



# Cloud

*The smartest syslog reporter in the world*

Training Material- 報表

Henry Yu  
henry@npartnertech.com



**N-Partner**

Next Generation Technologies & Security of Network

## ■ TOP N

- ✓ 產生TopN統計報表
- ✓ 定期匯出離線報表

## ■ 分時監控報表

- ✓ 以時間軸為基準的圖表
- ✓ 設定告警門檻值
- ✓ 可將2個監控報表設為群組，方便比較差異

## ■ 趨勢分析

- ✓ syslog事件即時趨勢分析
- ✓ 異常流量趨勢分析
- ✓ N-Cloud 會自動學習和判斷

## ■ 異常IP阻擋

- ✓ 阻擋清單和紀錄

## ■ Flow專屬報表

- ✓ Flow 報表/ protocol 報表/ 封包大小分布報表
- ✓ N-Cloud 會自動學習和判斷
- ✓ 在[名稱解析]啟動flow分析功能就可以分析組織流量

	報表
	Top N
	分時監控報表
	趨勢分析
	異常IP阻擋
	Flow 專屬報表

報表

- Top N
- 分時監控報表
- 趨勢分析
- 異常IP阻擋
- Flow 專屬報表

Top N 報表  
已儲存報表

起始時間 2016 年 5 月 18 日 0 時 0 分

結束時間 2016 年 5 月 23 日 0 時 0 分 OK

事件 ▶ 事件查詢  頁面自動更新 (120秒)

+ 查詢條件 進階條件 Show All 重新輸入

查詢時間區段 ● 選擇時間區段 5分鐘內 過去 起迄時間

報表製作依據 ● Syslog ○ Flow 事件型態  Security  Traffic  Audit  Web  Other

時間區段選擇

事件型態

調整查詢依據為syslog  
事件或flow紀錄。  
可以從[系統管理 > 偏好設定]調整預設值

報表

- Top N
- 分時監控報表
- 趨勢分析
- 異常IP阻擋
- Flow 專屬報表

Top N 報表  
已儲存報表

進階條件

- 應用服務
- 使用者名稱
- 時間範圍
- Policy ID
- Protocol
- 區域過濾
- 流量過濾
- 封包大小
- 主機名稱
- 寄件者
- 收件者
- MAC
- 介面過濾
- 路徑
- 作業系統
- 分類
- 狀態
- 無線基地台
- AP SSID
- Session ID

事件 ▶ 事件查詢  頁面自新 (120秒)

查詢條件     進階條件    Show All

查詢時間區段  選擇時間區段 5分鐘內  過去

Syslog  Flow    事件

Priority  Traffic  Audit  Web  Other

基本條件

- 設備
- 事件關鍵字
- IP過濾
- Port 過濾
- 動作
- 等級

報表

- Top N
- 分時監控報表
- 趨勢分析
- 異常IP阻擋
- Flow 專屬

報表 ▶ Top N 報表  頁面自動更新 (120秒)

+ 查詢條件      進階條件      Show All      重新輸入

時間區段 ▶ ● 選擇時間區段 1小時 迄時間

事件依據 ▶ ● Syslog ○ Flow      事件型態  Security

Top N 報表  
已儲存報表

顯示所有條件

支援邏輯判斷式, [+] 代表 or,  
[!] 代表not

URL, 檔案路徑

查詢條件留空代表查詢any



事件關鍵字 ▶   查詢空事件 

應用服務 ▶

使用者名稱 ▶

Policy ID ▶

主機名稱 ▶

寄件者 ▶

收件者 ▶

MAC ▶

路徑 ▶

作業系統 ▶

分類 ▶

無線基地台 ▶

狀態 ▶

AP SSID ▶

Session ID ▶

報表 ▶ Top N 報表  頁面自動更新 (120秒)

查詢條件 進階條件 Show All 重新輸入

查詢時間區段 選擇時間區段 1小時 逾時間

報表製作依據  Syslog  Flow 事件型態  Security

報表

Top N 已儲存報表

分時監控報表

趨勢分析

異常IP阻擋

Flow 專屬

1 查詢指定IP

2 點這

3 輸入IP

3 使用名稱解析

4 [+] 代表新增, [!] 代表排除

5 OK

6 指定設備

使用者名稱

Protocol N/A

IP過濾  同時判定來源與目的IP  判定來源或目的IP

Port過濾  同時判定來源與目的Port  判定來源或目的Port

區域過濾  同時判定來源與目的區域  判定來源或

介面過濾  同時判定流入與流出介面  判定流入或

流量過濾  流量(bytes) >  封包

封包大小

時間範圍

設備 Global - Cisco6509-A  
Global - Cisco6509-B

IP網段過濾條件

單一IP或網段:

IP範圍:

IP名稱解析: Network Domain

Home  
[!]192.168.0.1

確定 取消

報表

- Top N
- 分時監控報表
- 趨勢分析
- 異常IP阻擋
- Flow 專屬報表

Top N 報表  
已儲存報表

啟動查詢

點這

9

選擇報表形式

7

報表型式  圓餅圖  長條圖  曲線圖

排序依據 事件

排序欄位 來源IP  
目的IP  
等級  
來源區域

排序數值 Hit Count 比對圖 Byte

數值顯示:  Hit Count  Session  Packet  Byte

排序依據

選擇排序欄位

8

排序數值

選擇哪些數值會顯示在報表中

報表

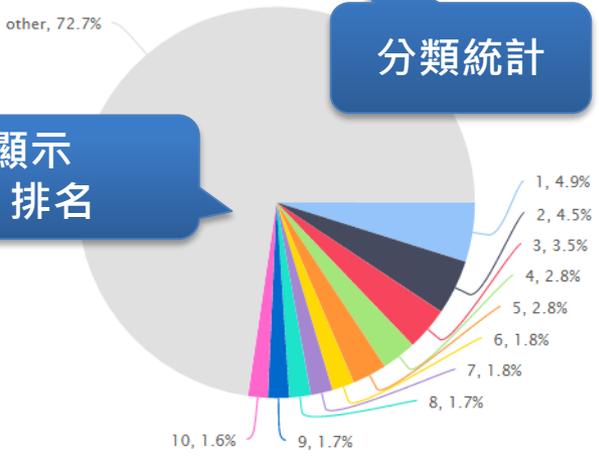
- Top N
- 分時監控報表
- 趨勢分析
- 異常IP阻擋

Top N 報表  
已儲存報表

N-Cloud 報表支援滑鼠左鍵點擊：  
點擊圖片或表格後會啟動[事件查詢]



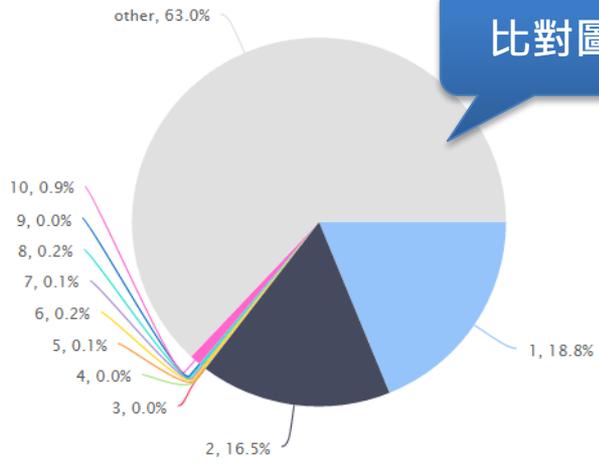
Top 100 Byte  
2016/5/24 15:18 ~ 2016/5/24 15:48



分類統計

以%顯示  
TOP N 排名

Top 100 Session  
2016/5/24 15:18 ~ 2016/5/24 15:48



比對圖

TOP N 排名表格

總筆數: 100

NO	來源IP	目的IP	Hit Count	Sessions	Packets	Bytes	流量圖
1	61.219.36.250	163.30.82.250	0	6.31K	2.4M	3.21G	
2	61.219.36.120	163.30.82.250	0	5.54K	2.11M	2.97G	
3	210.59.185.6	163.30.37.15	0	7	1.58M	2.31G	

報表

- Top N
- 分時監控報表
- 趨勢分析
- 異常IP阻擋
- Flow 專屬報表

Top N 報表  
已儲存報表

儲存報表 啟動查詢

1 點擊儲存報表

2 設定報表名稱

儲存報表

輸入報表名稱: \_\_\_\_\_

定義工作時段: 起 0 : 00 迄 23 : 59

定義工作日:  週日  週一  週二  週三  
 週四  週五  週六

報表型態:  日報表  週報表 寄送日 週日  
 月報表  半月報表  
 季報表  年報表  半年報表

E-Mail 群組: ---不寄送---

資料格式:  HTML  PDF  CSV  XML

樣版:  設為樣版

確定 取消

3 定義工作時段

4 離線報表型態

5 接收報表的 Mail 群組

6 資料格式

7 OK

工作時段以外的資料，  
不會被列入報表內



報表

- Top N
- 分時監控報表
- 趨勢分析
- 異常IP阻擋

已儲存報表

Top N 報表

已儲存報表

報表 ▶ 已儲存報表

總筆數: 3

操作	報表名稱	報表製作依據
 	外部廣播行為日報表	Flow
 	外部查詢DNS主機日報表	Flow
 	大陸地區瀏覽學校網站月報表	Flow

編輯條件或刪除報表

1 點擊這邊  
瀏覽歷史報表

操作	報表名稱	報表型態	報表起始時間	報表結束時間	瀏覽	下載報表
	外部查詢DNS主機日報表	手動	2016-05-24 08:27:49	2016-05-24 09:27:49		  

2 下載離線報表

報表

Top N

**分時監控報表**

趨勢分析

異常IP阻擋

Flow 專屬報表

**訂製分時監控報表**

查看分時監控報表

分時監控報表群組

報表製作依據  Syslog  Flow

事件型態  Security  Traffic  Audit  Web  Other

事件關鍵字   查詢空事件 i

應用服務

使用者名稱

Policy ID

主機名稱

寄件者

收件者

MAC

路徑

作業系統

分類

無線基地台

狀態

AP SSID

Session ID

支援邏輯判斷式, [+] 代表 or,  
[!] 代表not

URL, 檔案路徑

你可以根據折線圖來監控指定的條件，並且定義門檻值。當到達門檻值，N-Cloud就會發出告警。

報表

- Top N
- 分時監控報表**
- 趨勢分析
- 異常IP阻擋
- Flow 專屬

**訂製分時監控報表**

查看分時監控報表

分時監控報表群組

7 儲存

1 查詢指定IP

2 點這

3 輸入IP

3 使用名稱解析

4 [+] 代表新增, [!] 代表排除

6 指定設備

5 OK

確定 取消

IP網段過濾條件

單一IP或網段: [ ]

IP 範圍: [ ] - [ ]

IP名稱解析: [Network Domain] [ ]

Home [192.168.0.1]

Global - Cisco6509-A

Global - Cisco6509-B

報表

- Top N
- 分時監控報表
- 趨勢分析
- 異常IP阻擋
- Flow 專屬報表

訂製分時監控報表

查看分時監控報表

分時監控報表群組

分時監控異常列表

訂製分時監控報表

分時監控報表名稱:  <<簡易

Hit Count/Sec 門檻值: Red:  Hit Count/Sec Yellow:  Hit Count/Sec

Session/Sec 門檻值: Red:  K Session/Sec Yellow:  K Session/Sec

pps 門檻值: Red:  K pps Yellow:  K pps

bps 門檻值: Red:  M bps Yellow:  M bps

E-Mail 群組: ---不寄送---

E-Mail 通報週期: 10分

樣版:  設為樣版

確定 取消

8 設定報表名稱

9 定義門檻值

10 告警寄送Mail群組

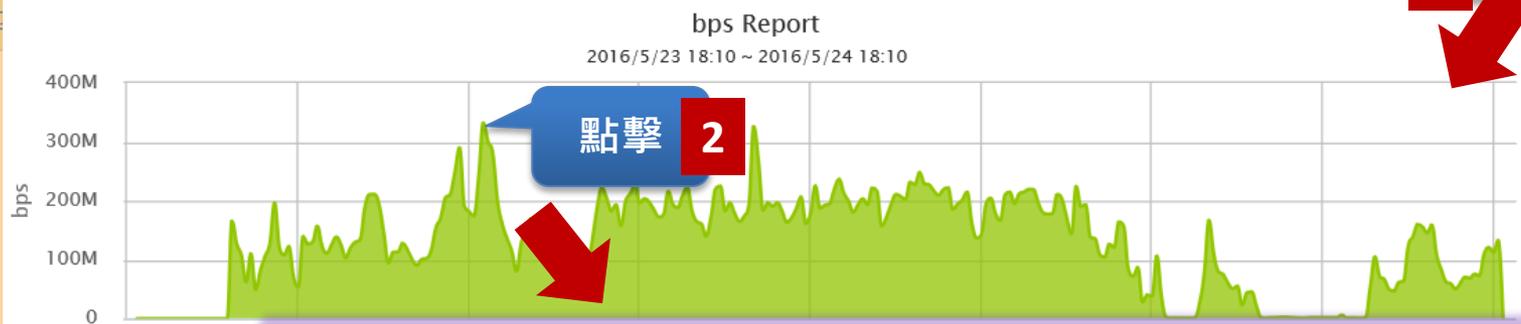
11 OK

已存報表

操作	報表名稱	報表製作依據	報表建立時間	最近修改時間	狀態				瀏覽
					Hit Count/Sec	Session/Sec	pps	bps	
	DNS流量監控	Flow	2016/05/23 19:47						
	中國大陸到市網中心總流量	Flow	2016/05/24 17:40				Green		
	市網中心到中國大陸總流量	Flow	2016/05/24 17:41						
	廣播封包								

狀態

1 瀏覽



點擊 2

時間	來源IP	來源Port	Protocol	目的IP	目的IP名稱解析	目的區域	目的Port
2016/05/24 00:19:59	185.103.109.180	43613	UDP	163.30.18.197	桃園區文山國小	TW	53
2016/05/24 00:19:59	198.48.92.104	53965	UDP	163.30.170.238	新屋區頭洲國小	TW	53
2016/05/24 00:19:59	185.103.109.180	49946	UDP	163.30.22.162	Home	TW	53
2016/05/24 00:19:59	185.103.109.180	48136	UDP	163.30.141.193	中壢區新街國小	TW	53

- 報表
- Top N
- 分時監控報表
- 訂製分時監控報表
- 查看分時監控報表
- 趨勢
- 分時監控報表群組
- 異常
- 分時監控異常列表

	報表	訂製分時監控報表
	Top N	查看分時監控報表
	分時監控報表	分時監控報表群組
	趨勢分析	分時監控異常列表
	異常IP阻擋	
	Flow 專屬報表	

**3** 選擇類型

報表 ▶ 分時監控報表群組  頁面自動更新 (04:02)

**1** 新增

分時監控報表群組

名稱: 中國大陸流量統計

類型:  Syslog  Flow

In:

Out:

**2** 設定群組名稱

**4** 選擇IN方向的報表

**5** 選擇out方向的報表

**6** OK

可以選擇多個監控報表到一張圖表內呈現。

報表

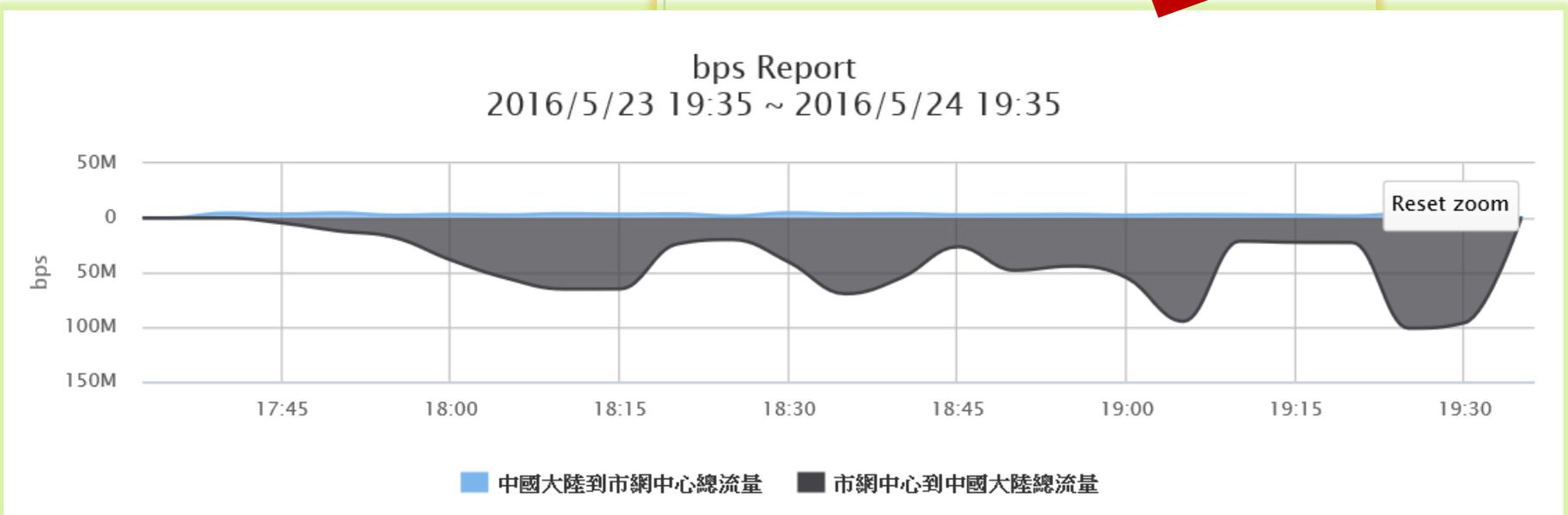
- 訂製分時監控報表
- Top N 查看分時監控報表
- 分時監控報表 分時監控報表群組**
- 趨勢分析 分時監控異常列表
- 異常IP阻擋
- Flow 專屬報表

報表 ▶ 分時監控報表群組  頁面自動更新

總筆數: 1

操作	領域	報表名稱
	Global	中國大陸流量統計

1 點擊名稱



報表

- Top N
- 分時監控報表
- 趨勢分析
- 異常IP阻擋
- Flow 專屬報表

訂製分時監控報表

查看分時監控報表

分時監控報表群組

**分時監控異常列表**

查詢條件

分時監控異常列表

查詢時間區段  選擇時間區段 1天內  過去  起迄時間

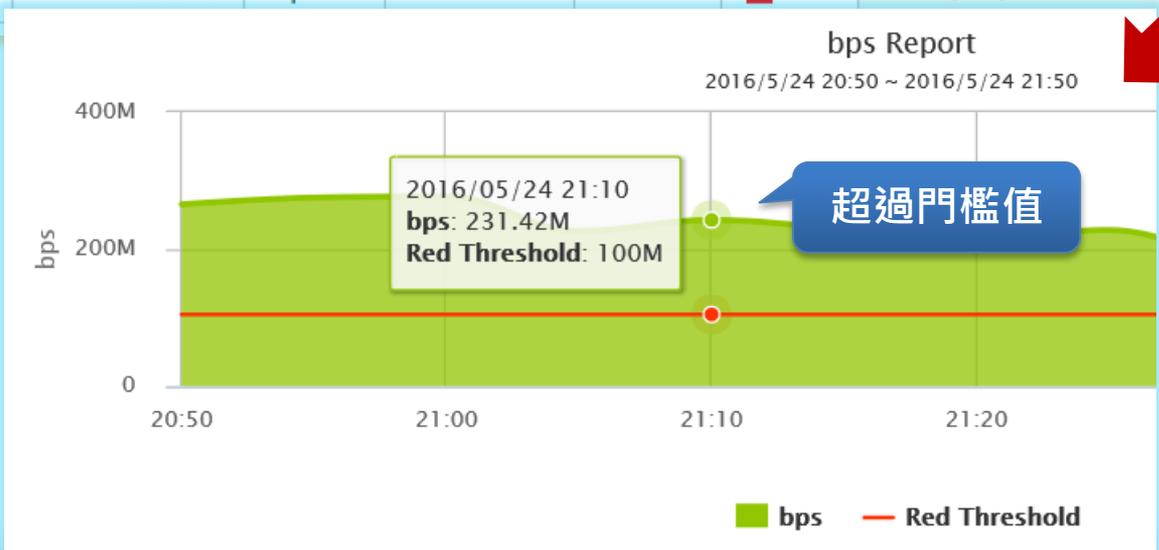
查詢範圍 **Global**

類型  All  Hit Count/Sec  Session/Sec  pps  bps

狀態  All  Green  Yellow  Red

報表名稱搜尋

領域名稱	報表名稱	類型	數值	門檻值	狀態	告警發生時間	點擊	覽
Global	DNS流量監控	bps	100.84M	100M	<span style="color: red;">■</span> Red	2016/05/24 19:45		



**報表**

- Security事件即時異常告警
- Flow即時異常告警
- 白名單
- 趨勢分析
- 異常IP阻擋
- Flow 專屬報表

**查詢條件**

查詢時間區段: 選擇時間區段 1小時 過去 起迄時間

查詢範圍: Global

查詢突增項目: 發生突增之事件

關鍵字搜尋:

趨勢分析是N-Cloud的人工智慧功能

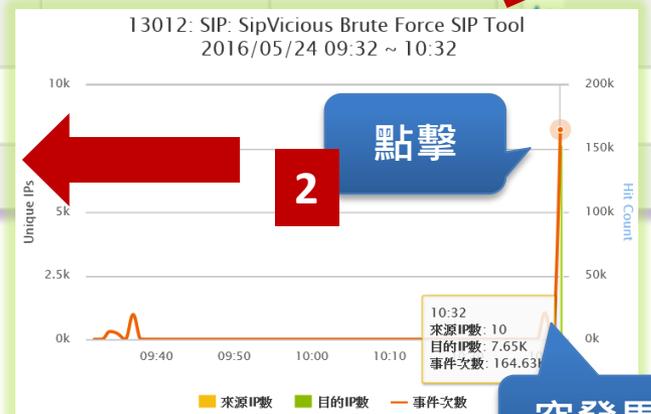
事件	突增發生時間	突增次數	過去一小時平均	突增率(%)	瀏覽突增曲線
Black List 22	2016/05/24 09:27:00	49,349	822	5,999	
13012: SIP: SipVicious Brute Force SIP Tool	2016/05/24 08:53:00	97,455	1,835	5,309	
Black List 16	2016/05/24 08:36:00	71,667	2,917	2,456	
Black List 16	2016/05/24 08:36:00	71,606			

詳細攻擊內容

1 點擊

資料時間範圍: 2016/05/24 10:30:06 ~ 2016/05/24 10:30:15 總筆數: 10000

事件	來源IP	來源Port	來源區域	次數
13012: SIP: SipVicious Brute Force SIP Tool	16	6	5061	1
13012: SIP: SipVicious Brute Force SIP Tool	16	6	5061	1
13012: SIP: SipVicious Brute Force SIP Tool	16	6	5061	1
13012: SIP: SipVicious Brute Force SIP Tool	16	6	5061	1



2 點擊

突發異常

查詢條件

報表

- Top N
- 分時監控報表
- 趨勢分析
- 異常IP阻擋
- Flow 專屬報表

Security事件即時異常

Flow即時異常告警

白名單

報表 ▶ Flow即時異常告警  頁面自動更新 (101%)

查詢時間區段  選擇時間區段 1小時內  過去  起迄時間

查詢範圍 ▶ Global

查詢異常項目 ▶

N-Cloud的智慧偵測異常流量技術

- All -----
- UDP Port Scan
- TCP SYN Port Scan
- Host Scan
- TCP SYN Host Scan
- SQL Server Host Scan
- MySQL Host Scan
- Possible Spoofed UDP DDoS Attack
- Possible Spoofed TCP SYN DDoS Attack
- Possible Spoofed TCP SYN/ACK DDoS Attack
- Possible Spoofed TCP FIN/ACK DDoS Attack
- Possible Spoofed TCP Rst DDoS Attack
- Possible Spoofed TCP NULL Flag Attack
- Possible Spoofed ICMP DDoS Attack
- Land Attack
- Burst Session on Source
- Burst Session on Destination

報表

Flow ATD Report

2016/05/24 00:00 ~ 2016/05/24 23:59



1 點擊

資料時間範圍: 2016/05/24 18:34:02 ~ 2016/05/24 18:34:31 總筆數: 10000

攻擊明細

時間	來源IP	來源IP名稱解析	來源區域	來源Port	Protocol	目的IP	目的區域	目的Port
2016/05/24 18:34:31	163.30.0.232	Home	TW	56510	TCP	141.182.113.229	US	3389
2016/05/24 18:34:31	163.30.0.232	Home	TW	53732	TCP	141.182.104.39	US	3389

— Session/sec

- 報表
- Top N
- 分時監控報表
- IP 阻擋列表**
- 趨勢
- 異常IP阻擋
- Flow 專屬報表

當你在事件進行IP阻擋時，所有的紀錄都會在這呈現



所有的阻擋歷史紀錄都在這

報表 ▶ IP 阻擋列表  頁面自動更新 (114秒)

查詢時間區段 ▶  選擇時間區段 3天內  過去  起迄時間  全部資料

查詢範圍 ▶  查詢所有管轄領域

資料來源 ▶  目前阻擋資料  歷史阻擋資料

阻擋狀態 ▶  全部  已阻擋  已復原  執行失敗  阻擋中

阻擋IP搜尋 ▶   可輸入『阻擋IP』、『執行阻擋設備名稱』或

總筆數: 0

<input type="checkbox"/>	所屬領域	阻擋IP	執行阻擋設備名稱	阻擋類別
No records found.				

手動復原阻擋

搜尋阻擋紀錄

	報表	流量報表
	Top N	Protocol
	分時監控報表	封包大小分佈
	趨勢分析	Flow Top N報表
	異常IP阻擋	網段流量異常告警
x Flow 專屬報表		

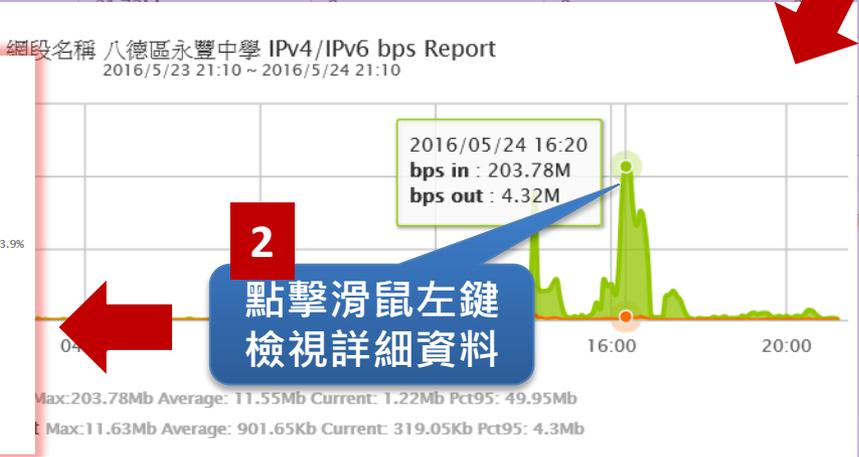
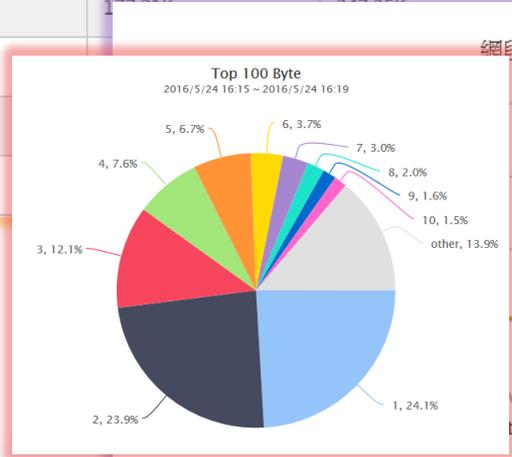
當你在[名稱解析]啟動流量分析後，會在這邊呈現流量圖表



流量

網段名稱	流入量			流出量			流量圖
	Sessions	Packets	Bytes	Sessions	Packets	Bytes	
Home	284.07M	8.81G	6,290.70G	368.17M	12.67G	6,394.76G	
八德區永豐中學	1.23M	99.78M	122.15G	1.54M	55.55M	9.30G	
八德區茄苳國小	392.85K	31.77M	23.40G	478.48K	44.49M	44.48G	
市立體育場	1.77M	147.85M	21.70M	1.77M	147.85M	21.70M	
觀音區大潭國小	1.77M	147.85M	21.70M	1.77M	147.85M	21.70M	
觀音區觀音高中	1.77M	147.85M	21.70M	1.77M	147.85M	21.70M	
觀音區奇仁國小	1.77M	147.85M	21.70M	1.77M	147.85M	21.70M	

1 點擊



2 點擊滑鼠左鍵 檢視詳細資料

**報表**

- Top N
- 分時監控報表
- 趨勢分析
- 異常IP阻擋
- Flow 專屬報表**

**流量報表**

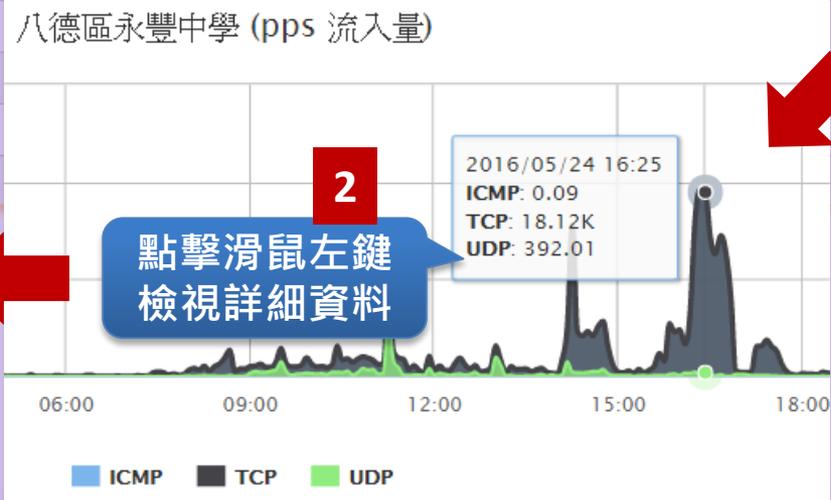
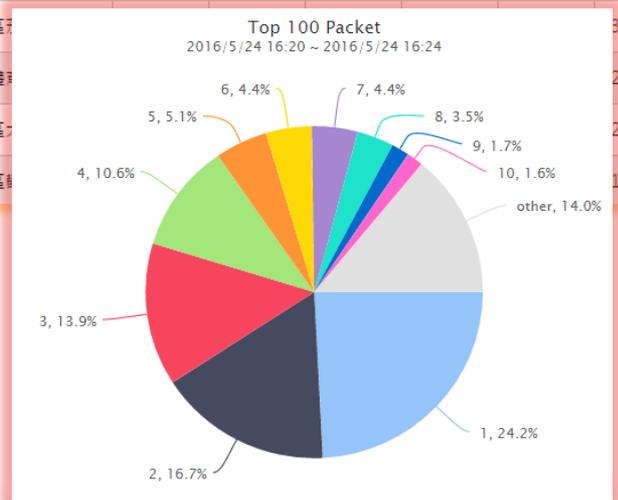
- Protocol**
- 封包大小分佈
- Flow Top N報表
- 網段流量異常告警

顯示每個[名稱解析]的 protocol 流量



By protocol

網段名稱	流入量								流出量								分佈圖
	ICMP		TCP		UDP		Other		ICMP		TCP		UDP		Other		
	packet	byte	packet	byte	packet	byte	packet	byte	packet	byte	packet	byte	packet	byte	packet	byte	
Home	9.46M	821.41M	6.72G	5,190.58	2.06G	1,096.67	2.05M	1.56G	9.71M	0.98G	7.91G	1,074.14	4.68G	5,280.57	1.95M	1.17G	
八德區永豐中學	34.43K	1.94M	87.97M	109.19G	11.69M	12.84G			14.96K	1.6M	45.57M	5.34G	9.93M	3.97G			
八德區...			3.16G														
市立體...			22.35M														
觀音區...			2.82G														
觀音區...			15.60G														
																3.03K	



1 Click

2 點擊滑鼠左鍵 檢視詳細資料

報表

- 流量報表
- Protocol
- 封包大小分佈**
- Flow Top N報表
- 網段流量異常告警

Top N

分時監控報表

趨勢分析

異常IP阻擋

Flow 專屬報表

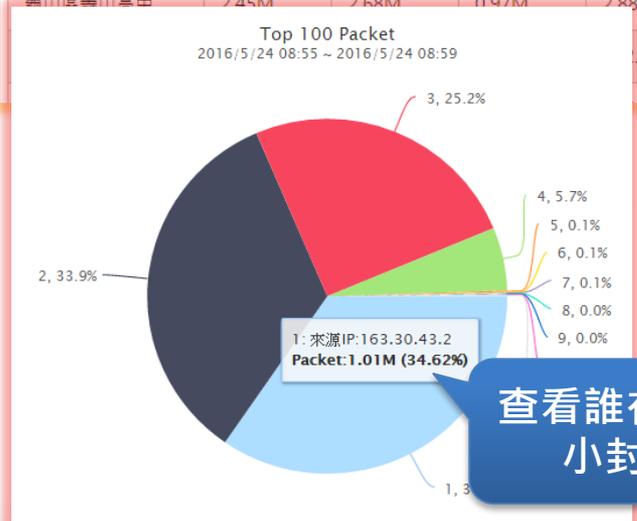
顯示每個[名稱解析]的封包大小分佈



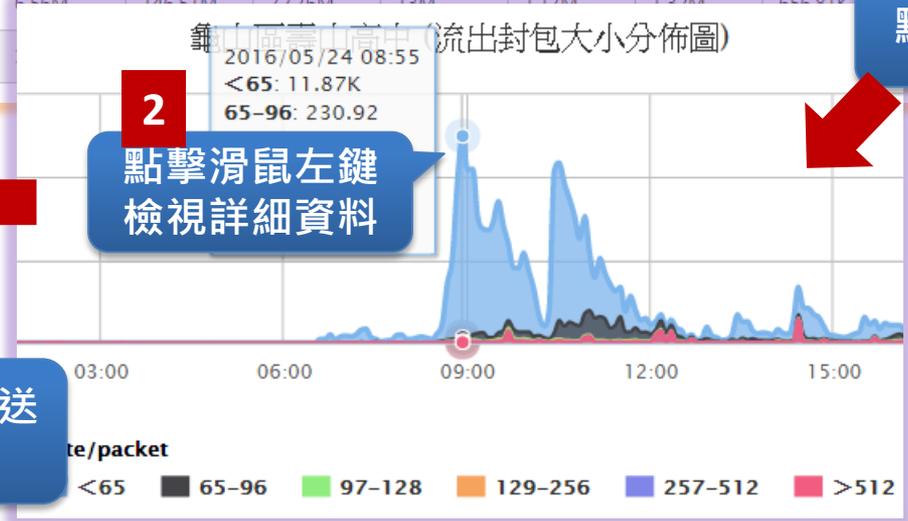
封包大小分佈

網段名稱	流入封包總數 (Packet)						流出封包總數 (Packet)						分佈圖
	< 65	65-96	97-128	129-256	257-512	> 512	< 65	65-96	97-128	129-256	257-512	> 512	
Home	2.46G	1.22G	98.67M	227.08M	312.7M	4.48G	7.21G	586.19M	92.57M	158.01M	73.16M	4.46G	
楊梅區仁美國中	1.93G	11.7M	130.45K	167.64K	580.31K	10.79M	4.79G	745.37K	197.58K	241.05K	208.52K	65.2	
龜山區泰山高中	2.45M	2.68M	0.97M	2.88M	6.56M	146.51M	72.76M	12M	1.17M	1.22M	656.91K		

1 點擊



查看誰在發送小封包



2 點擊滑鼠左鍵 檢視詳細資料

**報表**

- 流量報表
- Top N
- 分時監控報表
- 趨勢分析
- 異常IP阻擋
- Flow 專屬報表

**網段流量異常告警**

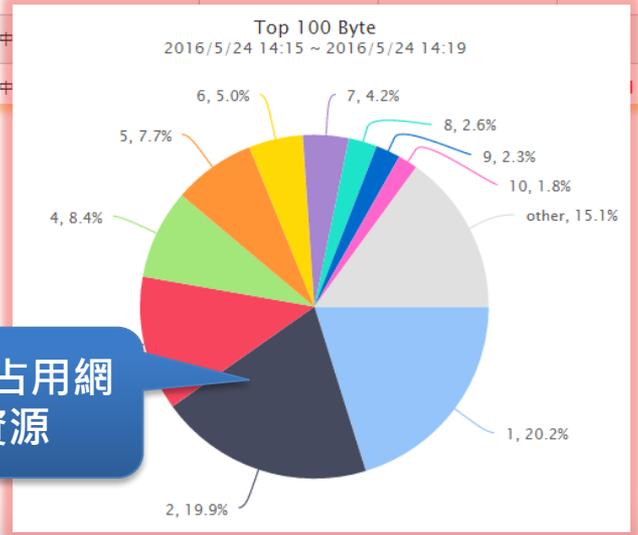
N-Cloud的人工智慧功能。當發現異常流量、協定、封包數，N-Cloud會自動發出告警。



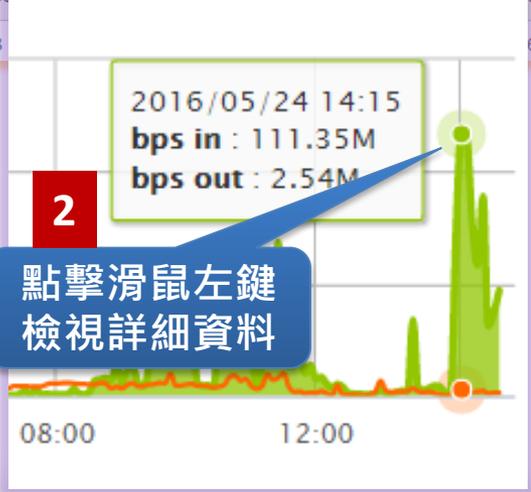
異常項目

領域名稱	網段名稱	流入量			流出量			告警發生時間	流量圖
		Session/sec	pps	bps	Session/sec	pps	bps		
Global	大園區大園國中	54.06	10.18K	111.35M	67.57	5.6K	2.54M	2016/05/24 14:15:00	
Global	中壢區忠福國小	19.12	6.75K	76.55M	22.03	3.47K	1.3M	2016/05/24 14:15:00	
Global	八德區永豐中學	53.58	15.18K	166.58M	73.27	8.06K	7.07M	2016/05/24 14:15:00	
Global	中壢區中壢國中	130.58	4.8K	2.11M	35.68	1.1K	0.04M	2016/05/24 14:10:00	

1 點擊



檢查誰占用網路資源



2 點擊滑鼠左鍵檢視詳細資料

# Practice



**N-Partner**

Next Generation Technologies & Security of Network