N-Partner
User Training

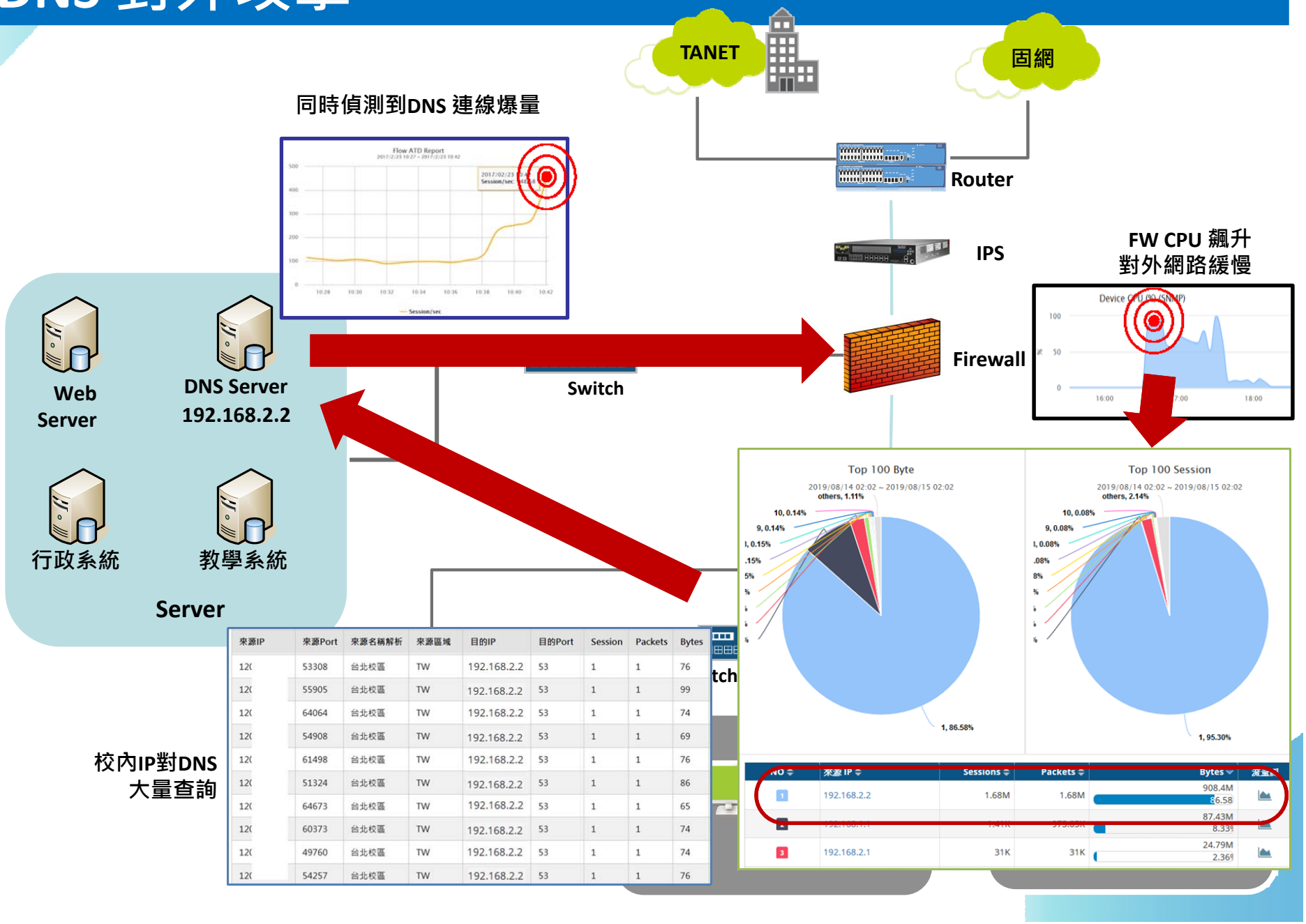
N-Partner

王聖雄 Sherman Wang
Sales Engineer
sherman@npartnertech.com
0926-834979

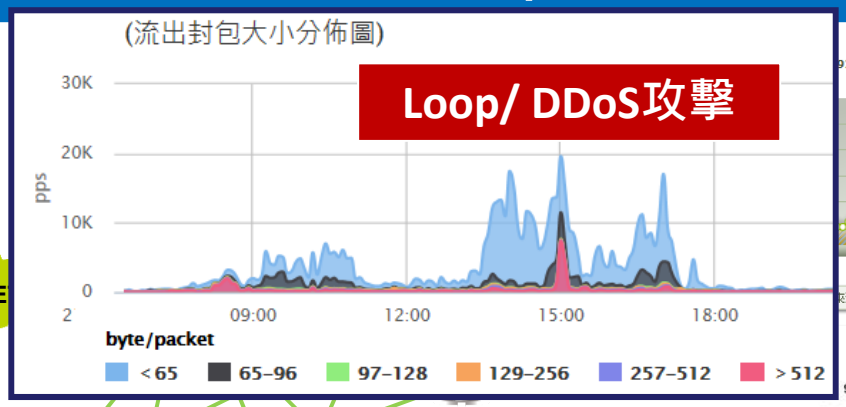
N-Reporter/N-Cloud
解決方案

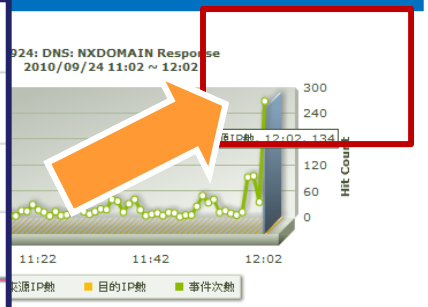
N-Partner

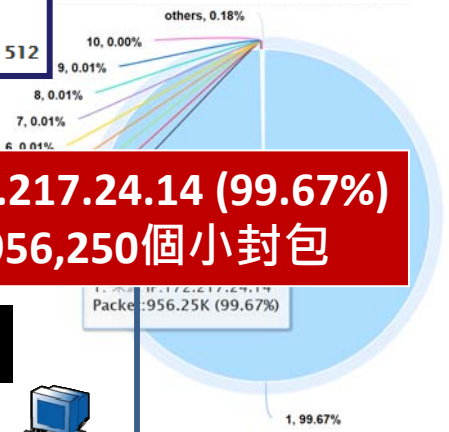
DNS 對外攻擊


TANET
固網
同時偵測到DNS 連線爆量
Router
IPS
FW CPU 飆升
對外網路緩慢
Firewall
Switch
Web Server
DNS Server
192.168.2.2
行政系統
教學系統
Server
校內IP對DNS
大量查詢
Top 100 Byte
2019/08/14 02:02 ~ 2019/08/15 02:02
Top 100 Session
2019/08/14 02:02 ~ 2019/08/15 02:02
1, 86.58%
1, 95.30%
來源IP 來源Port 來源名稱解析 來源區域 目的IP 目的Port Session Packets Bytes
53308 台北校區 TW 192.168.2.2 53 1 1 76
55905 台北校區 TW 192.168.2.2 53 1 1 99
64064 台北校區 TW 192.168.2.2 53 1 1 74
54908 台北校區 TW 192.168.2.2 53 1 1 69
61498 台北校區 TW 192.168.2.2 53 1 1 76
51324 台北校區 TW 192.168.2.2 53 1 1 86
64673 台北校區 TW 192.168.2.2 53 1 1 65
60373 台北校區 TW 192.168.2.2 53 1 1 74
49760 台北校區 TW 192.168.2.2 53 1 1 74
54257 台北校區 TW 192.168.2.2 53 1 1 76
NO 來源 IP Sessions Packets Bytes
192.168.2.2 1.68M 1.68M 908.4M
192.168.2.1 31K 31K 24.79M

智慧維運-無須人工設定的智慧分析,聯防企業端設備







172.217.24.14 (99.67%)
956,250個小封包

N-Cloud
- NOC+SOC
- Central Management
- Global View and Individual Portal

TAINE

Firewall /IPS/UTM

無線網路控制管理機制

IDC

Data Center

DMZ/
網路服務主機群

主機群/Radius

Server Farm

Core Switch

Firewall

Access

Access Switch

固網

Wireless AP

L2 Switch

L3 Switch

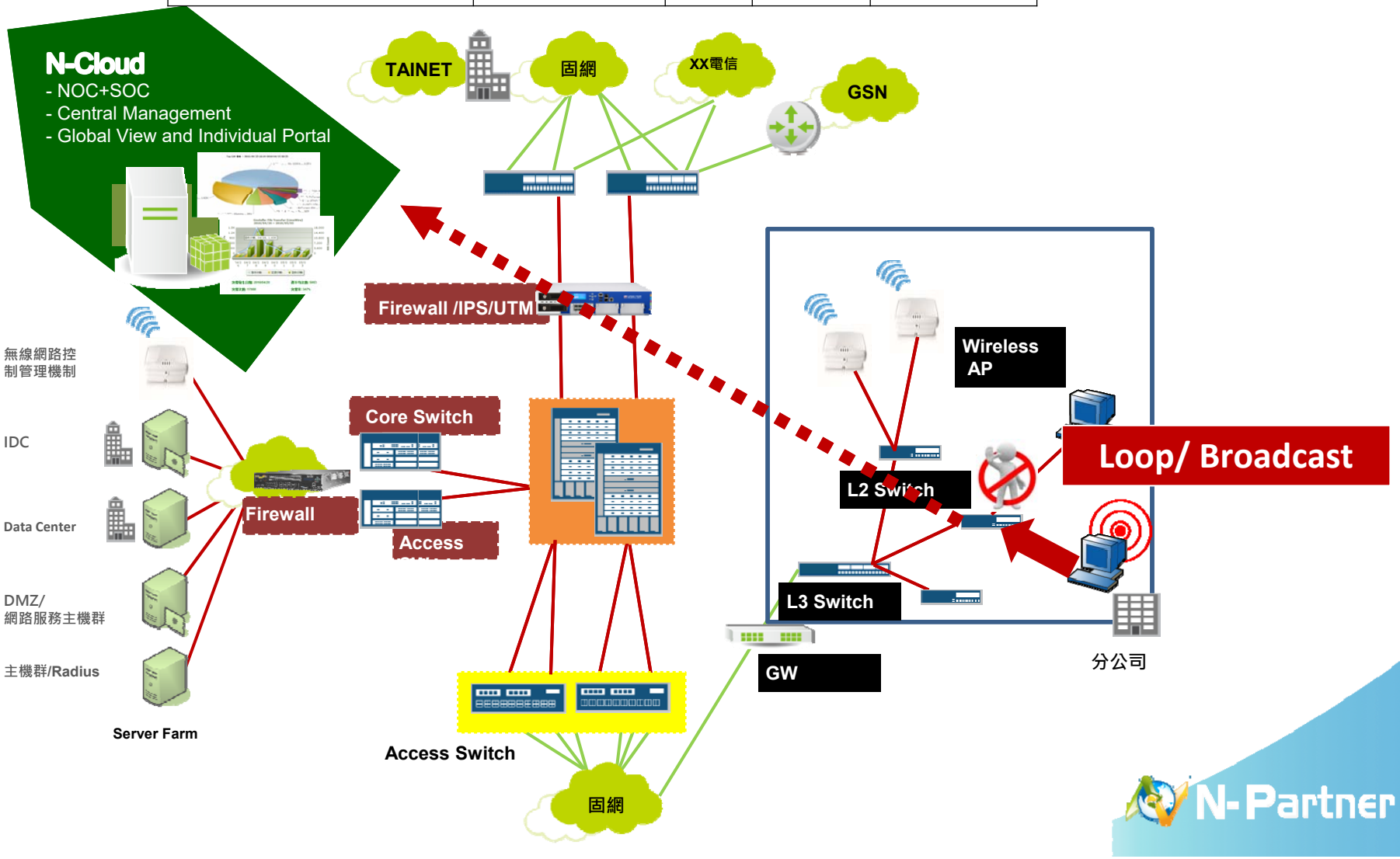
GW

分公司

N-Partner

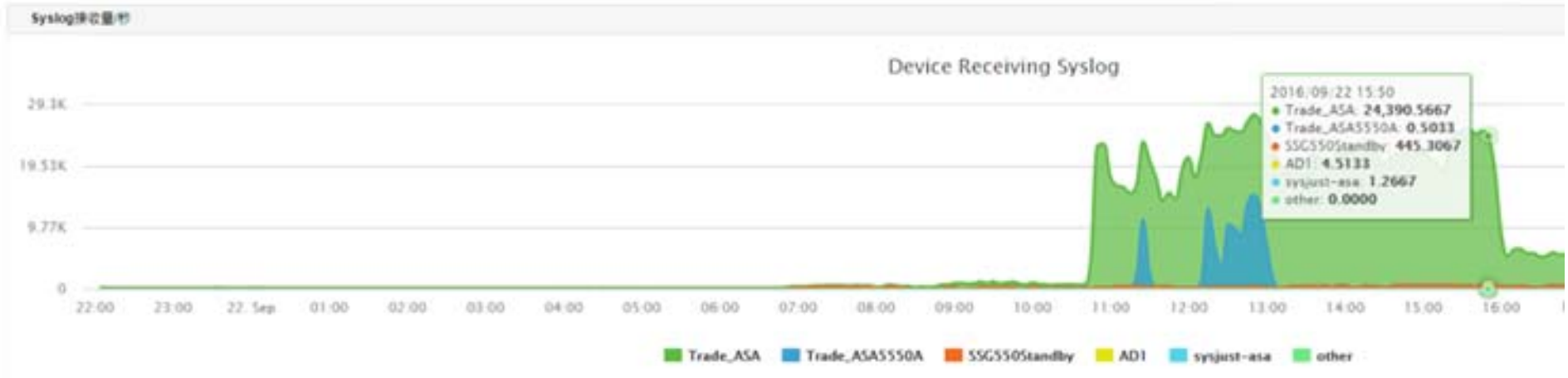
智慧維運-交換機阻擋Loop, N-Cloud查詢日誌

事件行為	來源 MAC	單位	動作	所在位置
Loop Detection	AA:BB:CC:DD:EE	財務	Block	SW-1-GE1/0/1



N-Partner

By量收集日誌，遇到異常暴量該怎麼辦?



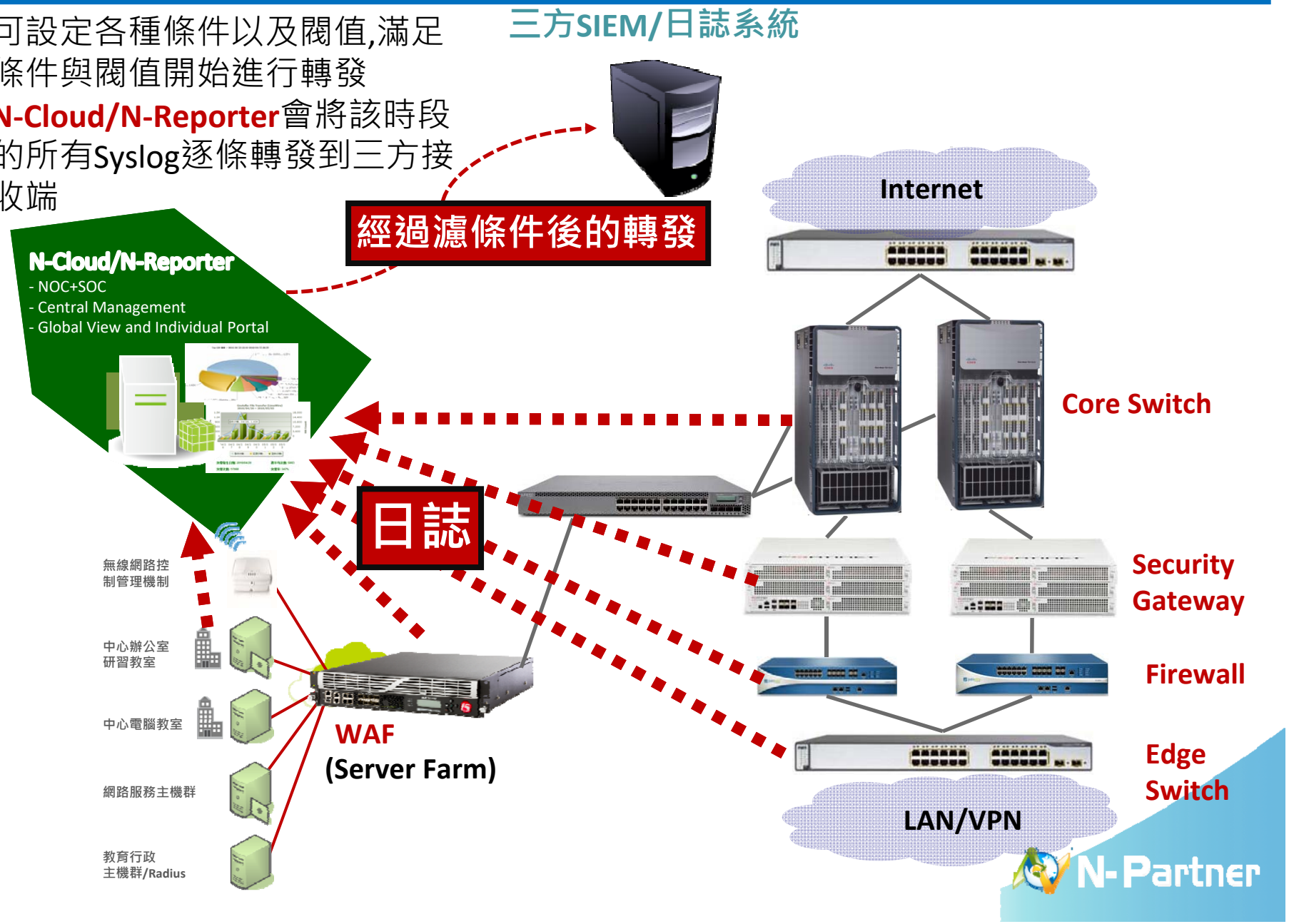
遭到DDoS攻擊時, 防火牆的日誌量從平時每秒600暴增到25,000(Event Per Second)的圖形,攻擊發生導致日誌量大漲到將近100GB

N-Reporter/N-Cloud可以完整收容,不須額外付費

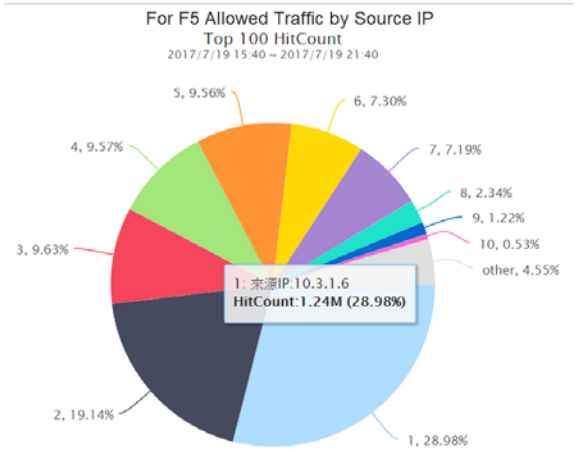
N-Partner

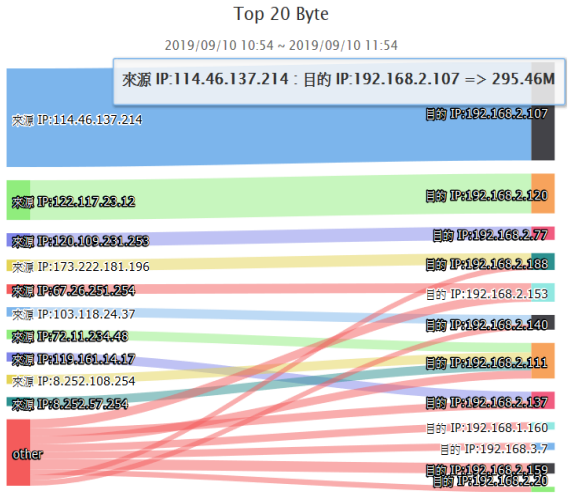
安全閘道設備/網路設備/伺服器日誌(Syslog)減量轉發

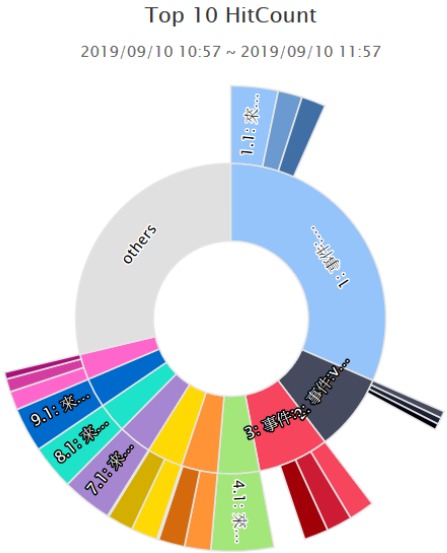
1. 可設定各種條件以及閥值,滿足條件與閥值開始進行轉發
2. **N-Cloud/N-Reporter**會將該時段的所有Syslog逐條轉發到三方接收端

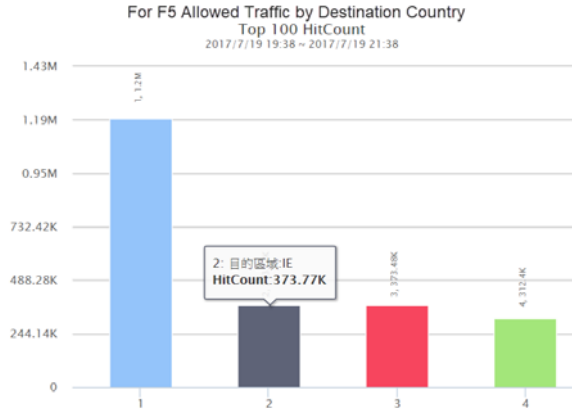


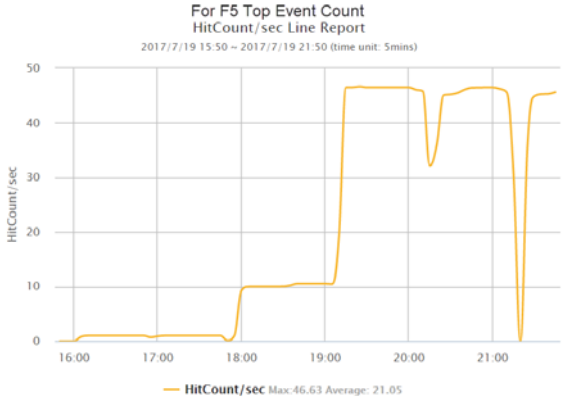
內建各種品牌的專屬資安分析圖表,無須人工設定

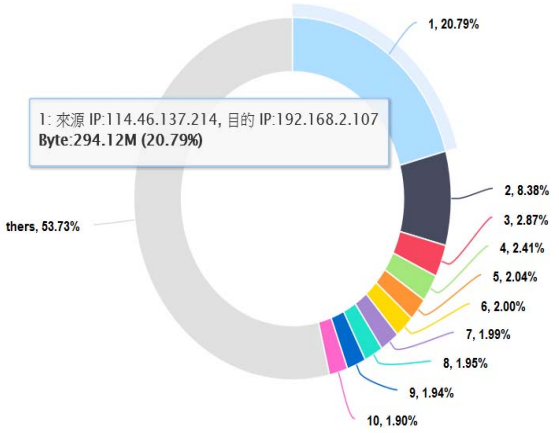












N-Partner

N-Cloud/ N-Reporter
新功能介紹

N-Partner

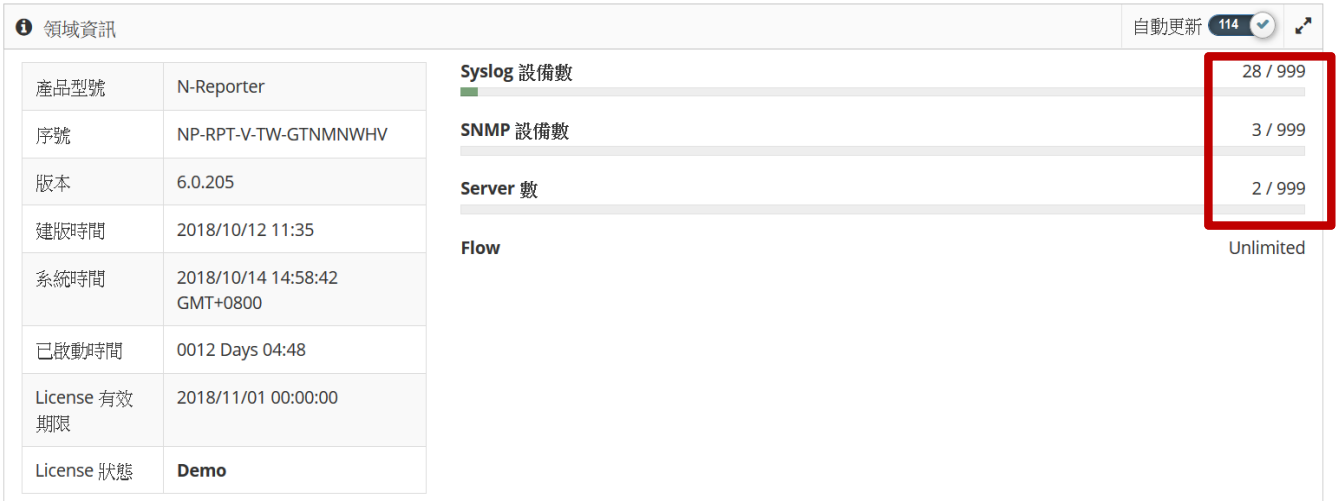
-強化N-Cloud/N-Reporter 功能

-N-Reporter 6.x 新增功能

N-Partner

強化舊版N-Cloud/N-Reporter 功能

調整授權計算方式



✓ License 不會重複扣

例如:

✓ 防火牆送出syslog，且開啟SNMP監控，僅扣 [Syslog設備數]

✓ Switch送出syslog，且開啟SNMP監控，僅扣 [SNMP設備數]

✓ AD送出syslog，且開啟SNMP監控，僅扣 [Server設備數]

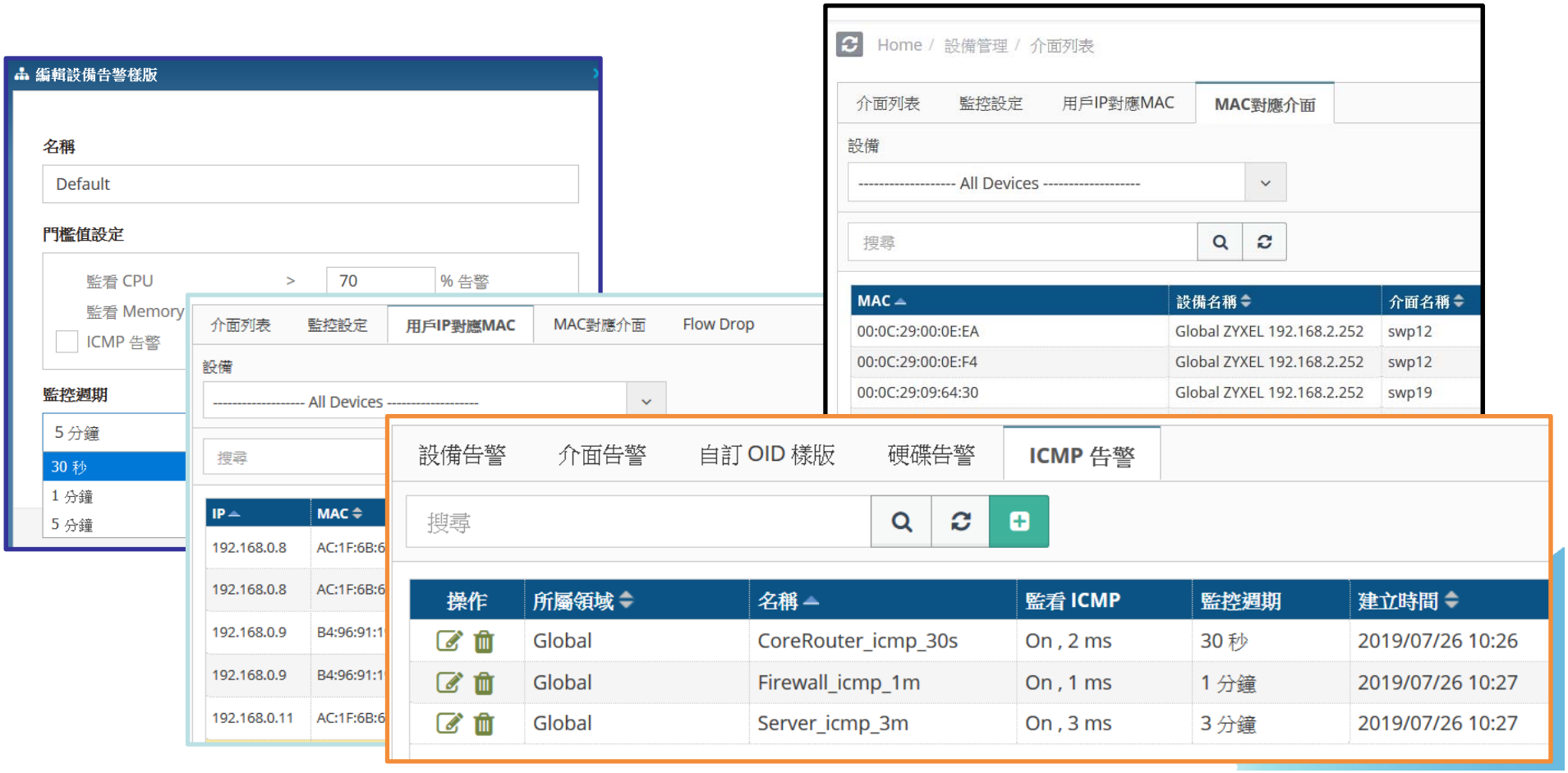
N-Partner

優化名稱解析設定功能

- 新增資料匯出
- 批次修改

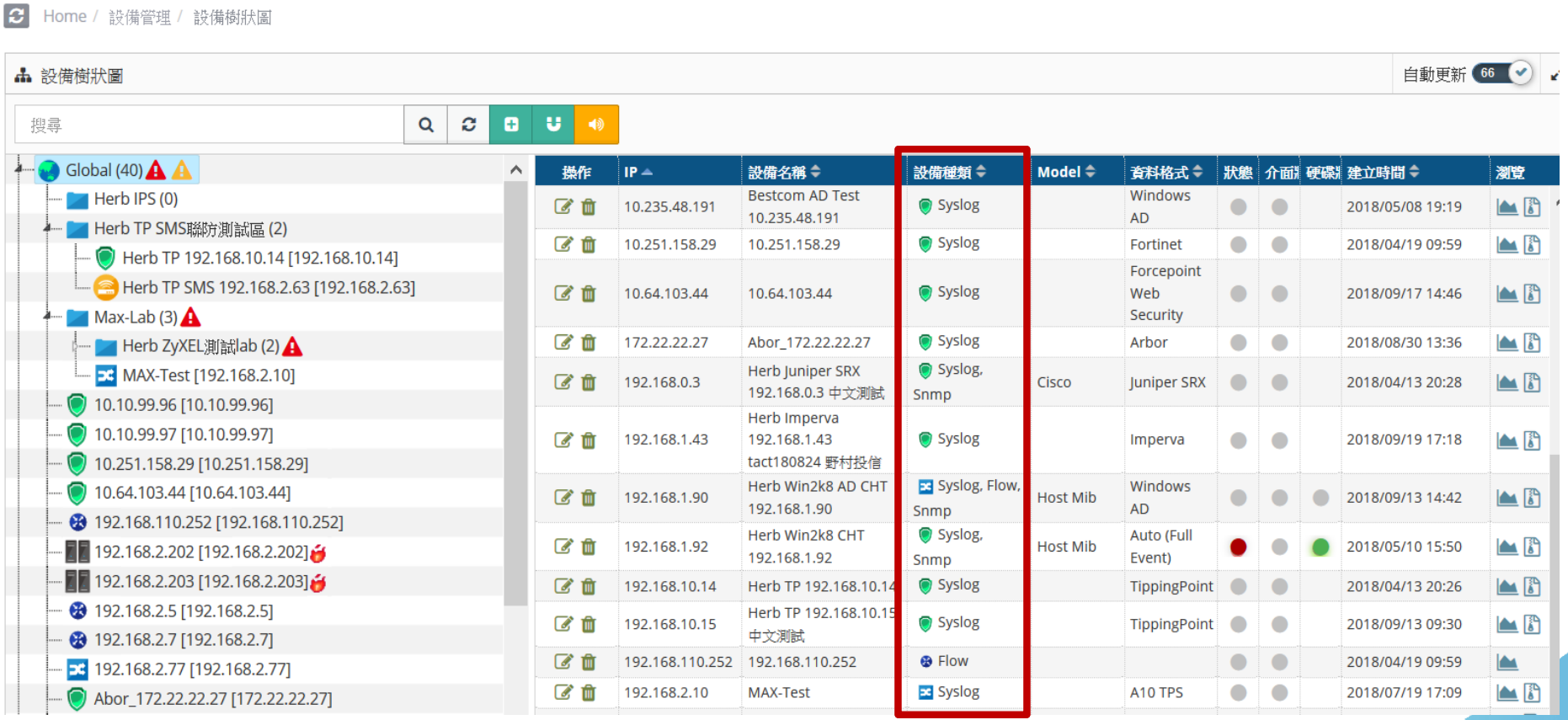
優化SNMP功能

- 可指定SNMP 輪詢時間
- 可查閱IP-MAC-Switch port對應關係
- ICMP 監控獨立



設備管理 - 設備樹狀圖

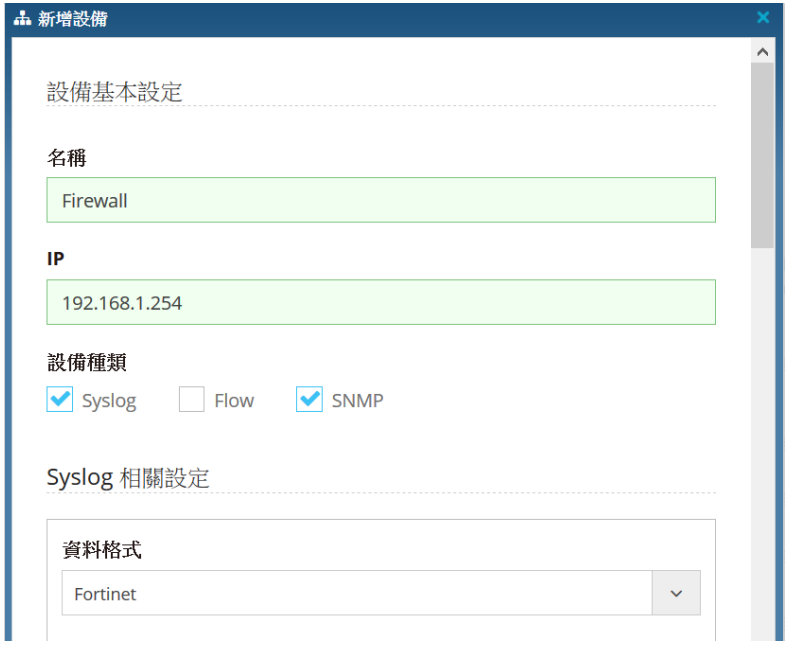
- **Syslog/SNMP/Flow設備整合在同一頁面**
- 統一管理所有設備狀態



N-Partner

自動新增預設報表、監控

- 可依需求再手動編輯



操作	查詢條件名稱
	For Fortigate Key Applications Crossing The Network
	For Fortigate Malwares Discovered
	For Fortigate Top Allowed Applications by Bandwidth
	For Fortigate Top Application Categories by Bandwidth Usage
	For Fortigate Top
	For Fortigate Top
	For Fortigate Top
	For Fortigate Top
	For Fortigate Top
	For Fortigate Top
	For Fortigate Top
	For Fortigate Top
	For Fortigate Top

操作	查詢條件名稱
	For Checkpoint Top Applications
	For Checkpoint Top Attack Country
	For Checkpoint Top Destinations of Security Attacks and their Top Attacks
	For Checkpoint Top Security Attacks

操作	查詢條件名稱
	For Paloalto TOP Applications
	For Paloalto TOP Attack Country
	For Paloalto TOP Attackers
	For Paloalto TOP Attack Event
	For Paloalto TOP Connections by Byte
	For Paloalto TOP Connections by Session
	For Paloalto TOP External Attackers

N-Partner

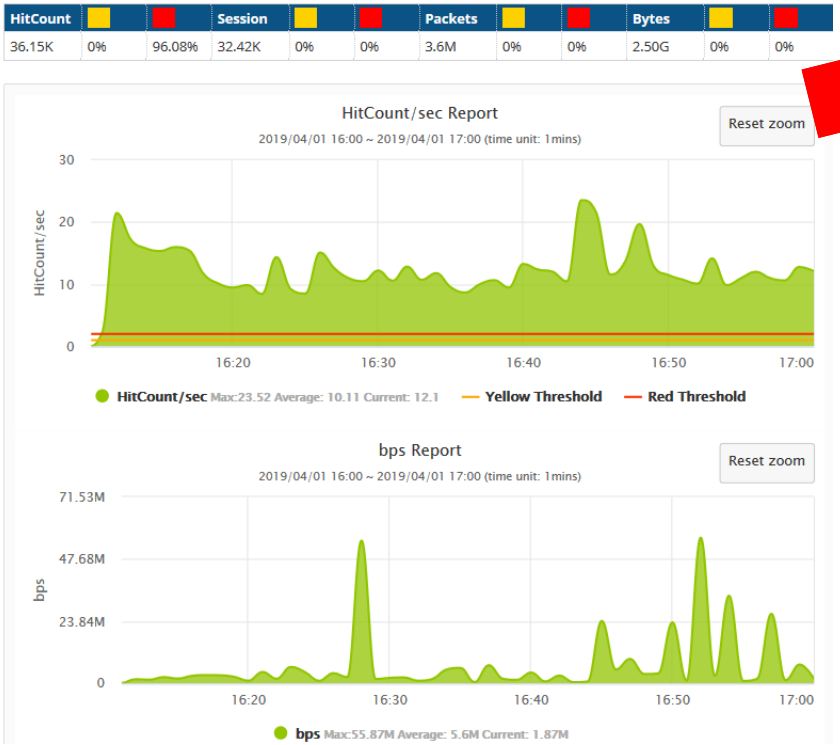
強化分時監控功能

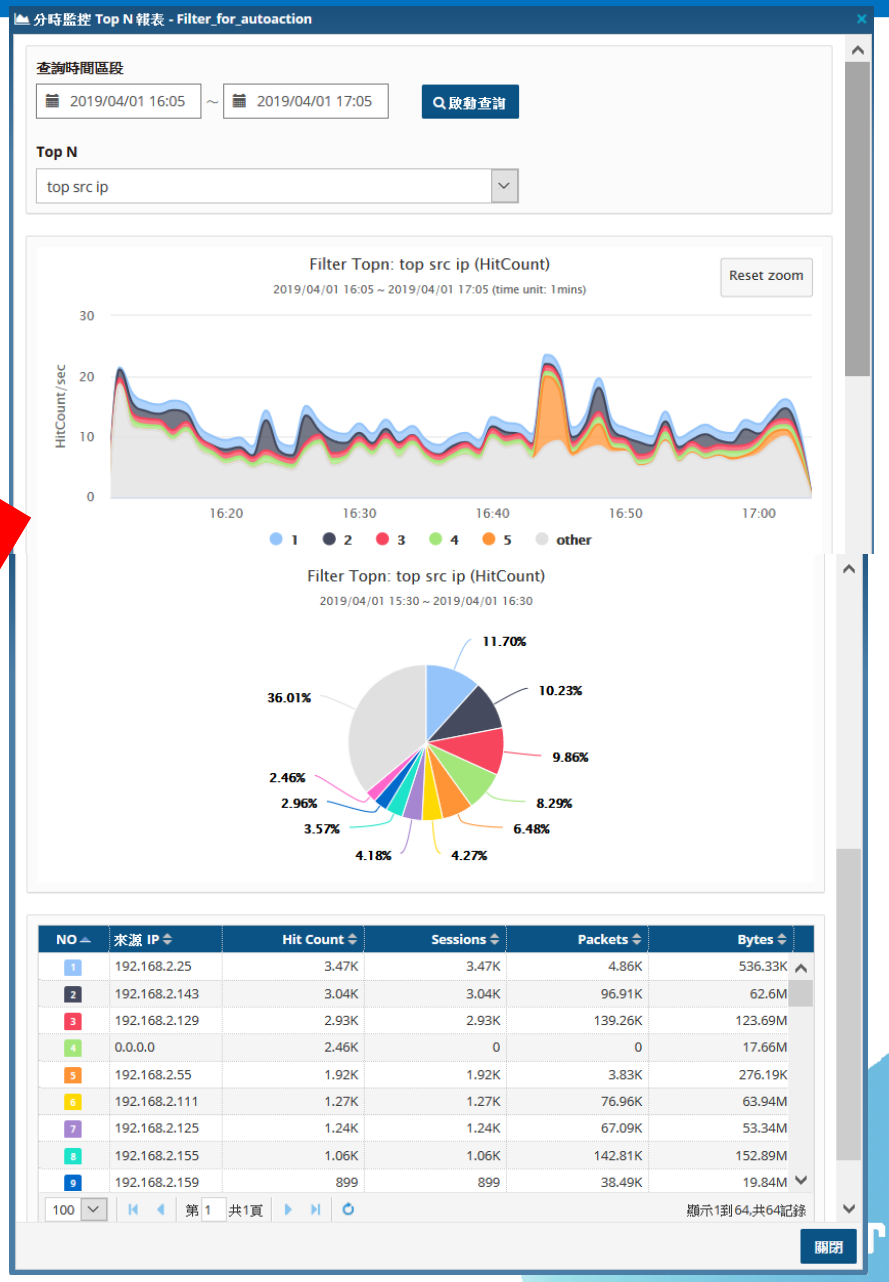
- 新增監控時間間距調整、分時監控TopN、抑制次數

N-Partner

分時監控TopN

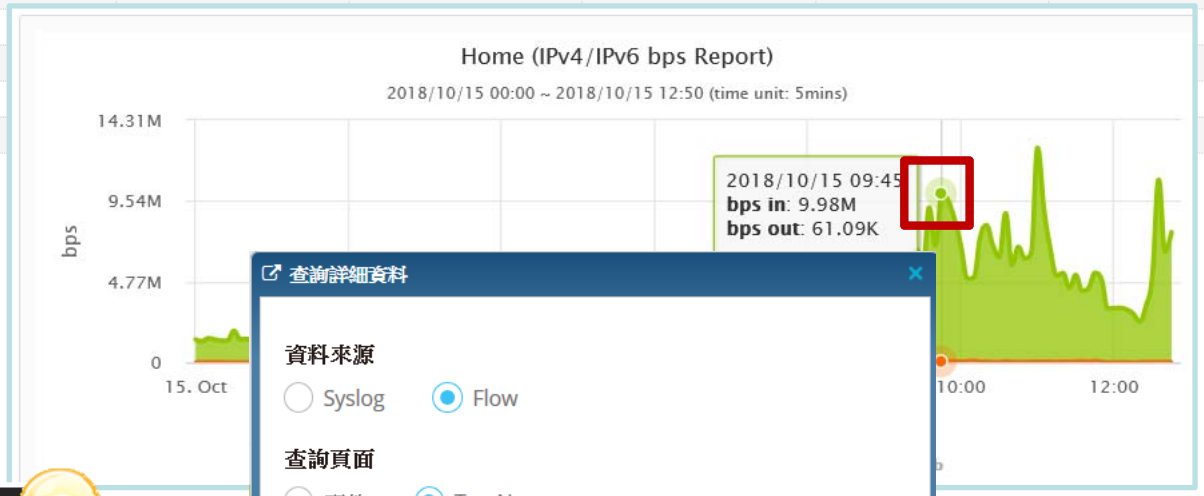
- 提供更詳盡內容分析
- 可自定義TopN欄位





強化資料跳查自由度

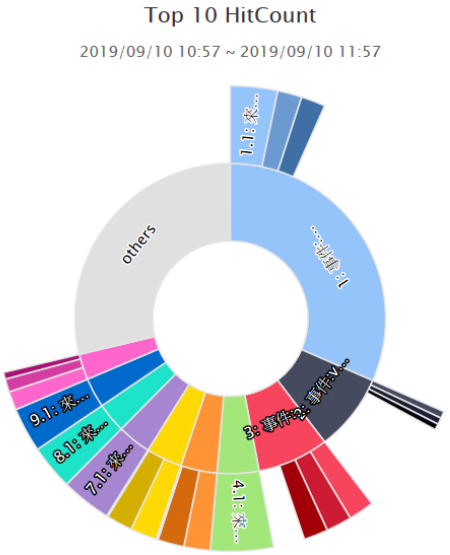
網段名稱	流入量			流出量			流量圖
	Sessions	Packets	Bytes	Sessions	Packets	Bytes	
Home	60.44M	60.44M	15.12G	828K	828K	316.14M	
財務部門 Finance Deparment 192.168.2.0/24	60.16M	60.16M	14.87G	827.5K	827.5K	316.12M	
人事部門 HR Department 192.168.1.0/24	228.25K						
Gookey_test_auto2	55.25K						
Gookey_test4	55.25K						
Sales Department	55.25K						

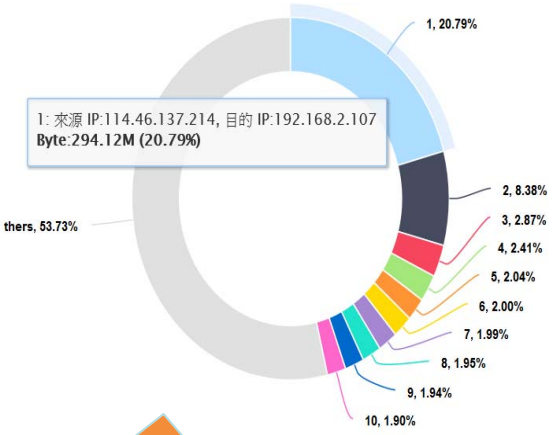


- ✓ Flow專屬報表
- ✓ 趨勢分析
- ✓ 分時監控
- ✓ 設備CPU、interface

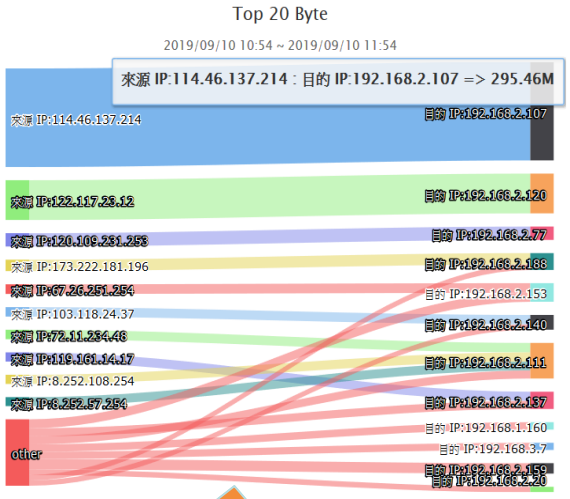
N-Partner

提供更多種報表型式選擇





環圈圖



桑基圖

TopN x TopN

N-Partner

強化趨勢分析功能

- 趨勢分析例外清單
- 提供IP、Port、事件關鍵字白名單

N-Partner

ATD異常流量即時分析告警

- 提供不同等級靈敏度調整
- 提供長時間連線監控

套用預設敏感度設定

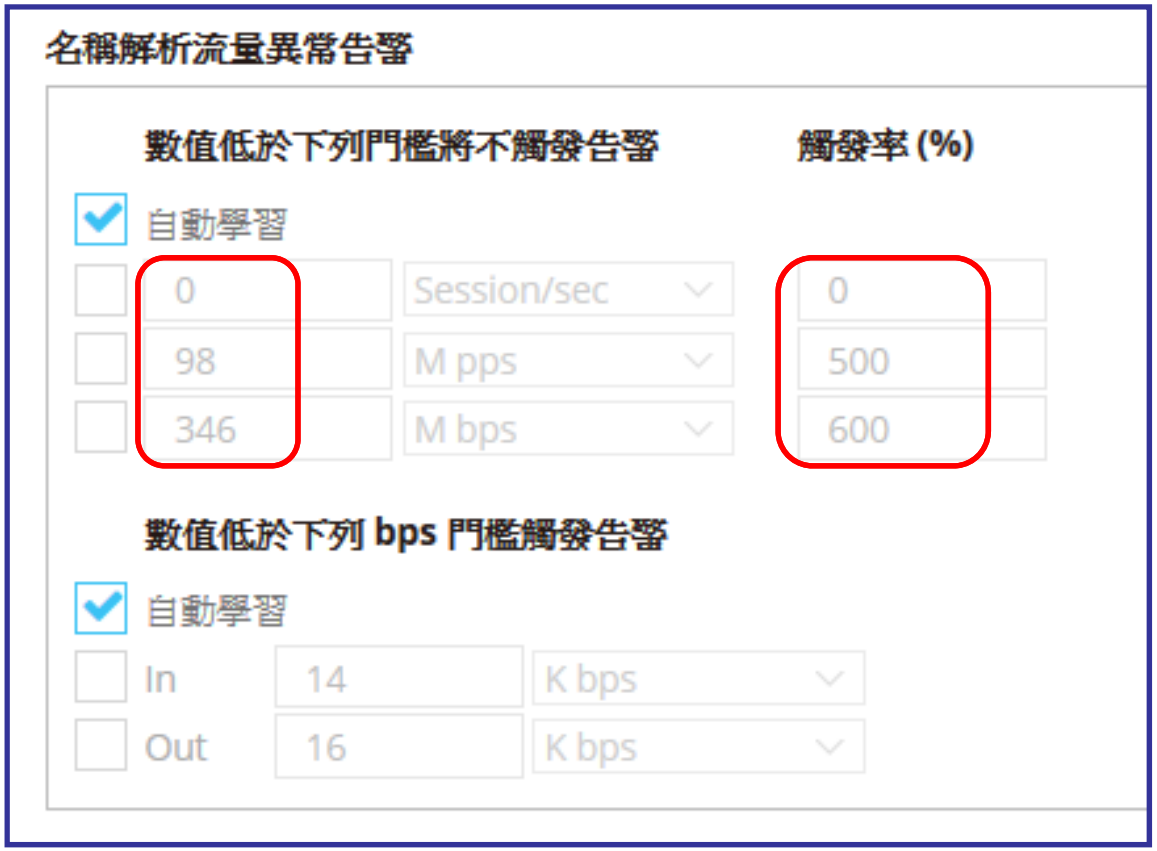
Low Medium High

所屬領域	異常項目	攻擊者 IP	攻擊者區域	受害者 IP	受害者區域	協定	目的 Port	Session	Packet	Byte	開始時間	結束時間	瀏覽
Global	Long Time Session Monitor	60.0.0.4	CN	192.168.1.4		TCP	1004	64.79K	2.78M	6.58M	2019/07/26 10:15	2019/09/10 12:14 (持續連線 46 days 01:58:59)	
Global	Long Time Session Monitor	60.0.0.5	CN	192.168.1.5		TCP	1005	64.79K	3.48M	6.64M	2019/07/26 10:15	2019/09/10 12:14 (持續連線 46 days 01:58:59)	
Global	Long Time Session Monitor	30.0.0.6	US	192.168.1.6		TCP	1006	64.79K	4.18M	6.71M	2019/07/26 10:15	2019/09/10 12:14 (持續連線 46 days 01:58:59)	

N-Partner

優化網段告警機制

- 可自動學習網段 流量上限/下限 閥值
- 學習到的安全值可呈現在UI



N-Partner

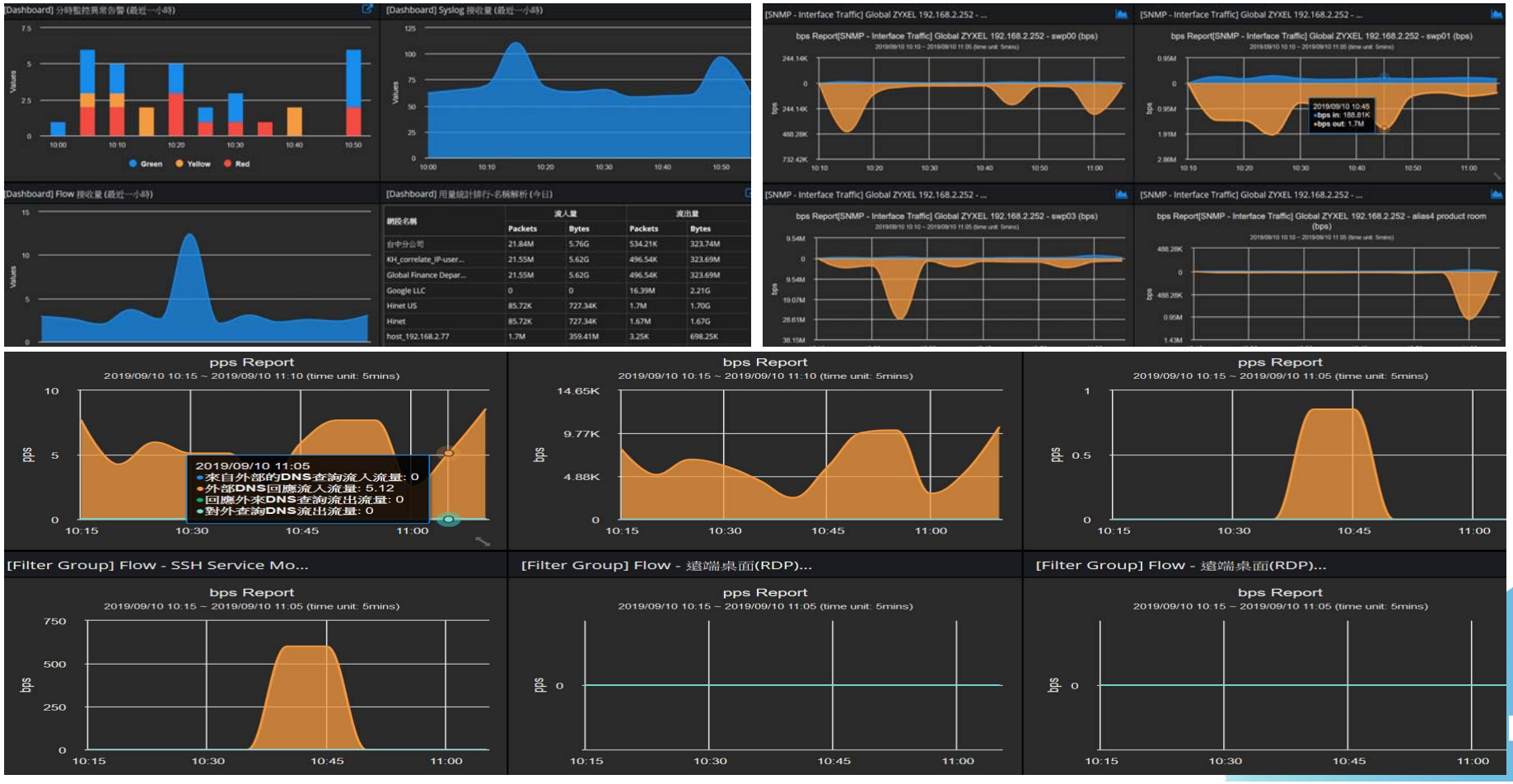
優化事件欄位顯示設定

- 每個帳號可自訂自己喜歡的欄位設定，亦可讓其他帳號套用
- 事件查詢可動態顯示資料欄位，僅顯示有資料的欄位，方便瀏覽

N-Partner

強化dashboard功能

- 可預設同時開啟多個dashboard，並優化瀏覽介面
- 可將SNMP監控放入
- 可隨意拖曳內部視窗位置、調整大小



N-Partner

N-Reporter 6.x 新增功能

新增使用者權控

- 可新增權限樣版，並細部調整功能權控套用至指定帳號

新增SNMP功能

- 可自定義OID監控

N-Partner

新增TopN報表群組化功能

- 一封email即可整合多份TopN報表至一份pdf

新增 單位用量統計與佔比

- 可統計各系統、線路流量佔用百分比

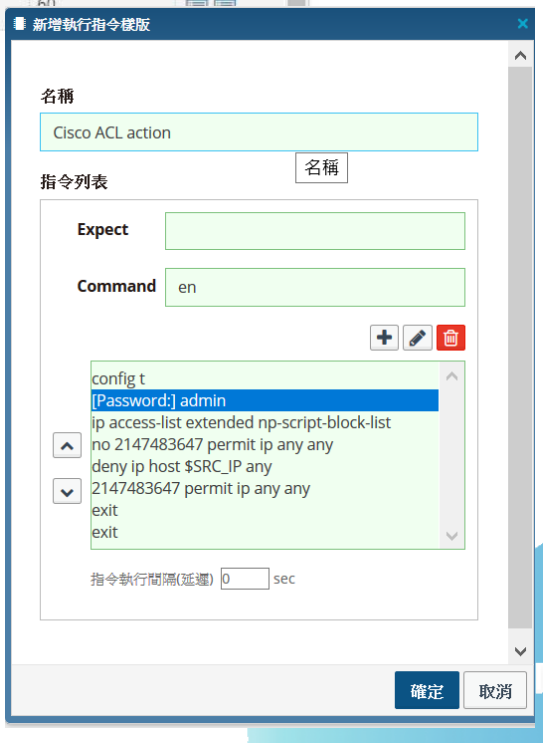
項目名稱	In	Out	項目總流量	佔總使用流量百分比(%)
外部SSH流量	0	0	0	0.00%
內部SSH流量	0	799.00K	799.00K	100.00%
各項目流量加總	0	799.00K	799.00K	100.00%

N-Partner

更彈性的自動聯防

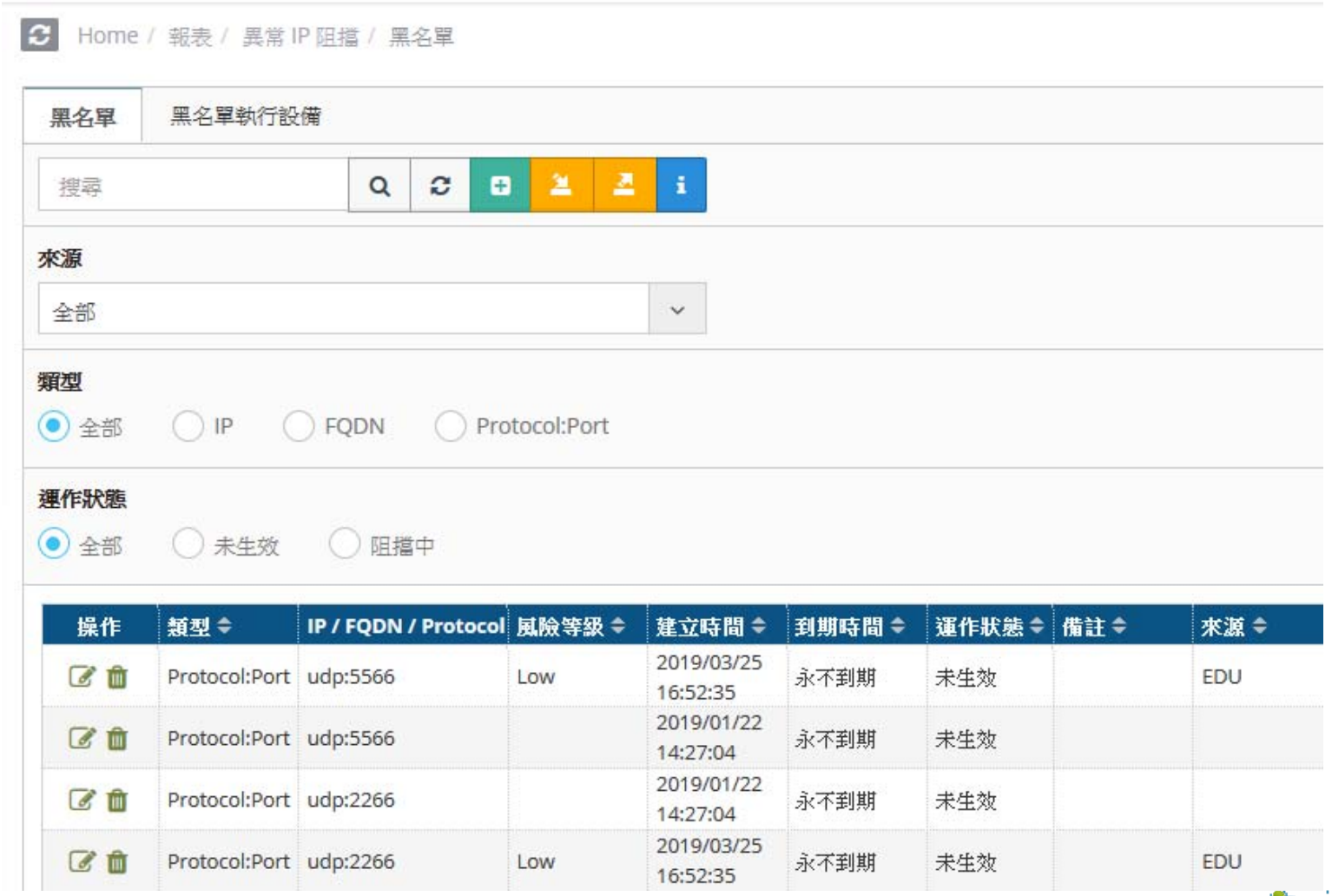
- 可自訂連防指令、自動定位switch

阻擋於內建Action設備
加入黑名單
自動定位 Switch (以IP阻擋)
自動定位 Switch (以MAC阻擋)



黑名單聯防機制

- 將已知惡意IP快速佈署到資安設備阻擋

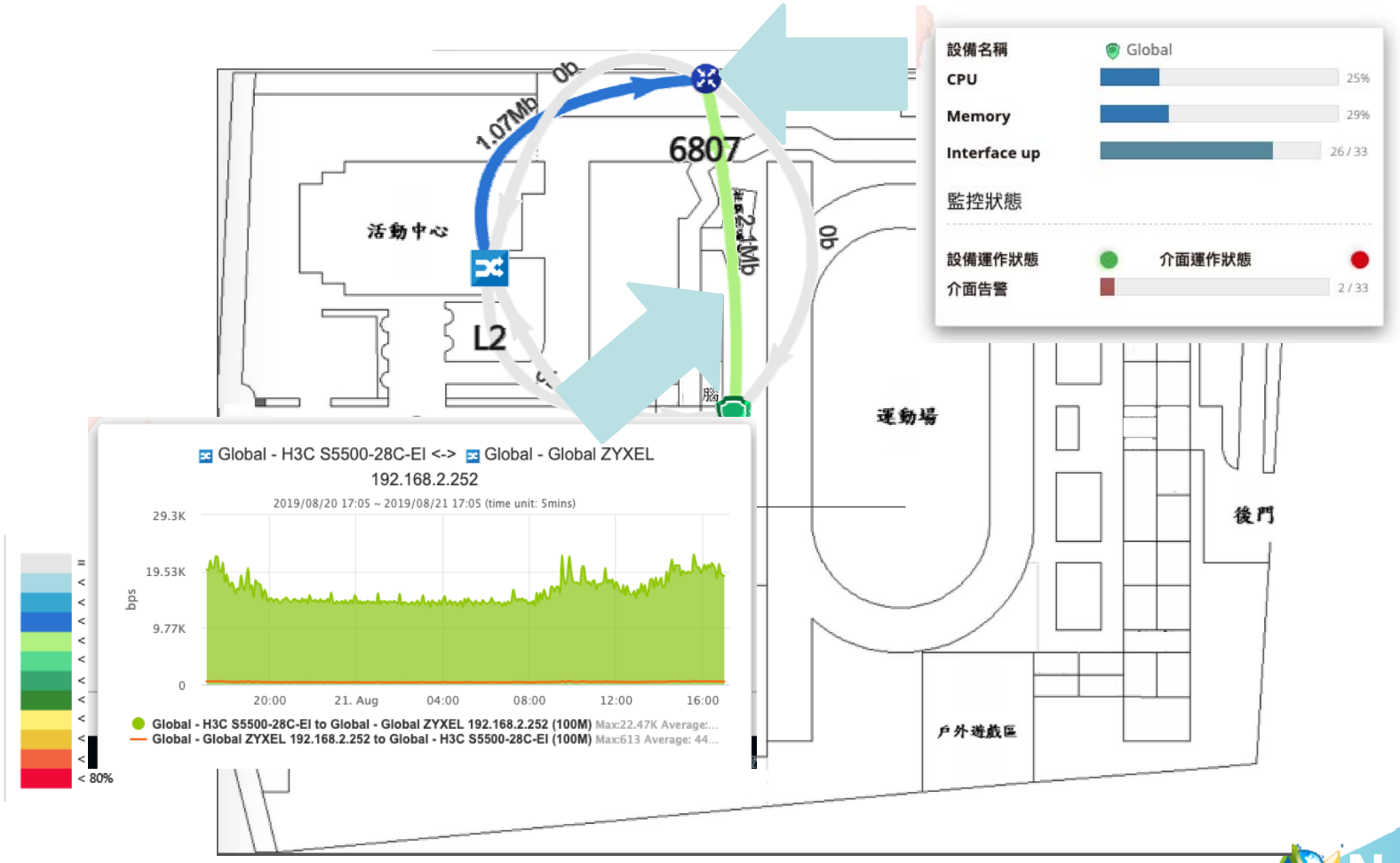


操作	類型	IP / FQDN / Protocol	風險等級	建立時間	到期時間	運作狀態	備註	來源
	Protocol:Port	udp:5566	Low	2019/03/25 16:52:35	永不到期	未生效		EDU
	Protocol:Port	udp:5566		2019/01/22 14:27:04	永不到期	未生效		
	Protocol:Port	udp:2266		2019/01/22 14:27:04	永不到期	未生效		
	Protocol:Port	udp:2266	Low	2019/03/25 16:52:35	永不到期	未生效		EDU

N-Partner

提供拓樸圖

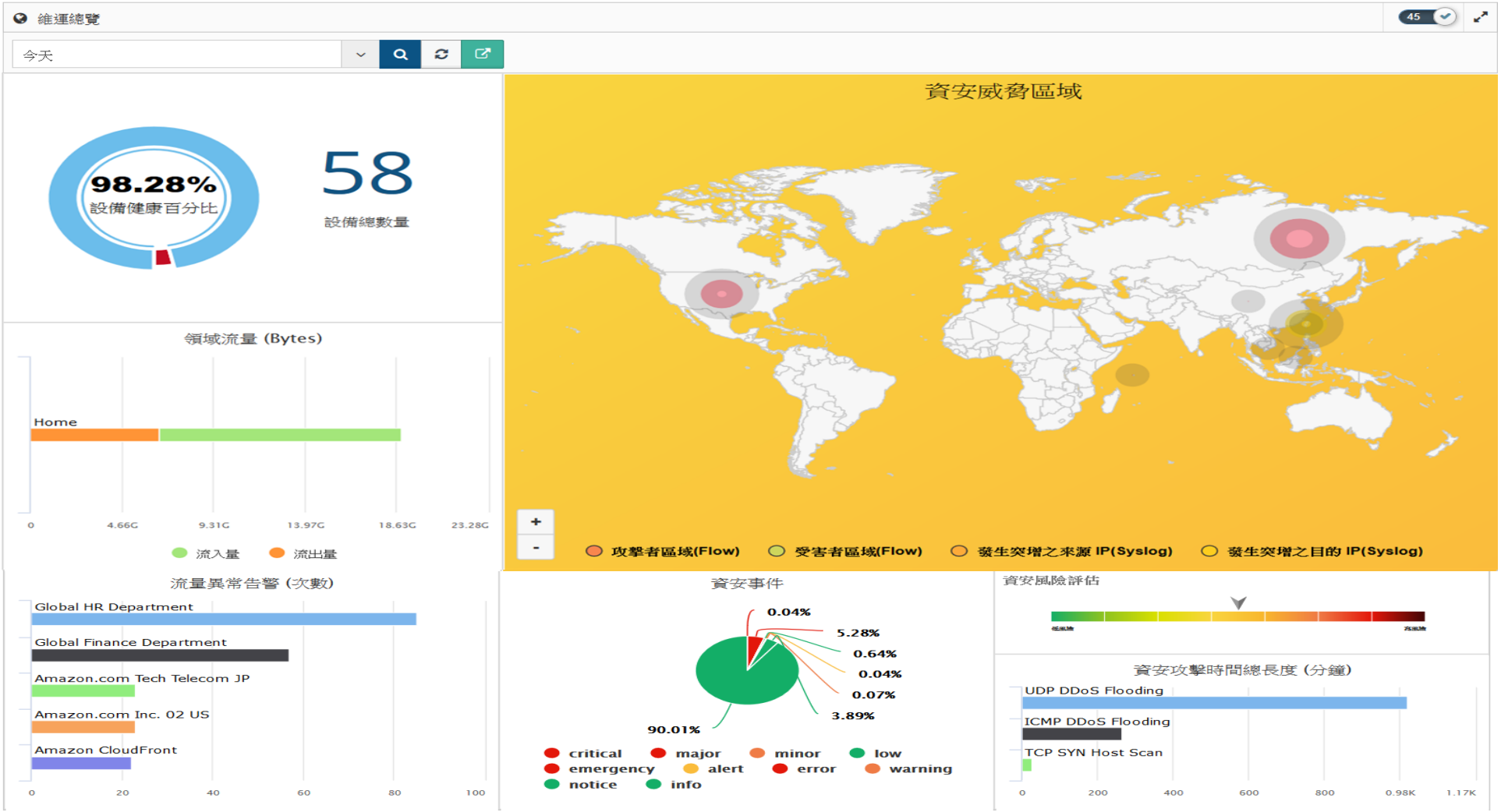
- 可呈現設備狀態
- 可將介面流量依使用狀況以不同顏色呈現



N-Partner

新增維運總覽

- 可快速掌握監控概況



彈性的架構轉換

- 單機架構不夠用時，可擴充至N-Cloud
- 單機版報表、監控設定、log皆可移轉至N-Cloud