N-Reporter 7

DATASHEET

Next Generation IT Operation Platform

Integrate Network Management, Flow Analysis and Log Reporting

2024/03/29

Nowadays, most network devices, servers, and security products can send Syslog and Flow data; for IT administrators, with complete Syslog data, it will be easier to query events, and Flow record helps understand traffic in Home network.

N-Reporter, N-Partner developed with multiple innovative technologies, can collect, store, and analyze Syslog/ Flow data to make various reports and for users to do query. What's more, it correlates L3/L4 packet/byte from Flow with L7 events from Syslog, so IT administrators can know completely about every detail in Home network. N-Reporter is the most efficient, user-friendly reporter and analyzer with powerful functions.

Software Features

- Collect Syslog data from various devices and brands.
- User can query system status like version, CPU and memory utilization, received Syslog/Flow data amount, etc.
- Collect Flow data with different format, including Netflow v5/v9/v10, sFlow v4/v5, Jflow, etc. and can do traffic analysis with traffic logs.
- With Chinese and English Web (HTTP/HTTPS) interface; user access right can be verified as need.
- User can connect to the system with Console cable or through SSH and open CLI (Command Line Interface) for operation.
- Provide basic settings in web interface, like IP address, gateway, DNS, and static route. Users can also perform the operations of reboot and shutdown. Additionally, N-Reporter supports users to reset the password and restore the system to factory settings.
- Support IPv6 environment and IPv4/IPv6 dual stack environment.
- Support SNMP v1/v2c/v3 to monitor network devices, and can show a particular IP in Home network is on which switch.
- Built-in treeview topology, able to add each device into a categorized list as root directory and subdirectory, and it can be folded and unfolded. When there is anomaly in any device, an icon will show right after the category name and the upper ones and an alert sound will be emitted to notify users.
- Use SNMP to monitor device status, including CPU/Memory utilization,interface traffic, broadcast/error information, ICMP, etc. User can set threshold value for all monitored items above, and the system will send alert when threshold is exceeded.
- Users can drill down by clicking CPU/ memory utilization chart, and the system will correlate the Syslog/Flow data to make TOP N report and a ranking list. Users can also set own OID and monitor the status as need.
- Make automatic topology for all devices in Home network, and interfaces with different traffic amount will be marked in a separate color.
- User can set multiple query criteria for the system to do logical calculation (or/not); the criteria include keywords, IP, severity, and so on, and the number is unlimited.
- With IP name mapping function, IP and network name will show in event query and reports.
- With port name mapping function, user can define different name for each port as need (e.g., Port 80 as HTTP).
- Built-in Flow analysis and statistics; automatically make Flow charts (Packet/Byte) and Top N utilization reports.
- Provides user-defined threshold report of the packet size (64/128/256/512 Bytes) in units of service/department/branch.
- Provides IP geolocation information (country category), flow correlation graphs for departmental organizations or IPs or even well-known services (such as Google/Facebook/Line, etc.) and a suspicious domain/IP database for users to perform log and flow matching functions.

Additionally, the system has an automatic database update mechanism.

- Receive logs through the Syslog protocol and has built-in normalization function, which can display the date, event name, severity level, IP address, user name, packet/byte transfer amount and other information in the log in different fields of the same table.
- Built-in real-time flow analysis and statistics function. According to the monitoring criteria such as traffic source, destination IP segment, host name, username, port number, protocol, network interface, traffic output device, MAC address, country, packet size distribution and other criteria to make a TOP N report or an instant flow (Packet/Byte) line graph, and the threshold value can be customized, and the alert will be triggered if the threshold value is exceeded.
- With Flow analysis function, N-Reporter is able to detect and analyze abnormal traffic (DDoS, Host Scan, Port Scan, Flooding, Burst Session etc.) in real time.
- Users can send commands blocking particular IP addresses to network or security devices for collaborative defense (only support devices of some brands).
- About the collaborative defense in the previous point, user can set criteria for N-Reporter to send blocking commands automatically.
- Able to define dynamic base line with received Syslog/Flow data, detect events and IP with traffic burst in real time, and then send alerts.
- Users can do drill down by clicking any spot in charts to get further information.
- Built-in pie charts, bar charts, and line charts; user can make customized reports as need.
- Traffic reports can show Max/Avg/PCT 95 amount.
- Users can customize columns for event display and PDF files output.
- Make Chinese reports; users can also export Chinese PDF files.
- Users can customize PDF output Logo and layout.
- With Windows AD analyzing function, able to find the corresponding username of each IP.
- Provide login and logout audit logs of various operating systems, including Linux, Windows server 2003/2008/2012/2016, and so on.
- Send real-time alerts when abnormal login or brute-force attack appears.
- Provide login and logout audit logs of various databases, like Oracle, MSSQL, MySQL, etc.
- Provide audit reports of Windows file sharing.
- Built-in dynamic Dashboard can present information such as real-time event content, alert status, and event statistics; users can define and adjust Dashboard content, grid size and screen arrangement according to needs. There are also event statistics reports, flow graphs and system status for various time periods (one hour/day/week) for users to apply.
- Provide access control list; user can set IP white list.
- Able to back up Syslog original raw data.

- Record user's complete historical operation records and user can output them as PDF files.
- Users can get event details through open interface.
- Complete alert system, with which user can send different alerts and reports to different email groups.
- Monitor CPU, fan and disk status; send alerts when there is anomaly.
- With SNMP Trap, alert will be triggered in real time when the status of hard disk is abnormal.
- With SNMP Agent, users are able to view information about the system's operational status.
- Newest self-developed compression and storage technology; it conforms to the internationally recognized cryptographic hash, FIPS 140-2, SHA2-256 , SHA2-512 and AES, ensuring the data is complete and undeniable. The compression ratio is 10:1, highly increasing storage utilization.
- Always connect to N-Partner; the system can get the latest firmware automatically.
- Supports WMI (Windows Management Instrumentation) to retrieve Windows Server logs.
- Supports real-time visualization of attack dynamics in both 2D and 3D global views.
- Able to generate the Top 1,000 report for 10 million Syslog data within 48 seconds and search for a specific IP in 100 million Flow data in just 250 seconds.
- Able to receive Syslog more than 10,000 EPS (Events Per Second) and with the highest level of Flow module can receive up to 20,000 Flow Records per second.
- Supports continuously monitor the node's availability and network quality (Round Trip Time, RTT) of the monitoring node through the ICMP protocol.
- Automatically associates IP addresses with their corresponding Switch/Interface information and allows users to trace and query historical mapping records.
- Provides a mobile application that allows users to check real-time status and receive fault notifications on their mobile devices.
- Provides a two-layer TOP N report function. For each result sorted by the first layer TOP N, new statistical aggregation criteria can be set again to generate the second layer TOP N report. The statistical aggregation criteria set in the two-layer TOP N report can be different. For example, the first layer is IP traffic ranking and the second layer can be event ranking.
- Built-in Top N module that allows users to customize and query Top N statistical reports at any time. Users can select various parameters such as time intervals, event keywords, source/destination IP addresses, source/destination ports, devices, chart types, etc., to create various types of reports, including hourly, daily, weekly, monthly, quarterly, semi-annual, and annual reports.
- Built-in event module, users can search for Syslog and Flow detailed data at any time.
- Provides a database storage days prediction function.

- Supports database backup and restoration.
- Features an automatic learning capability that utilizes historical usage data from Syslog/Flow (e.g., data from the past hour or past few days) to create a baseline using advanced algorithms. This allows the system to instantly analyze and identify abnormal spikes in events or IP traffic. We can present the occurrence of these spikes with accurate timestamps in the form of trend grap hs and send out alerts to users accordingly. There is no need for manual threshold configuration as our system establishes dynamic thresholds automatically based on historical patterns and usage data.
- Built-in monitoring reports, and users can customize their own monitoring conditions based on different criteria. When abnormalities occur, the system will immediately notify the administrators.
- Users can set multiple offline reports as a group.
- Users can export analysis result and reports as different formats, like PDF, XML, CSV, and so on.

System Specifications

N-Partner's RD department has dedicated in efficient big data collection, storage, and analysis. With self- developed database optimization named N-Partner 《Smart DB》, N-Reporter can minimize the time of data query, statics, and sorting. Practical tests show that it takes only 48 seconds for the system to analyze 10 million Syslog data and make TOP 1,000 report, and only 250 seconds to find single or multiple IP addresses in 100 million Flow records.

Every piece of Syslog/Flow data should be received to show complete Syslog/Flow events and traffic and to ensure statistical results are accurate. With Flow module, N-Reporter receives up to 10,000 Syslog data per second and from 500 devices; under no circumstances will it lose Syslog data from the devices. What's more, with Flow module of the highest level, it can receive more than 20,000 Flow records per second.

Besides high speed and stable performance, we also use appliance for its simple maintenance process. During warranty period, if the hardware is broken, we will run RMA process, so users don't have to wait for debugging.

Multiple Criteria for Logical Calculation and Reports Making

In IT operation, data query takes the most time. Since there is increasing Syslog/Flow data to receive, user need reporting tools that provide flexible criteria and can get results quickly.

N-Reporter has intelligent query function, and with logical calculation, it can help user do various query as need.

Event Column and Filtering Parameters

Device (User can query events in single or multiple devices)
Interface
Time
Event Keyword
User name
Source/destination IP (support CIDR and discontinuous sections)
Source/destination Port
Source/destination location
Severity
Event type (Security, Traffic, Audit, Web, etc.)
Action (block, permit, etc.)
Packet/byte amount and size
Policy ID
AS Number

Logical calculation is using (Or) and (Not) to find correlation result of every criterion. For example, user can put (Or) between each keyword to search for events with plural criteria and use (Not) to exclude some particular keywords from showing in the result.

Not only “keyword” but also “IP” can user do logical calculation with, or with both of them. The following are some examples:

Event Keyword
P2P+Streaming Search for all events whose name includes P2P and Streaming
P2P+Streaming! BT Search for all events whose name includes P2P and Streaming, but exclude those with BT

IP
192.168.1.0/24+192. 168.2.0/24 Search for all events in the two network segments
192.168.1.0/24+192.168.2.0/24 !192.168.1.100-192.168.1.200 Search for all events in the two network segments, but exclude the events in 192.168.1.100-200

The number of query criteria is unlimited; with N-Partner《Smart DB》, N-Reporter can do query rapidly, and even if there are lots of criteria, the searching process will not take much time.

Flow Analysis by Flow Module

Flow data (e.g. Netflow/sFlow) play an important role for traffic analysis in IT management; IT administrators learn which IP or unit uses the most network resource and which protocol (e.g. Port 80, Port 21) consumes the most bandwidth with Flow.

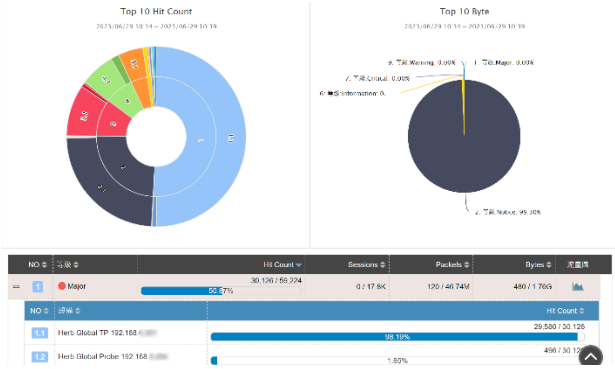
Flow module provides functions fitting IT administrators’ needs for Flow analysis mentioned above, such as Top N analysis and advanced drill down query, long-term Flow charts on specific targets, and Flow records of certain IPs or units.

Flow module can be used for different formats, like Netflow V5/V9, sFlow V4/V5, and JFlow; also, it can be used in the environment without Flow device but with switch mirror port. Using N-Probe, user can transfer the mirror port data and Flow information to N-Reporter.

Syslog and Flow Correlation

IT administrators had to build Syslog storage and Flow analysis for IT management or regulatory requirements. However, the two separate systems each has only partial, incomplete data, so IT administrators spent much time doing query and cross reference when operating and debugging to analyze and find possible correlation.

N-Reporter correlates L3/L4 packet/byte from Flow with L7 user behavior from Syslog, so IT administrators can know every detail of Home network. For example, when IT administrators find in TOP N report query by Flow that some IP or unit sends numerous packets, through N-Reporter’s correlation analysis, the details will soon be shown: in this example, the packets are from P2P sharing. The other way round, when Syslog data from L7 security devices show that there is a DDoS attack, through N-Reporter’s correlation analysis and traffic chart of the attack, IT administrators can know the source IP and how much it impacts Home network. With this information, it’s easier for IT administrators to defend.



Various Realtime Reports

N-Reporter's realtime online reports can show dynamic content and have various statistical charts. User can choose different types as need, including pie chart, bar chart, line chart, etc. Reports also support logical calculation (Or/Not), and user can use all the criteria to make customized reports for various events.Logical calculation correlates multiple filtering parameters, and the reports can be closer to user's needs. For example, user can make daily reports about sever attacked events, weekly traffic reports about employees visiting social networking sites and using streaming media, and monthly statistics about database access.

Report Parameters

Event keywords, source/destination IP/port, device, and report type

Working time (daily time period, like 8:00~18:00)

Working days (user can set to record the eventfrom Mon. to Fri.)

Types (hourly, daily, weekly, semi-monthly, monthly, quarterly, semi-annual, and annual)

Sending time

Report receiver

Report format (HTML, PDF, XML, CSV)

Regular Off-line Reports

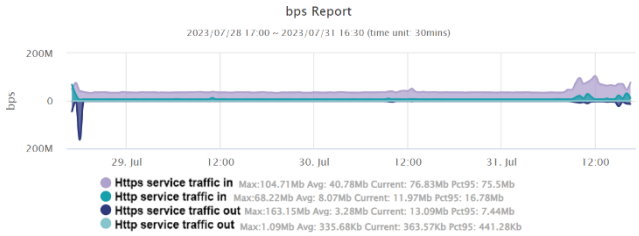
The system would make regular reports, so users do not have to make and output reports manually. User can set parameters for the system to make reports, and N-Reporter will send them to particular e-mail addresses.

N-Reporter also has daily, weekly, and monthly audit reports conforming to regulatory requirements, including reports about user login/logout, login failure, and password guessing for each sever and database.

Customized Line Chart and Anomaly Surveillance

IT administrators can use different criteria to make various line charts to see the trend of events or traffic. With different keywords, IT administrators can see some particular events' timely changes. For example, set "Telnet/SSH Login Fail" to see if there is account/password guessing event; set any server to see the connected times, Flow records, and whether there is anomaly; set "Port 445" to see the traffic amount and if it is malware-infected. User can also set threshold value for line charts, and if the hit count of an event exceeds threshold or there is abnormal traffic, the system will send abnormal alert email to the manager.

With Flow module, user can make line charts about event, bps, pps, and session in the same report to do cross reference and analysis.



Abnormal Login Report

N-Reporter analyzes login in home network, and when anomaly occurs, it will send realtime alerts to manager. It is the second line of security defense of host and can effectively blocks hacker invading.

Intelligent Auditing

Account/password guessing

Unknown IP login

Alert IP login

Dashboard: Dynamic Statistics and Status

User can define own dashboards in N-Reporter. Dashboards are dynamic and will keep updating.

Dashboards can be made based on different criteria as preference, like system status, event ranking, trend analysis, abnormal alert, and so on. N-Reporter would list the information in one interface, and user can view all the details at any time. User can also click any item in dashboard to drill down, and the system will go to the corresponding page for user to see further information and deal with the anomaly. This function is user-friendly, and with this, user can build proper security center for Home network.

Action Module for Collaboration Defense

N-Reporter has extraordinary real-time analysis function; user can do more advanced management with the results. With action module, N-Reporter can quickly find which switch and interface the abnormal IP is on, and IT administrators can precisely do further operation by its severity to make Home network back to normal. As for the attacks from non-home, user can send IP blocking command to the network or security device at internet entrance to defend in real time.

User can also set keywords for the system to automatically block some events. The system will analyze the criteria set by user, and once threshold value is exceeded, the system will block the abnormal IP on devices executing collaborative defense.

N-Reporter's Action module with trend analysis is the most efficient way to detect and block DDoS attacks!

Built-in AI, Automatic Trend Report by Historical Data

N-Reporter has built-in AI which receives Syslog/Flow data to see if there is IP with abnormal event hit count, packet or byte, and sends alert about the event details to IT administrators for them to deal with it right away. User do not have to guess or manually set threshold value; with behavior-based monitoring and analysis, user can know all anomaly in Home network, and IT operation will be easier.

N-Reporter is an event query and report making system with powerful functions and is also an analyzer that can do actual trend analysis.

Performance Monitoring Module – Network Node Ping Monitoring

N-Reporter will continuously send Ping tests through ICMP protocol to the monitored network nodes, allowing administrators to understand whether the nodes are functioning properly and measure and record their response times. This function helps assess the quality of the network. Depending on the licensing quantity, users can conduct Ping measurements for multiple network nodes (IPs), with a minimum measurement interval of one minute. Network administrators will be able to monitor selected network nodes, such as network devices, critical IP gateways, and external IP nodes, to determine operating normally and to assess response times. With built-in self-learning function, N-Reporter will automatically detect poorly performing network nodes and send alerts. A key feature is its ability to correlate with Flow and Log data, analyzing the reasons for poor performance. This functiom enables network administrators to quickly address issues and restore network quality.

Performance Monitoring Module - Web Website Service Monitoring

Our system simulates the process of users opening a web browser and viewing a webpage, continuously performing simulations on the monitored web websites. This allows for the assessment of its normal functioning, measurement and recording of response times at various stages throughout the browsing process, and analysis to determine the quality of the web application's service. Based on the licensing quantity, our system can measure multiple web applications with intervals as short as one minute. This aids network administrators in assessing the normalcy and response speeds of user browsing for selected web services, including self-hosted, cloud-based, and important public services.The entire process of the response is recorded in five stages: DNS resolution, TCP connection establishment, SSL encryption, connection establishment response, and homepage download completion. With bulit-in self-learning function, N-Reporter will automatically detects poorly performing web services and sends alerts, allowing network administrators to quickly address issues and restore web service quality.

SNMP Topology

For software using star topology, it is hard to make topology for large network. User usually have to view it in several divided pages or zoom in/out the original image to find a particular device. N-Reporter uses treeview topology, which categorizes devices as root directory and subdirectory and can be folded and unfolded. This way, user can view all the device status in only one interface. When there is anomaly in any device, an icon will show right after the category name and the upper ones, so user can find it immediately.

User-friendly Operation Interface and Functions for Management

User can use Web interface to operate N-Reporter. Also, the data in N-Reporter's database can be backed up or restored with FTP, NFS, and SMB.

Relay Syslog and Flow

Users can define the forwarding function for Syslog and Flow data, which preserves the original source IP of the received data and forwards it to other receiving devices.

High Expandability

N-Reporter has high expandability mechanism. If user's devices are increasing and need better processing capacity, user can expand the system by transferring N-Reporter into a part of private cloud, N-Cloud. The original settings and data can be retained; at the same time, the storage and efficiency will increase.

Conform to Audit Regulations

N-Reporter conforms to the cryptographic module recognized internationally, FIPS 140-2, and uses SHA2-256, SHA2-512 & AES for encryption, ensuring that the data is complete and undeniable.

Hardware

	NP-RPT-K-EN	NP-RPT-D-EN
Features	All-in-One Appliance, Built- in Dedicated OS, Database, and Program	All-in-One Appliance, Built- in Dedicated OS, Database, and Program
Size	1U Rackmount, 19 Inch Standard Wide RackMount Industry Server	1U Rackmount, 19 Inch Standard Wide RackMount Industry Server
CPU	Intel Xeon E-2334 Processor (8M Cache, 3.40GHz)	Intel Xeon E-2334 Processor (8M Cache, 3.40GHz)
Memory	32G DDR4 x 2	32G DDR4 x 2
Ethernet Controller	Dual Port GbE LAN	Dual Port GbE LAN
IPMI	Integrated IPMI 2.0 and KVM with Dedicated LAN	Integrated IPMI 2.0 and KVM with Dedicated LAN
I/O Port	1 VGA, 1COM	1 VGA, 1 COM
Power Supply	350W Platinum Level	400W Platinum Level x 2
SSD	500GB	500GB
HDD	4TB, up to 12TB HDD (4x4T with RAID5)	4TB, up to 12TB HDD (4x4T with RAID5)
RAID Card	Supports RAID 0, 1, 5	Supports RAID 0, 1, 5
AC Power	100v-240v, 4.2-1.8A, 50-60Hz	100v-240v, 4.2-1.8A, 50-60Hz
Operating Temperature	0°C-50°C (32°F-122°F)	0°C-50°C (32°F-122°F)
Operating Relative Humidity	8% to 90% (Non-condensing)	8% to 90% (Non-condensing)

N-Reporter 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 its later versions.
   - ✓ Memory: 80GB or more
   - ✓ HDD space: 500GB, 1T, 2T or more, according to the needs. 2T is recommended.
   - ✓ Install VMware Esxi 6.0 or its later versions.
   - ✓ Install Windows Hyper-V 2016 or its later versions
   - ✓ Install KVM 4.2.0 or its later versions
2. When N-Reporter is running, in order to achieve the best performance, it will need at least 64G of memory.
3. Please prepare a Windows computer for managing VMware / Hyper-V / KVM Servers.
4. For N-Reporter VM, it is recommended to have a CPU with 8 cores running at 3.40GHz each, and a memory of 64GB.
5. For the Hyper-V version of N-Reporter VM, the minimum memory requirement is 64G.

■ Material

Material Code	Description
NP-RPT-VM-EN	Syslog collector, reporter and analyzer including 5 devices license and 10 managed SNMP devices with 1 Year MA. VM Version
NP-RPT-K-EN	Syslog collector, reporter and analyzer including 5 devices, 5 services license and 10 managed SNMP devices with 1 Year MA
NP-RPT-D-EN	Syslog collector, reporter and analyzer including 10 devices license, 10 managed SNMP devices and dual power with 1 Year MA
NP-RPT-EN-5Dev	Add 5 devices license
NP-EN-20SNMP	Add 20 managed SNMP devices
NP-EN-50SNMP	Add 50 managed SNMP devices
NP-EN-200SNMP	Add 200 managed SNMP devices
NP-EN-500SNMP	Add 500 managed SNMP devices
NP-RPT-EN-Server-10	Server Module, 10 Services with username resolution feature
NP-RPT-EN-Server-50	Server Module, 50 Services with username resolution feature
NP-RPT-EN-Server-100	Server Module, 100 Services with username resolution feature
NP-RPT-EN-Server-200	Server Module, 200 Services with username resolution feature
NP-RPT-EN-Server-500	Server Module, 500 Services with username resolution feature
NP-RPT-EN-Flow-Lite	Flow Module Lite Version, 2000 records/per second, extra 4T HDD*1 (HDD For B/D/K model Only)
NP-RPT-EN-Flow-Plus	Flow Module Plus Version, 4000 records/per second, extra 4T HDD*1 (HDD For B/D/K model Only)
NP-RPT-EN-Flow-Adv	Flow Module Advance Version, 6000 records/per second, extra 4T HDD*2 (HDD For B/D/K model Only)
NP-RPT-EN-Flow-Pre	Flow Module Premiun Version, 10,000 records/per second, extra 4T HDD*2 (HDD For B/D/K model Only)
NP-RPT-EN-Flow-Unl	Flow Module Unlimited Version, extra 4T HDD*2 (HDD For B/D/K model Only)
NP-EN-PM-100Ping	PM Module. Ping up to 100 nodes (IP Address)
NP-EN-PM-250Ping	PM Module. Ping up to 250 nodes (IP Address)
NP-EN-PM-1000Ping	PM Module. Ping up to 1000 nodes (IP Address)
NP-EN-PM-2500Ping	PM Module. Ping up to 2500 nodes (IP Address)
NP-EN-PM-20Web	PM Module. Do browse web site testing regularly. Support up to 20 web sites

NP-EN-PM-100Web	PM Module. Do browse web site testing regularly. Support up to 100 web sites
NP-RPT-EN-RAID-SM	RAID Software Module and 4T HDD kit*1
NP-RPT-EN-HDD-4T-Kit	4T HDD*1
NP-EN-Ticket-G	Ticket System Module. Gold Version with 1 Year MA
NP-EN-Ticket-P	Ticket System Module. Premium Version with 1 Year MA
NP-EN-PS-I	One-Day Professional Service
NP-EN-PS-T	4 Hours Training coupon
NP-EN-PS-U	N-Reporter/N-Cloud Hardware Upgrade

Tel : +886-4-23752865 Fax : +886-4-23757458
Sales Information : sales@npartner.com
Technical Support : support@npartner.com