EXA8 应用

February 2020

CUBRO
NETWORK VISIBILITY
SIMPLE | SCALABLE | SUSTAINABLE

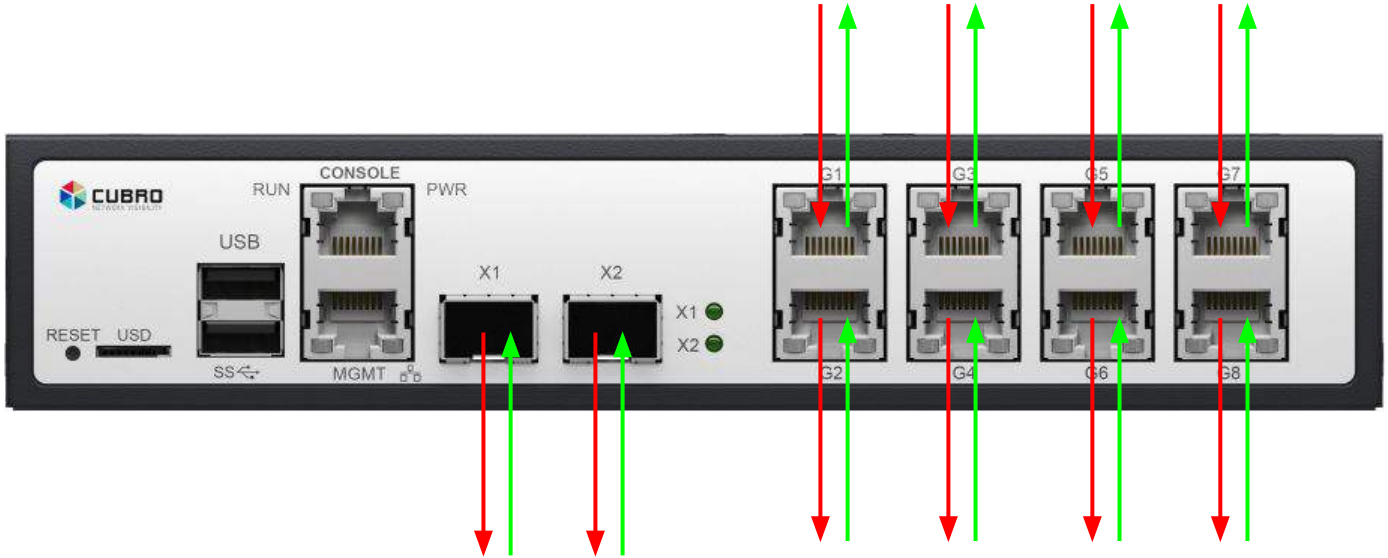
EXA8 - “多合一工具”

EXA8是一款紧凑型的多应用设备，可以用于实时聚合、过滤和捕获网络流量。

- 4链路铜TAP
- 4链路聚合
- Octeon 4 Core ARM CPU
- 1TB SSD存储
- 16 RAM
- 8 x 10/100/1000铜
- 2 x 10G SFP+

CUBRO
NETWORK VISIBILITY
SIMPLE | SCALABLE | SUSTAINABLE

EXA8



2个1/10 Gbit光/电端口，可用作输入和输出(取决于SFP模块)

4 x 1 Gbit链路带内部 TAP (bypass)

CUBRO
NETWORK VISIBILITY
SIMPLE | SCALABLE | SUSTAINABLE

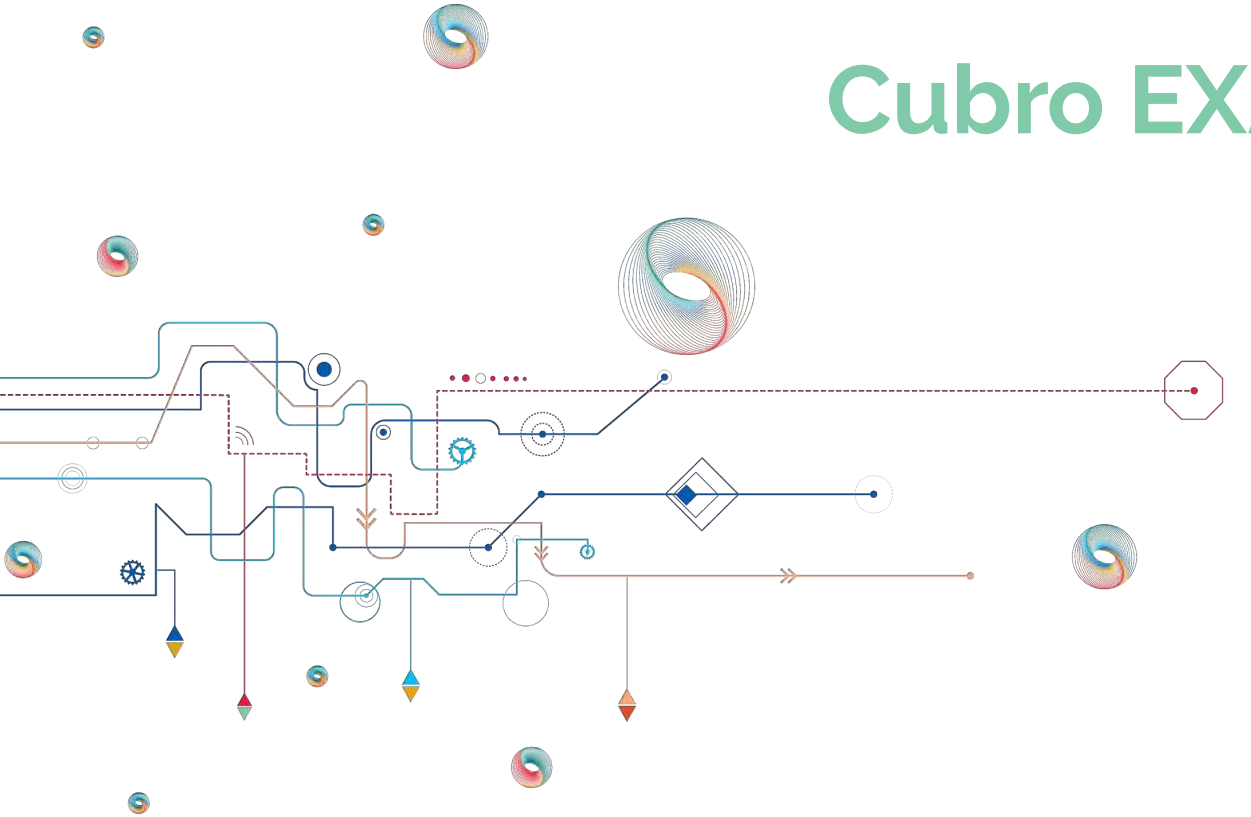
多重功能在1个盒子里

EXA8平台目前提供3个不同的软件版本：

下一张幻灯片解释每个软件的功能集，并帮助确定哪些功能适合个人使用案例。

CUBRO
NETWORK VISIBILITY
SIMPLE | SCALABLE | SUSTAINABLE

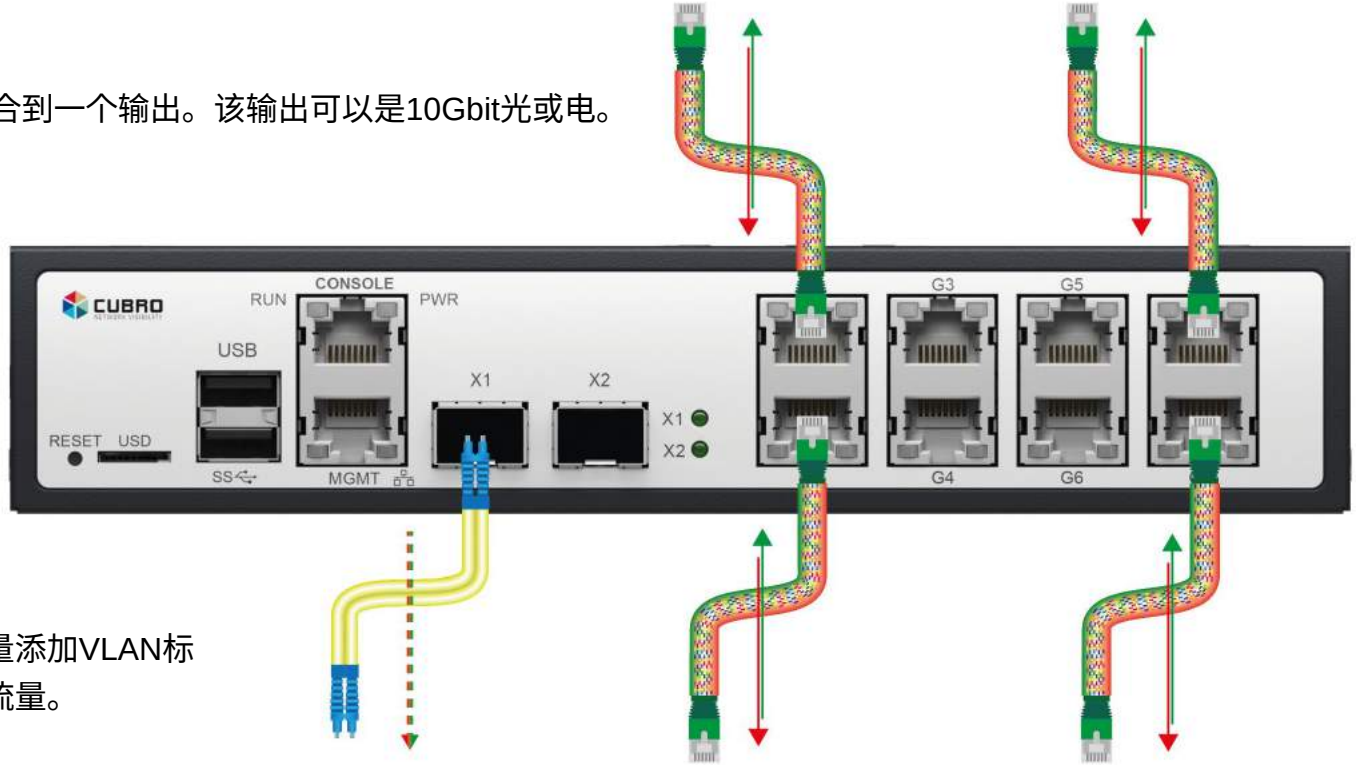
Cubro EXA8聚合



CUBRO
NETWORK VISIBILITY
SIMPLE | SCALABLE | SUSTAINABLE

聚合

最多可将4条链路/8个端口聚合到一个输出。该输出可以是10Gbit光或电。



可以为每个输入的输出流量添加VLAN标签，以在监控工具中分隔流量。

CUBRO
NETWORK VISIBILITY
SIMPLE | SCALABLE | SUSTAINABLE

直观的Web GUI

EXA8 | Device | Ports | Aggregation | Tapping | Settings | Welcome! admin | Sign out | CUBRO

Device Information

Device Model	EXA8
Image Version	1.3.1-4.0
Revision	a9d3236
Serialnumber	124B-1960015
Custom Device Label	Test Lab [Save]

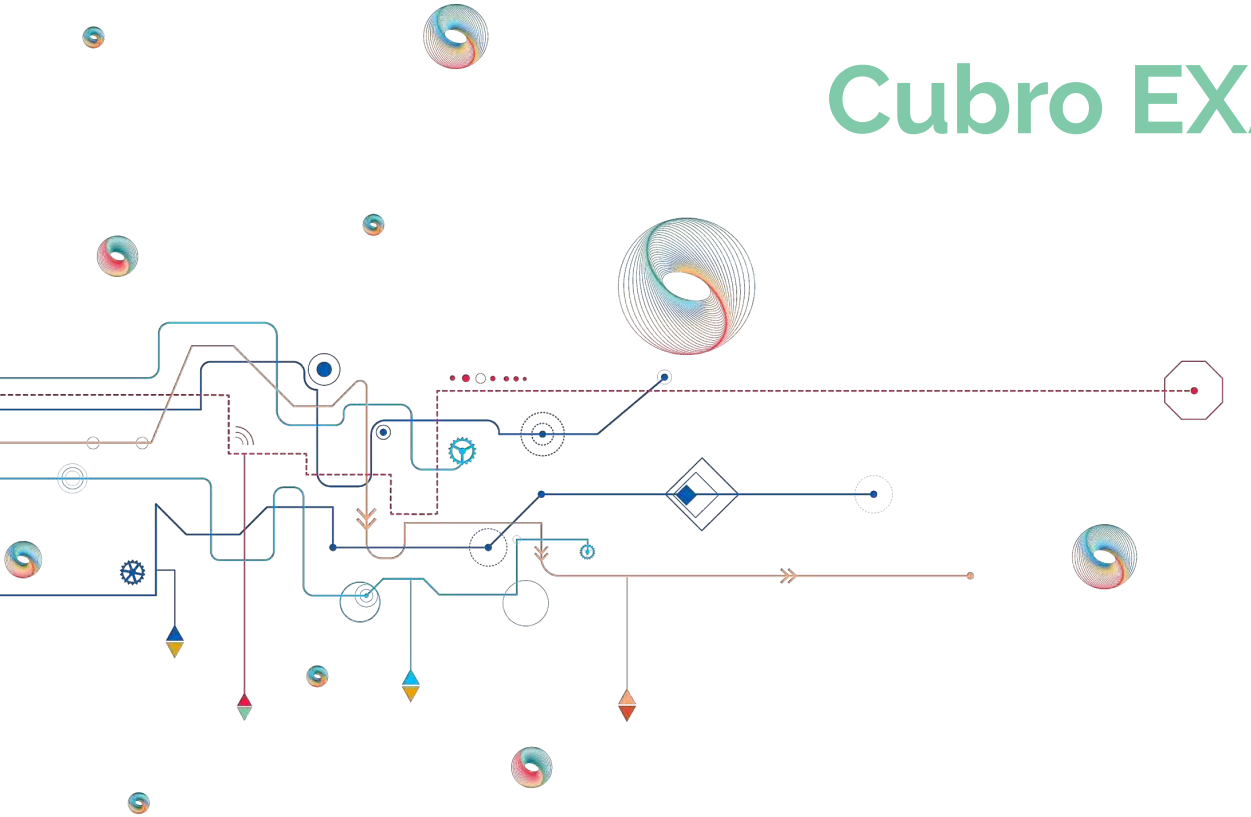
Device Image

Device Configuration

[✔ Save configuration] [↻ Restore configuration] [✖ Reset configuration]

CUBRO NETWORK VISIBILITY
SIMPLE | SCALABLE | SUSTAINABLE

Cubro EXA8捕获探针



CUBRO
NETWORK VISIBILITY
SIMPLE | SCALABLE | SUSTAINABLE

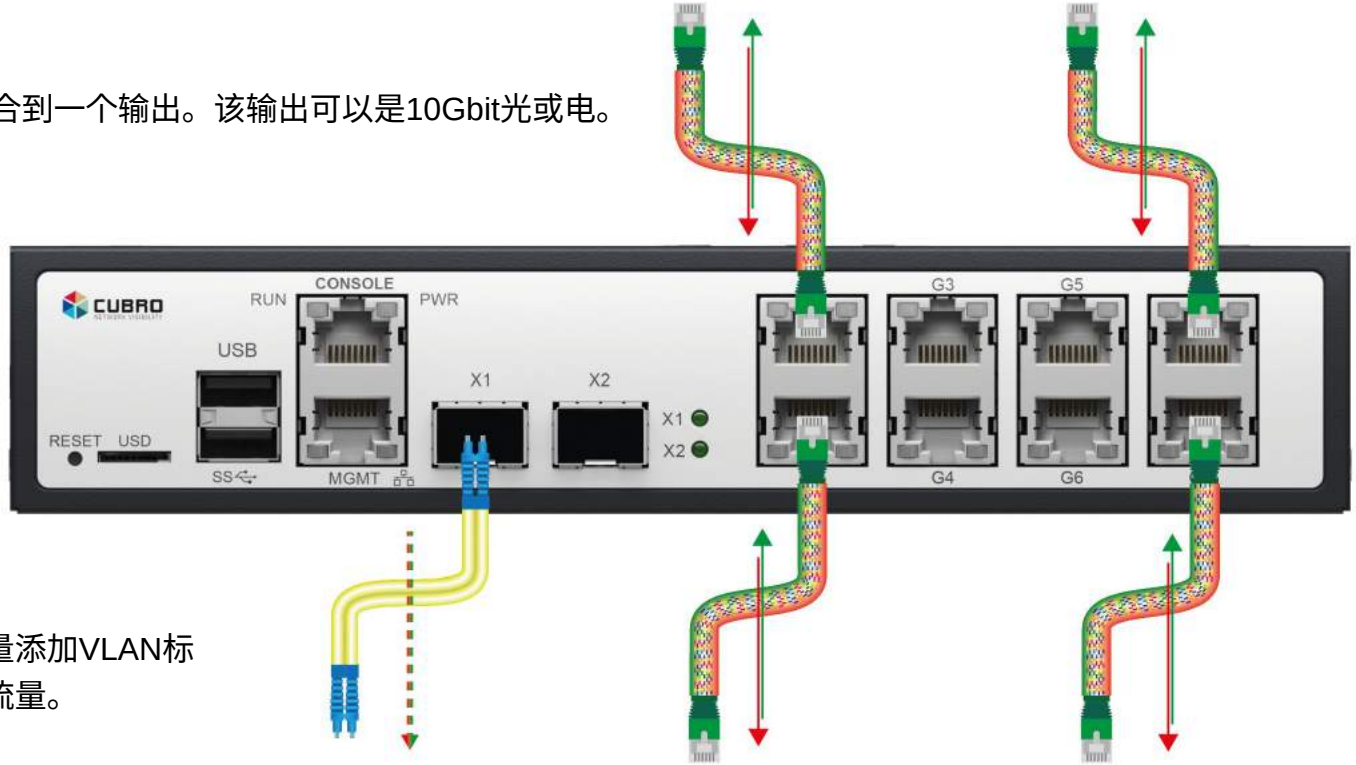
EXA8 - 捕获探针

- 100%捕获所有数据以进行实时分析和历史回放-非常适合故障排除
- 捕获到USB或SSD
- 能够执行其他几个高级应用程序，如Sessionmaster
- 能够运行第三方应用程序
- 滚动捕获 “ 回看时间捕获 ”

CUBRO NETWORK VISIBILITY
SIMPLE | SCALABLE | SUSTAINABLE

聚合

最多可将4条链路/8个端口聚合到一个输出。该输出可以是10Gbit光或电。



可以为每个输入的输出流量添加VLAN标签，以在监控工具中分隔流量。

CUBRO
NETWORK VISIBILITY
SIMPLE | SCALABLE | SUSTAINABLE

直观的Web GUI

EXA8 | Device | Ports | Aggregation | Tapping | Applications | Shell | Settings | Welcome! admin | Sign out | CUBRO

Device Information

Device Model	EXA8
Image Version	1.3.1-4.0
Revision	a9d3236
Serialnumber	124B-1960015
Custom Device Label	Test Lab [Save]

Device Image

Device Configuration

[✔ Save configuration] [↻ Restore configuration] [✖ Reset configuration]

System Information

Booted from: SD-Card

CPU - 53.85% - Temperature 48°C

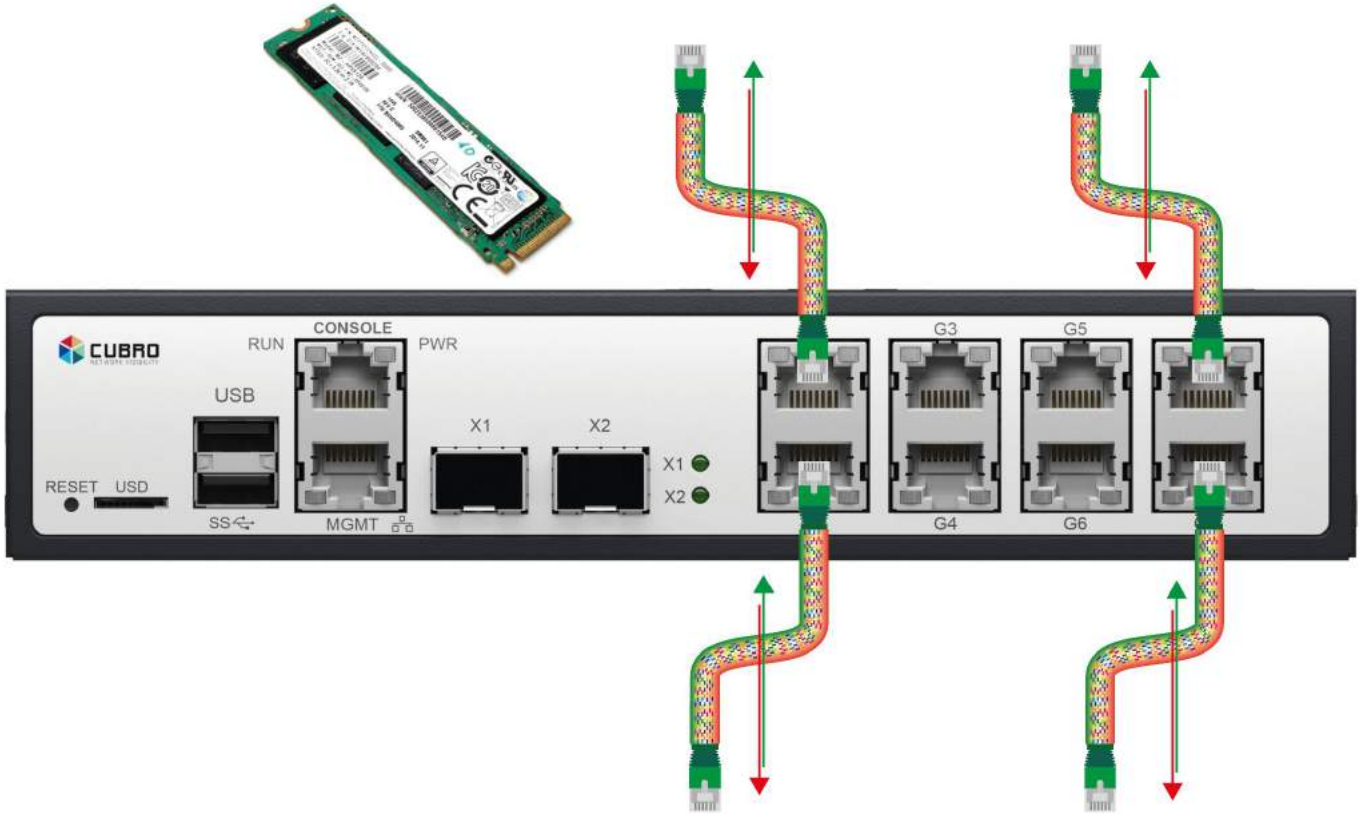
Disk **/** free 2.88 GiB - used 3.95 GiB - total 7.22 GiB

Disk **/mnt/data** free 743.29 GiB - used 33.45 GiB - total 818.33 GiB — SMART OK

Memory free 7.96 GiB - used 4.66 GiB - total 15.89 GiB

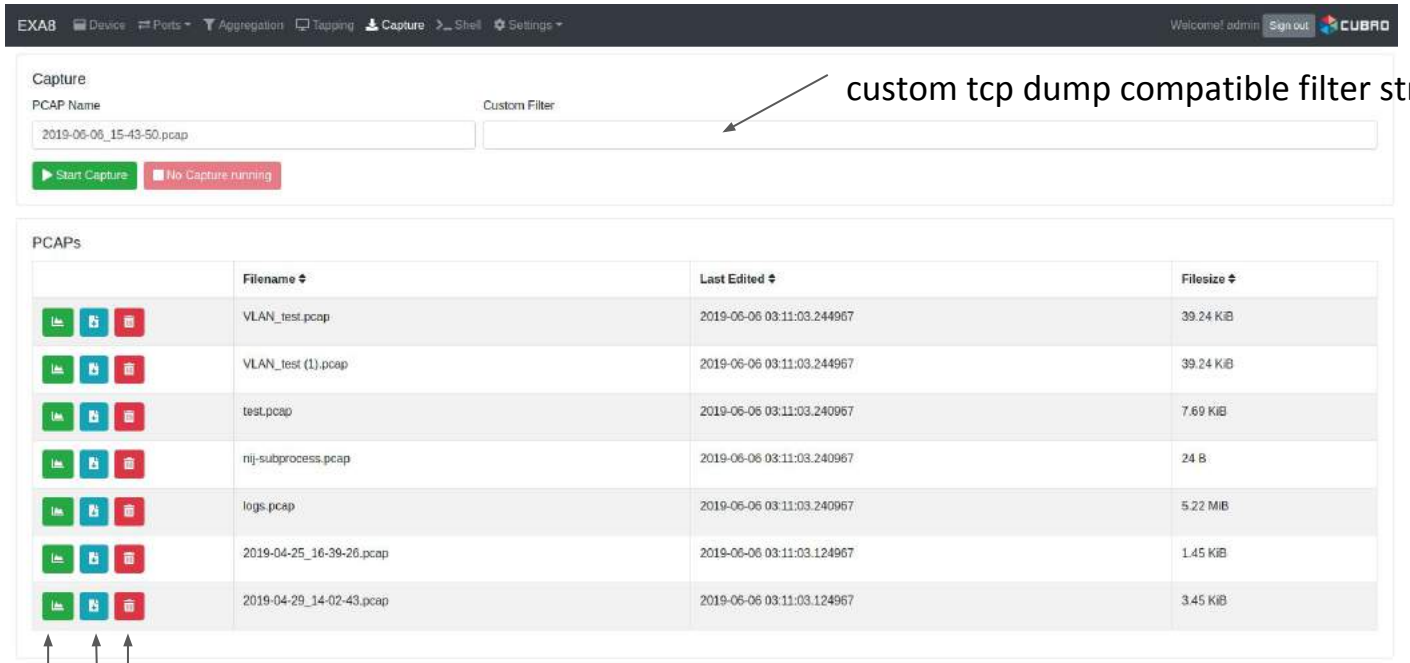
CUBRO NETWORK VISIBILITY
SIMPLE | SCALABLE | SUSTAINABLE

聚合&捕获到SSD



CUBRO
NETWORK VISIBILITY
SIMPLE | SCALABLE | SUSTAINABLE

捕获GUI



custom tcp dump compatible filter string

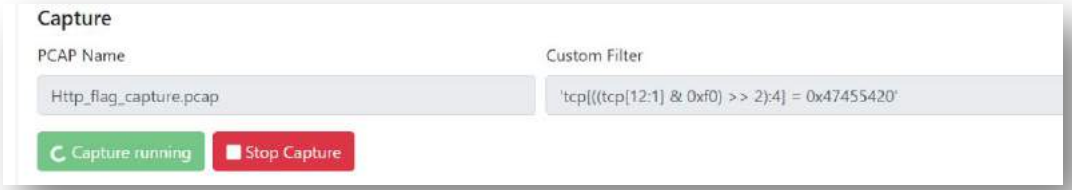
删除捕获文件

下载捕获文件

启动Webshark（分析捕获文件）

CUBRO NETWORK VISIBILITY
SIMPLE | SCALABLE | SUSTAINABLE

自定义过滤器示例



这些过滤器减少捕获的流量以节省磁盘空间。

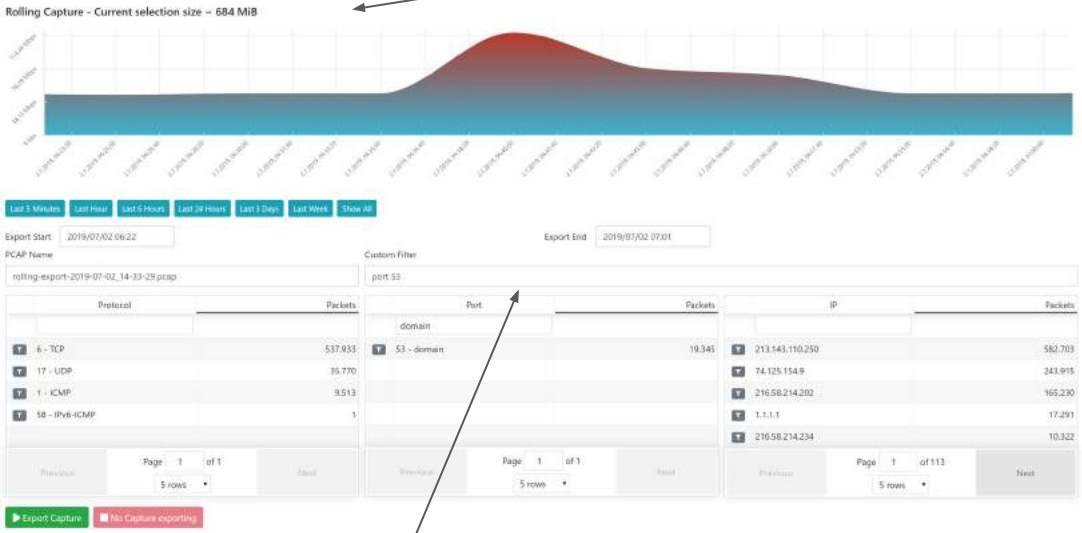
CUBRO
NETWORK VISIBILITY
SIMPLE | SCALABLE | SUSTAINABLE

滚动捕获&索引

滚动捕获24/7运行，用户可以按时间或IP索引提取捕获文件，并将其转换为PCAP以供以后分析。在导出过程中，还可以通过tcpdump选择post过滤。

CUBRO NETWORK VISIBILITY
SIMPLE | SCALABLE | SUSTAINABLE

滚动捕获&索引



在此示例中，我们希望仅从此时间范围提取DNS流量

滚动捕获&索引

滚动捕获是EXA8不断从配置的端口或链路捕获流量的功能。如果保留的磁盘空间已满，滚动捕获将自动覆盖较旧的捕获。

滚动捕获还会生成捕获流量的索引(时间、IP地址和端口信息)。借助该索引，可以提取相关流量并将其导出到PCAP文件中以供分析。

此功能提供了回顾时间并查找过去事件的选项。

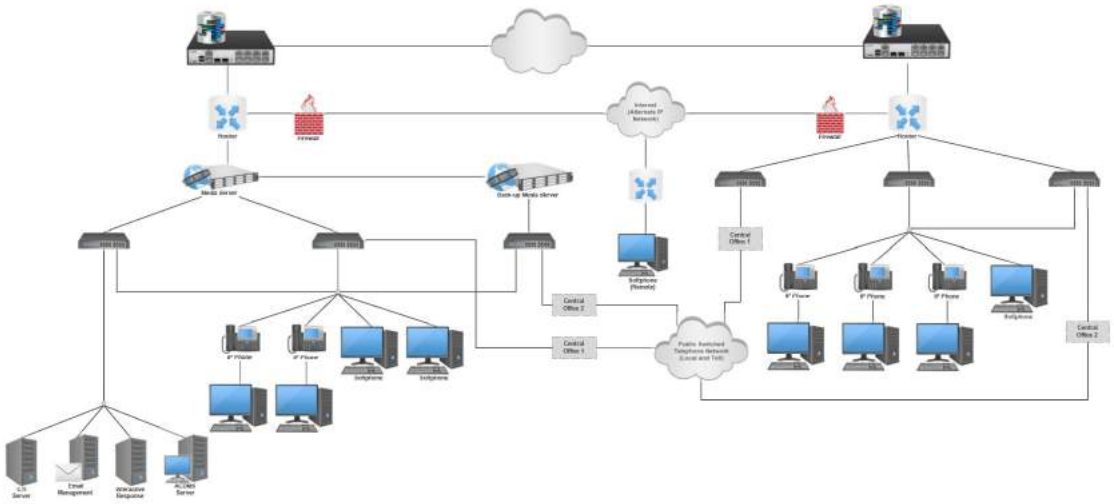
CUBRO NETWORK VISIBILITY
SIMPLE | SCALABLE | SUSTAINABLE

滚动捕获&索引应用案例

网络故障排除通常没有那么容易，因为问题只是偶尔出现。在这种情况下，标准捕获将无济于事。

Cubro 滚动捕获可以快速解决问题，因为采集是连续运行的，当发生错误时，工程师可以通过采集文件及时回溯。在查询语言的帮助下，您可以提取正确的时间范围以及按IP地址和端口过滤的相关流量。

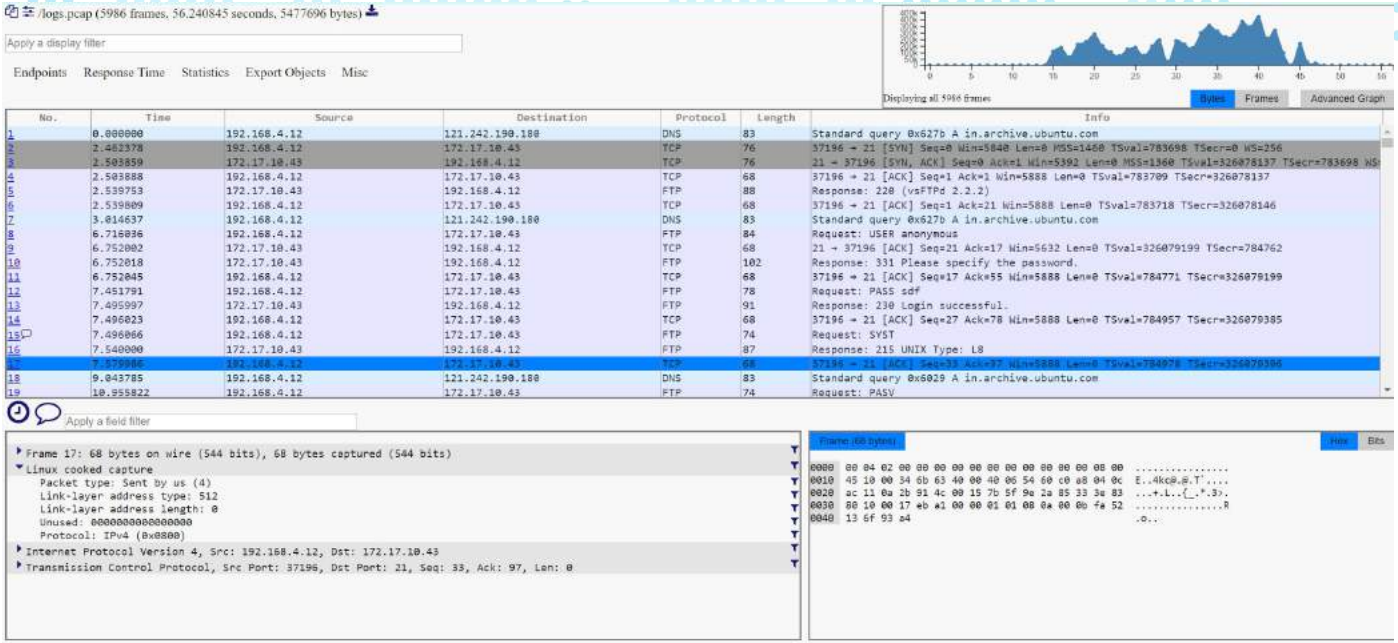
与分路器TAP和远程访问相结合，EXA8是完美的远程站点故障排除工具。



在本例中，在两个WAN接口上使用滚动捕获，以查看错误事件发生时WAN的行为。

CUBRO NETWORK VISIBILITY
SIMPLE | SCALABLE | SUSTAINABLE

Webshark GUI

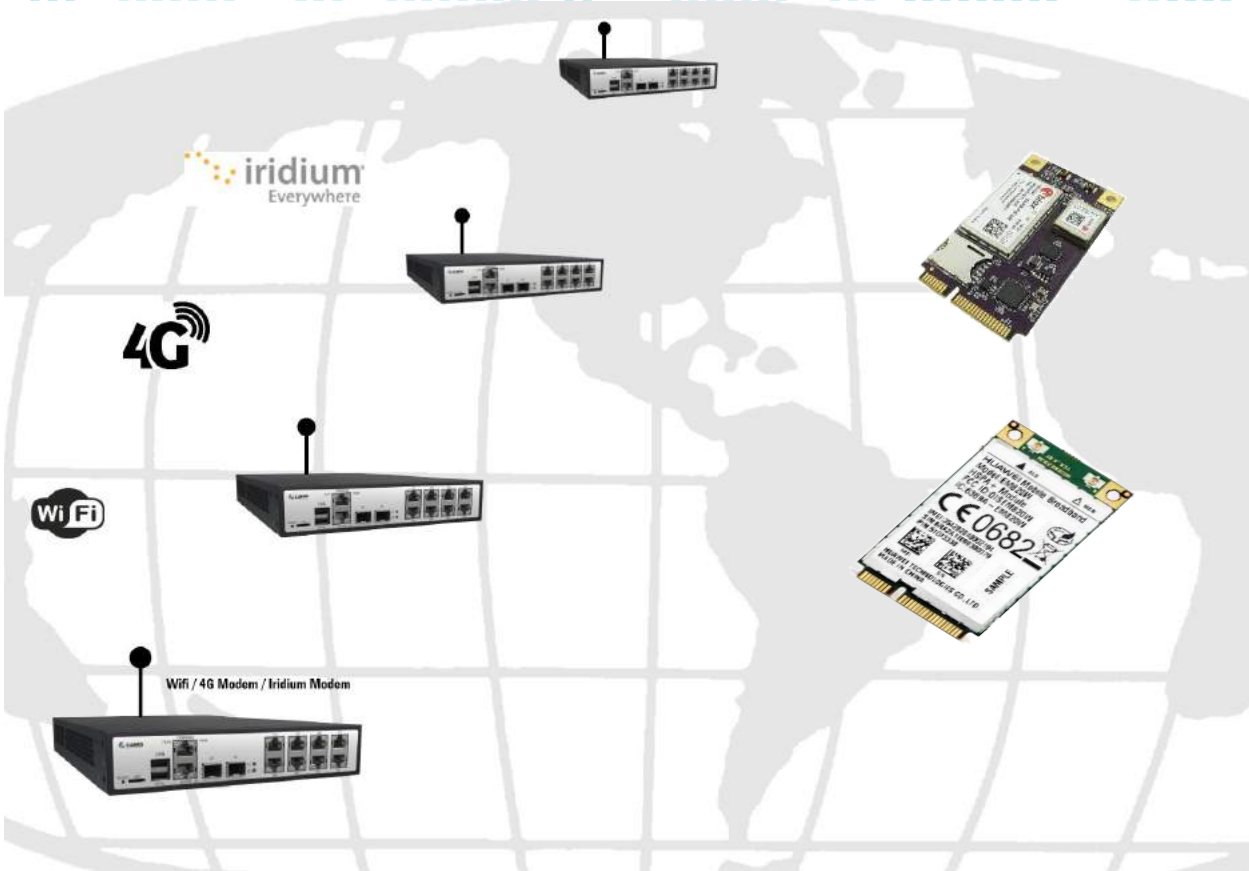


可以通过按Web GUI上的绿色按钮直接在exa8上打开捕获的pcap文件，而无需下载该文件。这提供了仅使用exa8进行远程故障排除的选项。

WebShark提供与知名Wireshark类似的功能集。

CUBRO NETWORK VISIBILITY
SIMPLE | SCALABLE | SUSTAINABLE

远程捕获



凭借可选的内置Wifi/2G/3G/4G调制解调器或铱卫星调制解调器，EXA8是一个多功能监控平台，可连接地球上各个地点的各种无线技术。

EXA8支持PCIe连接器扩展插槽以及外壳中的天线孔。

一个盒子就能完成所有任务-多个接口上的网络连接，功能强大的多核CPU，高性能SSD存储，以及支持远程连接的调制解调器。

强大的CPU使用户可以选择在远程站点运行分析软件，从而无需通过慢速连接链路下载捕获文件。

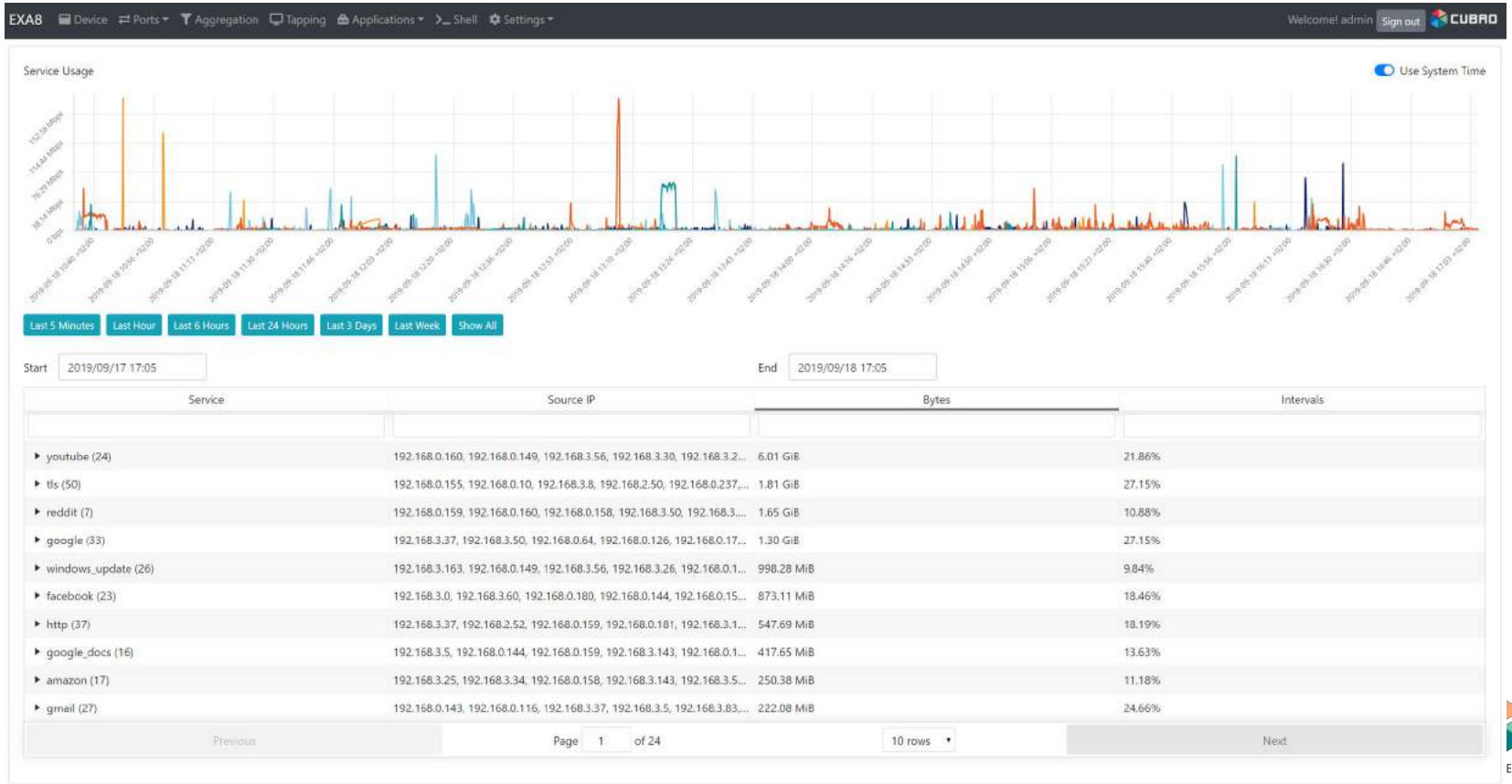
CUBRO
NETWORK VISIBILITY
SIMPLE | SCALABLE | SUSTAINABLE

EXA8上的流分析

EXA8提供功能齐全的流分析（NTopng）。

该软件对连接到EXA8的流量进行全面在线监控。

DPI应用检测“ 2000+”



CUBRO
NETWORK VISIBILITY
E | SCALABLE | SUSTAINABLE

DPI应用程序检测“ 2000+”

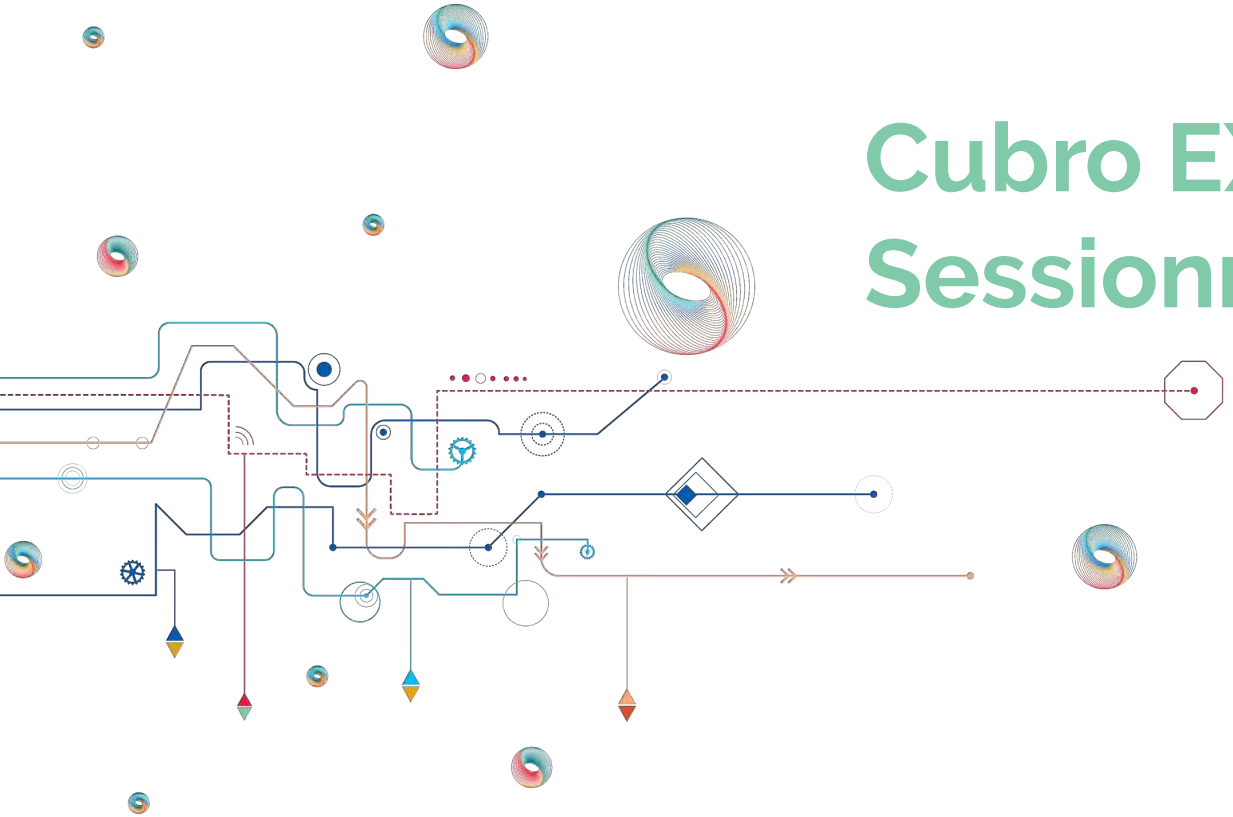
DPI“ 应用程序检测” 之所以重要，有两个原因：

查看**网络上发生了什么**，在用户和应用程序使用方面，以防止滥用公司网络。“ 我们不关注内容，只产生元数据” 。

DPI非常有用的第二个原因是有可能**减少必须通过删除已知应用程序进行分析的流量**。要发现攻击，必须对流量进行取证分析，但是由于流量太大，这通常很麻烦。DPI现在可以通过否定过滤帮助分类保存的流量。 我们可以使用DPI索引从捕获中删除所有“ 已知好的” 流量。

其余流量必须包含攻击的证据。通常情况下，我们预计不会有来自YouTube/Netflix/Facebook服务器的攻击，这很容易代表95%的流量。

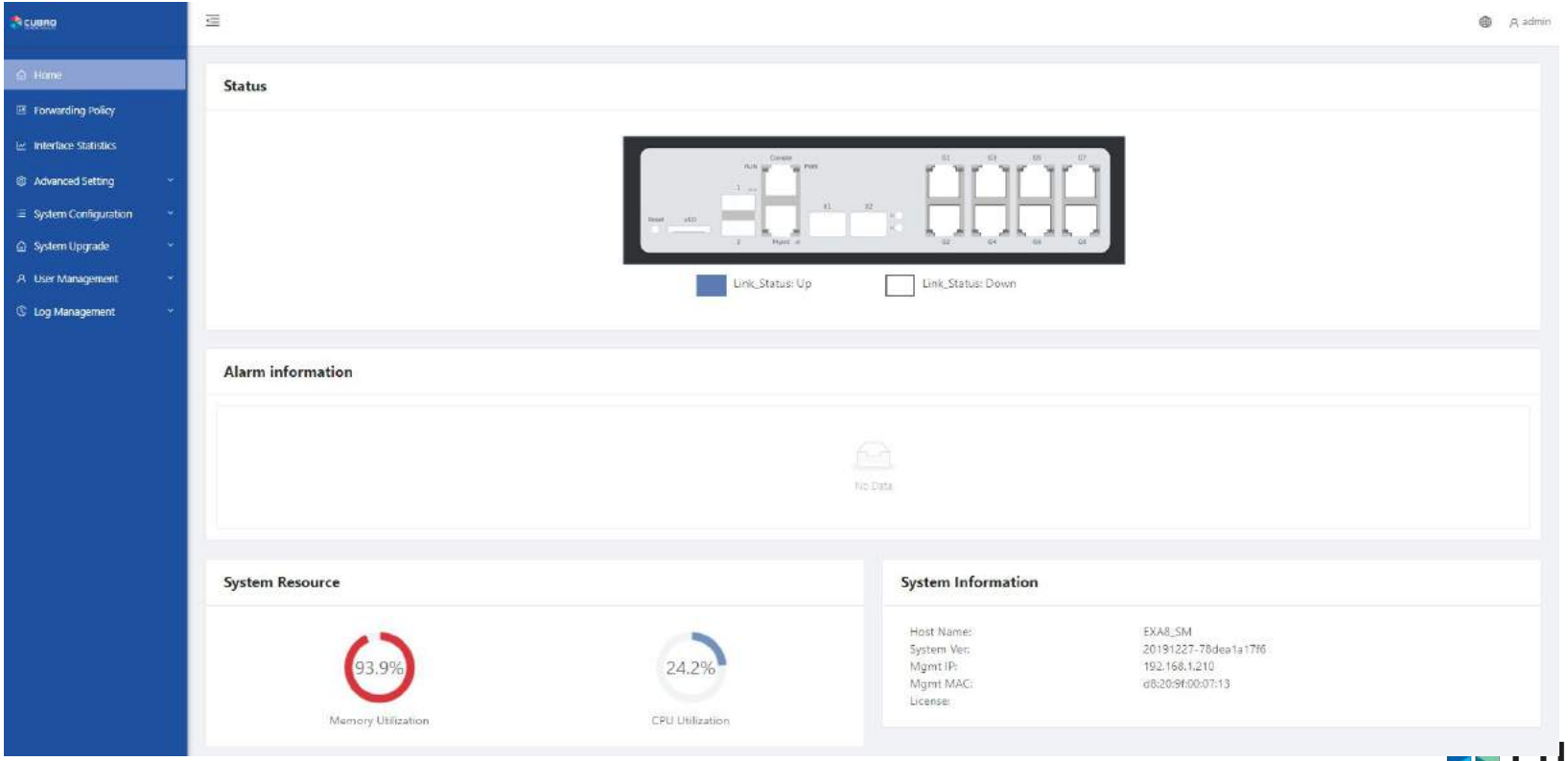
此功能将必须分析的流量减少了90%以上，并**减少了事件响应所需的时间和成本。**



Cubro EXA8 Sessionmaster

CUBRO
NETWORK VISIBILITY
SIMPLE | SCALABLE | SUSTAINABLE

直观的Web GUI



CJBRO NETWORK VISIBILITY
SIMPLE | SCALABLE | SUSTAINABLE

EXA8作为传统网络数据包代理

与Capture Appliance软件相比，Sessionmaster EXA8更像是一个众所周知的网络数据包代理，并与其他Cubro Packetmaster和Sessonmaster系列相结合。

功能列表概述：

- 基于L2 - L4的过滤
- 内部IP过滤/负载均衡
- NetFow探针
- 隧道封装/解封装
- 多到多&多到一聚合
- DPI过滤

CUBRO NETWORK VISIBILITY
SIMPLE | SCALABLE | SUSTAINABLE

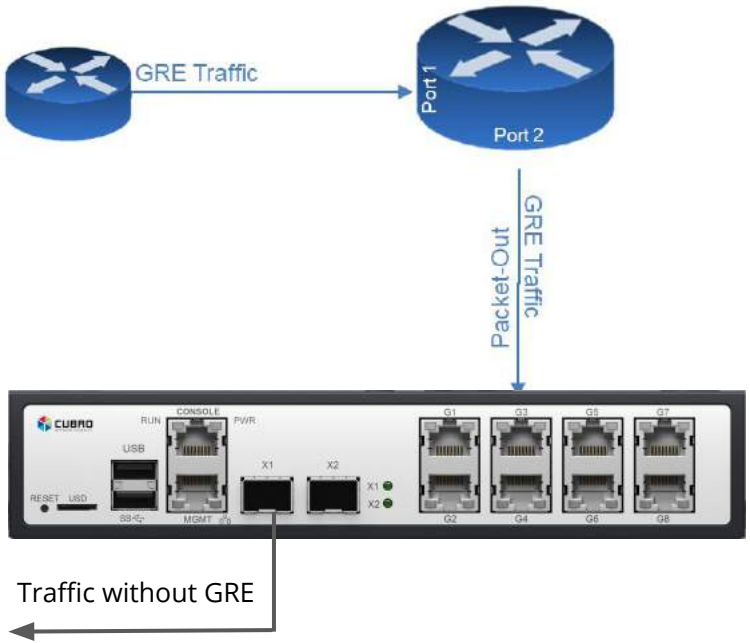
EXA8作为隧道端点

EXA8支持解封装许多不同类型的隧道封装。

这允许监控来自任何虚拟设备的流量。

支持的隧道协议：

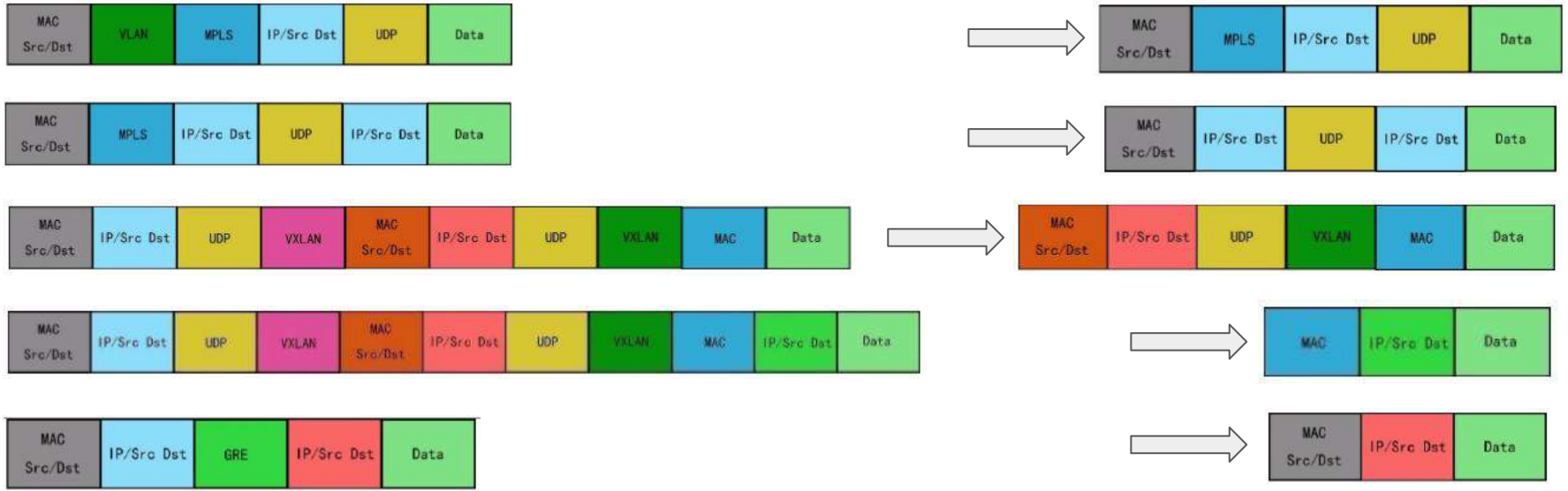
- GRE
- VXLAN
- MPLS
- ERSPAN



CUBRO NETWORK VISIBILITY
SIMPLE | SCALABLE | SUSTAINABLE

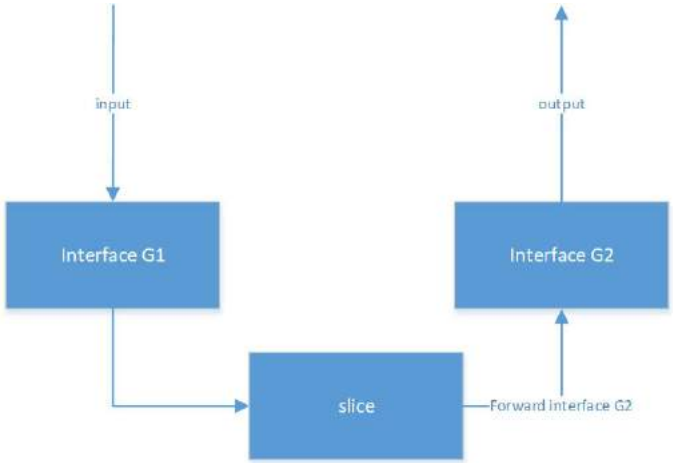
隧道报头删除

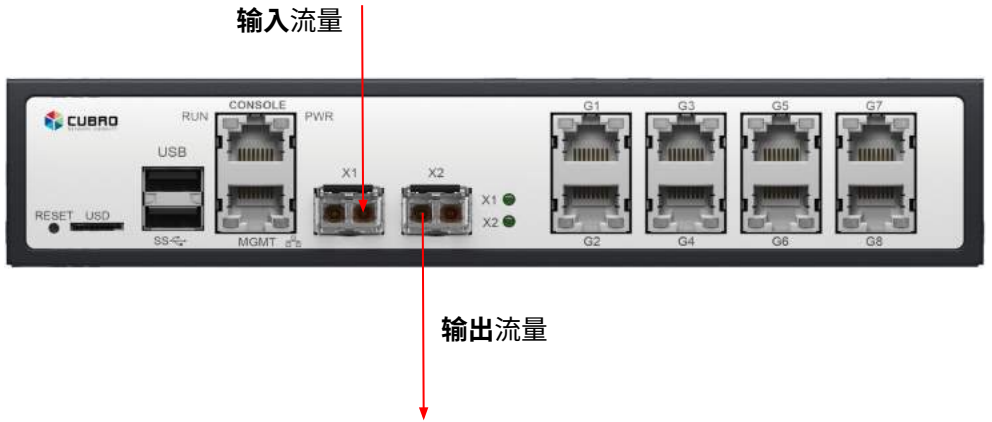
报头删除不限于单个报头，可以一次删除多个报头。



数据包切片和数据脱敏(Data Masking)

Cubro EXA8 Sessionmaster支持对流量的有效负载进行分片或脱敏，范围在40到1550字节之间。可以重新计算CRC。

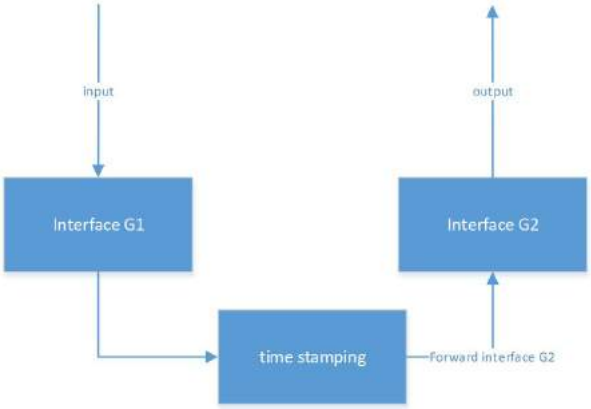


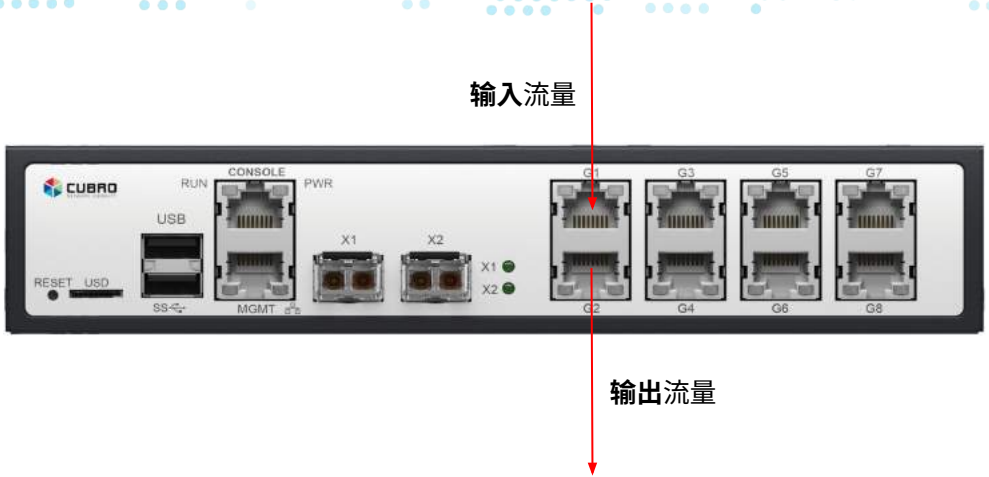


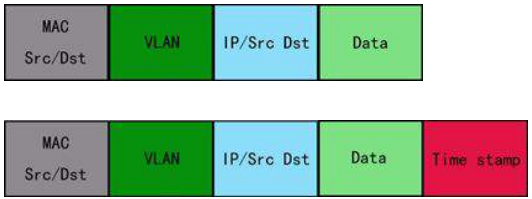
CUBRO NETWORK VISIBILITY
SIMPLE | SCALABLE | SUSTAINABLE

时间戳

启用此功能后，输出数据包帧将带有时间戳，分辨率在20-200 ns之间。

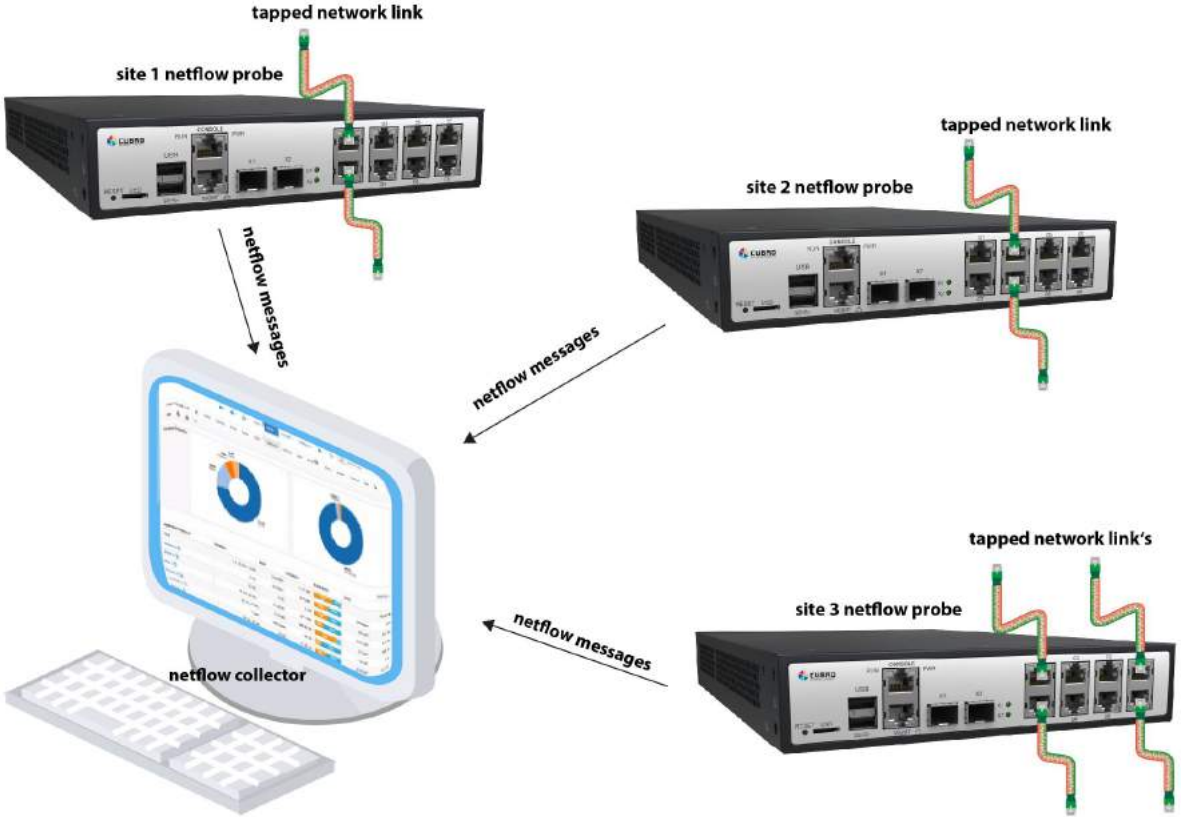






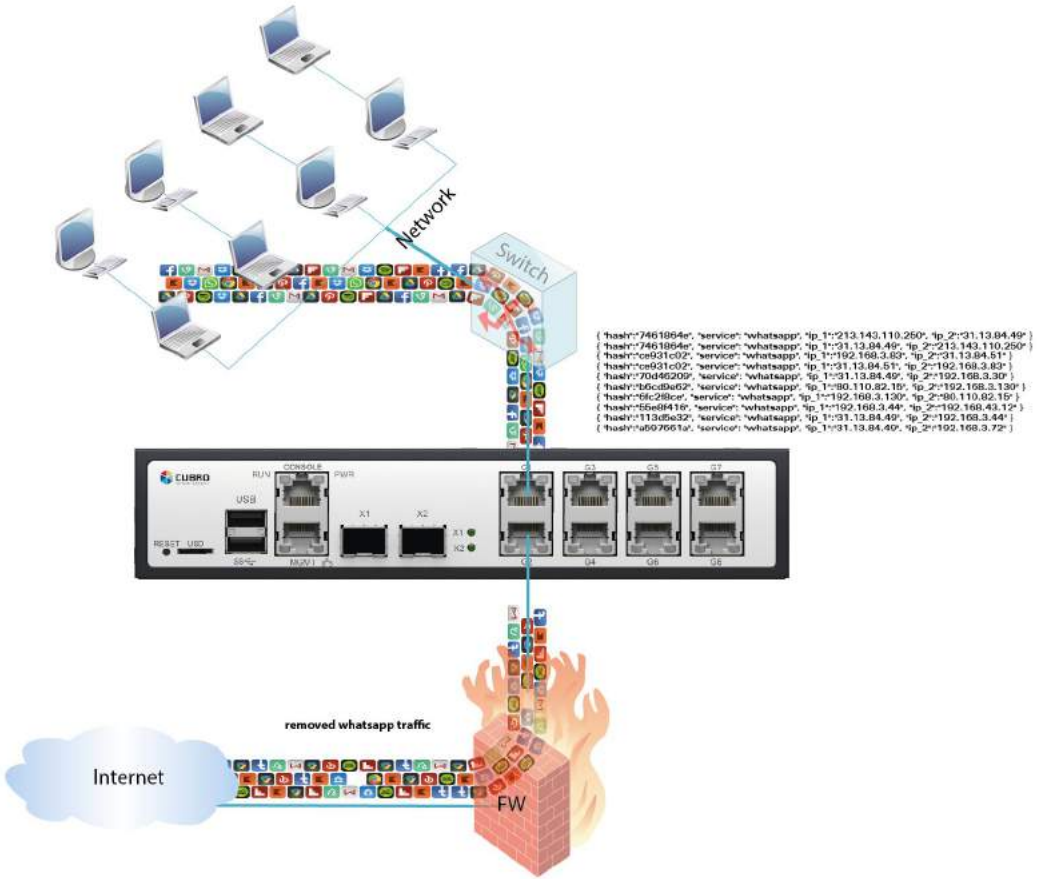
CUBRO NETWORK VISIBILITY
SIMPLE | SCALABLE | SUSTAINABLE

EXA8作为NetFow探针



CUBRO
NETWORK VISIBILITY
SIMPLE | SCALABLE | SUSTAINABLE

Roadmap: EXA8上的DPI过滤



EXA8可用于在应用程序级别阻止内联任何类型的流量，如该示例的WhatApp。

Cubro当前支持多达2000个签名和应用程序。

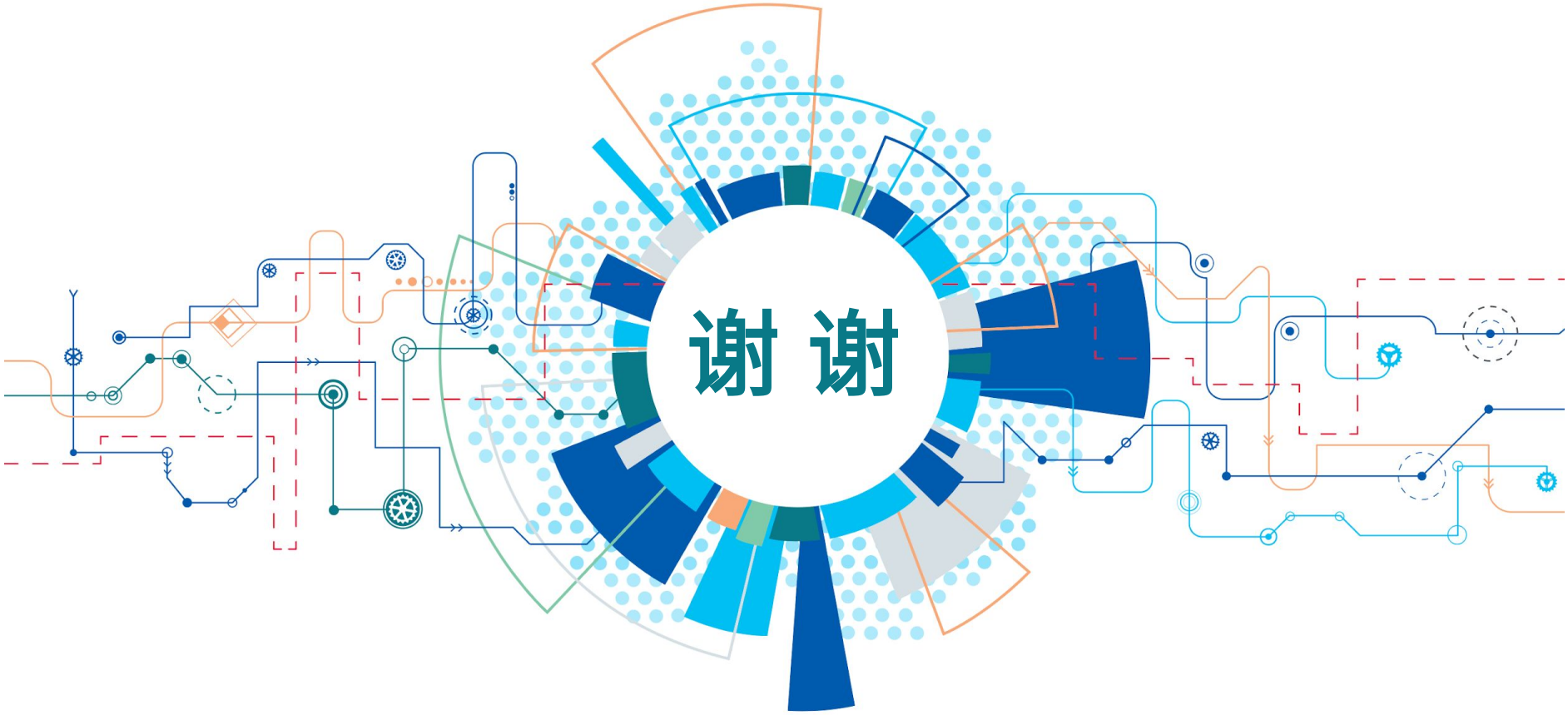
CUBRO
NETWORK VISIBILITY
SIMPLE | SCALABLE | SUSTAINABLE

质量&环境管理

Cubro已通过ISO 9001质量管理认证，以确保提供最佳的产品和服务

Cubro已通过ISO 14001认证，以管理我们保护环境的努力。

CUBRO
NETWORK VISIBILITY
SIMPLE | SCALABLE | SUSTAINABLE



HongKe 虹科

关注我们

hongwangle

广州虹科电子科技有限公司

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