OMNIA

聚合&捕获设备

Oct. 2020

HongKe 虹科

Omnia 10: 跨越多个部署的多功能性

CPU	Quad-Core ARMv8
Switch	88E6190X Marvell
Memory	DDR4 ECC UDIMM 16GB
eMMC	16 GB
MGMT	10/100/1000 Base-T RJ45
Console	1 * RS232 (RJ45)
I/O	2 * USB3.0 (Type A) MicroSD Card slot
Bypass	Support 4 groups Copper Ports
Port	2 * 10GbE 8*GbE(RJ45)
Internal extended I/O	1* mini PCIex1 Gen 3 2* M.2(PCIex4 Gen3,2280) 1* M.2(Sata Gen3, 2242 & 2280 compatible 1* SATA (Gen3, support 2,5 inch HDD or SSD)
Power Supply	AC 100 - 264 or DC 48V
Size (W x H X D) mm	335 x 220 x 44.4
Power consumption	30 W

Omnia 10（原名EXA8）是一款多功能网络设备，非常适合中小企业、分支机构和远程部署。它具有内置的被动分流能力、10G接口、板载存储和多种软件选项可供选择，是一款能够解决多种网络和安全挑战的设备。

HongKe 虹科

Omnia 20: 满足高要求的工作负载的性能

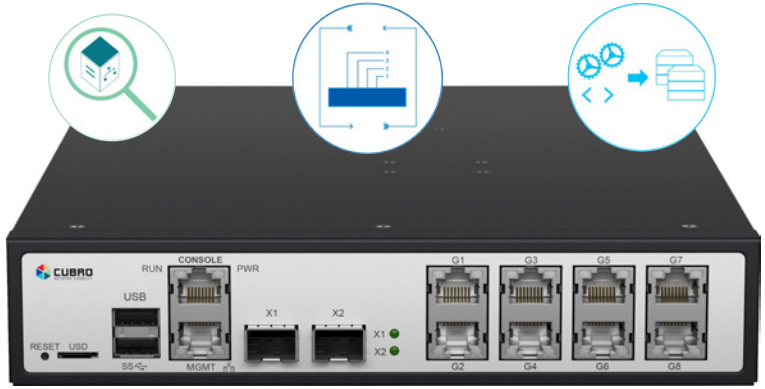
CPU	Quad-Core ARMv8
Switch	88E6190X Marvell
Memory	DDR4 ECC UDIMM 16 GB
eMMC	16 GB
MGMT	10/100/1000 Base-T RJ45
Console	1 * RS232 (RJ45)
USB	1 * USB3.0 (Type A)
Bypass	Support 4 group Copper Ports
Port	2 * 10GbE 2 * 1 GbE (SFP) 8*GbE(RJ45)
Internal extended I/O	1* mini PCIex1 Gen 3 2* M.2(PCIex4 Gen3,2280) 1* M.2(Sata Gen3, 2242 & 2280 compatible 1* SATA (Gen3, support 2,5 inch HDD or SSD)
Power Supply	AC 100 - 264 or DC 48V
Size (W x H X D) mm	335 x 220 x 44.4
Power consumption	30 W

Omnia 20在Omnia 10的基础上增加了额外的1G SFP接口和两倍的处理能力。它保留了Omnia 10的多功能性，同时也是执行特别苛刻任务的首选。

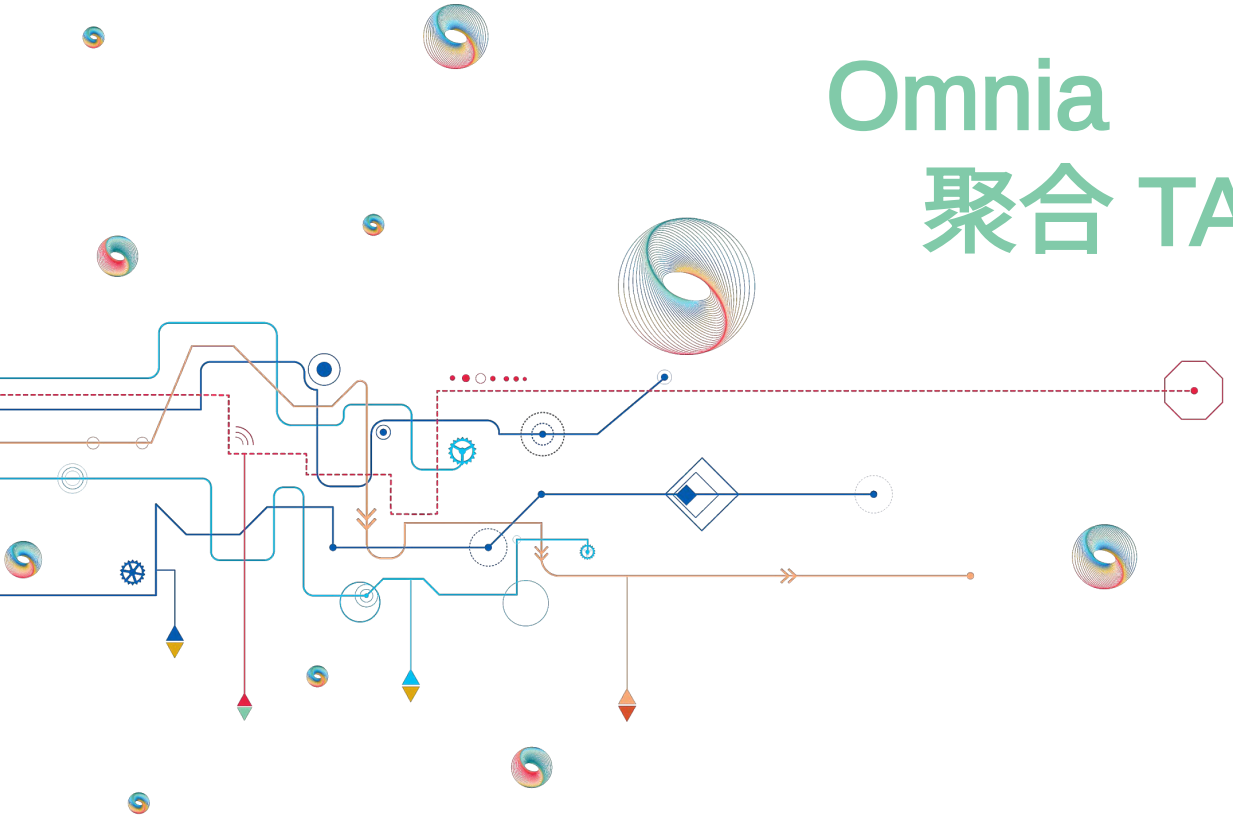
在一个设备中实现多种应用

通过AppMaster，Omnia平台可以支持来自Cubro、合作伙伴和Linux社区的多个应用程序。

来自Cubro的两个这样的应用程序是聚合软件和数据包捕获软件。



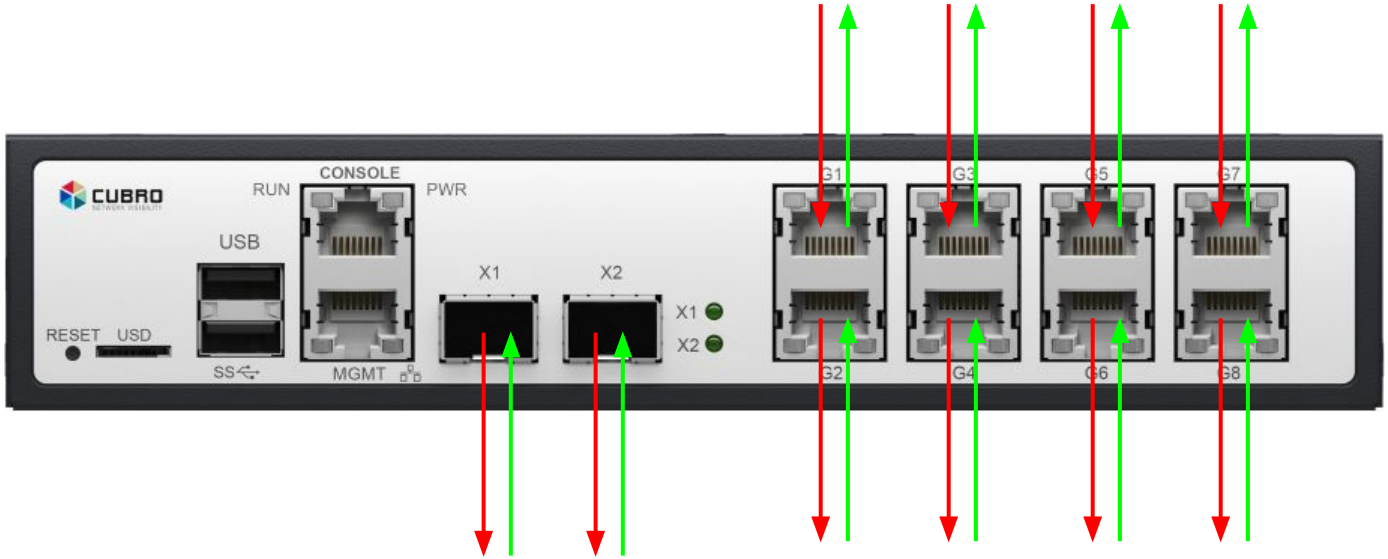
HongKe 虹科



Omnia
聚合 TAP

HongKe 虹科

Omnia 10/20 内置 TAP



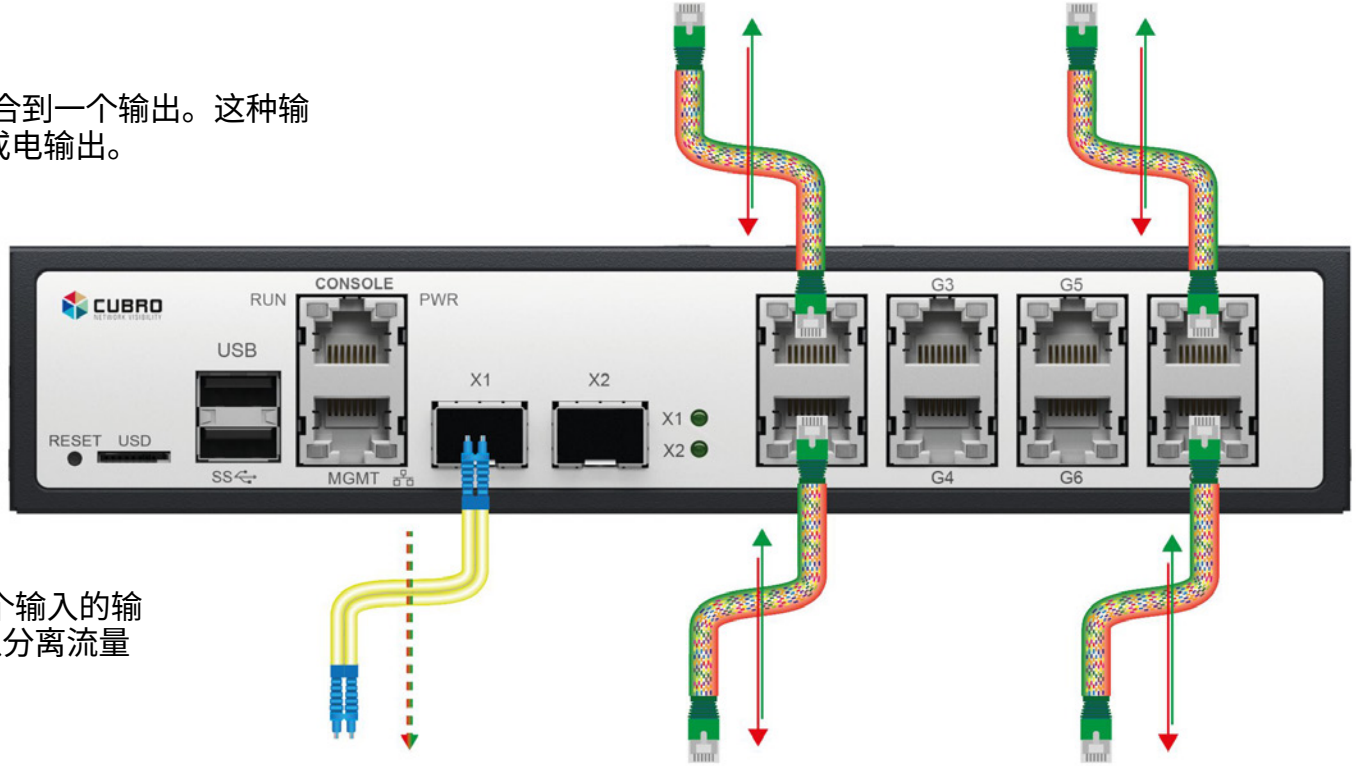
2 x 1/10 Gbit
可作为输入和输出的光/电端口（取决于SFP模块）

4 x 1 Gbit链路，带内部TAP（旁路）

HongKe 虹科

聚合

最多可将4条链路/8个端口聚合到一个输出。这种输出可以是1/10 Gbit的光输出或电输出。



在监控工具中，可以对每个输入的输出流量进行VLAN标记，以分离流量。

HongKe 虹科

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

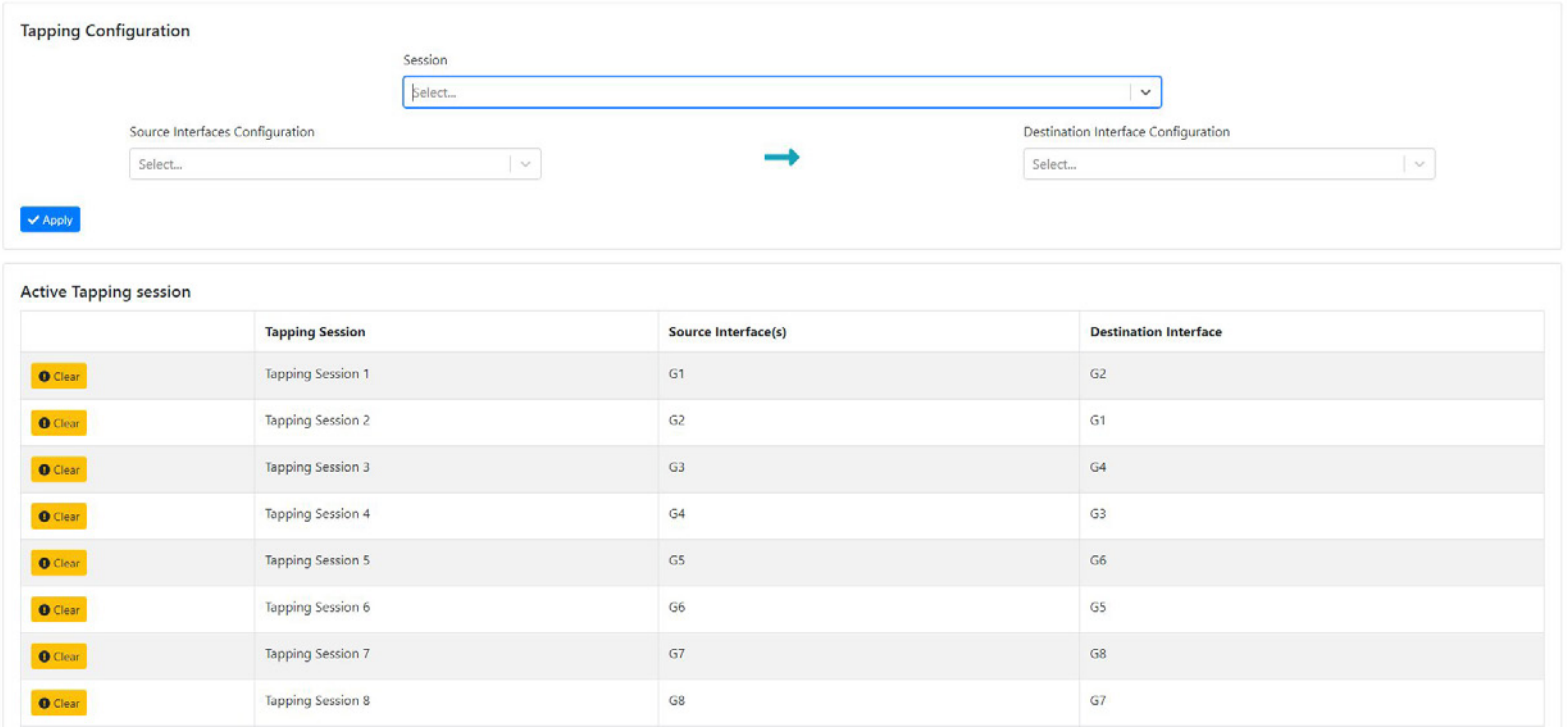
Disk **/mnt/data** free 743.29 GiB - used 33.45 GiB - total 818.33 GiB SMART OK

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

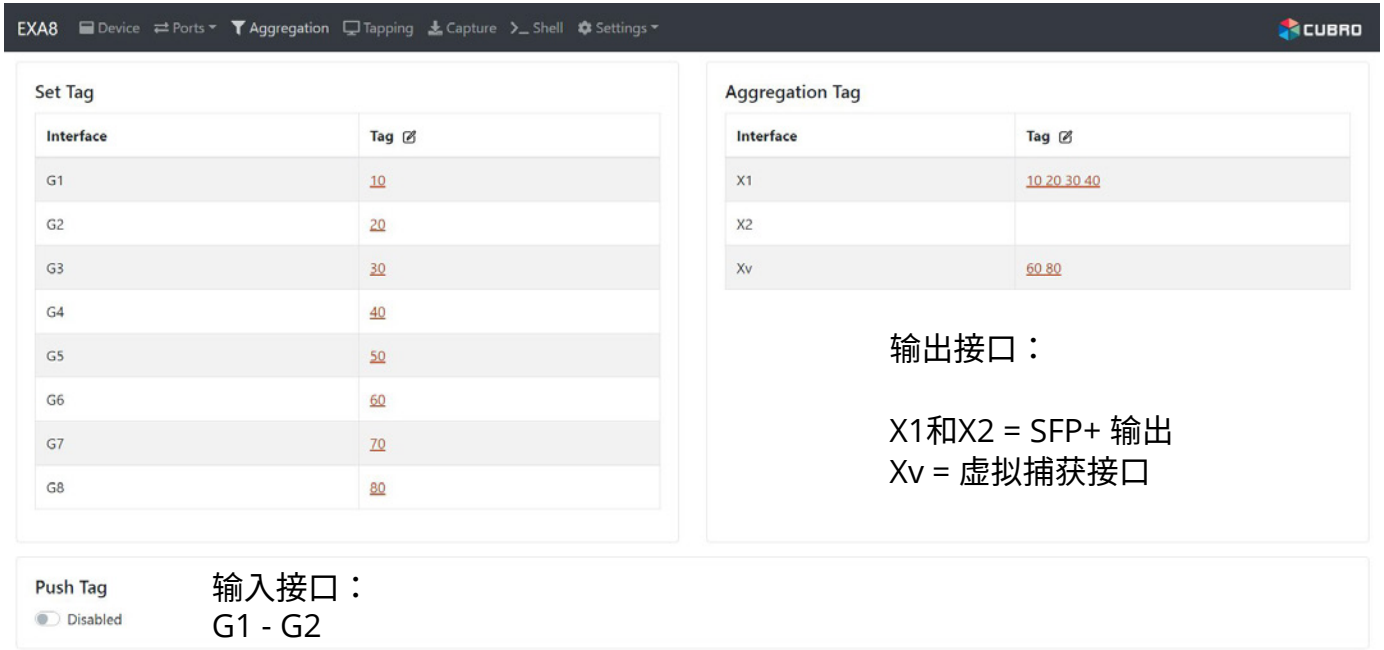
HongKe 虹科

Tapping Session GUI

通过映射实时链路来定义active tapping sessions。



Aggregation GUI



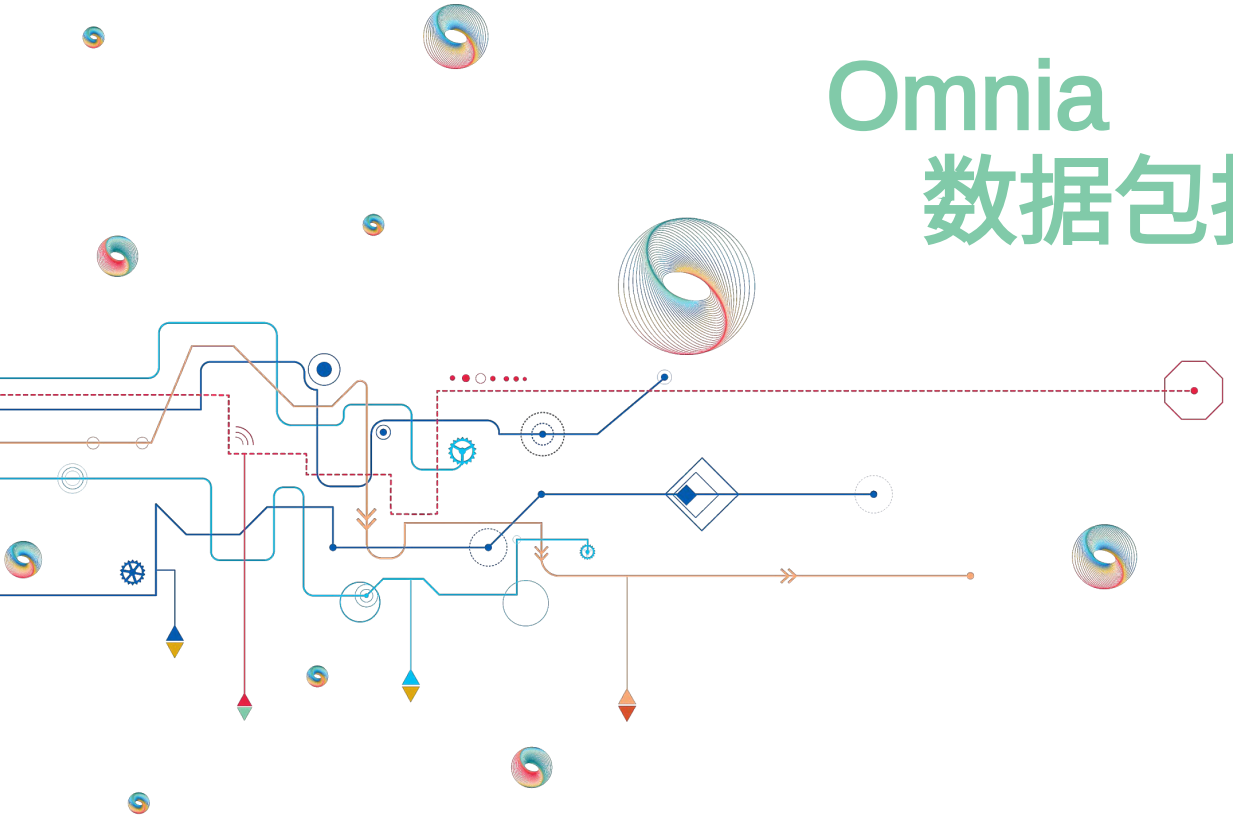
输出接口：

X1和X2 = SFP+ 输出
Xv = 虚拟捕获接口

输入接口：
G1 - G2
G3 - G4
G5 - G6
G7 - G8

4链路

HongKe 虹科



Omnia
数据包捕获

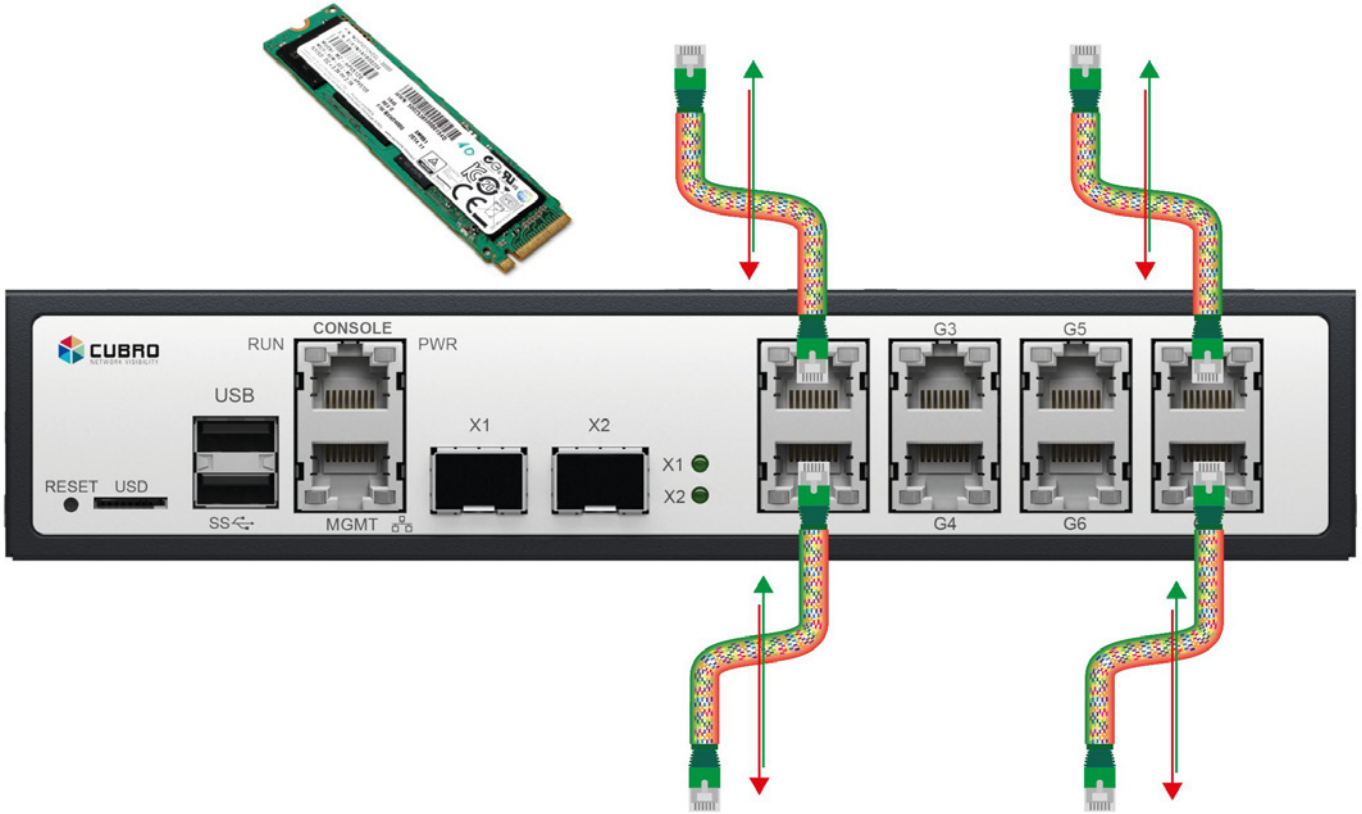
HongKe 虹科

Omnia 10/20 - 捕获设备

- 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
- 能够执行其他一些应用程序，如ntop和DPI。
- 能够运行第三方应用程序
- 滚动捕获提供了过去流量的历史查询

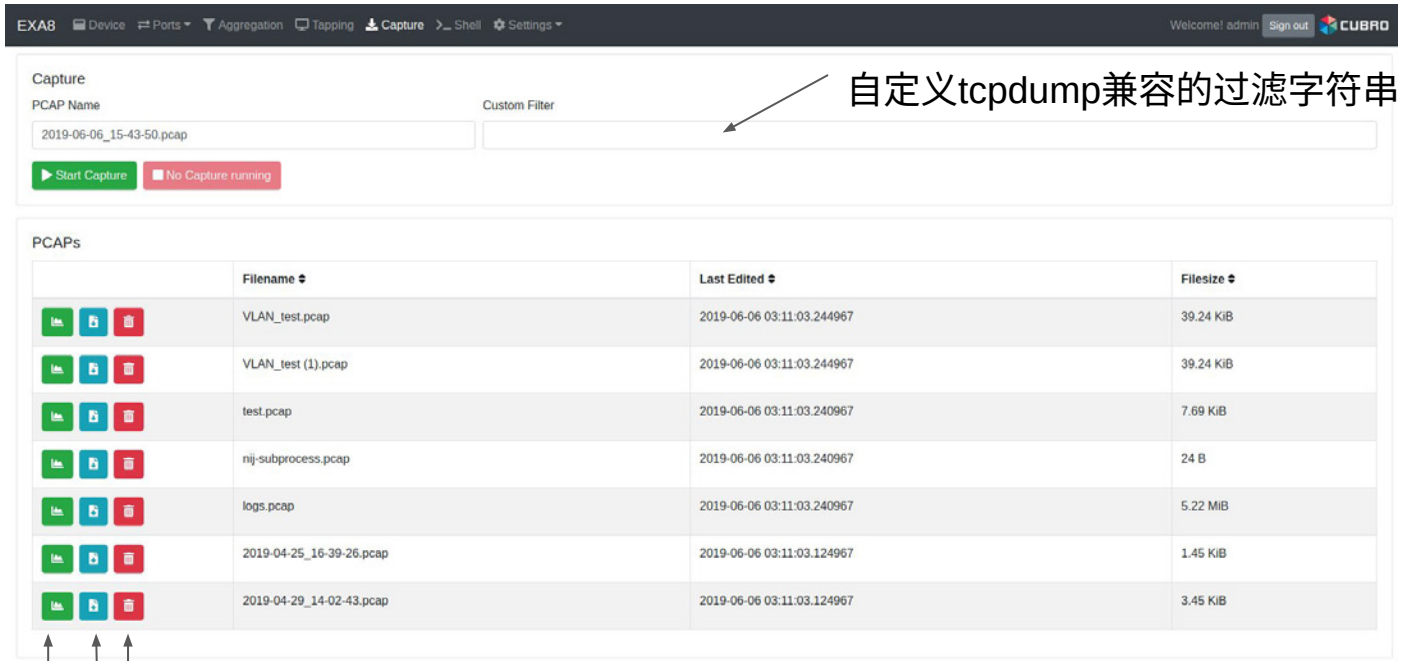
HongKe 虹科

聚合&捕获到SSD



HongKe 虹科

Capture GUI



自定义tcpdump兼容的过滤字符串

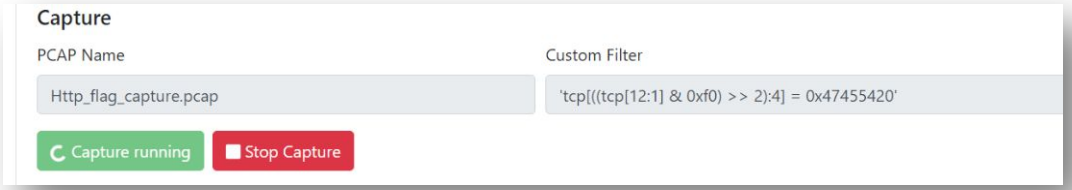
删除捕获文件

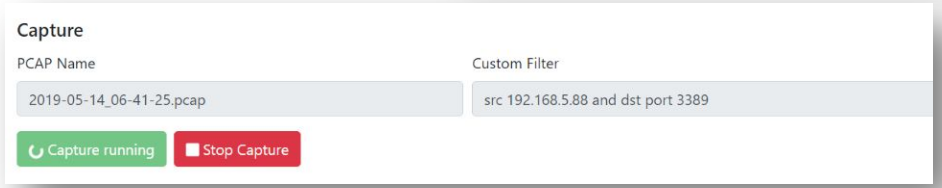
下载捕获文件

启动webshark (分析捕获文件)

HongKe 虹科

自定义过滤器示例

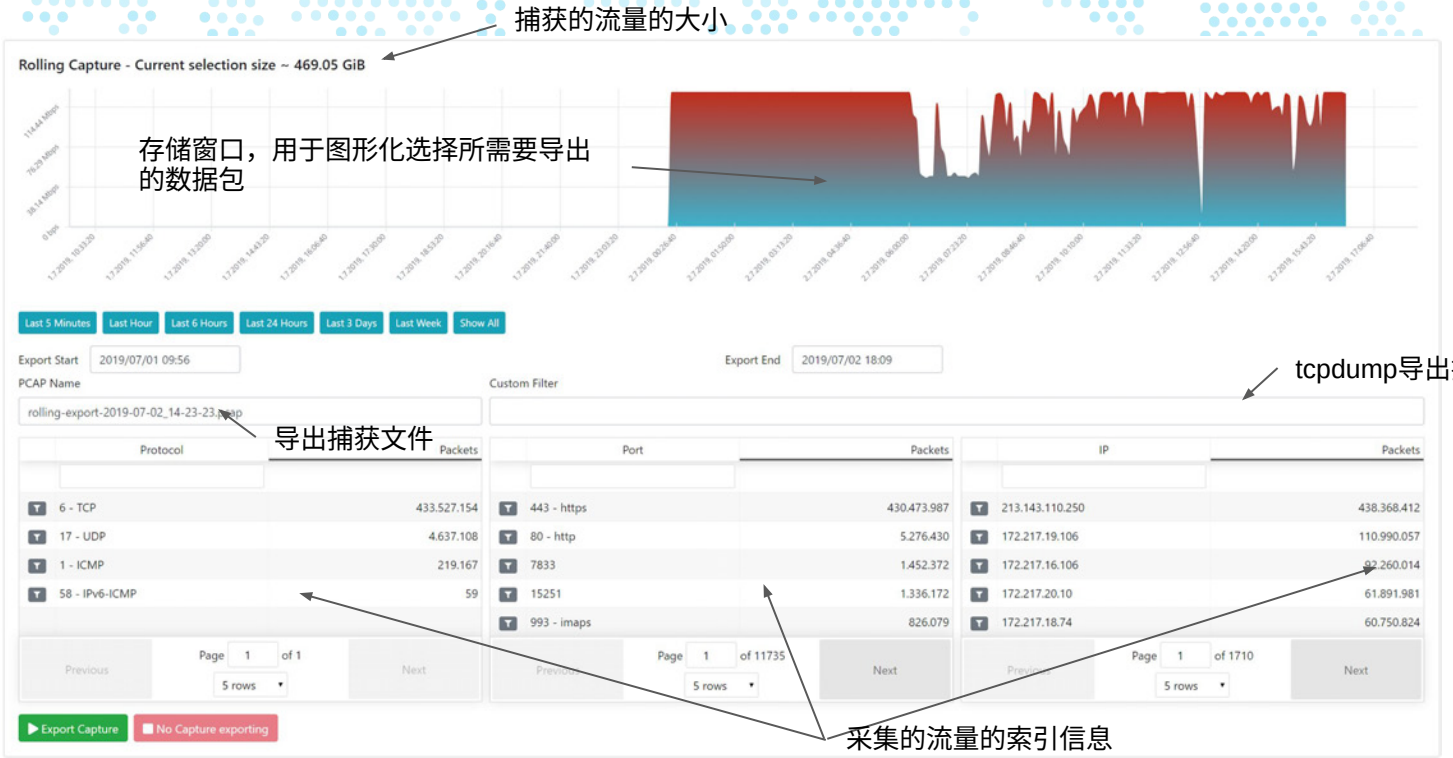




这些过滤器减少了捕获的流量以节省磁盘空间。

HongKe 虹科

Rolling Capture & Indexing

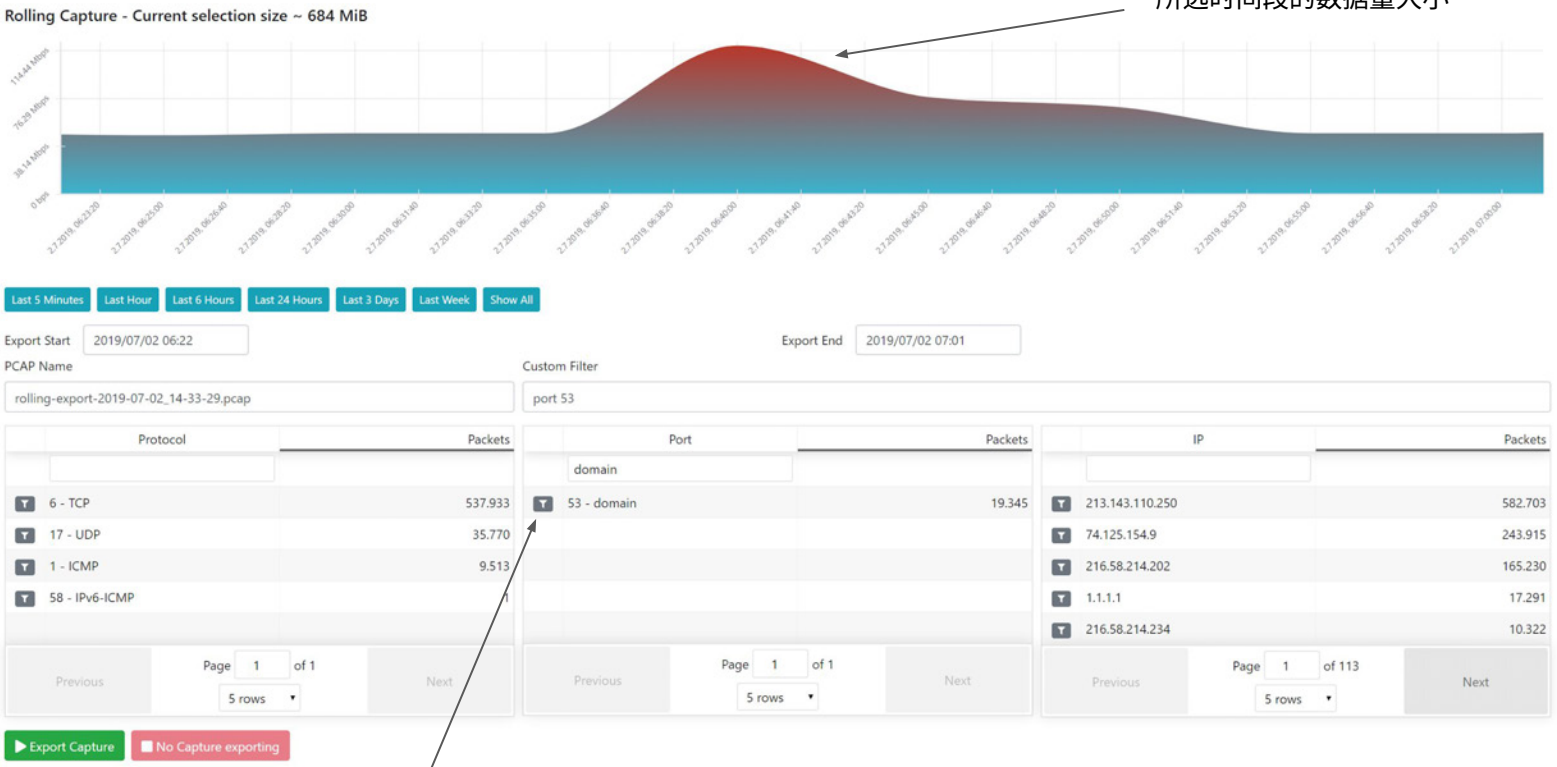


滚动捕获24/7运行，用户可以按时间或IP索引提取捕获文件，并将其转换为PCAP供以后分析。在导出过程中，还可以选择通过tcpdump进行post过滤。

HongKe 虹科

Rolling Capture & Indexing

所选时间段的数据量大小



在这个例子中，我们只想从这个时间框架中提取DNS流量。

HongKe 虹科

Rolling Capture & Indexing

滚动捕获是Omnia 10和Omnia 20从配置的端口或链路连续捕获流量的功能。如果预留的磁盘空间已满，滚动捕获将自动覆盖最老的数据。

滚动捕获也会产生一个捕获流量的索引（时间、IP地址和端口信息）。在该索引的帮助下，相关的流量可以被提取并导出到PCAP文件中进行分析。

该功能提供了查看历史流量模式和事件以进行取证和故障排除的选项。

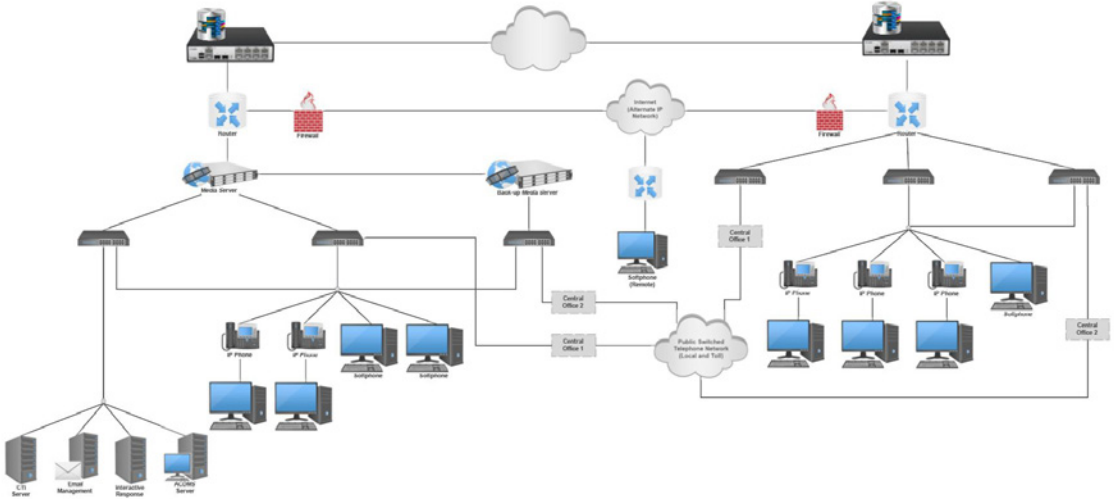
HongKe 虹科

Rolling Capture & Indexing用例

网络故障排除往往很困难，因为问题只是偶尔出现。在这种情况下，标准的捕获是无济于事的。

而Cubro滚动捕获可以快速解决问题，因为捕获是持续运行的，当错误发生时，工程师可以通过捕获文件及时回看。在查询语言的帮助下，可以提取出合适的时间段，以及通过IP地址和端口过滤的相关流量。

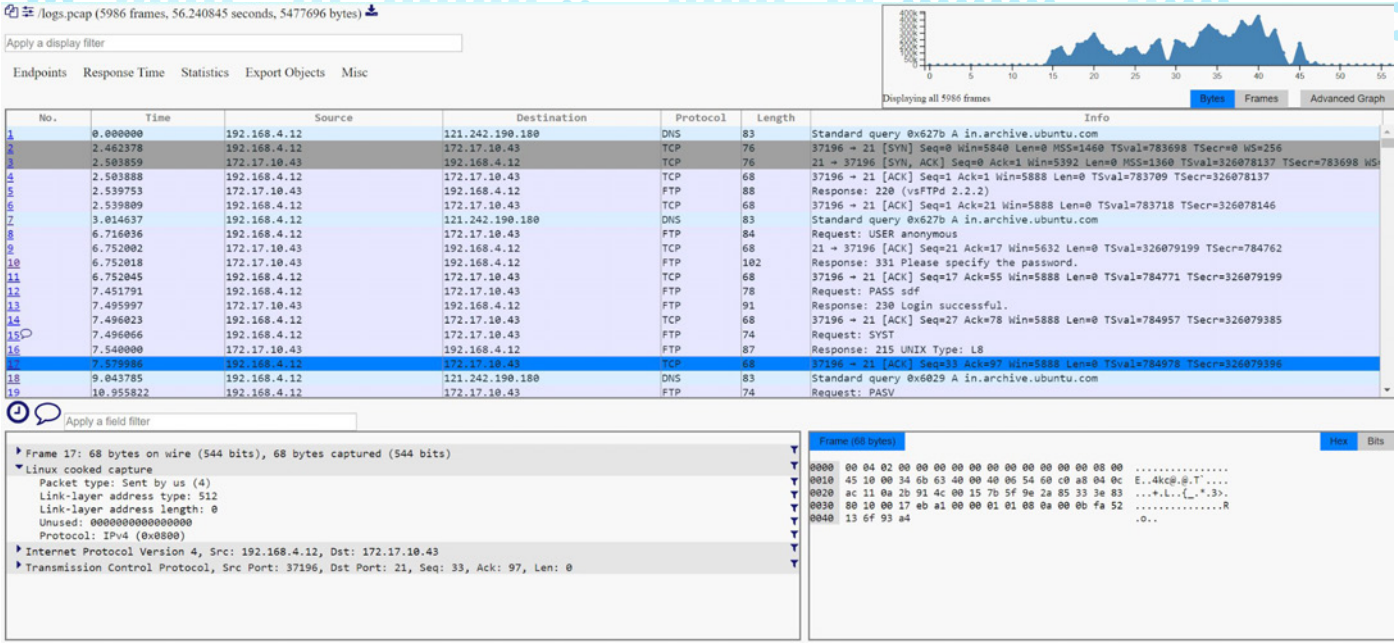
结合TAP和远程访问，Omnia 10和Omnia 20是完美的远程站点故障诊断工具。



在这个例子中，在两个WAN接口上使用滚动捕获，以查看错误事件发生时WAN在完全同一时间的行为。

HongKe 虹科

Webshark GUI

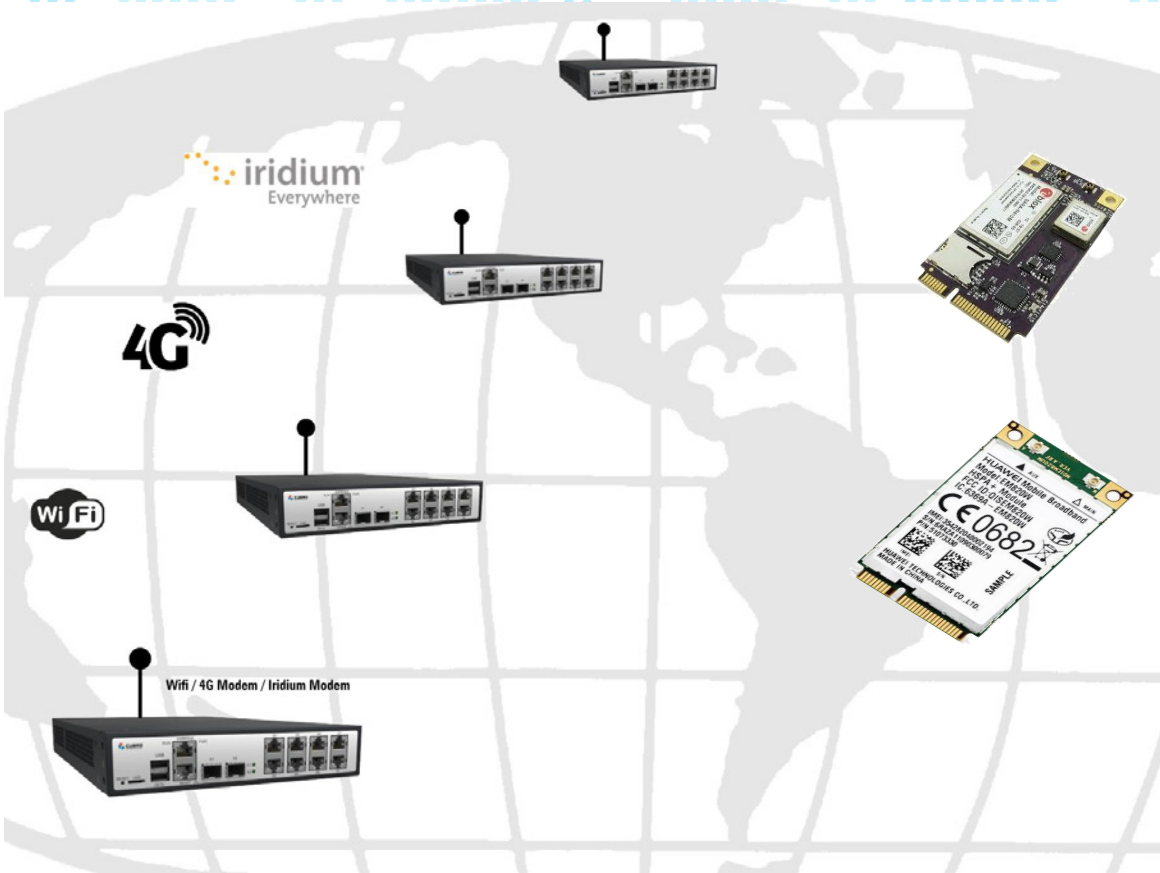


可以直接在Omnia设备上打开捕获的pcap文件，而无需下载文件，只需按下Web GUI中的绿色按钮即可。这提供了仅使用Omnia设备进行远程故障诊断的选项。

Webshark提供了一个类似于大家都知道的Wireshark的功能集。

HongKe 虹科

远程捕获



通过可选的内置Wifi / 2G/3G/4G调制解调器或铱星卫星调制解调器，Omnia设备是多功能监控平台，可通过各种无线技术连接到地球上的每个点。

Omnia 10和Omnia 20支持一个PCIe连接器扩展槽，以及外壳中的天线开口。

一个盒子就可以做到这一切--多接口的网络连接，强大的多核CPU，高性能的SSD存储，以及支持远程连接的调制解调器。

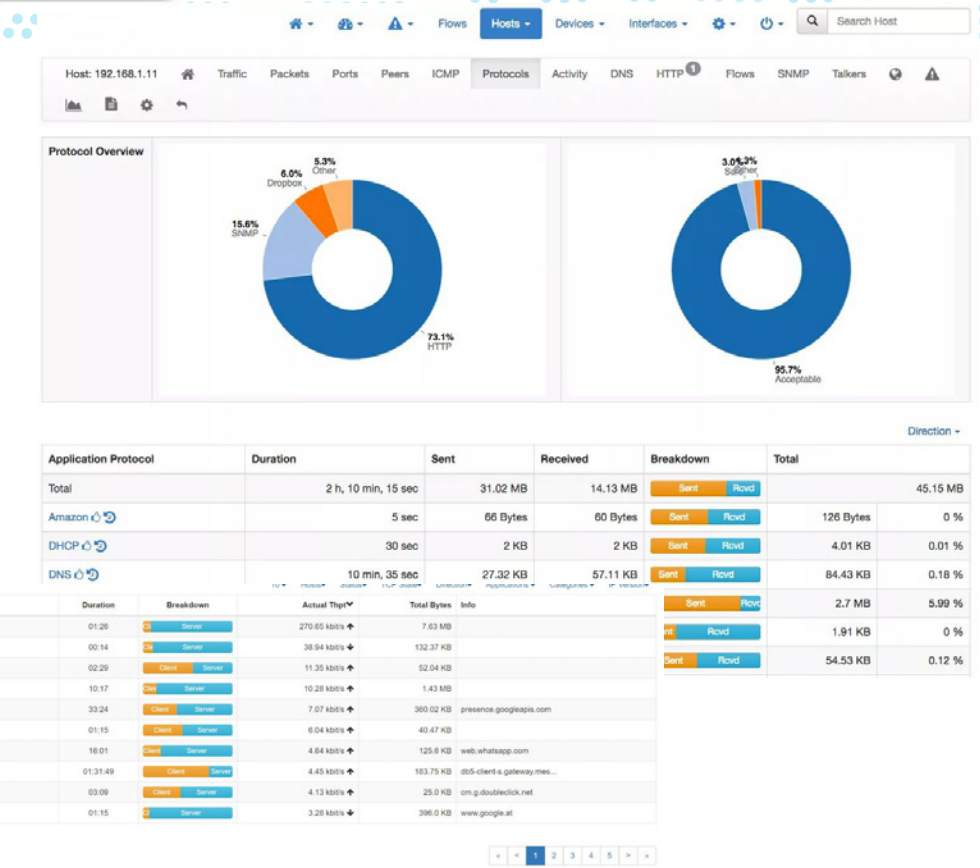
强大的CPU为用户提供了在远程站点运行分析软件的选项，从而避免了通过缓慢的连接链接下载捕获文件的需要。

HongKe 虹科

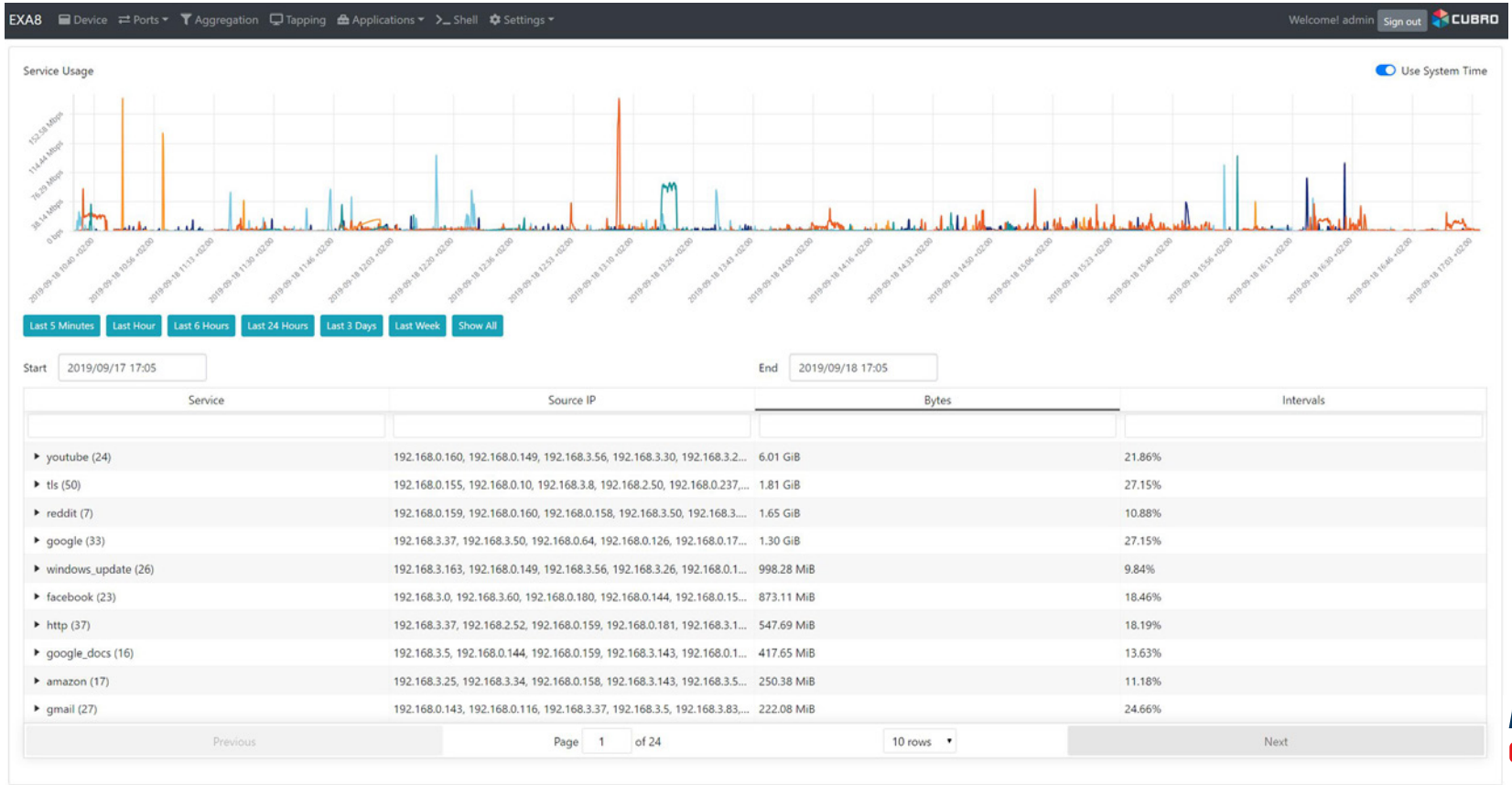
Omnia上的Flow分析

Omnia AppMaster支持NTOPng，这是一款功能齐全的Flow分析仪。

该软件提供对连接到Omnia的分接网络链接的全面在线监控。



DPI应用检测“ 4000+”



HongKe 虹科

DPI应用检测“ 4000+”

DPI “ 应用检测” 的重要性在于两个方面：

查看**网络上正在发生什么**，在用户和应用程序使用情况，以防止滥用企业网络。*“ 我们根本不查内容，我们只产生元数据。”*

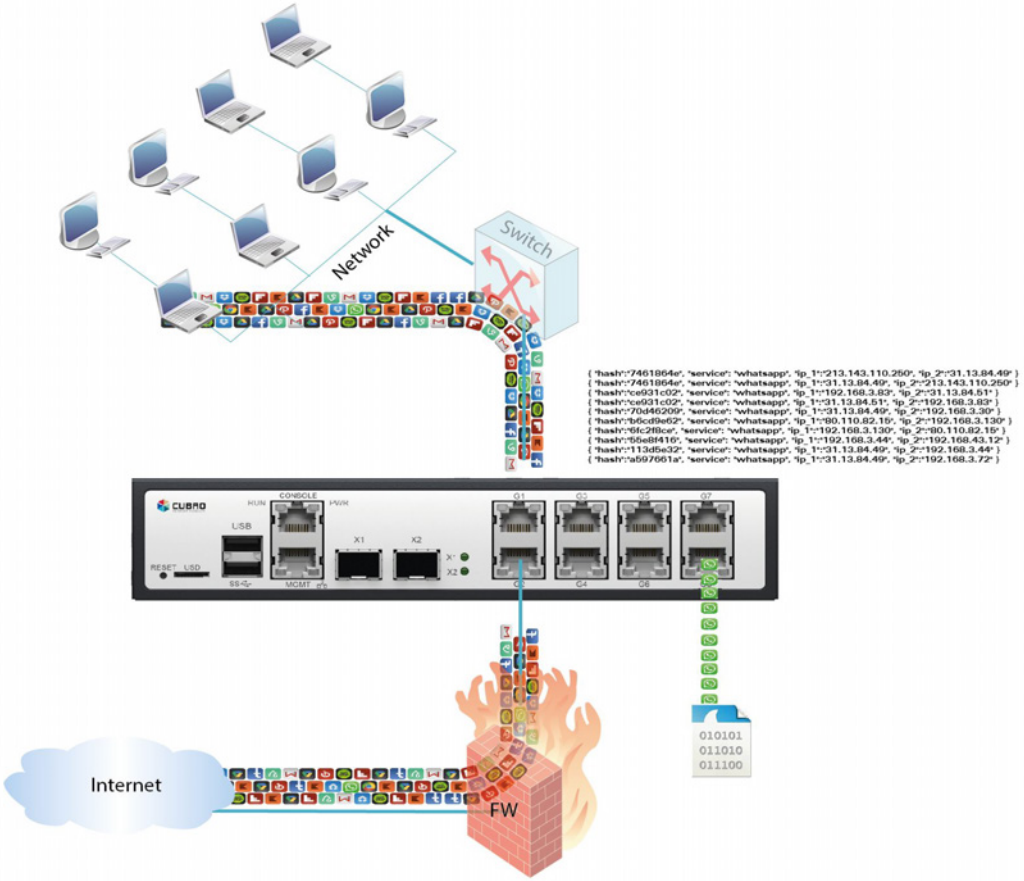
DPI非常有用的第二个原因是有可能**通过删除已知的应用程序来减少必须分析的流量**。要找到攻击，必须对通信量执行取证分析，但由于通信量太大，这通常很麻烦。DPI现在可以通过负过滤来帮助整理保存流量。我们可以通过DPI索引从捕获中删除所有 "已知的好 "流量。

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。**

HongKe 虹科

利用OMNIA对捕获的流量进行DPI过滤



Omnia设备也可以只用于捕获一个应用程序，在这个例子中，Whatsapp。

目前我们最多支持4000个签名和应用。

使用滚动捕获功能在Omnia 10或Omnia 20上捕获流量，并通过元数据表从DPI服务中提取流量。

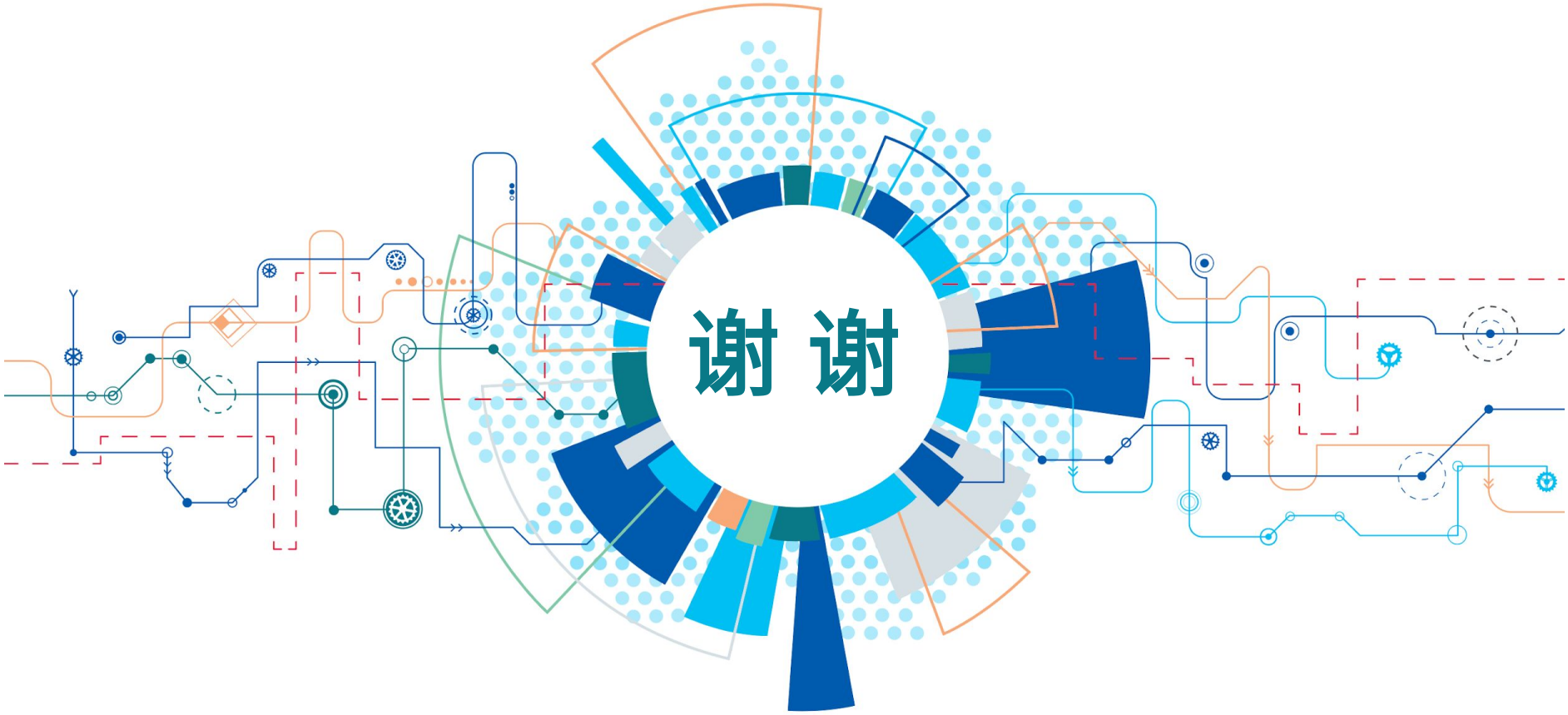
HongKe 虹科

质量&环境认证

CUBRO已通过ISO9001质量管理体系认证，确保提供最好的产品和服务

CUBROO已通过国际标准化组织14001认证，致力于保护我们的环境。

HongKe 虹科



HongKe 虹科

广州虹科电子科技有限公司

关注我们

hongwangle

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