

N-Partner User Training



N-Partner

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



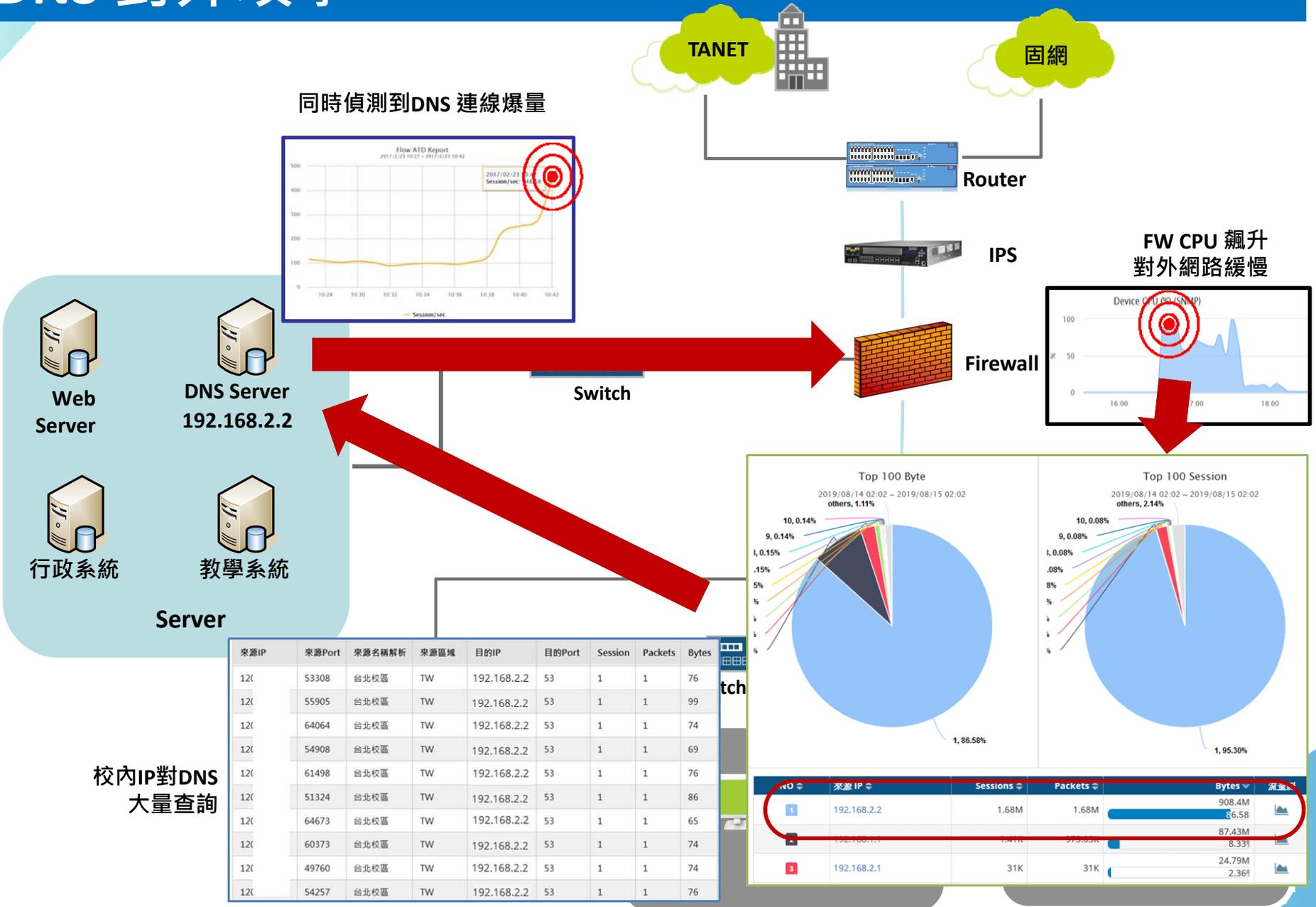
N-Reporter/N-Cloud 解決方案



N-Partner



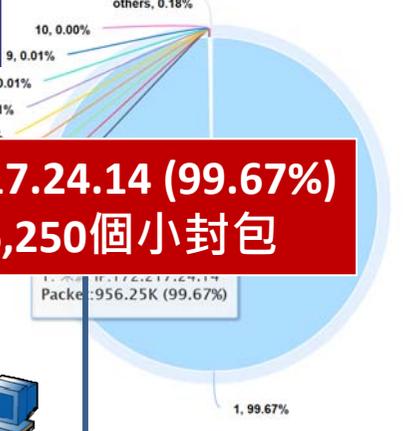
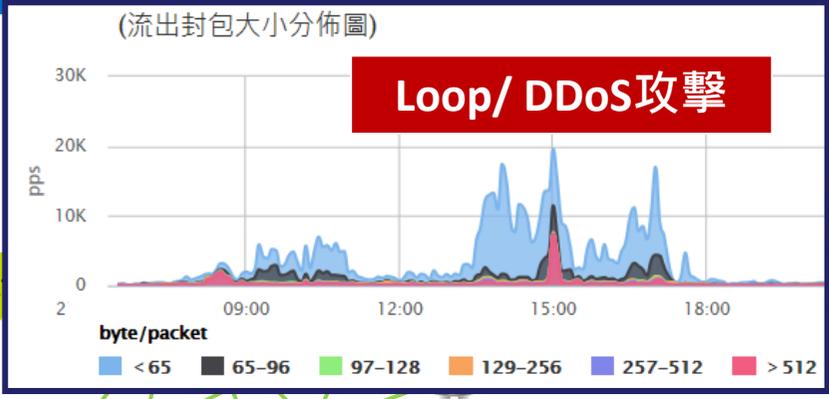
DNS 對外攻擊



智慧維運-無須人工設定的智慧分析,聯防企業端設備

N-Cloud

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



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

TAINET

Firewall /IPS/UTM

Core Switch

Access

Access Switch

固網

GW

172.217.24.14 (99.67%)
956,250個小封包

Wireless AP

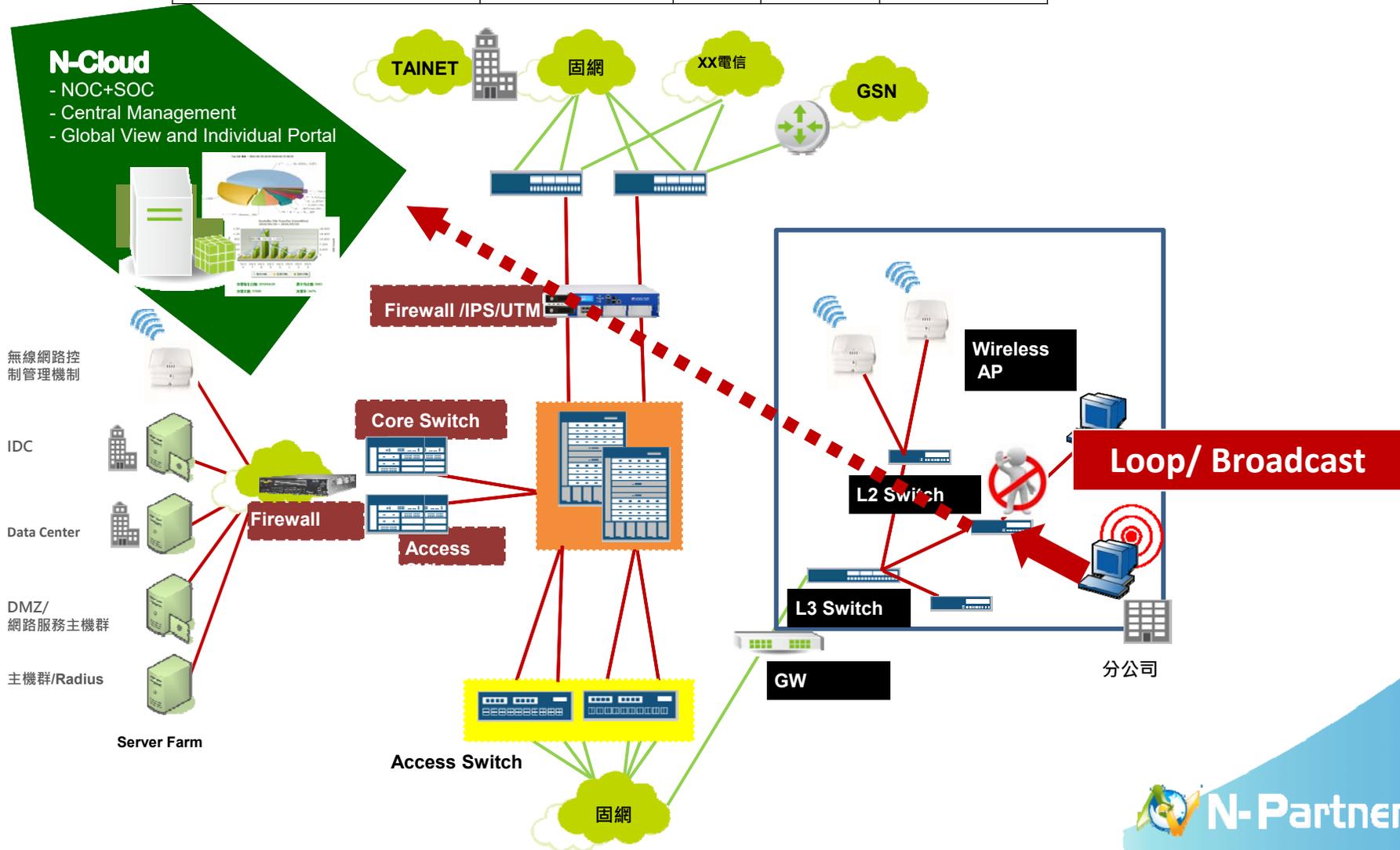
L2 Switch

L3 Switch

分公司

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



By量收集日誌，遇到異常暴量該怎麼辦？



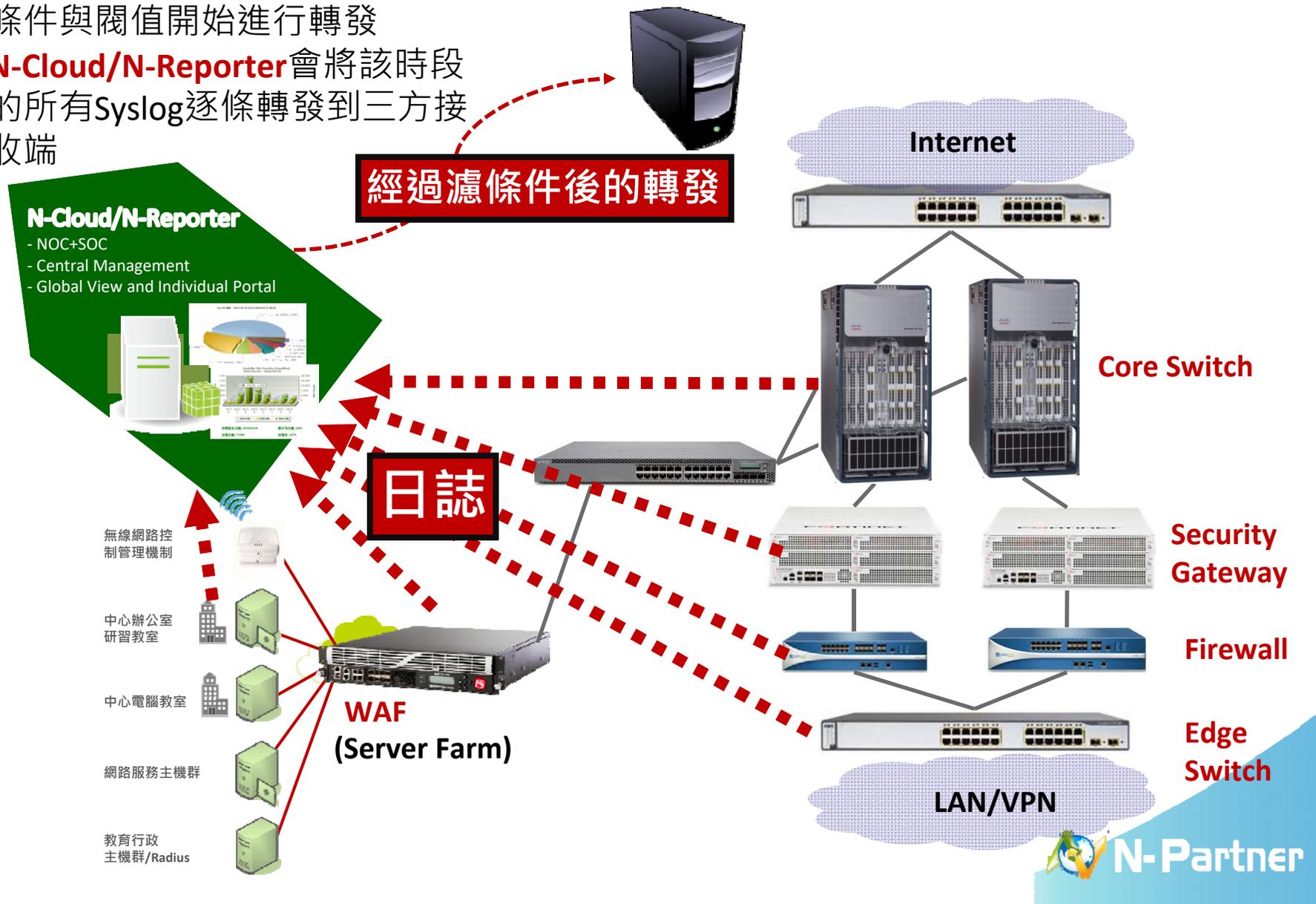
遭到DDoS攻擊時, 防火牆的日誌量從平時每秒600暴增到25,000(Event Per Second)的圖形, 攻擊發生導致日誌量大漲到將近100GB

N-Reporter/N-Cloud可以完整收容, 不須額外付費

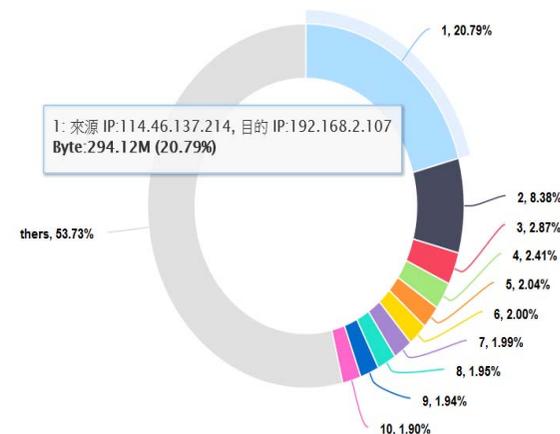
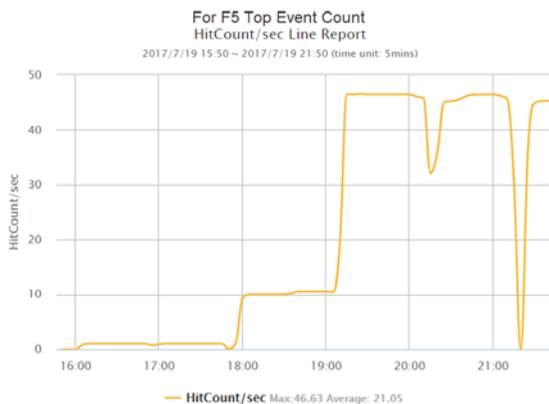
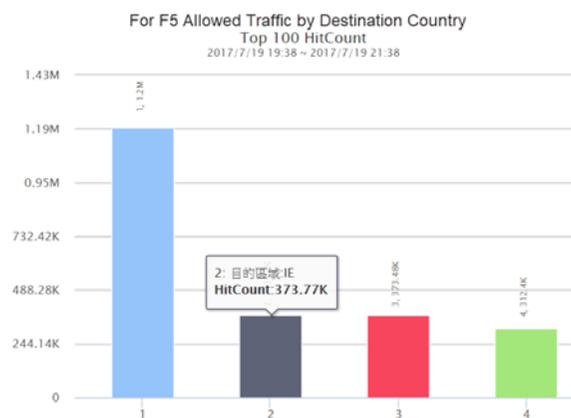
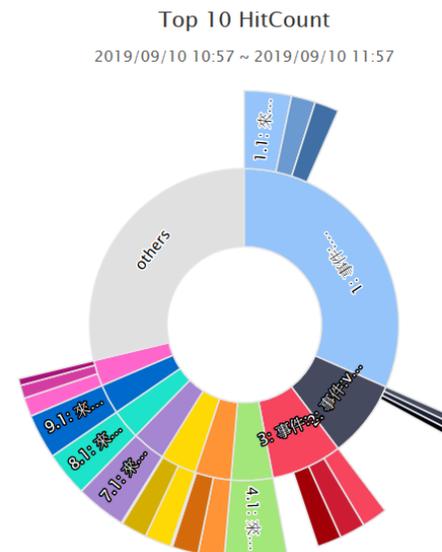
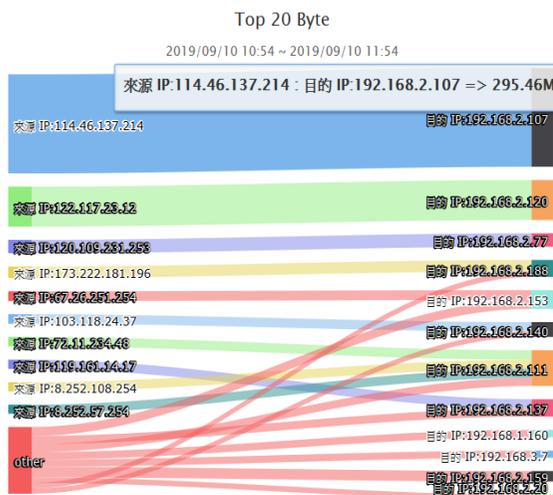
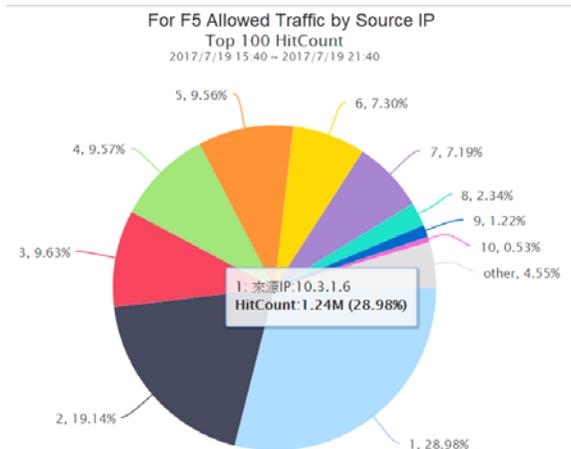
安全閘道設備/網路設備/伺服器日誌(Syslog)減量轉發

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

三方SIEM/日誌系統



內建各種品牌的專屬資安分析圖表,無須人工設定



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

系統管理

- 領域資訊
- 網路參數設定
- 使用者總表
- IP 名稱解析
- Port 名稱解析
- 告警通報設定
- 操作歷程
- 偏好設定
- Dashboard

領域資訊

產品型號	N-Reporter
序號	NP-RPT-V-TW-GTNMNWHV
版本	6.0.205
建版時間	2018/10/12 11:35
系統時間	2018/10/14 14:58:42 GMT+0800
已啟動時間	0012 Days 04:48
License 有效期限	2018/11/01 00:00:00
License 狀態	Demo

自動更新 114

Syslog 設備數	28 / 999
SNMP 設備數	3 / 999
Server 數	2 / 999
Flow	Unlimited

✓ 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]



優化名稱解析設定功能

- 新增資料匯出
- 批次修改

Home / 系統管理 / IP 名稱解析

Botnet

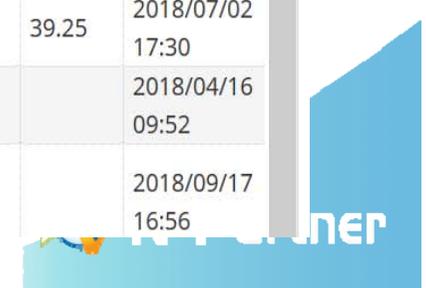
匯入/匯出

批次修改/刪除

	網段名稱	網段定義	Flow	數值低於下列門檻將...			觸發率 (%)			數值低於下列 b...		最近修改時間
				Session/	pps	bps	Session/	pps	bps	In	Out	
<input type="checkbox"/>	Gookey	192.168.9	啟動	256		102.4 K	101	101			2018/07/17 11:16	
<input type="checkbox"/>	Gookey_test4	192.168.4.0/24,192.168.4	啟動	512		1.5 M	101	101			2018/07/17 10:08	
<input type="checkbox"/>	Gookey_test_auto1	192.168.9.0/24,192.168.9	啟動	0	0.98 K	0.98 K	0	500	600	0.01	0	2018/07/03 09:50
<input type="checkbox"/>	Gookey_test_auto2	192.168.4.0/24,192.168.4	啟動	0	0.98 K	0.98 K	0	500	600	238.5	0.6	
<input type="checkbox"/>	Home	16.0.0/16	啟動	0	29.44 K	67.62 M	0	500	600	177	39.25	2018/07/02 17:30
<input type="checkbox"/>	Sales Department	192.168.4.0/24	啟動		10 K	50 M		500	600			2018/04/16 09:52
<input type="checkbox"/>	人事部門 HR Department	192.168.1.0/24	啟動		70 K	50 M		500	600			2018/09/17 16:56

此頁全選

可同時選多筆



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

編輯設備告警樣版

名稱
Default

門檻值設定

監看 CPU > 70 % 告警

監看 Memory

ICMP 告警

監控週期

- 5 分鐘
- 30 秒
- 1 分鐘
- 5 分鐘

介面列表 監控設定 用戶IP對應MAC MAC對應介面 Flow Drop

設備
----- All Devices -----

搜尋

IP	MAC
192.168.0.8	AC:1F:6B:6
192.168.0.8	AC:1F:6B:6
192.168.0.9	B4:96:91:1
192.168.0.9	B4:96:91:1
192.168.0.11	AC:1F:6B:6

Home / 設備管理 / 介面列表

介面列表 監控設定 用戶IP對應MAC MAC對應介面

設備
----- All Devices -----

搜尋

MAC	設備名稱	介面名稱
00:0C:29:00:0E:EA	Global ZYXEL 192.168.2.252	swp12
00:0C:29:00:0E:F4	Global ZYXEL 192.168.2.252	swp12
00:0C:29:09:64:30	Global ZYXEL 192.168.2.252	swp19

設備告警 介面告警 自訂 OID 樣版 硬碟告警 ICMP 告警

搜尋

操作	所屬領域	名稱	監看 ICMP	監控週期	建立時間
	Global	CoreRouter_icmp_30s	On, 2 ms	30 秒	2019/07/26 10:26
	Global	Firewall_icmp_1m	On, 1 ms	1 分鐘	2019/07/26 10:27
	Global	Server_icmp_3m	On, 3 ms	3 分鐘	2019/07/26 10:27

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

Home / 設備管理 / 設備樹狀圖

設備樹狀圖 自動更新 66

搜尋

操作	IP	設備名稱	設備種類	Model	資料格式	狀態	介面	硬碟	建立時間	瀏覽
	10.235.48.191	Bestcom AD Test 10.235.48.191	Syslog		Windows AD				2018/05/08 19:19	
	10.251.158.29	10.251.158.29	Syslog		Fortinet				2018/04/19 09:59	
	10.64.103.44	10.64.103.44	Syslog		Forcepoint Web Security				2018/09/17 14:46	
	172.22.22.27	Abor_172.22.22.27	Syslog		Arbor				2018/08/30 13:36	
	192.168.0.3	Herb Juniper SRX 192.168.0.3 中文測試	Syslog, Snmp	Cisco	Juniper SRX				2018/04/13 20:28	
	192.168.1.43	Herb Imperva 192.168.1.43 tact180824 野村投信	Syslog		Imperva				2018/09/19 17:18	
	192.168.1.90	Herb Win2k8 AD CHT 192.168.1.90	Syslog, Flow, Snmp	Host Mib	Windows AD				2018/09/13 14:42	
	192.168.1.92	Herb Win2k8 CHT 192.168.1.92	Syslog, Snmp	Host Mib	Auto (Full Event)				2018/05/10 15:50	
	192.168.10.14	Herb TP 192.168.10.14	Syslog		TippingPoint				2018/04/13 20:26	
	192.168.10.15	Herb TP 192.168.10.15 中文測試	Syslog		TippingPoint				2018/09/13 09:30	
	192.168.110.252	192.168.110.252	Flow						2018/04/19 09:59	
	192.168.2.10	MAX-Test	Syslog		A10 TPS				2018/07/19 17:09	

自動新增預設報表、監控

- 可依需求再手動編輯

新增設備

設備基本設定

名稱
Firewall

IP
192.168.1.254

設備種類
 Syslog Flow SNMP

Syslog 相關設定

資料格式
Fortinet

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

 是否啟用預設報表，將套用至相同廠牌型號設備？

Yes No

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

訂製分時監控報表

分時監控報表名稱

報表時間單位

1分鐘 5分鐘

分時監控 Top N ON

名稱

排序依據

事件

來源 IP
目的 IP
等級
來源區域

排序數值

Hit Count

連續高於門檻值次數

1次 (初次就告警)

樣版

設為樣版 OFF

報表型態

日報表
 週報表
 月報表

寄送日 週日

離線報表 E-Mail 群組

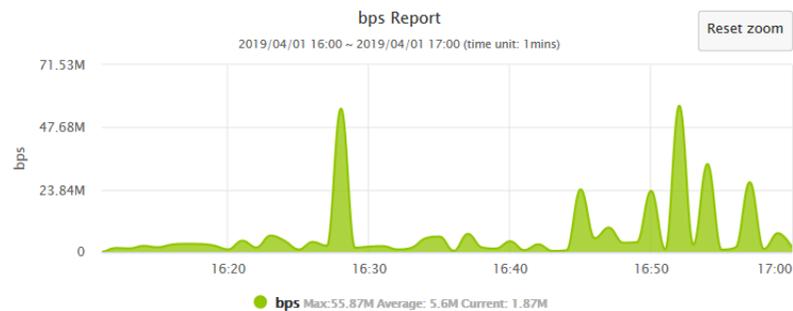
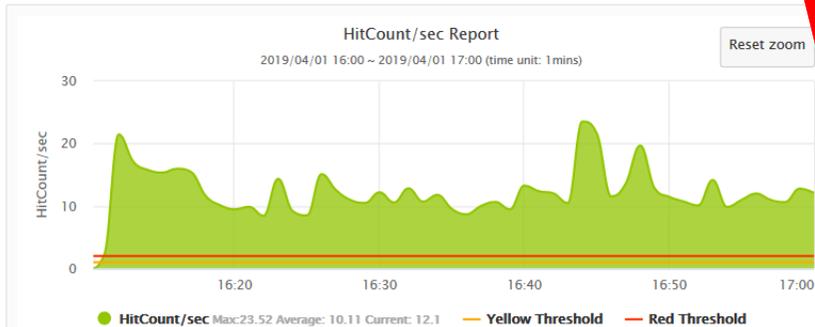
GLOBAL_ADMIN

進階 確定 取消

分時監控TopN

- 提供更詳盡內容分析
- 可自定義TopN欄位

HitCount	Session	Packets	Bytes
36.15K	32.42K	3.6M	2.50G
0%	0%	0%	0%
96.08%	0%	0%	0%



分時監控 Top N 報表 - Filter_for_autoaction

查詢時間區段
2019/04/01 16:05 ~ 2019/04/01 17:05 啟動查詢

Top N
top src ip

Filter Topn: top src ip (HitCount)
2019/04/01 16:05 ~ 2019/04/01 17:05 (time unit: 1mins)

Reset zoom

Filter Topn: top src ip (HitCount)
2019/04/01 16:30 ~ 2019/04/01 16:30

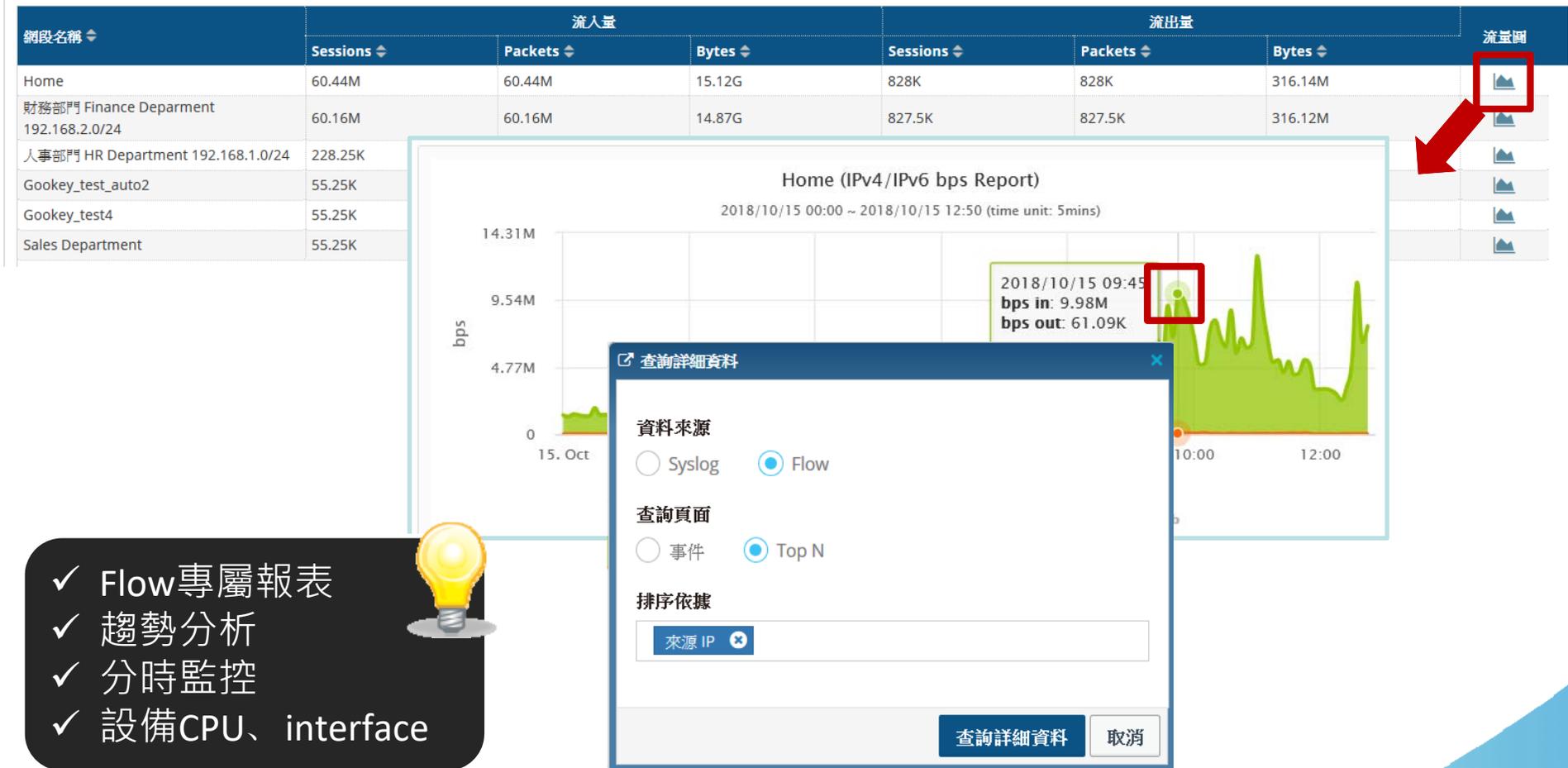
36.01% 11.70% 10.23% 9.86% 8.29% 6.48% 4.27% 4.18% 3.57% 2.96% 2.46%

NO	來源 IP	Hit Count	Sessions	Packets	Bytes
1	192.168.2.25	3.47K	3.47K	4.86K	536.33K
2	192.168.2.143	3.04K	3.04K	96.91K	62.6M
3	192.168.2.129	2.93K	2.93K	139.26K	123.69M
4	0.0.0.0	2.46K	0	0	17.66M
5	192.168.2.55	1.92K	1.92K	3.83K	276.19K
6	192.168.2.111	1.27K	1.27K	76.96K	63.94M
7	192.168.2.125	1.24K	1.24K	67.09K	53.34M
8	192.168.2.155	1.06K	1.06K	142.81K	152.89M
9	192.168.2.159	899	899	38.49K	19.84M

顯示 1 到 64 共 64 記錄

關閉

強化資料跳查自由度



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

提供更多種報表型式選擇

Top N 報表

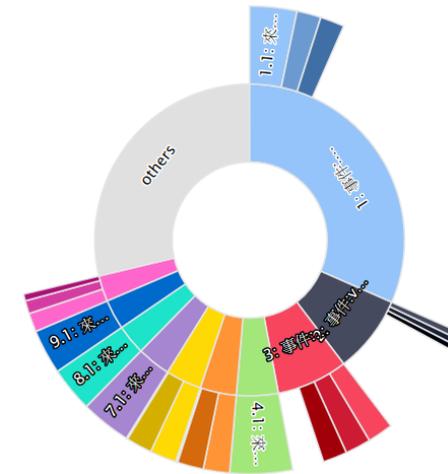
+ 查詢條件 ▾ 進階條件 ▾ Show All 重新輸入 啟動查詢

查詢時間區段 選擇時間區段 1小時內 ▾ 過去 起迄時間

報表製作依據 Syslog Flow

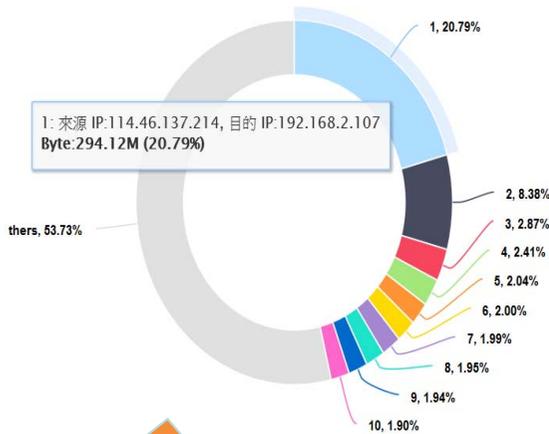
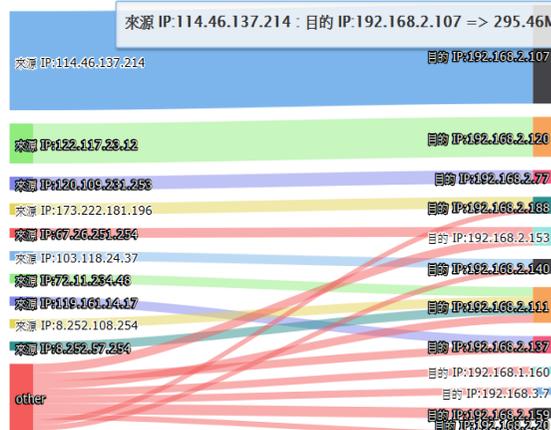
報表型式 圓餅圖 環圈圖 長條圖 柱狀圖 桑基圖 曲線圖

Top 10 HitCount
2019/09/10 10:57 ~ 2019/09/10 11:57



Top 20 Byte

2019/09/10 10:54 ~ 2019/09/10 11:54



環圈圖

桑基圖

NO	事件	Hit Count	Sessions	Packets	Bytes	流量圖
1	C006958: P2P: Kademia Request	114,49K 31.54%	0	0	0	
NO	來源 IP					
1.1	60.0.0.1					
1.2	192.168.1.11					
1.3	192.168.1.12					

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

事件	報表	智慧分析	設備管理	系統管理		
趨勢分析例外清單	異常流量	長時間連線監控				
搜尋	Q	↺	+	≡	↻	i
類型	<input checked="" type="radio"/> IP	<input type="radio"/> Port	<input type="radio"/> 事件關鍵字			
操作	IP	建立時間				
 	5.101.40.241	2018/12/03 17:02				
 	192.168.1.111	2019/01/21 14:59				

操作	所屬領域	事件關鍵字	安全值	建立時間
 	Global	https	10000	2019/07/17 15:27

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)	

優化網段告警機制

- 可自動學習網段 流量上限/下限 閾值
- 學習到的安全值可呈現在UI

名稱解析流量異常告警

數值低於下列門檻將不觸發告警			觸發率 (%)
<input checked="" type="checkbox"/>	自動學習		
<input type="checkbox"/>	0	Session/sec	0
<input type="checkbox"/>	98	M pps	500
<input type="checkbox"/>	346	M bps	600

數值低於下列 bps 門檻觸發告警

<input checked="" type="checkbox"/>	自動學習		
<input type="checkbox"/>	In	14	K bps
<input type="checkbox"/>	Out	16	K bps

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

動態欄位顯示 Auto Default Security 達標

事件欄位偏好設定

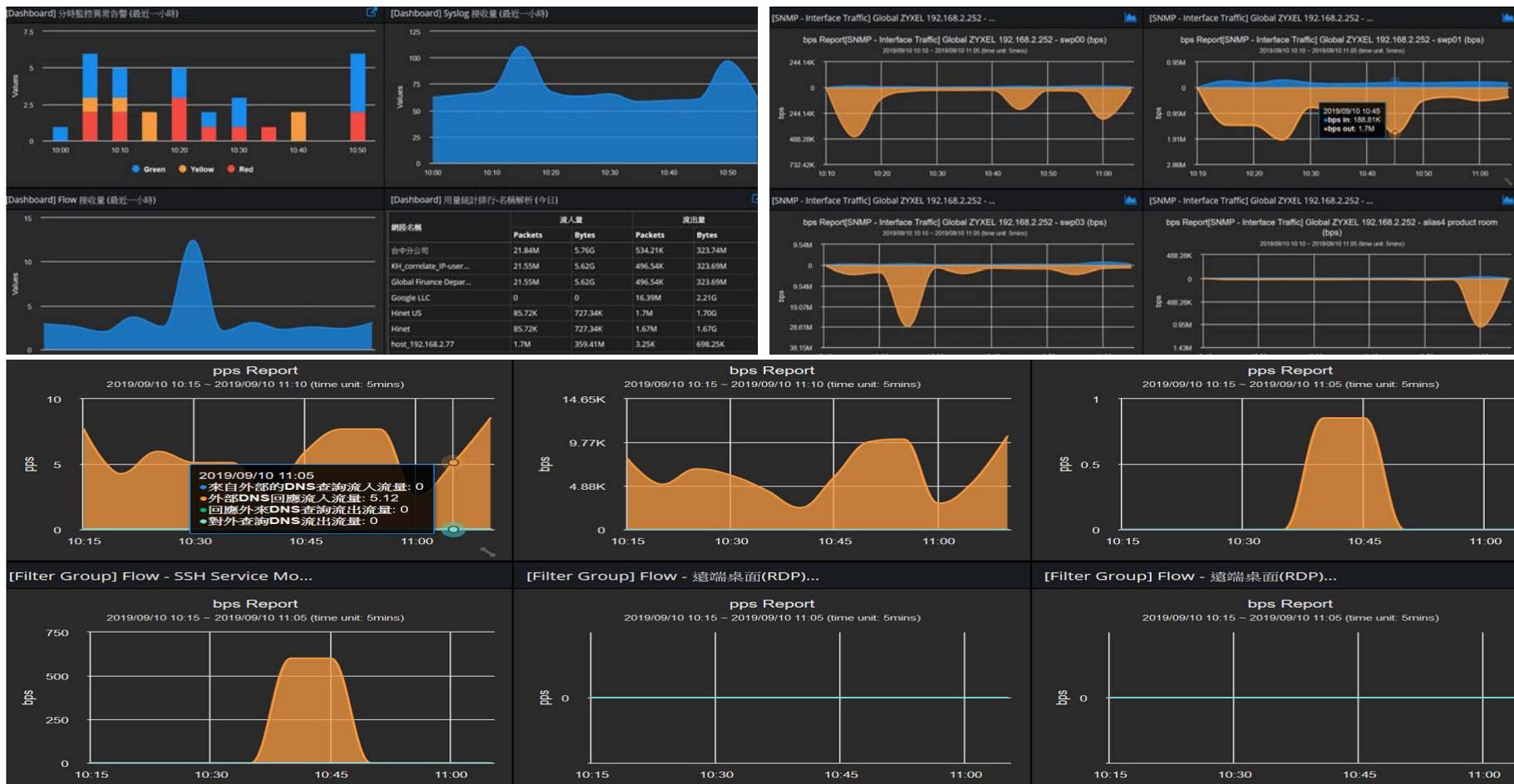
欄位樣版名稱

預設查詢依據 Syslog Flow

事件欄位	可選欄位
<input type="checkbox"/> <input type="checkbox"/>	時間 設備 等級 事件 來源 IP 目的 IP
PDF 事件欄位	可選欄位
<input type="checkbox"/> <input type="checkbox"/>	時間 設備 等級 事件 來源 IP 目的 IP

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

目錄樣板

樣板名稱

類別

Backend Domain

Menus

- 事件
 - 事件查詢 R R+W
 - 已儲存查詢條件 R R+W
- 報表
 - Top N
 - Top N 報表 R R+W
 - 已儲存報表 R R+W
 - Top N 離線報表群組 R R+W
 - ☆ 加值報表
 - 郵件統計* R R+W

新增SNMP功能

- 可自定義OID監控

Home / 設備管理 / 告警樣版

設備告警	介面告警	自訂 OID 樣版	硬碟告警	ICMP 告警				
搜尋								
🔍	🔄	+						
操作	自訂 OID 樣版名稱	OID	繪製曲線圖	啟用告警	種類	告警條件	監控週期	建立時間
 	Aruba CPU	.1.3.6.1.4.1.11.2.14.1	啟用	啟用	Instance	> 50 %	5 分鐘	2018/08 21:37
 	Aruba Fan	.1.3.6.1.4.1.11.2.14.1	啟用	停用	Instance	> 0	5 分鐘	2018/08 21:39
 	Aruba Memory	.1.3.6.1.4.1.11.2.14.1	啟用	停用	Instance	> 0 %	5 分鐘	2018/08 21:38
 	Dell iDRAC-CPU Status	1.3.6.1.4.1.674.1089	啟用	啟用	Table [Average]	!= 3	5 分鐘	2019/06 17:12
 	Dell iDRAC-Memory Status	1.3.6.1.4.1.674.1089	啟用	啟用	Table [Average]	!= 3	5 分鐘	2019/06 17:46

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

The screenshot displays the N-Partner web interface. On the left is a dark sidebar with navigation options: '事件', '報表', 'Top N', 'Top N 報表', '已儲存報表', and 'Top N 離線報表群組' (highlighted with a red box). The main content area shows a breadcrumb path: 'Home / 報表 / Top N / Top N 離線報表群組'. Below this is a section titled '已儲存報表' with a search bar and a green '+ ' button. A table is displayed with the following data:

操作	報表名稱	已選報表
 	AD報表群組	AD Recently Created Users, AD Recently Deleted Users, AD Recently Locked Out Users, AD Recently Password Change Users, AD Terminal Services Activity, AD User Failed to Change Password, AD Logon Failures, AD Frequently Lockedout Users

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

Home / 報表 / 分時監控報表 / 總量流量總表

已儲存報表

搜尋

操作	總量流量報表名稱	類型	建立時間	最近修改時間	瀏覽
 	SSH流量報表	Byte	2018/06/07 12:17		 



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%

更彈性的自動聯防

- 可自訂連防指令、自動定位switch

阻擋類別

全部 IP Switch / Port 介面 Script + 設備 Script Only

狀態

全部 已阻擋 已復原 阻擋失敗 復原失敗 準備阻擋中 復原中 執行成功

搜尋

復原阻擋	所屬領域	阻擋標的	執行阻擋設備名稱	阻擋類別	狀態	阻擋時間	復原時間	自動復原週期 (min)	執行結果
<input type="checkbox"/>	Global	\$SRC_IP:10.24.91.1	10.24.91.232	Script + 設備(自動阻擋: Cisco 2960)	已阻擋	2019/03/25 16:25		60	
<input type="checkbox"/>	Global	\$SRC_IP:10.24.91.1	10.24.91.232	Script + 設備(自動阻擋: 960)	已復原	2019/03/25 16:21	2019/03/25 16:24	60	
<input type="checkbox"/>				Script / 自動阻擋		2019/03/25			

編輯自動阻擋

名稱

自動定位IP阻擋_Henry

判定條件

分時監控報表 syslog any

分時監控 Top N Switch 自動定位 action_Henry

判定時間區段 1分鐘

觸發門檻值 5 M

觸發執行指令 自動定位 Switch (以IP阻擋)

自動復原時間 1小時

復原執行指令 不執行

確定 取消

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)

新增執行指令樣版

名稱

Cisco ACL action

指令列表

Expect

Command en

```
config t
[Password:] admin
ip access-list extended np-script-block-list
no 2147483647 permit ip any any
deny ip host $SRC_IP any
2147483647 permit ip any any
exit
exit
```

指令執行間隔(延遲) 0 sec

確定 取消

黑名單聯防機制

- 將已知惡意IP快速佈署到資安設備阻擋

Home / 報表 / 異常 IP 阻擋 / 黑名單

黑名單 黑名單執行設備

搜尋 [Q] [↺] [+] [↵] [i]

來源
全部

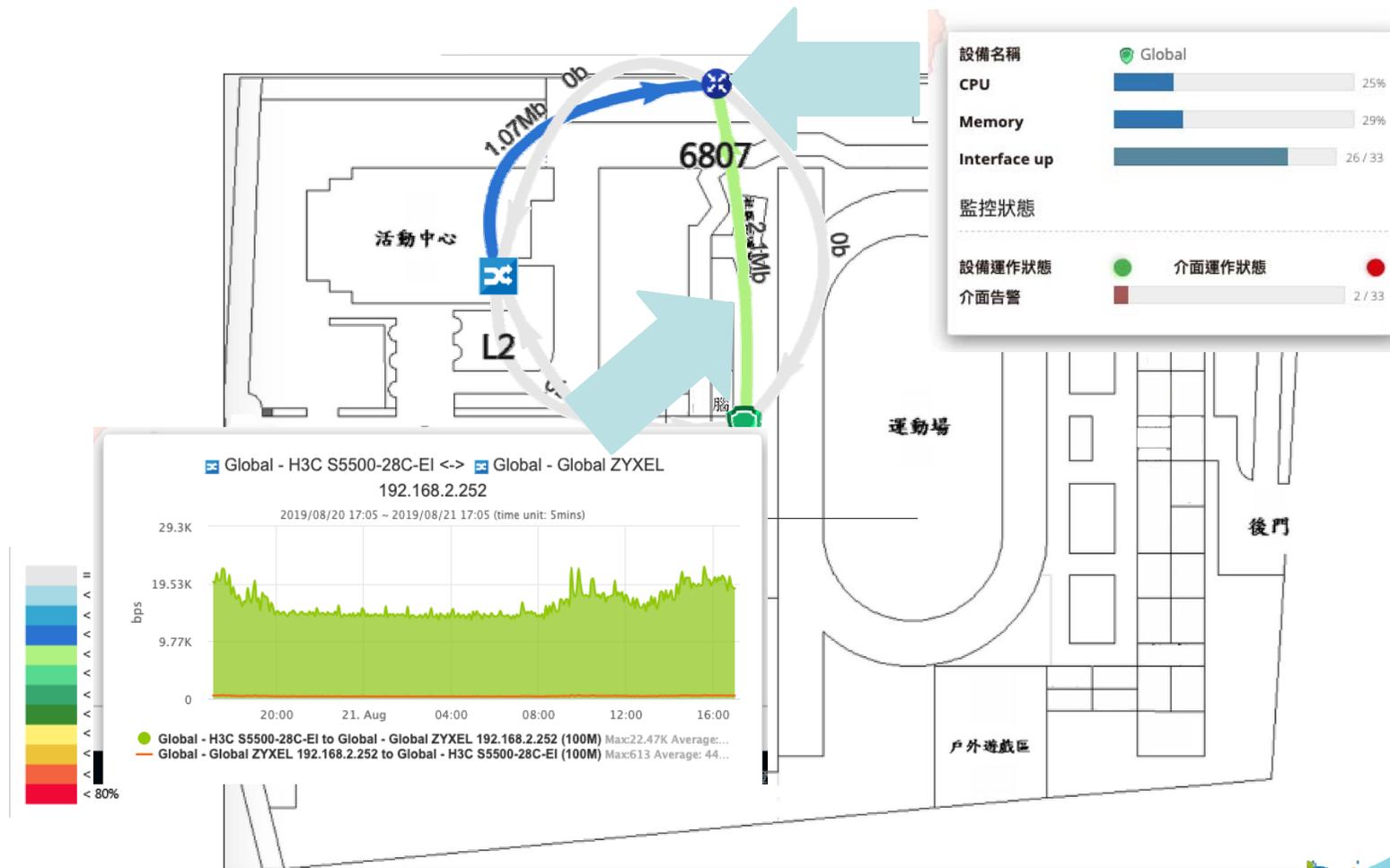
類型
 全部 IP FQDN Protocol:Port

運作狀態
 全部 未生效 阻擋中

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

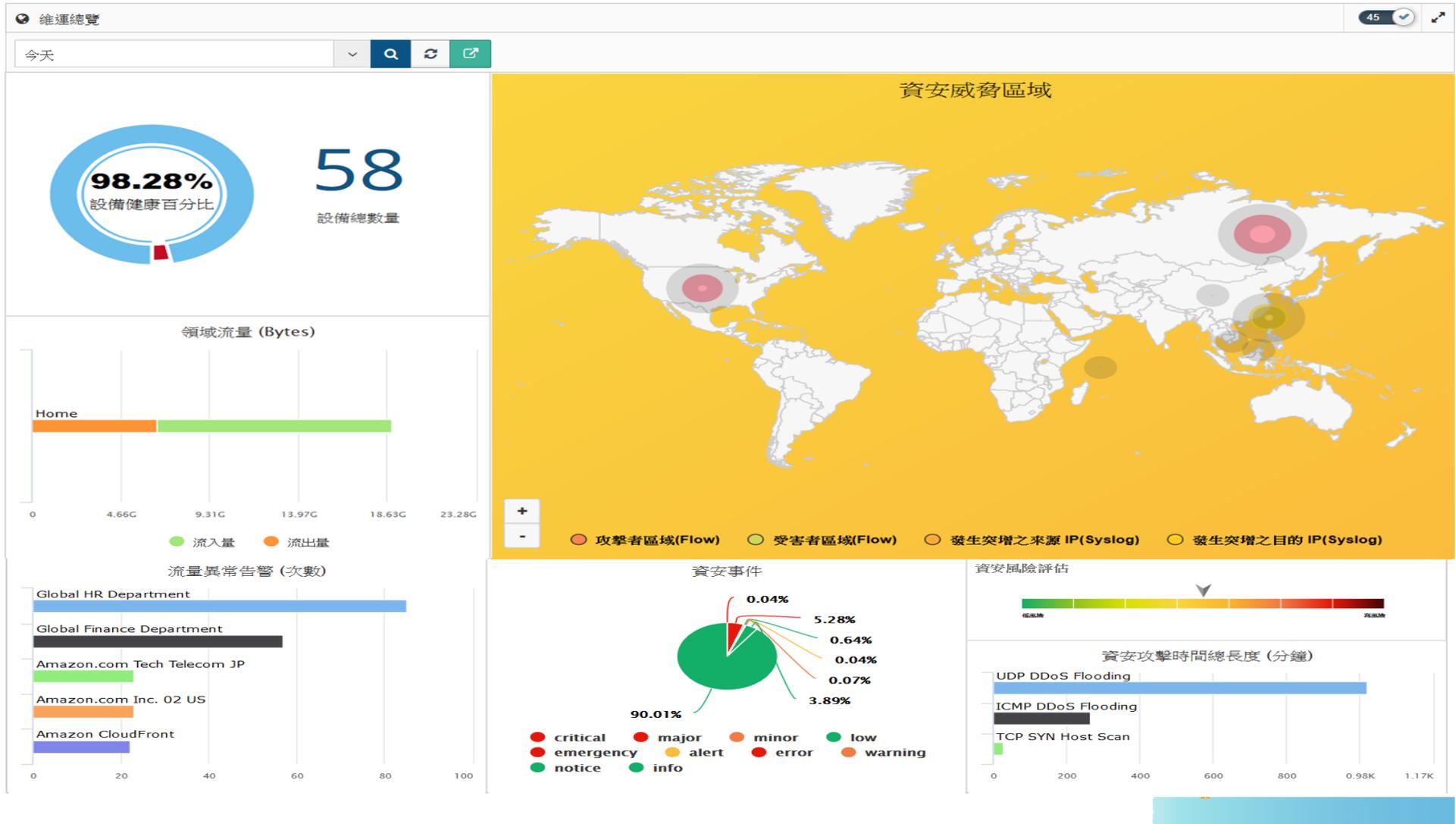
提供拓樸圖

- 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



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

