HongKe 虹科

OMNIA

Power & Versatility for Enterprises

手册

广州虹科电子科技有限公司 | 虹科网络可视化与安全 | www.hongwangle.com | 400-999-3848 | network@hkaco.com

目录

前言.....3

应用案例.....4
- 下一代网络数据包代理(Network Packet Broker).....5
- 托管安全监控.....6
- 网络故障排除和诊断.....7
- 网络性能监控和管理SLA.....8
- Netflow探针.....9
- 更快的事件响应和减少停机时间.....10

Omnia软 件.....11
- PacketMaster功能：L2-L4 可见性.....13
- SessionMaster功能：深度过滤&分析.....14
- AppMaster功能：软件生态系统.....15
  - AppMaster合作伙伴.....15

Omnia 硬件.....16
- Omnia 10.....17
- Omnia 20.....18
- Omnia 120.....19

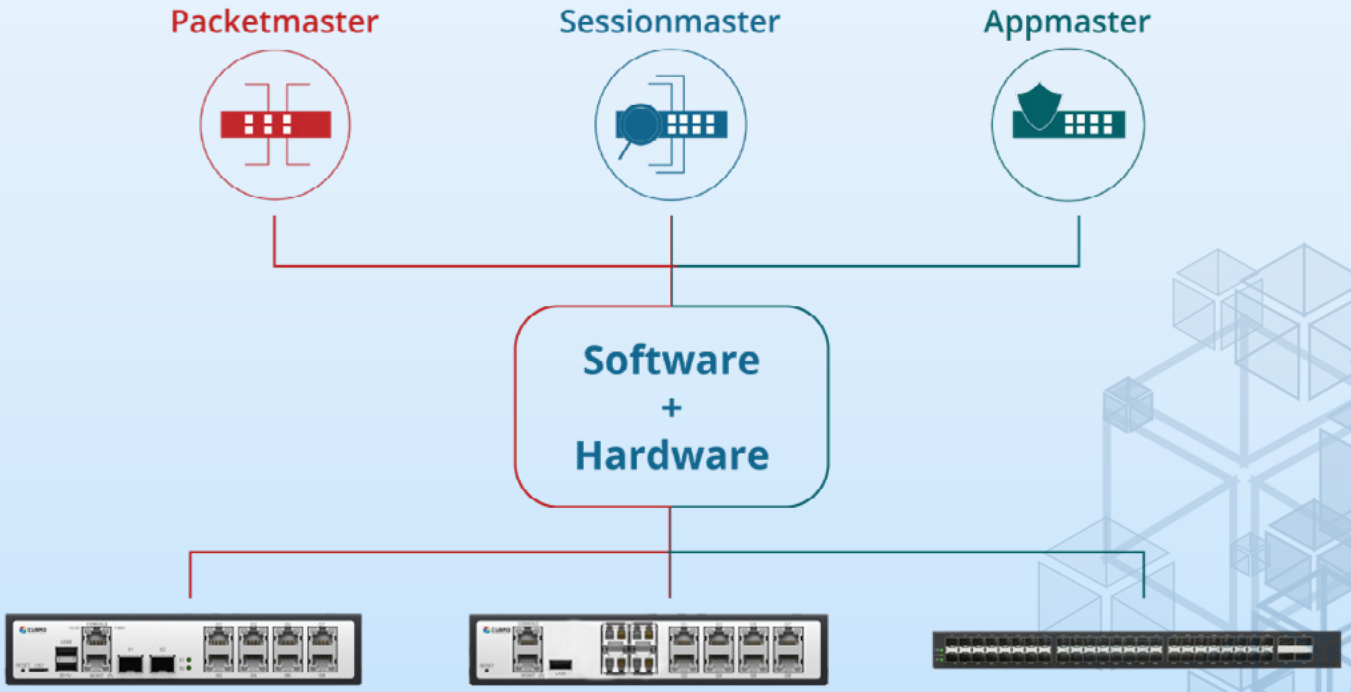
Cubro 优势.....20

其他资源.....21

前言

Omnia系列产品通过融合Cubro在网络可见性方面的经验与Omnia的平台和功能相融合，给客户提供更多的选择和功能。Omnia提供专门制造的硬件，性能从10Gbps到几百Gbps，功能是多年经验和工程设计的成果。

Omnia将高级网络数据包代理中包含的功能与高性能多核CPU结合起来，使众多应用得以实现，包括合作伙伴和开源社区的应用。



HongKe 虹科

应用案例

下一代网络数据包代理(Network Packet Broker)

Omnia系列产品的规模从适合小型或远程办公地点的低成本、入门级产品到高性能的数据中心。每个产品都是下一代数据包代理，具有先进的功能，可以观察流过组织网络的所有流量，并从内部、虚拟和公共云域的任何部分复制相关数据。这些数据将根据第三方网络安全、分析和/或监控工具的条件、时间和方式有效地传递给他们，以确保没有监控“ 盲点” 。

好处：

- 提高了信息技术网络的性能、安全和规划，因为网络工具对所有流量有充分的可见性，使它们能够有效地执行其功能。
- 不再有网络 “ 盲点 ” 。
- 通过部署Cubro低成本、入门级的Omnia10或20产品，可以将以前监控成本不合理的增量小地点纳入网络可见性解决方案中。
- 降低了网络工具的成本，提高了投资回报率(ROI)。
- 最大限度地减少和优化向监控工具的数据馈送，从而减轻了这些监控工具的负荷，延长了它们的使用寿命（不会很快达到容量）。最终，这些工具能够监控以前不同的、速度不兼容的网络和服务。

托管安全监控

2019年全球数据泄露的平均成本为392万，欧元，美国为829万美元，安全团队面临着保护网络免受此类网络威胁的严峻挑战。2020年加速了数字化转型，以支持分散的劳动力和远程业务运营，这些变化使网络更容易受到网络威胁和欺诈。为了使安全团队能够有效地工作，需要网络流量进行全面的洞察。

Omnia产品能够托管软件应用程序，以提供额外的功能，这些功能是对整体NPB功能的增量。从Omnia生态系统或其他第三方应用程序（如开源Zeek）中安装安全监控软件，可提供一个集成的故障安全（fail-safe）网络TAP、NPB、数据包捕获和安全监控设备，可在本地或远程（带外）管理和操作。

好处：

- 通过部署Omnia10 或20，将便捷、低成本的安全监控部署扩展到以前不合理的较小或VIP位置，从而提高了网络安全性。
- 通过部署单个Omnia设备解决方案来替代多个设备解决方案，降低了成本、空间、机架和电源要求。
- 由于Omnia解决方案与多个设备解决方案相比，组件部件较少，因此降低了因安全监控失败而导致网络安全漏洞的风险。

网络故障排除和诊断

进行网络故障排除的人对数据包捕获和分析并不陌生。通常情况下，处理工具是带有协议分析器（如Wireshark）的笔记本电脑，从镜像端口收集流量，或者更好的是与笔记本电脑配合使用小型TAP。

Omnia10将这些功能整合到一个紧凑的集成套装中。此外，Omnia10可以处理超过1Gbps的流量捕获，而对于传统的笔记本电脑设置来说，这需要额外的昂贵硬件。Omnia10的另一个好处是便于远程、带外管理和链路的故障安全（fail-safe）分路，使工程师能够在不同的地点部署一个或多个Omnia，并更有效地诊断问题，或者在较长的时间内搜集数据，而无需留在现场。

Omnia提供了一个集成的故障安全（fail-safe）网络TAP、NPB、数据包捕获和网络故障诊断设备，可在本地或与远程（带外）进行管理和操作。该设备运行Omnia 软件协议栈和Omnia生态系统中的第三方应用程序，或者工程师可以安装运行在Omnia的ARM CPU上的开源软件。

好处：

- 可见性在一个设备里 - 故障诊断和监控工具的流量比以前减少了60%。
- 通过部署Omnia10 或20，将便捷、低成本的安全监控部署扩展到以前不合理的较小或VIP位置，从而提高了网络安全性。
- 通过部署单个Omnia设备解决方案来替代多个设备解决方案，降低了成本、空间、机架和电源要求。
- 由于Omnia解决方案与多个设备解决方案相比，组件部件较少，因此降低了因安全监控失败而导致网络安全漏洞的风险。

网络性能监控和管理SLA

网络是当今任何企业的支柱。然而，现代网络非常复杂，需要正确的工具来避免任何数据丢失或防止最终可能导致收入损失的安全漏洞。网络性能监控使网络团队能够主动排除网络速度变慢或故障。

Omnia有助于主动嘉能可网络，为用户提供更好的服务质量。无论是作为内部单位运营还是为外部客户提供服务，网络运营团队通常都要遵守设定为99.99%正常运行时间的服务级别协议(SLA)。达到SLA，终端用户或客户才会满意。如果达不到SLA，人们就会开始提出尖锐的问题。

Omnia产品能够托管软件应用程序，以提供网络数据包代理（NPB）功能的附加功能。使用Omnia生态系统或其他第三方应用程序（如ntop）安装性能管理监控软件，可提供一个集成的故障安全（fail-safe）网络TAP、NPB、数据包捕获和网络监控设备，可在本地或远程（带外）管理和操作。

好处：

- 通过部署Omnia10 或20，将便捷、低成本的安全监控部署扩展到以前不合理的较小或VIP位置，从而提高了网络安全性。
- 通过部署单个Omnia设备解决方案来替代多个设备解决方案，降低了成本、空间、机架和电源要求。
- 通过减少内部和外部的SLA违规行为，提高网络服务的可靠性。

Netflow探针

Omnia平台可以作为NetFlow探针进行整合和部署。Omnia的被动分流功能可用于将Omnia内联到网络链路中，然后从网络链路中产生Flow数据。Omnia是从网络设备中获取NetFlow数据的一种经济方式。Omnia可以部署在多个站点，并将其NetFlow数据发回中央采集器进行分析，以增强组织的监控能力。

好处：

- 减少网络工具收集的数据量，提高其效率。
- 通过关联数据识别网络设备的错误配置。
- 通过发现问题来增强网络安全和流量分析。

https://hongwangle.com/wp-content/uploads/2020/12/CUB-Omnia-Netflow-IPFIX-DPI-Probe-ZH.pdf

更快的事件响应速度和更短的停机时间

根据Ponemon Institute的年度报告，计划外停机的平均成本是每分钟8850美元。避免网络停机的第一步是监控网络的健康状况，第二步是在事故发生时迅速做出反应。

Omnia结合了直接在磁盘上执行滚动流量捕获以进行历史分析的能力。在捕获过程中还对信息进行了索引，以快速识别和提取感兴趣的流量。有了这些功能，Omnia在排除网络中断和潜在数据泄露的故障时，提高了事件响应的效率。

没有意识到网络漏洞或链路性能不佳的企业面临受损和潜在收入损失的风险。必须对网络进行实时分析和监控，才能发现任何潜在问题和机会，以优化基础设施。Omnia可以有效地捕获100%网络流量，进行实时和历史分析。网络监控是一种高效经济的方式，可以保护您的网络资产并节省宝贵时间和金钱，可以将这些时间和金钱用于其他重要的IT目标。

Omnia还可以执行DPI过滤，它可以阻止不需要的应用程序，以减少非业务关键网络流量消耗的带宽，并提高网络优化。

好处：

- 增加网络服务正常运行时间
- 提高效率
- 提高业务灵活性
- 通过网络优化降低运营成本

HongKe 虹科

Omnia软件

Omnia附带几个不同的软件包，用户可以选择。下表列出了这些软件包以及不同硬件平台的可用性。由于Omnia120的双CPU架构，它可以配备2个软件包，其中一个必须是Sessionmaster软件。

SW Package #	SW package	描述	Omnia10	Omnia20	Omnia120
1	聚合TAP	8 x Copper to 2 x 10 聚合，没有过滤	x	x	
2	聚合TAP + 捕获	8 x Copper to 2 x 10G & 2 x 1G 聚合+ 实时 & 滚动捕获，没有过滤， 但是使用了过滤捕获	x	x	
3	Sessionmaster	L2-L4 Packetmaster + L7 Sessionmaster with advanced features	x	x	x
4	Appmaster	在Linux环境下运行Cubro和合作伙伴的应用程序	x	x	x

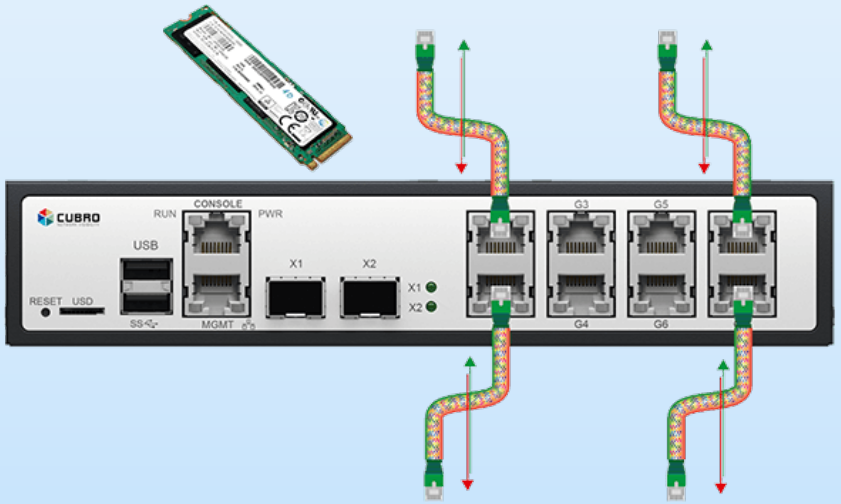
Omnia系列的最大可能组合如下表所示：

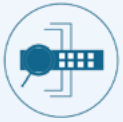
Omnia/SW	Option 1	Option 2	Option 3	Option 4
Omnia10	1	2+4	3	4
Omnia 20	1	2+4	3	4
Omnia 120	3	3+3	3+4	-

PacketMaster功能: L2-L4可见性

PacketMaster功能栈包含了传统的网络数据包代理功能，如任意对多或多对任意的流量转发、过滤和拦截、报头修改和剥离、负载均衡、隧道终止等。

- ACL内联过滤
  - 通过OSI L4标准过滤L2上的流量
  - 向一个或多个接口转发指定的流量
  - 丢弃指定的流量
- 负载均衡
  - 从多种对称或非对称负载均衡算法中选择
- GRE termination
- ERSPAN termination
- VXLAN termination
- 时间戳
- 数据包切片
- 隧道报头移除
- VLAN增加/修改/分割
- MAC修改
- 偏移剥离
  - 为特定应用创建自定义报头剥离偏移
- GRE和VXLAN活动隧道端点





SessionMaster功能: 深度过滤&分析

SessionMaster的功能栈借鉴了Cubro的先进的网络数据包代理。这些功能包括流量重复数据删除、正则表达式搜索、数据脱敏（数据屏蔽）、SSL/TLS解密等。在当今的网络中，在许多情况下，仅仅过滤L2-4层的流量已经不够了。Sessionmaster的功能为尖端的部署提供了必要的深度可见性。

- ACL关键词过滤
- 流量关联
- 隧道报头移除
- 数据脱敏/数据屏蔽
- TCP重排序和数据包片段重构
- 内联或SPAN端口上的重复数据删除
- 在光纤TAP后被动进行重复数据删除
- SSL/TLS 解密
- Netflow 生成
- 元数据输出器: Netflow / Netflow - DPI / DPI

AppMaster功能: 软件生态系统

AppMaster功能栈提供了一个完整的Linux环境来运行Cubro和我们的合作伙伴的应用程序，以及定制软件和各种开源项目。通过访问PacketMaster和SessionMaster堆栈的流量，潜在的应用案例是无穷无尽的。Omnia平台上的AppMaster有可能在单一设备中取代整个机架设备的功能。

- DPI分析
- Netflow 搜集器
- SIEM
- 数据包捕获
- 协议分析
- IDS/IPS
- 威胁搜寻
- 内容重构
- 应用性能分析
- 合法拦截
- DDoS检测&缓解

AppMaster合作伙伴

HongKe 虹科

Omnia硬件

Omnia 10

Omnia 10有2组端口。G1-G8是带有旁路功能的10/100/1000 Mbit RJ45端口，可作为4个链路铜分路器或8个SPAN端口。 X1-X2是2 x 1/10G端口。

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 * 10 GbE 8*GbE (RJ45)
Internal extended I/O	1* mini PCIe x1 Gen 3 2* M.2 (PCIe x4 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 (WxHxD) mm	335 x 220 x 44.4
Power consumption	30 W

Omnia 20

Omnia 20有2组端口。G1-G8是带有旁路功能的10/100/1000 Mbit RJ45接口，可用作4个链路铜分路器或8个SPAN端口。X1-X4是2 x 1/10G和2 x 1G端口。

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)
USB	2 * USB3.0 (Type A)
Bypass	Support 4 groups Copper Ports
Port	2 * 10GbE 2 * 1 GbE (SFP) 8*GbE(RJ45)
Internal extended I/O	1* mini PCIe x1 Gen 3 2* M.2 (PCIe x4 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 (WxHxD) mm	335 x 220 x 44.4
Power consumption	30 W

Omnia 120

Omnia 120是面向大型企业，它有48 x 1/10G SFP+和 4 x 40/100G QSFP28端口。.

CPU	2 x Multi-Core ARM CPU
Switch	Cavium Xpliant
Memory	DDR4 ECC UDIMM
MGMT	10/100/1000 Base-T RJ45
Console	1 * RS232 (RJ45)
Port	48 * 1/10GbE SFP+ 4 * 40/100GbE QSFP28
Power Supply	AC 100 - 264 or DC 48V
Size (WxHxD) mm	440 x 660 x 44.4
Power consumption	400 W

Cubro优势

提高网络性能和安全态势

改善网络服务正常运行时间、可用性和服务质量

提高网络和网络工具的优化和投资回报率

提高IT操作的灵活性

简单，易于部署的解决方案，快速获得收益

入门成本低

低总拥有成本和高投资回报率的解决方案

其他资源

https://hongwangle.com/cubro/omnia/