N-Partner

N-Partner solution

VPN should be able to do AI and Abnormal Analysis detect problems and solve them

There will be huge loss if the intranet is disconnected for only an hour

For multinational corporations and enterprises with branches in different places, whether the VPN (Note 1) is stable or not has a great influence on operating and branching out. It is crucial for enterprises to prevent VPN from being disconnected when making loss estimation and system recovery plans. The infrastructure of telecommunications and network is more and more completed, and little VPN disconnection is caused by the problem of wire or telecommunication facilities. After analyzing, we can find out that most of the connection problems come from intranet. It is closely related to the fact that computer invaded problems are more and more serious. The invaded internal devices send huge amounts of packets and break VPN, which brings much negative effects to enterprises' productivity and leads to a great loss.

To prevent enterprises from suffering the damage, IT department must give up the old way and set up a new one that can do intelligent analysis for operation.

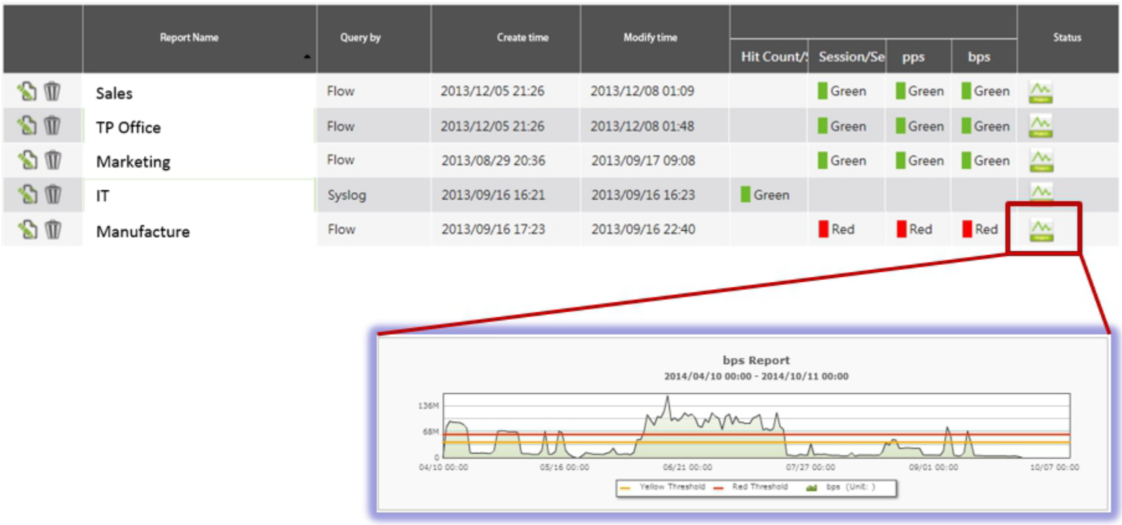
Note 1

VPN here refers to every cross- regional internet technology which users can build by themselves or rent from service providers. If users connect their devices with public network to set up VPN it will be inexpensive but unstable in contrast if users rent VPN from service providers it will be much more stable but expensive if used to communicate with other countries. That is why keeping the expensive VPN from being abused is extremely crucial in IT maintenance.

Automatic learning and analysis technology develop intelligent network operations

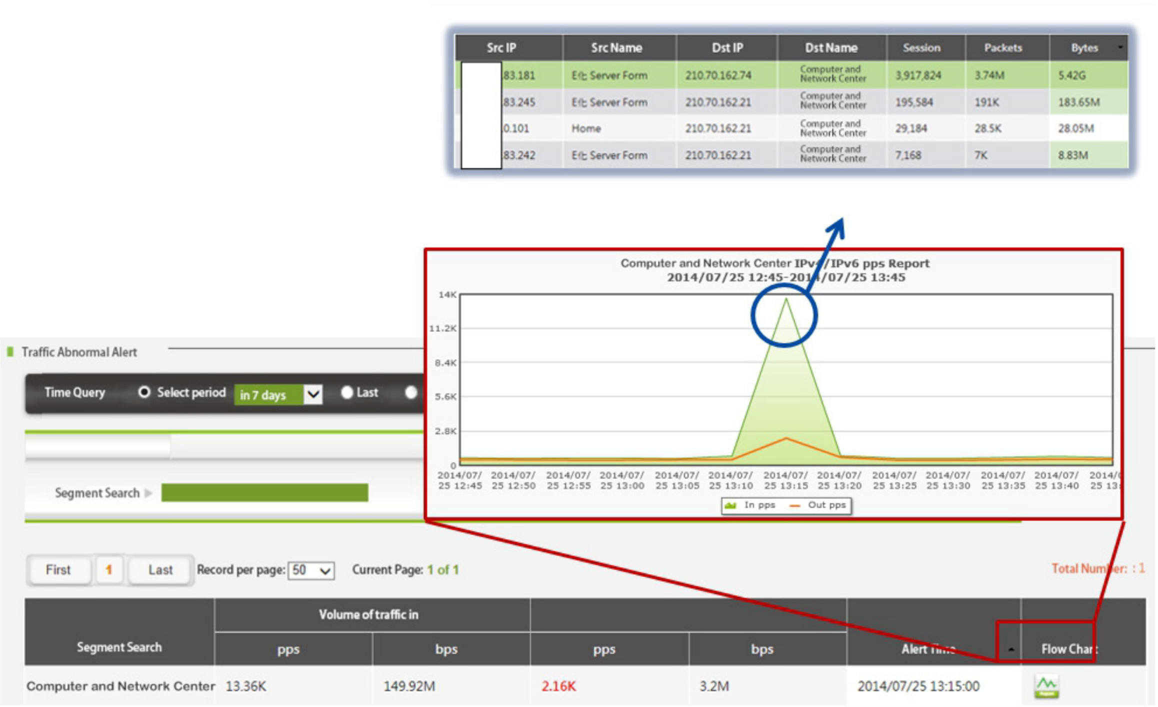
N-Partner's big data analysis can do historical data automatic learning. It records date usage and builds dynamic base line of every IP address, department, and server. It compares the data of each concurrent usage to find out why the number of bytes, packets and sessions explode and it detects the source IP address (attacker) and destination IP address (victim). Then, it sends out alert for users to defend themselves, making IT operation more efficient. There are two main advantages of using this big data analysis. First, IT administrators do not have to set threshold for each IP, but they can still learn the daily usage, receive real time warnings, and deal with the problems right away. Second, no matter how complicated the network is or how many people are using it, the device being attacked can be positioned very soon. It saves lots of time, comparing to the traditional IT operation method, which collects data only after users call help desk and needs administrators to find the attacked device and solve the problems.

Also, it is more efficient to cut the network into different area to monitor. It is best cut according to the work unit's location or based on department; for example, cut it into Plant 1 and Plant 2, floor 1 and floor 2, Engineering Department and Marketing Department, different usages like DNS, Web, Mail Server, and so on, to separately monitor and analyze flow and make reports. Through that way, IT administrator can quickly understand the internet usage of the sections they take charge of. Big data analysis builds dynamic base line for each unit and detects which one has byte explosion. Drill Down can find out where the internet problems come from for IT administrator to fix and recover.



	Report Name	Query by	Create time	Modify time	Hit Count/!	Session/Se	pps	bps	Status
	Sales	Flow	2013/12/05 21:26	2013/12/08 01:09		🟩 Green	🟩 Green	🟩 Green	
	TP Office	Flow	2013/12/05 21:26	2013/12/08 01:48		🟩 Green	🟩 Green	🟩 Green	
	Marketing	Flow	2013/08/29 20:36	2013/09/17 09:08		🟩 Green	🟩 Green	🟩 Green	
	IT	Syslog	2013/09/16 16:21	2013/09/16 16:23	🟩 Green				
	Manufacture	Flow	2013/09/16 17:23	2013/09/16 22:40		🟥 Red	🟥 Red	🟥 Red	

Analyze each organization s flow by CIO point of view users will receive alerts when there is abnormal network usage



Src IP	Src Name	Dst IP	Dst Name	Session	Packets	Bytes
[redacted]83.181	E化 Server Form	210.70.162.74	Computer and Network Center	3,917,824	3.74M	5.42G
[redacted]83.245	E化 Server Form	210.70.162.21	Computer and Network Center	195,584	191K	183.65M
[redacted]0.101	Home	210.70.162.21	Computer and Network Center	29,184	28.5K	28.05M
[redacted]83.242	E化 Server Form	210.70.162.21	Computer and Network Center	7,168	7K	8.83M

Record per page: 50

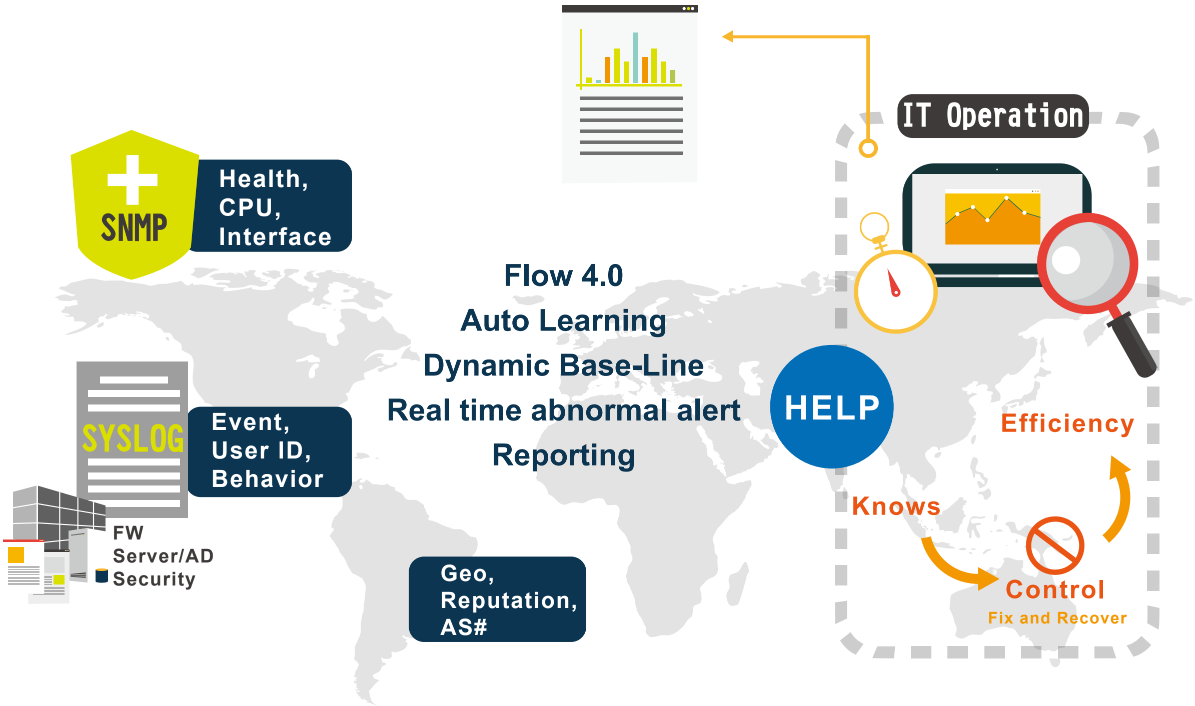
Current Page: 1 of 1

Total Number: : 1

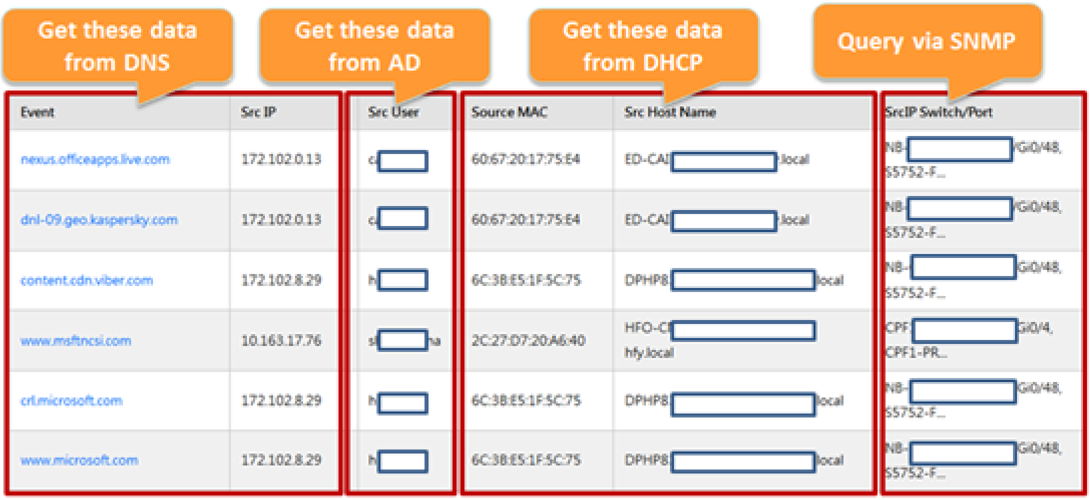
Segment Search	Volume of traffic in				Alert Time	Flow Chart
	pps	bps	pps	bps		
Computer and Network Center	13.36K	149.92M	2.16K	3.2M	2014/07/25 13:15:00	

With Big data analysis IT department can fully understand the daily usage receive real time alerts and deal with the problems in real time.

Correlate AD and SNMP with the analysis result to get the user name and location info



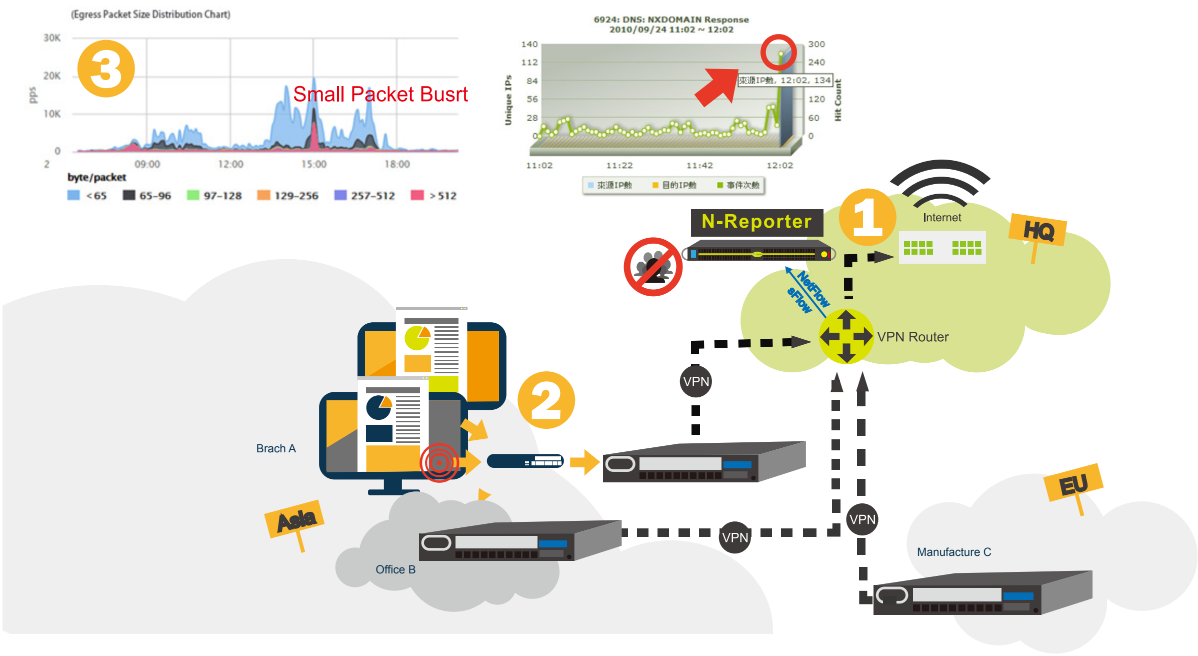
Besides big data automatically learning and real-time flow analysis, N-Partner has another core technology that can integrate SNMP, the health monitoring technique, Flow, the flow analysis technique, and Syslog, the behavior awareness technique, for the IT departments to keep tabs on the network usage. When detecting which IP address is sending abnormal flow, it can find the user name with the information from Windows AD log. SNMP is used to find out the IP address's location, that is, the switch and interface it belongs in.



Event	Src IP	Src User	Source MAC	Src Host Name	SrcIP Switch/Port
nexus.officeapps.live.com	172.102.0.13	c[redacted]	60:67:20:17:75:E4	ED-CA[redacted].local	NB-[redacted]/Gi0/48, S5752-F...
dnl-09.geo.kaspersky.com	172.102.0.13	c[redacted]	60:67:20:17:75:E4	ED-CA[redacted].local	NB-[redacted]/Gi0/48, S5752-F...
content.cdn.viber.com	172.102.8.29	h[redacted]	6C:3B:E5:1F:5C:75	DPHP8[redacted]local	NB-[redacted]Gi0/48, S5752-F...
www.msftncsi.com	10.163.17.76	s[redacted]ha	2C:27:D7:20:A6:40	HFO-C[redacted] hfy.local	CPF[redacted]Gi0/4, CPF1-PR...
crl.microsoft.com	172.102.8.29	h[redacted]	6C:3B:E5:1F:5C:75	DPHP8[redacted]local	NB-[redacted]Gi0/48, S5752-F...
www.microsoft.com	172.102.8.29	h[redacted]	6C:3B:E5:1F:5C:75	DPHP8[redacted]local	NB-[redacted]Gi0/48, S5752-F...

Use Flow/Syslog/SNMP correlation to find the IP address and location with flow anomaly

How VPN problems can be solved in one minute?



Step 1:

Get as much global Flow data as possible. N-Reporter/N-Cloud IT Intelligent operation platform analyze the NetFlow/sFlow data (Note 2) from nodes like core switch, VPN Gateway, and core switches of other factories.

Step 2:

When any unit or IP address has abnormal flow or sends packets abnormally, N-Reporter/N-Cloud will detect it instantly. N-Reporter/N-Cloud can monitor and analyze data from unlimited numbers of IP addresses. Also, besides IP addresses in the intranet, those outside the intranet sending out a great amount of information can also be detect in real time.

Step 3:

When detecting abnormal flow, N-Reporter/N-Cloud will send warnings and show the chart of the flow and packet size. IT managers can click on the graph to drill down and knowing the source IP address, user name, how large the flow is, which department the IP belongs to, and which switch and interface it belongs in.

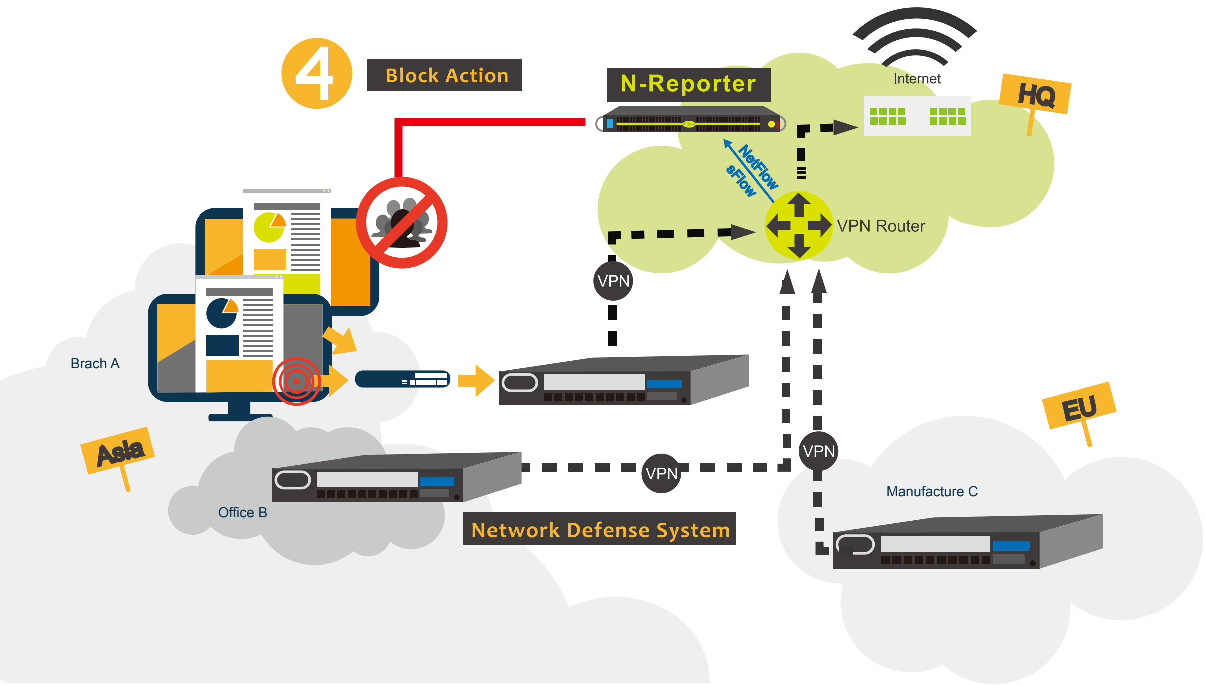
Note 2

When users analyze sFlow data to improve efficiency sampling rate should be as low as possible. If not being able to get NetFlow/sFlow data users can use N-Probe equipment instead. Mirror the flow of important nodes to N-Probe and N-Probe will transform it to NetFlow data in one-to-one scale for N-Reporter/N-Cloud to analyze. Users can deploy N-Probe in every important network segment.

Automatic collaboration defense system

Step 4:

The collaboration defense system is used in N-Reporter/N-Cloud to automatically or manually send blocking instruction to the equipment set in VPN Gateway after recognizing the source IP address and its location, that is, which switch and interface it belongs in (Note 3). This way, VPN will not be blocked or abused, and the damage can be controlled.



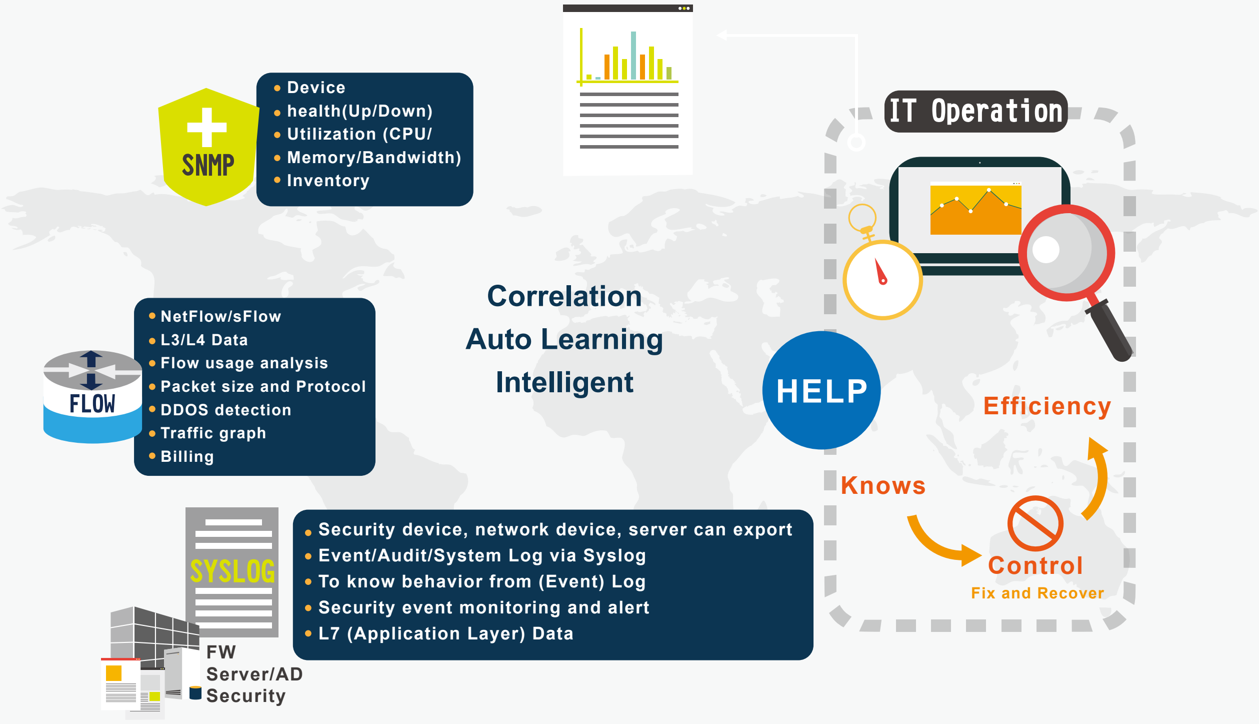
N-Reporter/N-Cloud can also get the location of attackers through SNMP/Flow/Syslog technology, so collaboration defense instruction can be sent to intranet switch to block them. IT Department can set a period of time; after it, the blocking will be removed automatically. All of the IP blocked by mutual defense system will be recorded for future use.

Note 3

At the present stage the collaboration defense equipment N-Reporter/N-Cloud support may change. Please contact N-Partner or dealers for the latest support list.

The core technology of N-Partner helps IT department improve the efficiency to next level

SNMP is usually used to monitor device status, NetFlow/sFlow data from switches and routers to calculate packet numbers and bandwidth utilization, and Syslog to check login, access record, and show security events. SNMP (network management tool) /Flow(flow analysis) /Syslog(log collector or SIEM) are crucial for IT operation; however, now the three methods operate separately, and none of them can show full information of the internet or security status. IT Department has to spend lots of time analyzing the data and finding connection among those from SNMP/Flow/Syslog to find out why there are connection problems. IT Department has lots of trouble dealing with the problems but usually blamed for the instability and poor quality of the system.



- Device
- health(Up/Down)
- Utilization (CPU/
- Memory/Bandwidth)
- Inventory

- NetFlow/sFlow
- L3/L4 Data
- Flow usage analysis
- Packet size and Protocol
- DDOS detection
- Traffic graph
- Billing

- Security device, network device, server can export
- Event/Audit/System Log via Syslog
- To know behavior from (Event) Log
- Security event monitoring and alert
- L7 (Application Layer) Data

To solve the problem, N-Partner develops leading IT operation technology which combines SNMP/Flow/Syslog; artificial Intelligence is built in to connect the data from these three methods together and analyze them. It aims to help IT administrators, through single management platform, to know every detail in the networks they are responsible for and to use big data analysis to record what users often do as well as what all systems are used for to find out Threshold at different moment. This way, abnormal activities can be found soon and the source locked onto; the fixing and recovery IT department had to spend hours, days, or even weeks to do can be completed in just a few minutes. IT department will save lots of time from debugging and will greatly improve its efficiency. Also, it saves all the dealing process as charts to show work performance.

The core technology of N-Partner helps IT department improve the efficiency to next level

- Use SNMP for device status monitoring, including utility of CPU/Memory, Interface flow, Broadcast and Error messages, and disk space. Users can set threshold limit, and warnings will be sent when it is exceeded.

- Have built-in tree topology to categorize devices into root directory and subdirectory based on users' subordination, and like Windows Explorer, it can be folded and unfolded. When there are errors in any device, the indicator lights of parent directory will flash.

- Provide flow graphs by bps, pps, and session, including traffic usage charts, Protocol (TCP/UDP/ICMP) distribution charts, packet size (64/128/256/512 Bytes) distribution charts.

- Users can set particular events or units to be monitored. Time-line reports will be made as line charts to show the data of one particular event at different moments.

- Users can set Threshold on the reports mentioned above; when anyone exceeds the Threshold, warnings will be sent out.

- Get the computer name with DNS, NetBIOS, and DHCP

- Have built-in 2D/3D charts, pie charts, bar charts, and curve diagrams. Users can build customized TOPN report as need.

- Provide Drill Down function, click on CPU monitoring graph and the Flow data will be analyzed and the ranking list will be showed (monitoring devices should be able to get Flow data to execute the function).

- Create security event report, audit report, and web statistic report with Syslog data.

- Create specially-made flow charts for different IP Range (organization), Protocol/Port, AS#, countries, or wire.

- Have built-in correspondence table between IP addresses and countries, IP addresses and AS#, and show which country or AS# one IP address is in.

- Have built-in correspondence table between IP addresses and countries, IP addresses and AS#, and show which country or AS# one IP address is in.

- Work with AD to transfer IP addresses to user names; then record and search for them.

- Input time, keyword, IP, Port, AS#, device, Interface, user name, sender and receiver, packet size, country, and severity to do logical searching. Users can use any number of the search criteria.

- Users can use Drill Down to get further information of all statics and charts.

- Have built-in automatic-learning big data analysis. Automatically calculate the reasonable Threshold by history records, such as in the past hour or past days, for each IT system and user's IP. They are used to make comparison to detect Hit Count explosion, source IP, and destination IP; make run charts to show the exact moment the explosion happens and send out warnings. Users don't have to set up Threshold by manual.

- Use AI and Abnormal Analysis to analyze the log-in and log-out logs of different operating systems, including Unix, Linux, Windows 2003, 2008, 2010, 2013, 2016, and so on. Provide real-time warnings when abnormal login or brute-force attack appears.

- Support build-in Windows file sharing report.

- Have built-in correlation function, integrate the data it gets with those from Syslog and NetFlow/sFlow to show the Packet/Byte/Session numbers (from NetFlow/sFlow) of each event (from Syslog). SNMP locates one IP's MAC address and which Interface it's in.

- Users can set condition. Under specified condition, the collaboration defense function will operate automatically, a useful way to defend DDoS attack.

- Do collaboration defense by sending instructions to block particular IP/MAC address.

- Users can set working time and days, and it will create offline reports and automatically send them to specified targets. The reports can be times, daily, weekly, monthly, quarterly, or semi-annual; the format PDF, CSV, HTML, or XML.

- Have warning system which sends different warnings to different groups.

- Personalized interface, users can set up the fields and orders as their preference.

- Personalized LOGO, data fields and layouts.

- Support build-in audit analysis report for different databases including Oracle, MS SQL, and MySQL.

- Users can create couples of Dashboards on demand, and the Dashboards will present the analysis result of N-Reporter/N-Cloud on several pop-up windows.

- Through analyzing the correlation, it can create bps/PPS/Session charts with the Layer 7 application and get the bandwidth usage of every user.

- The automatic-learning big data analysis function includes Flow analysis, it can detect the attackers (like DDoS, Scan attacks) and the targets in real time.

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 15 years of 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 integrate SNMP, Flow, and Syslog, and that make IT administrators debug more easily. We use the leading technology including Any-to-Any analysis, which establishes Dynamic Benchmarks based on each event log and history to detect abnormal activities and to send out real-time alerts. 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 is the first SaaS Service with both NOC and SOC, and it has been used by many educational networks, multinational corporation, and telecommunications for operation. By 2015, N-Partner has expanded the business scale to China and gradually to Southeast Asia.

contact information

Address: Rm. B1, 14F., No.497, Zhongming S. Rd., West Dist., Taichung City 403, Taiwan (R.O.C.)
Website address: www.npartnertech.com
Telephone number: 886-4-2375-2865
E-mail address: sales@npartnertech.com
Support service: support@npartnertech.com

N-Partner