



Cubro DPI

Feb 2020

目录



1. 介绍
2. Cubro DPI方法
3. DPI应用概述
4. 分析应用程序
5. 过滤应用程序
6. 拦截应用程序
7. 内联应用完整示图
8. Cubro DPI的优势

介绍: DPI在电信



深度数据包检查（DPI）是一项技术，使网络所有者可以实时分析通过网络的Internet流量，并根据其有效负载对其进行区分。

DPI通常用于了解订户的性能或行为，他们使用哪些应用程序，使用频率等。这有助于运营商专注于为重要应用程序改善服务。例如，像Netflix，YouTube等视频流服务消耗大量带宽。DPI可以用来限制这一点。

DPI通过提供网络可见性和实时应用程序感知，有助于分析和管理IP流量，并实时保护IP网络。除了影响带宽和流量管理决策外，DPI还可以提供以下方面的见解：

- 网络安全
- 网络管理
- 网络和订户分析
- 内容监管
- 定向广告
- 应用程序分发和负载均衡

深度数据包检查（DPI）是通过签名检测流量类型；超越端口和协议

```
{ "hash": "7461864e", "service": "whatsapp", "ip_1": "213.143.110.250", "ip_2": "31.13.84.49" }  
{ "hash": "7461864e", "service": "whatsapp", "ip_1": "31.13.84.49", "ip_2": "213.143.110.250" }  
{ "hash": "ce931c02", "service": "whatsapp", "ip_1": "192.168.3.83", "ip_2": "31.13.84.51" }  
{ "hash": "ce931c02", "service": "whatsapp", "ip_1": "31.13.84.51", "ip_2": "192.168.3.83" }  
{ "hash": "70d46209", "service": "whatsapp", "ip_1": "31.13.84.49", "ip_2": "192.168.3.30" }  
{ "hash": "b6cd9e62", "service": "whatsapp", "ip_1": "80.110.82.15", "ip_2": "192.168.3.130" }  
{ "hash": "6fc2f8ce", "service": "whatsapp", "ip_1": "192.168.3.130", "ip_2": "80.110.82.15" }  
{ "hash": "55e8f416", "service": "whatsapp", "ip_1": "192.168.3.44", "ip_2": "192.168.43.12" }  
{ "hash": "113d5e32", "service": "whatsapp", "ip_1": "31.13.84.49", "ip_2": "192.168.3.44" }  
{ "hash": "a597661a", "service": "whatsapp", "ip_1": "31.13.84.49", "ip_2": "192.168.3.72" }
```

这是Cubro DPI引擎的输出，因此即使被加密也可以找到WhatsApp！我们可以找到多达4000个不同的应用程序。

DPI通常有两种不同的主要应用程序

1. 分析

在此应用程序中，DPI引擎可以对全部流量进行解码，并生成DB格式的结果用于分析。这只能在基于CPU的设备上实现，如(exa8/EXA24160/EXA40等)。由于每个数据包都要处理，因此在CPU负载和数据输出方面需要付出很大的努力。

2. 标记/过滤/拦截

该应用与Cubro方法产生了共鸣-从监视中删除不需要的应用程序类型。最常见的是删除所有视频流服务，因为它与监视无关。

同一应用程序用于阻止某些应用程序，或将某些流量发送到特殊的监控设备。在这种情况下，不需要进行完全解码，因为采样可以得出相似的结果，但工作量却少得多。

DPI 签名 (应用程序&协议)



我们最多支持4000个签名。这些签名分为两部分：

- 1400请参阅[DPI Services](#) - 这些是手动维护的顶级签名。
- 其他签名由深度学习和人工智能（AI）维护。

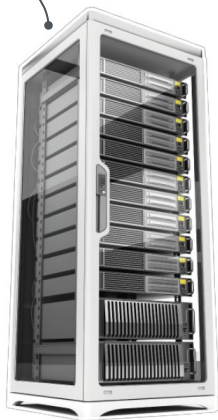
(更新周期约为7-10天)

分析应用程序高达数TB

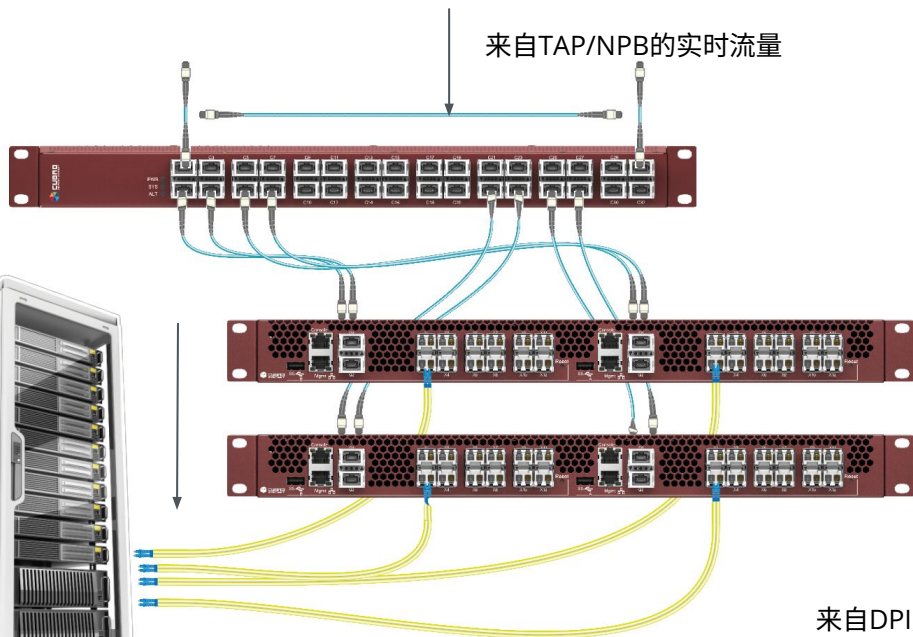


可用的元数据：

- 时间戳
- 用户
- 用户IP
- 服务IP
- 应用程序 (4000+)
- 数据包数
- 每个APP字节



Kafka / Hadoop Cluster



推荐设备EXA8和EXA1008
(从8 Gbit/sec到高达400 Gbit/sec
每个设备)

来自DPI应用的元数据

```
{ "hash": "7461864e", "service": "whatsapp", "ip_1": "213.143.110.250", "ip_2": "31.13.84.49" }  
{ "hash": "7461864e", "service": "whatsapp", "ip_1": "31.13.84.49", "ip_2": "213.143.110.250" }  
{ "hash": "ce931c02", "service": "whatsapp", "ip_1": "192.168.3.83", "ip_2": "31.13.84.51" }  
{ "hash": "ce931c02", "service": "whatsapp", "ip_1": "31.13.84.51", "ip_2": "192.168.3.83" }
```


过滤应用程序



全部流量输入

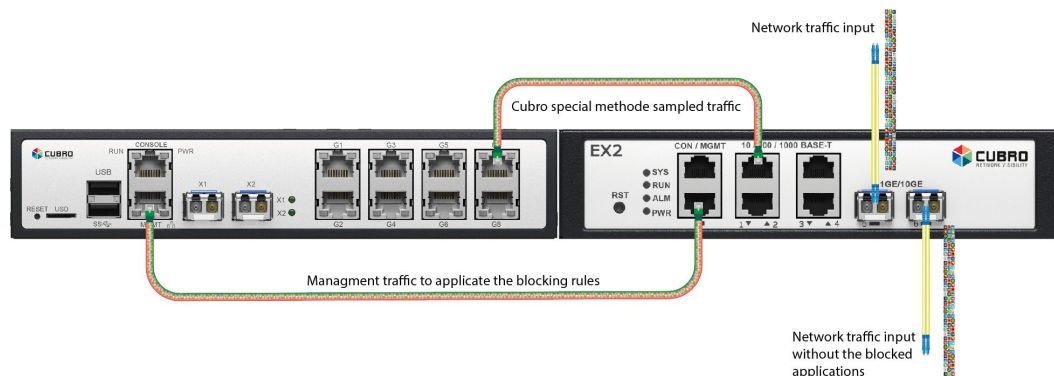


输出没有视频流的流量，以减轻监控或捕获设备的负载

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 Shortline 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 au...
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	Direct TV 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.
	video	go90 is an American video streaming service, launched in October 2015

还有更多

应用: 10 Gbit流量的拦截 EXA8 & EX2



EXA8结合EX2还可以用来拦截WhatsApp、Skype、YouTube等应用程序。

我们目前支持多达4000个签名和应用程序。

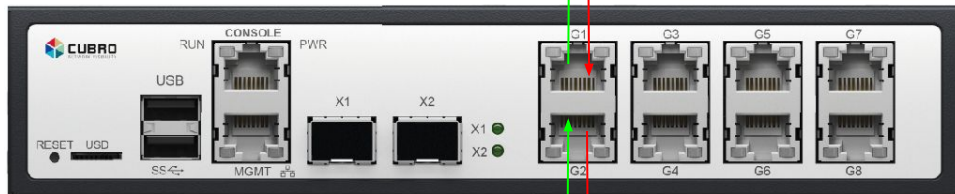
流量通过EX2，EX2执行特殊的采样方法以向EXA8提供流量。

EXA8上的DPI引擎解码流量并在EX2上配置丢弃规则。

拦截应用程序



流量正通过“内联”设备

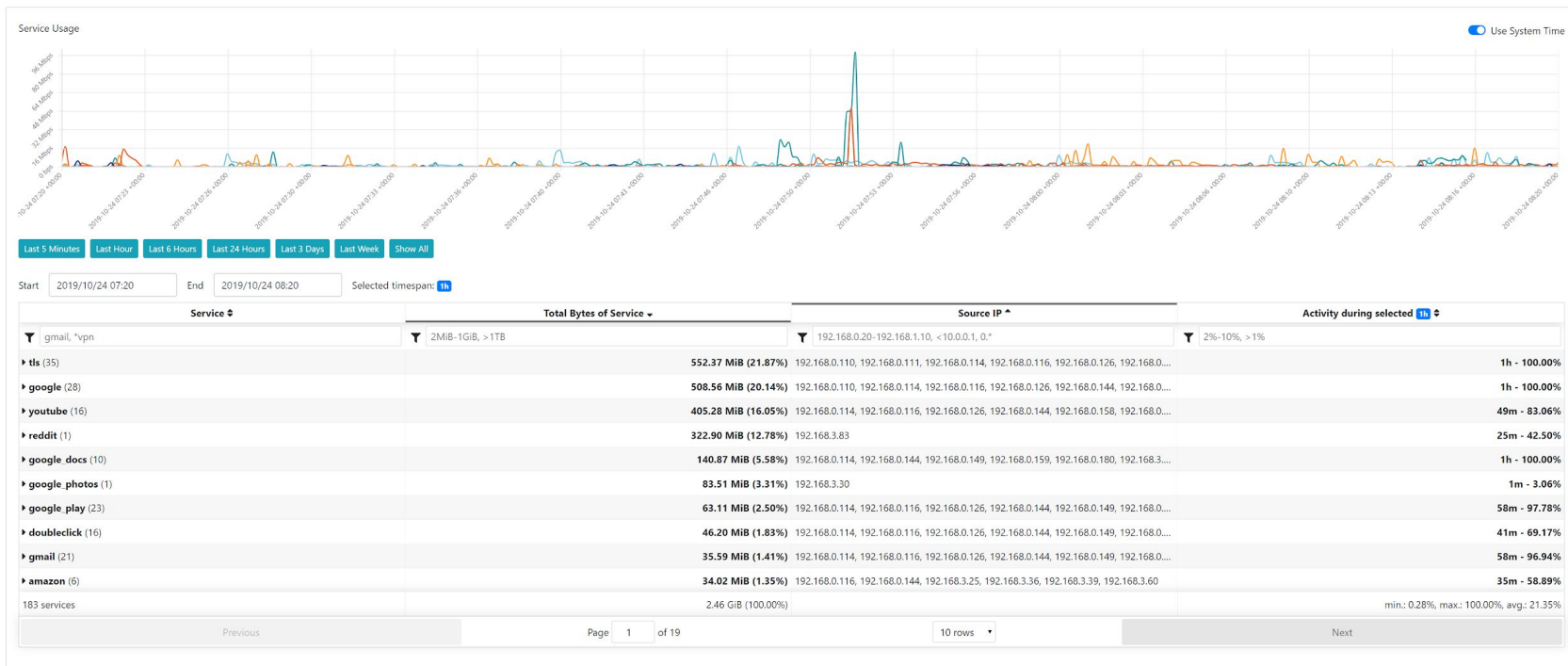


流量正通过“内联”设备

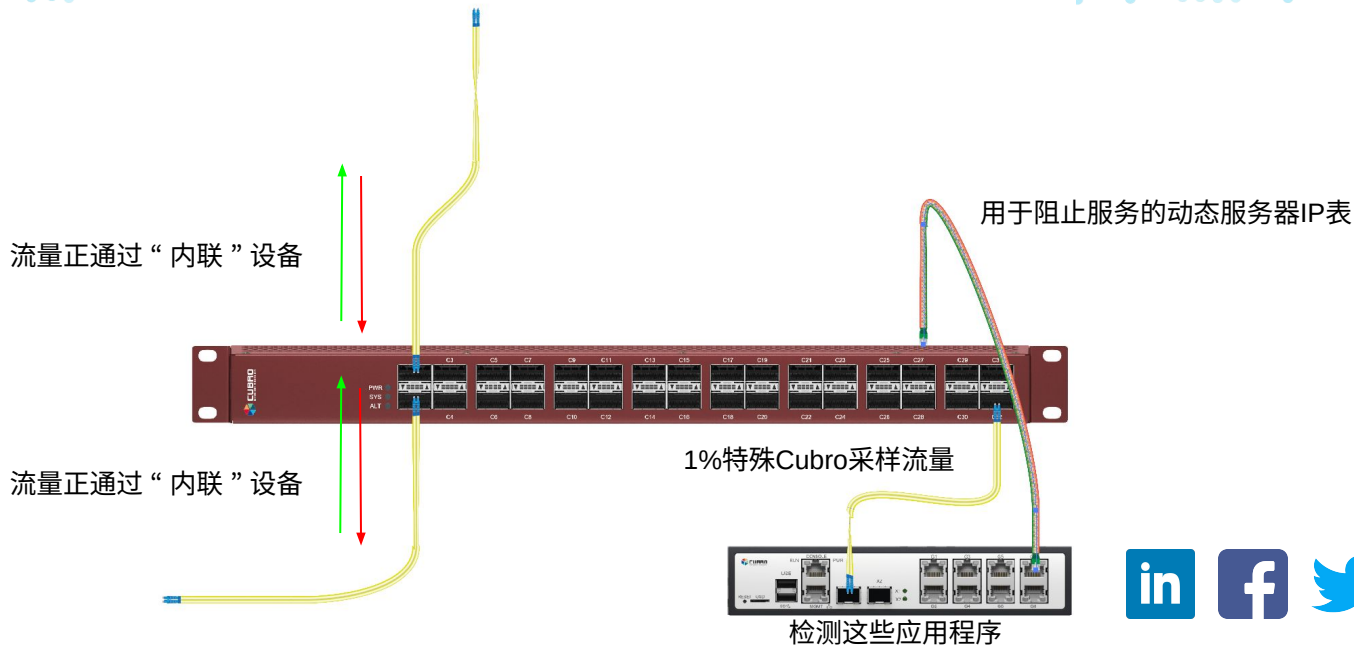
去除这些应用



在EXA8上实施DPI分析



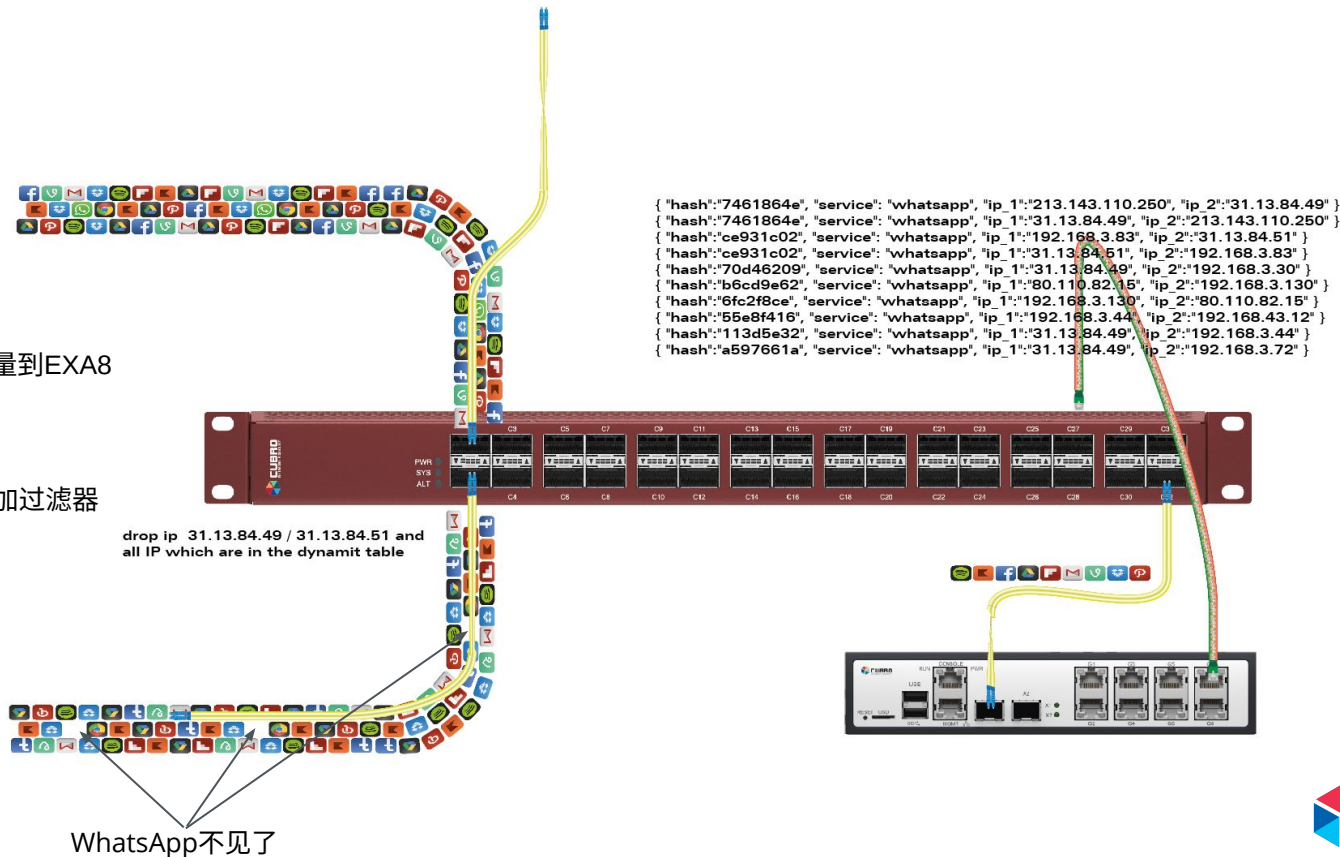
用G5网络数据包代理拦截应用程序



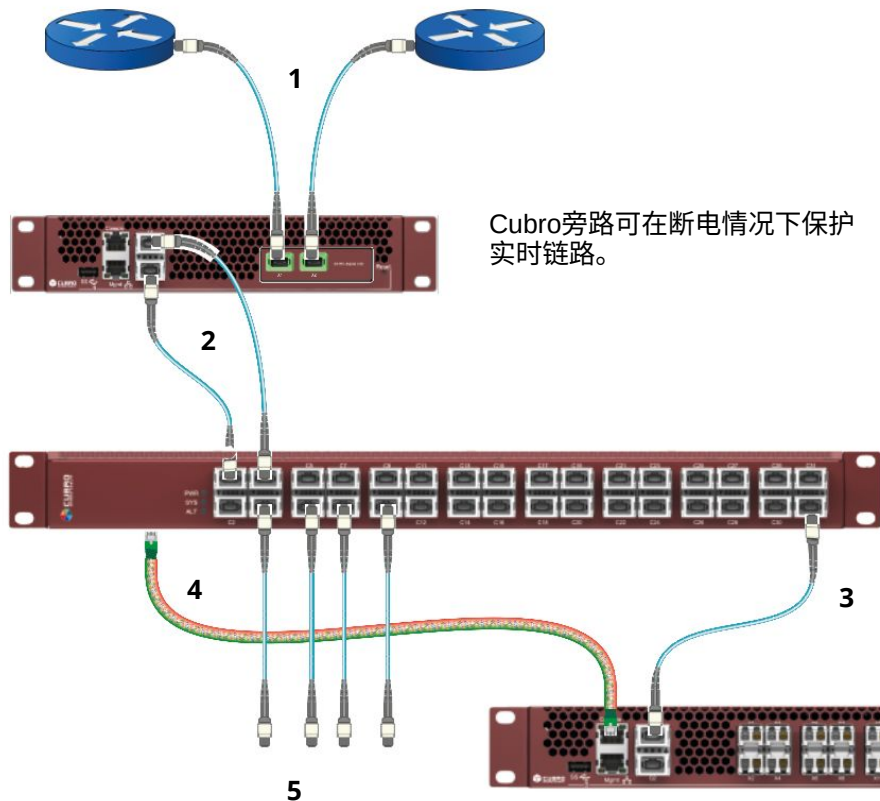
检测器可以是任何基于CPU的单元，也可以是服务器。
也可以在G5单元主机控制器上进行此操作（正在调查中）

用G5网络数据包代理拦截应用程序

- 1) 输入流量
- 2) 特殊Cubro采样流量到EXA8
- 3) 生成过滤表
- 4) 在EXA32100上添加过滤器



内联应用完整示图



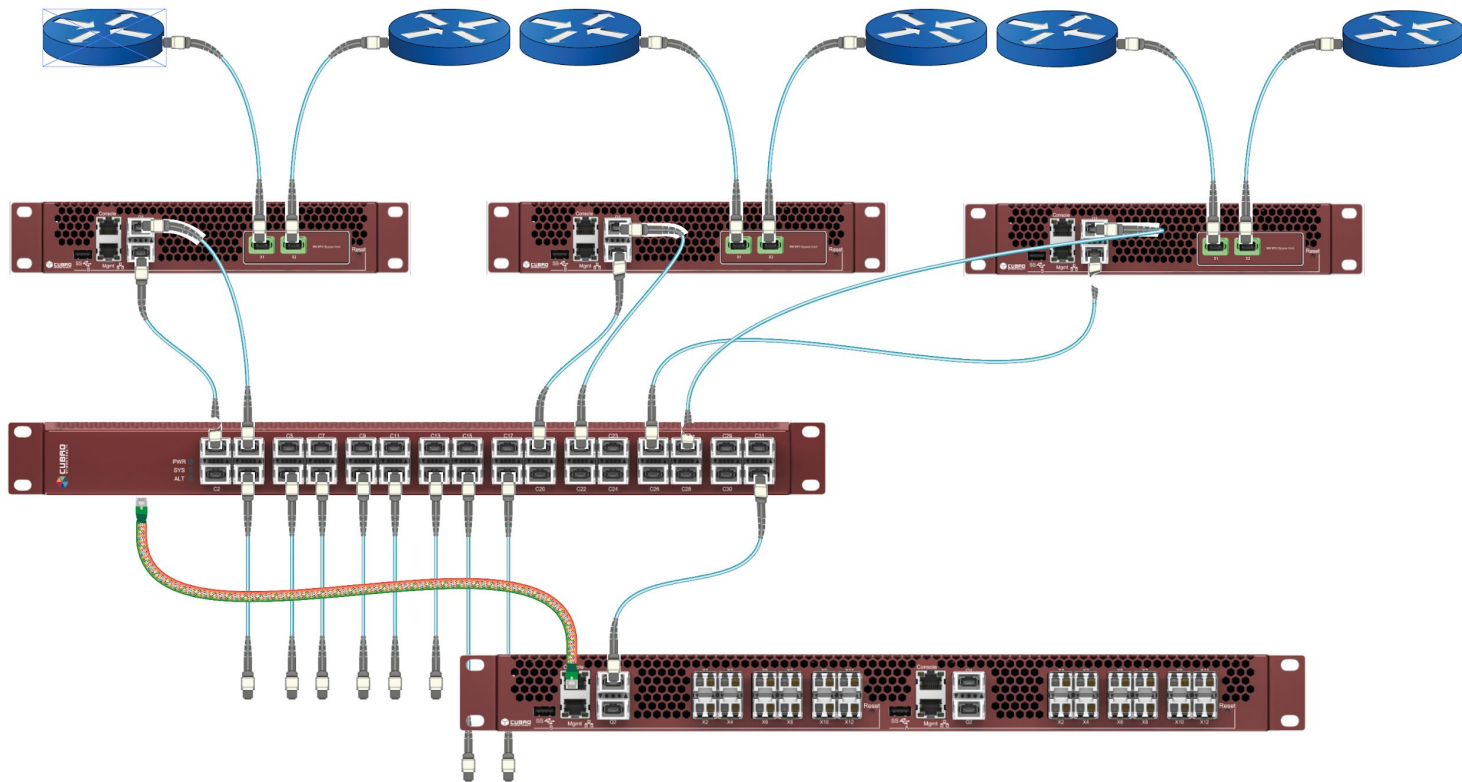
Cubro旁路可在断电情况下保护实时链路。

- 1 实时链路
- 2 旁路输出
- 3 Cubro采样（正在申请专利）到DPI单元 unit
- 4 从DPI到Cubro NPB的管理
- 5 (负载均衡)输出到下游挡位

Cubro G5 NPB处理流量分离、负载均衡和流量重新插入。

DPI引擎基于所需的资源。
不同的型号可用从EXA8 - 高达400 Gbit单元

内联高达2 TB和8 x 100 Gbit链路



Cubro DPI的优势



Cubro DPI将智能引入互联网网络。与大多数其他供应商不同，Cubro的DPI方法包括**旁路**和**应用拦截功能**，使互联网服务提供商能够有效地监控、加速、过滤、拦截用户流量，并做出任何其他有用的决定。

获取商业智能以应对5G挑战

确保降低网络的总体拥有成本
(TCO)

保持高水平的网络性能

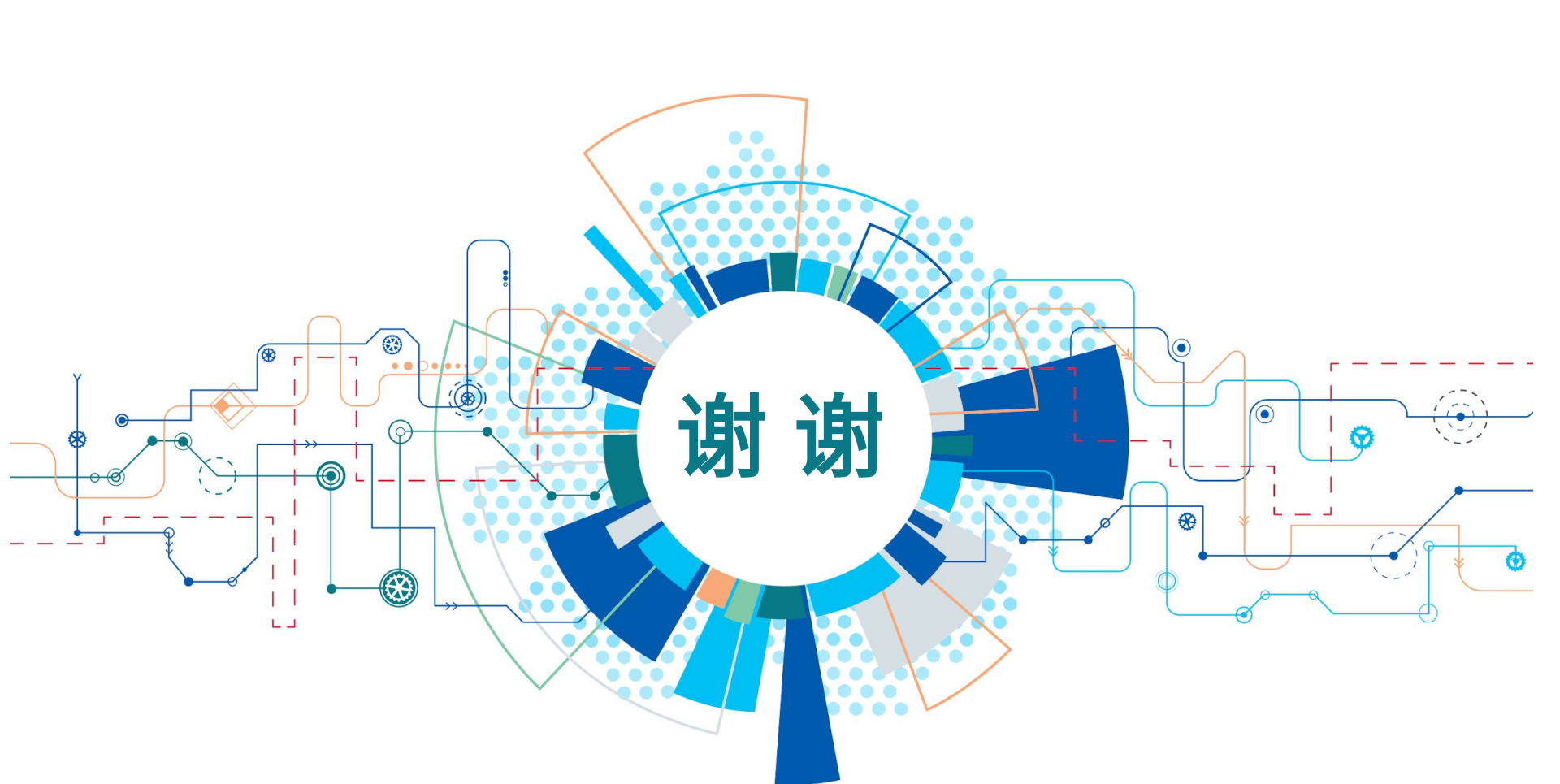
增强整体QoS



Cubro已通过ISO9001认证，按照国家标准进行质量管理。



Cubro通过了ISO14001认证，以为保护环境做出努力。



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

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