HongKe 虹科

数据表

Cubro FlowVista系列

产品概述

Cubro FlowVista提供灵活的签名语法和标识，同时专注于高性能和实时DPI处理。
支持ACL和负载均衡规则的引擎是基于IP 5元组应用协议。此外，FlowVista可以识别和标记原始数据，并根据NetFlow v9标准中的IP 5元组输出流日志。

功能/优点：

- 内置逻辑签名处理引擎，支持规则优先级和输出最高优先级的识别结果
- 灵活的规则语法描述：用户可以基于PDL* 语法定义协议规则
- 支持跨包搜索
- 支持规则热插拔，无需中断流量处理即可实现规则升级
- 关联识别：关联多会话协议，统一识别结果
- 数据包过滤负载平衡：FlowVista可以基于IP 5元组和应用程序协议规则处理数据包，并支持组合的ACL规则和多维负载平衡（保留会话/用户完整性）。

*（PDL语法是Cubro Regex编译器生成新指纹的语言）

网络探针

概览

定义

探针是一种无源设备，它从TAP和数据包代理器中接收网络流量并提取元数据。

FlowVista的优点

- 小尺寸和低功耗设计
- L7应用程序检测
- 嵌入式网络处理器设计
- 可根据客户要求定制
- NetFlow v9
- 支持任何种类的SFP和SFP +（也可以是10 Gbit BASE_T）和QSFP
- 24个10 Gbit和4个40 Gbit

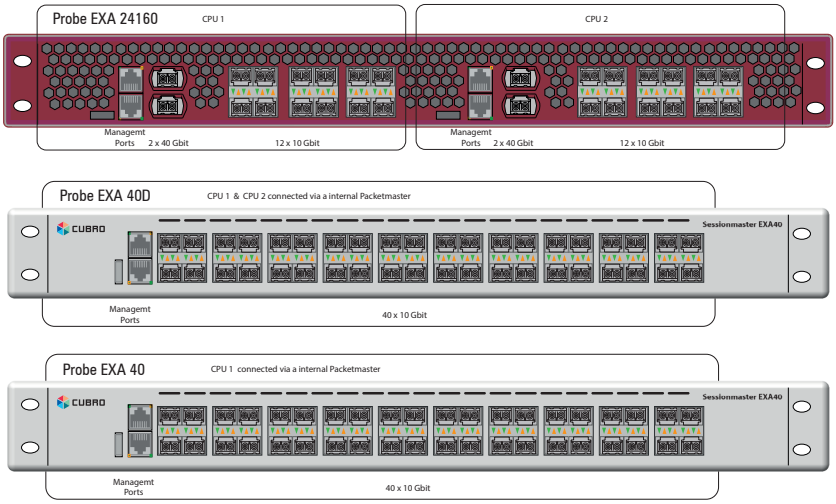
HongKe 虹科

产品功能/特性

识别功能	根据端口，签名和流量类型进行识别 跨包匹配 关联识别（FTP/DNS/bbc-iPlayer/afreecavideo） 非标准端口的HTTP标识
协议识别规则	协议识别引擎：查找优先级最高的应用ID 规则编译器：使用PDL *，最多8K规则生成图形使用PCRE的用户定义规则
其他DPI功能	热插拔规则升级 在数据包以太网标头上标记签名信息
数据包预处理	巨型框架，IP-重新组装 TCP重组，例如乱序数据包，TCP状态跟踪隧道标识（例如GTP/GRE），支持隧道内部的协议处理
分类	6元组ACL规则（IP 5元组+应用ID，最大值：4K） 用操作对应用程序ID进行重新定义以对应用程序进行分类 负载平衡（保留会话/订户的完整性）
流明细记录	在Netflow V9标准中生成流日志
端口EXA241	24 个 10 Gbps / 1 Gbps和 4 个 QSFP 40 Gbps
60配置/通讯	Serial/SSH/Telnet/FTP
EXA24160性能	吞吐量160 Gbps DPI性能60 Gbps 2000万会话同时在线（最多）
CPU	Mips 64 96 Core
MTBF	178,125 hours

（PDL语法是Cubro Regex编译器生成新指纹的语言）

技术数据/规格



操作规格：

工作温度：0ºC至45ºC

储存温度：-10ºC至70ºC

相对湿度：最小10%，最大95%不凝结

机械规格：

尺寸（HxWxD）：W = 440.00mm，L = 660mm，H = 4

4.4mm重量：9.4kg

电气规格：

输入电源：100-240V，2A，47-63 H

最大功耗：400W

认证：

完全符合RoHS

符合CE

Safety - UL 60950-1/CSA C22.2 60950-1-07/IEC 60950-1 (2005)EN 60950-1 (2006)

输出*

1、10、40 Gbit接口可用作TAP或NPB的输入。在EXA40和EXA40D上，探针内建有NPB。在EXA24160上，可以使用外部NPB来负载均衡流量。

输出*

任何端口都可以用作元数据流输出。Netflow CDR还可以通过多个端口发送负载均衡的流量，以减少服务器上的负载。

性能

提供了将近1000多种预配置的指纹应用程序ID

先进的多核CPU设计

每Gbit流量处理的功耗业内最低

管理

管理端口：（1）RJ45 10/100/1000 Mbit

配置（CLI）端口：（1）RS-232 DB9

USB 3.0用于软件更新

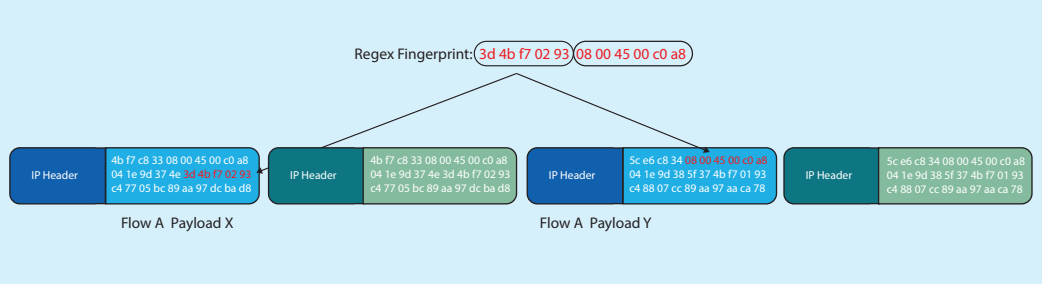
指示

每个RJ45端口：速度，链接/活动

每个SFP +端口：状态，接收，发送，链接

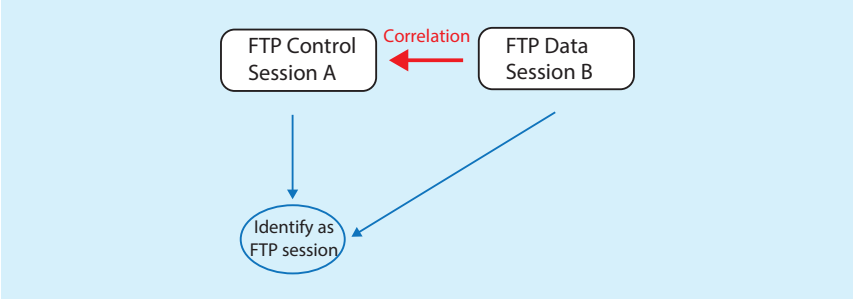
每个设备：电源，状态

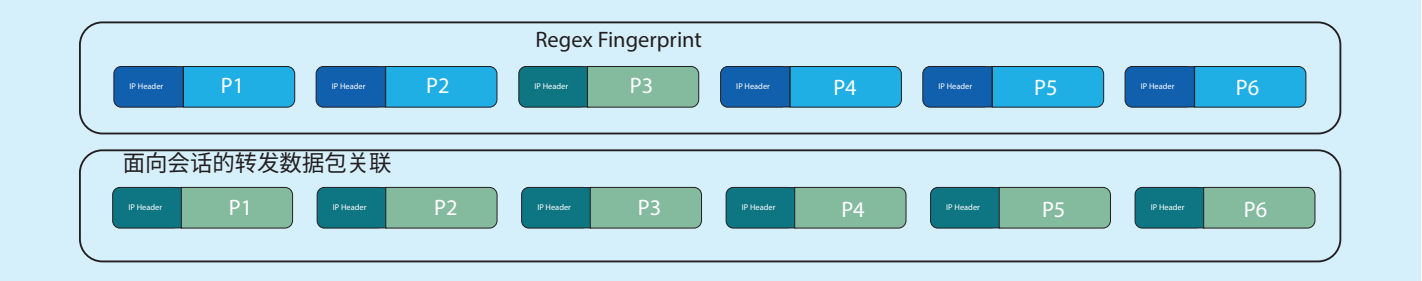
高级功能说明



支持跨包搜索：
例如，签名S分为S1和S2。 S1和S2在两个相邻的 数 据 包 中 ，并 且FlowVista仍可以识别签名S。

相关标识：
关联多会话协议并统一识别结果。

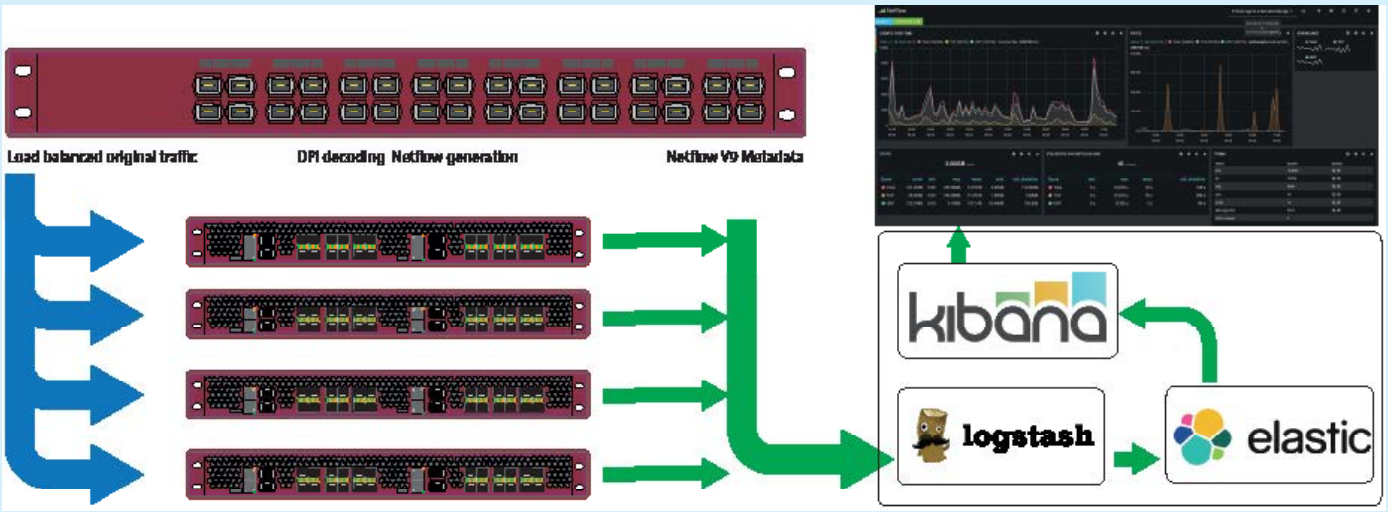




原始数据包标记：
在原始数据包标头的“ MAC” 字段中标记识别信息。FlowVista支持标记缓冲功能。例如：在同一会话中，数据包A在数据包B的前面，数据包B携带签名。当FlowVista识别数据包B携带的签名时，它仍可以使用签名信息标记数据包A。

FDR：
FlowVista可以统计会话的上行链路/下行链路流量，会话状态，开始/结束时间以及协议标识信息。FlowVista以NetFlow V9标准输出统计信息。

典型应用： 大数据开源



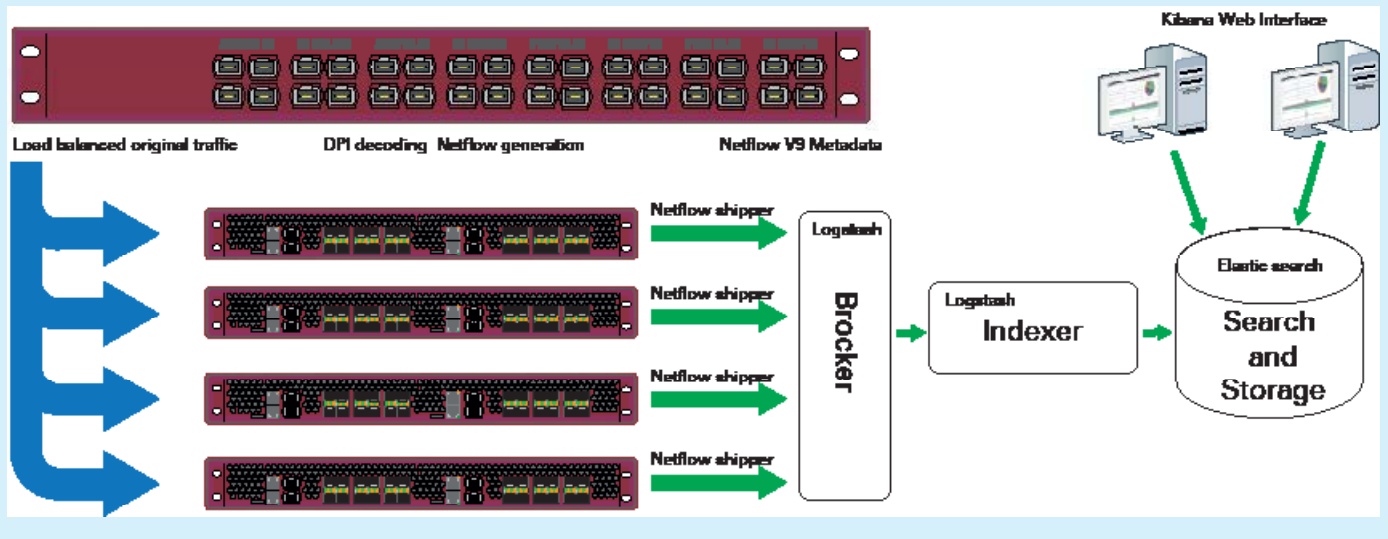
Cubro FlowVista探针还可用于从网络生成元数据，并为大数据应用程序提供数据。作为此类安装的一个示例，图片显示了3个开源应用程序（ELK ore kibana堆栈），用于构建功能强大且灵活的收集器。

Logstash提供许多类型的集中式日志聚合，例如服务器日志以及Netflow。这是一个非常简单的基于消息的体系结构。 Logstash具有配置为与其他ELK组件结合执行不同功能的单个代理。

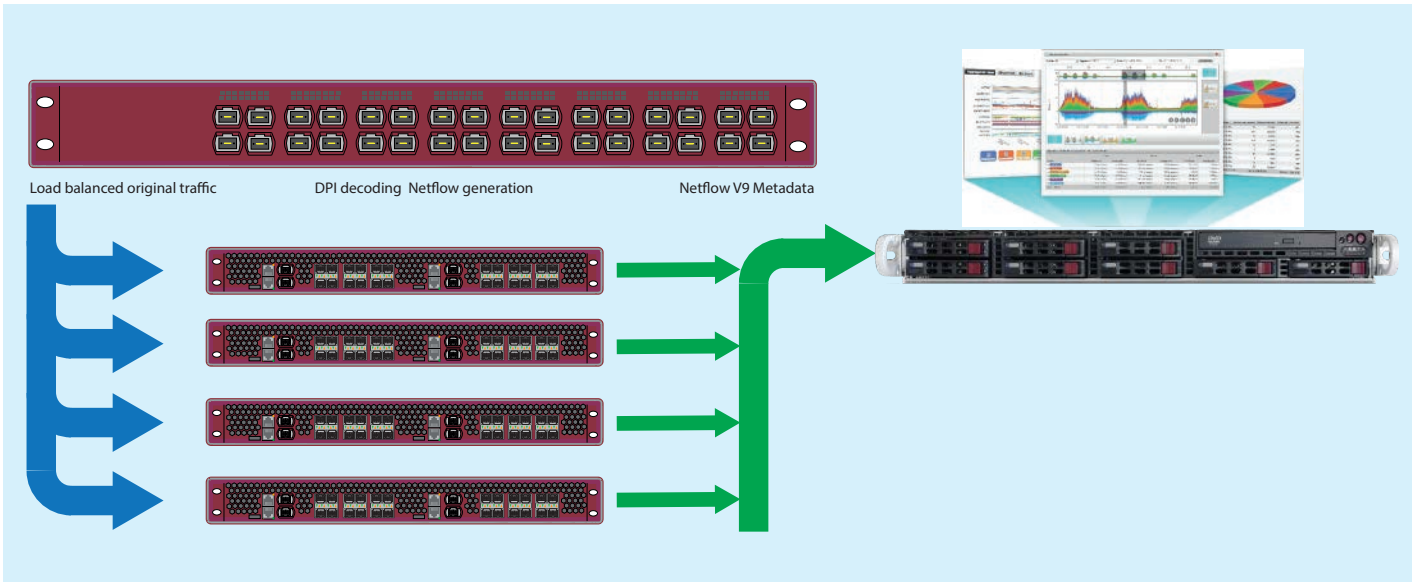
Elasticsearch是一个分布式搜索和分析引擎。它是一个模式自由、全文搜索引擎，具有多语言支持。它提供对地理位置、建议性搜索、自动补充和搜索片段的支持。

Kibana是为Elasticsearch构建的分析和可视化平台。它提供流数据的实时摘要和图表，并具有共享和嵌入仪表板的功能。

还应该提到Marvel和Shield这两个组件，前者用来监视整个系统本身，后者负责ELK的安全功能，例如基于角色的访问控制等等。



典型应用



此图显示了监视大量流量（在这种情况下超过250 Gpbs）的典型解决方案。 通过各种接口通过TAP接收到EX32100的流量。 EX32100将流量聚合，过滤和负载均衡到4个FlowVista探针，每个探针处理60-70Gbps的流量。

探针将流CDR发送到流收集器。收集器是第三方产品。TheNetflow v9是一种通用格式，可以由许多第三方和开放源代码产品处理。

订购信息

产品组成：

- CubroFlowVista探针
- AC/ DC电源
- 欧洲电源线
- （不包括SFP）

Part Number	Description
CUB.FVP-S	FlowVista Probe, single CPU, AC power
CUB.FVP-D	FlowVista Probe, dual CPU, AC power
CUB.FVP-Q	FlowVista Probe, quad CPU, AC power
CUB.FVP-S-DC	FlowVista Probe, single CPU, DC power
CUB.FVP-D-DC	FlowVista Probe, dual CPU, DC power
CUB.FVP-Q-DC	FlowVista Probe, quad CPU, DC power

更多详细信息，请点击网络了解：**www.hongwangle.com**