N-Probe 7

DATASHEET

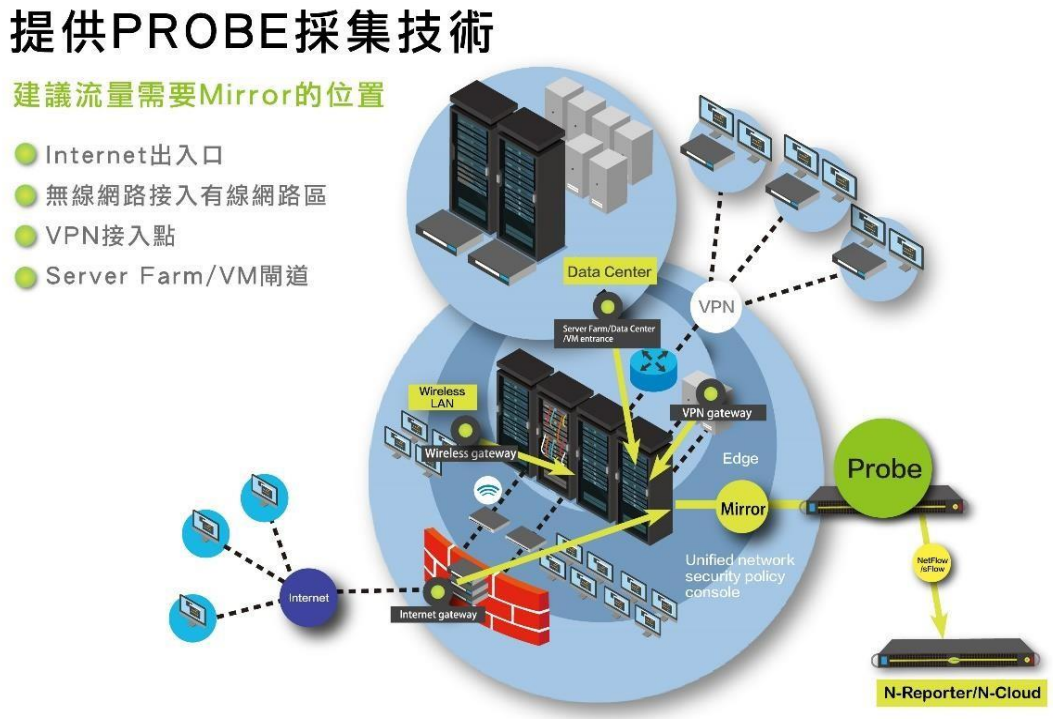
Next Generation IT Operation Platform

Integrate Network Management, Flow Analysis and Log Reporting

2024/10/25

現今若要執行流量Flow分析，慣用的方式是讓路由器或是交換機吐出NetFlow 或是 sFlow，然而並非所有的交換器皆可以支援NetFlow/sFlow的吐出功能。還存在另一個問題是由於Flow資料的產生將會耗損路由器與交換機不少的CPU資源，許多網路管理者對於開啟NetFlow/sFlow功能存有疑慮。sFlow雖然支援封包取樣Sampling功能，可以降低CPU的損耗，但也因為取樣的緣故導致大多數的流量行為未被記錄而導致分析結果失真。

要解決上述問題，由N-Partner公司所生產的N-Probe是一個非常好的解決方案。N-Probe 可做到1:1的流量採集，具有部署容易且運作上幾乎不影響交換設備效能之優點，原因是大多數的交換器皆支援鏡像端口(Mirror Port)功能，使用者只要把複製的Mirror流量接入到N-Probe即可，N-Probe會將Mirror流量轉換成1:1 NetFlow資料格式輸出到流量分析系統進行後續的分析工作。對網路管理者來說，流量分析是維運工作中非常重要的一環，因為透過好的Flow解析工具(諸如N-Partner公司生產的N-Reporter/N-Cloud產品)，能夠清楚知道環境中所有的網路使用行為、封包流向、用量統計等重要訊息，當網路發生異常，可以快速定位根源，協助網路管理者進行排錯。N-Probe讓流量分析變成一件非常簡單的工作。



要做好全域的流量監控與使用者行為分析，必須要在重要的網路節點進行流量採集，諸如Internet出入閘道、數據中心的核心交換器、分支單位透過VPN連回至總部的接入點、無線網路接入核心之處等，皆可透過鏡像端口的設定將流量Mirror出來，接入N-Probe後轉換成1:1的NetFlow格式導出到流量分析設備，幾乎能夠涵蓋全網的連線行為。

除了產出1:1 NetFlow數據，N-Probe亦提供針對DNS訪問流的七層內容解析功能，同樣採用Mirror Traffic接入方式，N-Probe能將流量裡的DNS查詢封包擷取出來寫成DNS Query Log後，透過Syslog協議吐出到外部任何指定日誌以及SIEM平台進行稽核要求所需的儲存備查與統計報表製作；或是網域(Domain)瀏覽分析等更進階的維運工作。N-Probe即時產出DNS Log的效能超過百萬EPS(Event Per Second)，因此適用於在絕大多數的網路環境中替代DNS伺服器必須自己記錄與發送Log所肇致的效能傷害。從強化資安防禦的觀點來說，比對DNS Log與威脅情資(Threat Intelligent)是確保內網電腦不會訪問惡意網域的有效方式，也能夠及早發覺潛伏於內網的惡意程式。再者，N-Probe所產出的DNS Log裡亦包含了查詢不存在網址(NX Domain)的資訊，N-Cloud/N-Reporter將根據來自N-Probe的NX Domain記錄建立不存在網址列表(NX Domain List)，啟動聯防機制自動寫入防禦設備(註1)，保護DNS伺服器免遭受巨量NX Domain查詢癱瘓攻擊。

(註1)支援本聯防功能的設備廠牌與型號陸續增加中，詳情請洽N-Partner公司查詢。

DNS查詢分析Dashboard範例(包含惡意域名訪問監控)

N-Probe提供軟體版與硬體版，因應不同客戶之需求。軟體版支援於虛擬化平台，如VMware；

硬體產品則可根據不同網路環境之介面需求，提供多種介面，如配置1G或10G或40G或100G介面之Mirror Traffic網路接入埠(Interface)，其中光介面有LR或是SR型態可供選購。N-Probe最高可達到100Gbps 的Mirror Traffic轉換成1:1 v5或v9格式NetFlow 輸出之工作效能，亦支援Sampling與送出到多個接收目的地。

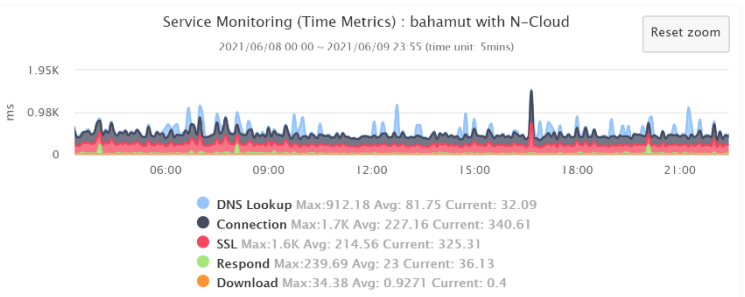
加值模組

除了上述1:1 NetFlow數據產出與DNS內容解析功能，N-Probe亦提供以下加值功能，用戶可依實際需求選購。

若用戶的網路架構分散在不同地理位置的機房或是分支機構，各地透過Internet/VPN彼此連接，最佳操作建議是將N-Probe佈署到各地並啟動External Receiver模組功能，在本地採集SNMP/Flow/Syslog(含 TCP 與 UDP 協定 Syslog)數據後加密壓縮轉發至N-Reporter/N-Cloud系統，壓縮率達5倍，大幅降低Internet/VPN的頻寬負載同時也強化了傳輸期間資料完整與安全性。External Receiver支援斷線續傳(Store and Forward)的功能，當連接的Internet/VPN線路發生中斷障礙時將Flow/Syslog數據暫存，待連線恢復後完整重新轉發至N-Reporter/N-Cloud系統。External Receiver可建置成HA(Master/Slave)架構，提升可用度。再者，External Receiver模組包含SNMP監控功能，負責本地端設備的SNMP Polling工作取得IP/MAC及 MAC/Port對應表，以協助網路管理。

N-Probe亦提供效能監控(Performance Monitor, PM)模組，功能一是以ICMP Ping封包監測各量測點的網路延遲(Round Trip Time, RTT)；功能二是模擬人們瀏覽網頁服務(Web Service)的過程，N-Probe會分別記錄過程中幾個階段的回應時間(Response Time)：DNS查詢及回應、與Web伺服器建立連線、SSL傳輸、網頁回應與內容下載，並將上述數據繪製成可視化線圖。為了可以更貼近使用者每個時刻的使用感受，資訊管理人員可以將含PM模組的N-Probe佈署在任何網路位置，例如辦公室OA區、分公司裡、外部電信承租的IDC機房裡等等，讓N-Probe從不同地點量測，N-Probe會將收集到的延遲數據送到N-Reporter/N-Cloud智慧維運平台繪製圖形，供用戶查看每個被監控點的網路品質，達成多點、多角度的持續性監控與分析。此外，搭配N-Reporter/N-Cloud的趨勢預測功能，還能預測未來數小時到數個月的成長走勢，在延遲變得嚴重之前收到預警，早一步處理。

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



N-Partner公司簡介

新夥伴科技股份有限公司(N-Partner Technology Ltd. Co.)成立於2011年，是一個專長於高效能大數據蒐集(Big Data)、人工智慧分析技術(AI and Abnormal Analysis)的研發團隊，總部位於台灣台中市。核心成員均擁有超過20年的電信等級網路維運以及軟體開發經驗，集合網路、資安、作業系統與Kernel、電腦硬體與虛擬機、C語言、PHP/Java、資料庫、大數據處理與雲架構、美術與設計等各領域專長的人才。由N-Partner公司所開發的N-Reporter以及N-Cloud雙產品線為當前全球唯一能夠完美整合SNMP、Flow與Syslog三種主流網管和資安事件分析技術的IT維運系統，領先的技術包括：Any-to-Any分析，能針對各個日誌事件與所有IP進行歷史行為自動學習進而建立動態基準，用以發覺異常並即時告警；關聯SNMP、Flow與Syslog三種數據，提供IT管理者清楚的障礙除錯依據等。此外，N-Cloud維運平台更運用了雲架構來提供高處理效能、幾無限制的延展性以及萬人同時操作使用的能力，適合做為NOC/SOC合一SaaS服務，已經獲得多家大型教育網、金融公司、跨國企業與電信公司採用做為網路與資安的維運平台。在2015年之前，N-Partner公司的商業版圖已經橫跨海外。

■ 硬體規格

	NP-RPT-TW-Probe-5Port	NP-RPT-TW-Probe-2Port-SR/NP-RPT-TW-Probe-2Port-LR	NP-RPT-TW-Probe-40G	NP-RPT-TW-Probe-100G	NP-RPT-TW-Probe-2Port-C	NP-CLD-E-REC-TW
功能	All-in-One Appliance，內建專屬 OS、數據庫與應用程式					
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	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 Gold 5315Y (12M Cache, 3.20GHz)	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 100 GbE LAN + Dual Port 10GbE 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	64G DDR4 x1	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	Integrated IPMI 2.0 and KVM with Dedicated LAN
Power Supply	350W Platinum Level	350W Platinum Level	350W Platinum Level	600W Platinum Level	350W Platinum Level	350W Platinum Level
SSD	500GB	500GB	500GB	480GB	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	10 Gigabit Management Port x 1, 10 Gigabit Mirror Port x 1, 100 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	14TB	4TB	4TB

■ N-Probe VM 建議規格

1. 請準備一台 Server，建議規格如下：

   ✓CPU 建議 E-2334 (8M 快取記憶體，3.40GHz)以上。

   ✓ RAM 記憶體空間須 48 G 或以上

   ✓ 硬碟空間 500G 以上，請依實際需求決定。

   ✓ 安裝 VMware Esxi 6.0 或以上的版本。

2. N-Probe 運行時，若要達到最佳效能，至少需要 32G 的 RAM 記憶體空間。

3. 請準備一台 Windows 電腦，用於管理 VMware Server。

4. 請準備 N-Reporter/N-Cloud系統，接收 N-Probe/External Receiver 送來的 Flow 或 Syslog 流量。

■ 產品料號

產品料號	料號說明
NP-RPT-TW-Probe	Flow and DNS/HTTP data export. Software Module with 1 Year MA
NP-RPT-TW-Probe-M	Standalone mini box model with 1 Year MA
NP-RPT-TW-Probe-5Port	Flow and DNS/HTTP data export. Hardware device. 1G interface. 5 ports build-in with 1 Year MA
NP-RPT-TW-Probe-2Port-LR	Flow and DNS/HTTP data export. Hardware device. 10G LR interface. 2 ports build-in with 1 Year MA
NP-RPT-TW-Probe-2Port-SR	Flow and DNS/HTTP data export. Hardware device. 10G SR interface. 2 ports build-in with 1 Year MA
NP-RPT-TW-Probe-2Port-C	Flow and DNS/HTTP data export. Hardware device. 10G Copper interface. 2 ports build-in with 1 Year MA
NP-RPT-TW-Probe-40G	Flow and DNS/HTTP data export. Hardware device. 40G QSFP+ interface. 2 ports build-in with 1 Year MA
NP-RPT-TW-Probe-100G	Flow and DNS/HTTP data export. Hardware device. 100G QSFP28 interface. 2 ports build-in with 1 Year MA
NP-CLD-E-REC-TW	External-Receiver platform. Collect and forward data. Include 1 year MA
NP-CLD-E-REC-VM-TW	External-Receiver VM version. Collect and forward data. Include 1 year MA

Tel / 04-23752865 Fax / 04-23757458
業務詢問 / sales@npartner.com
技術詢問 / support@npartner.com