

# EXA8 应用

February 2020



# EXA8 - “多合一工具”

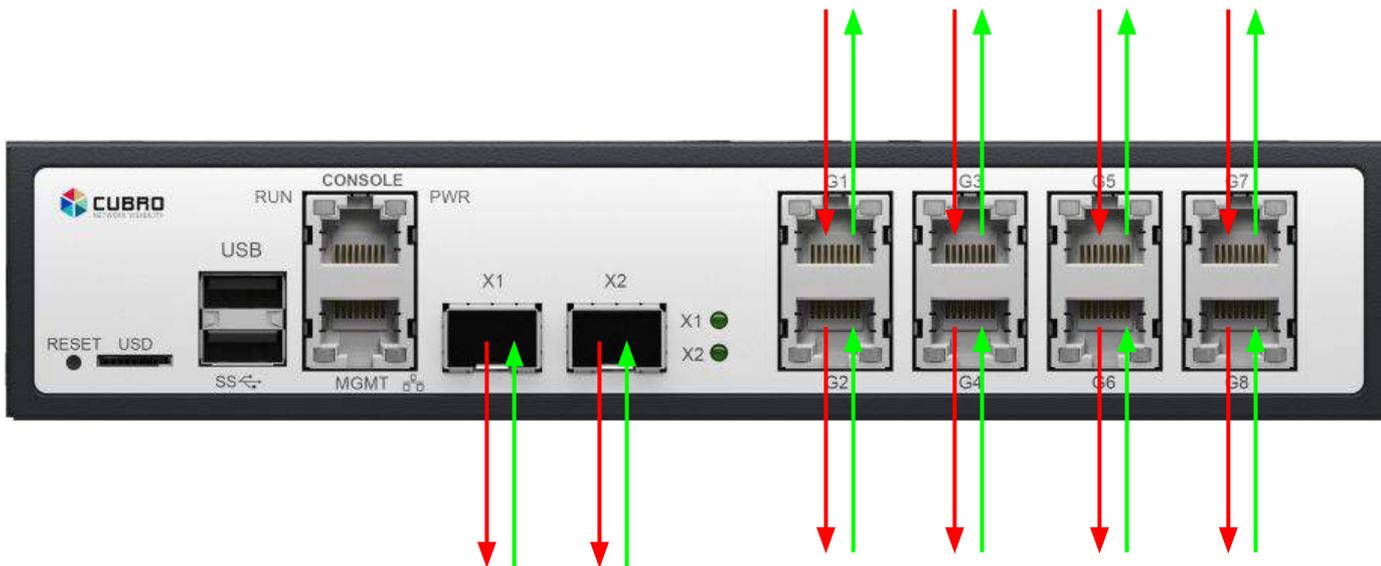


EXA8是一款紧凑型的多应用设备，可以用于实时聚合、过滤和捕获网络流量。

- 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+



# 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)

# 多重功能在1个盒子里

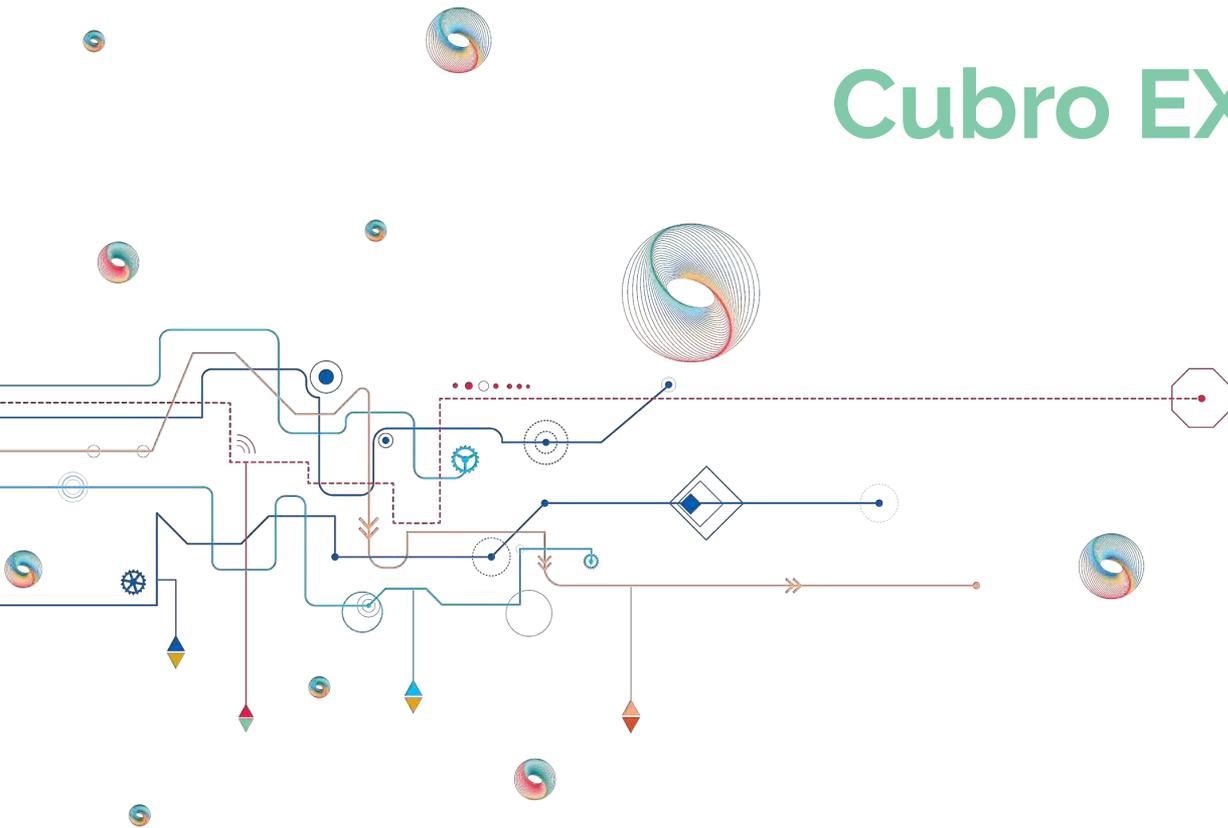


EXA8平台目前提供3个不同的软件版本：

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。



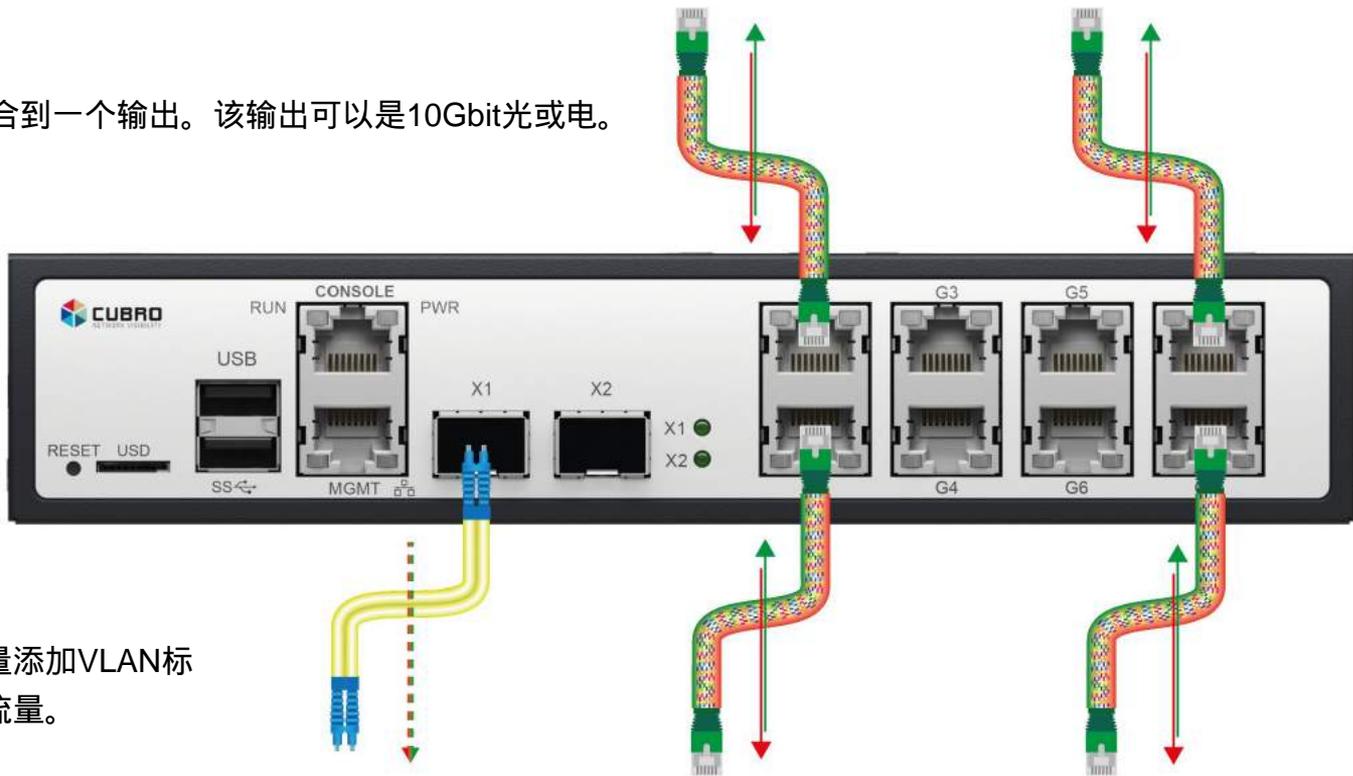
# Cubro EXA8聚合



# 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。

# 直观的Web GUI



EXA8 [Device](#) [Ports](#) [Aggregation](#) [Tapping](#) [Settings](#)

Welcome! admin

[Sign out](#)



## Device Information

Device Model EXA8  
Image Version 1.3.1-4.0  
Revision a9d3236  
Serialnumber 124B-1960015  
Custom Device Label

[Save](#)

## Device Image



## Device Configuration

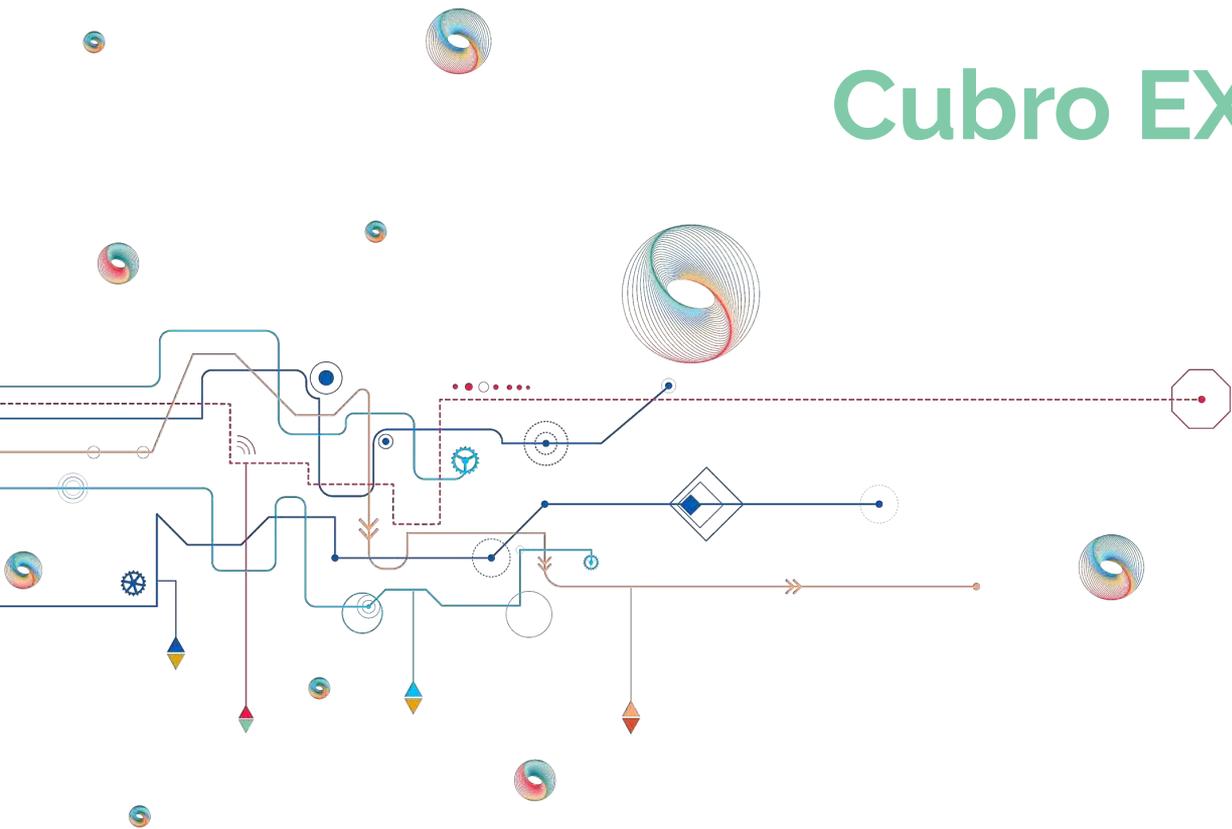
[Save configuration](#)

[Restore configuration](#)

[Reset configuration](#)



# Cubro EXA8捕获探针



# EXA8 - 捕获探针



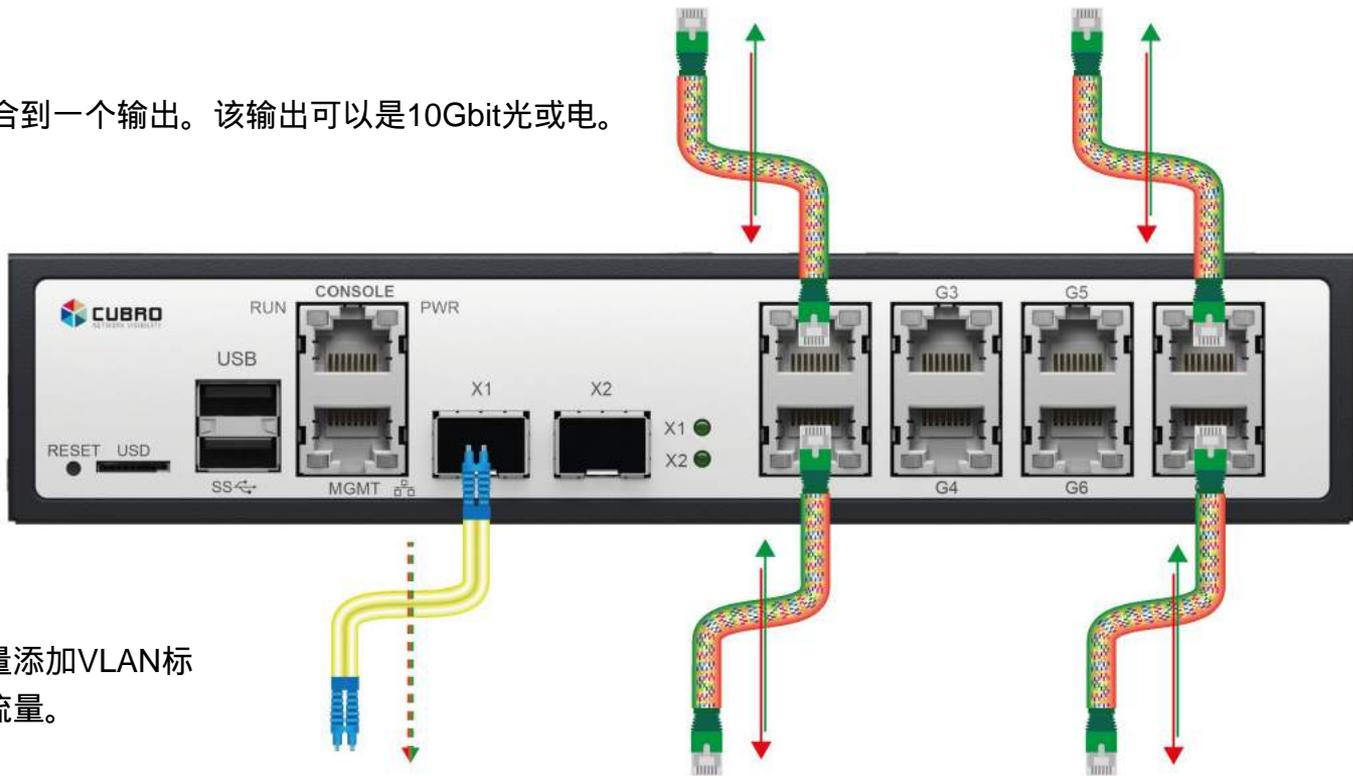
- 100%捕获所有数据以进行实时分析和历史回放-非常适合故障排除
- 捕获到USB或SSD
- 能够执行其他几个高级应用程序，如Sessionmaster
- 能够运行第三方应用程序
- 滚动捕获“回看时间捕获”



# 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。

# 直观的Web GUI



EXA8 [Device](#) [Ports](#) [Aggregation](#) [Tapping](#) [Applications](#) [Shell](#) [Settings](#)

Welcome! admin

[Sign out](#)



## Device Information

Device Model EXA8  
Image Version 1.3.1-4.0  
Revision a9d3236  
Serialnumber 124B-1960015  
Custom Device Label

[Save](#)

## Device Image



## Device Configuration

[Save configuration](#)

[Restore configuration](#)

[Reset configuration](#)

## System Information

Booted from: SD-Card

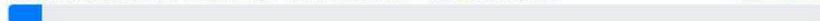
CPU - 53.85% - Temperature 48°C



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

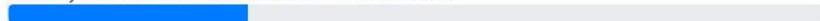


Disk /mnt/data free 743.29 GiB - used 33.45 GiB - total 818.33 GiB

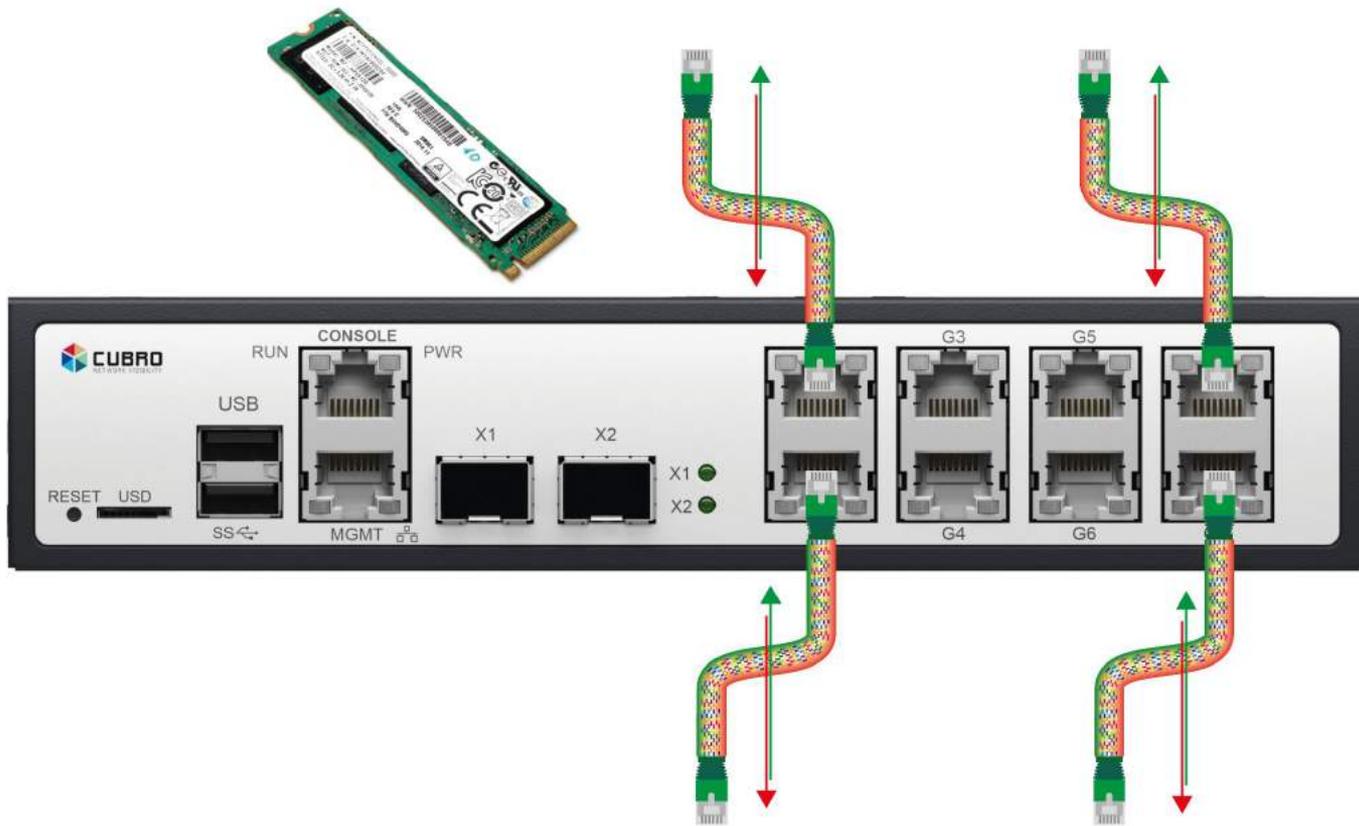


SMART OK

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



# 聚合&捕获到SSD



# 捕获GUI



## Capture

PCAP Name

Custom Filter

2019-06-06\_15-43-50.pcap

custom tcp dump compatible filter string

Start Capture

No Capture running

## PCAPs

	Filename	Last Edited	Filesize
  	VLAN_test.pcap	2019-05-06 03:11:03.244967	39.24 KiB
  	VLAN_test (1).pcap	2019-05-06 03:11:03.244967	39.24 KiB
  	test.pcap	2019-05-06 03:11:03.240967	7.69 KiB
  	nij-subprocess.pcap	2019-05-06 03:11:03.240967	24 B
  	logs.pcap	2019-05-06 03:11:03.240967	5.22 MiB
  	2019-04-25_16-39-26.pcap	2019-05-06 03:11:03.124967	1.45 KiB
  	2019-04-29_14-02-43.pcap	2019-05-06 03:11:03.124967	3.45 KiB

删除捕获文件

下载捕获文件

启动Webshark (分析捕获文件)

# 自定义过滤器示例



**Capture**

PCAP Name:  Custom Filter:

Capture running  Stop Capture

**Capture**

PCAP Name:  Custom Filter:

Capture running  Stop Capture

**Capture**

PCAP Name:  Custom Filter:

Capture running  Stop Capture

这些过滤器减少捕获的流量以节省磁盘空间。

# 滚动捕获&索引



捕获的流量大小

以图形方式选择要导出的请求数据包的存储窗口

tcpdump导出捕获过滤器

导出捕获文件

捕获流量的索引信息

Rolling Capture - Current selection size -- 469.05 GiB

Last 5 Minutes Last Hour Last 6 Hours Last 24 Hours Last 3 Days Last Week Show All

Export Start 2019/07/01 09:56 Export End 2019/07/02 18:09

PCAP Name: rolling-export-2019-07-02\_14:23-23.pcap Custom Filter: tcpdump导出捕获过滤器

Protocol	Packets	Port	Packets	IP	Packets
6 - TCP	433,527,154	443 - https	430,473,967	213.143.110.250	438,368,412
17 - UDP	4,637,108	80 - http	5,276,430	172.217.19.106	110,990,057
1 - ICMP	219,167	7833	1,452,372	172.217.16.106	62,260,014
58 - IPv6-ICMP	59	15251	1,336,172	172.217.20.10	61,891,981
		993 - imaps	826,079	172.217.18.74	60,750,824

Export Capture No Capture exporting

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。

# 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。



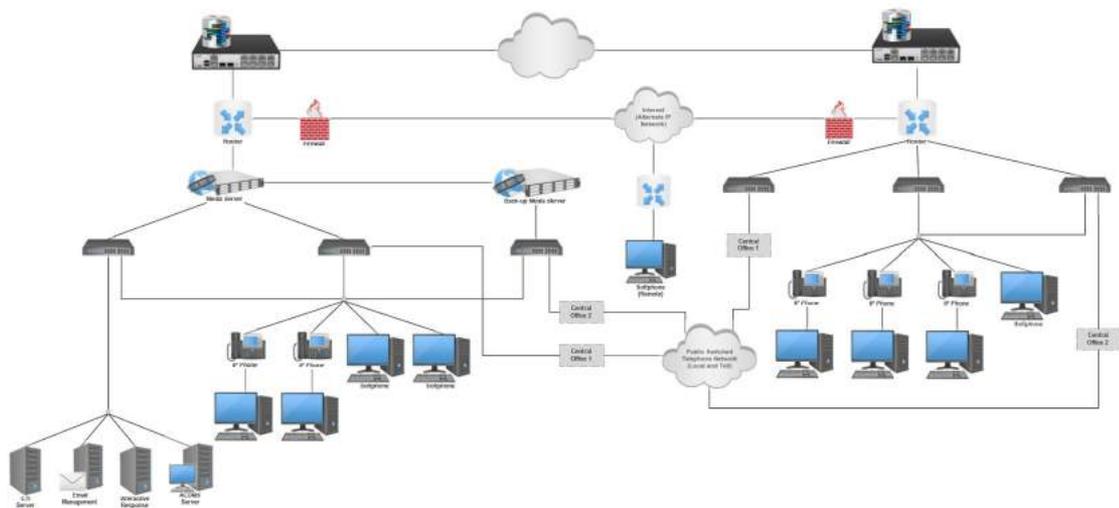
# 滚动捕获&索引应用案例



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。

# Webshark GUI



📁 /logs.pcap (5986 frames, 56.240845 seconds, 5477696 bytes) 🗑

Apply a display filter

Endpoints Response Time Statistics Export Objects Misc



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.4.12	121.242.190.188	DNS	83	Standard query 0x627b A in.archive.ubuntu.com
2	2.482378	192.168.4.12	172.17.10.43	TCP	76	37196 → 21 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 TSval=783698 TSecr=0 WS=256
3	2.503859	172.17.10.43	192.168.4.12	TCP	76	21 → 37196 [SYN, ACK] Seq=0 Ack=1 Win=5392 Len=0 MSS=1360 TSval=526078137 TSecr=783698 WS=
4	2.508753	192.168.4.12	192.168.4.12	FTP	88	Response: 230 (vsFTPd 2.1.2)
5	2.538809	192.168.4.12	172.17.10.43	TCP	68	37196 → 21 [ACK] Seq=1 Ack=21 Win=5888 Len=0 TSval=783718 TSecr=326078137
7	3.014637	192.168.4.12	121.242.190.188	DNS	83	Standard query 0x627b A in.archive.ubuntu.com
8	6.718036	192.168.4.12	172.17.10.43	FTP	84	Request: USER anonymous
9	6.752002	172.17.10.43	192.168.4.12	TCP	68	21 → 37196 [ACK] Seq=21 Ack=17 Win=5632 Len=0 TSval=326079199 TSecr=784762
10	6.752018	172.17.10.43	192.168.4.12	FTP	102	Response: 331 Please specify the password.
11	6.752045	192.168.4.12	172.17.10.43	TCP	68	37196 → 21 [ACK] Seq=17 Ack=55 Win=5888 Len=0 TSval=784771 TSecr=326079199
12	7.451791	192.168.4.12	172.17.10.43	FTP	78	Request: PASS sdf
13	7.495997	172.17.10.43	192.168.4.12	FTP	91	Response: 230 Login successful.
14	7.495923	192.168.4.12	172.17.10.43	TCP	68	37196 → 21 [ACK] Seq=27 Ack=78 Win=5888 Len=0 TSval=784957 TSecr=326079385
15	7.498866	192.168.4.12	172.17.10.43	FTP	74	Request: SYST
16	7.540000	172.17.10.43	192.168.4.12	FTP	87	Response: 215 UNIX Type: L8
17	7.579885	192.168.4.12	172.17.10.43	TCP	68	37196 → 21 [ACK] Seq=33 Ack=77 Win=5888 Len=0 TSval=784978 TSecr=326079386
18	9.043785	192.168.4.12	121.242.190.188	DNS	83	Standard query 0x69029 A in.archive.ubuntu.com
19	10.955822	192.168.4.12	172.17.10.43	FTP	74	Request: PASV

🔍 Apply a field filter

▶ Frame 17: 68 bytes on wire (544 bits), 68 bytes captured (544 bits) on eth0

▼ Linux cooked capture

- Packet type: Sent by us (4)
- Link-layer address type: 512
- Link-layer address Length: 0
- Unused: 0000000000000000
- Protocol: IPv4 (0x0800)

▶ Internet Protocol Version 4, Src: 192.168.4.12, Dst: 172.17.10.43

▶ Transmission Control Protocol, Src Port: 37196, Dst Port: 21, Seq: 33, Ack: 97, Len: 0

▶ Frame (68 bytes)

0000	00 04 02 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
0010	45 10 00 34 0b 03 40 00 40 06 54 00 c0 a8 04 0c	E..4kCP..T....
0020	cc 11 0a 2b 21 4c 00 15 70 5f 9a 1e 85 33 3a 83	...L...[...B.
0030	80 10 00 17 eb a1 00 00 01 01 08 0a 00 00 fa 52	.....R
0040	13 6f 93 a4	..o..

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。

VLAN\_test.pcap 39.24 KiB 2019-06-06 03:11:03.244967

WebShark提供与知名Wireshark类似的功能集。



# 远程捕获



iridium  
Everywhere

4G

WiFi

Wifi / 4G Modem / Iridium Modem

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。

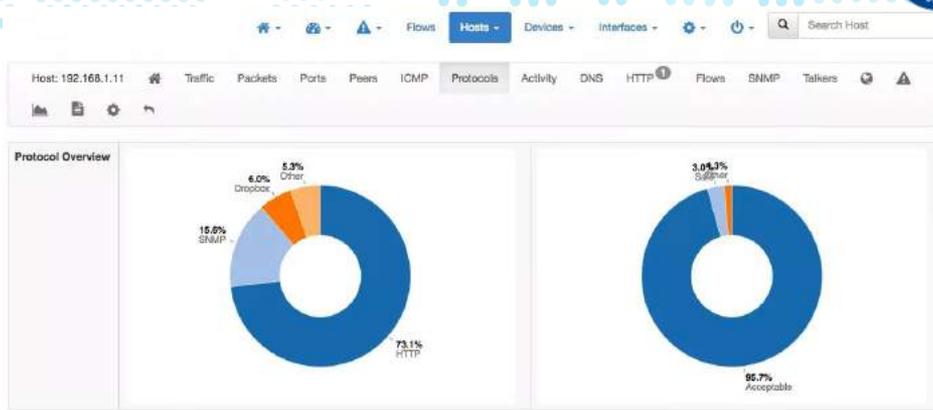
强大的CPU使用户可以选择在远程站点运行分析软件，从而无需通过慢速连接链路下载捕获文件。

# 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。



Application Protocol	Duration	Sent	Received	Breakdown	Total
Total	2 h, 10 min, 15 sec	31.02 MB	14.13 MB	<a href="#">Sent</a> <a href="#">Recv</a>	45.15 MB
Amazon	5 sec	66 Bytes	60 Bytes	<a href="#">Sent</a> <a href="#">Recv</a>	126 Bytes 0 %
DHCP	30 sec	2 KB	2 KB	<a href="#">Sent</a> <a href="#">Recv</a>	4.01 KB 0.01 %
DNS	10 min, 35 sec	27.32 KB	57.11 KB	<a href="#">Sent</a> <a href="#">Recv</a>	84.43 KB 0.16 %

Application	Protocol	Client	Server	Duration	Breakdown	Actual Thru	Total Bytes	Info
Unknown	UDP	193.89.244.42	193.89.244.42	01:28	Server	276.65 kbps	7.63 MB	
IMAPS Gmail	TCP	174.125.133.105	174.125.133.105	00:14	Server	36.84 kbps	132.37 KB	
WhatsApp	TCP	174.125.133.105	174.125.133.105	02:28	Client Server	11.36 kbps	52.04 KB	
SSL	TCP	193.89.244.42	193.89.244.42	10:12	Server	16.26 kbps	1.13 MB	
SSL Google	TCP	174.125.133.105	174.125.133.105	33:24	Client Server	7.07 kbps	360.02 KB	presence.googleapps.com
Google	UDP	174.125.133.105	174.125.133.105	01:15	Client Server	6.04 kbps	40.67 KB	
SSL WhatsApp	TCP	193.89.244.42	193.89.244.42	14:01	Client Server	4.64 kbps	125.9 KB	web.whatsapp.com
SSL Skype	TCP	174.125.133.105	174.125.133.105	01:31:49	Client Server	4.45 kbps	163.75 KB	skype-stun-a.gammasys.net
SSL Google	TCP	174.125.133.105	174.125.133.105	03:09	Client Server	4.13 kbps	25.2 KB	on.g.doubleclick.net
SSL Google	TCP	174.125.133.105	174.125.133.105	01:15	Client Server	3.26 kbps	206.2 KB	www.google.it

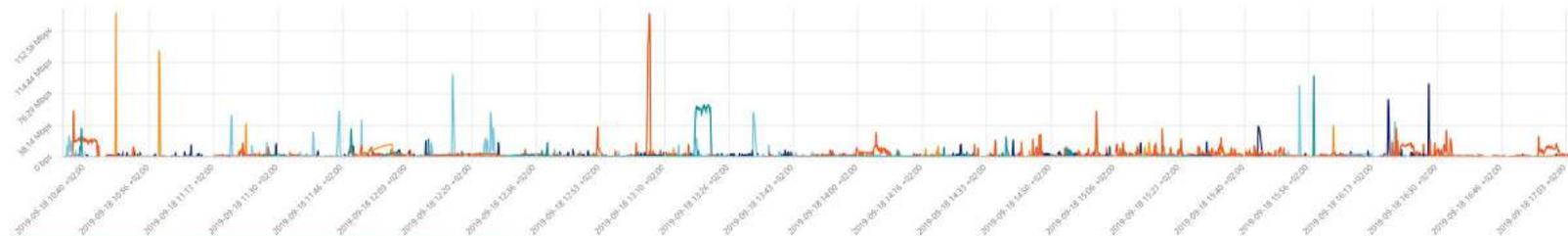
Showing 1 to 10 of 980 rows. The flows not listed.

# DPI应用检测“2000+”



## Service Usage

Use System Time



Last 5 Minutes Last Hour Last 6 Hours Last 24 Hours Last 3 Days Last Week Show All

Start 2019/09/17 17:05

End 2019/09/18 17:05

Service	Source IP	Bytes	Intervals
▶ youtube (24)	192.168.0.160, 192.168.0.149, 192.168.3.56, 192.168.3.30, 192.168.3.2...	6.01 GiB	21.86%
▶ tfs (50)	192.168.0.155, 192.168.0.10, 192.168.3.8, 192.168.2.50, 192.168.0.237,...	1.81 GiB	27.15%
▶ reddit (7)	192.168.0.159, 192.168.0.160, 192.168.0.158, 192.168.3.50, 192.168.3.1...	1.65 GiB	10.88%
▶ google (33)	192.168.3.37, 192.168.3.50, 192.168.0.64, 192.168.0.126, 192.168.0.17...	1.30 GiB	27.15%
▶ windows_update (26)	192.168.3.163, 192.168.0.149, 192.168.3.56, 192.168.3.26, 192.168.0.1...	998.28 MiB	9.84%
▶ facebook (23)	192.168.3.0, 192.168.3.60, 192.168.0.180, 192.168.0.144, 192.168.0.15...	873.11 MiB	18.46%
▶ http (37)	192.168.3.37, 192.168.2.52, 192.168.0.159, 192.168.0.181, 192.168.3.1...	547.69 MiB	18.19%
▶ google_docs (16)	192.168.3.5, 192.168.0.144, 192.168.0.159, 192.168.3.143, 192.168.0.1...	417.65 MiB	13.63%
▶ amazon (17)	192.168.3.25, 192.168.3.34, 192.168.0.158, 192.168.3.143, 192.168.3.5...	250.38 MiB	11.18%
▶ gmail (27)	192.168.0.143, 192.168.0.116, 192.168.3.37, 192.168.3.5, 192.168.3.83...	222.08 MiB	24.66%

Previous

Page 1 of 24

10 rows

Next

# 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：

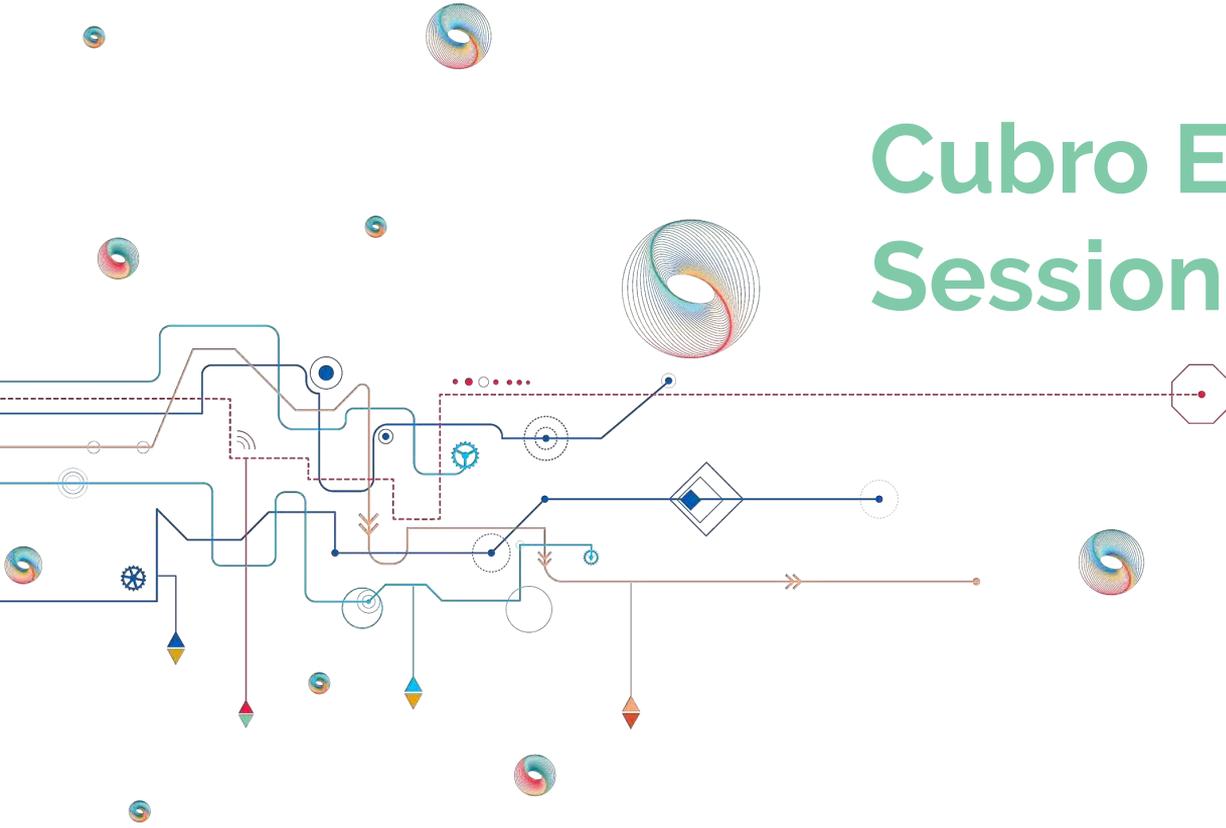
查看网络上发生了什么，在用户和应用程序使用方面，以防止滥用公司网络。“我们不关注内容，只产生元数据”。

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



# 直观的Web GUI



The screenshot displays the CUBRO web GUI interface. On the left is a dark blue sidebar with navigation options: Home, Forwarding Policy, Interface Statistics, Advanced Setting, System Configuration, System Upgrade, User Management, and Log Management. The main content area is divided into several sections:

- Status:** Features a network topology diagram with various ports (e.g., S1, S2, S3, S4, S5, S6, S7, S8, S9, S10) and a legend for Link\_Status: Up (blue square) and Link\_Status: Down (white square).
- Alarm information:** Currently shows "No Data" with a server icon.
- System Resource:** Contains two circular progress indicators: Memory Utilization at 93.9% and CPU Utilization at 24.2%.
- System Information:** Lists system details:

Host Name:	EXA8_SM
System Ver:	20191227-78dea1a17f6
Mgmt IP:	192.168.1.210
Mgmt MAC:	08:20:9f:00:07:13
License:	

# 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Sessionmaster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



# EXA8作为隧道端点

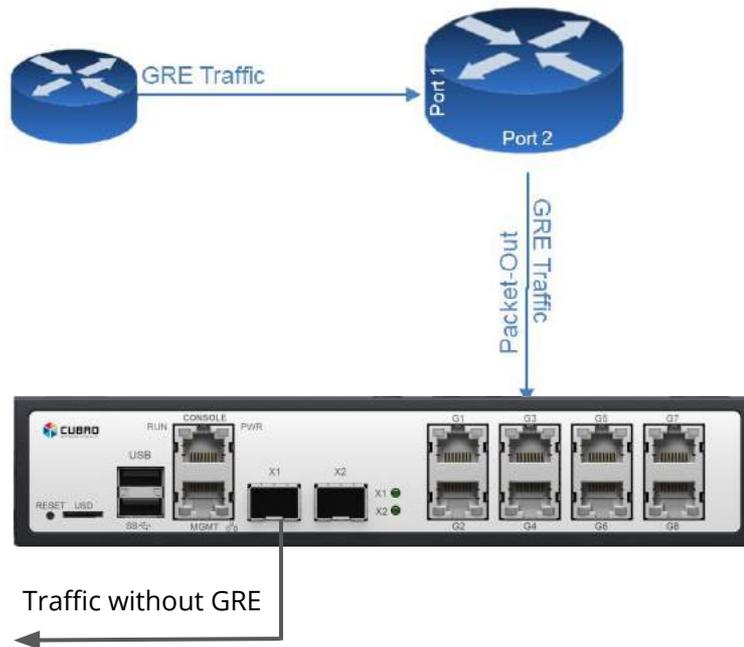


EXA8支持解封装许多不同类型的隧道封装。

这允许监控来自任何虚拟设备的流量。

支持的隧道协议：

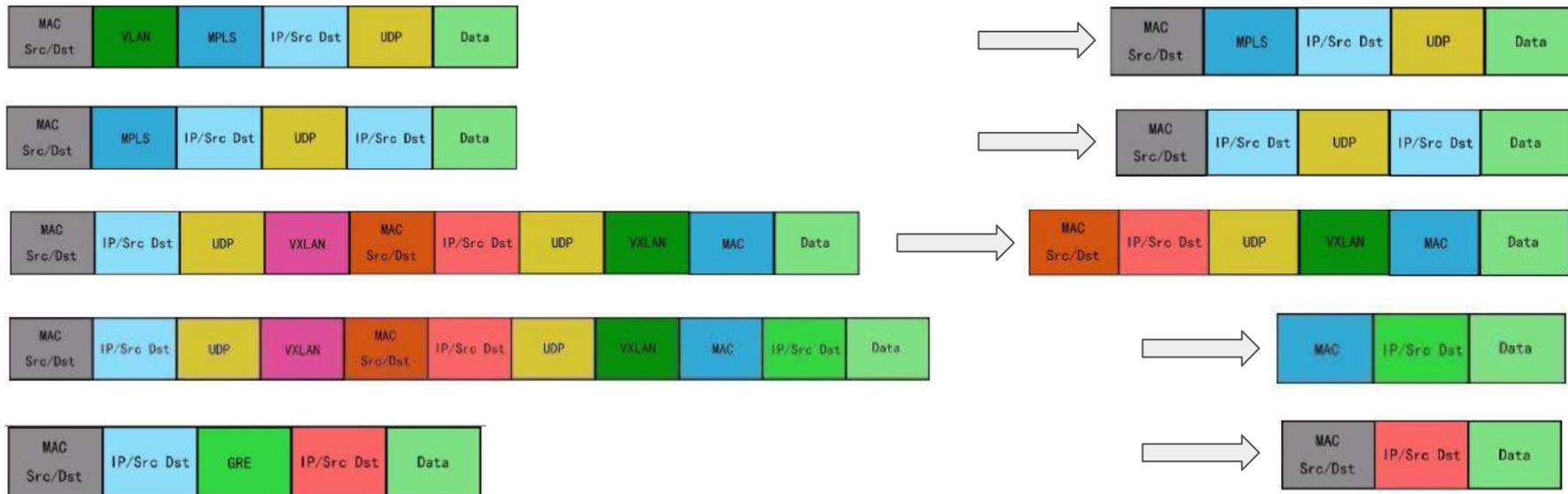
- GRE
- VXLAN
- MPLS
- ERSPAN



# 隧道报头删除



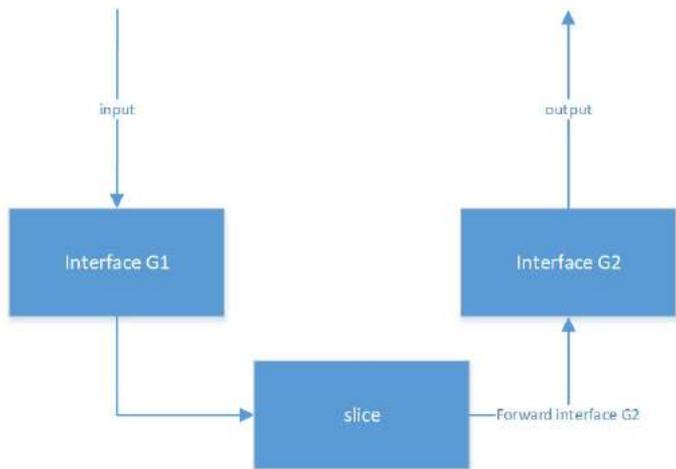
报头删除不限于单个报头，可以一次删除多个报头。



# 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。



# 时间戳

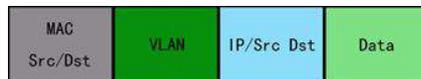
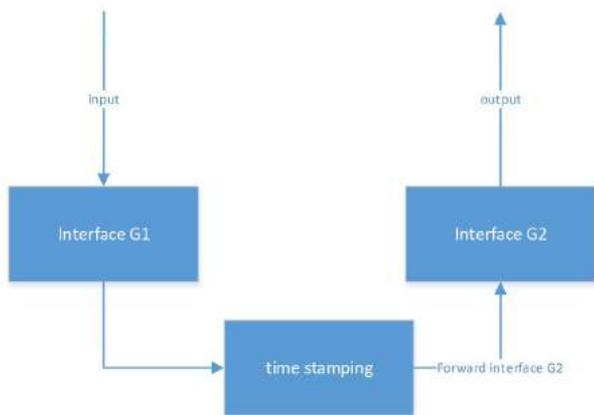


启用此功能后，输出数据包帧将带有时间戳，分辨率在20-200 ns之间。

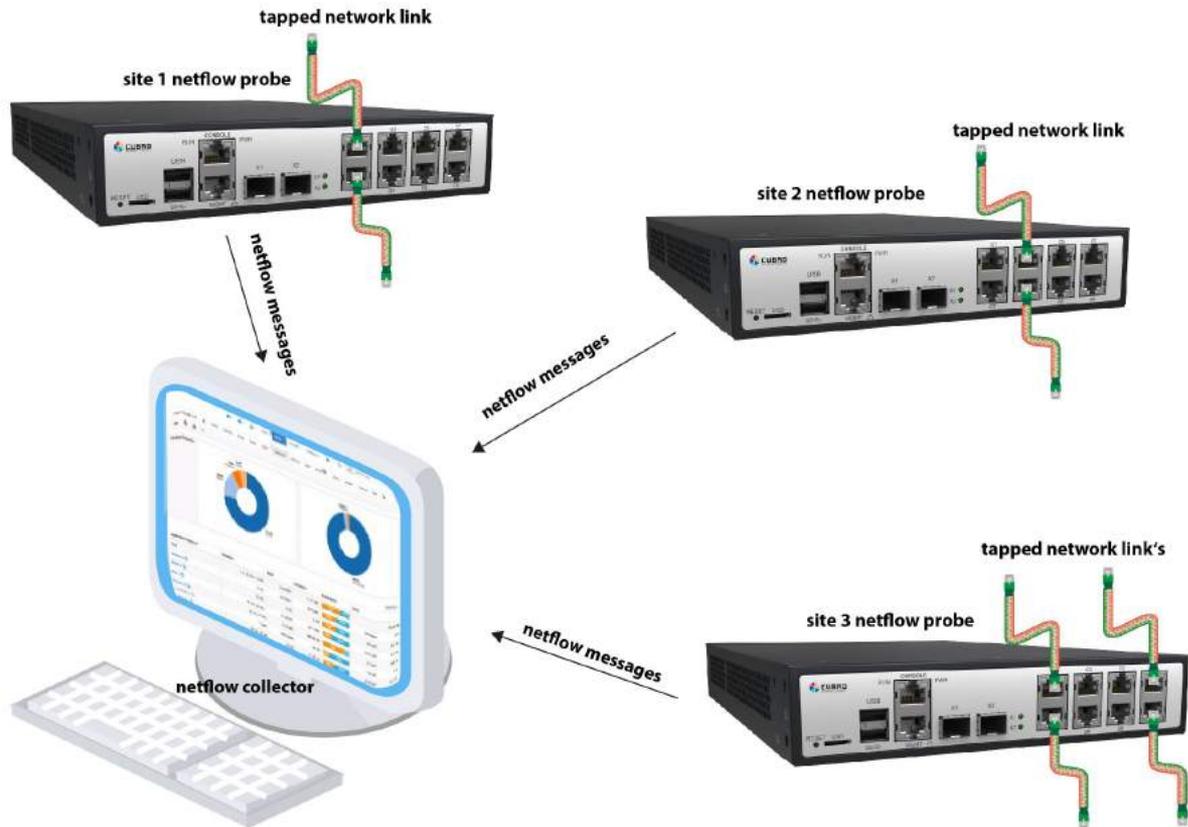
输入流量



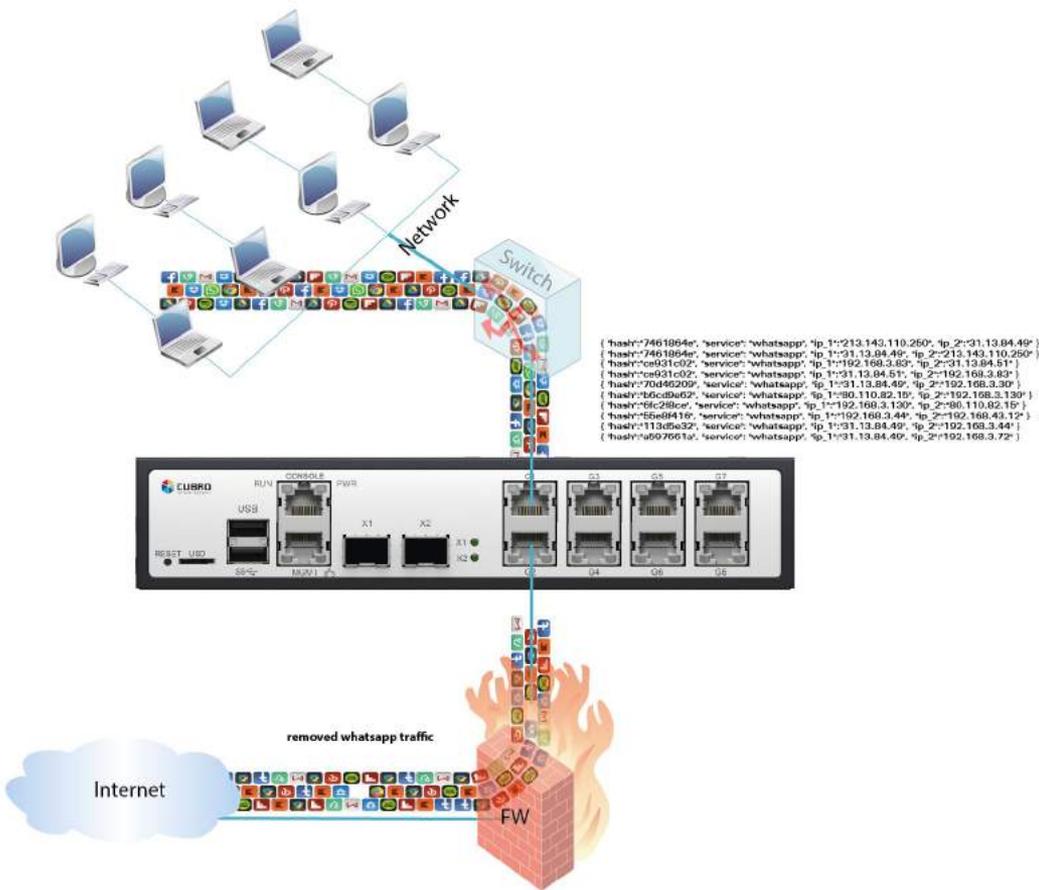
输出流量



# EXA8作为NetFow探针



# 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WhatsApp。

Cubro当前支持多达2000个签名和应用程序。

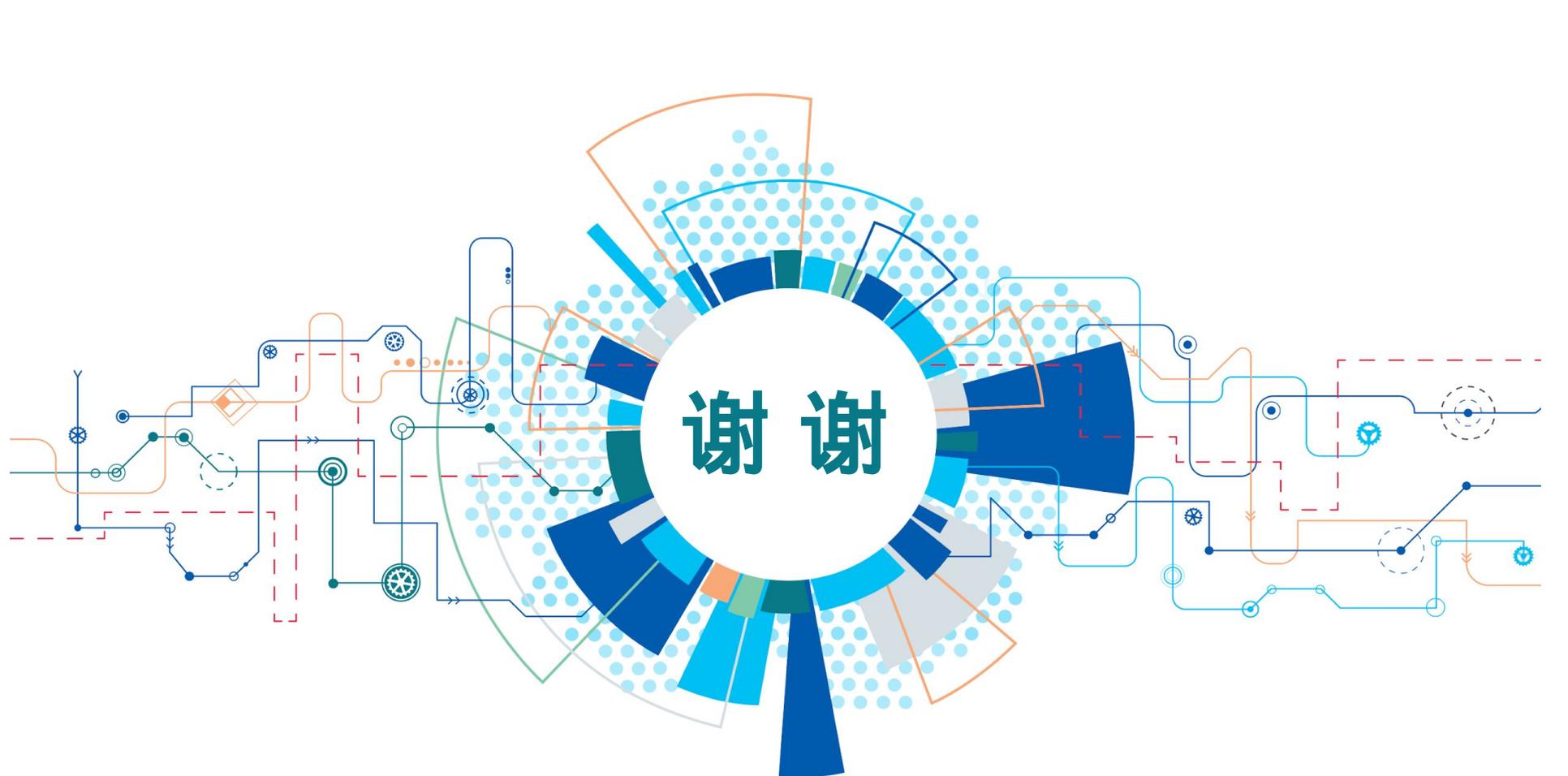
# 质量&环境管理



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。



谢谢

**HongKe**  
虹科

广州虹科电子科技有限公司

需要详细信息？请通过[sales@hkaco.com](mailto: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



关注我们



hongwangle