N-Probe 7

DATASHEET

Next Generation IT Operation Platform
Integrate Network Management, Flow Analysis and Log Reporting

N-Partner

2024/03/20

Nowadays, the usual way to get Flow data for analysis is setting routers or switches to send NetFlow or sFlow. However, some switches cannot send it; also, recording Flow data would cause high CPU usage for routers and switches. The problems make IT administrators uncertain whether to enable NetFlow/sFlow function. sFlow occupies less CPU resource by using packet sampling to record data, but this way, most traffic wouldn't be recorded, and there can be discrepancy between the real situation and the analyzing result.

N-Probe made by N-Partner can deal with the problems easily. N-Probe can collect all the traffic data, can be deployed with simple steps, and will barely impact on the devices it connects with. Most switches support port mirroring, so users only have to send the mirrored data to N-Probe; it will transfer them into 1:1 NetFlow and send to Flow analysis system for analyzing. For IT administrators, traffic analysis is an essential part of IT management, and with appropriate Flow analysis tools, like N-Reporter/N-Cloud made by N-Partner, the important messages like events, packet direction, and usage statistics will all be very clear. When there are abnormal events or traffic, IT administrators can use them to locate where they come from and debug with better efficiency. With N-Probe, traffic analysis will be much easier.
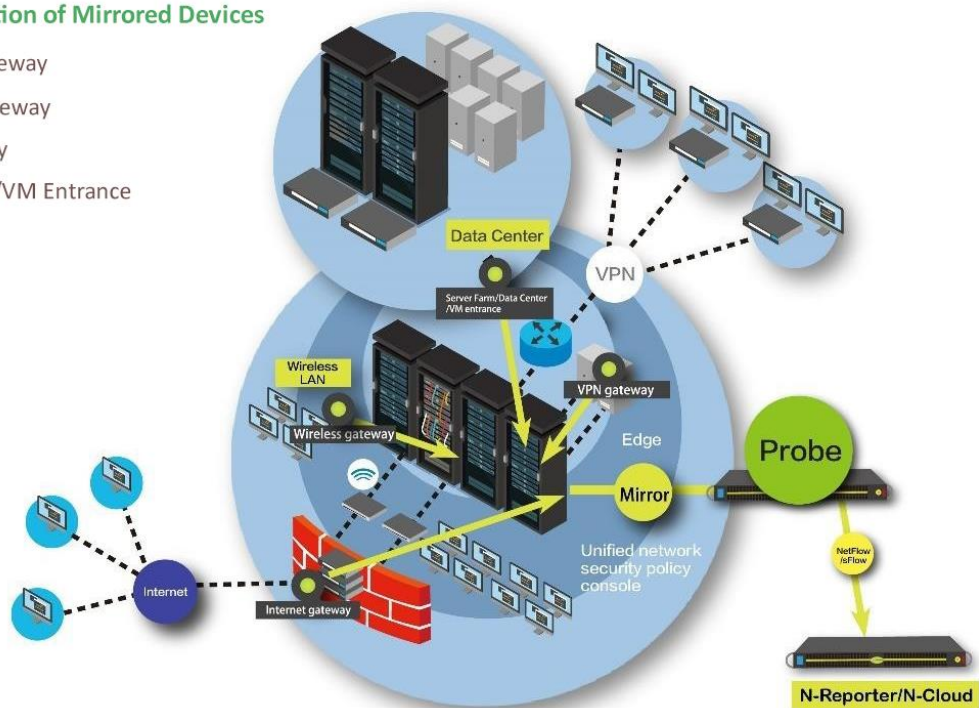
To have full understanding of global traffic and user behavior, the data of each major network node, like internet gateway, core switch in data center, VPN gateway of headquarter, and wireless gateway, must be recorded. The data of these devices can be mirrored with mirror port and will be sent to Flow analysis system after being transferred into 1:1 NetFlow by N-Probe. This way, user can know clearly about the traffic information of Home network.

N-Partner

Besides transferring 1:1 NetFlow, N-Probe can also analyze DNS traffic of layer 7. DNS traffic will be sent to N-Probe the same way as mirror traffic. N-Probe will analyze DNS query packets to get DNS query logs and then send them to any log system or SIEM with Syslog protocol for storage or report making to meet auditing standards or for IT management such as domain access analysis. N-Probe gets DNS log in real time with efficiency over a million EPS(Event Per Second). It is applicable to most network environments, and with it recording and sending DNS log, DNS servers can maintain their efficiency. As for cyber security, comparing DNS log with threat intelligent list helps keep Home network from connecting to malicious domains, and users can detect sooner if there is malware in Home network. What is more, DNS logs form N-Probe contain NX domain information, and N-Cloud/N-Reporter will make NX domain list accordingly and write them into devices to activate action function(Note 1) to protect DNS servers from enormous NX domain query attack.

(Note 1) The list of devices supporting the function is keeping upgraded, please contact N-Partner for the latest information.

Dashboard (DNS Analysis and Malicious Domain Connection Monitoring)

We have hardware and software version of N-Probe for users' different needs. Software version can be applied in virtual platforms, like VMware; hardware version has several interfaces for network environments with different needs. For example, there are 1G and 10G mirror traffic interface, and user can also choose LR or SR optical interface. N-Probe can transfer up to 40Gbps mirror traffic into 1:1 NetFlow each time and output; it supports NetFlow v5 and NetFlow v9.
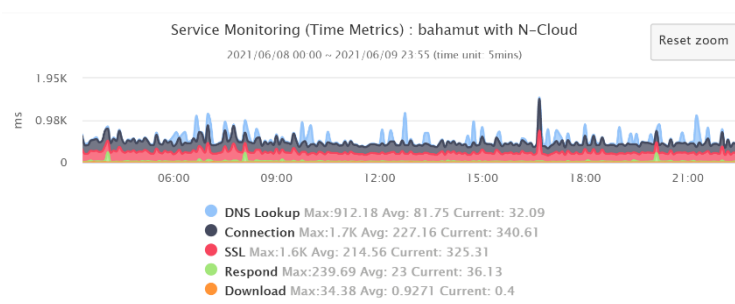
N-Partner

Value-added Module

In addition to the 1:1 Netflow data output and DNS analysis functions mentioned above, N-Probe also provides the following value-added functions which users can purchase as need.

If user's network structure contains server rooms or branch offices in different geographical locations and each connects through internet/VPN, the best operation suggestion is to deploy N-Probe in all places and activate External Receiver module to collect SNMP/Flow/Syslog data. The data are encrypted and compressed before being forwarded to N-Reporter/N-Cloud with a compression ratio that is 5:1, greatly reducing the bandwidth load of internet/VPN and strengthening the integrity and security of the data during transmission. External Receiver can also store and forward data; when internet/VPN is disconnected, the Flow/Syslog data will be temporarily stored and completely reforwarded to N-Reporter/N-Cloud after the connection is restored. External Receiver can be built in HA(Master/Slave) cluster for availability. Furthermore, External Receiver module includes SNMP monitoring function, which does SNMP polling to local devices to obtain IP/MAC and MAC/Port corresponding tables to assist in network management.

N-Probe also has performance monitoring (PM) module. The first function is to monitor the round trip time (RTT) of each monitored target by using ICMP ping packets; the second function is to simulate the process of people browsing web services and N-Probe will separately record the response time of several stages in the process: DNS query and response, connection establishment with web server, SSL transaction, web page response and content download; the system will make time charts with the data. To be closer to users' experience at every moment, IT administrators can deploy N-Probe with PM module in any network location, such as office areas (OA), branch offices, and IDC leased by telecommunications carriers. N-Probe will send the monitoring data to the intelligent IT operation platform, N-Reporter/N-Cloud, to make reports for users to view the network quality of each monitored target, achieving multi-point, multi-angle, and continuous monitoring and analysis. Besides, with the prediction function of N-Reporter/N-Cloud, it can also predict the trend in the next few hours to several months, and users can receive an alert before the delay becomes serious.

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

Service Monitoring (Time Metrics) : bahamut with N-Cloud
2021/06/08 00:00 ~ 2021/06/09 23:55 (time unit: 5mins)

● DNS Lookup Max:912.18 Avg: 81.75 Current: 32.09
● Connection Max:1.7K Avg: 227.16 Current: 340.61
● SSL Max:1.6K Avg: 214.56 Current: 325.31
● Respond Max:239.69 Avg: 23 Current: 36.13
● Download Max:34.38 Avg: 0.9271 Current: 0.4

N-Partner

N-Partner Introduction

      N-Partner Technology Ltd. Co., founded in 2011, specializes in Big Data and AI and Abnormal Analysis. The headquarters is set in Taichung, Taiwan. All of our core members have over 20-year experience in network operations and software development. We have professional experts in various fields, including internet, information security, operation system, Kernel, hardware and virtual machine, C language, PHP/Java, database, big data processing and Cloud computing architecture, artistic designing, etc.

      N-Reporter and N-Cloud, developed by N-Partner, are the only IT operating systems that can correlate the three main technologies, SNMP, Flow, and Syslog, to do data analysis. We use the leading technology including Any-to-Any analysis, which establishes dynamic threshold for each event and IP based on event logs and history records to detect abnormal activities and to send out real-time alerts. With correlation and analysis, IT administrators can have detailed information to debug readily.

      What is more, Cloud computing architecture is used in N-Cloud for high processing efficiency, high expandability and the ability for lots of people to use simultaneously; it can be used as SaaS Service with both NOC and SOC, and has been applied by plenty educational networks, finance companies, multinational corporations, and telecommunications as operation platform for network security. By 2015, N-Partner has expanded the business scale to China and gradually to Southeast Asia.

■ Hardware

|	NP-RPT-EN-Probe-5Port	NP-RPT-EN-Probe-2Port-SR/NP-RPT-EN-Probe-2Port-LR	NP-RPT-EN-Probe-40G	NP-RPT-EN-Probe-2Port-C	NP-CLD-E-REC-EN
Feature	All-in-One Appliance, Built- in Dedicated OS, Database, and Program				
Size	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 Recommended Specification

1. Please prepare a server; the recommended specifications are as follows:

   ✓ CPU: E-2334 (8M cache memory and 3.40 GHz) or later versions

   ✓ Memory: 48GB or more

   ✓ HDD space: 500GB or more, according to the needs

   ✓ Install VMware Esxi 6.0 or later versions

2. To reach the best performance of N-Probe, at least 32G RAM memory is needed.

3. Please prepare a Windows computer to manage VMware server.

4. Please deploy N-Reporter/N-Cloud to receive Flow or Syslog data sent from N-Probe/External Receiver.

N-Partner

■ Material

Material Code	Description
NP-RPT-EN-Probe	Flow and DNS/HTTP data export. Software Module with 1 Year MA
NP-RPT-EN-Probe-5Port	Flow and DNS/HTTP data export. Hardware device. 1G interface. 5 ports build-in with 1 Year MA
NP-RPT-EN-Probe-2Port-LR	Flow and DNS/HTTP data export. Hardware device. 10G LR interface. 2 ports build-in with 1 Year MA
NP-RPT-EN-Probe-2Port-SR	Flow and DNS/HTTP data export. Hardware device. 10G SR interface. 2 ports build-in with 1 Year MA
NP-RPT-EN-Probe-2Port-C	Flow and DNS/HTTP data export. Hardware device. 10G Copper interface. 2 ports build-in with 1 Year MA
NP-RPT-EN-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-EN	External-Receiver platform. Collect and forward data. Include 1 year MA
NP-CLD-E-REC-VM-EN	External-Receiver VM version. Collect and forward data. Include 1 year MA

N-Reporter   N-Cloud   N-Probe   N-Robot
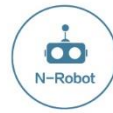
Tel : +886-4-23752865   Fax : +886-4-23757458
Sales Information : sales@npartner.com
Technical Support : support@npartner.com