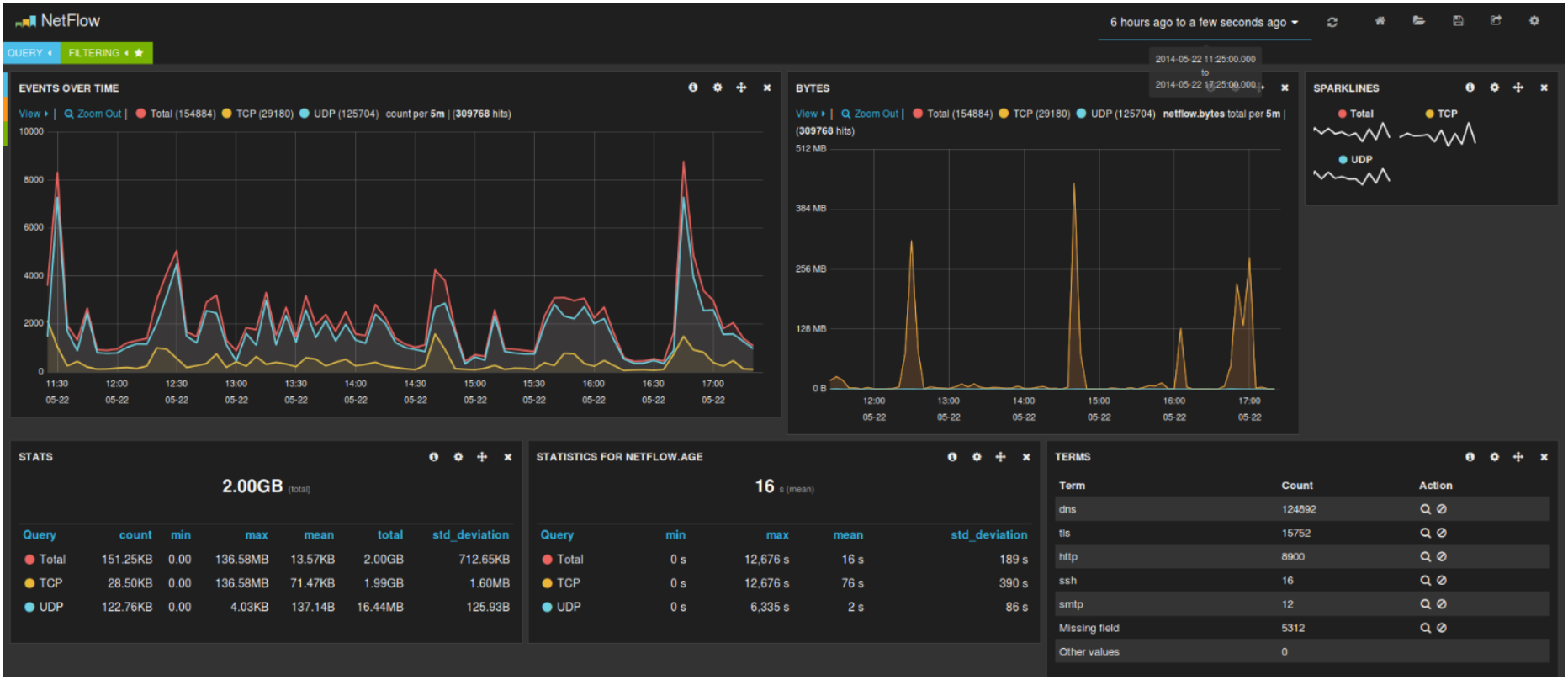
CUBRO
NETWORK VISIBILITY
SIMPLE | SCALABLE | SUSTAINABLE

FlowVista

The Different Flow Monitoring Approach

May 2018

Cubro's Flow Monitoring Approach



The Difference

- Cubro provides a solution from L1 to L7 from TAP over aggregation and load balancing to probe.
  - One vendor for the full metadata extraction
  - Collector agnostic (we don’t provide collectors)
- Cubro provides also solutions for mobile providers with there special needs in many terms
  - Tunnelled traffic
  - Big amount of traffic (load balancing)
  - Enrichment by subscriber data (IMSI,IMEI …)
- Solutions from Gbit to Tbit
  - High performance embedded solution on non Intel multi-core CPU
- Additional features on Netflow V9
  - DPI support on Netflow V9
  - RTT support on Netflow V9

The Units

EXA8 up to 6 Gbit performance and
4 link TAP included

EXA40 and EXA40D up to 40 Gbit

EXA24160 up to 120 Gbit

ATCA Platform up to 2 TB

Why do we not provide Collectors ?

We at Cubro think generating metadata from L1 to L7 is a big challenge anyway but database and business intelligence and analytics is another challenge.

We at Cubro are hardware and embedded software experts and this is what we are doing.

There are so many collector solutions out in the market from open source to the fully integrated commercial solutions.

We are fine with all of them - we are agnostic. We provide the customer solutions ranging from tapping, aggregation, load balancing and metadata extraction, layer all from one hand and one responsibility.

But for the analytics layer you need to choose a different vendor. We are open to work with all vendors, to deliver a good, sustainable solution to the end customer.

DPI on Netflow V9

Typically Netflow was developed for L4 statistics out of the network elements but this is often not enough, especially when you want to target security applications.

That is the reason why we have added DPI functionality to our Netflow solution.

We can detect applications like Whatsapp, Skype, Wechat .. based on DPI regex rules.

At the moment we support the top 900 used applications and the amount is growing on

customers demand.

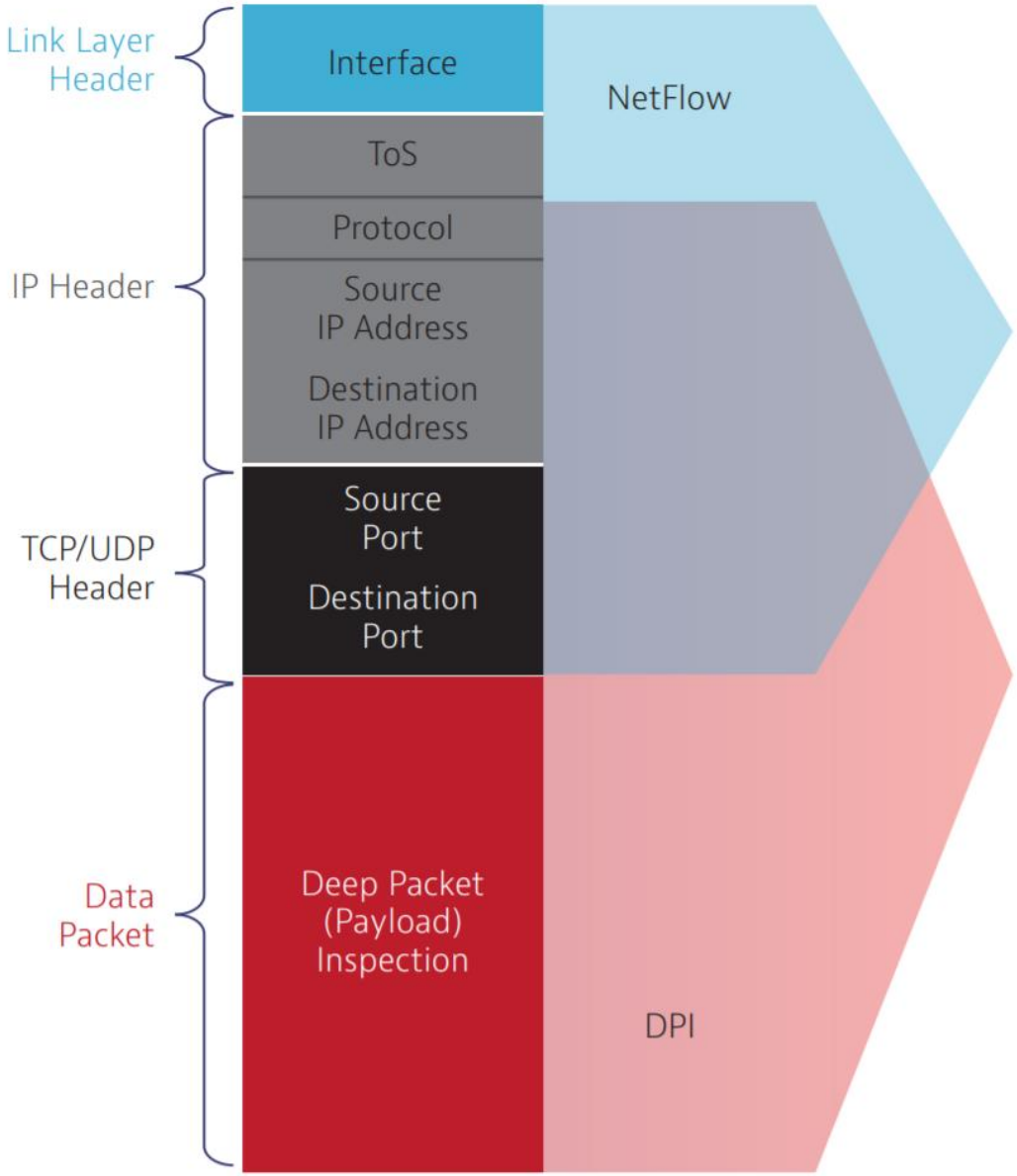
But not only specific applications can be detected, the flexible regex implementation can

also be used to look deeper into the content of the packet to use this as data for enrichment.

Example: Trading applications, power plant steering protocols and much more.

NetFlow and DPI Integration: NetFlow is the de-facto mechanism to provide visibility on network utilization — who/what/where/when. Applications can no longer be identified by just L3/L4 information. Application visibility is a must; Example: port 80 is overloaded; Deep packet inspection boxes to identify applications a cottage industry; With NetFlow + DPI integration provides single report mapping L2-L7 information (CISCO)

DPI on Netflow V9



NetFlow

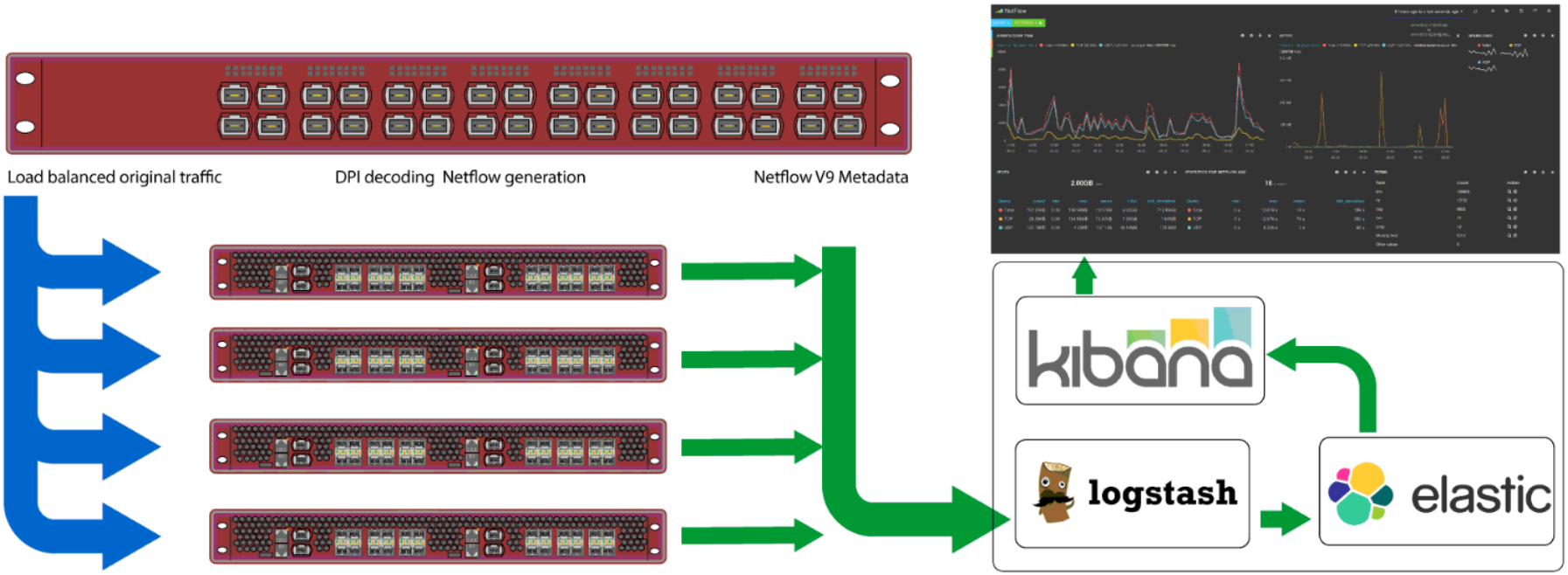
- ✓Monitors data in Layers 2 through 4
- ✓Determines applications by port
- ✓Utilizes a seven-tuple for flow
- ✓Flow information who, what, when, where

DPI

- ✓Examines data from Layers 3 through 7
- ✓Utilizes Layers 3 and 4 plus packet inspection for classification
- ✓Stateful inspection of dynamic-port traffic
- ✓Packet and byte counts

The Typical Approach with Open Source

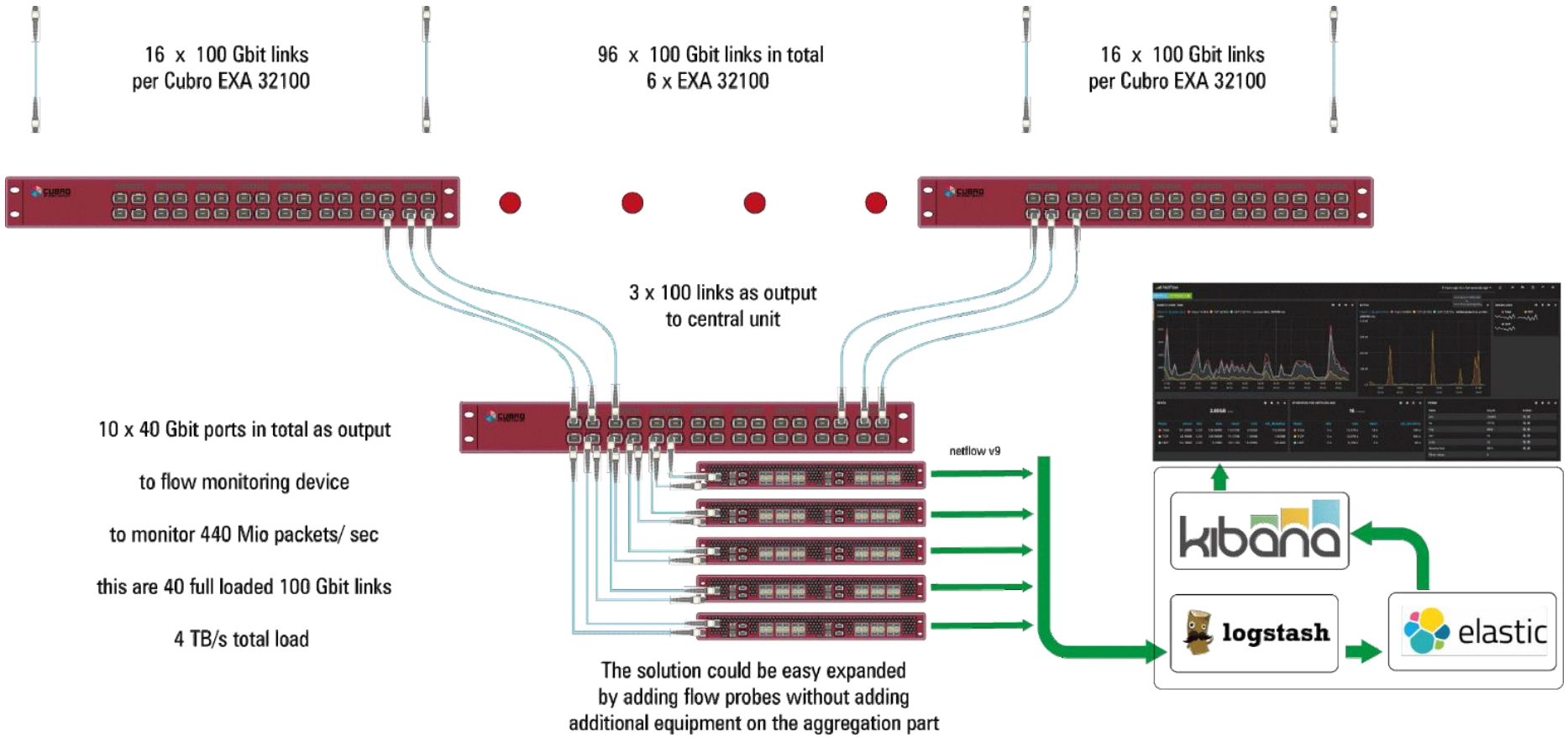
This shows a typical approach - a NPB receives the data, load balances the traffic to multiple probes and the probe provides Netflow CDRs. These CDRs are collected by servers running logstash. The information is stored in elastic as database and display with Kibana or Grafana.



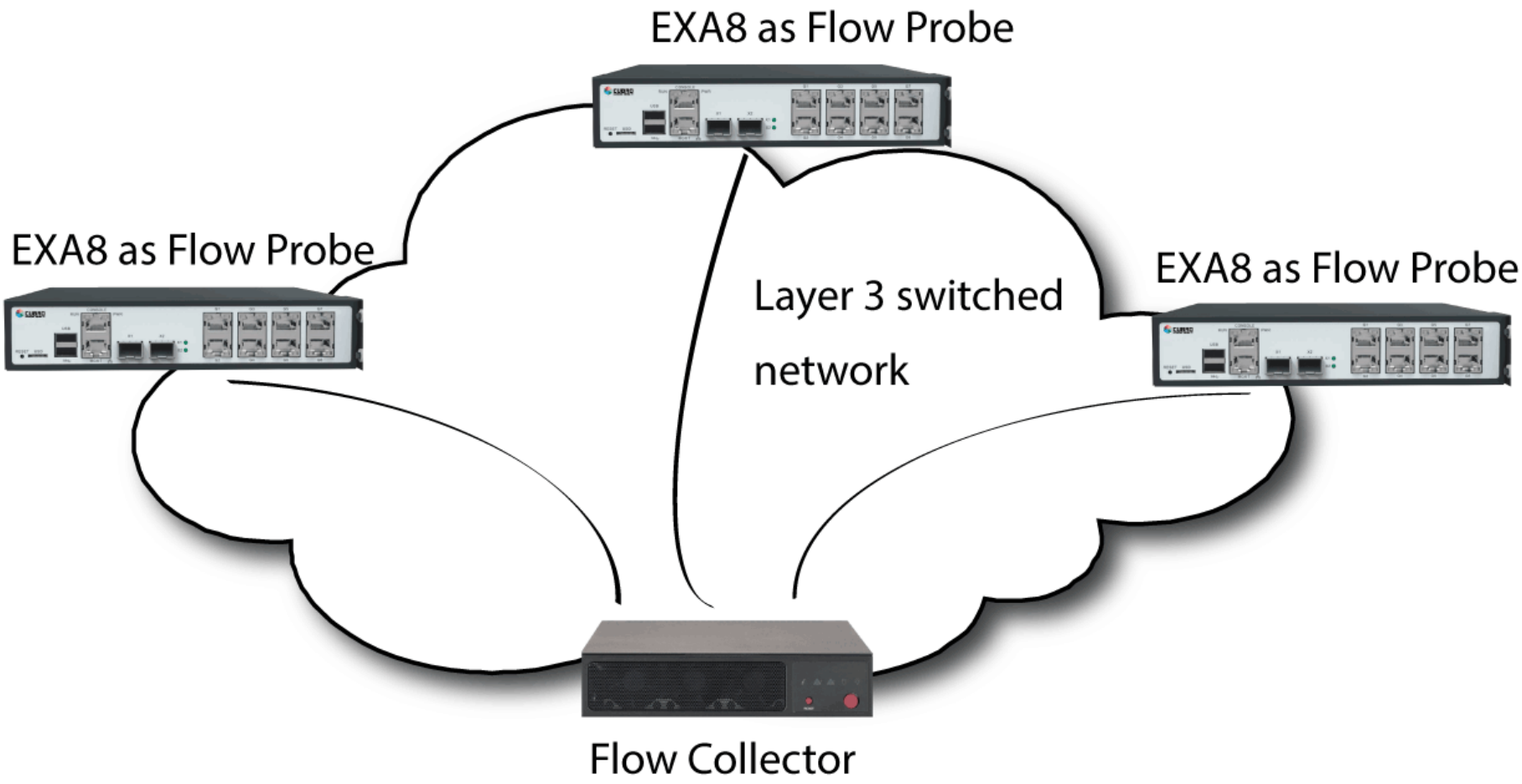
Such a solution can scale up to multiple 100 Gbit input traffic

The Advantage of Working with Cubro!

Cubro can deliver the full visibility stack from TAP to Metadata probe, with a unique feature set. Packet Slicing in multiple 100 Gbit in line rate!



Small Distributed Solution Cubro!



Thank you

EMEA

North America

APAC

Japan

HongKe 虹科

hkaco.com

关注我们

需要详细信息？请通过sales@hkaco.com联系我们 | 电话: 400-999-3848

办事处： 广州 | 北京 | 上海 | 深圳 | 西安 | 武汉 | 成都 | 沈阳 | 香港 | 台湾 | 美国