N-Probe 7

DATASHEET

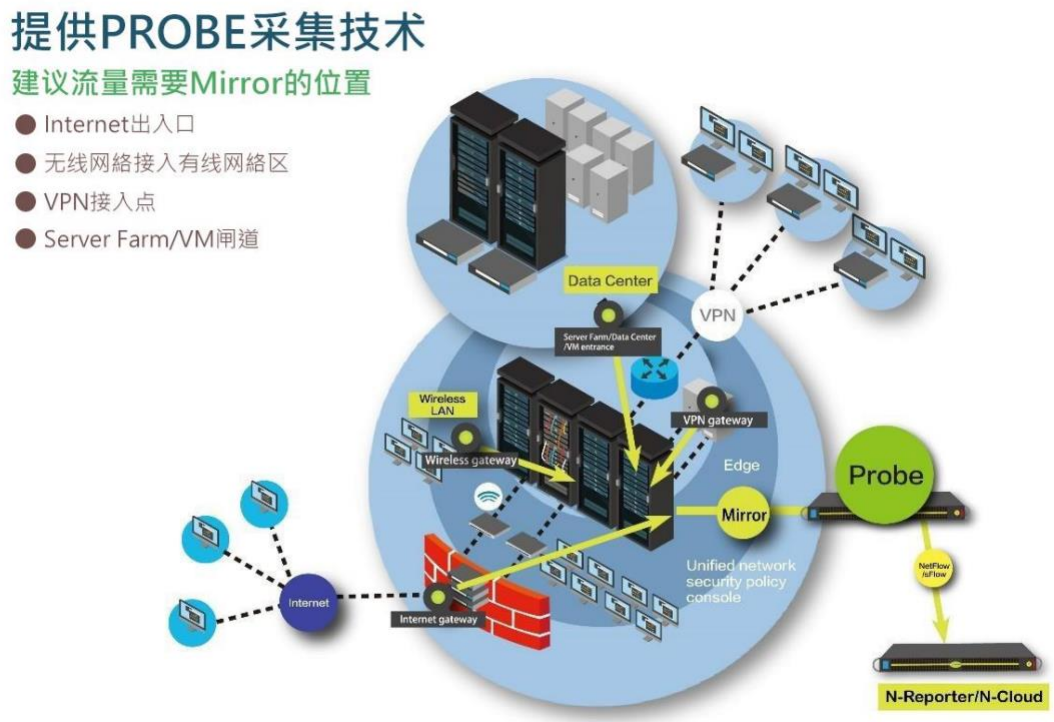
Next Generation IT Operation Platform

Integrate Network Management, Flow Analysis and Log Reporting

2024/03/20

当今若要执行流量Flow分析，常用的方法是让路由器或交换机吐出NetFlow 或是 sFlow。然而并非所有的交换器都能支持NetFlow/sFlow数据的吐出功能。还存在另一个问题是由于实施Flow数据的产出会消耗路由器与交换机不少的CPU资源，许多网络管理者对于开启NetFlow/sFlow功能存有疑虑。sFlow虽然支持数据包取样Sampling功能，可以降低CPU的损耗，但也因为取样的缘故让大多数的流量行为未被记录而导致分析结果失真。

要解决上述问题，由 N-Partner 公司所生产的 N-Probe 是一个非常好的解决方案。N-Probe 可做到1:1的流量采集，具有部署容易且运作上几乎不影响交换设备效能之优点，原因是大多数的交换器皆支持镜像端口(Mirror Port)功能，用户只要把复制的Mirror流量接入到N-Probe即可，N-Probe 会将 Mirror 流量转换成 1:1 NetFlow 数据格式输出到使用分析系统进行后续的分析工作。对网络管理者来说，使用分析是维运工作中非常重要的一环，因为透过好的 Flow 解析工具(诸如 N-Partner 公司生产的N-Reporter/N-Cloud产品)，能够清楚知道环境中所有的网络使用行为、封包流向、用量统计等重要讯息，当网络发生异常，可以快速定位根源，协助网络管理者进行排错。N-Probe让使用分析变成一件非常简单的工作。



要做好全局的流量监控与使用者行为分析，必须要在重要的网络节点进行流量采集，诸如 Internet 出入网关、数据中心的核心交换器、分支单位透过 VPN 连回至总部的接入点、无线网络接入核心之处等，皆可透过镜像端口的设定将流量 Mirror 出来，接入 N-Probe 后转换成 1:1 的 NetFlow 格式导出到使用分析设备，几乎能够涵盖全网的联机行为。

除了产出1:1 NetFlow数据，N-Probe 亦提供针对 DNS 访问流的七层内容解析功能，同样采用Mirror Traffic接入方式，N-Probe能将流量里的 DNS 查询封包撷取出来写成 DNS Query Log 后，透过 Syslog 协议吐出到外部任何指定日志以及 SIEM 平台进行稽核要求所需的储存备查与统计报表制作；或是网域(Domain)浏览分析等更进阶的维运工作。N-Probe 实时产出 DNS Log 的效能超过百万 EPS(Event Per Second)，因此适用于在绝大多数的网络环境中替代 DNS 服务器必须自己记录与发送 Log 所肇致的效能伤害。从强化资安防御的观点来说，比对 DNS Log 与威胁情资(Threat Intelligent)是确保内网计算机不会访问恶意网域的有效方式，也能够及早发觉潜伏于内网的恶意软件。再者，N-Probe 所产出的 DNS Log 里亦包含了查询不存在网址(NX Domain)的信息，N-Cloud/N-Reporter 将根据来自 N-Probe的 NX Domain 记录建立不存在网址列表(NX Domain List)，启动联防机制自动写入防御设备(注1)，保护 DNS 服务器免遭受巨量 NX Domain 查询瘫痪攻击。

(注1)支持本联防功能的设备厂牌与型号陆续增加中，详情请洽 N-Partner 公司查询。

Dashboard 范例(DNS 分析与恶意域名联机监控)

N-Probe提供软件版与硬件版，因应不同客户之需求。软件版支持于虚拟化平台，如VMware；硬件产品则可根据不同网络环境之接口需求，提供多种接口，如配置1G或10G接口之Mirror Traffic网络接入端口(Interface)，其中光接口有LR或是SR型态可供选购。N-Probe最高可达到40Gbps 的 Mirror Traffic 转换成 1:1 NetFlow 输出之工作效能，并同时支持 v5 及 v9 格式。

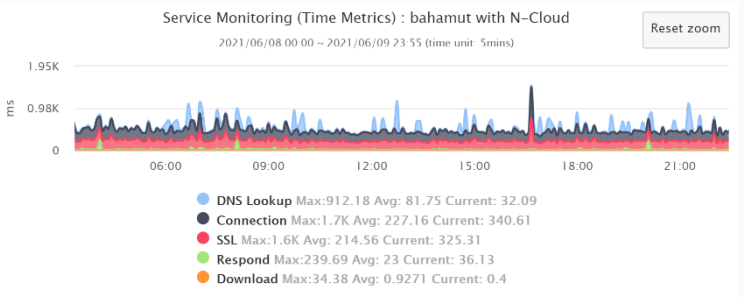
加值模块

除了上述 1:1 NetFlow 数据产出与 DNS 内容解析功能，N-Probe亦提供以下加值功能，用户可依实际需求选购。

若用户的网络架构分散在不同地理位置的机房或是分支机构，各地透过 Internet/VPN 彼此连接，最佳操作建议是将 N-Probe 布署到各地并启动 External Receiver 模块功能，在本地采集 SNMP/Flow/Syslog(含 TCP 与 UDP 协议 Syslog)数据后加密压缩转发至 N-Reporter/N-Cloud 系统，压缩率达5倍，大幅降低Internet/VPN的带宽负载同时也强化了传输期间数据完整与安全性。External Receiver 支持断线续传(Store and Forward)的功能，当连接的Internet/VPN线路发生中断障碍时将 Flow/Syslog 数据暂存，待联机恢复后完整重新转发至 N-Reporter/N-Cloud 系统。External Receiver 可建置成 HA(Master/Slave)架构，提升可用度。再者，External Receiver 模块包含 SNMP 监控功能，负责本地端设备的 SNMP Polling 工作取得 IP/MAC 及 MAC/Port 对应表，以协助网络管理。

N-Probe 亦提供效能监控(Performance Monitor, PM)模块，功能一是以 ICMP Ping 封包监测各量测点的网络等待时间(Round Trip Time, RTT)；功能二是仿真人们浏览网页服务(Web Service)的过程，N-Probe 会分别记录过程中几个阶段的响应时间(Response Time)：DNS查询及响应、与 Web 服务器建立联机、SSL传输、网页响应与内容下载，并将上述数据绘制成可视化线图。为了可以更贴近使用者每个时刻的使用感受，信息管理人员可以将含PM模块的 N-Probe 布署在任何网络位置，例如办公室OA区、分公司里、外部电信承租的IDC机房里等等，让 N-Probe 从不同地点量测，N-Probe会将收集到的延迟数据送到 N-Reporter/N-Cloud 智能维运平台绘制图形，供用户查看每个被监控点的网络质量，达成多点、多角度的持续性监控与分析。此外，搭配 N-Reporter/N-Cloud 的趋势预测功能，还能预测未来数小时到数个月的成长走势，在延迟变得严重之前收到预警，早一步处理。

1. DNS Query and Response
2. TCP Connection
3. SSL
4. Respond
5. First Page Download



N-Partner公司简介

新伙伴科技股份有限公司(N-Partner Technology Ltd. Co.)成立于2011年，是一个专长于高效能大数据搜集(Big Data)、人工智能分析技术(AI and Abnormal Analysis)的研发团队，总部位于台湾台中市。核心成员均拥有超过20年的电信等级网络维运以及软件开发经验，集合网络、资安、操作系统与 Kernel、计算机硬件与虚拟机、C语言、PHP/Java、数据库、大数据处理与云架构、美术与设计等各领域专长的人才。由 N-Partner 公司所开发的 N-Reporter 以及 N-Cloud 双产品线为当前全球唯一能够完美整合 SNMP、Flow与 Syslog 三种主流网管和资安事件分析技术的 IT维运系统，领先的技术包括：Any-to-Any分析，能针对各个日志事件与所有IP进行历史行为自动学习进而建立动态基准，用以发觉异常并实时告警；关联SNMP、Flow与Syslog三种数据，提供IT管理者清楚的障碍除错依据等。此外，N-Cloud维运平台更运用了云架构来提供高处理效能、几无限制的延展性以及万人同时操作使用的能力，适合做为NOC/SOC合一SaaS服务，已经获得多家大型教育网、金融公司、跨国企业与电信公司采用做为网络与资安的维运平台。在2015年之前，N-Partner公司的商业版图已经横跨海外。

■ 硬件规格

	NP-RPT-CN-Probe-5Port	NP-RPT-CN-Probe-2Port-SR/NP-RPT-CN-Probe-2Port-LR	NP-RPT-CN-Probe-40G	NP-RPT-CN-Probe-2Port-C	NP-CLD-E-REC-CN
功能	All-in-One Appliance，内建专属 OS、数据库与应用程序				
尺寸	1U Rackmount, 19 Inch Standard Wide Rack Mount Industry Server				
I/O ports	1 VGA, 1 COM	1 VGA, 1 COM	1 VGA, 1 COM	1 VGA, 1 COM	1 VGA, 1 COM
CPU	Intel Xeon E-2334 Processor (8M Cache, 3.40GHz)	Intel Xeon E-2334 Processor (8M Cache, 3.40GHz)	Intel Xeon E-2334 Processor (8M Cache, 3.40GHz)	Intel Xeon E-2334 Processor (8M Cache, 3.40GHz)	Intel Xeon E-2334 Processor (8M Cache, 3.40GHz)
Ethernet Controller	Dual Port GbE LAN	Dual Port 10 GbE LAN + Dual Port GbE LAN	Dual Port 40 GbE LAN + Dual Port GbE LAN	Dual Port 10 GbE LAN + Dual Port GbE LAN	Dual Port GbE LAN
Memory	32G DDR4 x 1	32G DDR4 x 1	32G DDR4 x 1	32G DDR4 x 1	32G DDR4 x 1
IPMI	Integrated IPMI 2.0 and KVM with Dedicated LAN	Integrated IPMI 2.0 and KVM with Dedicated LAN	Integrated IPMI 2.0 and KVM with Dedicated LAN	Integrated IPMI 2.0 and KVM with Dedicated LAN	Integrated IPMI 2.0 and KVM with Dedicated LAN
Power Supply	350W Platinum Level	350W Platinum Level	350W Platinum Level	350W Platinum Level	350W Platinum Level
SSD	500GB	500GB	500GB	500GB	500GB
Interface	1 Gigabit Management Port x 1, 1Gigabit Mirror Port x 5	1 Gigabit Management Port x 1, 1 Gigabit Mirror Port x 1, 10 Gigabit SR/LR Mirror Port x 2	1 Gigabit Management Port x 1, 1 Gigabit Mirror Port x 1, 40 Gigabit Mirror Port x 2	1 Gigabit Management Port x 1, 1 Gigabit Mirror Port x 1, 10 Gigabit Copper Mirror Port x 2	1 Gigabit Management Port x 1, 1Gigabit Mirror Port x 1
HDD	4TB	4TB	4TB	4TB	4TB

■ N-Probe VM 建议规格

1. 请准备一台 Server，建议规格如下：

   ✓CPU 建议 E-2334 (8M 高速缓存，3.40 GHz) 以上。

   ✓ RAM内存空间须 48 G 或以上

   ✓ 硬盘空间 500G 以上，请依实际需求决定。

   ✓ 安装 VMware Esxi 6.0 或以上的版本。

2. N-Probe 运行时，若要达到最佳效能，至少需要 32G 的RAM 内存空间。

3. 请准备一台 Windows 计算机，用于管理 VMware Server。

4. 请准备 N-Reporter/N-Cloud系统，接收 N-Probe/External Receiver 送来的 Flow 或 Syslog 流量。

■ 产品料号

產品料號	料號說明
NP-RPT-CN-Probe	Flow and DNS/HTTP data export. SofCNare Module with 1 Year MA
NP-RPT-CN-Probe-5Port	Flow and DNS/HTTP data export. Hardware device. 1G interface. 5 ports build-in with 1 Year MA
NP-RPT-CN-Probe-2Port-LR	Flow and DNS/HTTP data export. Hardware device. 10G LR interface. 2 ports build-in with 1 Year MA
NP-RPT-CN-Probe-2Port-SR	Flow and DNS/HTTP data export. Hardware device. 10G SR interface. 2 ports build-in with 1 Year MA
NP-RPT-CN-Probe-2Port-C	Flow and DNS/HTTP data export. Hardware device. 10G Copper interface. 2 ports build-in with 1 Year MA
NP-RPT-CN-Probe-40G	Flow and DNS/HTTP data export. Hardware device. 40G QSFP+ interface. 2 ports build-in with 1 Year MA
NP-CLD-E-REC-CN	External-Receiver platform. Collect and forward data. Include 1 year MA
NP-CLD-E-REC-VM-CN	External-Receiver VM version. Collect and forward data. Include 1 year MA

Tel：+886-4-23752865　Fax：+886-4-23757458
业务咨询：sales@npartner.com
技术咨询：support@npartner.com