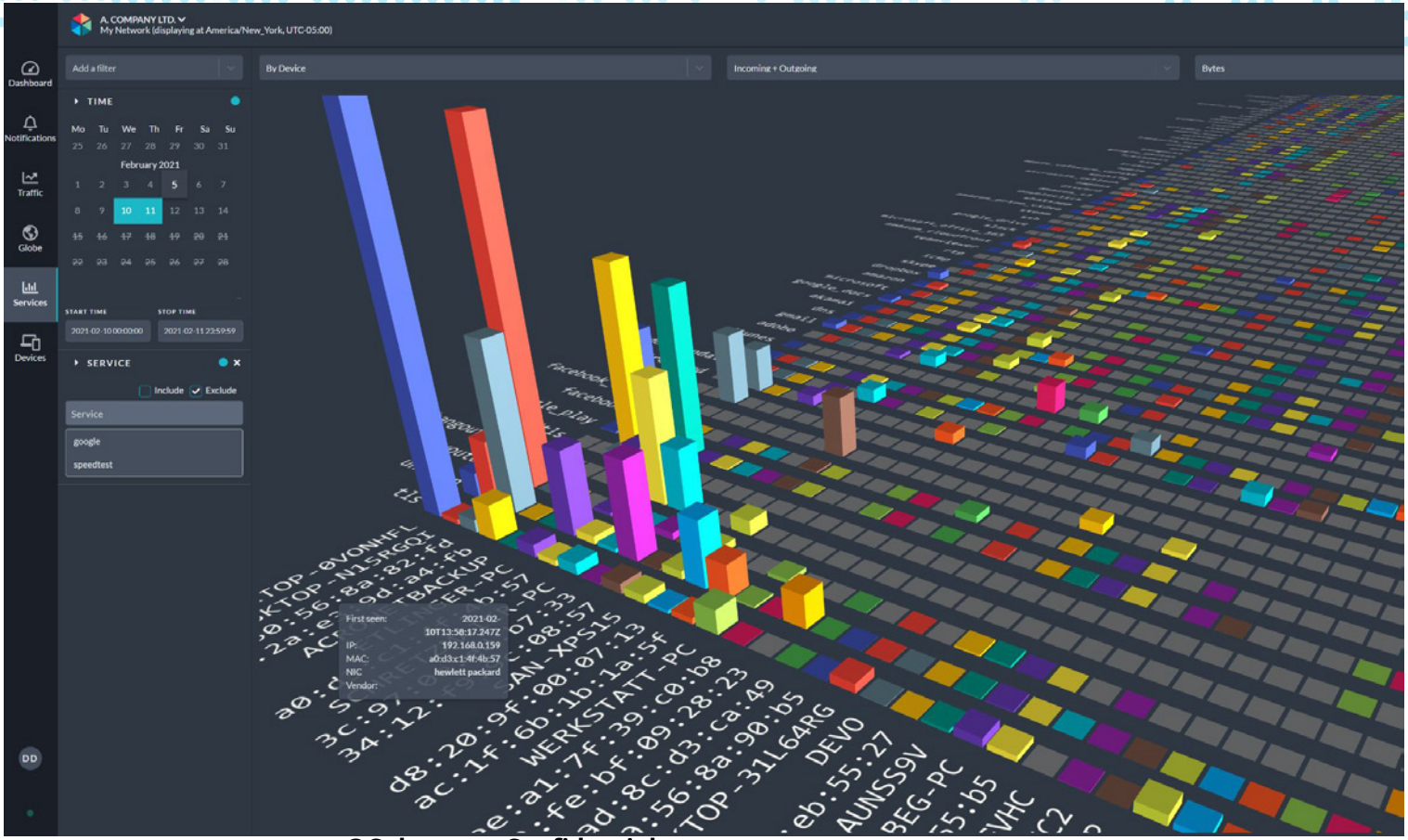
Probe and Collector on 19” tray

The collector is Intel(Xeon) Platform, where you can run any collector software commercial and open source.

OMNIA 10 does the tapping / aggregation/ filtering / IPFIX / DPI and forward the metadata to the collector software.

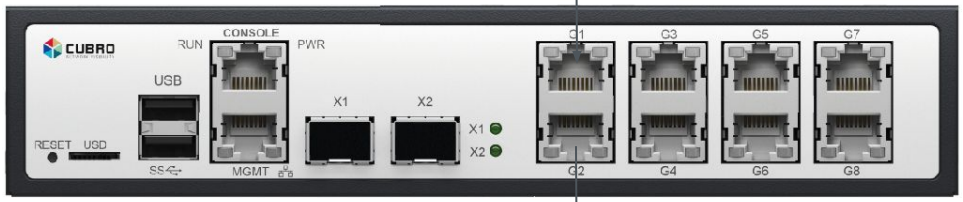
CUBRO NETWORK VISIBILITY
SIMPLE | SCALABLE | SUSTAINABLE

DPI Analysis implemented on Omnia10



Filtering application

full traffic in



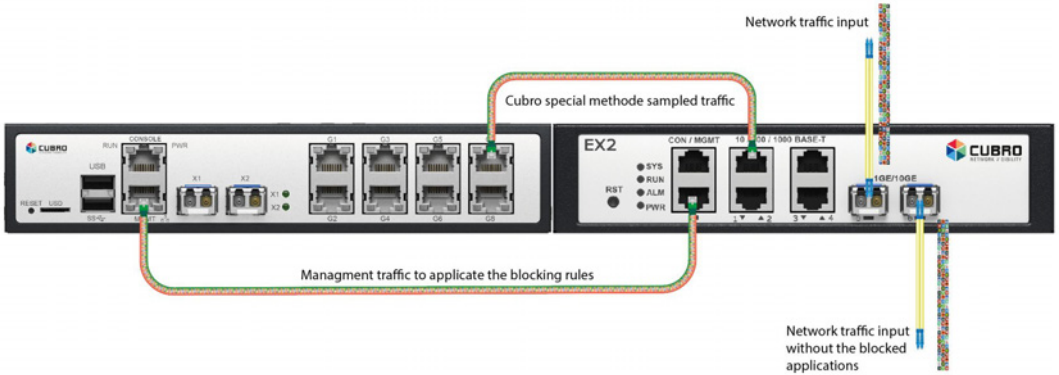
Traffic out without video stream traffic to reduce load on monitoring or capture device

Services		
_1kxun	video	1kxun is a chinese video sharing website.
abc	video	The American Broadcasting Company (ABC) is an American commercial broadcast television network that is owned by the Disney–ABC Television Group, a subsidiary of the Disney Media Networks division of T...
acestream	video	Ace Stream is a peer-to-peer multimedia streaming protocol, built using BitTorrent technology.
amazon_prime_v	video	Amazon Video is an Internet video on demand service that is developed, owned and operated by Amazon.com.
apple_tv	video	Apple TV is a digital media player and microconsole developed and sold by Apple Inc. It is a small network appliance and entertainment device that can receive digital data from a number of sources and...
bbc_iplayer	video	BBC iPlayer is an internet streaming, catchup, television and radio service from the BBC. The service is available on a wide range of devices, including mobile phones and tablets, personal computers, ...
bilibili	video	Bilibili is a video sharing website themed around anime, manga, and game fandom based in China, where users can submit, view, and add commentary subtitles on videos. It is a domain having .tv extensio...
cheddar	video	Cheddar Inc. is a live streaming financial news network founded by Jon Steinberg in the United States. Cheddar broadcasts live daily from the floor of the New York Stock Exchange (NYSE), NASDAQ, the F...
crackle	video	Watch free movies and TV on your iPhone, iPod Touch and iPad. Break away with Crackle. Crackle is the destination to watch free TV, movies and exclusive originals. All free, anytime, anywhere and ...
cravetv	video	Stream the best of TV all in one place. The Showtime Collection features breakthrough series such as Billions, The Affair, Ray Donovan or Homeland. The HBO Collection includes Entourage, Sex and t...
creative_cloud	video	Adobe Creative Cloud is a software as a service offering from Adobe Systems that gives users access to a collection of software developed by Adobe for graphic design, video editing, web development, p...
crunchyroll	video	Crunchyroll is an American distributor, publisher and international online community focused on video streaming East Asian media including anime, manga, drama, music, electronic entertainment, and aut...
curiositystream	video	CuriosityStream is the world's first on-demand streaming service for award-winning documentaries that enlighten, entertain and inspire.
dailymotion	video	Dailymotion is a video-sharing technology platform.
dazn	video	DAZN is a subscription video streaming service owned by Perform Group. The service is dedicated to sports, offering live and on-demand streaming of events from various properties.
directv_now	video	DirecTV Now (or simply DTV Now) is a subscription streaming television service by AT&T, which allows subscribers in the United States to stream programming from cable channels without the long term co...
fc2	video	FC2 Video App lets you search for a video or user, and easily watch the video of interest. Use it while waiting for someone or something. Use it in many situations! Feature description ...
flash_show	video	Miaopai is a Chinese video sharing and live streaming service with 70 million daily active users.
flickr	video	Flickr (pronounced "flicker") is an image hosting and video hosting website and web services suite that was created by Ludicorp in 2004 and acquired by Yahoo on March 20, 2005.
flipagram	video	Impress friends with amazing videos and photo video slideshows plus free popular music! Get featured & become famous with fun challenges for every talent - like dance, beauty, art, comedy, music, anim...
funshion	video	Funshion is a Chinese peer-to-peer streaming video network software and website.
		go90 is an American video streaming service, launched in October 2015

and some more

CUBRO NETWORK VISIBILITY
SIMPLE | SCALABLE | SUSTAINABLE

Application: Blocking on 10 Gbit traffic Omnia10 & EX2



The Omnia10 in combination with the EX2 can also be used to block applications like WhatsApp, Skype, Youtube, etc.

We currently support up to 4000 signatures and applications.

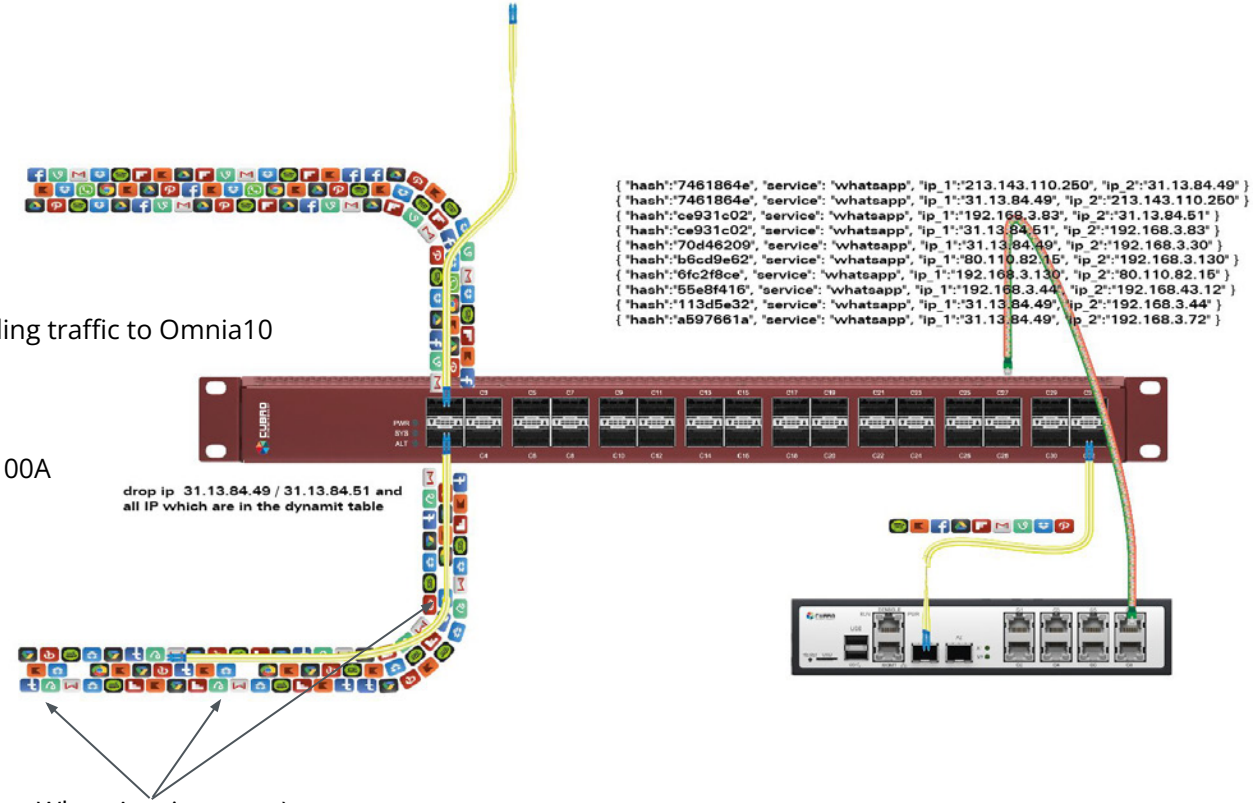
The traffic passes EX2 which performs a special sampling method to feed the Omnia10 with traffic.

The DPI engine on Omnia10 decodes the traffic and configures the drop rules on EX2.

CUBRO NETWORK VISIBILITY
SIMPLE | SCALABLE | SUSTAINABLE

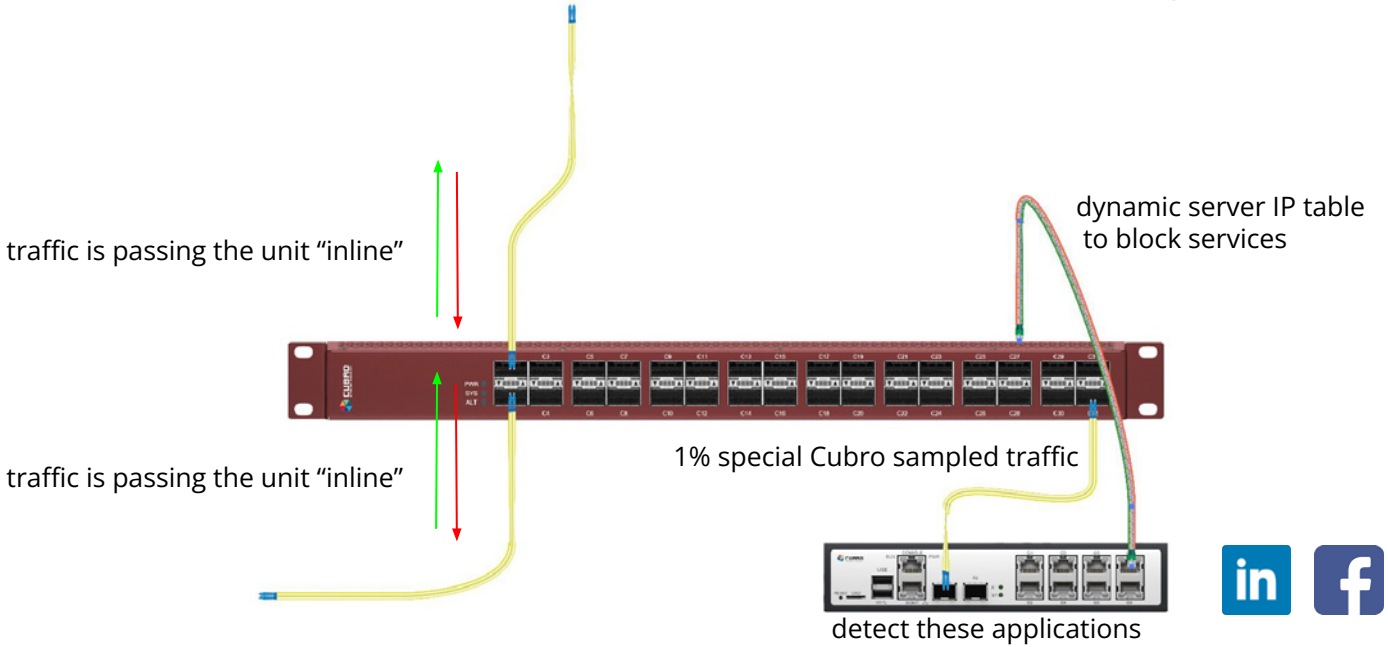
Blocking applications with G5 (EXA32100A/EXA64100)

1) Input traffic
2) Special Cubro sampling traffic to Omnia10
3) Generate filter table
4) Add filter on EXA32100A



CUBRO NETWORK VISIBILITY
SIMPLE | SCALABLE | SUSTAINABLE

Blocking applications with G5 (EXA32100A/EXA64100)

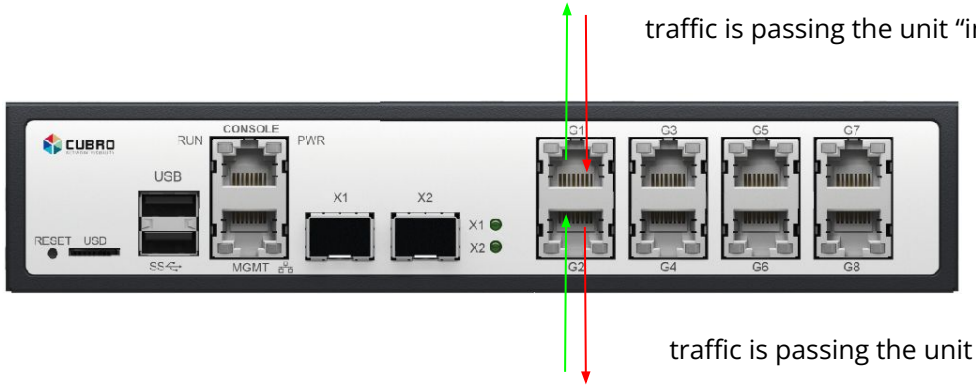


The detector can be any CPU based unit, also a server.

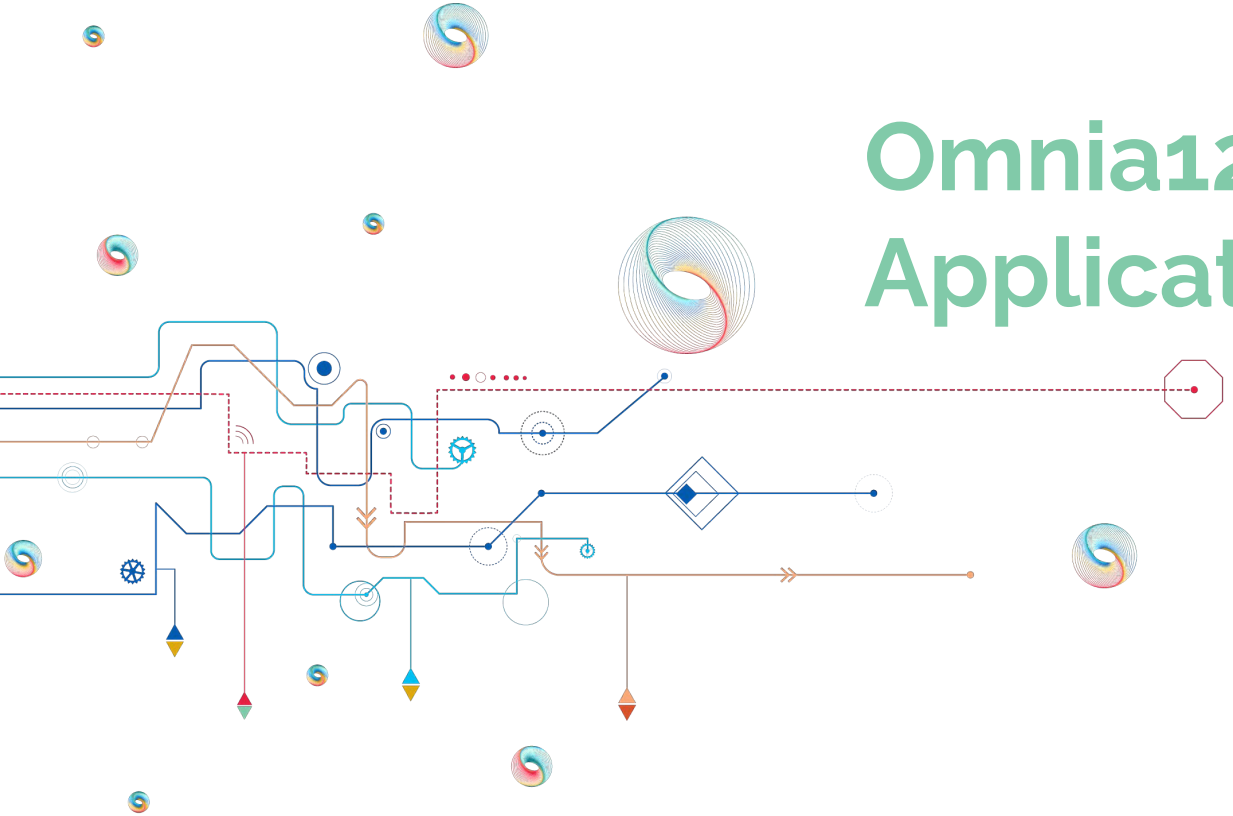
It is also possible to do this on the G5 units host controller (under investigation)

CUBRO NETWORK VISIBILITY
SIMPLE | SCALABLE | SUSTAINABLE

Blocking applications



Omnia120 Applications



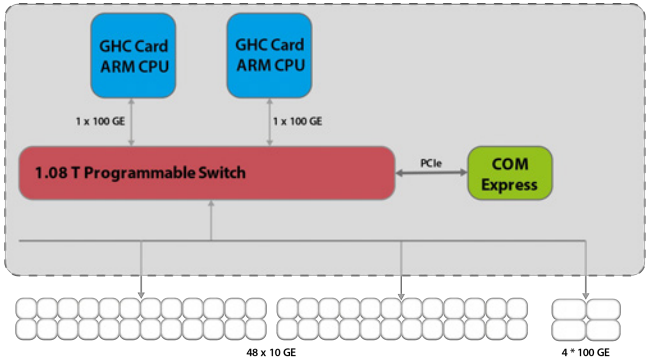
CUBRO
NETWORK VISIBILITY
SIMPLE | SCALABLE | SUSTAINABLE

Omnia120

The Omnia120 is a much more than an NPB, it is a visibility node which combines a programmable packet pusher for up to L7 hardware based packet handling features, like filtering and load balancing (more details in the Omnia presentation). It has two multicore ARM CPUs connected to the switch over a 100 Gbit full duplex link.

On one of the CPUs we perform features which cannot be done in hardware, like advance REGEX filtering, special type of load balancing, tunnel handling and much more.

The second CPU is reserved for analytics purpose like IPFIX and DPI export.



Cubro Omnia120 workflow

Packetmaster Hardware Features

a) ACL filtering inline
b) Load balancing
c) GRE encapsulation
d) ERSPAN encapsulation
e) VLAN and VXLAN encapsulation
f) Timestamping
g) Packet slicing
h) Tunnel header removal
i) MAC modification
j) Offset stripping
k) GRE and VXLAN endpoint

Sessionmaster Software Features

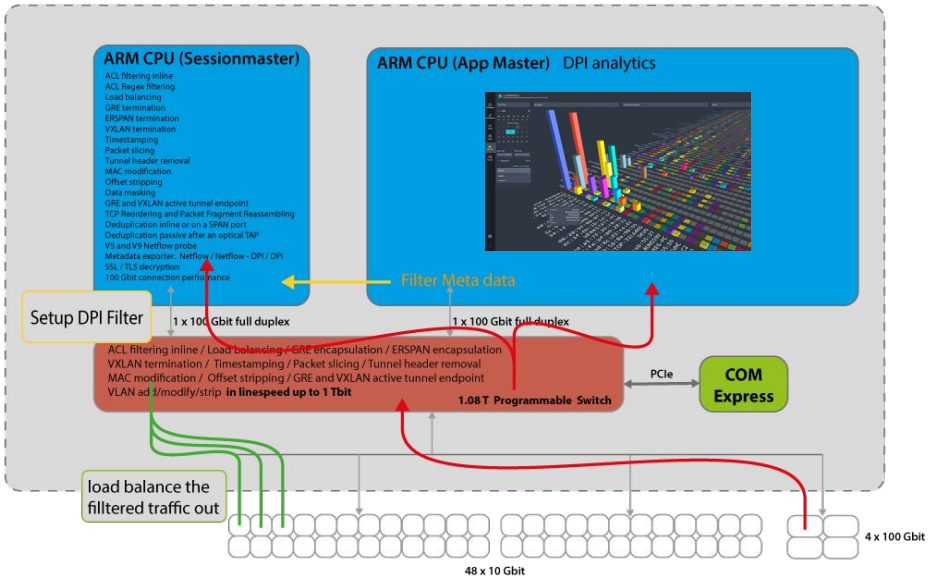
a) ACL filtering inline
b) Load balancing
c) GRE encapsulation
d) ERSPAN encapsulation
e) VLAN and VXLAN encapsulation
f) Timestamping
g) Packet slicing
h) Tunnel header removal
i) MAC modification
j) Offset stripping
k) Data masking
l) GRE and VXLAN endpoint
m) TCP Reordering and Packet Fragment Reassembling
n) Deduplication inline or on a SPAN port
o) Deduplication passive after an optical TAP
p) V5 and V9 Netflow probe
q) Metadata exporter:
Netflow / Netflow - DPI / DPI

Software “3rd” party applications

1) DPI analytics
2) Netflow Collector
3) Security Node
4) Content reconstructing
5) Capture
6) IDS
7) Application Performance
8) Protocol Analyzer
9) Lawful Intercept

CUBRO NETWORK VISIBILITY
SIMPLE | SCALABLE | SUSTAINABLE

DPI on Omnia120

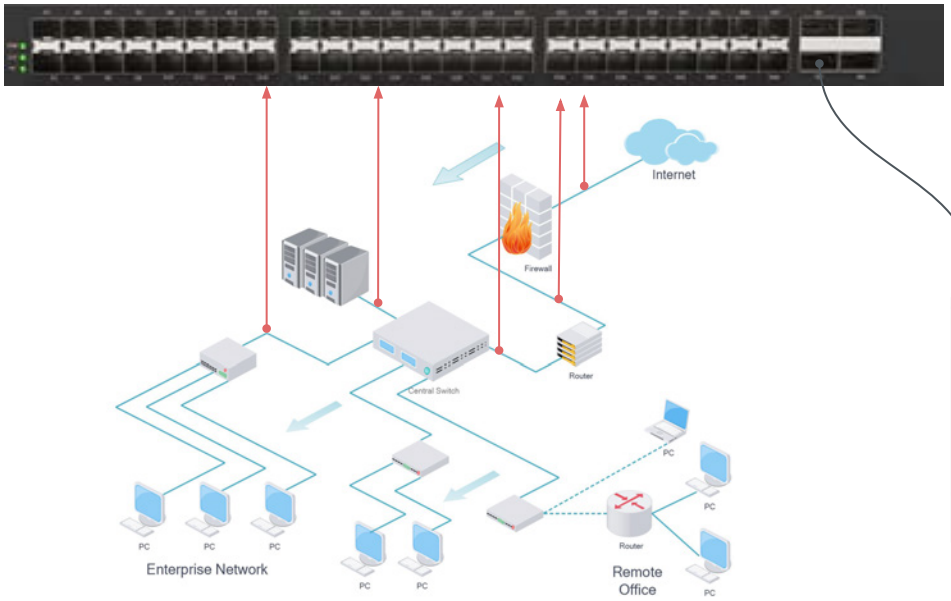


The dual CPU concept of Omnia120
Gives the option to use the unit as NPB in combination with and DPI probe. Depending on the performance several options of usage are possible.

- DPI filtering (analytics in CPU filtering in silicon)
- Flow based Metadata (IPFIX + DPI) external storage and GUI
- Time sliced DPI Metadata -> external Storage and GUI
- Custos (internal storage and GUI)

CUBRO NETWORK VISIBILITY
SIMPLE | SCALABLE | SUSTAINABLE

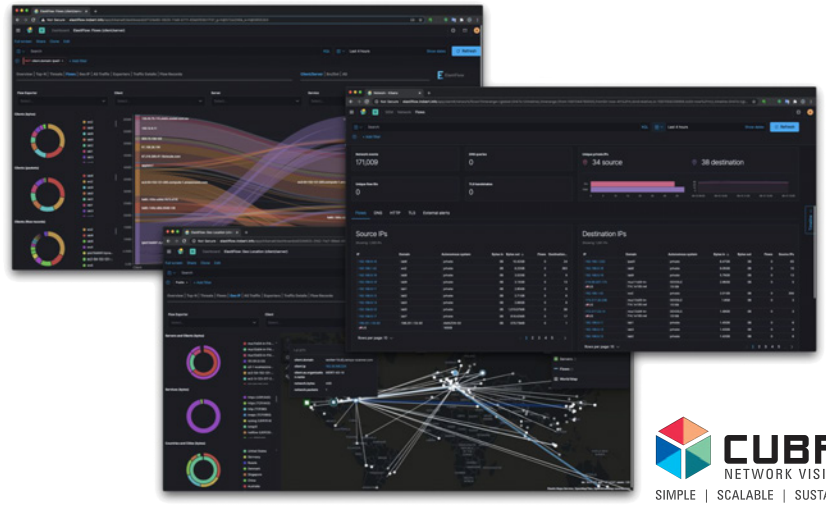
IPFIX - DPI with Omnia120
(with external IPFIX collector)



Omnia120 connected to all relevant links in the network to monitor and protect the network.

Omnia120 does the tapping / aggregation/ filtering / IPFIX / DPI and forwards the metadata to the collector software. (Any IPFIX collector can be used) The IPFIX DPI performance is > 60 Gbit

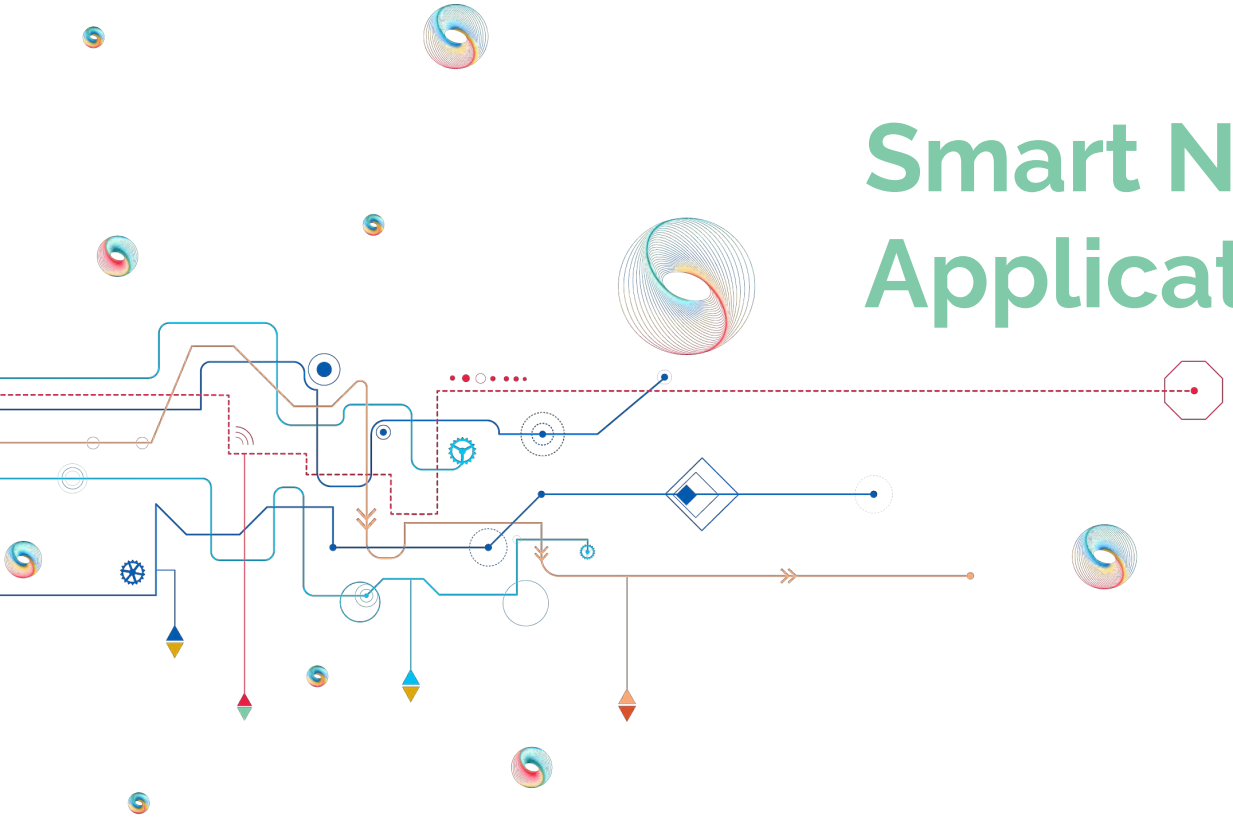
The screenshot shows collector (external appliance)



Advanced NPB + Netflow Producer

Server Netflow Collector and analytics

CUBRO NETWORK VISIBILITY
SIMPLE | SCALABLE | SUSTAINABLE



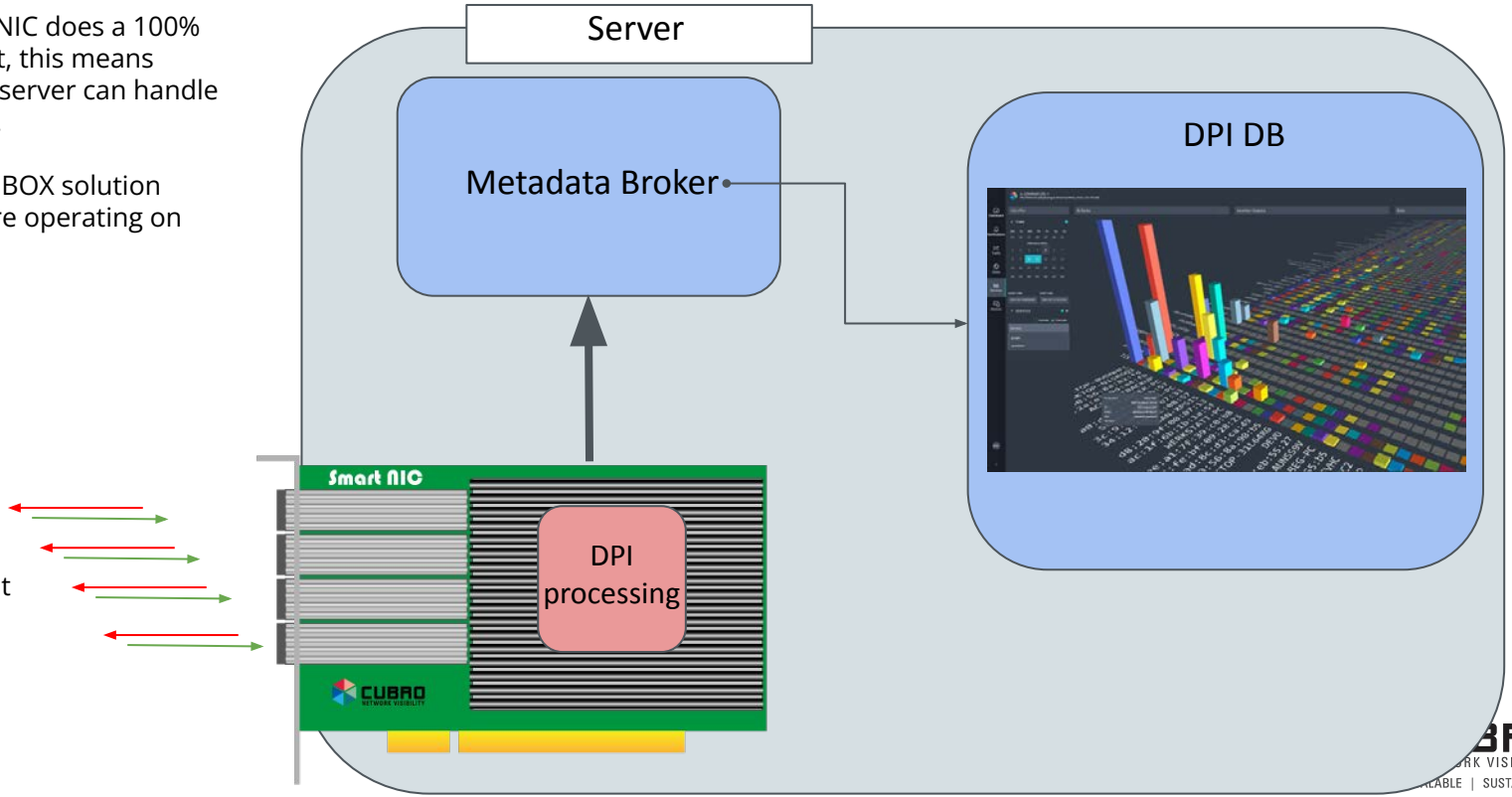
Smart NIC Applications

CUBRO
NETWORK VISIBILITY
SIMPLE | SCALABLE | SUSTAINABLE

Smart NIC DPI application (for other Smart NIC application look at the Smart NIC PPT)

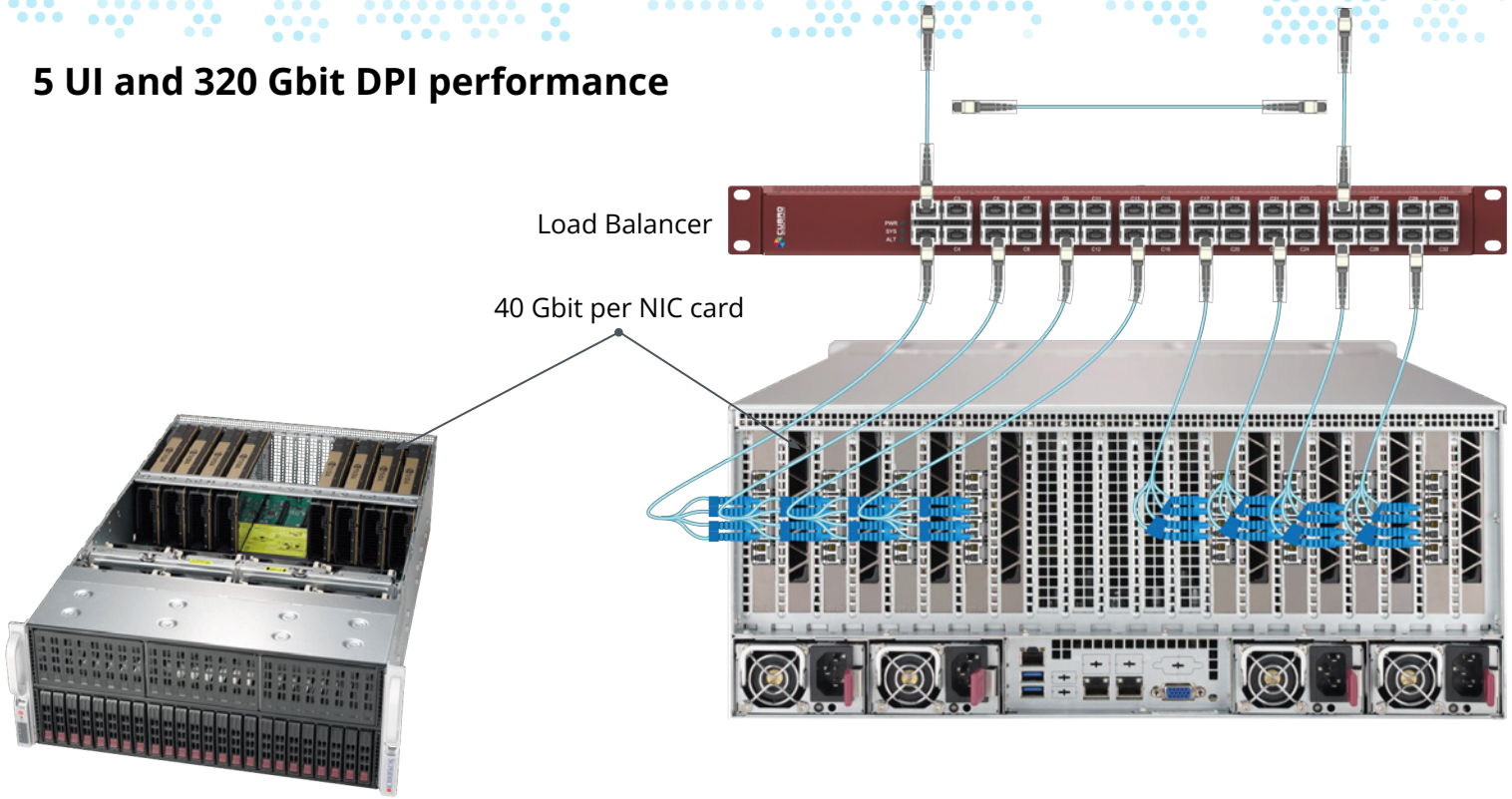
The Cubro Smart NIC does a 100% offload of the host, this means even a small host server can handle 40 Gbit DPI traffic.

This is a all in one BOX solution
All components are operating on the same server



Multi Smart NIC in Super Server

5 UI and 320 Gbit DPI performance



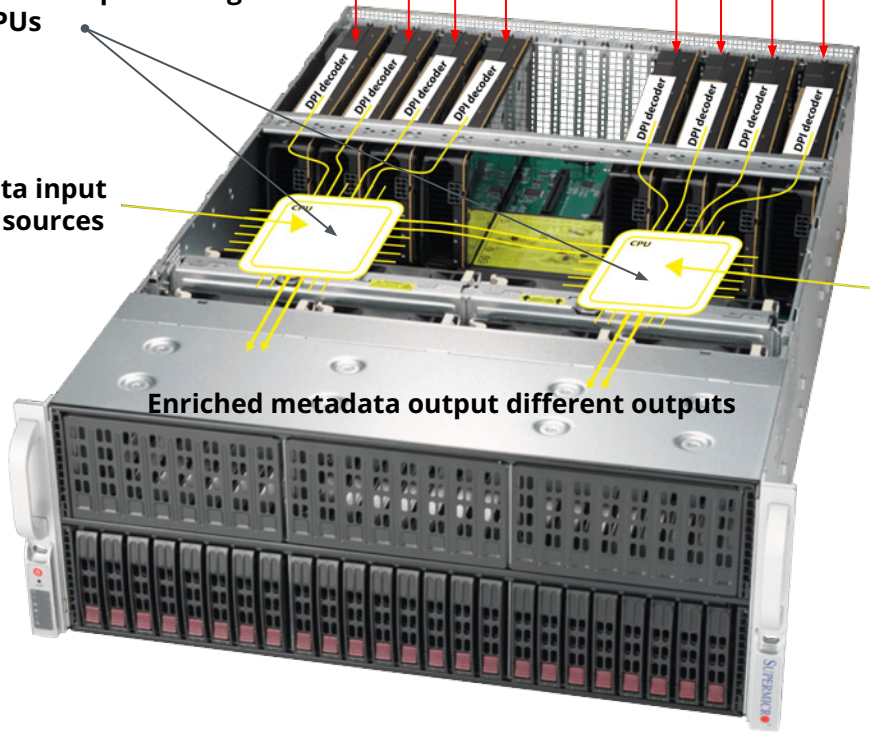
CUBRO NETWORK VISIBILITY
SIMPLE | SCALABLE | SUSTAINABLE

Super Server internal function

raw packet input up to 40 Gbit per Smart NIC

Enrichment and data processing on the Intel CPUs

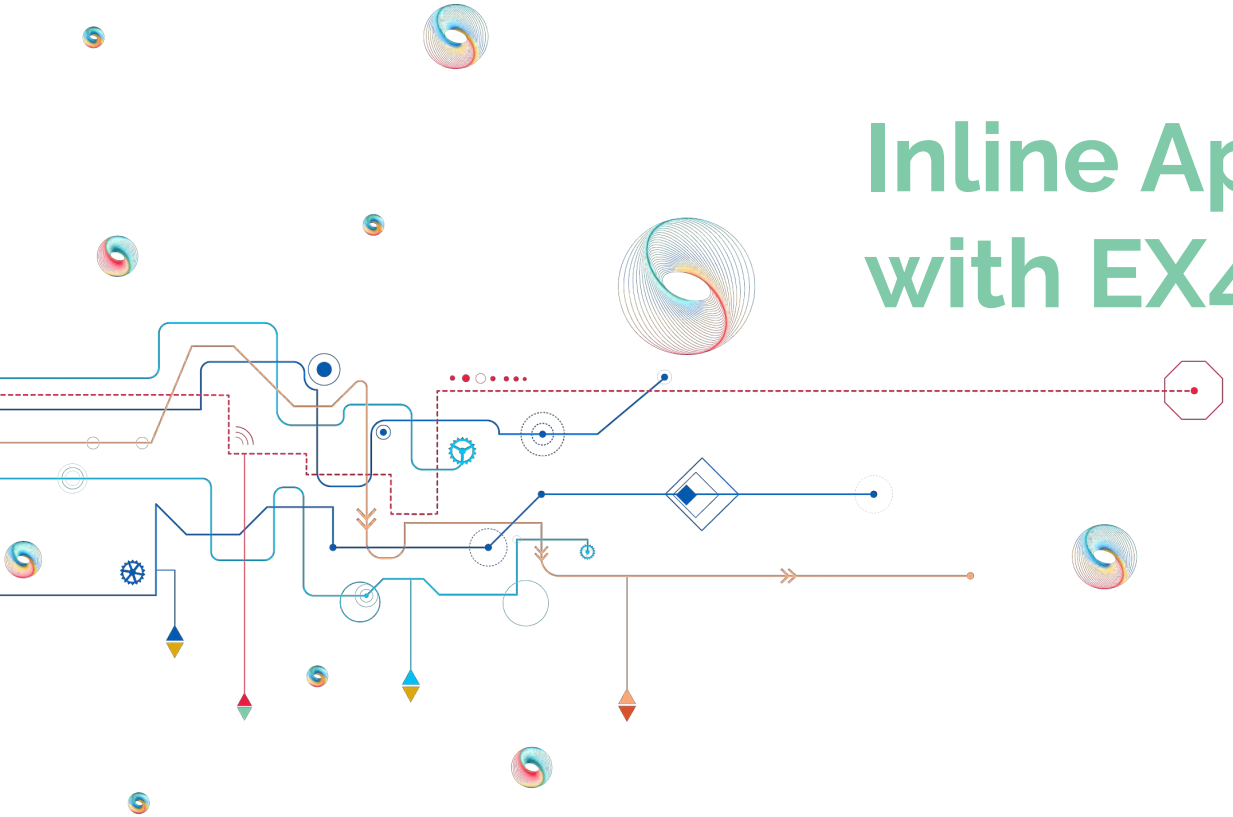
enrichment data input from different sources



enrichment data input from different sources

Enriched metadata output different outputs

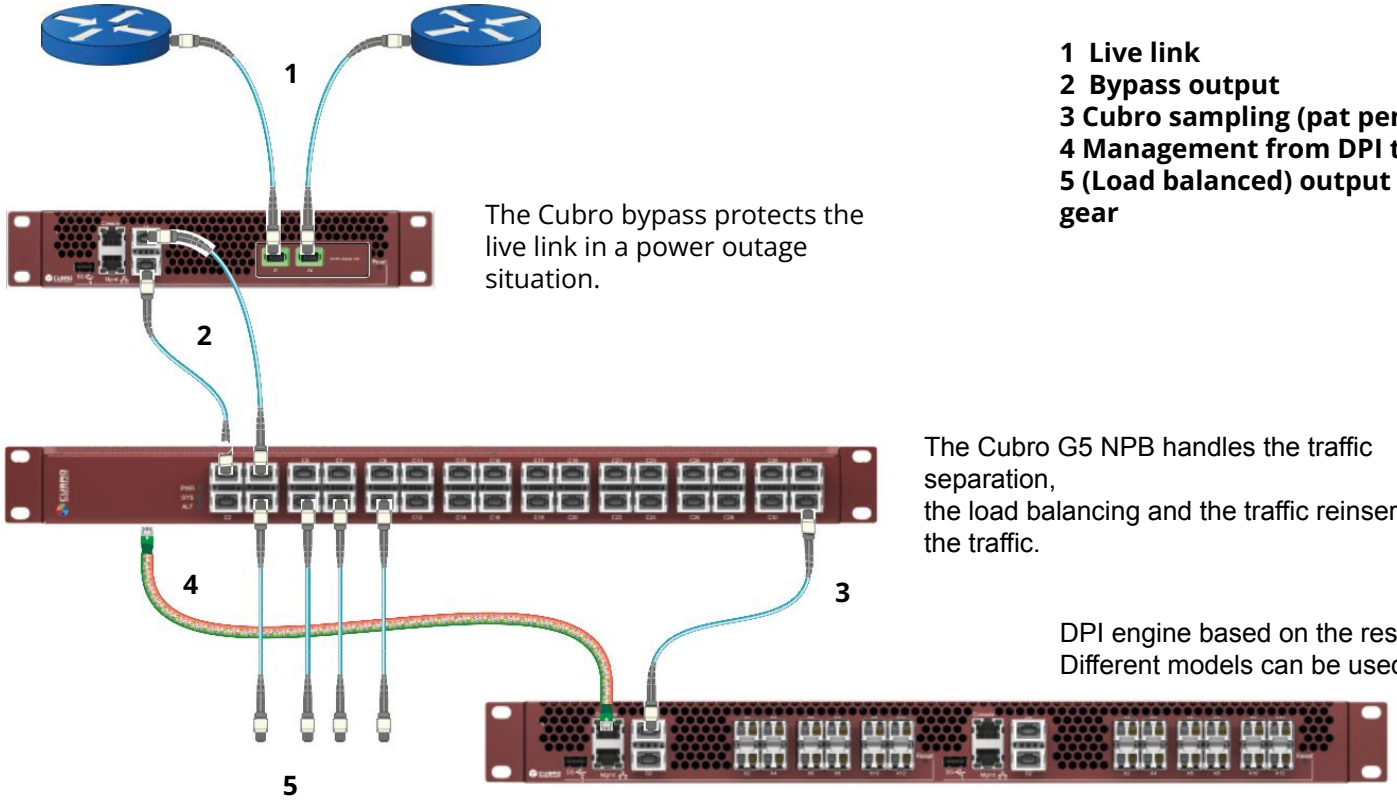
CUBRO NETWORK VISIBILITY
SIMPLE | SCALABLE | SUSTAINABLE



Inline Applications with EX400 bypass

CUBRO
NETWORK VISIBILITY
SIMPLE | SCALABLE | SUSTAINABLE

The full picture inline application



The Cubro bypass protects the live link in a power outage situation.

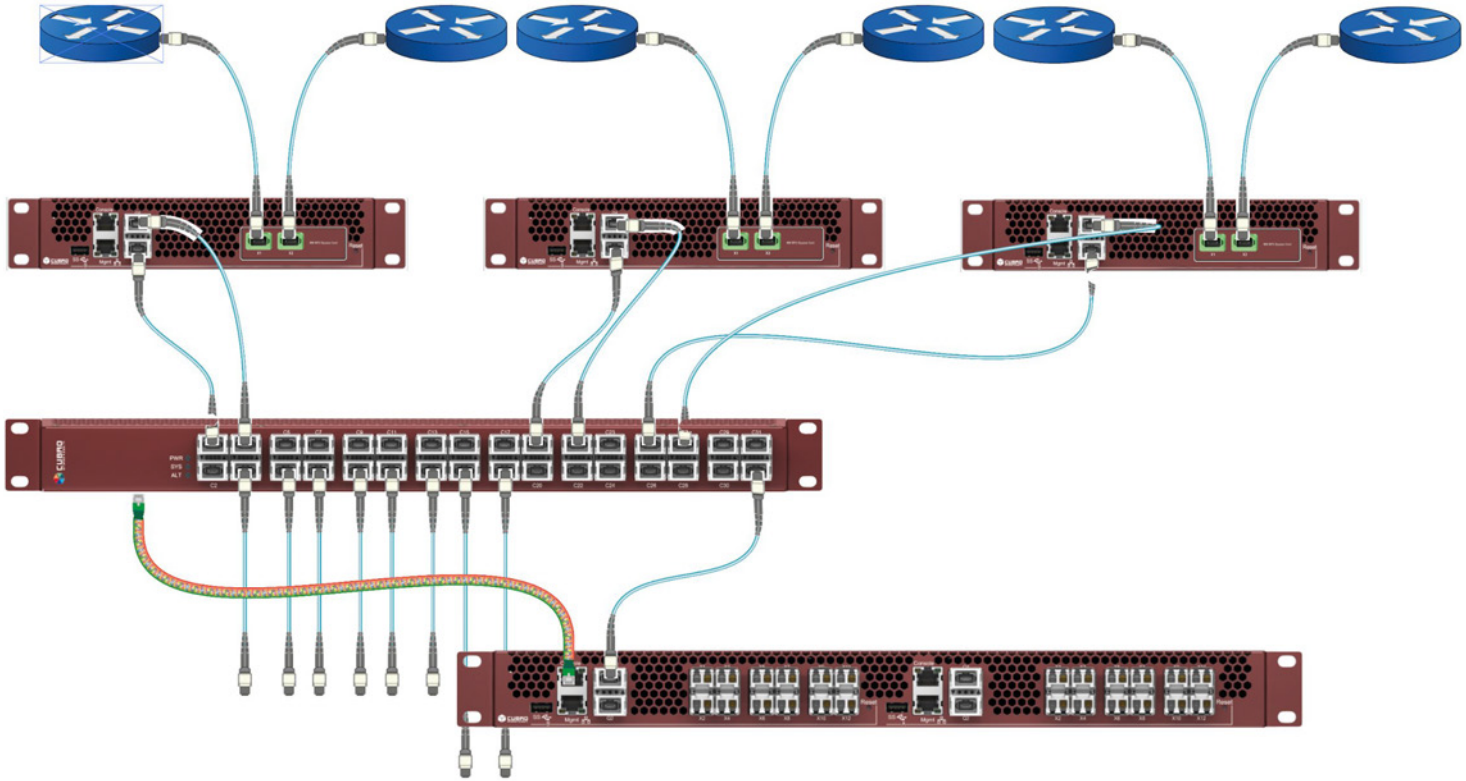
1 Live link
2 Bypass output
3 Cubro sampling (pat pending) to DPI unit
4 Management from DPI to Cubro NPB
5 (Load balanced) output to downstream gear

The Cubro G5 NPB handles the traffic separation,
the load balancing and the traffic reinserting of the traffic.

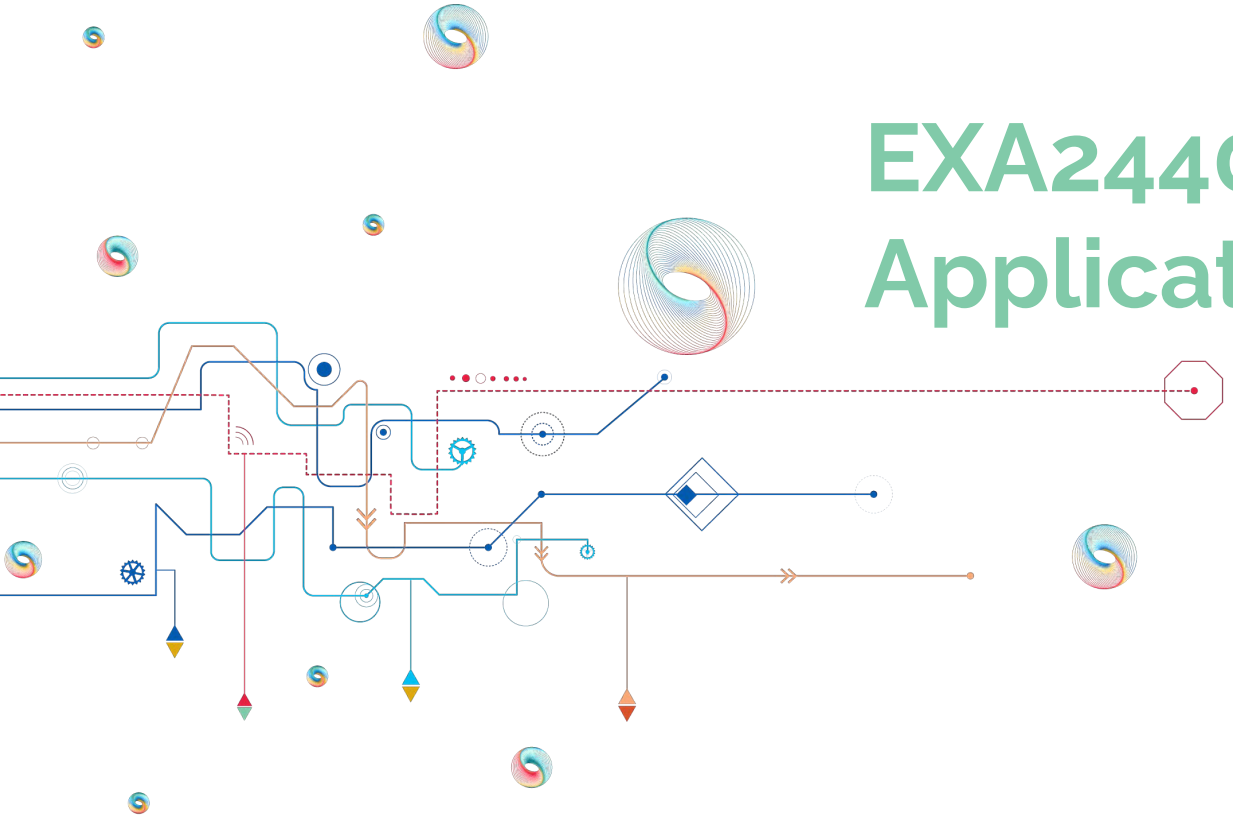
DPI engine based on the resources which are needed.
Different models can be used from Omnia10 - up to Ingens.

CUBRO NETWORK VISIBILITY
SIMPLE | SCALABLE | SUSTAINABLE

Up to 2 TB and 8 x 100 Gbit link inline



CUBRO NETWORK VISIBILITY
SIMPLE | SCALABLE | SUSTAINABLE



EXA24400 DPI Applications

CUBRO
NETWORK VISIBILITY
SIMPLE | SCALABLE | SUSTAINABLE

Analytics Applications up to multiple 100 GB with EXA24400

Live traffic from TAP / SPAN ports
multiple 100 Gbit input

DPI DB

Metadata Broker

Function of Metadata Broker see pages 35/36

Advanced load balancing

EXA 24400 DPI analytics

Up to 100 Gbit per 1 U unit

multiple units

Very efficient UDP metadata stream
with DPI application enrichment.

CUBRO NETWORK VISIBILITY
SIMPLE | SCALABLE | SUSTAINABLE

Analytics Applications up to 900 GB with EXA24400 with Mobile Network signaling

DPI DB

Enriched output

Metadata Broker

[More details on the Broker see here]

Live traffic from TAP / SPAN ports
multiple 100 Gbit input

Mobil core signaling

Advanced load balancing

EXA 24400 DPI analytics

Up to 100 Gbit per 1 U unit

multiple units

Very efficient UDP metadata stream
with DPI application enrichment.

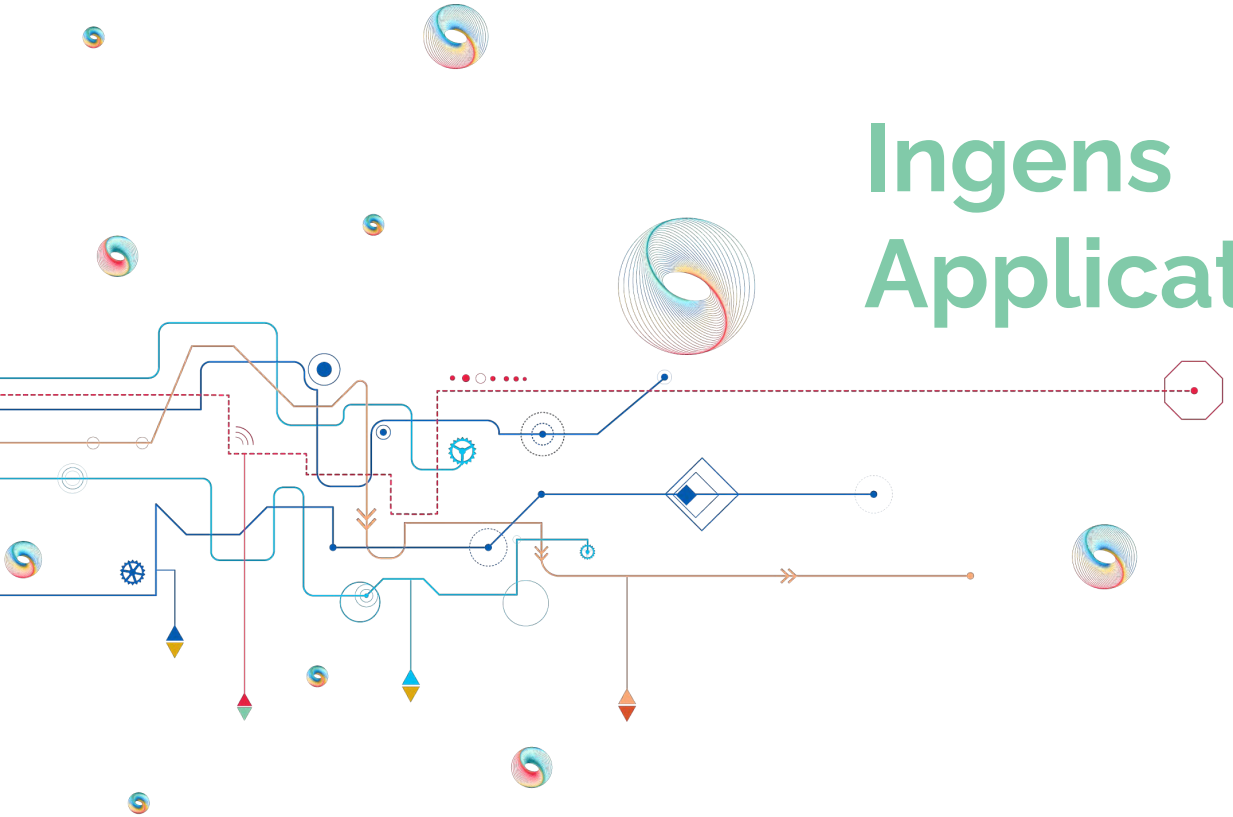
S11/Sxa/Sxb/S5-S8/N4
input from the Network

UDP Metadata stream
to the Broker

Signaling extractor
/ probe

Typical only one CPU is needed to process the signaling, the second CPU can be used for DPI as well

CUBRO NETWORK VISIBILITY
SIMPLE | SCALABLE | SUSTAINABLE

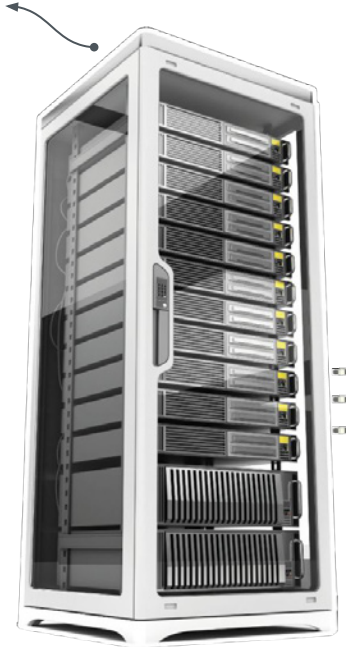


Ingens Applications

CUBRO
NETWORK VISIBILITY
SIMPLE | SCALABLE | SUSTAINABLE

DPI Analytics Applications up to 1.4 TB with Ingens

Kafka / Hadoop Cluster

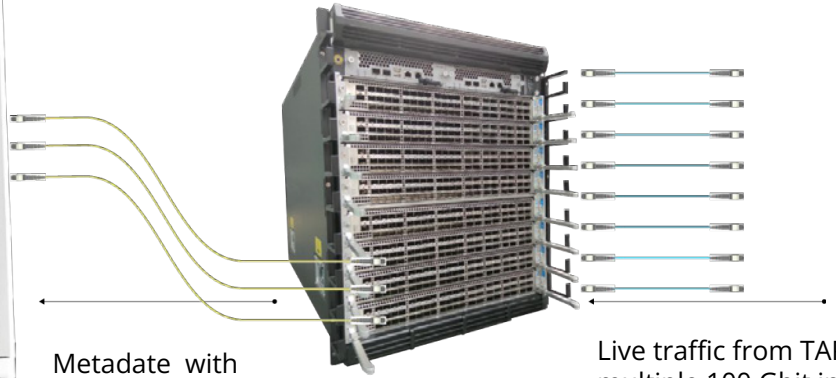


The Ingens platform acts as NPB and as a Probe

Aggregation & Load Balancing on the front blades

Metadata extraction on the rear blades up to 16 x 24 core ARM CPU.
Gives a lot performance for any kind of metadata extraction.

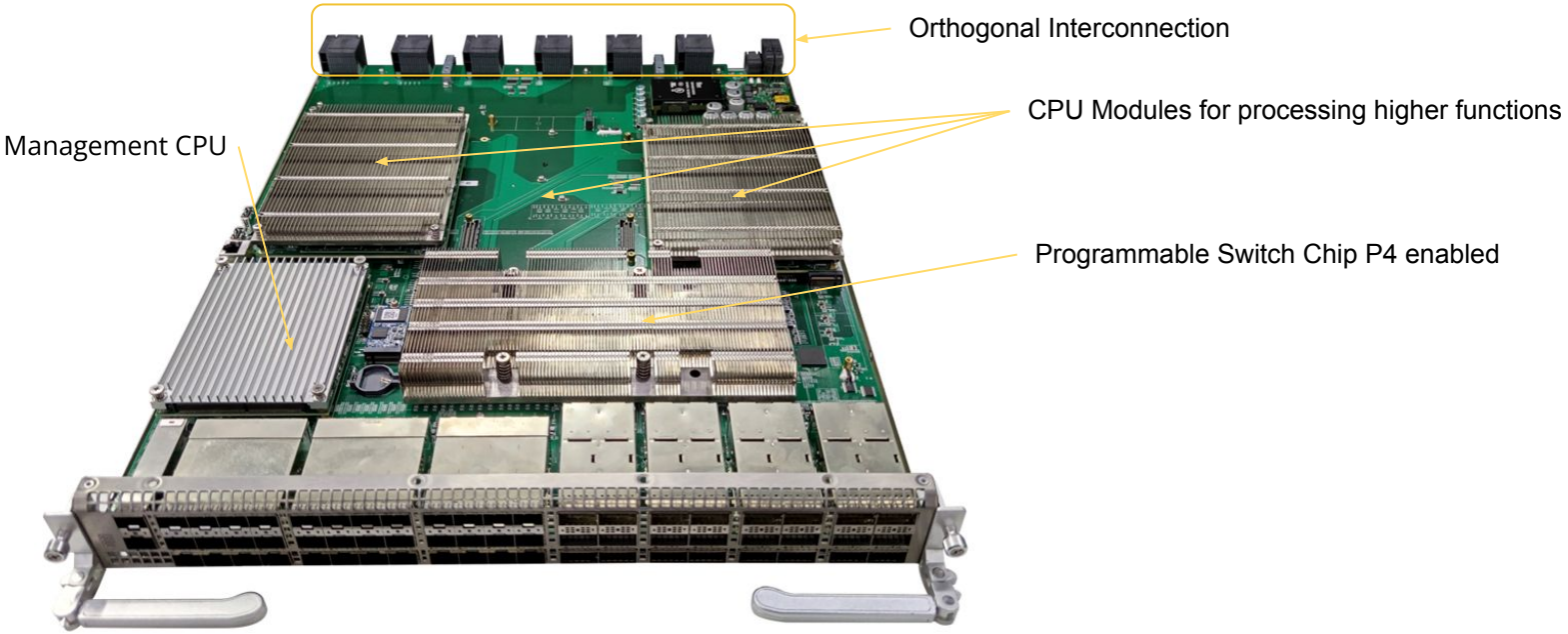
(see the Inges description for more details)



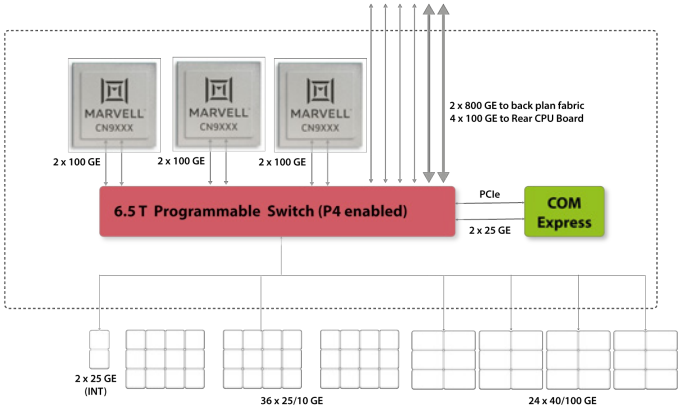
Metadate with
DPI application enrichment.

Live traffic from TAP / SPAN ports
multiple 100 Gbit input

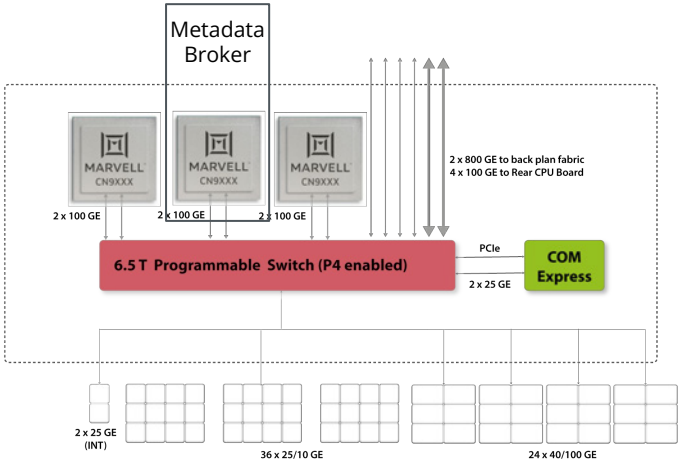
Ingens Service Board internal



Ingens Service boards options

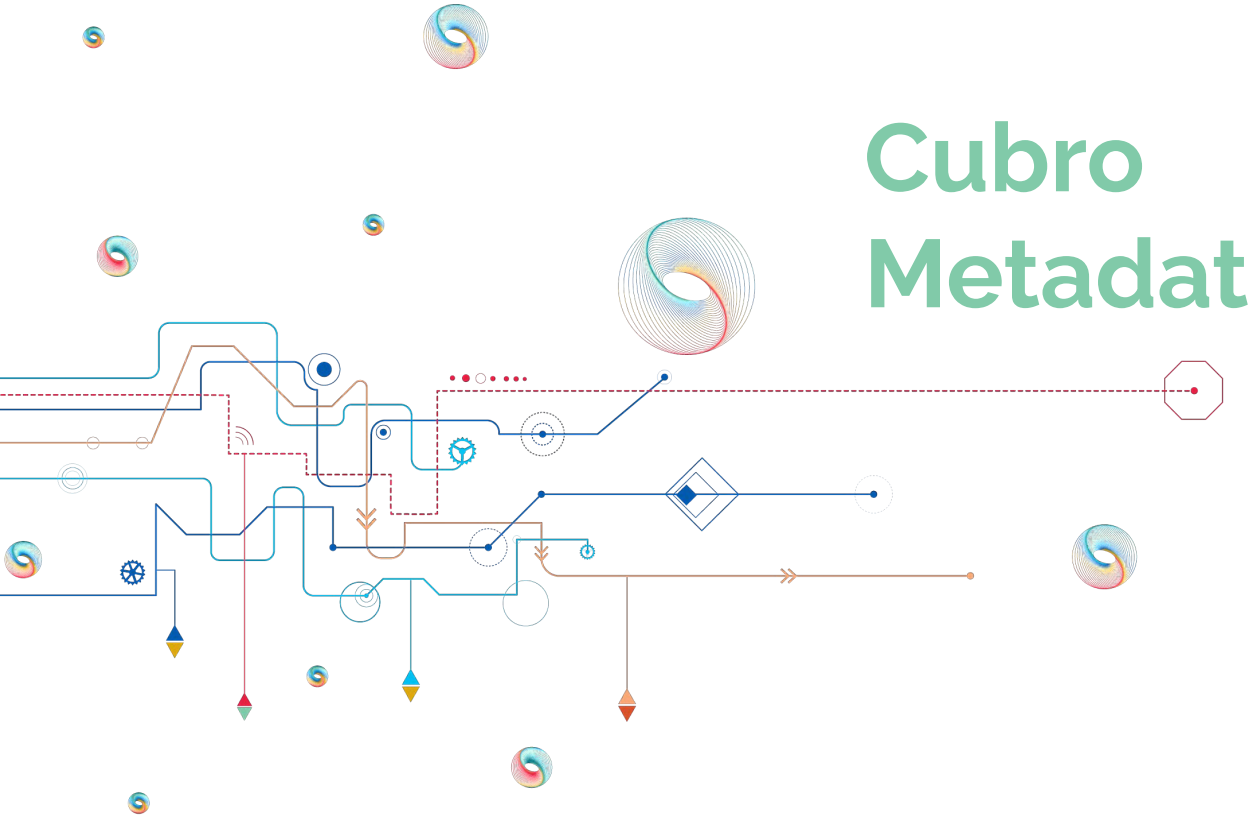


All 3 CPUs do DPI and than you us an external Metadata Broker



In this case one CPU is used to run the Metadata Broker to feed results direct to any other tool

CUBRO NETWORK VISIBILITY
SIMPLE | SCALABLE | SUSTAINABLE



Cubro
Metadata Broker

CUBRO
NETWORK VISIBILITY
SIMPLE | SCALABLE | SUSTAINABLE

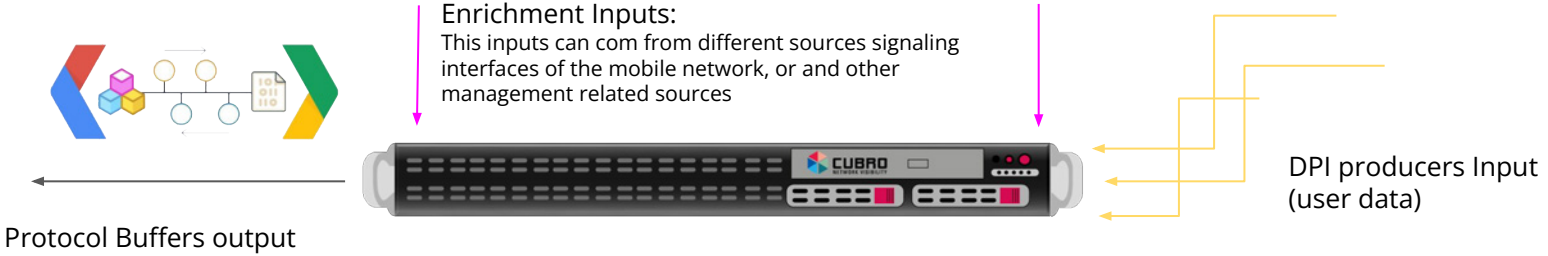
Cubro Metadata Broker

The Cubro Metadata Broker is a server based application available on Intel or ARM which receives the UDP streams from the DPI producers and performs several actions to generate an output stream which fulfills the customers requests.

- Data Enrichment from other sources
- Data Aggregation
- Time Aggregation
- Output Formation

The prefered output format is Google Protocol Buffers because it is a very efficient format. (see next page)

This format is supported by and modern programming language and is a very efficient way to serialize and deserialize data.



Protocol Buffers as Output

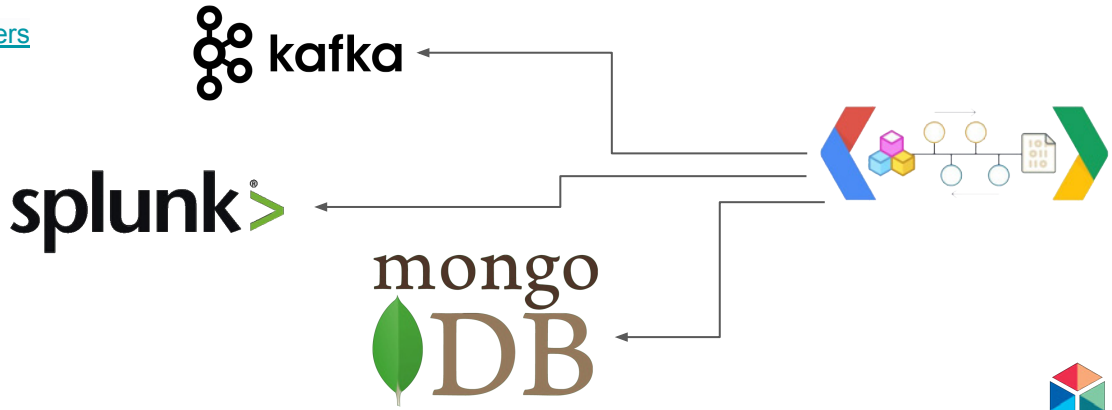
Google developed Protocol Buffers for use in their internal services. It is a binary encoding format that allows you to specify a *schema* for your data using a specification language.

Protocol Buffers offers several compelling advantages over JSON or YAML for sending data over the wire between internal services. While not a wholesale replacement for JSON, especially for services which are directly consumed by a web browser, Protocol Buffers offers very real advantages not only in the ways outlined above, but also typically in terms of speed of encoding and decoding, size of the data on the wire, and more.

Confluent just updated their Kafka streaming platform with additional support for serialising data with Protocol buffers (or protobuf) and JSON Schema serialisation. This makes integration much more easy.

https://developers.google.com/protocol-buffers

Protocol Buffers is supported by all Big Data platforms



Advantages of Cubro DPI

Cubro DPI introduces intelligence into the internet network. Unlike most other vendors, Cubro's DPI approach includes **bypass** and **application blocking** which can enable Internet Service Providers to effectively monitor, speed up, filter, block and make any other useful decision about the traffic of the users.

- Gain the business intelligence to tackle the 5G challenge
- Maintain high levels of network performance
- Ensure a lower TCO for the network
- Enhance the overall QoS

Quality & Environment Management

TÜV NORD

CERTIFICATE

Management system as per
DIN EN ISO 9001 : 2015

In accordance with TÜV NORD CERT procedures, it is hereby certified that

Cubro Acronet GesmbH
Ghegastraße 3
1030 Wien
Austria

CUBRO

applies a management system in line with the above standard for the following scope

Sales and development of network monitoring and network visibility solutions

Certificate Registration No. 44 100 18600030
Audit Report No. ZER1634a

Valid from 2019-06-12
Valid until 2022-06-11
Initial certification 2019

Certification Body
at TÜV NORD CERT GmbH

TÜV Nord Austria GmbH
Dieferbachgasse 35
1150 Vienna, Austria

Vienna, 2019-06-12

This certification was conducted in accordance with the TÜV NORD CERT auditing and certification procedures and is subject to regular surveillance audits.

TÜV NORD CERT GmbH Langemarckstraße 20 45141 Essen www.tuev-nord-cert.com

IAF DAkkS

TÜV NORD

CERTIFICATE

Management system as per
DIN EN ISO 14001 : 2015

In accordance with TÜV NORD CERT procedures, it is hereby certified that

Cubro Acronet GesmbH
Ghegastraße 3
1030 Wien
Austria

CUBRO

applies a management system in line with the above standard for the following scope

Sales and development of network monitoring and network visibility solutions

Certificate Registration No. 44 104 18600030
Audit Report No. ZER1634a

Valid from 2019-06-12
Valid until 2022-06-11
Initial certification 2019

Certification Body
at TÜV NORD CERT GmbH

TÜV Nord Austria GmbH
Dieferbachgasse 35
1150 Vienna, Austria

Vienna, 2019-06-12

This certification was conducted in accordance with the TÜV NORD CERT auditing and certification procedures and is subject to regular surveillance audits.

TÜV NORD CERT GmbH Langemarckstraße 20 45141 Essen www.tuev-nord-cert.com

IAF DAkkS

Cubro is certified with ISO 9001 for Quality management according to international standards.

Cubro is certified with ISO 14001 for managing the efforts to protect our environment.

CUBRO
NETWORK VISIBILITY
SIMPLE | SCALABLE | SUSTAINABLE

Cubro Network Visibility
Ghegastraße 3
1030 Vienna, Austria

Tel.: +43 1 29826660
Fax: +43 1 2982666399
Email: support@cubro.com

Cubro Asia Pacific
8, Ubi Road 2 #04-12 Zervex
Singapore 408538

Tel.: +65-97255386
Email: jl@cubro.com

THANK YOU

Cubro North America
Cubro Network Visibility Inc.
225 Peachtree Street NE,
Suite 1100, Atlanta, GA, 30303, USA

Email: americas@cubro.com

Cubro Japan
6-7-22, Shinjuku, Shinjuku,
Tokyo, 160-0022 Japan

Tel: +81(0)50-3708-5839
Email: japan@cubro.com