HongKe 虹科

虹科网络流量可见性及监控解决方案产品目录

hongwangle.com

1
ONE

2
TWO

3
THREE

虹科网络流量可见性及监控解决方案产品目录

网络可见性

流量复制——网络分路器

- 监控解决方案的可靠数据包来源
- 为什么是网络分路器而不是SPAN?
- 虹科流量复制（网络分路器）产品列表
  - 铜分路器
  - 光分路器
  - 聚合分路器
  - 再生光纤分路器
  - 便携USB分路器——Profishark
    - > *Profishark长期捕获解决方案*
  - 虚拟分路器

流量优化——TAP汇聚分流设备

- 为什么需要？——增强安全和性能监控工具

旁路解决方案

网络流量监控

一体化网络监控设备-Allegro

网络端到端和应用性能可视化-LiveNX

软件网络流量监控分析方案-ntop

虹科网络流量可见性及监控解决方案产品目录

伴随着IT与互联网应用的快速发展，如物联网设备规模性增长，5G商业落地等，网络流量迎来爆炸性增长。安全方面，网络边界模糊对流量监测带来了一定的挑战，同时流量的发展特性对企业安全也提出了一定的挑战，如恶意流量和加密流量的发展。

网络流量分析技术NTA和其发展而来的网络检测和响应（NDR）应运而生。

NTA/NDR主要分析南北向和东西向的流量，通过使用工具组合来检测攻击，包括机器学习、行为分析、危害指标和回顾性分析。

网络可见性对保证NTA/NDR工具性能至关重要。网络可见性方案可以复制来自网络任何部分的相关数据，包括内部、云和虚拟环境中的数据。通过网络汇聚分流设备，数据可被有效地传递到网络监控，安全和分析解决方案，以确保没有“盲点”。

虹科电子提供网络流量可见性及网络流量监控解决方案。

网络可见性

流量复制——网络分路器

在物理和虚拟网络中的关键捕获点访问网络流量

- 监控解决方案的可靠数据包来源

网络分析始于以可靠和安全的方式获得可操作的数据。虽然有很多方法可以捕获实时网络上的数据包，但往往有严重的弊端，如数据包丢失、数据包失序，或使用易被攻击的设备。所有这些都直接影响到分析的质量和网络本身的安全。

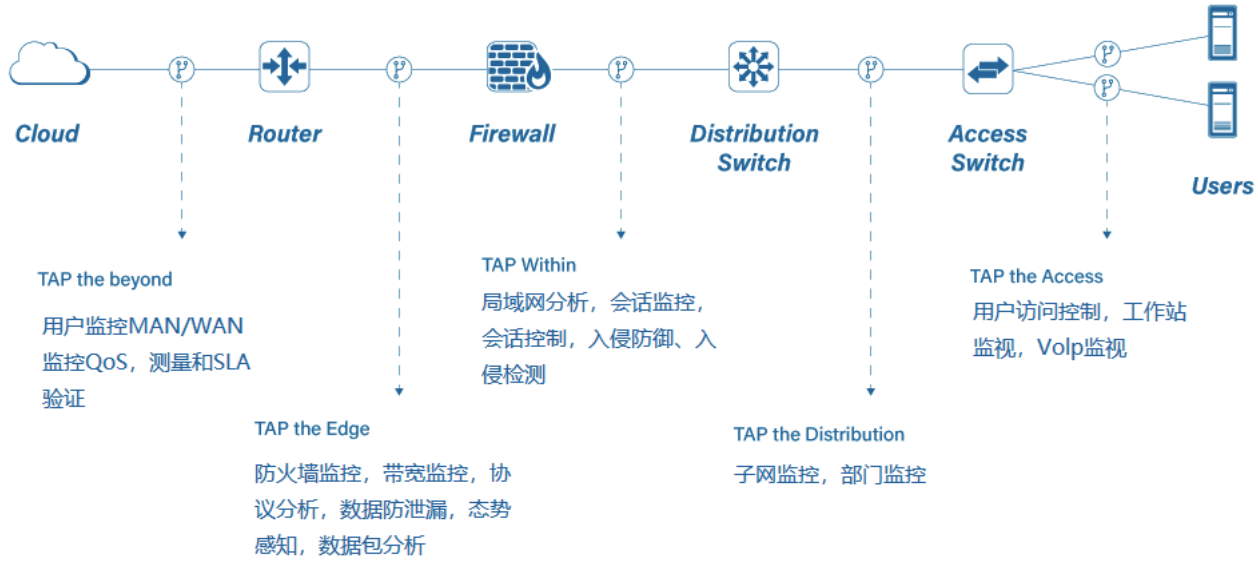
最佳做法是部署网络TAP（测试接入点，网络分路器）作为访问网络流量的关键方法。网络分路器是部署在网络基础设施中两点之间的关键位置的硬件设备，如路由器、交换机或防火墙，这些位置需要进行数据访问以进行监控或故障排除。在虚拟环境中，虚拟TAP或vTAP被安装在虚拟化服务器上，提供对东西向流量的完全访问和可见性。

- 为什么是网络分路器而不是SPAN?

专门设计的网络分路器比交换机端口分析器（SPAN）端口更可靠，特别是在高数据速率下。与使用SPAN端口监控网络相比，网络分路器具有明显的优势，如以线速提供对所有大小和类型的数据包的访问，向监控端口提供所有流量的精确拷贝，并将监控设备与网络隔离，以减少数据泄露的风险。

网络分路器使您能够:

- 实现对你的物理和虚拟网络的完全访问和可视性
- 在高速网络中获得故障安全、永久的内联网络访问实时流量
- 保护内联安全工具的网络链接可用性
- 消除访问网络流量时的单点故障风险
- 从多个内联链接或带外链接中提供无损的流量聚合



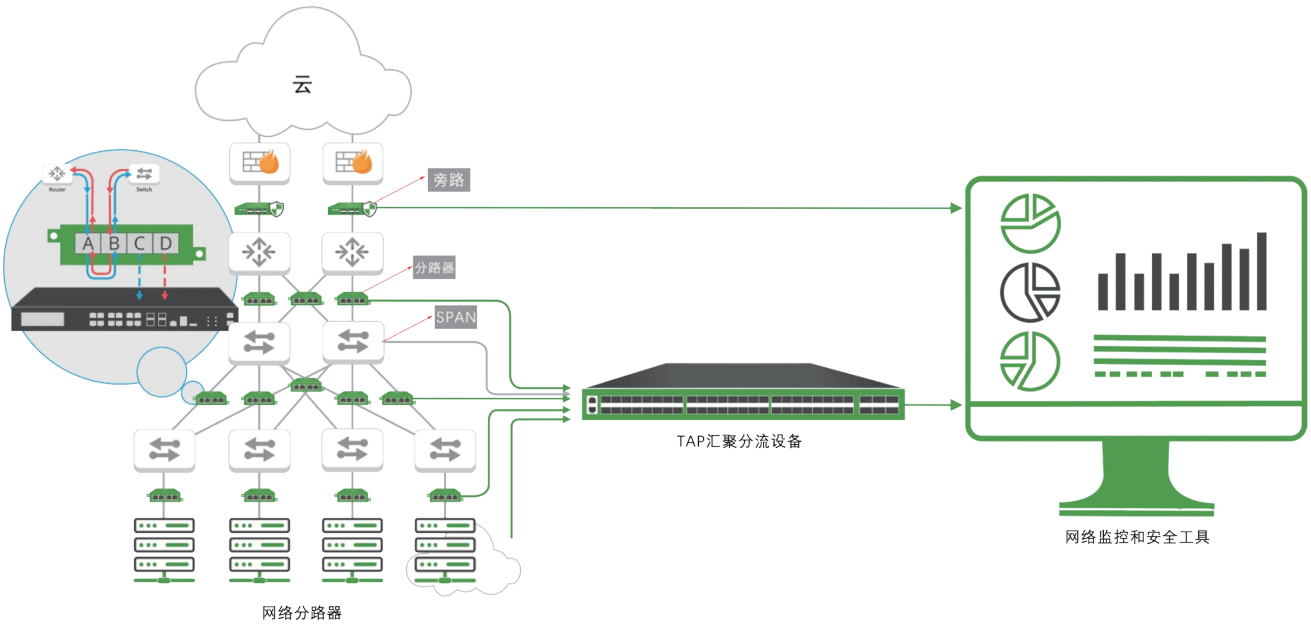
- 虹科流量复制（网络分路器）产品列表

- ***铜分路器***

用于在线监测10M/00M/1G/10G网络的故障安全访问

虹科铜分路器通过创建全双工10M/100M/1G/10G流量的精确副本，在不影响网络链接的情况下，为您的网络提供完整的访问和可见性。虹科铜分路器不会给网络带来任何故障点。冗余电源设计，如果第一个电源不可用，即激活第二个电源，在完全断电的情况下，虹科铜分路器通过立即切换到完全被动模式来保证该链路保持运行。

为了保持网络连接并防止流量中断，所有虹科被动铜分路器都具有无中断故障安全功能 - 一种快速切换机制，由于使用高速继电器，可确保网络链路的恢复时间非常短，并允许网络流量通过分路器，即使电源中断也是如此。



* 微信扫码咨询更多产品详细参数信息

型号	网络链路	监控链路	速度	尺寸大小	安装/电源选项
HK/C1R-100	1	1	10/100Mbps	1/3U	机架/便携/DIN 导轨
HK/C20-100	20	20	10/100Mbps	1U	机架
HK/C1R-1G	1	1	10M/100M/1G	1/3U	机架/便携、48V/备用电池
HK-C8-1G	8	8	10M/100M/1G	1/3U	机架
HK/C1-1G-RG2	1	2	10M/100M/1G	1/3U	机架
HK/C1R-10G	1	1	10M/100M/1G/10G	1/3U	机架
HK/CS1G-C4G	1（SPAN）	4	10M/100M/1G	1/3U	机架
HK/CBR.TAP-10/100-R3	1	1	10/100Mbps	1/3U	机架
HK/CBR.FLEX-T100	1(最多 21)	2（42）	10/100Mbps	3U	机箱

- ***光分路器***

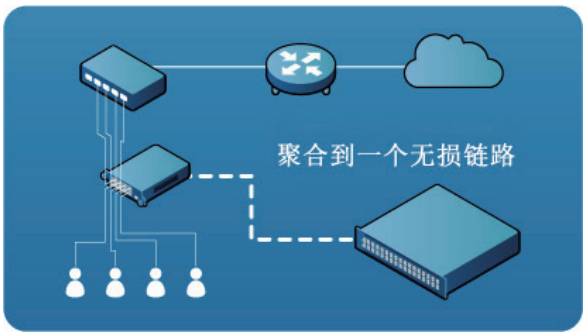
虹科光纤分路器为监控1-400 Gbps光纤网络提供安全的内联网络访问。通过分流流经网络链路的光，光纤分路器可提供准确的数据副本，以便实时监控和分析，而不会中断网络。被动光纤分路器不需要电源，因此在网络中部署时不会出现故障点。

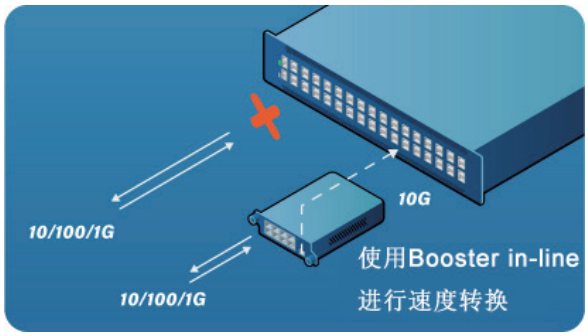
虹科光纤分路器在装配前后都经过了我们的专家团队的广泛测试，有各种分流比和配置可供选择，以满足您的特定要求。

* 微信扫码咨询更多产品详细参数信息

高密度光分路器模块	LC 光纤分路器	MPT/MPO 分路器	BiDi 光纤分路器	SC 光纤分路器
				
MOD-TAP 是一种模块化光纤分路器解决方案，支持从 100Mbps 到 400Gbps 的不同网速。MOD-TAP 提供了灵活性，允许您在单个机箱组合中具有不同速度的分路器模块。1U 机箱中最多可支持 24 个模块。	非侵入式、无源 LC 光纤分路器，为监控 1-100G 光纤链路提供永久的在线网络接入，并以灵活的分光比提供低插入损耗。	虹科 MTP 光纤分路器是高密度 MTP 光纤分路器，可提供对 40/100G 光纤网络的在线监控，确保您的 40GBASE-SR4、100GBASE-SR4 和 100GBASE-SR10 网络的完全可见性，而不会丢失数据包。	BIDI 光纤分路器旨在为监控双向光纤网络提供永久的在线网络访问。虹科 40/100G BiDi 分路器可让您全面查看双工 40/100G 思科双向链路。虹科双向 PON 分路器可监控单工双向单模连接。	虹科 SC 光纤分路器是高性能设备，可安全可靠地访问高速网络中的实时流量。虹科 SC 光纤接头对网络完全不可见，不会给网络带来故障点。

- ***聚合分路器***





聚合分路器用于将来自多个内联链路或带外链路的流量无损聚合到单个输出中（M-1），从而优化监控工具上端口的使用。

虹科Booster还可以用作速度转换器，使您可以将支持不同速度的工具连接在一起。例如，可以在不支持10G以下速度的分析工具上提供10M、100M、1G的支持。

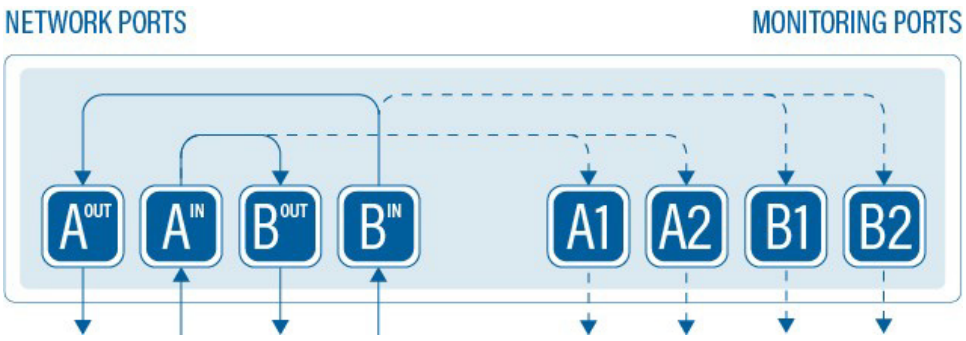
* 微信扫码咨询更多产品详细参数信息

Booster in-line	Booster SPAN
	
Booster 内联千兆铜聚合分路器，将 4 个 10/100M/1G 故障保护内联链路连接到 1 个 1/10G 输出端口（4-1）。	Booster SPAN 聚合分路器，将 8 个 10/100M/1G 带外连接（SPAN）连接到 1 个 1G/10G 输出端口（8-1）。

- ***再生光纤分路器***

再生光纤分路器允许对光纤网络进行分路，同时减轻因分路而导致的光信号的功率降低。LC再生分路器对网络和监控端口的信号进行再生。

双LC再生分路器和四LC再生分路器对监控端口的信号进行再生，以提供多份网络流量，同时只分光一次网络链接的信号。这在关键网段需要一系列安全和合规工具同时监控的情况下非常有用。



* 微信扫码咨询更多产品详细参数信息

产品	型号	网络：监控链路数	分光原理
	HK/F1L-AT	1：1	通过在网络和监视端口上再生信号来减轻因分光而导致的光信号的减弱
	HK/F1L-RG2	1：2	只进行一次分光，然后复制和再生监控信号，可连接到 2 个独立监控系统
	HK/F1L-RG4	1：4	只进行一次分光，然后复制和再生监控信号，可连接到 4 个独立监控系统

- ***便携USB分路器——Profishark***

ProfiShark是便携式流量捕获设备，可在部署它们的任何位置提供快速数据包级洞察。ProfiShark具有不受数据包速率限制的捕获功能和高质量的硬件时间戳，可提供高保真的捕获文件，为故障排除或网络取证提供了理想的起点。专为轻松、非侵入性流量捕获而设计。

与性能较差的方案(如交换机上的SPAN端口或笔记本电脑上的直接捕获)相比，ProfiShark提供了有价值的改进。它们可以可靠地洞察网络，确保分析质量，优化工作流程，而不会丢弃任何数据包。

通过USB连接到主机PC或笔记本电脑，内联或带外流量可以直接转发到数据包分析软件(如Wireshark)，或存储到磁盘。为确保最佳网络保护，受监控的网络与管理界面在物理上是分开的。捕获控制和硬件设置可以通过附带的ProfiShark管理器应用程序进行管理。

Profishark能够捕捉TSN、EtherCAT、Profinet等工业现场协议。

* 微信扫码咨询更多产品详细参数信息

产品	说明	型号	参数
	ProfiShark 1G和10G可以捕获任何流量、任何大小和类型的帧、内联或跨区，以便使用Wireshark或任何主要软件分析器进行分析和监控。随附的ProfiShark管理器软件提供附加信息、统计数据以及配置和捕获选项。	HK/C1AP-1G	2×RJ45输入 USB3.0输出 69 x 124 x 24 mm
		HK/C1AP-10G	2×SFP/SFP+输入 USB3.0输出 105 x 124 x 26 mm
	ProfiShark 1G+和10G+的GPS/GLONASS功能可以用准确的UTC时间戳标记数据包。ProfiShark 1G+和10G+还可以接收或生成PPS信号，从而在各种拓扑中实现精确的时间戳同步。	HK/C1AP-1G2	2×RJ45输入 USB3.0输出 1×SMA PPS输入 1×SMA GPS输入 105 x 124 x 26 mm
		HK/C1AP-10G2	2×SFP/SFP+输入 USB3.0输出 1×SMA PPS输入 1×SMA GPS输入 105 x 124 x 26 mm
	ProfiShark 100M专为捕获10/100M以太网流量而设计。它是排除实时工业以太网协议故障的完美工具。这款袖珍便携式流量捕获设备为您提供监控工业网络所需的所有灵活性和易用性。	HK/C1AP-100	2×RJ45输入 USB3.0输出 69 x 124 x 24 mm

> *Profishark长期捕获解决方案*

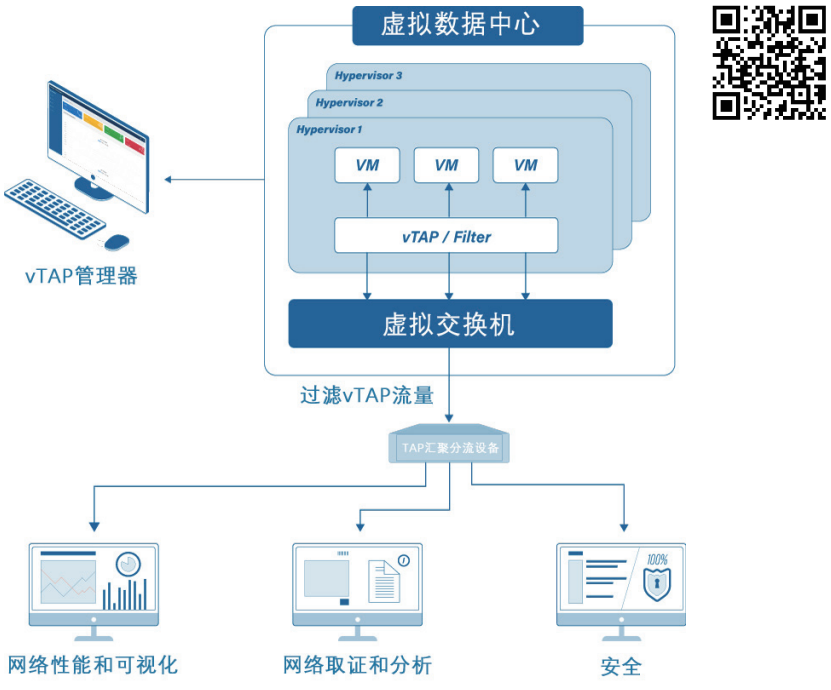
ProfiShark长期捕获解决方案的设计考虑到了灵活性。
长期捕获功能与为您的特定需求量身定做的NAS存储相结合，
可轻松捕获运行中的间歇性问题。

- ***虚拟分路器***

——全面了解您的虚拟网络

虚拟分路器为安全、可用性和性能监控提供虚拟机流量(包括虚拟机间)的完全可见性。在十年的时间里，服务器虚拟化的使用已经成为一种标准的行业实践。这一转变极大地提高了世界各地公司的IT效率，得益于更高的可扩展性、高可用性和更强的工作负载便携性。企业现在可以用更少的钱做更多的事情。

这种转变还意味着您需要一种新的、可扩展且易于管理的方法来全面了解(虚拟机之间)流量，以便监控性能、安全性和可用性。要获得虚拟流量的可见性并将过滤后的网络流量转发到网络安全和网络监控工具，您需要虚拟分路器。



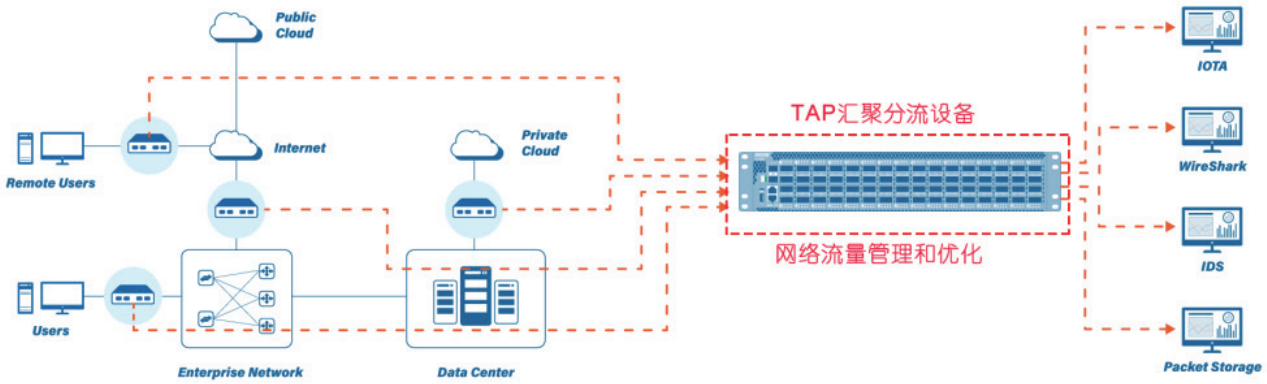
流量优化——TAP汇聚分流设备

- 为什么需要？——增强安全和性能监控工具

随着5G、SD-WAN、虚拟化和物联网等转型技术的应用，网络变得比以往更加复杂。今天对服务提供商和企业的数据要求是，他们必须能够实时查看所有的数据和应用，以保护和管理其不断增长的网络和流量需求，同时提高生产力，并随时注意攻击和泄漏。网络安全漏洞和关键应用的性能问题给了公司很多理由来监控他们的网络。为了获得网络的完整概览，在架构中有许多点需要访问流量；例如：在客户端、在网络基础设施、在边缘、在数据中心和在云中。

然而，在许多情况下，这导致了更多的分路器连接超过了监控工具的处理能力。这时，TAP汇聚分流设备为监控平台提供了一个额外的层，它有助于有效地聚合和分配正确的流量给正确的工具。汇聚分流设备被放置在监控和安全工具与网络分路器或镜像/SPAN端口之间。它们协调来自多个网络链接的流量，并能执行先进的智能流量管理，以确保监控工具收到适当的数据包。部署TAP汇聚分流设备增加了一个智能层，以优化监控架构，提高监控和安全工具的性能。汇聚分流设备帮助您：

- 获得对你的物理和虚拟网络的完全可见性
- 通过先进的过滤功能精简监控和安全工具的数据，降低成本和复杂性
- 提高安全和监控工具的利用率和生产力，以获得更好的投资回报率
- 轻松扩展您的网络基础设施，随着网络的发展，灵活部署或有效升级您的工具



汇聚分流设备（NPB）可以看作为数据中转站，能够确保监控和安全设备全面了解网络流量，并确保这些工具以最高效率运行。虹科TAP汇聚分流设备集成了流量聚合、流量复制、过滤、负载均衡、标头修改等功能。更高级的汇聚分流设备还支持深度数据包检查（DPI），这是一种高级监视技术，常用于电信公司的应用。

* 微信扫码咨询更多产品详细参数信息

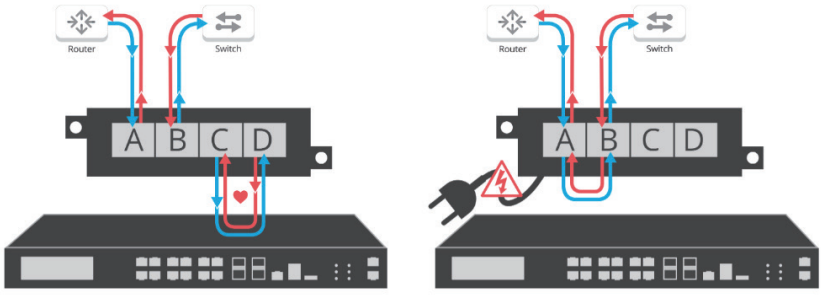
端口数	过滤功能	解封装	其他功能
高达 64×100G/40G QSFP*	L2，VLAN，EtherType，IPv4，IPv6，L4，RegEx，数据包类型，GTP inner IP，VxLAN ID，分段 IP 包，IMSI	VLAN，GRE，MPLS，ERSPAN，GTP，VXLAN，思科 FabricPath 等	数据包切片，NetFlow/IPX、重复数据删除、数据掩码、时间戳、分段重组，FEC， TXForce 等

旁路解决方案

- 旁路交换机

- ***简介***

旁路（Bypass）交换机/TAP是提供不间断服务的故障保护、高可用性解决方案的重要工具。当需要高可用性时，它是内联网络、安全和监控工具的必备工具。



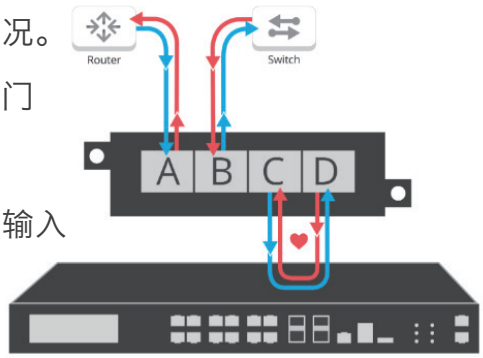
旁路交换机是专门为解决导致网络中出现单点故障（SPOF）的“嵌入”式工具的问题而开发的。如果内联设备不可用，则会绕过该设备，并在发生故障的工具两端自动转发流量。

- ***应用场景***

在网络中设计内联安全工具时，引入网络旁路技术是避免昂贵的网络停机时间的最佳方法。简而言之，旁路交换机（也称为“旁路TAP”）提供了管理内联工具可用性的能力，即在不断开网络可影响业务可用的情况下完成设备维护或升级。

在不能停机的时候，如果工具发生故障，旁路交换机可以快速解决问题，绕过故障工具，并保持网络正常运行或故障转移到高可用性（HA）解决方案。

- ***内部原理***



心跳数据包是一种软检测技术，用于监控内联设备的运行状况。旁路交换机无需依赖于网络与工具的直接连接，而是经过专门设计用于来回的传递心跳数据包来检测所连接设备的问题。心跳包由旁路交换机添加到数据，并且都发送到串联设备的输入端口。内联设备执行其任务，然后通过心跳将数据发送回旁路交换机。旁路交换机会从数据中剥离心跳数据，这些数据会从交换机中发送出去并返回到实时网络中。

心跳数据永远不会发送到真实网络中。如果未收到从旁路交换机发送的心跳信号，表明设备由于某种原因处于脱机状态，则交换机将自动旁路该设备，即使设备处于脱机状态也可以保持网络正常运行。这样就没有网络停机时间也没有单点故障。

- ***应用优势***

虹科旁路交换机为内联主动安全设备(如入侵防御系统(IPS)、下一代防火墙(NGFW)等)提供故障安全接入端口。旁路设备部署在网络和安全设备之间，在网络和安全层之间提供可靠的分隔点。它还可以在多个设备之间实现网络流量负载均衡，从而为设备故障提供额外的服务恢复能力。使用旁路交换机可为网络和安全工具提供全面支持，而不会有网络中断的风险。

- 当内联设备发生故障时，保持网络流量畅通。
- 允许在不影响网络流量的情况下拆除或维修在线设备。例如，可以将IPS脱机，以便进行升级、维护或故障排除。
- 在线设备可以从一个网段移动到另一个网段，而不影响网络流量。

- ***对比内置旁路***

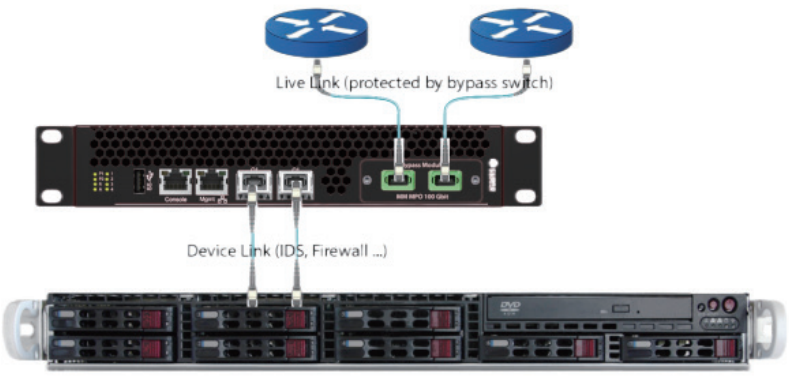
设备可能具有内部旁路功能，但是添加此功能的成本很高，并且仍然缺外部旁路交换机相关的关键功能，包括：

- 管理隔离-无维护窗口
- 操作隔离-加速停机的问题解决，而不会影响网络连接
- 工具沙箱-测试或部署新工具
- 网络弹性-灵活旁路并保持网络正常运行，或故障转移到高可用性[HA]解决方案
- 在线升级-在不中断网络的情况下进行设备的维护或者升级

- 解决方案

- ***内联旁路***

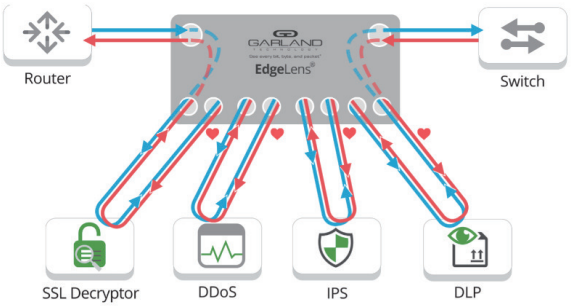
最常用的解决方案是单个内联设备旁路解决方案。如果检测到中断，旁路交换机将绕过连接的硬件设备，从而有效地从链路中移除中断。当旁路交换机检测到串联硬件设备已恢复时，链路将自动重新建立。



- ***管理内联工具链***

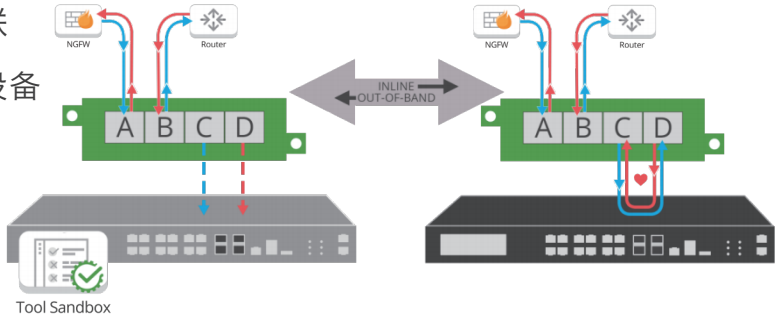
管理多个安全解决方案的 IT 团队需要一种简单的方法来连接他们所有的内联和带外工具，这样他们才能有效地保持网络正常运行并同时保持安全。

虹科旁路交换机允许您通过多个内联工具传递流量，同时能够通过旁路心跳独立监控每个内联工具的健康状况。在心跳失败的情况下，您可以手动或自动将内联设备移至带外以进行管理、更新或优化。



- ***内联设备生命周期管理***

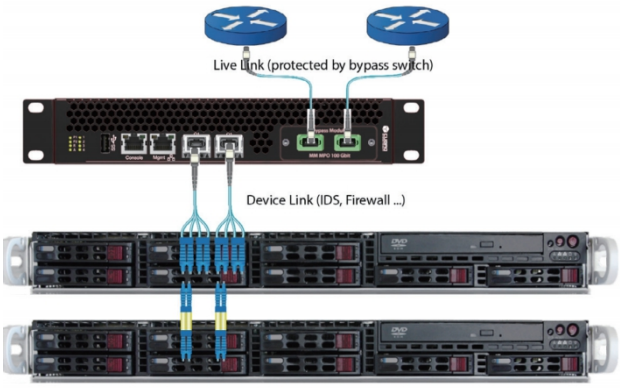
利用外部旁路交换机，而不依赖于内联工具中的旁路功能，可提供实现内联设备的生命周期管理的独特功能。从沙箱部署新工具到轻松进行工具进行更新，安装补丁，进行维护或故障排除以优化和验证，然后再推回内联，外部旁路交换机迅速成为任何内联工具的重要补充。



在不影响网络可用性的情况下，使用实时数据包数据在实际环境中对新工具进行沙箱测试或试运行，从而能够在将其实时部署到网络中之前对其进行带外评估和优化。被测试的工具使用与生产环境相同的数据类型，而不是测试数据，从而增加了测试的真实性。

- ***旁路负载均衡***

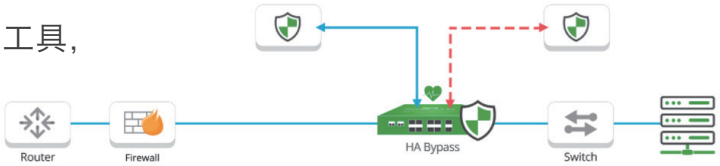
在某些情况下，由于性能问题，内联设备肯无法支持100Gbit。在这种情况下，旁路可以支持设备端口的L3负载均衡。作为输出，支持10 Gbit和25 Gbit。



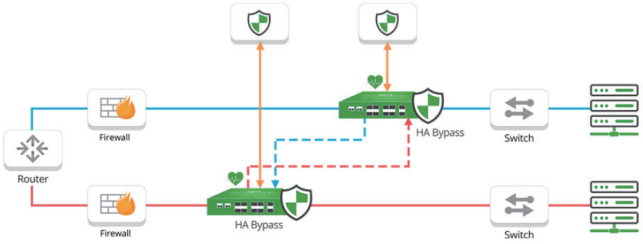
- ***高可用性（HA）***

虹科提供两个可用的高可用性 (HA) 解决方案，Active/Standby 和 Active/Active。

1） Active/Standby（主/备）部署到辅助工具，
提供从主设备到备用设备的故障转移。



2） Active/Active 部署到冗余链路，
在任一活动设备出现故障时提供故障转移。



网络流量监控

一体化网络监控设备-Allegro

Allegro网络万用表 重新思考网络

- ✓ 1-100GBit/s的移动设备
- ✓ 高速全流量捕获分析
- ✓ 直观的Web界面
- ✓ 快速进行2-7层故障排除
- ✓ 分析和关联所有元数据
- ✓ 灵活的pcap文件提取
- ✓ 实时/回溯分析
- ✓ 即插即用，无需配置
- ✓ 中文界面支持

- ***快速排除故障***

Allegro可进行网络流量实时和回溯分析。它分析和关联整个网络第2至第7层的所有数据，使网络问题或意外流量在几秒钟内被发现。该设备有不同的版本：移动或机架版本，即适用小型数据中心、大型ISP，也适用于本地公司网络。

- ***对Wireshark的补充***

故障诊断设备既能显示大画面，也能显示更细的细节。网络或应用程序的问题可以被搜索到，预先过滤，然后提取为pcap。这简化了Wireshark 的分析，因为只需要分析总流量的一小部分。Allegro 的集成pcap环形缓冲区（Allegro 1000/3000系列的标准配置）提供了该功能，即使是过去发生的事件。

- ***快速诊断***

点击式结构和选择性的pcap 提取帮助您快速找到您需要的内容。Web界面的搜索功能允许您按照MAC或IP地址、端口、VLAN、TCP握手、HTTP延迟等进行排序、搜索和过滤。你可以在一秒内得到结果，实现即时分析。

- ***全面的分析***

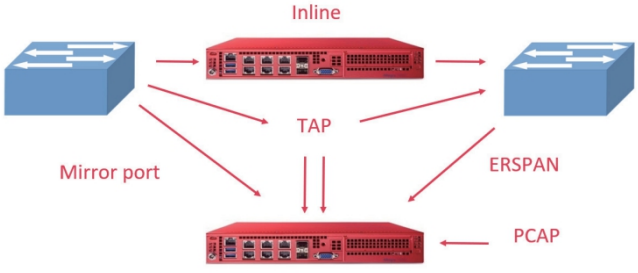
Allegro包括许多不同的分析模块，适用于L2至L7层。例如，搜索和提取所有不同的以太网类型，如L2上的LLDP，或自动搜索链路上的微爆现象。你可以使用L4 TCP来分析全局或每个IP终端的重传，L7来识别SIP和RTP流中潜在的VoIP质量问题。Allegro Packets正在不断努力扩展这些模块。

- ***简单的启动***

Allegro可以在您的网络中的任何地方快速、轻松地集成。你不需要安装任何额外的软件。通过独立于浏览器的网络界面访问数据，也可以远程访问。

- 部署方式

虹科Allegro网络万用表支持内联或者接收来自TAP或镜像端口的流量的部署方式。



- 故障排除的真实案例

故障排除往往需要快速获取相关数据。这里有一个典型的问题：

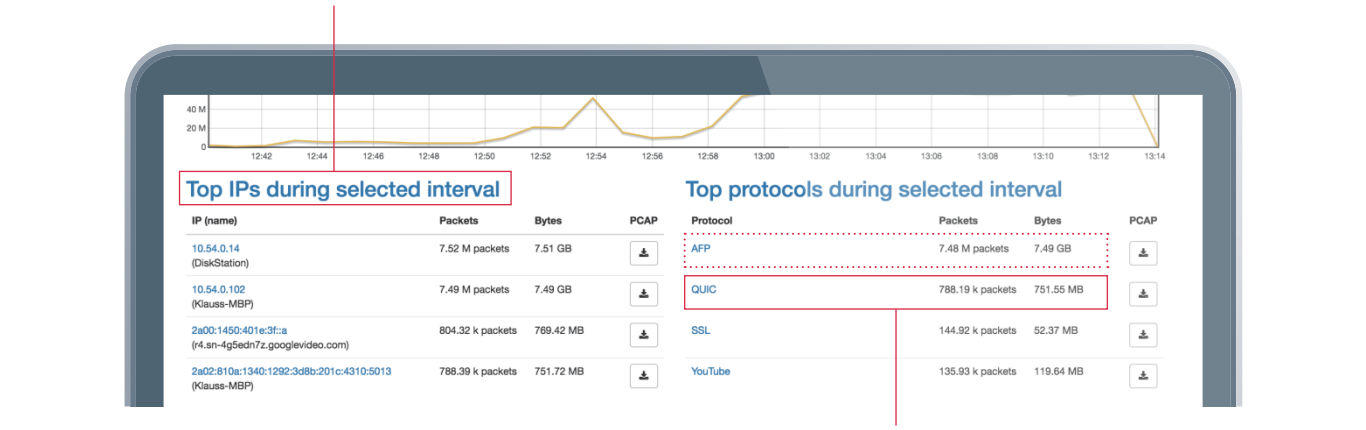
"一小时前我试图访问文件服务器，它非常慢。我无法继续我的工作，现在工作好些了，但它浪费了我很多时间，我不希望再发生这种情况。"

- → 在某一时刻，网络中的某一点上有什么流量？
- → 是否有任何其他的数据传输正在进行中，如备份或更新？
- → 是否存在带宽问题？如果是的话，是谁或什么原因造成的？
- → 如何详细检查这些过去的数据？

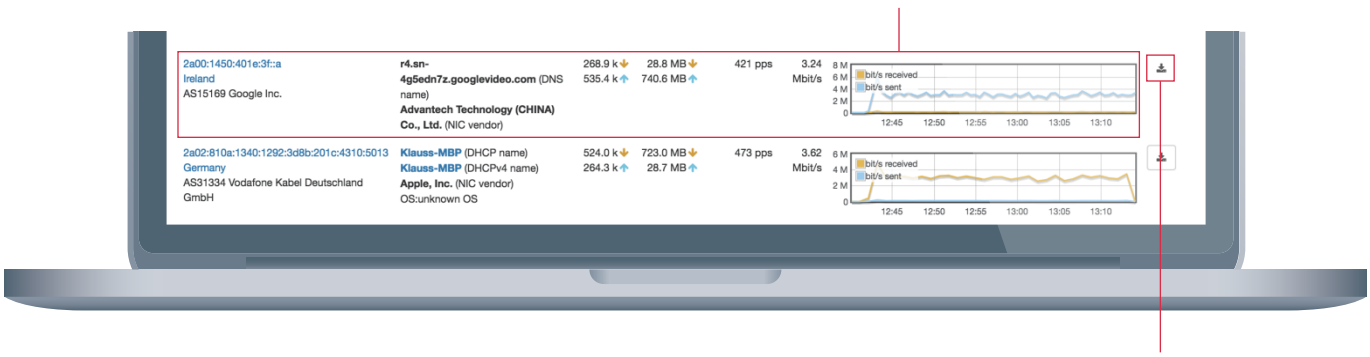
Allegro网络万用表可以帮助你快速、轻松地回答这些问题。

- 细节方面

仪表板只需一次点击就能显示特定时间间隔的Top-IPs和协议。这使你能够快速确定是否是一个特别的事件，如一个大型的更新或只是一个视频流在那个时候产生的负载。使用它可以立即在仪表板上查看每个协议的Top-IPs。



使用我们的仪表板来仔细查看一个L7协议或IP。仪表板上还显示TOP连接伙伴。在上面的截图中可以看到AFP协议被用于备份和QUIC。通过点击QUIC，TOP QUIC-IPs会在间隔中显示。



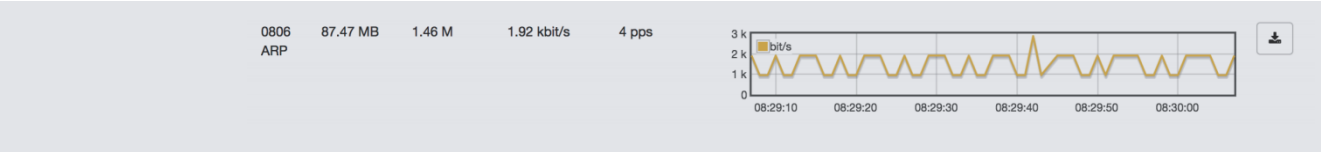
使用pcap按钮，可以提取和分析一个协议的IP通信的所有数据包，例如用Wireshark。大约5MBit/s的额外负载是由谷歌视频服务器通过IPv6产生的。找到了原因就可以采取进一步行动。

- 分析模块的概述

Allegro为您提供广泛的第2至第7层的分析，它可以实时显示，也可以追溯给定的时间范围。此外，它可以用来显示每个IP和MAC的大量信息，如解码的DNS、DHCP或HTTP主机名称或SSL通用名称。也可以用这些信息进行过滤。

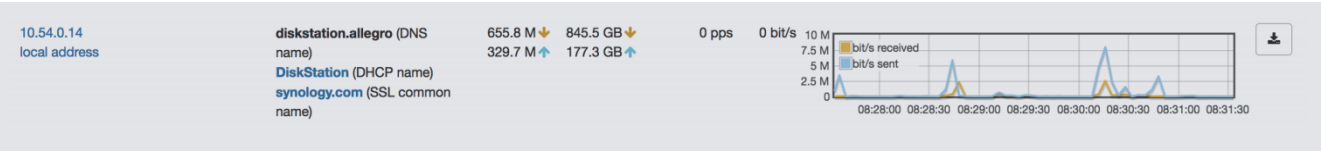
第2层

- 分析L2上出现的所有以太网类型
- MAC地址分析，包括L7协议、连接伙伴和每个MAC使用的IP
- VLAN分析：显示每个中继线的所有VLAN，对于Q-in-Q，显示每个VLAN的所有MAC
- 利用率分析：带宽测量在毫秒范围内，当超过阈值时自动报警。
- QoS分析



第3层

- IP分析：显示所有IPv4/v6地址，每个地址都有L7协议，连接伙伴和使用的MAC地址，TCP传输，QoS等级等。

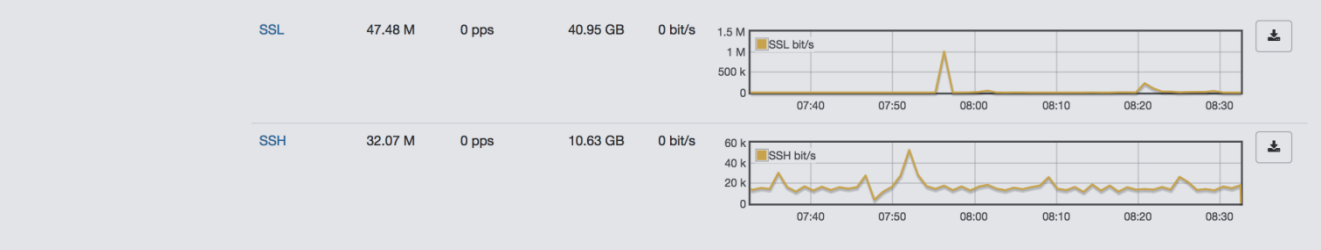


第4层

- TCP重传：基于时间的重传分析，包括全局和每个IP
- TCP：握手、响应时间、标志、零窗口
- 端口分析：使用的TCP和UDP端口

第7层

- 协议分析：基于签名的使用协议，每个协议的TOP-IPs
- HTTP/SSL分析：HTTP请求或SSL握手的时间分析，包括全局和每个IP
- SIP分析：一个SIP电话的分析，包括状态代码、RTP相关性、RTP抖动和丢包
- 通用响应时间分析：使用请求或响应中的模式进行测量



所有的统计数据都可以用可自由配置的时间范围来查看。

主要功能	详细内容		
全局视图	Top用户	三重播放（Triple play）	回溯分析
	质量分析	自定义仪表盘	
全局流量统计信息	自定义虚拟链路		
	全局流量统计		
常用功能	流量捕获	全流量存储	事件告警
	路径测量	离线数据包分析	报告生成
数据链路层监控	MAC统计	VLAN统计	MPLS统计
	QoS统计	MAC协议	LLDP统计
	数据包大小统计	STP状态	PPPOE统计
	ARP统计	网络利用率分析	IEEE802.11统计
网络层监控	IP统计	地理位置信息统计	NetBIOS统计
	数据包下载	DHCP统计	ICMP统计
	QoS状态	DNS统计	组播统计
传输层监控	会话分析	端口统计	
	TCP状态统计	IPSec统计	
数据链路层监控	应用协议统计	SMB统计	Profinet统计
	SSL统计	SIP统计	OPC UA统计
	HTTP统计	NTP统计	IEC 60870-5-104统计
	响应时间分析	PTP统计	RTP统计
			响应时间概览
其他功能	SNMP管理	历史流量PCAP下载	多用户管理
	远程访问	自定义虚拟链路	邮件警告

- 设备概述

设备	Virtual Edition	Allegro 200	Allegro 500
监控端口	1 x virtual mirror port	2 x 1000Base-T	4 x 1000Base-T
最大吞吐量	About 1 GBit/s (CPU dependent)	2 GBit/s	4 GBit/s
内部数据库内存	Unlimited	2 GB	4 -8 GB
集成环形缓冲器	Unlimited	-	0.5 - 1 TB
版本	Virtual	Portable	Portable
重量	-	260 g	1kg
包装	-	Portable soft shell case	Portable soft shell case
适用领域	云	办公室或小型数据中心	

设备	Allegro 1000 / 1200	Allegro 3000 / 3200	Allegro 3500 / 5500
监控端口	3 x 1000Base-T 2 x 10GBase-T 2 x SFP+ 1 extension slot	3 x 1000Base-T 2 x 10GBase-T 2 x SFP+ 1 extension slot	5 extension slots: SFP+, QSFP, QSFP28 etc.
最大吞吐量	20 GBit/s	40 GBit/s	50 - 100 GBit/s
内部数据库内存	16-256 GB	64 -256 GB	96 - 1536 GB
集成环形缓冲器	Up to 10 TB	Up to 10 TB	Up to 360 TB
版本	Portable / 1 U	Portable / 1 U	4 U
重量	2 -4 kg	2 -4kg	40 -80kg
包装	Portable soft shell case/ server cardboard	Portable soft shell case/ server cardboard	Server cardboard
适用领域	办公室或小型数据中心		大数据中心

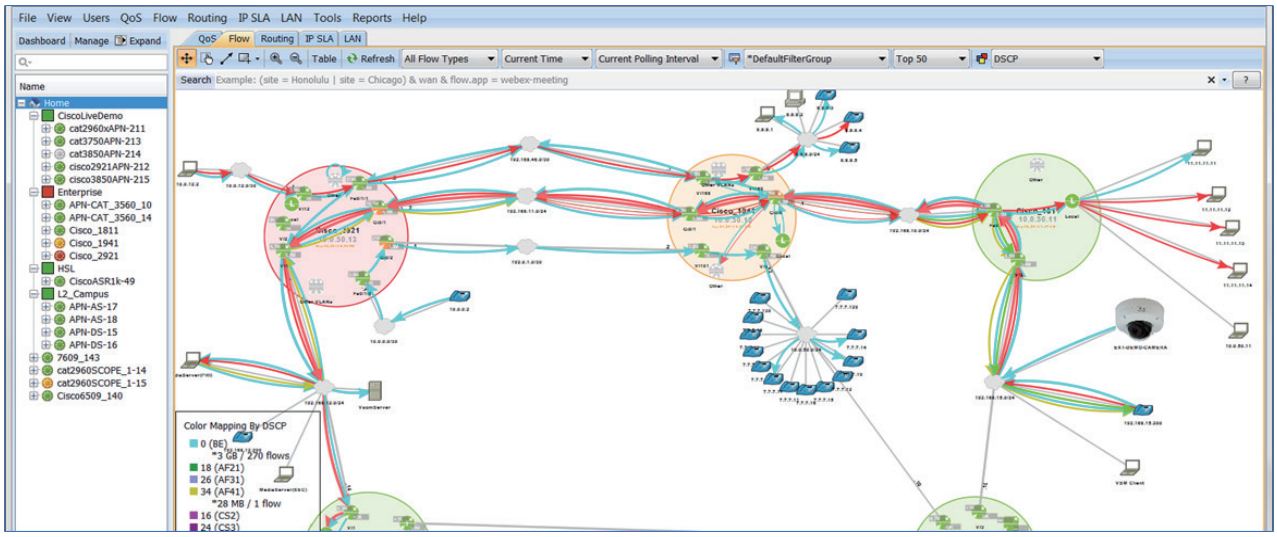
网络端到端和应用性能可视化-LiveNX

- 网络端到端和应用性能可视化-LiveNX

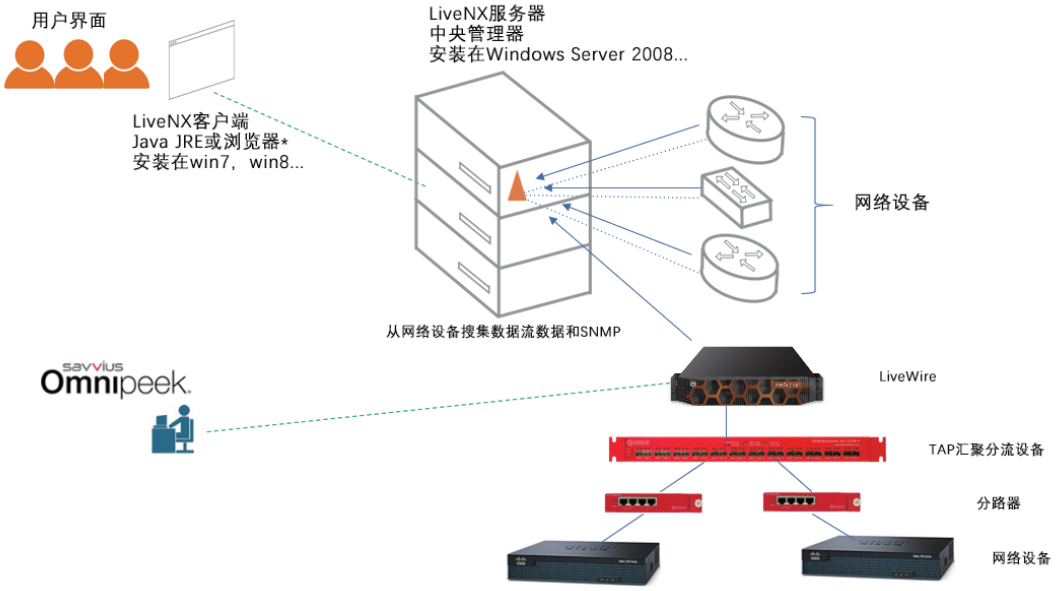
LiveNX基于流（即 Netflow、IPFIX、SFlow、JFlow 等）,SNMP和数据包等多种数据源，通过来自几乎任何地方的数据——WAN、SD-WAN、WiFi、远程站点、数据中心，查看并整个网络，关联多种数据源，实现端到端的可视化分析。轻松地从警报和上下文数据下钻到 Flow 性能数据，并进一步深入到目标数据包级分析，以实现全面的故障解决工作流程 - 实现加速网络、减少延迟抖动并减少 MTTR。LiveNX 提供从多个事件聚合的特定的警报，从而仅显示需要立即关注的警报。此外，LiveNX Insight 模块利用机器学习进行主动异常检测和路径更改通知。

LiveNX 可帮助您以前所未有的方式排除网络故障:

- 用于应用程序故障排除的可视化分析
- 综合仪表板和报告
- 主动警报和异常检测
- 端到端的可视化分析
- 从Flow到数据包取证分析



- 方案架构



- 平台组成

- ***LiveNX***

网络性能与分析平台 LiveNX 是具有专利技术的端到端可视化网络性能与分析平台，用户可以从中看到完整的网络架构视图，从网络操作宏观全局到每一台设备的详细状况，一览无余。LiveNX 直接从网络设备收集和分析实时数据，为规划、诊断和优化环境提供数据支持和最佳用户体验。

- ***Omnipeek***

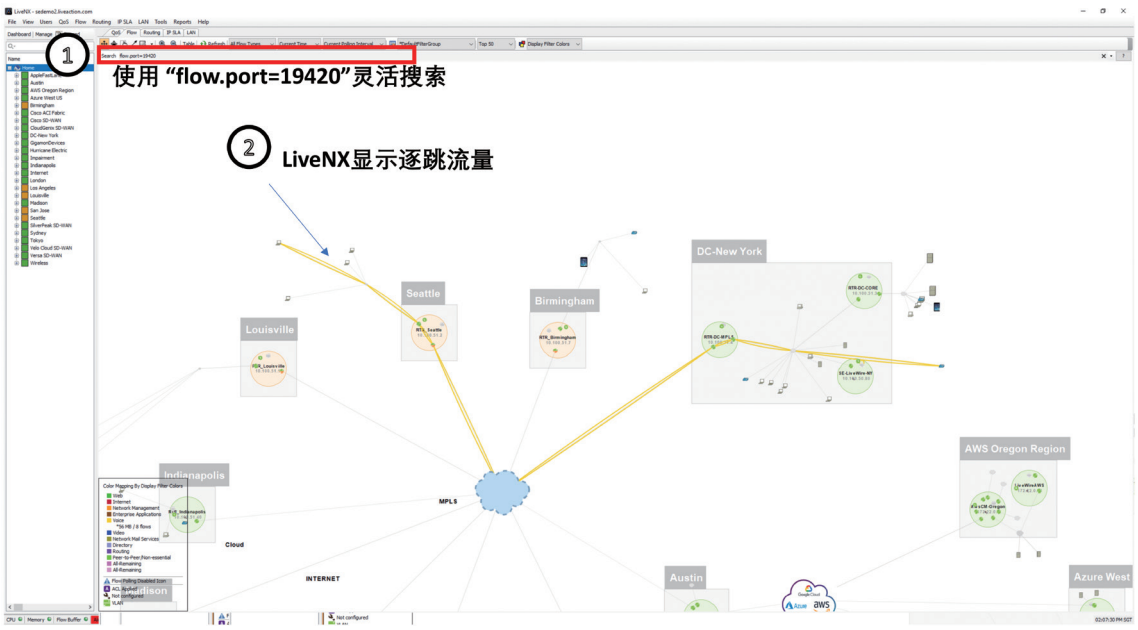
Omnipeek 数据抓包分析组件能让 LiveNX 用户快速从数据流分析过渡到数据包取证分析。还可用作对数据包进行分析的独立解决方案。

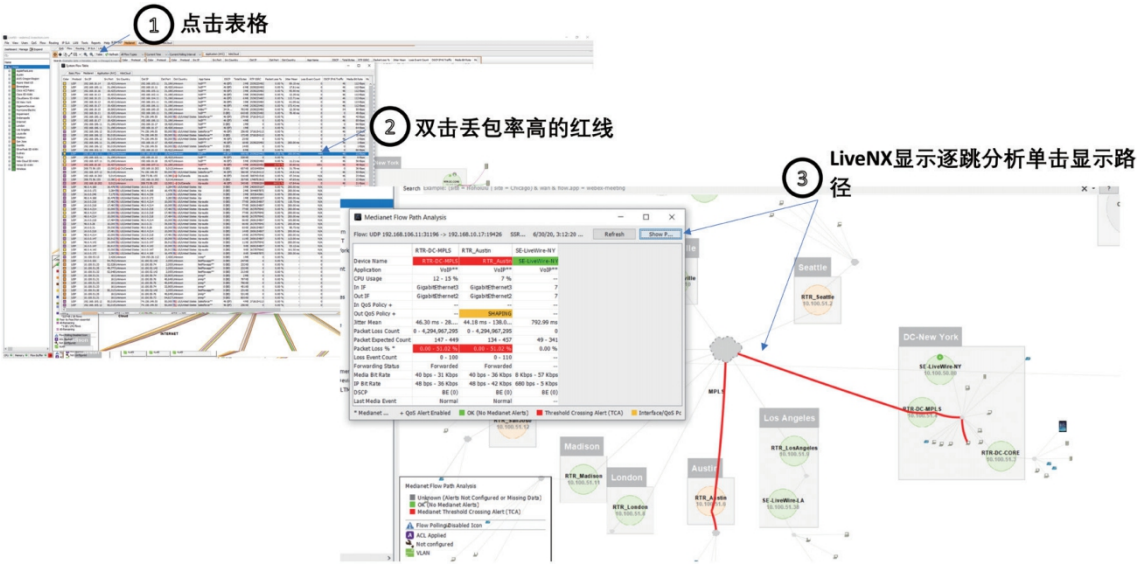
- ***LiveWire***

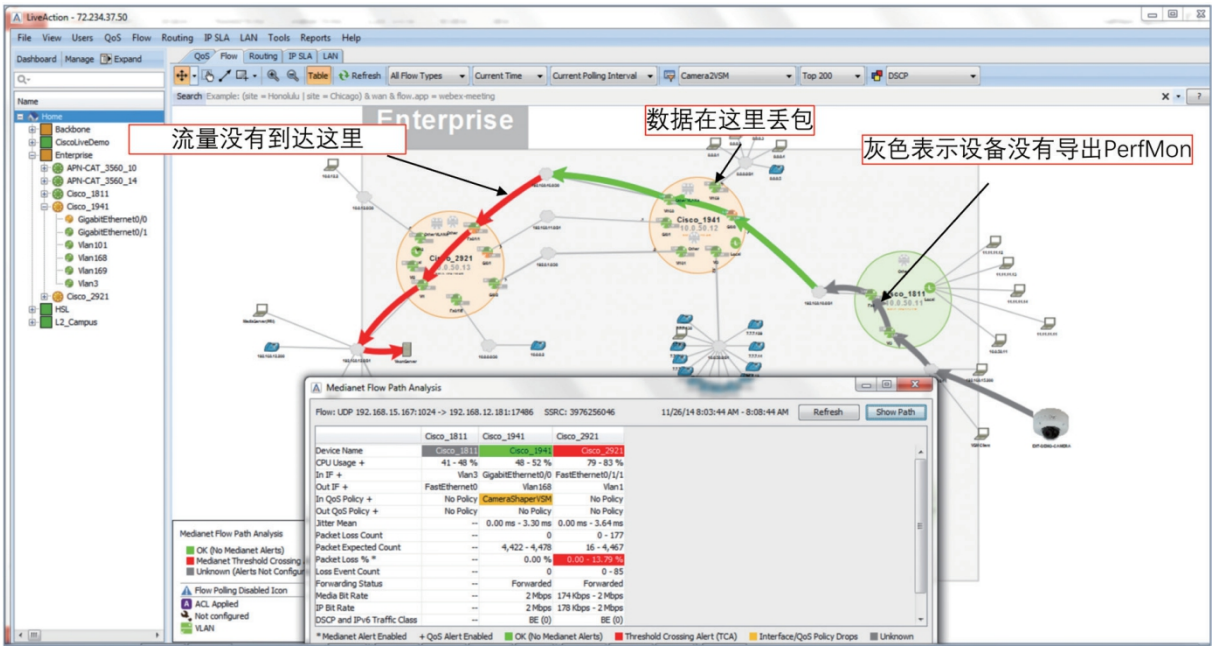
LiveWire 高性能数据包捕获设备能从远程站点、WAN 链接和数据中心生成流数据，扩展 LiveNX 的网络性能监视功能。

- 应用示例

- ***逐跳分析***







- ***从Flow到数据包分析***

允许用户从Flow到深度数据包分析的故障排除

软件网络流量监控分析方案-ntop

ntop是不依赖任何硬件设备的经济的纯软件网络流量监控解决方案，可任意部署在物理、虚拟、容器等环境中。可接收NetFlow，Sflow等流数据和SNMP、镜像流量等多种数据源进行流量监控分析，并支持全流量存储和元数据存储，实现长时间回溯分析。该方案由多个组件构成，组件之间既可以组合使用亦可以和第三方方软件集成。

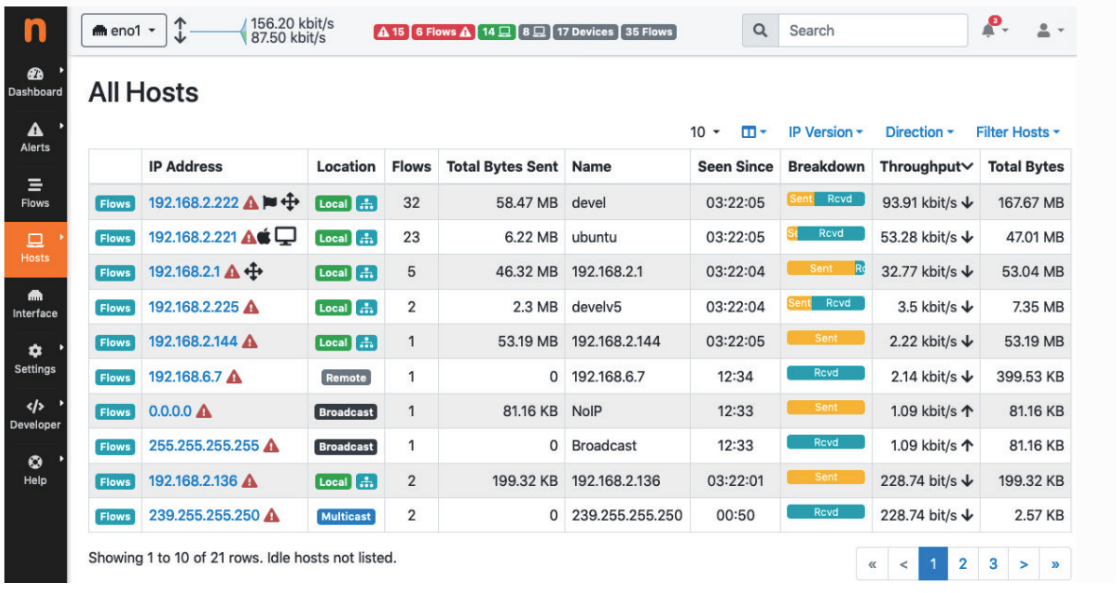
- 组件

- ***ntopng***

ntopng 是一个基于 Web 的流量监控应用程序，是监视网络使用情况的网络流量探测器，主要功能有：

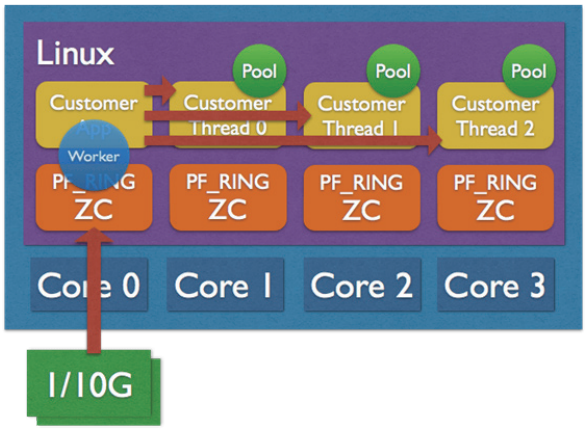
- 通过被动捕获网络流量来监控流量
- 收集网络流（NetFlow、sFlow 和 IPFIX）
- 主动监控选定的网络设备
- 通过 SNMP 监控网络基础设施

ntopng 和普通流量收集器之间的主要区别在于，ntopng 不仅报告流量统计数据，而且还分析流量、对观察到的流量类型得出结论并报告网络安全指标。ntopng是ntop解决方案中的核心组件，它既可以单独使用，也可用于其他组件配合使用。



- ***PF_RING（ZC）***

PF_RING™ 是一种新型的网络套接字，用于抓取网络数据包，可显着提高数据包捕获速度。
PF_RING ZC（Zero Copy）更进一步，可让您在任何数据包大小下实现1/10 Gbit的线速数据包处理（RX和TX）。



和DPDK相比PF_RING ZC有更加丰富且易用的API，只需要简单的几行代码创建一个复杂的应用程序，大大缩短研发难度和时间。
因此许多客户选择使用PF_RING ZC作为DPDK的替代方案。

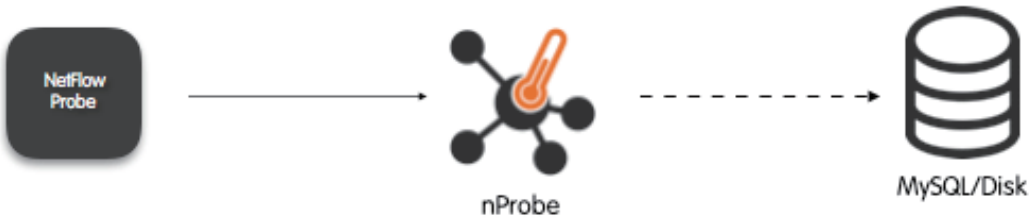
- ***nProbe***

nProbe™是一个网络流探针，既可以用于收集NetFlow/Sflow/IPFIX等流信息，也可以用于接收镜像流量生成流数据输出到监控工具，还可输出到ElasticSearch，kafka，MySql等。通常和ntopng一起使用，也可以和第三方工具集成。

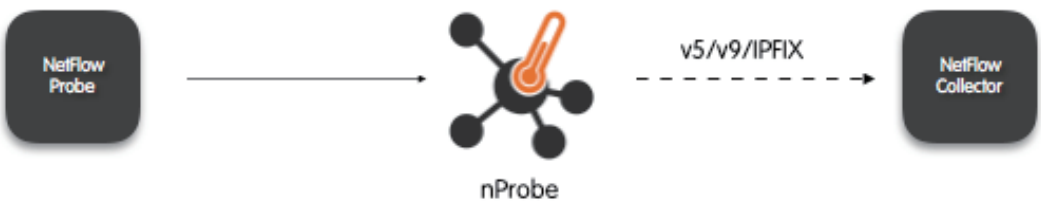
常用三种模式：

- 探针模式

- 收集器模式



- 代理模式



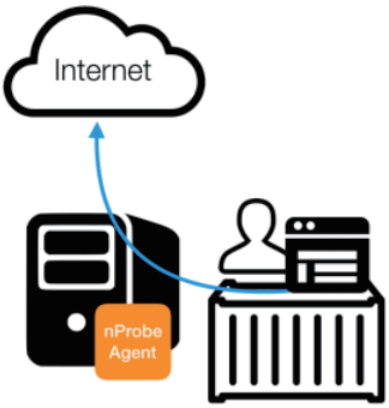
- ***nProbe Cento***

nProbe™Cento是一款高速NetFlow探针。被设计为模块化监控系统的一个组件：除了捕获入口数据包和计算流数据之外，它还可以用于通过DPI（深度数据包检测）对流量进行分类。

nProbe™Cento旨在在商品硬件上保持1/10/100 Gigabit速度。在足够的硬件上，nProbe™Cento能够处理每个物理核心10 Gbit，并可以线性地扩展核心数量（只要有足够的可用内存带宽）。

- ***nProbe Agent***

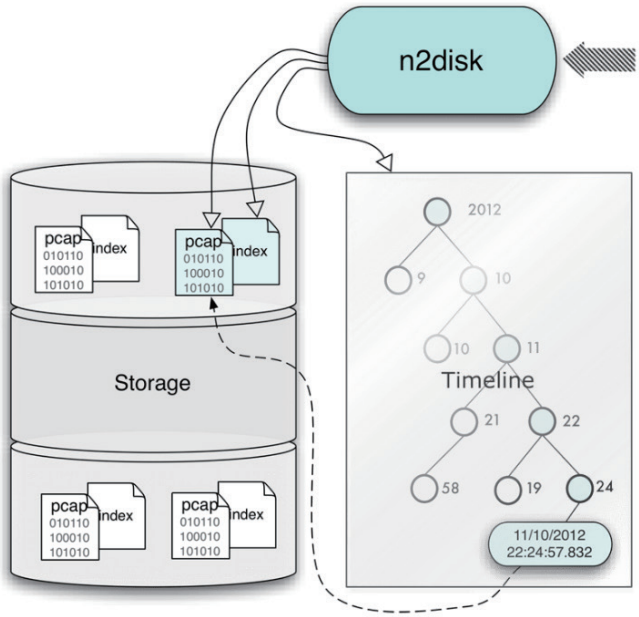
nProbe ™是一种流量探测器，能够处理实时流量（网络链路上的原始数据包）或收集Netflow。nProbe™利用深层数据包检查（nDPI）通过查看数据包有效负载来识别应用程序协议。nProbe™Agent更进一步，可提供生成给定流量的应用程序的可见性，跟踪网络活动背后的用户和进程，对容器间网络通信具有可见性。



- ***n2disk***

n2disk™是网络流量记录器应用程序。使用n2disk™，您可以从实时网络接口以几Gigabit速率（在足够的硬件上以10 Gigabit / s以上）捕获全量的网络数据包，并将其写入文件中而不会丢失任何数据包。

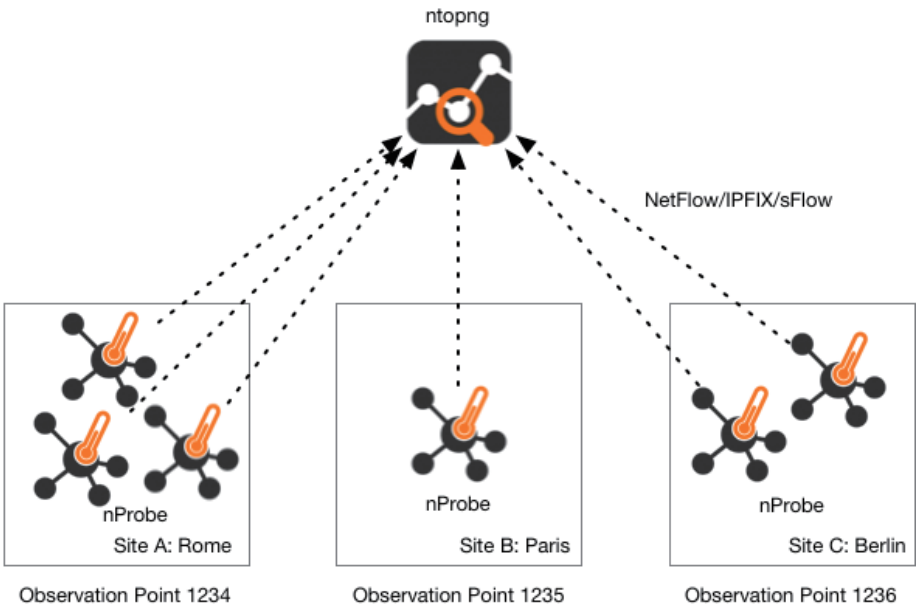
n2disk™旨在将文件长时间写入磁盘，您必须指定在执行过程中可以写入的不同文件最大数量，如果n2disk™达到最大文件数量，它将开始回收文件从最旧的一个。这样，您可以在固定的时间窗口中完整了解流量，并提前知道所需的磁盘空间量。



- 典型应用

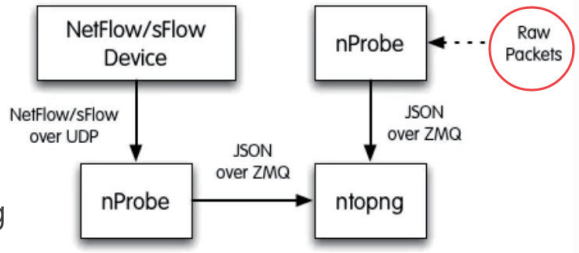
- ***监控Netflow/Sflow流数据***

基于流的监控是最常见的网络流量监控方法，这是我们需要nProbe和ntopng配和使用，使用nProbe接收流数据，并转换为ntopng支持的数据格式转发到ntopng进行集中监控，使用该方法在硬件性能足够的条件下可以同时监控上百个数据源。



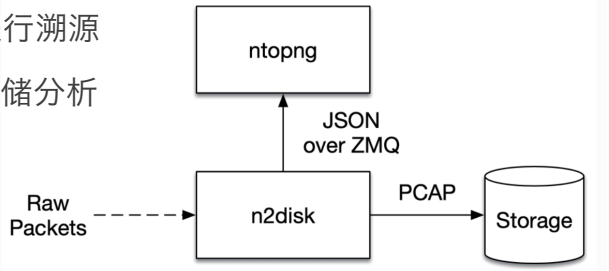
- ***监控Span/Tap流量数据***

当基于流的监控无法满足需要时，需要更进一步的监控方法。使用TAP或者SPAN的方法获取全部的流量副本进行全流量监控是常用的方法。这是将使用nProbe捕获原始流量数据并生成元数据发送到ntopng镜像监控，与基于流的监控方式相比，监控原始流量能获得更高颗粒度的分析能力。



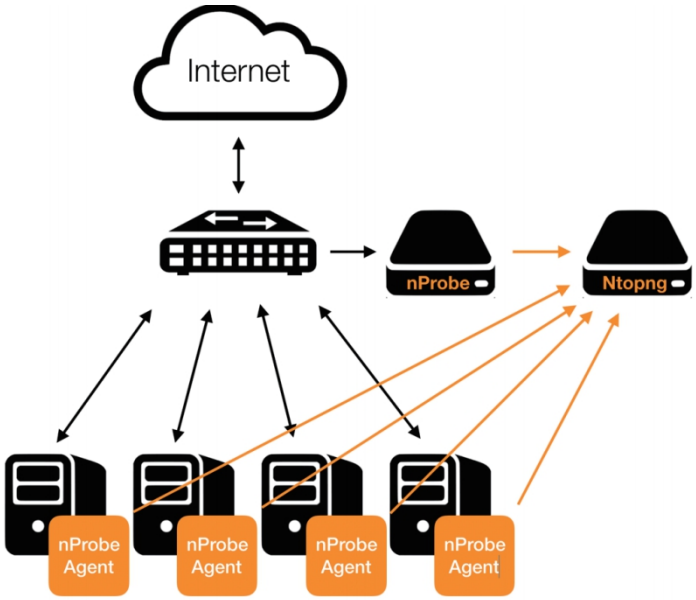
- ***全流量存储分析***

某些场景下，需要对原始流量进行全量存储分析以进行溯源和取证。使用ntopng配和n2disk可以进行全流量存储分析功能。n2disk使用环形存储的方式存储所以原始流量并生成索引供ntopng进行提取分析。



- ***服务器监控***

nProbe™ Agent 通过系统自省增强网络可见性。它通过系统内省的进程、用户、容器、协调器和其他性能指标来丰富经典网络数据，例如 IP 地址、字节和数据包。配和使用时，可用于监控服务器网络流量详细使用情况。



▶▶ 如果对上述产品有所兴趣，欢迎来电洽谈。

HongKe 虹科

hongwangle.com

sales@hkaco.com

400-999-3848

广州市黄埔区神舟路18号
润慧科技园C栋6层

各分部：广州 | 成都 | 上海 | 苏州 |
西安 | 北京 | 台湾 | 香港 | 美国

更多案例

联系我们