N-Reporter

使 用 者 手 冊

N-Reporter User Manual

5.X

2017/12/14

版權聲明

商標

手冊說明

1. 產品更新時畫面可能略有變更，請以最新版本畫面為主。
2. **Action** 用於標示該項目僅於申裝 Action Module 後顯示。
3. **Server** 用於標示該項目僅於申裝 Server Module 後顯示。
4. **Flow** 用於標示該項目僅於申裝 Flow Module 後顯示。

Contents

前言

現今網路設備、伺服器與資安產品多能支援 Syslog 或 Flow 流量資料的輸出功能，其提供足夠的資訊告訴管理者什麼人在什麼時間做了什麼事。對 IT 人員來說，最大的挑戰在於面對各式各樣的設備所產生的大量 Log 資料，要怎麼有效率的把資料轉化為有用的資訊，且在資安事件發生時，能快速還原事發當時的真相，甚至在攻擊行為發生的瞬間察覺，以達到安全防禦。

N-Reporter 把收集的資料分為資安事件、流量及伺服器 Log 三大類。訊息完整的資安事件提供簡單易懂的查詢基礎，管理者可以從網路環境中了解使用者做了哪些可疑的行為，藉由分析資安事件，可以逐步調整、改善資安設備的防禦能力，再結合流量資料可以更深入了解各個資安事件的網路用量。

N-Reporter 利用多項創新開發技術，具備蒐集、儲存、分析、查詢與報表製作等功能，為業界效能最優越、功能最強大、操作最親和的報表系統(Reporter)與分析儀(Analyzer)。為確保順利使用本產品，建議在使用前，務必閱讀本說明書。

在開始使用本產品時，基於安全的考量，強烈建議重新設定管理者密碼。如果不重新設定密碼，本產品可能被網路上的任何使用者登入並且變更設定而導致資料的流失。密碼設定方式請參考「快速安裝指引」、或是下述之首次使用章節。

首次使用

本產品提供兩種管理模式 ー 命令列模式(Command Line Interface ; CLI)與網頁模式(Graphical User Interfac ; GUI)。透過命令列模式可進行基本網路設定、密碼重置與系統回復出廠值；透過網頁模式則可進行功能操作。

當首次使用此產品時，可以使用 CLI 模式來進行基本網路設定。此外，也可以將您的電腦 IP 設定為與此設備同網段之 IP(此設備的預設 IP 為 192.168.2.1/24)，再開啟網頁瀏覽器輸入 http://192.168.2.1，登入本系統的 GUI 模式，預設帳號為「admin」，預設密碼為「admin」。詳細說明，請參考「快速安裝指引」。

使用者若忘記密碼，則可在登入頁面填上忘記密碼之帳號(如下圖)，再點選「Forget Password」，密碼就會 email 到此帳號資料的電子郵件信箱。

首次使用設定

為了讓 N-Reporter 能快速上線，並且能保持與原廠同步的更新，請確認以下設定皆正確:

網路設定

- **IP/Gateway**：N-Reporter IP 出廠預設值為 192.168.2.1，可採用 Web 或 CLI 方式進行設定。

(1) **Web 方式**：將個人電腦的 IP 設為與 N-Reporter 同網段 (例如：192.168.2.100)，用網路線直接對接個人電腦與 N-Reporter，再以瀏覽器登入 N-Reporter(預設 IP：192.168.2.1，預設帳號/預設密碼：admin/admin)。

設定方式請參考「系統管理 ➔ 網路參數設定」章節。

(2) **CLI (command line interface)**：以指令的方式設定網路，有以下兩種連線方法

使用 SSH 連線(Port 22)：將個人電腦的 IP 設為與 N-Reporter 同網段(例如 192.168.2.100)，用網路線直接對接個人電腦與 N-Reporter，再以 SSH 登入 N-Reporter(預設 IP 192.168.2.1，預設帳號/預設密碼：npartner/npartner)。

(a) 使用 Console 連線：請設定 Com 連線參數為 9600,N,8,1 (預設帳號/預設密碼：npartner/npartner)。

設定指令為：

```
N-Reporter# configure terminal
N-Reporter(config)# interface eth0 192.168.2.1 255.255.255.0 gw 192.168.2.250
```

測試方式：Ping Gateway 看是否能正確回應

```
N-Reporter# nshell
bash-3.2# ping 192.168.2.253
PING 192.168.2.253 (192.168.2.253) 56(84) bytes of data.
64 bytes from 192.168.2.253: icmp_seq=1 ttl=63 time=0.913 ms
64 bytes from 192.168.2.253: icmp_seq=2 ttl=63 time=0.967 ms
64 bytes from 192.168.2.253: icmp_seq=3 ttl=63 time=0.985 ms
64 bytes from 192.168.2.253: icmp_seq=4 ttl=63 time=0.970 ms
^C
--- 192.168.2.253 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3000ms
rtt min/avg/max/mdev = 0.913/0.958/0.985/0.046 ms
```

若發現如下訊息，則表示網路無法正確建立連線，請檢查網路設定

(例如：IP 是否衝突，網路線是否正確連接等)

```
bash-3.2# ping 192.168.2.252
PING 192.168.2.252 (192.168.2.252) 56(84) bytes of data.
From 192.168.2.66 icmp_seq=1 Destination Host Unreachable
From 192.168.2.66 icmp_seq=2 Destination Host Unreachable
From 192.168.2.66 icmp_seq=3 Destination Host Unreachable
^C
--- 192.168.2.252 ping statistics ---
packets transmitted, 0 received, +3 errors, 100% packet loss, time 3017ms
```

■ **DNS 設定**：CLI 設定指令為：

```
N-Reporter# configure terminal
N-Reporter(config)# ip dns1 168.95.1.1
```

■ **NTP**：CLI 設定指令為：

```
N-Reporter# configure terminal
N-Reporter(config)# ntp server tock.stdtime.gov.tw
```

Web 設定方式請參考「系統管理➔網路參數設定」章節

▶ 名稱解析

請依您的網路狀況設定名稱解析，詳細設定方式請參考「系統管理➔名稱解析」章節

系統預設的兩個名稱解析，強烈建議要依實際狀況設定，讓 N-Reporter 可以更準確的判定攻擊行為的嚴重程度。

■ Home 網段設定：定義哪些網段屬於內部網路使用。

正確的 Home 網段設定可以助於更準確的分析，主要功能如下:

(1) 可用來區分發出的攻擊 IP 或是被攻擊的 IP 是在內部還是外部

(2) 進行資安聯防阻擋惡 IP 時，能更準確的只阻擋外部 IP

(3) 進行報表分析時，定義「外網到內網」、「內網到外網」是重要的分析依據

■ 接收 Log

請在 N-Reporter 上設定 Flow 接收 Port，再把路由器或交換器的 Flow 資料送入 N-Reporter，

詳細設定方法請參考「系統管理　網路參數設定　Flow 接收 Port」章節

■ 事件/報表：

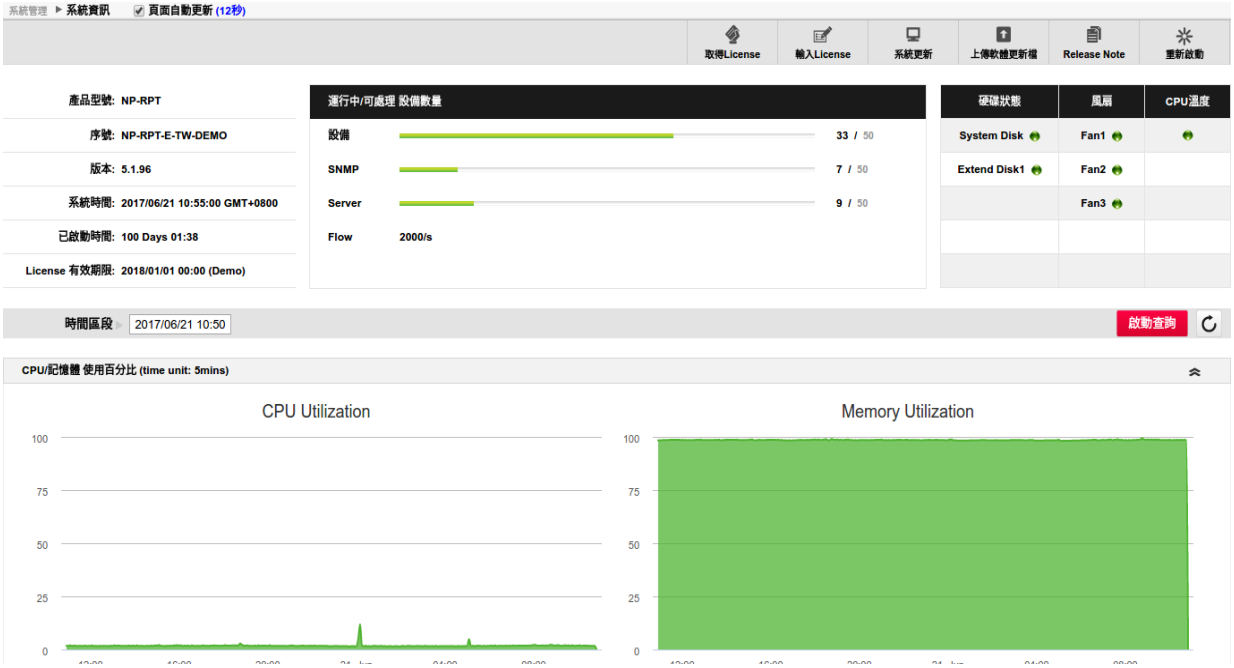
當資料成功導入 N-Reporter 之後，就可開始查詢及製作報表，詳細操作方式請參考「事件」及「報表」章節。

Chapter 1 系統管理

在此章節會介紹「系統管理」下之子功能：「系統資訊」、「網路參數設定」、「資料庫管理」、「使用者管理」、「IP 名稱解析」、「Port 名稱解析」、「報表 LOGO 上傳」、「操作歷程」、「偏好設定」、「Dashboard」等各項設定。

1.1 系統資訊

此選項的功能主要在於顯示系統資訊，包含韌體版本資訊、系統運行資訊、資料接收量等相關資訊。點選「系統資訊」選項，系統畫面如下圖所示。



頁面自動更新

當勾選「頁面自動更新」則會以每 2 分鐘(120 秒)刷新此頁

取得 License

按下取得 License 鈕，系統將連線至 N-Partner 公司的 License 資料庫主機，以取得最新的 License 授權，若有可更新的 License，即進行 License 更新，更新後會重啟系統。

- 系統若可對外連線，按下取得 License 鈕後，系統會經由 Internet 連線到 N-Partner 公司的資料庫主機，確認是否有新的 License，若有新的 License，則會自動下載更新，License 更新完畢會自動重新啟動系統(請保持 Internet 連網暢通與 DNS 設定正確)。

輸入 License

由 N-Partner 公司取得的授權 License 檔案 license.np 後，按下「輸入 License」鈕後，可經由以下畫面上傳 license 檔案，以進行 License 的輸入。系統完成 License 驗證後，將重新開機，以啟動新輸入的 License。

■ 本系統提供離線更新 License 的方式，此離線更新方式是為了因應系統無法上網的狀況(如安全控管或是網段隔離等)，取得離線 License Key 請洽銷售的經銷商。

請將取得的 License 檔案儲存於可被瀏覽到的硬碟或網路磁碟機上，按下輸入 License 鈕後，系統會彈出「輸入 License」視窗(如下圖)，請按「瀏覽」指定 License 檔案所在位置後，按上傳鈕將 License 上傳至您的 N-Reporter 設備上，License 更新完畢會自動重新啟動系統。

系統更新

按下系統更新鈕，系統將連線至 N-Partner 公司的資料庫主機，以取得最新系統版本，若有可更新版本即可進行軟體更新，更新後會重啟系統。

上傳軟體更新檔

本系統亦提供離線更新系統版本，請先取得最新版的 N-Reporter 映像檔，按下上傳軟體更新鈕，系統會彈出「上傳軟體更新檔」視窗，請按「瀏覽」指出新映像檔所在位置後，按上傳鈕將更新檔上傳至您的 N-Reporter 設備上，系統更新完畢會自動重新啟動系統。

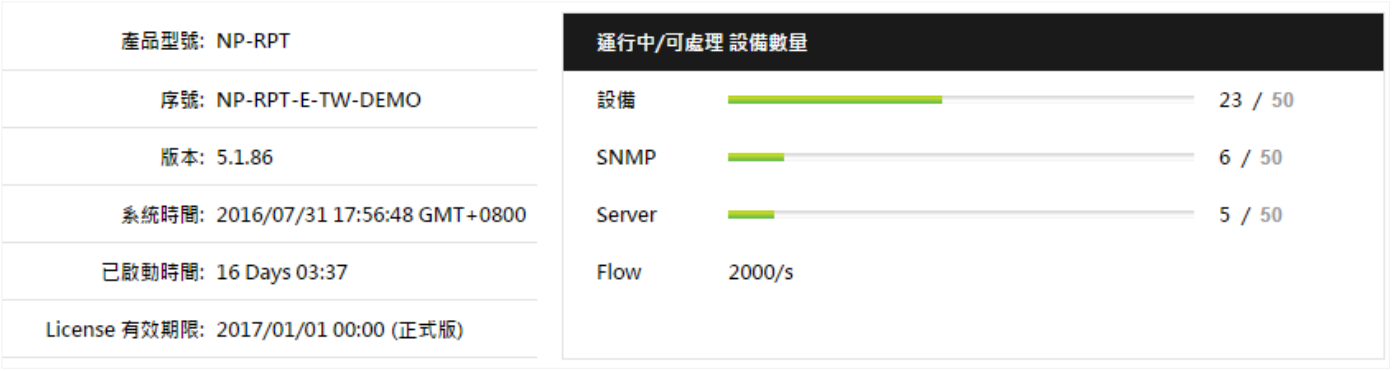
(請注意檔案名稱應為 NReporter-x.x.x.img，其中 x.x.x 為軟體版本)。

Release Note

按下 Release Note 鈕，以取得目前系統版本之 Release Note。

重新啟動

按下按重新啟動鈕後，系統會彈出一新視窗，詢問是否重新啟動(Reboot)本系統。



序號

顯示本系統的產品序號。

版本

顯示系統目前運行的軟體版本。

系統時間

顯示系統時間。管理者可從「網路參數設定　系統時間」，自行修改設定。自行設定時間的詳細方法，請參考「網路參數設定」章節。

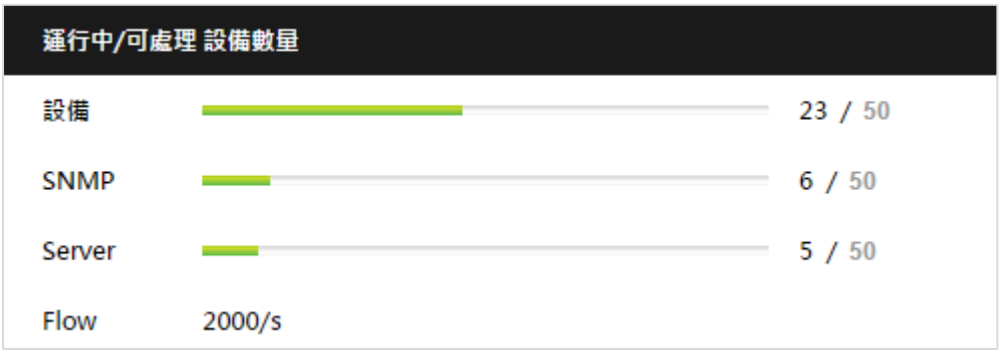
已啟動時間

顯示系統從啟動後至目前的時間。

License 有效期限

顯示本系統 License 到期日。若 License 到期，系統將無法更新版本以獲取新的功能，硬體保固也將暫時終止，建議使用者續購保固。如欲更新 License，請先跟本公司購買新 License。本公司提供 2 種更新 License 的方式：

運行中/可處理設備數量



■ **設備**：顯示本系統運行中及可處理之設備數量。

(1) 運行中設備數量，顯示目前系統處理中的 Syslog 設備總數(設備狀態設定為「暫停接收」 的設備，並不計算於此數值)。

(2) 可處理設備數量，顯示系統可接收 Syslog 資料的設備總數，預設值為 5(標準型)或 10(雙備援電源機型)，若想增加可處理設備總數量，則需另購 License。

(3) 設備接收狀態設定，請參考「設備管理➔Syslog 設備」章節。

Action ■ **SNMP**：顯示本系統運行中及可處理之 Switch 與 Host 數量。

(1) 運行中 SNMP 監控設備數量，顯示目前系統管理中的 Switch 與 Host 設備總數。

(2) 可處理 SNMP 監控設備數量，顯示系統可管理的 Switch 與 Host 總數，預設值為 10，若想增加可處理 Switch 與 Host 總數，則需另購 License。

(3) Switch 與 Host 管理設定，請參考「設備管理➔Switch 與 Host」章節。

Server ■ **Server**：顯示本系統運行中及可處理之 Server 數量。

(1) 運行中 Server 數量，顯示目前系統處理中的 Server 設備總數(設備狀態設定為「暫停接收」 的設備，並不計算於此數值)。

(2) 可處理 Server 數量，顯示系統接收 Server 資料的設備總數，若未購買 Server 模組，則所管理的 Server 總數會併入 Syslog 設備總數計算之。

(3) Server 模組所管理的設備種類包含主機類(Windows/Windows AD/Unix/Linux)、資料庫類(MSSQL/MySQL/Oracle/PostgreSQL)及 Application(Apache/IIS/Exchange/Mail Server 等)。

(4) 設備的資料格式設定及接收狀態，詳細設定請參考「設備管理➔Syslog 設備」章節。

Flow

■ **Flow**：顯示系統可處理的 Flow 速限(flow/sec)，不同版本的 Flow Module 可處理不同級距的 Flow 資料。

燈號

正常：此燈號代表設備狀況正常

警示：出現此燈號代表設備硬體裝置發生問題，請聯絡 N-Partner 或代理商以進行檢修。

無法提供監控：出現此燈號代表此硬體裝置在設備上不存在或無法進行監控，如在虛擬機(Virtual Machine, VM)上，風扇等設備將無法進行監控。

硬碟狀態	風扇	CPU溫度
System Disk	Fan1	
	Fan2	
	Fan3	

硬碟狀態

顯示目前系統磁碟的運作狀態，磁碟運作正常時顯示綠色燈號，磁碟無法正常驅動時將以紅色燈號警示，並發送 E-mail 給所有系統管理者，請儘速處理以避免資料流失。磁碟列表說明如下：

■ System Disk：系統設定所在磁碟，若未啟動 Syslog NFS 時，亦同時存放 Syslog 資料。

■ Extend Disk1/Disk2/Disk3：目前系統上所擴展的磁碟。

風扇

顯示目前系統風扇的運作狀態，運作正常時顯示綠色燈號，無法提供監控資訊則顯示灰色燈號，無法正常運作時將以紅色燈號警示，並發送 E-mail 給所有系統管理者，若此問題持續發生請聯繫代理商或原廠處理。

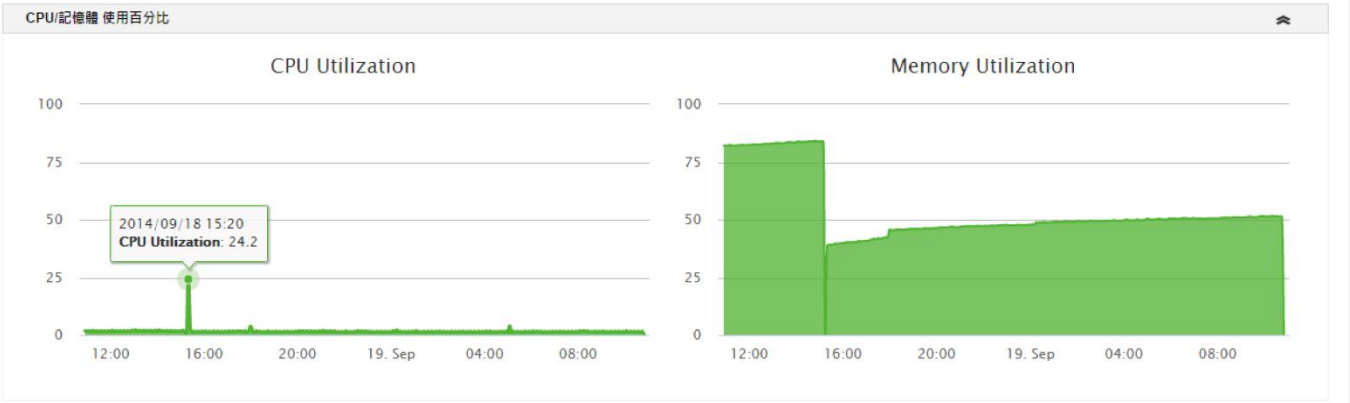
CPU 溫度

顯示系統/處理器核心溫度狀態。目前系統採用四核心處理器，溫度正常時顯示綠色燈號，溫度異常時將以紅色燈號警示，若發現系統長時間處於異常狀態而無法改善時，請聯繫代理商或原廠處理。

查詢時間區段

如下圖，選擇一時間區段，按下啟動查詢鈕，可查閱該時段的「CPU/記憶體使用百分比」、「Syslog 接收量 / 秒」、「Traffic 接收量/秒」及「Flow 接收量/秒」。

CPU/記憶體使用百分比

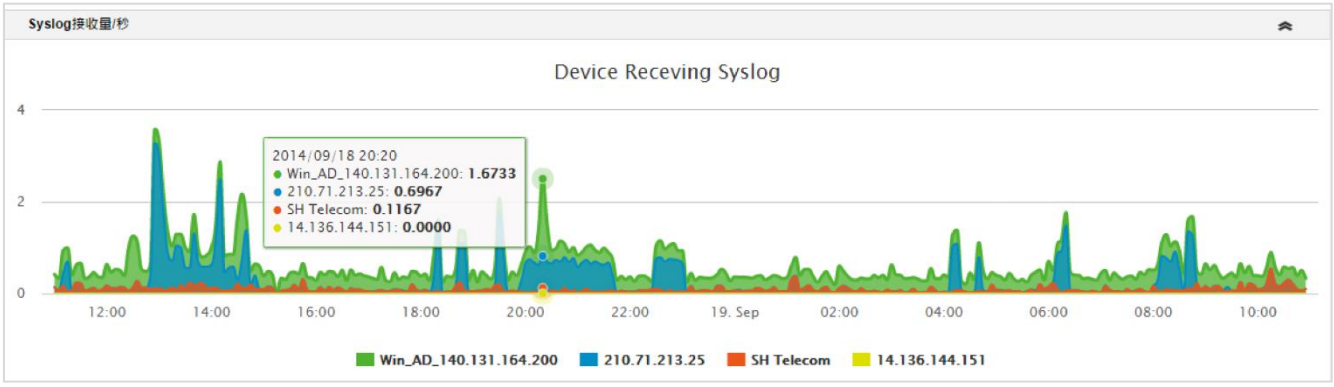


以圖示呈現系統的 CPU 與記憶體使用率。將滑鼠移至 CPU 使用率圖表之特定點(如上圖指標所指處)，系統會顯示事件發生的精確時間及使用率。

將滑鼠移至記憶體使用率圖表之特定點，系統會顯示事件發生的精確時間及使用率。

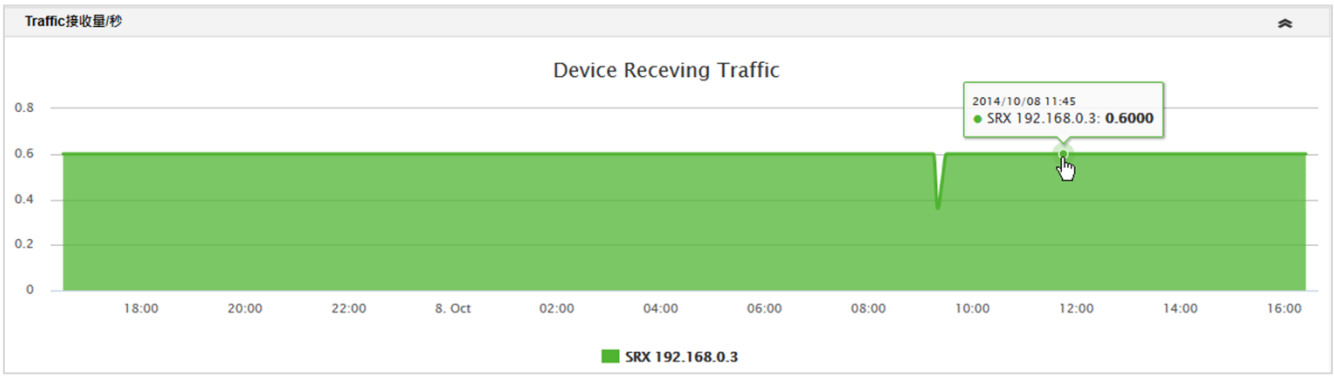
為了提供更好的資料收取與運算查詢效能，N-Reporter 會在開機後把所有的記憶體全都充份利用，記憶體使用率畫面看起來都是滿載，屬正常運作不會影響系統效能。

Syslog 接收量 / 秒



以圖示呈現來自各 Syslog 設備的資料接收量分時量表，以秒為單位，並顯示累計 24 小時的 Syslog 接收總筆數。將滑鼠移至 Syslog 接收量圖表之特定點(如上圖滑鼠指標所指處)，系統會顯示設備名稱、每秒接收量/總量及時間。

Traffic 接收量 / 秒

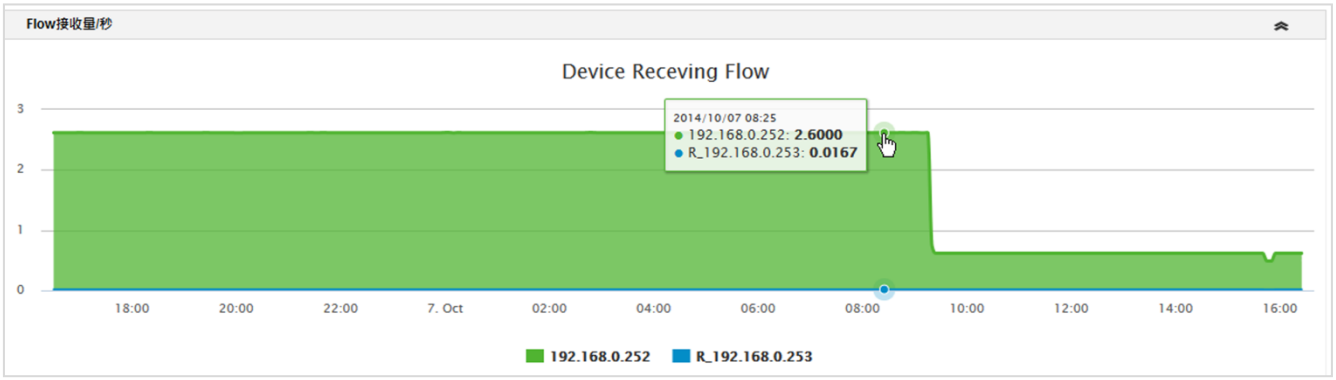


以圖示呈現來自各 Syslog Traffic 設備的資料接收量分時量表，以秒為單位，並顯示累計 24 小時的 Traffic 接收

總筆數。若未購買 Flow 模組，預設 Traffic 限速 500 筆/秒。將滑鼠移至 Traffic 接收量圖表之特定點(如上圖滑鼠指標所指處)，系統會顯示設備 IP、每秒接收量及時間。

Flow

Flow 接收量 / 秒



以圖示呈現來自各 Flow 設備的資料接收量分時量表，以秒為單位，並顯示累計 24 小時的 Flow 接收總筆數。將滑鼠移至 Flow 接收量圖表之特定點(如上圖滑鼠指標所指處)，系統會顯示設備 IP、時間及每秒接收量。

1.2 網路參數設定

此選項的功能主要在於設定「系統時間」、「IP 設定」、「Syslog 轉發」、「Flow 接收 Port」、「Flow 轉發」、「設定 Access List」及「Open Interface」等相關設定。點選「網路參數設定」選項。

系統時間

顯示目前系統時間，系統時間更改的方式:

- 同步電腦時間：按下 同步電腦時間 鈕，執行儲存當前使用者電腦的時間。
- 使用手動設定：管理者可自行輸入日期、時間、時區。
- 使用 NTP：採用 NTP(Network Time Protocol)對時方式，請輸入 NTP 時間伺服器位址。

IP 設定

設定相關 IP 參數。按下 確定 鈕，以儲存相關設定。基本參數說明如下：

- 管理 IP：設定系統的管理 IP。
- 子網路遮罩：設定系統管理 IP 的子網路遮罩。
- 預設閘道：設定系統管理 IP 的預設閘道。
- 主要 DNS：設定系統的主要 DNS。
- 次要 DNS：設定系統的次要 DNS(非必要選項)。
- Proxy 伺服器 : 如需透過 Proxy 才能連上 Internet，請設定 Proxy 伺服器的 IP 與服務 Port (非必要選項)。
- Proxy 認證帳號密碼：上述 Proxy 伺服器如需認證，請設定其帳號與密碼 (非必要選項)。

Syslog 轉發

N-Reporter 能將收到的 Syslog Raw Data 轉發

- 轉發來源：可指定只轉發某一部設備的 Syslog，或是選擇 Any 轉發所有收到的 Syslog。
- Syslog 伺服器 IP：輸入欲轉發的 Syslog 伺服器 IP 後，按下+鈕，即將此 IP 加入轉發伺服器列表。
- 轉發伺服器列表：點選「轉發伺服器列表」中任一 IP 後，按下移除鈕，即可刪除轉發某部 Syslog 伺服器。系統目前最多只允許轉發 16 部 Syslog 伺服器。
- Syslog Traffic 不論是否申裝 Flow Module，都將以 Syslog 方式轉發。

Flow

Flow 接收 Port

設定系統接收 Flow 的 Port Number。

- Port：輸入 Port 後，按下+鈕，即將此 Port 加入接收 Port 列表。

- 接收 Port 列表：點選「接收 Port 列表」中任一 Port 後，按下移除鈕，即可刪除該 Port。

  (N-Reporter 若會同時接收多台 Flow 設備時，可使用不同的 Port 來接收。)

- 當系統有設定「Flow 接收 Port」時，系統將切換為 Flow 模式，開始接收傳送來的 Netflow(v5/v9)/sFlow/Jflow，並進行 Flow 資料與資安 Syslog 交叉比對，以依據 Flow 資料產生「Flow 專屬報表」。

  (系統在切換 Flow 與 Syslog Traffic 接收模式時，即首次新增 Flow Port 及清空 Flow Port 設定時將重新啟動系統)

- 當未設定任何「Flow 接收 Port」時，系統則切換為 Syslog Traffic 模式(系統預設)，並採用 Traffic 資料與資安 Syslog 進行交叉比對及產生「Flow 專屬報表」。

Flow

Flow 轉發

N-Reporter 能將收到的 Flow Raw Data 轉發給其他 Flow Analyzer。

- 轉發來源：可指定只轉發某一部 Flow 設備所送出的 Flow packet，也可指定 Any 將所有收到的 Flow packet 進行轉發。
- Flow 伺服器 IP/Flow 伺服器 Port：輸入欲轉發的 Flow Analyzer IP 與 Port 後，按下+鈕即加入轉發伺服器列表。
- 轉發伺服器列表：點選「轉發伺服器列表」中任一項目後，按下移除鈕，即可刪除轉發此部 Flow Analyzer。系統目前最多只允許轉發 16 部 Flow Analyzer。

設定 Access List

Access List(ACL)用來限制可以連接到 N-Reporter 的網段。設定完成後，按下儲存設定鈕，系統將套用您設定可允許存取之網段並啟動 ACL 機制。

- 單一 IP 或網段：輸入要加入 Access List 的 IP 或網段，如：192.168.100.0/24，按下+鈕，即加入允許存取網段列表。
- 允許存取網段列表：點選「允許存取網段列表」中任一網段後，按下移除鈕，即可刪除該網段。

  錯誤的設定允許存取網段列表(ACL)將造成無法正常連線至 N-Reporter，請謹慎設定！若 Syslog 或 Flow 無法正常導入 N-Reporter，請確認是否已將 Syslog/Flow 設備網段加入 ACL！

Open Interface

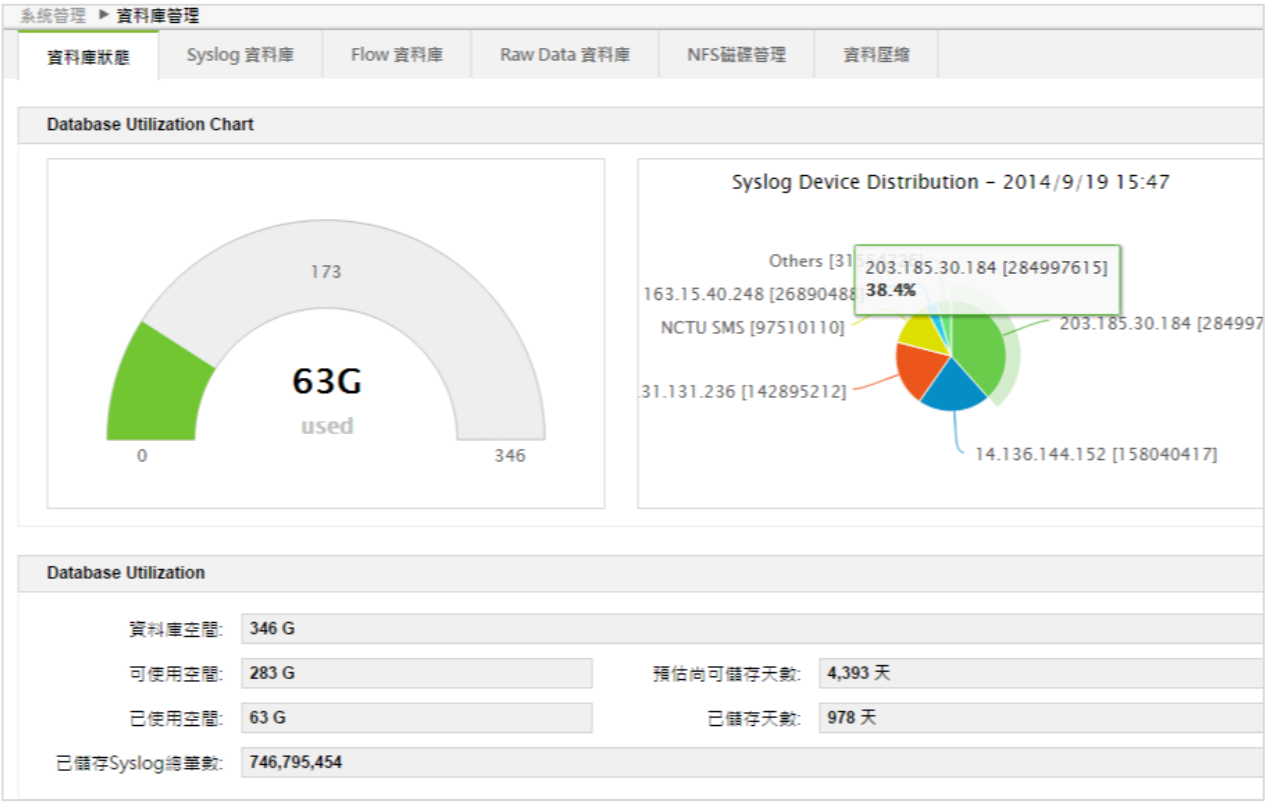
N-Reporter 允許使用者透過 Open Interface 介面批次取得所接受到的資料。關於 Open Interface 的詳細資訊，請參考 N-Reporter_OpenInterface 說明。

使用者在使用 Open Interface 查詢資料之前，必須先將欲連線查詢的 IP 加入許可列表，此 IP 才被允許查詢批次資料。各欄位說明如下:

- 單一 IP 或網段：輸入要加入的 IP 或網段，如：192.168.100.0/24，按下+鈕，即加入網段列表。
- 網段列表：點選「網段列表」中任一網段後，按下移除鈕，即可刪除該網段。

1.3 資料庫管理

此選項的功能主要在於顯示資料庫狀態、資料磁碟使用狀態及設定資料庫備份、資料庫回復、NFS 磁碟管理及資料壓縮等。點選「資料庫管理」選項。



資料庫狀態

顯示系統的資料庫使用狀況。

Database Utilization

顯示系統的磁碟使用狀況(如上圖所示)。在未設定 Syslog NFS 時(系統預設)，Syslog 資料將放置於系統資料庫中，故資料庫狀態為系統資料庫與 Syslog 資料庫加總顯示。若已設定 Syslog NFS 磁碟，資料庫狀態僅顯示 N-Reporter 系統資料庫使用狀態，所有項目皆不包含 Syslog 資料。

項目說明：

(1) 資料庫空間：系統儲存 Syslog 資料的硬碟空間大小。

(2) 可使用空間：儲存 Syslog 資料硬碟的尚可使用空間大小。

(3) 已使用空間：儲存 Syslog 資料硬碟的已使用空間大小。

(4) 預估尚可儲存天數：根據過去 Syslog Raw Data 接收速率來預估系統剩餘硬碟空間尚可儲存的天數。

(5) 已儲存天數：在系統開始運作後，截至目前為止已儲存的天數。

(6) 已儲存 Syslog 總筆數：目前系統已儲存的 Syslog 總筆數。

(7) Syslog Device Distribution：系統依各 Syslog 設備所佔用的 Syslog 資料筆數顯示比例分布圖。將滑鼠移至圖表之特定區塊，畫面會顯示設備名稱(或 IP)、資料筆數、及百分比。

Flow ■ 資料磁碟 / NFS 磁碟

顯示資料磁碟使用狀況(如上圖所示)，在購買 Flow Lite/Advance/Unlimited 模組時，會將所收到的 Flow 或防火牆所產生的 Syslog Traffic 放置於 Flow 磁碟中。若設定 NFS 後，N-Reporter 將 Flow 資料轉換為使用外部 NFS 磁碟，將顯示為 NFS 磁碟，所有的操作也將改為針對外接的 NFS 磁碟。

項目說明：

(1) 已使用空間：儲存 Flow 資料硬碟的已使用空間大小。

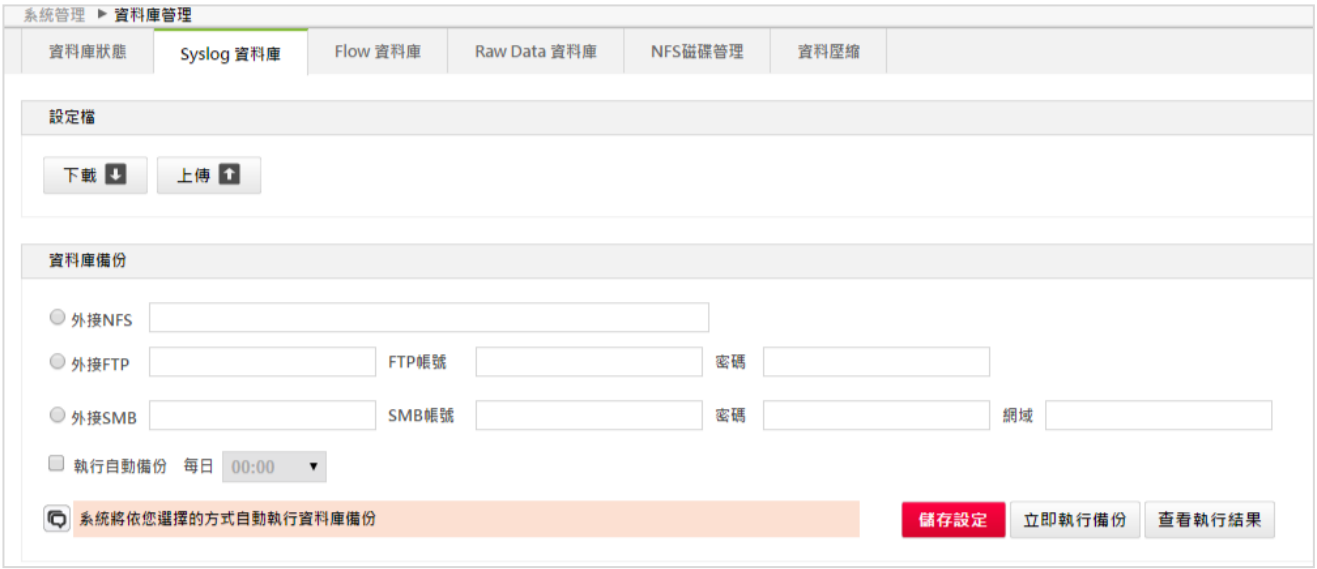
(2) 可使用空間：儲存 Flow 資料硬碟的尚可使用空間大小。

(3) 所有空間：系統儲存 Flow 資料的硬碟空間大小。

(4) 已存儲天數：從最早第一筆 Flow 資料計算至目前為止已儲存的天數。

(5) 預估尚可儲存天數：根據過去 Flow 接收速率來預估系統剩餘硬碟空間尚可儲存的天數。

Syslog 資料庫



N-Reporter 提供 Syslog 資料庫(包含系統資料庫)自動每日備份、回復、資料移除及設定檔上傳下載的功能(如上圖所示)。

■ 設定檔：可以把系統設定檔下載至個人電腦，或是將儲存於個人電腦上的備份設定檔還原至系統。

(1) 下載：可下載系統資料庫的設定檔，點下「下載」按鈕後將下載本系統設定檔。

(2) 上傳：可上傳資料庫設定檔至系統 (請注意檔案名稱應為 cfg.npdb)。

在按下「下載」按鈕後，請等待系統進行設定檔的整理及產生，完成後將會進行下載的動作；此過程所需耗費的時間，依設定及報表資料數量或是下載速率所影響將會有所變化，請務必耐心等待下載過程完成，勿重覆按押「下載」按鈕，以避免因此造成下載過程發生錯誤。若兩人以上同時登入本系統，也請勿同時進行下載動作，以避免發生錯誤。

■ 資料庫備份：

建議 Syslog 資料庫與 Flow 資料庫的備份路徑不要相同，以避免資料雜亂維護不易。

系統提供三種備份資料庫的方式。

(1) 外接 NFS：將系統資料(包含系統設定值、接收設備、已儲存查詢條件、已儲存報表、Syslog 資料表等)備份到外部 NFS(如：192.168.1.1:/home/nfs/backup)，依此例之目錄(掛接目的目錄)為例，「/home/nfs/backup」需要可進行「讀/寫」的權限，否則將會造成寫入失敗。

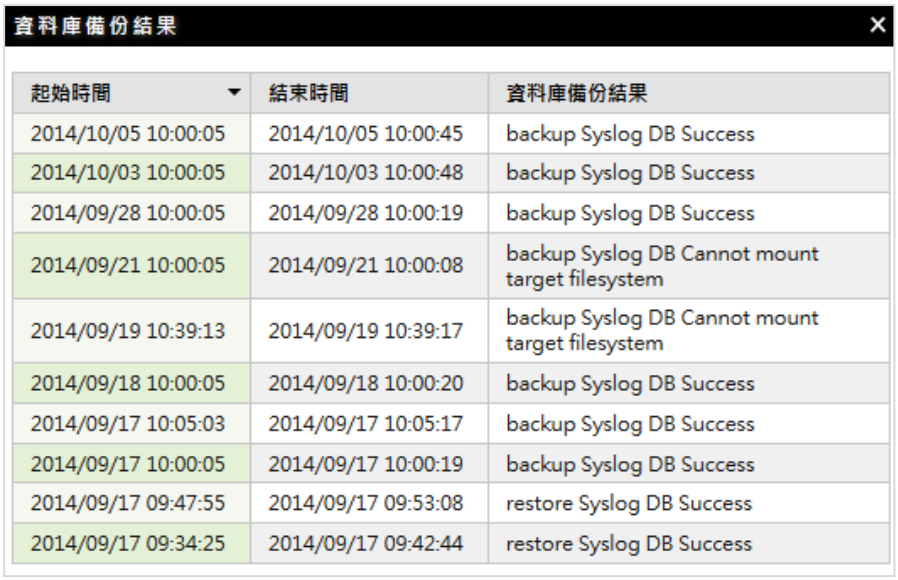
(2) 外接 FTP：將系統資料(包含系統設定值、接收設備、已儲存查詢條件、已儲存報表、Syslog 資料表等)備份到外部 FTP(File Transfer Protocol)協定空間。請輸入 FTP 的 FQDN/IP 及認證相關的帳號與密碼，此外請務必確認該用戶有讀取及寫入該 FTP Server 的權限，以避免寫入失敗。

(3) 外接 SMB：將系統資料(包含系統設定值、接收設備、已儲存查詢條件、已儲存報表、Syslog 資料表等)備份到外部 SMB(Server Message Block)協定空間。請輸入 SMB 的 FQDN/IP，若需帳號及密碼做認證，請輸入認證相關帳號、密碼與網域。(如：//192.168.1.1/public)。依此例之目錄(掛接目的目錄)為例，「/public」需要該指定用戶可進行「讀/寫」的權限，否則將會造成寫入失敗。

設定完成後，請按下儲存設定鈕，系統會儲存您所選定的備份方式及設定值。按下立即執行備份鈕，系統則會依據所選定的方式立即執行備份。按下查看執行結果鈕，系統會彈出資料庫備份結果視窗(如下圖)。

除了立即備份外，系統亦提供自動備份方式，供管理者做備份排程。

勾選「執行自動備份」，並選擇每日備份時間，系統將於每日所選定的時間(如 00:00)及所選定的備份方式，進行資料差異性備份。



由於 N-Reporter 採用差異性備份方式，所以第一次備份的執行時間可能稍長，請耐心等候。

■ 資料庫回復：N-Reporter 提供 Syslog 資料庫(包含系統資料庫)的功能，系統在資料庫回復完成後會重新啟動系統。系統提供三種回復資料庫的方式。

恢復備份的型式以目錄為單位，無法以單一檔案的方式選擇及回復。

(1) **從 NFS 導入：**從外部 NFS 回復系統資料備份檔 (如：192.168.1.1:/home/nfs/backup)，依此例之目錄(掛接目的目錄)為例，「/home/nfs/backup」需要可進行「讀/寫」的權限，否則將會造成讀取失敗。

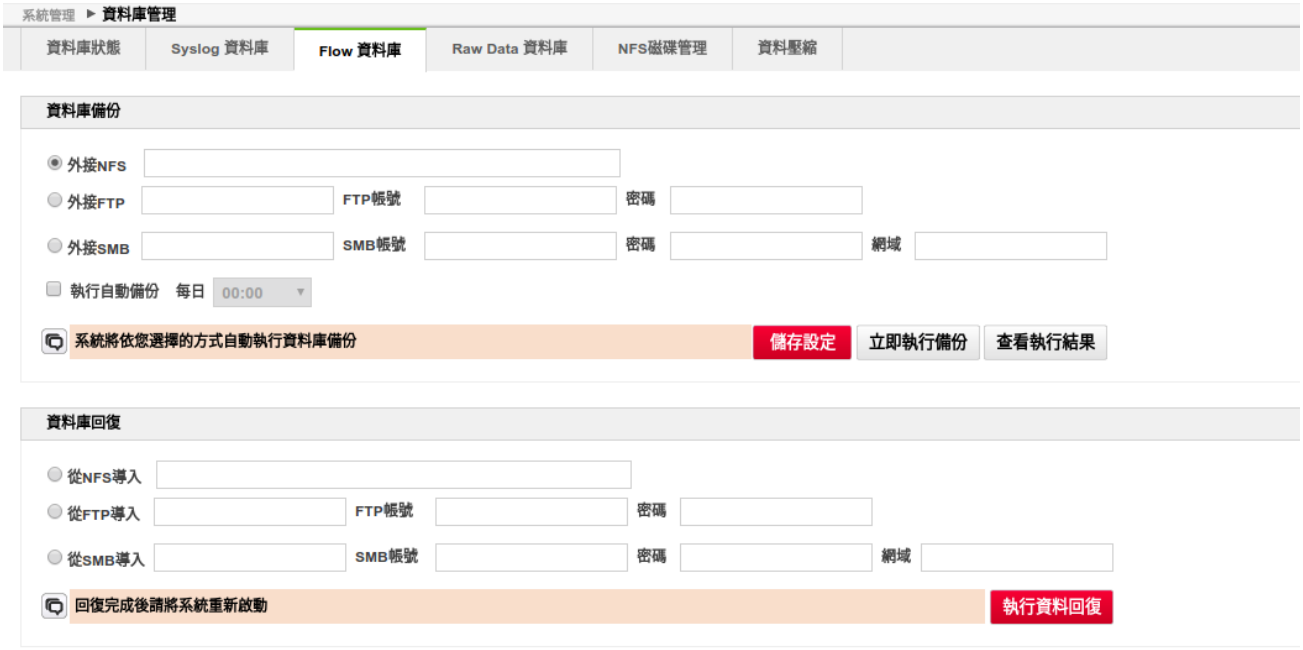
(2) **從 FTP 導入：**從外部 FTP 回復資料庫資料。請輸入 FTP 的 FQDN/IP 及認證相關的帳號與密碼，此外請務必確認該用戶有讀取及寫入該 FTP Server 的權限，以避免讀取失敗。

(3) **從 SMB 導入：**從外部 SMB 回復資料庫資料(如：//192.168.1.1/public)。請輸入 SMB 的 FQDN/IP，若需帳號及密碼做認證，請輸入認證相關帳號、密碼與網域(如：//192.168.1.1/public)。依此例之目錄(掛接目的目錄)為例，「/public」需要該指定用戶可進行「讀/寫」的權限，否則將會造成讀取失敗。

■ 選擇好資料庫回復方式後，按執行資料回復鈕，系統將執行資料庫回復作業。

Flow 資料庫

N-Reporter 提供 Flow 資料庫自動每日備份、回復及資料移除的功能。



- 資料庫備份：Flow 資料庫由於資料量大，約為 Syslog 資料量的數十倍到數百倍，執行備份前請您先確認儲存的空間是否足夠。建議 Syslog 資料庫與 Flow 資料庫的備份路徑不要相同，以避免資料雜亂維護不易。

  系統提供下列三種備份資料庫方式:

  (1) **外接 NFS**：將 Flow 資料備份到外部 NFS(如：192.168.1.1:/home/nfs/backup) ，依此例之目錄(掛接目的目錄)為例，「/home/nfs/backup」需要可進行「讀/寫」的權限，否則將會造成寫入失敗。

  (2) **外接 FTP**:將 Flow 資料備份到外部 FTP(File Transfer Protocol)協定空間。請輸入 FTP FTP 的 FQDN/IP 及認證相關的帳號與密碼，此外請務必確認該用戶有讀取及寫入該 FTP Server 的權限，以避免寫入失敗。

  (3) **外接 SMB**:將 Flow 資料備份到外部 SMB(Server Message Block)協定空間。請輸入 SMB 的 FQDN/IP，若需帳號及密碼做認證，請輸入認證相關帳號、密碼與網域(如：//192.168.1.1/public)。依此例之目錄(掛接目的目錄)為例，「/public」需要該指定用戶可進行「讀/寫」的權限，否則將會造成寫入失敗。

  設定完成後，請按下 儲存設定 鈕，系統會儲存您所選定的備份方式及設定值。按下 立即執行備份鈕，系統則會依據所選定的方式立即執行備份。按下 查看執行結果 鈕，系統會彈出資料庫備份結果視窗。

  除了立即備份外，系統亦提供自動備份方式，供管理者做備份排程。勾選「執行自動備份」(如上圖箭頭所示)，並選擇每日備份時間，系統將於每日所選定的時間(如 00:00)及所選定的備份方式，進行資料差異性備份。

由於 N-Reporter 採用差異性備份方式，所以第一次備份的執行時間可能稍長，請耐心等候。

■ 資料庫回復：N-Reporter 提供 Flow 資料庫回復的功能。

系統提供三種回復資料庫的方式。

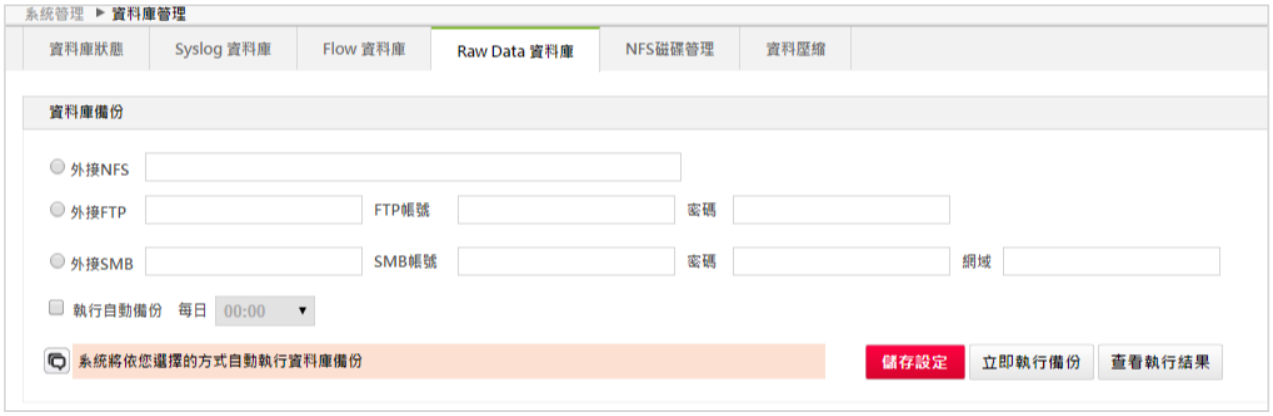
(1) **從 NFS 導入：**從外部 NFS 回復 Flow 資料(如：192.168.1.1:/home/nfs/ backup) ，依此例之目錄(掛接目的目錄)為例，「/home/nfs/backup」需要可進行「讀/寫」的權限，否則將會造成讀取失敗。

(2) **從 FTP 導入：**從外部 FTP 回復 Flow 資料。若需帳號及密碼做認證，請輸入 FTP FTP 的 FQDN/IP 及認證相關的帳號與密碼，此外請務必確認該用戶有讀取及寫入該 FTP Server 的權限，以避免讀取失敗。

(3) **從 SMB 導入：**從外部 SMB 回復 Flow 資料(如：//192.168.1.1/public)。若需帳號及密碼做認證，請輸入 SMB 的 FQDN/IP 及認證相關帳號、密碼與網域(如：//192.168.1.1/public)。依此例之目錄(掛接目的目錄)為例，「/public」需要該指定用戶可進行「讀/寫」的權限，否則將會造成讀取失敗。

■ 選擇好資料庫回復方式後，按執行資料回復鈕，系統將執行資料庫回復作業。

Raw Data 資料庫



■ 資料庫備份：

系統提供三種備份資料庫方式。建議與 Syslog 及 Flow 資料庫的備份路徑不要相同，避免資料雜亂維護不易。

(1) 外接 NFS：將 Raw Data 資料備份到外部 NFS(如：192.168.1.1:/home/nfs/backup)。依此例之目錄(掛接目的目錄)為例，「/home/nfs/backup」需要可進行「讀/寫」的權限，否則將會造成寫入失敗。

(2) 外接 FTP：將 Raw Data 資料備份到外部 FTP(File Transfer Protocol)協定空間。請輸入 FTP FTP 的 FQDN/IP 及認證相關的帳號與密碼，此外請務必確認該用戶有讀取及寫入該 FTP Server 的權限，以避免寫入失敗。

(3) 外接 SMB：將 Raw Data 資料備份到外部 SMB(Server Message Block)協定空間。請輸入 SMB 的 FQDN/IP，若需帳號及密碼做認證，請輸入認證相關帳號、密碼與網域(如：//192.168.1.1/public)。依此例之目錄(掛接目的目錄)為例，「/public」需要該指定用戶可進行「讀/寫」的權限，否則將會造成寫入失敗。

■ 設定完成後，請按下 儲存設定 鈕，系統會儲存您所選定的備份方式及設定值。按下 立即執行備份鈕，系統則會依據所選定的方式立即執行備份。

NFS 磁碟管理

■ NFS 磁碟管理

設定「外部磁碟分割區 1」或「外部磁碟分割區 2」啟用外接 NFS 磁碟，可享有 NFS 磁碟在資料可靠性及效能上的優勢。勾選及設定完成後，按下「儲存設定」鈕，將儲存相關設定並進行寫入模式切換，此時系統將重新啟動。取消勾選將停用「外部磁碟分割區 1」或「外部磁碟分割區 2」外接 NFS 磁碟(請注意兩者磁碟分割區不可重覆)。請注意，所設定之 NFS 磁碟，需要可進行「讀/寫」的權限，否則將會造成寫入或讀取失敗。

在設定採用或取消 NFS 磁碟時會有資料丟失疑慮，原有的資料將不會隨設定搬移，如有保留資料需求請先執行資料庫備份再還原。

資料壓縮

此頁面提供資料壓縮設定，若想在 N-Reporter 儲存大量資料，可勾選啟動資料壓縮後並輸入壓縮天數 (壓縮超過幾天前的資料，建議值 30 天)，按下儲存設定鈕後，系統將自動壓縮 30 天前的資料。N-Reporter 提供的壓縮技術，其壓縮比高達 8~12 倍，可大幅度地提升儲存空間的使用率，且不影響資料查詢。

1.4 使用者管理

此選項的功能主要在於管理(新增、刪除、編輯)使用者、及列表使用者資訊。

使用者列表

顯示目前系統所有使用者相關資訊。點選列表表頭任一項目標題，系統會根據該項目進行遞增排序與遞減排序

列表欄位說明如下：

- 登入帳號：為該使用者用來登入 N-Reporter 的使用者帳號。
- 使用者名 / 使用者姓：顯示該使用者姓名。
- 權限：分成「管理者」與「一般使用者」。管理者可以進行所有的操作；一般使用者僅能查詢事件與報表。
- 帳號狀態：分成「啟用」與「停用」。呈現「停用」的使用者將無法登入 N-Reporter。
- 連線狀態：呈現「On-line」的使用者表示目前正連線到 N-Reporter 進行操作中；呈現「Off-line」的使用者表示目前離線。
- 最近一次登入位址：顯示該使用者最近一次登入系統時的 IP 位址。
- 最近一次登入時間：顯示該使用者最近一次登入系統的時間。

按鈕操作

按下  按鈕，彈出使用者資訊視窗(如下圖)，請依序填入「登入帳號」、「登入密碼」、「確認密碼」、「使用者名」、「使用者姓」、「電子郵件地址」、「手機號碼」(非必要選項)及「選擇使用者語系」(目前提供 English、簡體中文、繁體中文三種語系)，並設定「權限」與「帳號狀態」後，按 確定 執行新增作業 (「電子郵件地址」需為唯一，不可與其他使用者重複)。

若欲修改使用者相關資訊，請在使用者列表「操作」欄位，點擊欲修改帳號圖示，系統會彈出同上圖視窗，供管理者編輯所選使用者帳號相關資訊。若欲刪除使用者帳號，則點擊刪除圖示，系統則會刪除該使用者帳號。

管理者亦可在使用者列表上點擊右鍵，彈出右鍵功能選單(如下圖)，供管理者新增、編輯、刪除所選使用者帳號相關資訊。

1.5 IP 名稱解析

為方便使用者辨識事件與報表資料中的 IP 位址，N-Reporter 支援「IP 名稱解析」的方式直接顯示 IP 所屬的網段名稱，在 IP 難以閱讀的 IPv6 的環境中更是一目瞭然。使用者依已知的 IP 網段資訊建立「IP 名稱解析」對應之後，除了呈現更加可讀的名稱之外，也可直接當作 IP 過濾條件使用，也能做為分析最小單位使用。

名稱解析列表

操作	網段名稱	網段定義	Flow	數值低於下列門檻將不觸發告警		觸發率(%)		數值低於下列bps門檻觸發告警		最近修改時間
				pps	bps	pps	bps	in	out	
	Home	192.168.0.0/16,10.0.0.0/8,172.16.0.0/12	啟動	10	50 M	500	600	1 M	1 M	2016/06/30 11:16:11
	IPV 6 test	2001:288:33A9::	啟動	10	50 K	500	600			2016/07/20 11:12:40
	業務部門	192.168.4.0/24	關閉							2016/06/30 11:18:59
	技術部門	192.168.3.0/24	啟動	10	50 K	500	600	1 M	1 M	2016/07/26 16:22:08

列表欄位說明如下：

- 網段名稱：顯示名稱解析對應中的名稱部分。
- 網段定義：顯示該名稱所代表的 IP 群。

Flow

- Flow：顯示系統是否針對該名稱所代表的 IP 群進行流量分析，啟動包含「Flow 專屬報表」中的各種報表及分析，如「流量報表」、「Protocol」、「封包大小分析」、「交叉分析」、「Flow Top N 報表」及「網段流量異常告警」等。

Flow

- 數值低於下列門檻值將不觸發告警：告警觸發的安全值設定，意即 bps/pps 在低於此設定值時將不會觸發「網段流量異常告警」，就算是流量暴增百分比有超過，避免觸發流量太低的告警。

Flow

- 觸發率：動態偵測網段異常流量的觸發比率，當網段流量超過自動學習的門檻值達觸發率時將觸發「網段流量異常告警」。

Flow

- 數值低於下列 bps 門檻觸發告警：此為低量告警功能，意即流進或流出的量(bps)低於此設定值時將會觸發「網段流量異常告警」。
- 最近修改時間：顯示該筆名稱解析對應資料最近一次修改的時間。
- 「Home」名稱解析為出廠的 Default 設定，其意義在於讓系統了解使用者下轄網路裡的所有 IP，針對「Home」網段裡輸入正確且完整的下轄 IP 資料至為重要，系統會根據「Home」網段來區分是否為「內部網路」，錯誤的設定會嚴重影響多種分析與管理動作的正確性。「Home」名稱解析出廠時已內含三個 Private 網段：10.0.0.0/8、172.16.0.0/12、192.168.0.0/16，此名稱解析可以更改網段名稱與 IP 對應資料，但是不可刪除。

按鈕操作

在搜尋列可以輸入網段名稱或網段定義(全部或是部份) 來進行過濾，例如輸入 “人事 " 或是 “192.168.1.0 " 都可以找到人事部門的名稱解析設定。按下 按鈕，彈出名稱解析視窗(如下圖)。

- 網段名稱：請輸入一個容易辨識的名稱字串。
- 啟動 Flow 分析：勾選此選項 (系統預設選項) 表示要求系統針對此名稱所代表的 IP 群，自動進行 Flow 流量分析，所有的分析結果會呈現在「報表」➔「Flow 專屬報表」功能中。網段流量異常告警則是採用動態門檻值分析技術，系統會自動依據此網段過去的流量自動產生門檻值，使用者只要調整以下兩個參數就能增加告警準確度：

(1) 數值低於下列門檻將不觸發告警: 告警觸發的安全值設定，意即 bps/pps 在低於此設定值時將不會觸發「網段流量異常告警」，就算是流量暴增百分比有超過，避免觸發流量太低的告警。

(2) 觸發率: 動態偵測網段異常流量的觸發比率，當網段流量超過自動學習的門檻值達觸發率時將觸發「網段流量異常告警」。過低的觸發率將產生過多的告警，請依告警狀況數量調整觸發率。

數值低於下列 bps 門檻觸發告警：此為低量告警功能，意即流進或流出的量(bps)低於此設定值時將會觸發「網段流量異常告警」。

- 單一 IP 或網段：請輸入 CIRD 格式的 IP 條件，如：210.71.213.0/24。
- IP 範圍：請輸入 IP 區間之起始及結束 IP。
- 按下 鈕將上述 IP 條件加入條件列表中。一個名稱解析可加入多筆 IP 設定表示之(邏輯運算中的 OR)。

點選 IP 條件列表中的任一筆資料按下 鈕或 鈕，可以執行該筆 IP 條件的修改與刪除動作。

若欲修改名稱解析相關資訊，請在名稱解析列表「操作」欄位，點擊欲修改項目 圖示，系統會彈出同上圖視窗，供管理者編輯所選名稱解析相關資訊。若欲刪除名稱解析，則點擊 圖示，系統則會刪除該名稱解析。

管理者亦可在名稱解析列表上點擊右鍵，彈出右鍵功能選單，供管理者新增、編輯、刪除所選名稱解析相關資訊。

按下 鈕，系統會彈出「匯入」視窗，請按「瀏覽」指出要匯入的 CSV 檔案後，按 上傳 鈕可以執行名稱解析的批次匯入動作。匯入的 CSV 檔案內容需寫成多行的「名稱, 網段定義」，每行代表一組名稱解析；網段定義可為單一 IP、網段或是 IP 區段，多個網段間以「+」串接，

(如：DomainABC,10.1.1.0/24+10.1.2.100-10.2.2.200+1208:0A0C::AA05)。CSV 可由 Excel 產生，附檔名為 .csv，檔案大小限制為 1MB。若名稱解析的定義中包含中文，請確認將檔案的編碼選擇為 UTF-8 編碼。

按下 鈕，系統會彈出「匯入線上操作說明」視窗(如下圖所示)

■ 批次修改

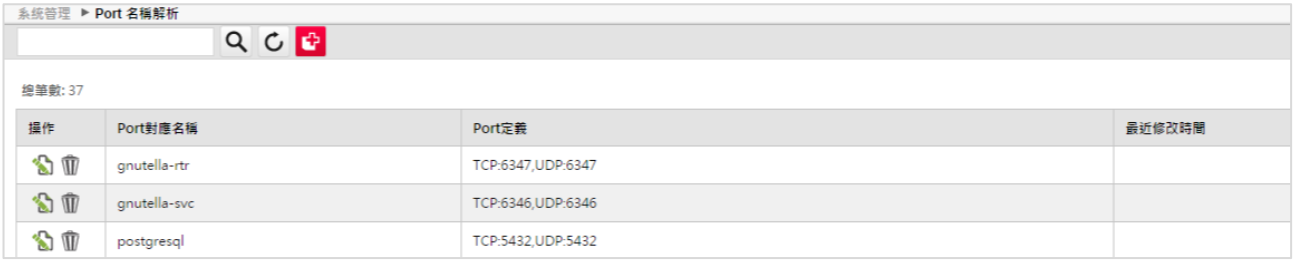
使用者可在一次選擇多個 IP 名稱解析(網段名稱)的情況下，批次修改 Flow 分析的相關設定。

此處相關數值的定義請參考前一節之說明，按下 確定 鈕後，系統即會針對所選擇之多個 IP 名稱解析(網段名稱)批次覆蓋舊有的 Flow 分析設定。

1.6 Port 名稱解析

此選項的功能主要在於做 Port 名稱解析管理。為方便使用者解讀及辨識事件與報表資料中的 Port，如 TCP:80 對應為 HTTP，N-Reporter 支援「名稱解析➔Port」對應方式。

在「事件」與「報表」功能中，使用者可以運用 Port 名稱解析作為「Port 過濾」的條件。



Port 名稱解析搜尋

提供字串搜尋功能，可輸入 Port(全部或是部份)或名稱作為查詢依據，按下搜尋鈕，執行搜尋。按下回復鈕，可以清除輸入的搜尋字串。

Port 名稱解析列表

顯示目前系統 Port 名稱解析相關資訊。

列表欄位說明如下：

- Port 對應名稱：顯示 Port 名稱解析對應中的名稱部分。
- Port 定義：顯示該名稱所代表的 Port 群。
- 最近修改時間：顯示該筆 Port 名稱解析對應資料最近一次修改的時間。

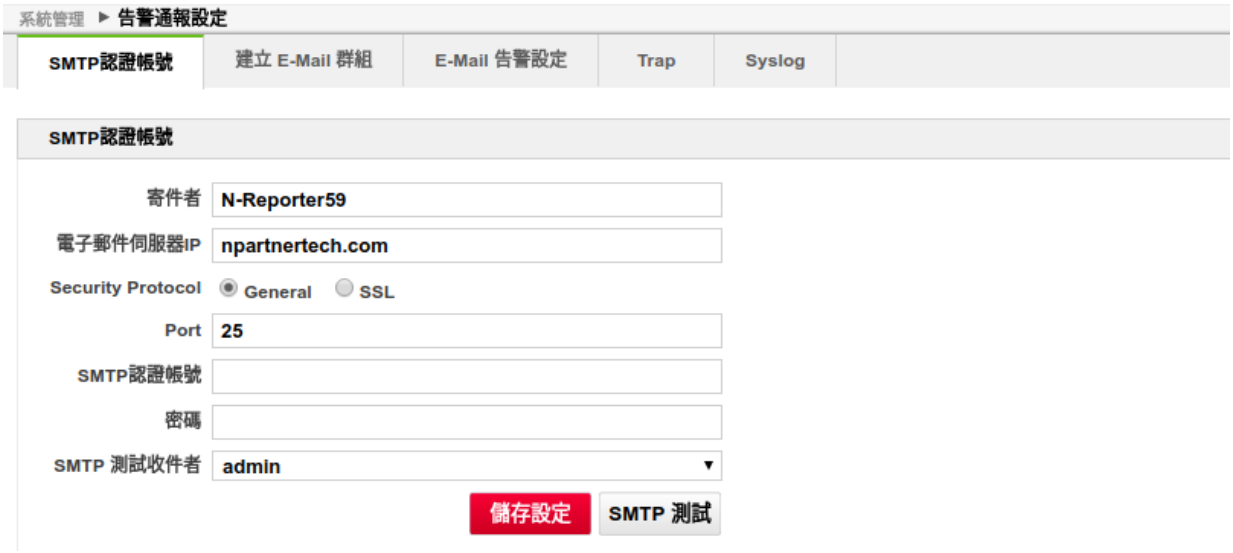
按鈕操作

按下  按鈕，彈出 Port 名稱解析視窗。「Port 對應名稱」中請輸入一個容易辨識的名稱字串；「協定」下拉選擇 TCP/UDP 或 Any；「Port」、「Port 區段」請輸入單一 Port 或是 Port 範圍。按下+鈕將上述 Port 條件加入條件列表中。一個 Port 名稱解析可加入多筆 Port 設定表示之(邏輯運算中的 OR)。點選 Port 條件列表中的任一筆資料按下編輯鈕或刪除鈕，可以執行該筆 Port 條件的修改與刪除動作。

若欲修改Port名稱解析相關資訊，請在Port名稱解析列表「操作」欄位，點擊欲修改項目編輯圖示，系統會彈出視窗，供管理者編輯所選 Port 名稱解析相關資訊。若欲刪除 Port 名稱解析，則點擊刪除圖示，系統則會刪除該 Port 名稱解析。

1.7 告警通報設定

此選項的功能主要在於設定「SMTP 認證帳號」、「建立 E-Mail 群組」及「E-Mail 告警設定」等相關設定。點選「系統通報設定」選項。



SMTP 認證帳號

設定 SMTP 相關參數。設定完成後請按下 儲存設定 鈕，以儲存相關設定。

參數說明如下：

- 寄件者：設定系統寄送電子郵件時所使用的寄件者電郵地址。
- 電子郵件伺服器 IP：設定系統寄送電子郵件時所使用的 SMTP 伺服器 IP 位址。
- Security Protocol：選用連線至電子郵件伺服器所需的連線加密方式，General 為一般無加密連線方式，SSL 為採用 SSL 加密的連線方式。
- Port：選用連線至電子郵件伺服器所需的連線傳輸 Port，一般為 Port 25，加密為 Port 465，請詢問電子郵件伺服器管理者以取得正確的連線傳輸 Port。
- SMTP 認證帳號 / 密碼：上述 SMTP 主機如需認證，請設定帳號與密碼(非必要選項)。
- SMTP 測試收件者：從下拉選項選定一系統使用者作為 SMTP 郵件測試的收件者。按下 **SMTP 設定** 鈕後，系統會寄送測試電子郵件到所選定的收件者信箱，用以確認上述設定與 SMTP 伺服器協同運作無誤。

建立 E-Mail 群組

設定 E-Mail 群組的作用在於方便以群組的方式管理收件人，有大量收件人需求時使用 E-Mail 群組進行分類，依單位之不同寄送相對應於該單位所重視的訊息，並確保同單位的人員都可收到通知。

操作說明如下：

- E-Mail 群組搜尋：提供字串搜尋功能，可輸入群組名稱或 E-mail(全部或是部份)作為查詢依據，按下

鈕，執行搜尋。按下 鈕，可以清除輸入的搜尋字串。

- E-Mail 群組列表：顯示 E-Mail 群組相關資訊，列表欄位說明如下：

(1) 群組名稱：顯示 E-Mail 群組對應中的名稱部分。

(2) 寄送 E-Mail 列表：顯示該名稱所代表的 E-Mail 群。

(3) 按鈕操作：建立報表或告警 E-Mail 收件群組。按下 鈕，彈出建立 E-Mail 群組視窗。

(a) 群組名稱：請輸入一個容易辨識的名稱；

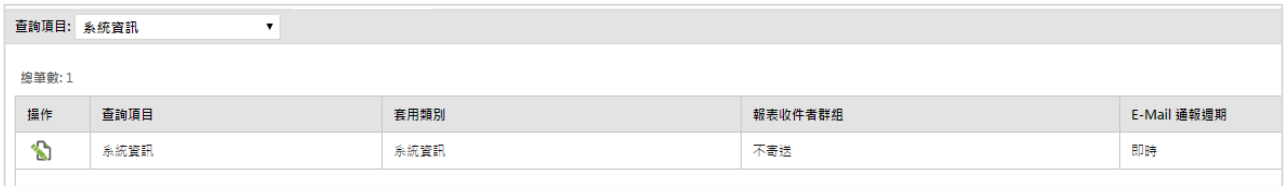
(b) 手動輸入 E-Mail：可手動輸入收件者 E-Mail；

(c) 選擇使用者：下拉式選項供使用者選取預先定義的使用者(請參考「系統管理➔使用者管理」章節)。

各欄位設定完後，按下+鈕，將使用者加入報表待寄送名單中。點選報表待寄送名單中的任一筆資料按下鈕，即可刪除寄送報表於該使用者。按下 確定 鈕完成 E-Mail 群組的建立動作。

若欲修改 E-Mail 群組相關資訊，請在 E-Mail 群組列表「操作」欄位，點擊欲修改項目 圖示，系統會彈出同上圖視窗，供管理者編輯所選 E-Mail 群組相關資訊。若欲刪除 E-Mail 群組，則點擊 圖示，系統則會刪除該 E-Mail 群組。

E-Mail 告警設定



- E-Mail 告警設定列表：顯示 E-Mail 群組相關資訊。
- 查詢項目：顯示目前所點選的查詢項目。
- 操作：查詢項目為「系統資訊」、「資料庫管理」、「設備異常告警」、「郵件異常告警」、「Security 事件即時異常告警」、「Flow 即時異常告警」、「網段流量異常告警」時，才可修改套用設定，其餘項

目只能查詢其 E-Mail 設定狀態。

- 套用類別/報表名稱：顯示目前被套用的類別或報表。
- 報表收件者群組：顯示該項目前套用的 E-Mail 群組。
- E-Mail 通報週期：顯示該項目通報的發送週期(Top N、伺服器稽核無通報週期)。
- 按鈕操作 : 當查詢項目為「系統資訊」、「資料庫管理」、「設備異常告警」、「郵件異常告警」、「Security 事件即時異常告警」、「Flow 即時異常告警」、「網段流量異常告警」時，若欲修改 E-Mail 套用設定，

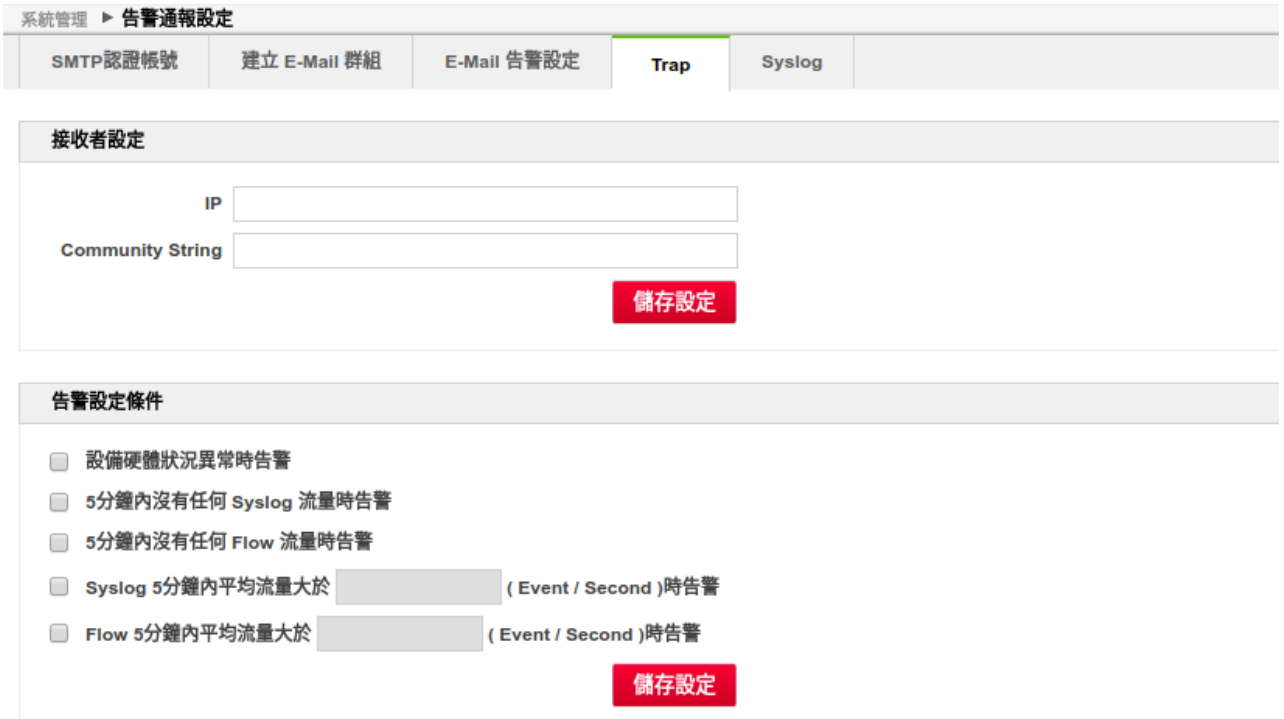
請在 E-Mail 套用列表「操作」欄位，點擊欲修改項目  圖示，系統會彈出套用 E-Mail 設定視窗(如下圖)。

(a) 報表收件者群組：下拉式選項供使用者選取預先定義的 E-Mail 群組。(請參考「系統管理➔系統通報設定➔建立 E-Mail 群組」章節)

(b) E-Mail 通報週期：選擇通報的發送週期(「系統資訊」及「資料庫管理」通報週期為即時，不可變更)。

Trap

Trap 是當指定的系統事件發生時，利用 SNMP Trap 技術進行通報的功能，在設定完接收者之後並選擇欲進行通報的事件後，在選定事件發生時，即可於接收者方收到 trap 通知。



■ 接收者設定：設定 Trap 接收者訊息，以發送 Trap 通報。

IP: 請輸入接收者 IP/FQDN，供系統發送 Trap，請注意，該設定之 IP 需有接收 SNMP Trap 的功能。

Community String：請輸入接收者指定之 Community String。請注意，若 Community String 設定錯誤，發送之 trap 訊息將被接收者直接丟棄。

若欲清除設定時，請清空設置並按下儲存設定鈕即可。

■ 告警設定條件：以下告警條件可供勾選並進行設置閥值。

設備硬體狀況異常告警：當本系統之硬體發生狀況時，即進行通報。

5 分鐘內沒有任何 Syslog 流量時告警：5 分鐘內皆未收到 Syslog 時，即進行通報。

5 分鐘內沒有任何 Flow 流量時告警：5 分鐘內皆未收到 Flow 時，即進行通報。

Syslog 5 分鐘內平均流量大於指定閥值(Event / Second)時告警：5 分鐘內收到超過閥值指定之 Syslog Event/Second 時，即進行通報。

Flow 5 分鐘內平均流量大於 指定閥值(Event / Second)時告警：5 分鐘內收到超過閥值指定之 Flow Event/Second 時，即進行通報。

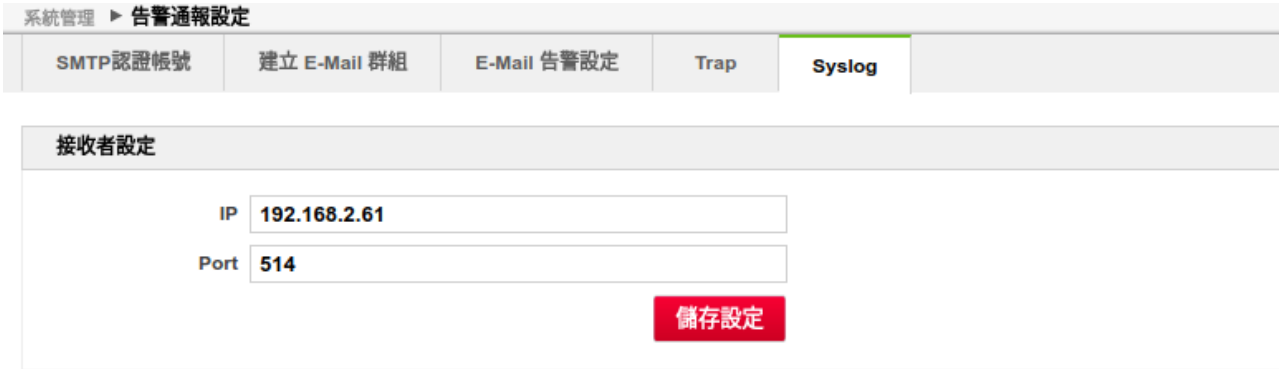
Syslog

當系統發生告警狀態時，可利用 syslog 的方式將系統告警內容再傳送至指定接收端。

IP：設定欲進行 syslog 接收的接收端 IP/FQDN。

Port：指定該 syslog 接收端連線所使用之傳輸 Port。

若欲清除設定時，請清空設置並按下儲存設定鈕即可。



1.8 報表 LOGO 上傳

此選項的功能主要在於提供管理者自訂報表 Logo。使用者可以自訂 Logo 樣式後上傳至 N-Reporter，該 Logo 樣式將顯示於輸出報表(Off-line Report)的頁面上。N-Reporter 目前支援 JPG/JPEG 檔案格式。

上傳項目

系統目前提供三種 Logo 樣式，詳細說明如下：

- **PDF Logo**：放置於 PDF 內頁左上角的 Logo 圖像。(建議上傳圖檔解析度 200×50 px，檔案大小限制為 1MB。)
- **PDF 直式報表封面**：放置於 PDF 直式報表封面圖像，包含 Top N 報表、趨勢報表、IP 阻擋列表等，其 PDF 皆為直式報表。(建議上傳圖檔解析度 595×842 px，檔案大小限制為 1MB。)

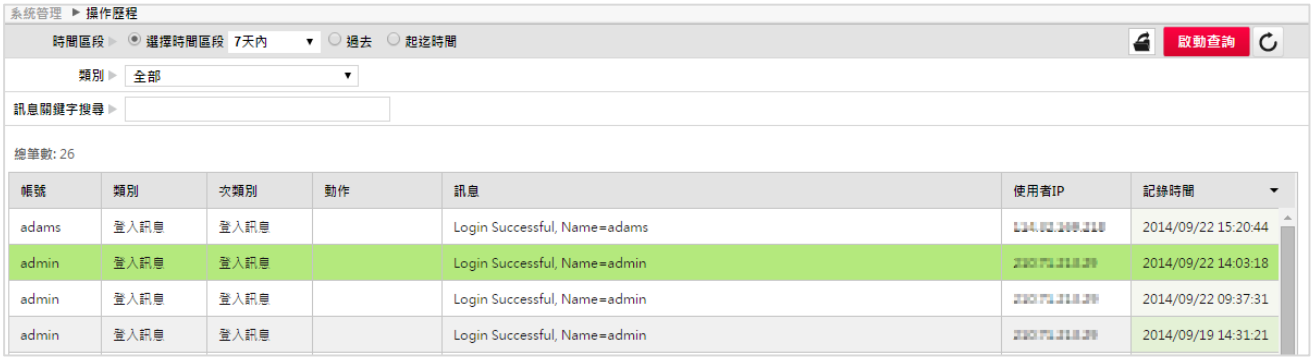
  請注意，此處指定的圖像為整個套用於文件封面，而非僅有 Logo，請確認所上傳的圖檔可完整覆蓋於所輸出的 PDF 封面上。以免造成封面輸出失真或是歪斜。

- **PDF 橫式報表封面**：放置於 PDF 橫式報表封面圖像，事件的 PDF 輸出為橫式報表。(建議上傳圖檔解析度 842×595 px，檔案大小限制為 1MB。)

  請注意，此處指定的圖像為整個套用於文件封面，而非僅有 Logo，請確認所上傳的圖檔可完整覆蓋於所輸出的 PDF 封面上。以免造成封面輸出失真或是歪斜。

1.9 操作歷程

此選項的功能主要在於提供管理者查看使用者操作 N-Reporter 的記錄。所有在 N-Reporter 中的設定修改及登入都將記錄於操作歷程。



操作歷程查詢與輸出

提供以下三種查詢功能，在輸入搜尋條件後，按 啟動查詢 鈕，執行查詢動作。按鈕，可清除所輸入的搜尋條件。按下 鈕，可將查詢結果輸出為 PDF、CSV 或 XML 檔案。

- 類別：下拉選擇「全部」、「登入訊息」、「系統管理」、「設備管理」、「事件」、「報表」等進行類別過濾查詢。
- 訊息關鍵字搜尋：可輸入訊息關鍵字(全部或是部份)進行過濾查詢。
- 查詢時間區段：點選「選擇時間區段」、「過去」或「起迄時間」的時間區段進行查詢。

操作歷程列表

顯示使用者操作歷程資訊，列表欄位說明如下：

- 帳號：顯示執行此動作的帳號。
- 類別：依左側主選單將使用者操作分類為「登入訊息」、「系統管理」、「設備管理」、「事件」、「報表」。
- 次類別：定義實際的操作項目。
- 動作：針對使用者的行為是設定的新增(Add)、刪除(Delete)還是修改(Modify)。
- 訊息：使用者操作的細節說明。
- 使用者 IP：顯示執行此動作時的用戶 IP。
- 記錄時間：顯示該筆操作歷程發生的時間。

1.10 偏好設定

此選項的功能主要在於提供管理者自訂事件顯示欄位。由於事件欄位繁多，為避免在呈現上太過於雜亂，使用者可以依實際需要，為不同的查詢依據訂定所需的欄位及呈現順序。

事件欄位

■ 預設事件欄位設定

(1) 預設查詢依據：為設定在執行事件時的預設查詢依據，例如：使用者環境中以 IPS 的資安分析為主，即可預設以 Syslog 作為查詢依據。

(2) 預設事件型態：為設定在執行事件時預設的事件型態，事件型態分別有「Security」、「Traffic」、「Audit」、「Web」、及「Other」(可多選)。設定完成後，按下 儲存設定 鈕，以儲存並套用相關設定。

■ 事件欄位偏好設定

顯示各偏好設定資訊，列表欄位說明如下：

(1) 偏好設定名稱：顯示偏好設定名稱。

(2) 事件欄位：顯示事件所呈現的欄位。

(3) PDF 事件欄位：輸出 PDF 所呈現的欄位。

「Syslog」、「Flow」、「Security」、「Traffic」、「Audit」、「Web」及「Other」為出廠預設的偏好設定，此偏好設定可以更改事件欄位呈現及事件輸出 PDF 欄位呈現，但是不可刪除。例如對 Traffic 而言，「事件」、「流入流出介面」較不重要，「Policy ID」、「NAT IP/Port」資訊較重要，就可以定義個人專屬的呈現方式。

按鈕操作

按下 按鈕，彈出事件欄位偏好設定視窗

- 偏好設定名稱：請輸入在系統中不重覆的偏好設定名稱；

  「事件欄位」請點選◀由「可選欄位」中選擇要加入的欄位，或點選▶移除「事件欄位」中選擇的欄位，可以利用▲▼調整欄位呈現順序；

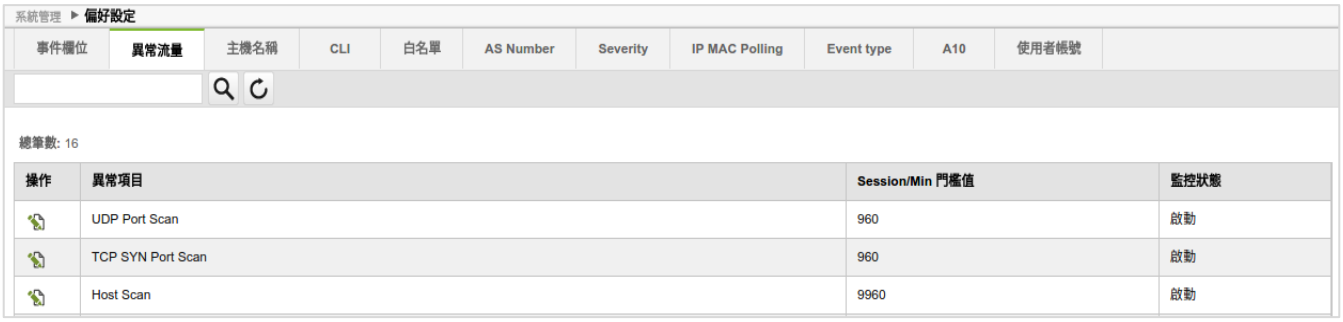
- 輸出 PDF 欄位設定 : 請點選◀由「可選欄位」中選擇要加入的欄位，或點選▶移除「輸出 PDF 欄位設定」中選擇的欄位，可以利用▲▼調整欄位呈現順序。

由於輸出 PDF 有 A4 紙張頁面寬度限制，建議選擇欄位不要超過 12 欄。

Flow

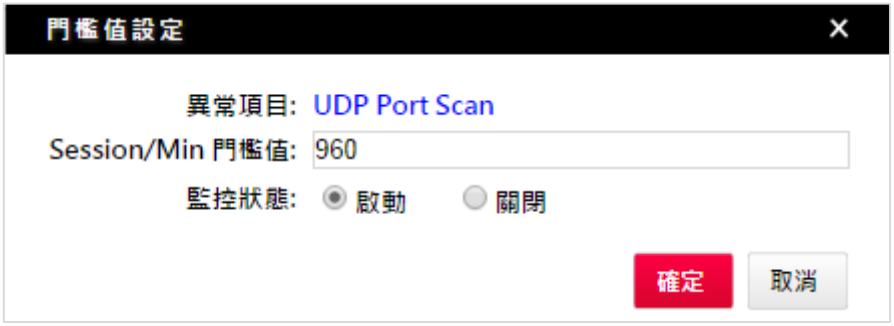
異常流量

設定 Flow 異常流量的 Session/Min 門檻值及監控狀態。



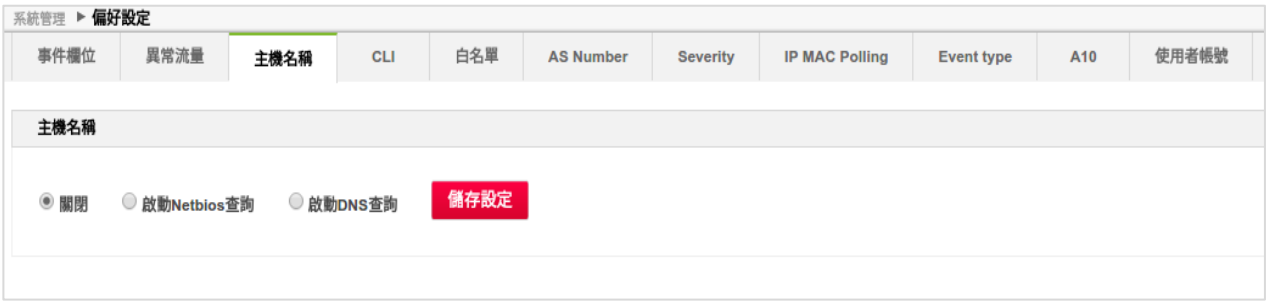
相關 Flow 異常流量報表請參考「報表➔趨勢報表➔Flow 異常流量報表」章節。

- 異常項目搜尋：提供字串搜尋功能，可輸入異常項目(全部或是部份)作為查詢依據，按下 鈕，執行搜尋。按下 鈕，可以清除輸入的搜尋字串。
- 異常流量列表：顯示異常流量相關資訊，列表欄位說明如下。
  (1) 異常項目：顯示異常項目的。
  (2) Session/Min：顯示該項目目前所設定的門檻值。
  (3) 監控狀態：顯示該項目目前所設定的監控狀態。
- 按鈕操作：在異常項目列表「操作」欄位，點擊欲修改項目 圖示，彈出門檻值設定視窗(如下圖)。「異常項目」顯示目前操作的項目；「Session/Min」請輸入欲監控的門檻值；「監控狀態」請選擇此項目是否"啟動"或"關閉"監控。



主機名稱

在動態 IP 的環境下，查詢內部異常 IP 所對應的使用者是個苦差事。N-Reporter 支援利用 Netbios 方式即時抓取主機名稱，或者是結合企業內部 DNS 的方式取得主機名稱，顯示於「來源主機名稱」及「目的主機名稱」欄位。



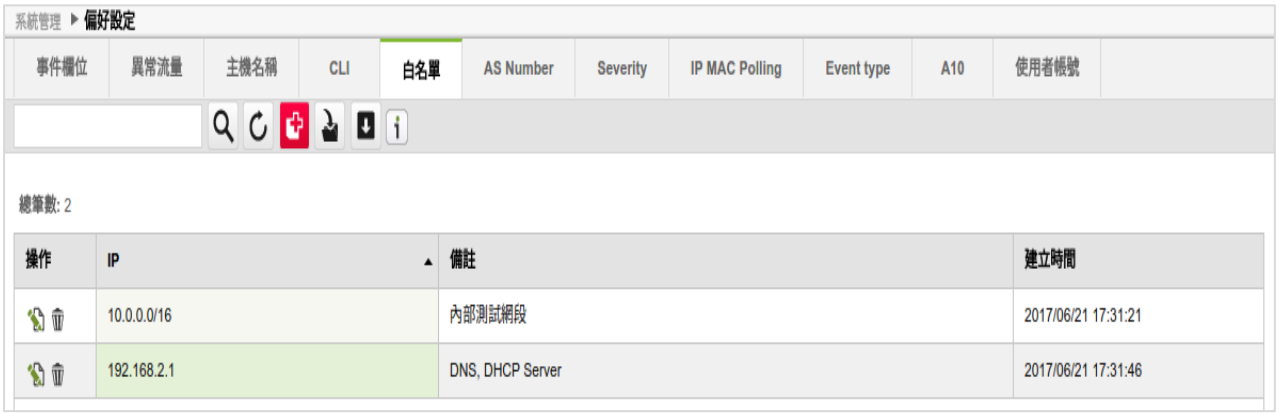
啟動主機名稱查詢僅針對 Home 網段所定義的內部網路 IP，由於此功能會造成額外的網路及系統負擔，在高資料量(EPS)的環境下建議不啟動。

CLI

在部份高安全性的環境中，只允許以實體線路(Console)方式連線，可在此頁面啟動或關閉 CLI (SSH 連線)。

白名單

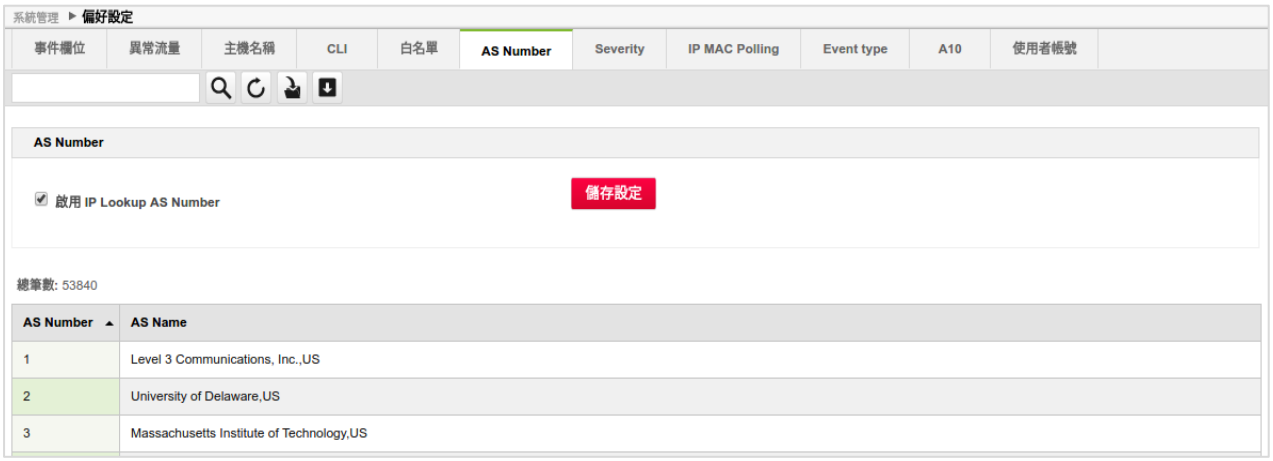
定義已知或無需關注的 IP 或網段。在白名單所定義的 IP，將不會在「趨勢分析」的告警中被列出，如 Security 事件週趨勢、Security 事件即時異常告警及 Flow 即時異常告警。



AS Number

可以搜尋，匯入自訂 AS Number 表格及匯出已存在的 AS Number 表格。

提供設置啟動或關閉在報表中利用 IP 查找 BGP AS Number 並將對應的機構顯示出來，並提供 AS Number 所屬的機構列表，供用戶查找 AS Number 或 AS Number 所對應的機構。



- 查詢：可在查詢欄位輸入欲查詢的機構部份字元或是 AS Number 按下 鈕，執行搜尋。按下 鈕，可以清除輸入的搜尋字串。
- 按下 鈕，系統會彈出「匯入」視窗，請按「瀏覽」指出要匯入的 CSV 檔案後，按 上傳 鈕可以執行 AS Number 的批次匯入動作。
- 按下 鈕，將會下載當前所有存在於系統中所有的 AS Number 資料。
- 啟用 IP Lookup AS Number：可選擇在進行流量分析時進行利用 IP 對應 AS Number 對於的功能。
- AS 列表：顯示 AS Number 及 AS Name 的對應關係列表。

  總筆數：顯示系統內 AS 資料的總筆數。

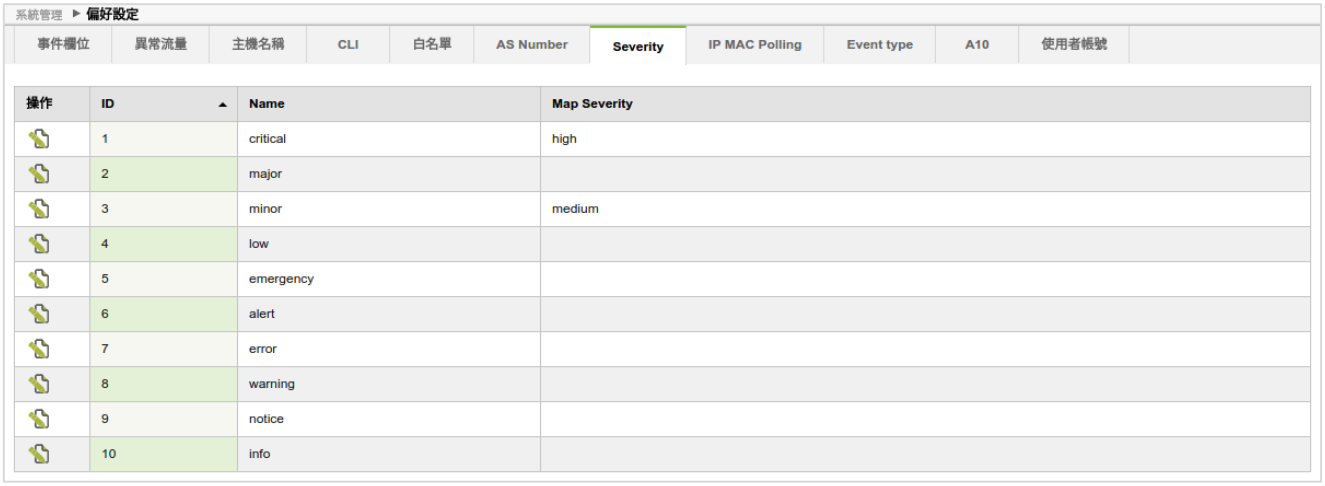
  AS Number：AS Number 為 IANA(Internet Assigned Number Authority)發放給申請機構的獨有編號，使用於 BGP 路由技術。

  AS Name：為擁有該 AS Number 的機構名稱。

1. 當使用「匯入」功能時，所要匯入的檔案需符合 UTF-8 編碼。
2. 「匯入」動作，將進行全系統 AS Number 資料覆蓋的動作，而非僅加入所匯入的項目，匯入前建議先進行「下載」備份，以免造成 AS Number 資料缺漏。若發現有缺漏，請聯繫 N-Partner 以取得原始 AS Number 列表。

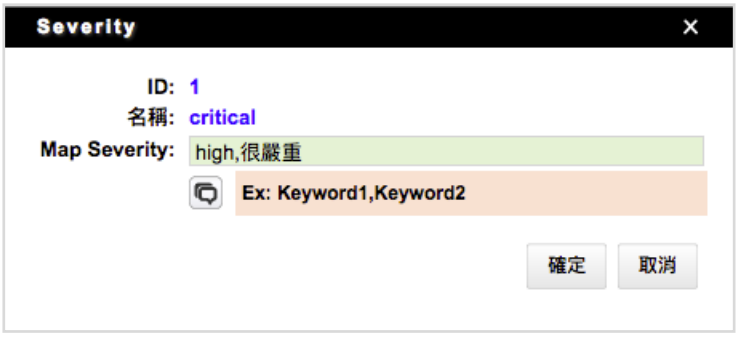
Severity

定義事件等級及可自定義相對應之關鍵字。在 Syslog 進行正規化時，當 LOG 中的 Severity 符合所定義的關鍵字時會對應到系統內定的 10 個嚴重等級。



操作	ID	Name	Map Severity
	1	critical	high
	2	major	
	3	minor	medium
	4	low	
	5	emergency	
	6	alert	
	7	error	
	8	warning	
	9	notice	
	10	info	

- 按鈕操作：在「操作」欄位，點擊欲修改項目圖示，彈出 Severity 設定視窗(如下圖)。「ID」及「名稱」顯示目前操作的項目；「Map Severity」請輸入欲自定義的對照關鍵字，如：high,很嚴重，當過濾條件的嚴重等級勾選 critical 時，將自動包含嚴重等級為 high 及 很嚴重 等告警。

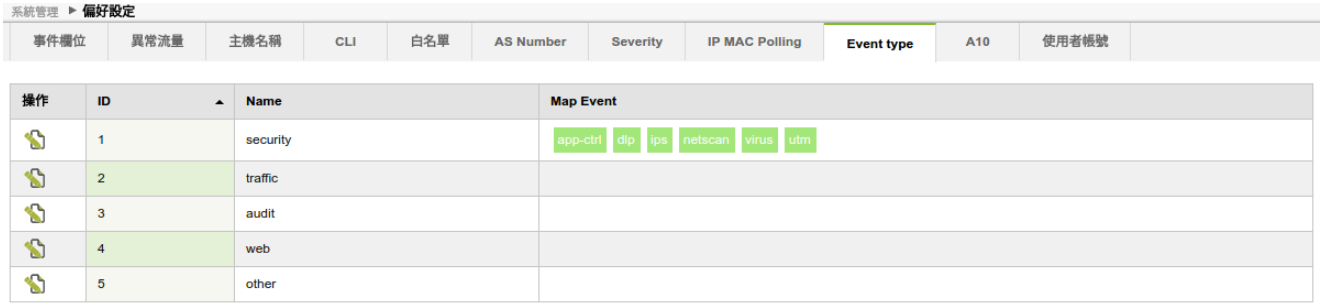


IP MAC Polling

為了使 IP Address 和 MAC Address 進行關聯，可在支援 IP MAC 對應的設備上取得對應表以進行關聯。此處可設置開啟或關閉取得設備 IP MAC 對應表的功能是否開啟。

Event type

為了方便將 Syslog 進行分類，依常見的事件分類設計了 Security,traffic,audit, web, other 等五大類別，但由於各個設備廠商設計研發的規劃不同，在類型名稱上會有所不同，因此提供此對應表將類型名稱和 Default 的類別進行對應，以便利相關事件查詢。



A10

在利用 A10 設備進行聯防的 Action 動作時，需指定 A10 設備的 BGP AS Number 才可遂行該動作，此處可指定該 BGP AS Number 以利連動 A10 設備。

使用者帳號

為強化系統安全性，此處可選擇在使用者設置密碼時的密碼複雜度需包含英文字器+數字+特殊符號，且密碼在指定的天數後會失效並要求使用者修改密碼。以及當認證失敗指定次數後，鎖定該帳戶指定的分鐘數。

- 密碼複雜度需包含 英文字母 / 數字 / 特殊符號：可勾選此功能，要求用戶之密碼需包含英文及數字及特殊符號。
- 密碼更新週期：設置密碼過期天數，超過設定天數後，將提示用戶更改密碼。預設為 0 (不過期)。
- 認證失敗：可設定在認證失敗於指定次數後，以鎖定登入的方式阻擋該 IP 於指定分鐘數內之認證請求。失敗次數預設為 4 次即進行鎖定。鎖定登入的時間預設為 30 分鐘。

Radius (Radius 認證功能)

為了提供使用者認證機制的彈性，N-Reporter 提供 Radius 的認證功能讓本身已經使用 Radius 認證設備的用戶可以直接接入 N-Reporter。設置完畢後用戶可使用 Radius 上之帳號及密碼登入至 N-Reporter 上進行操作。

該帳號必須同時存在於 N-Reporter 上

設定 Radius 所需的項目及說明如下：

- Radius 啟動：為啟動 Radius 的 checkbox，勾選啟動後，才可進行 Radius 相關的設置。
- Radius IP：為 Radius 設備之 IP Address，用以連接至 Radius 設備。
- Secret Key：為 N-Reporter 和 Radius 設備溝通時，所需利用的認證密碼。
- 測試登入帳號：為進行 Radius 連接測試，需提供在 Radius 上可進行認證之可用帳號，以便進行測試。
- 測試登入密碼：為進行 Radius 測試登入帳號上所使用是正確登入密碼。
- Radius測試 按鈕:點下此按鈕可以針對所輸入的資料進行 Radius 測試，測試後會 popup Radius 測試結果窗。
- 儲存設定 按鈕：點下此按鈕後，將完成 Radius 設置。此時所有新登入之用戶行為，將與 Radius 設備連動。

請注意，此時的帳號密碼需與 Radius 設備上的帳號訊息一致，而非與 N-Reporter 上的帳號訊息一致，以避免重覆登入失敗而遭到 N-Reporter 阻擋。

- 解除 Radius 連動

由於 Radius 連動的部份，在系統上的優先等級較高，因此若需解除 Radius 的連動需連線至 N-Reporter 之 CLI。步驟如下：

(a) 使用 CLI 帳號密碼登入 CLI (預設 npartner/npartner)。

(b) 登入後輸入 config terminal，以進入 config 模式。

(c) 在 config 模式中，輸入 radius off。結果如下圖所示。

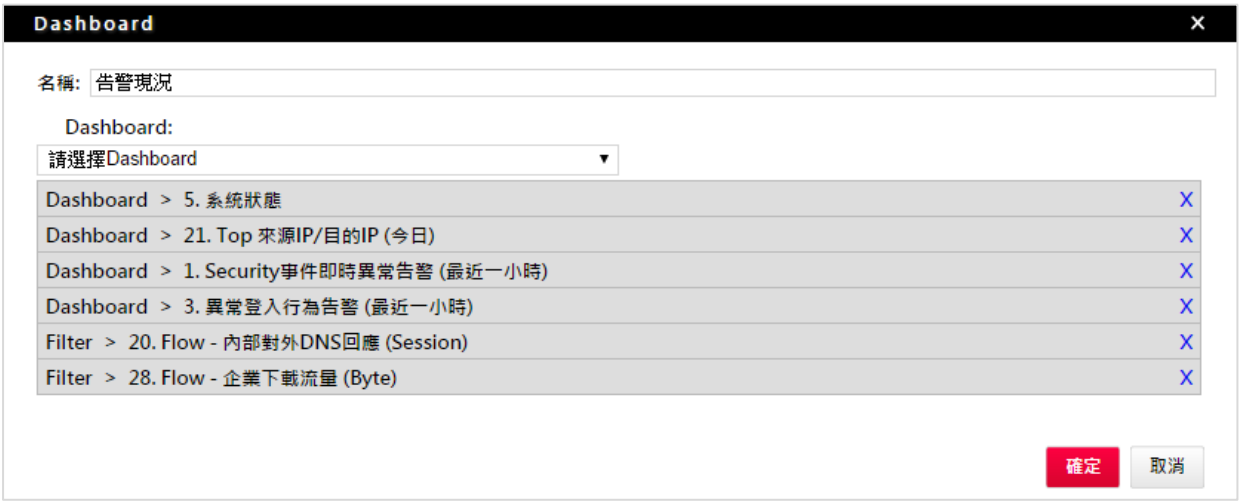
```
Welcome to CLI!
N-Reporter# config terminal
N-Reporter(config)# radius off
Radius is off!!
N-Reporter(config)#
```

1.11 Dashboard

提供使用者自訂的儀表版(Dashboard)，可用作即時監控使用，包含系統狀態、接收量、異常告警統計等。

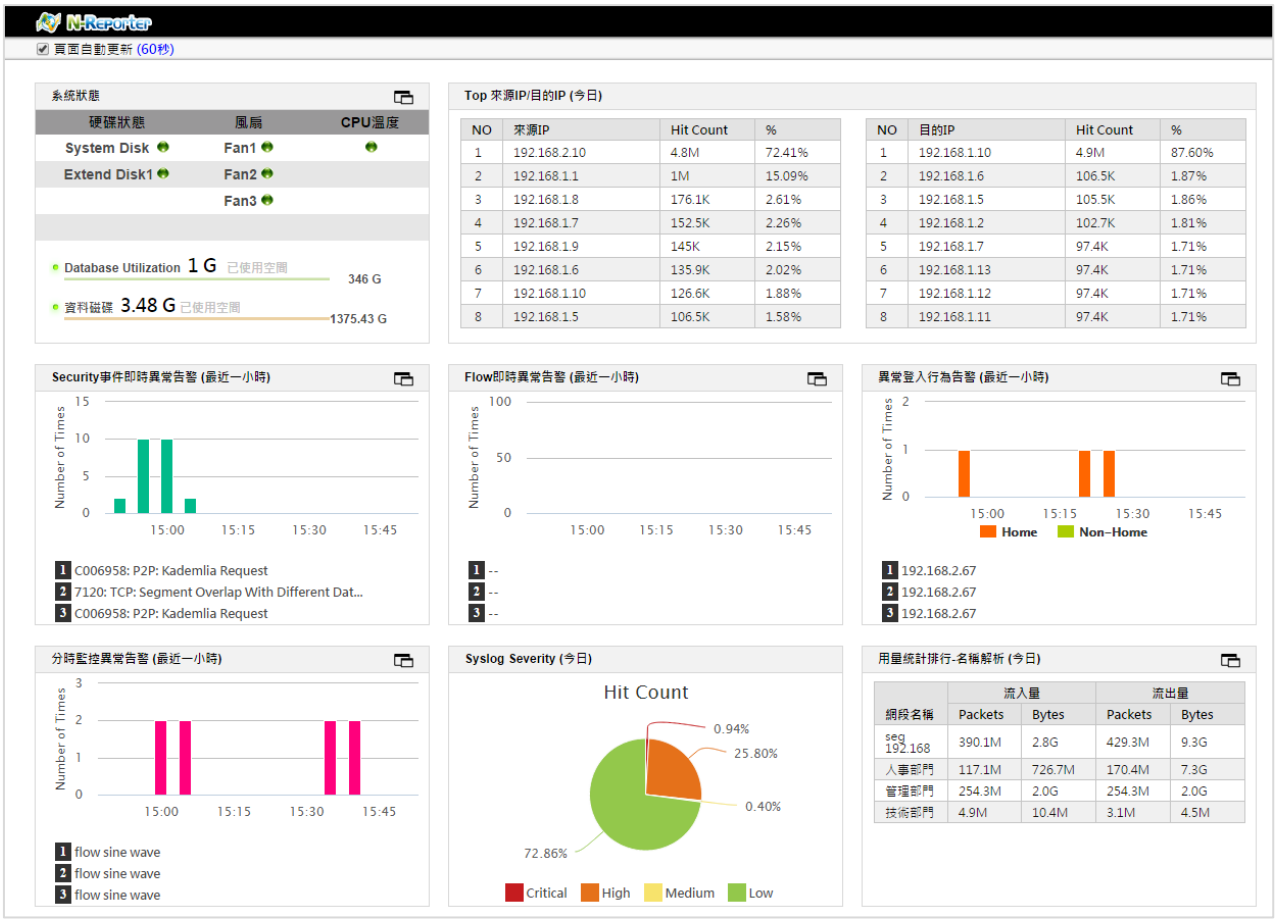
可以輸入 Dashboard 的名稱(部份或是全部)來過濾定義列表。

點選新增  圖示，將彈出「新增 Dashboard 視窗」(如下圖所示)



指定名稱後，可在「請選擇 Dashboard」中選擇想呈現的項目，項目有分 2 種: Dashboard(儀表板)及 Filter(分時監控報表)，最多可選擇 9 個項目。在某個項目的右側按「X」鈕可移除該項目，也可以點選某個項目直接利用拖拉的方式來調整呈現項目的順序。設定完成後點選「確定」來儲存設定。

點選列表最右側的 瀏覽 可以查看所設定的 Dashboard。可以設定預設 Dashboard，在登入時自動載入，設定方式為點選左方單選按鈕(Radio button)後點擊上方 **預設** 即可。



Dashboard 的上方可勾選網頁自動更新，此頁的資料將每 60 秒自動更新。

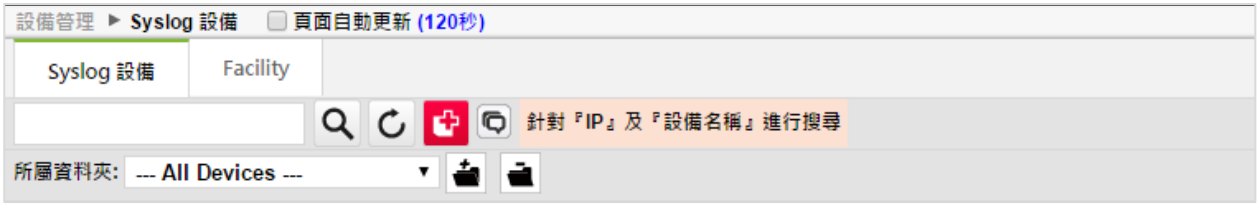
點選每個項目右上方的 ，可以跳到相對應的頁面，例如上圖箭頭處點選後將切換至「Flow 即時異常告警」頁面。

Chapter 2 設備管理

此章節會介紹「設備管理」下之子功能:「Syslog 設備」、「SNMP 監控設備」及「Flow 設備」等各項設定。

2.1 Syslog 設備

此選項的功能主要在於執行 Syslog 未知設備的新增、已接收設備的編輯及資料夾的管理。點選「Syslog 設備」選項。考慮到用戶一開始對報表的操作可能不熟悉，在新增 Syslog 設備後，將產生預設的 Top-N 報表，分時監控報表，及分時監控報表群組供用戶編輯使用。



頁面自動更新

當勾選「頁面自動更新」則會以每 2 分鐘(120 秒)刷新此頁面。

Syslog 設備搜尋

搜尋特定的 Syslog 設備，可輸入字串或 IP(全部或是部份)，按下鈕，針對「設備識別」、「IP」及「設備名稱」欄位進行搜尋。按下鈕，可以清除輸入的搜尋字串。

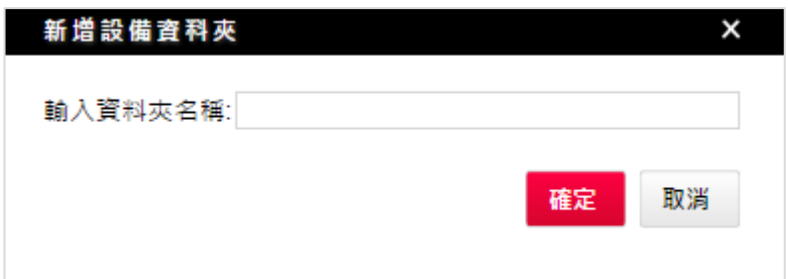
新增、編輯設備

按下鈕可新增設備。

所屬資料夾

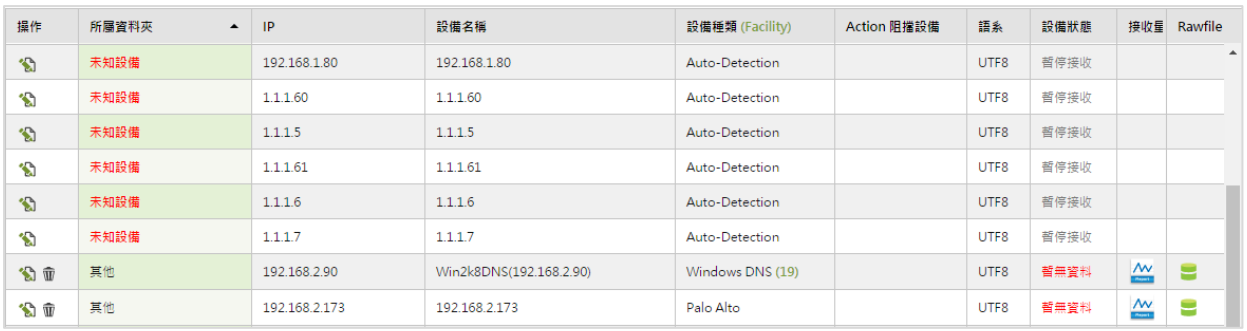
為了方便管理與找尋 Syslog 設備，N-Reporter 採用資料夾的管理方式。在「事件」及「報表」中，亦可勾選設備資料夾作為過濾條件。在「所屬資料夾」下拉選項中，可選擇特定的資料夾，系統將顯示位於此資料夾內的所有 Syslog 設備清單。

按下鈕，彈出新增設備資料夾視窗(如下圖)，請輸入一資料夾名稱即可完成。按下鈕，可刪除所選資料夾，原本在此資料夾內的所有 Syslog 設備則會改歸類到「其他」資料夾中，不會遭到刪除。「未知設備」及「其他」資料夾為系統 Default 功能性資料夾，不可刪除。



Syslog 設備列表

顯示目前系統 Syslog 設備相關資訊。

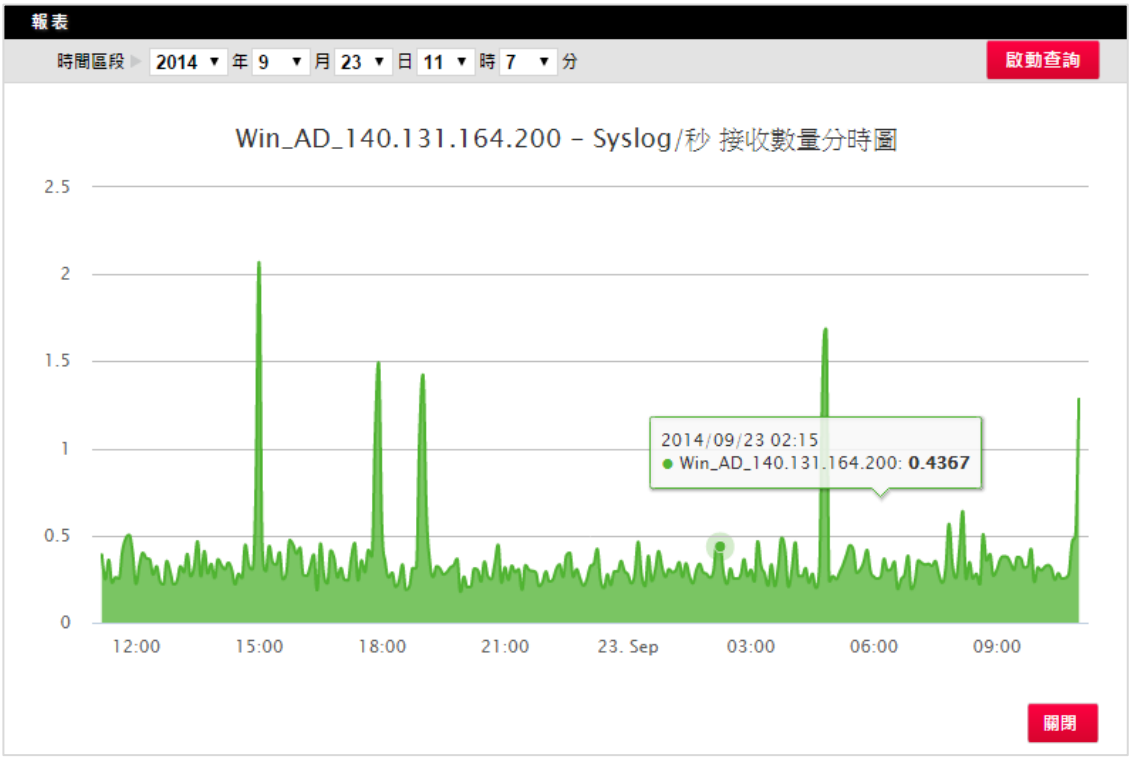


操作	所屬資料夾	IP	設備名稱	設備種類 (Facility)	Action 阻擋設備	語系	設備狀態	接收量	Rawfile
	未知設備	192.168.1.80	192.168.1.80	Auto-Detection		UTF8	暫停接收		
	未知設備	1.1.1.60	1.1.1.60	Auto-Detection		UTF8	暫停接收		
	未知設備	1.1.1.5	1.1.1.5	Auto-Detection		UTF8	暫停接收		
	未知設備	1.1.1.61	1.1.1.61	Auto-Detection		UTF8	暫停接收		
	未知設備	1.1.1.6	1.1.1.6	Auto-Detection		UTF8	暫停接收		
	未知設備	1.1.1.7	1.1.1.7	Auto-Detection		UTF8	暫停接收		
	其他	192.168.2.90	Win2k8DNS(192.168.2.90)	Windows DNS (19)		UTF8	暫無資料		
	其他	192.168.2.173	192.168.2.173	Palo Alto		UTF8	暫無資料		

說明如下：

- 操作：點擊 圖示，以編輯該筆 Syslog 設備，包括更改「設備名稱」、「設備種類」、「資料格式」、「接收狀態」及「所屬資料夾」等。點擊 圖示，則刪除該 Syslog 設備。
- 所屬資料夾：顯示該 Syslog 設備存放於哪個資料夾裡。
- IP：顯示該 Syslog 設備 IP。
- 設備名稱：為使用者自行定義的 Syslog 設備名稱，供使用者方便閱讀與辨識用。
- 設備種類(Facility)：顯示設備廠牌及型號，若有 Facility 的設定，會用( )表示。
- Action 阻擋設備：設定為 Action 設備時，將在欄位內顯示為 Action 阻擋設備類型。
- 語系: 指定 Syslog 語系編碼，系統預設為 UTF-8 編碼，如果接收到的 LOG 有亂碼的情況產生，請依設備設定來指定語系設定，例如繁體中文(Big5)或是簡體中文(GB2312)。
- 設備狀態：其狀態分別為：
  (1) 啟動接收：表示 N-Reporter 正在接收與處理中的 Syslog 設備，該設備會佔用一個「運行設備」數量。
  (2) 暫停接收 : 表示該設備的 Syslog 資料系統暫時不收。該設備不會佔用「運行設備」數量，但 Syslog Raw Data 也不會儲存到系統中。
  (3) 暫無資料：表示過去一小時內未曾收到來自該設備的 Syslog 資料，在表格中將以紅色字型標示，此仍會佔用一個「運行設備」數量。

■ 接收量：點擊該 Syslog 設備 圖示，彈出一視窗，顯示此設備的接收數量分時圖(如下圖)。



■ Rawfile：為設備送至本系統的原始內容，取得該內容可協助管理人員進行驗證。點擊 圖示，將彈出視窗並提供管理人員選擇下載 Rawfile 的開始時間及時間長度。在點擊下載按鍵後即進行該設備指定時段的下載任務。

管理未知設備或新增設備

N-Reporter 採用自動新增 Syslog 設備的方式，使用者只要在 Syslog 設備中，設定 Syslog Raw Data 輸出至 N-Reporter 的管理 IP 以及 Port 514 即可。

當一個新 Syslog 設備將 Syslog Raw Data 傳送至 N-Reporter 時，N-Reporter 會將此設備暫放在「未知設備」資料夾中，並於 Syslog 設備列表上標註為「未知設備」，等待使用者的確認。

操作步驟如下：

Action

(1) 在 Syslog 設備列表中，點擊所選的「未知設備」左方圖示後執行編輯工作以完成設備添加；此外也可以在 Syslog 設備列表畫面上點選鈕手動新增 Syslog 設備。

(2) 系統彈出的「新增或編輯 Syslog 設備」對話視窗中輸入一個易於辨識的「名稱」。

(3) 設備 IP：手動新增或編輯時，此處可輸入欲管理之 Syslog 設備(syslog 來源設備)所使用的 IP Address。由未知設備加入時，由於已自 Syslog 中取得來源設備之 IP，因此設備 IP 欄位為不可編輯的狀態。

(4) 選擇設備所屬之「設備種類」：

指定是否為 Action 設備，並選擇設備類別。勾選 Action 設備代表除了接收設備的 Syslog 之外，也支援將可疑的 IP 做阻擋的動作。可勾選「是否預設 Action 設備」做為批次阻擋的預設設備 (可指定多部設備為預設 Action 設備)。指定為 Action 設備時，同時也會要求輸入帳號及密碼，正確的帳號密碼才能確保後續的資安聯防的阻擋功能正確運作。

由於 Syslog 設備可進行 action 功能的種類及目的不同，部份總類的設備會有其他輸入的項目條件，以下為其他欄位之說明，optional 欄位可留空白，視需要輸入。

Enable 密碼(optional)：為設備經過 CLI 登入進行設置時需提供之管理密碼，請詳閱該設備說明，必要時才需輸入。

Nexthop(optional)：若進行 action 之設備為路由器，且進行 action 時為改變下一跳之 routing IP 時，可由此輸入，必要時才需輸入。

Action URL(optional)：該設備使用 http 進行 action 操作，但可能經由 http 或 https 或使用其他的 TCP port 提供連線，可利用此欄位輸入可連線至該設備進行 action 的 URL。請詳閱該設備說明，必要時才需輸入。

(5) 選擇設備所屬之「資料格式」：

請依設備廠牌及型號指定資料格式，錯誤的格式指定將造成正規化異常，預設的自動判定功能雖然會依 LOG 內容自動判別正規化規則，但為了更好的運行效能及分析效果，請儘量手動指定資料格式。

(6) 選擇設備所屬之「Facility」：

Syslog 標準傳輸格式中定義了 Facility 欄位以進行 log 的分類，如此可方便在同一部設備中管理來自系統中不同應用程序的 log，Facility 定義了各種常見類型的服務(kern,mail,auth...等等)所使用的預設 Facility 順序編號為 0~15，並保留 local0～local7 順序編號為 16～23 以因應未列於預設 Facility 的應用程序之 log 管理。因此在同一設備中，各種不同的應用程序經由 syslog 送出多種 log 格式時，需先在欲加入管理之設備上指定應用程序上設置對應的 Facility 編號，在 N-Partner 設備上則可利用指定對應 Facility 的方式分類納管來自該設備上所對應的應用程序之 syslog。不同的 IP+Facility 組合便可以各自指定所屬的資料格式，但請注意此種設定法將佔用多個設備 License。

例如 Linux 上架設 Apache 及 MySQL，除了在系統中新增原本的 Linux 設備(Facility 不指定)之外，可以新增 Apache(Facility=22[local 6])及 MySQL(Facility=17[local7])兩部設備，便可以分別指定不同的資料格式。此例中將佔用 3 個設備 License。

(7) 語系：由於各種操作系統可能提供不同語系的支援，如早期 Windows 可能提供繁體中文 BIG5 及簡體中文 GBK 或 GB2312 編碼的 syslog。此時為避免在接收 syslog 時，因使用錯誤的編碼而造成接收的 syslog 被存成亂碼的情形，請在此指定由此設備來的 syslog 所使用的編碼。

(8) 將接收狀態修改成「啟動接收」：

(a) 啟動接收：表示 N-Reporter 正在接收與處理中的 Syslog 設備，該設備會佔用一個「運行設備」數量。

(b) 暫停接收：表示該設備的 Syslog 資料系統暫時不收。該設備不會佔用「運行設備」數量，但 Syslog Raw Data 也不會儲存到系統中。

(9) 選擇一個適當的存放資料夾後，按下「確定」鈕，完成新增 Syslog 設備作業。

- Syslog 設備若處於「啟動接收」狀態會佔用一個「運行設備」數；若是處於「暫停接收」狀態則不計算於「運行設備」中。
- 使用者可透過「系統管理➔系統資訊➔運行中/可處理設備數量」了解目前所購 License 可支援最大的運行設備數量以及運行中的設備數量。
- N-Reporter 將依據所收到的 Syslog 格式，自動判斷其設備種類，若為特定設備的 Syslog，請選擇對應的資料格式。
- 各種 Syslog 設備的 Syslog Raw Data 丟出設定方式請參閱各原廠的操作手冊。若已確認送出設備的 Syslog，卻遲遲未在「未知設備」中出現，請確認是否正確設定 ACL：「系統管理➔網路參數設定➔設定 Access List」。

> 若 N-Reporter 已申裝 Action Module，在編輯支援 Action 阻擋協同運作的 Syslog 設備時，必須額外設定登入該 Syslog 設備的使用者帳號及密碼。

Windows WMI Syslog 設備管理

N-Reporter 通常採用自動新增 Syslog 設備的方式，但如果使用者是使用 WMI 的協定直接遠端擷取 Windows 登入稽核的相關事件的話，則需手動新增此 Syslog 設備。

點選鈕，系統會彈出「新增或編輯 Syslog 設備」視窗(如下圖所示)

■ 注意事項：

(1) 資料格式：請依照 Windows 主機的種類(Windows Server/Windows AD Server)來選擇適當的資料格式

(2) 登入帳號：請輸入具有足夠權限之帳號

(3) 有關 Windows AD audit to WMI 之詳細設定文件請參考此網址：

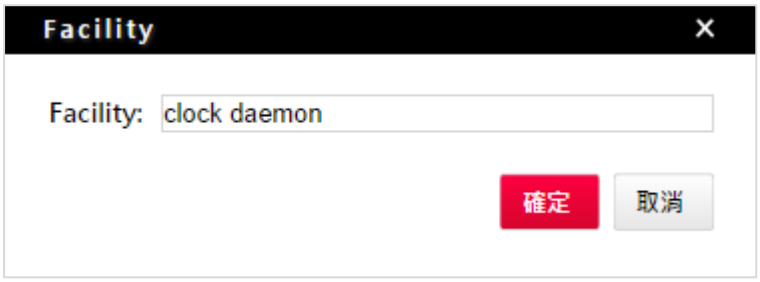
http://www.npartnertech.com/download/tech/N-Reporter-Windows-AD-auditToWMI_tw.pdf

Facility

Syslog 標準傳輸格式中定義了 Facility 欄位以進行 log 的分類，如此可方便在同一部設備中管理來自系統中不同應用程序的 log，Facility 定義了各種常見類型的服務(kern,mail,auth...等等)所使用的預設 Facility 順序編號為 0~15，並保留 local0～local7 順序編號為 16～23 以因應未列於預設 Facility 的應用程序之 log 管理。因此在同一設備中，各種不同的應用程序經由 syslog 送出多種 log 格式時，需先在欲加入管理之設備上指定應用程序上設置對應的 Facility 編號，在 N-Partner 設備上則可利用指定對應 Facility 的方式分類納管來自該設備上所對應的應用程序之 syslog。

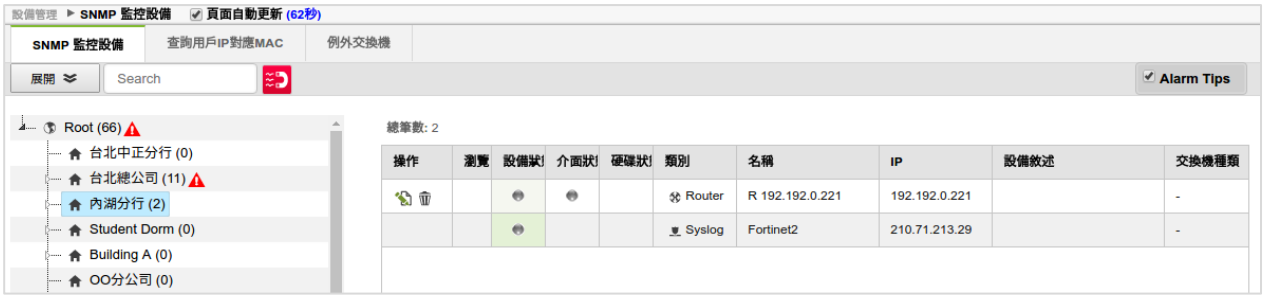
此選項的功能主要在於提供使用者可以修改 Facility 編號(Code)定義之名稱。

按  鈕，彈出修改 Facility 名稱之視窗：



若同一個設備 IP 執行了多種服務，請在送出各種服務 LOG 時指定不同的 Facility，N-Reporter 提供針對不同 Facility 指定不同的 LOG 資料格式。 在「設備管理→Syslog 設備」中編輯設備設定時，請同時指定「資料格式」及「Facility」

2.2 SNMP 監控設備



此選項的功能主要在於執行 Switch 與 Host 設備的新增、編輯，以及設備管理 Treeview 的呈現。

Action ▶ **SNMP 監控設備**

■ 搜尋列

點選 展開 可以打開所有區域及所包含的設備，點選 收合 可將所有區域收合起來。

針對關鍵字來搜尋 Treeview 上特定的區域及設備，可輸入設備名稱(部份或全部)或區域名稱，符合的項目會在 Treeview 上標示出來。

■ Treeview 操作

Treeview 可以提供網路設備與實體環境的聯結，方便使用者進行管理。可以針對 Treeview 進行以下操作行為。

(1) 新增：在區域節點(例如 Root)點選滑鼠右鍵選單，可以選擇新增「區域」或「Device」。

區域通常用來表示實體環境建置，例如大樓、樓層、部門、機房等，並允許多層次建立，例如 「第三大樓」 >> 「4 樓」 >> 「5 號機房」。當然，為了能更清楚的管理，不建議建立太過複雜的階層關係。

Device 則是用來新增及搜尋交換機或主機，可以將交換機或主機加入所點選的區域之下。有關交換機或主機的搜尋及管理，將在後續詳細說明。

(2) 更名：針對點選的區域進行名稱的修改

(3) 刪除：當區域並未包含任何區域及設備時，右鍵選單中可以選擇刪除功能，來移除不再需要的區域。

(4) 移動：點選 Treeview 上的設備，可以直接利用拖拉的方式來移動至其他區域

(5) 點選 Treeview 上的區域時，會在右側列表中呈現所屬設備列表。

(6) 點選 Treeview 上的設備時，則會顯示設備相關資訊及告警狀態，若是路由器或交換器，還會顯示介面列表。

Switch 與 Host 管理

顯示目前系統所有已管理的 Switch 或 Host 相關資訊。

操作	瀏覽	設備狀態	介面狀態	硬碟狀態	類別	名稱	IP	設備敘述	交換機種類	Model	監看設備	加入時間
					Router	R 192.168.0.252	192.168.0.252		-		Off	2016-0 09:26:4
					Router	R 192.168.100.2	192.168.100.2		-		Off	2016-0 10:26:1
					Router + Switch	GS3700 192.168.2.252	192.168.2.252	GS3700-24	管理交換機 (L3SW)	ZyXEL	On	2016-0 11:07:0
					Snmp Host	WIN2K8IIS 192.168.1.92	192.168.1.92	Hardwar Intel64 Family 6 Model 37 St...	-		On	2016-0 11:13:4
					Syslog	TP 192.168.10.14	192.168.10.14		-		Off	2016-0 17:38:3

列表欄位說明如下：

- 操作：點擊 圖示，以編輯該筆 Switch 或 Host 設備，包括更改「設備名稱」、「設備種類」、「Community」、「登入帳號」及「登入密碼」等。點擊 圖示，則刪除該 Switch 或 Host 設備。

> 刪除 Switch 或 Host 設備，將同時刪除由設備新增至設備刪除期間，所有已收集的 SNMP/Flow/Syslog Data，刪除前，請務必考慮週全。

- 瀏覽: 點選 可以查看交換器或主機的 CPU/Memory 使用率曲線圖。

- 類別：顯示該設備之類別。
  (1) Switch：指支援用 SNMP 去抓取介面及 IP/MAC 資訊之設備。
  (2) Router：指只收 Flow 資料之設備
  (3) Switch + Router：指同時支援用 SNMP 去抓取介面及 IP/MAC 資訊而且也收 Flow 資料之設備
  (4) Host：指支援 Host MIB 之主機(如: Windows/Liunx/Unix)
- 名稱：為使用者自行定義的 Switch 或 Host 設備名稱，供使用者方便閱讀與辨識用。
- IP：顯示該 Switch 或 Host 設備 IP，N-Reporter 會對此 IP 進行 SNMP Polling 以及必要的 Telnet 設定動作，亦為該設備在系統內唯一的識別資訊。
- 設備敘述：使用者可以撰寫一段敘述用以協助辨識，或是延用 SNMP Polling 得知的交換機或主機敘述。
- Model: 選用交換機的廠牌，如 Cisco、Juniper、H3C。
- 監看設備: 是否啟動 SNMP 監看設備狀態，除了繪製 CPU/Memory 使用率曲線圖之外，在使用率超過門檻值時能即時發送告警。
- 設備狀態：顯示目前設備的 CPU/Memory 的狀態，燈號如下。
   ：此燈號代表設備狀況正常
   ：出現此燈號代表設備硬體裝置發生問題，請聯絡 N-Partner 或代理商以進行檢修。
   ：出現此燈號代表此硬體裝置未套用監控樣板進行監控。

  在燈號圖示上點滑鼠左鍵，可將設備異常告警畫面彈出，並顯示所點選的設備的狀況。設備異常告警頁面的內容，請見設備異常告警說明。
- 介面狀態(設備透過 SNMP 取得介面資訊時才會顯示)：顯示目前設備上網路介面的狀態，燈號顯示介紹和設備狀態說明相同。
- 硬碟狀態(設備透過 SNMP 取得硬碟資訊時才會顯示)：顯示目前設備上硬碟的狀態，燈號顯示介紹和設備狀態說明相同。
- 接收量(於樹狀圖中點選 syslog 設備時，顯示於右方設備內容)：可看到該設備 syslog 的接收的狀況。
- 加入時間：顯示該 Switch 或 Host 與 N-Reporter 開始連結的時間。

按鈕操作

按下  按鈕，彈出搜尋交換機視窗或主機 (如下圖)，輸入欲連結的 Switch 或 Host 設備，或是定義一個搜尋 IP 範圍(CIRD 或是 IP 範圍)，讓 N-Reporter 自行透過 SNMP Polling 的方式查找出範圍內的交換機或主機。SNMP Read Community 資料為必填項目而且需要正確，按下確定鈕系統會開始執行交換機或主機搜尋動作。

為了避免搜尋的動作被誤判定為攻擊行為，N-Reporter 僅支援批次搜尋加入 255 筆交換機或主機。

搜尋的結果將會以列表的方式呈現，勾選欲連結的 Switch 或 Host 設備後，按下「新增」鈕，開始設備新增作業。

若欲新增的 SNMP 設備同時也是 Flow 設備時，需從 Flow 設備進行新增，再回到 SNMP 設備頁面進行屬性編輯，以避免在新增 Flow 設備時發生無法正確加入的狀況。

設備新增注意事項：

(a)「交換機搜尋結果」列表中，「管理狀態」若是「已管理」，表示該設備過去已經加入 N-Reporter 中；若是「暫不支援執行 Action 指令」，則表示使用者無法直接從 N-Reporter 的「事件」列表畫面按右鍵下達 IP 阻擋指令。

(b)「新增或編輯交換機設備」對話視窗中，必須指定「交換機或主機種類」，且一個環境中至少要有一部 L3 交換機，這樣 IP 定位之機制方能順利運作。

(c)「新增或編輯交換機設備」對話視窗中，「SNMP Read Community」資料為必填項目，且輸入值必需正確。

(d)「新增或編輯交換機設備」對話視窗中，「登入帳號」與「登入密碼」為 Telnet 到 L2 Switch 的必要資訊，該帳號的權限要是管理者(Admin)等級，才能讓 N-Reporter 進行 ACL 條件的新增與刪除。

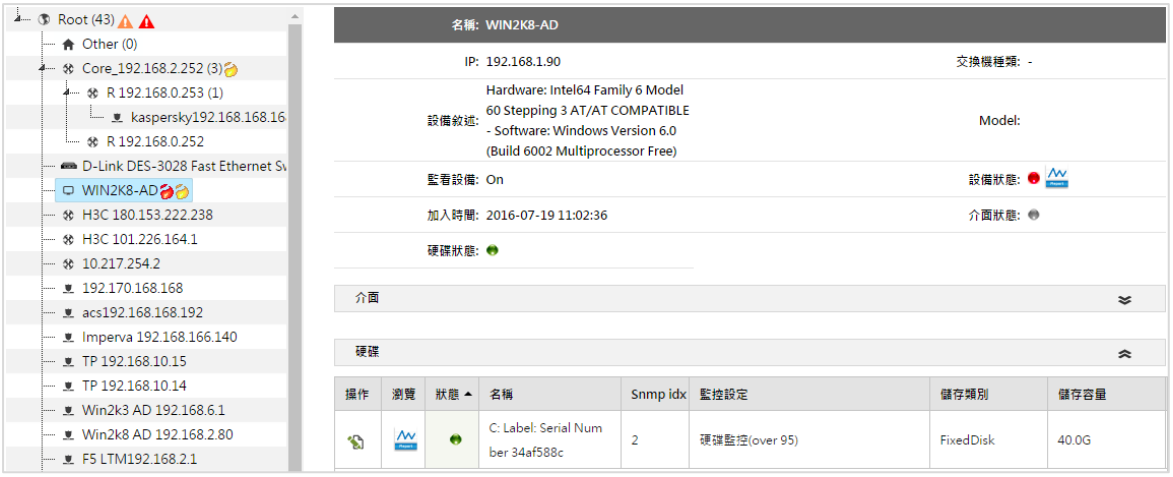
(e) 每新增一部交換機(不論 L2 或 L3)，都會佔去一個「可處理交換機」數量。使用者可透過「系統管理系統資訊 → 運行中/ 可處理 SNMP 監控設備數量」，了解目前所購 License 可以支援的最大「運行 SNMP 監控設備」數以及已使用多少數量。

(f) 如果希望一次新增多部交換機或主機，只要這群交換機或主機的「設備種類」、「Community」與「登入帳號」/「登入密碼」相同，使用者亦可在「搜尋結果列表」中，一次勾選多部交換機或主機加入。

(g) N-Reporter 提供透過 SNMP 擷取交換機或主機(如: Windows/Linux/Unix)CPU/Memory 使用率的功能，除了繪製 CPU/Memory 使用率曲線圖之外，在使用率超過門檻值時還能發送告警。指定監看樣版用來指定套用門檻值的設定。選用監看樣板時，需指定設備 Model，以便在進行 CPU/Memory 使用率抓取時選用正確的 SNMP OID，若不選取 Model 時，預設值為「 “ “」。

由於各廠牌產品之 CPU/Memory 所使用的 SNMP OID 屬於私有的(private) OID，各廠商甚至不同型號的設備可能使用不同的 SNMP OID，因此選取錯誤的 Model 將可能因 CPU/Memory 的使用率無法取得，造成數值恆為零的狀態。

(h) N-Reporter 提供透過 SNMP 方式監控主機硬碟使用率的功能，對於 Windows 主機(如：2003/2008/2012)或 Linux 主機，只要支援 Host MIB 的情況下，即可透過 SNMP 進行硬碟使用率的監控，在使用率超過門檻值時還能發送告警。

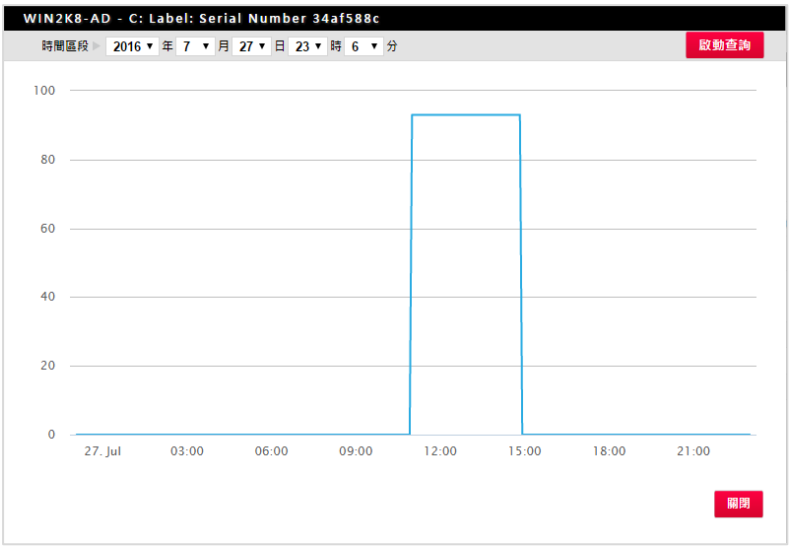


■ 點選 鈕，系統會彈出如下之視窗：

■ 選擇樣板：選擇監看樣版以套用(門檻值)樣版的設定，在硬碟使用率超過門檻值時即可發送告警。有關

監看樣板之設定請參考『2.6 告警樣板』之說明。

■ 點選 鈕，可查看硬碟使用率曲線圖：



Action Module 支援內網端點防護流程說明

(1) N-Reporter 從 Syslog 設備的 Event Log 取得內網惡意 IP 位址。

(2) N-Reporter 透過 SNMP 向 L2/L3 Switch 發送詢問，可得知惡意 IP 目前接在哪台 Switch 的哪個 Interface 上。

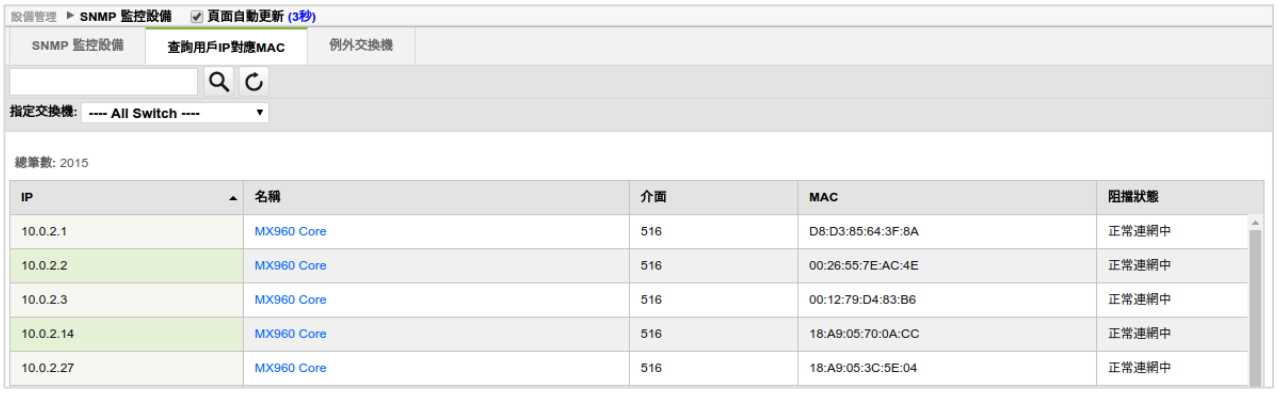
(3) N-Reporter Telnet 到該 L2 Switch 下達 ACL 指令將該惡意 IP 阻擋於所在 Interface 上。

(4) 完成內網端點防護管理。

對於尚未支援 ACL 指令自動下達的 Switch，只要該 Switch 支援 SNMP，N-Reporter 仍可進行關連對應，並將結果顯示「事件」列表中，讓使用者清楚得知內部的惡意 IP 接在哪台 Switch 的哪個 Interface 上，方便進行除錯與管理。

查詢用戶 IP 對應 MAC

為了確認 IP←→MAC←→L2 Switch Interface 的關連是否已被 N-Reporter 正確建立，可以輸入任何界接於已連結 L2 Switch 的用戶 IP 來進行測試，正常的情況下系統應顯示該 IP 所屬的交換機 IP、所在 Interface、該用戶 IP 的 MAC 資料及運作狀態(正常連網中或阻擋中)。為了此功能運作正常，請確認 L3 Switch(Core Switch)及 L2 Switch 的連結資訊皆輸入正確。

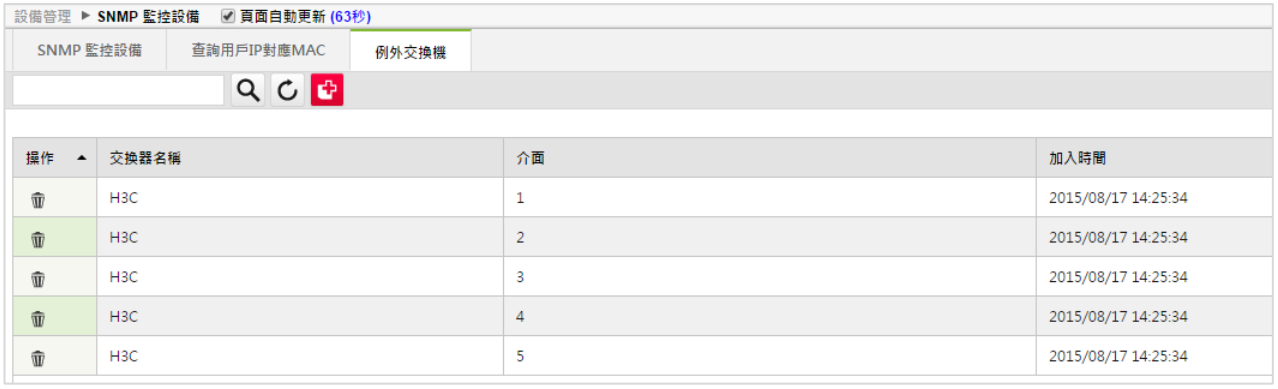


要讓此功能正確運作，必須要同時搭配網路中的管理交換機(L3 Switch)及使用者交換機(L2 Switch)，透過 SNMP 由 L3 交換機可以得知 IP 與 MAC 的對應關係，由 L2 交換機則可以得知 MAC 與 Port 的對應關係。

若資料缺少「IP」欄位表示 L3 資訊不足，若資料缺少「交換機名稱」及「介面」欄位表示 L2 資訊不足。

例外交換機

事件查詢時，可以依交換機上的 IP/MAC 資訊，提示使用者來源 IP/目的 IP 位於哪個交換機的哪個介面，但是在階層式的交換機架構下，IP/MAC 的對應關係可能會同時出現在多部交換機上，因此建議把交換機的上行(Trunk Port)，以及非 Edge 交換機都列為例外交換機。



■ 搜尋列

針對例外交換機列表中來搜尋特定的介面，可輸入交換機名稱(部份或全部)，按下 鈕進行搜尋。

按下 鈕，清除所輸入的查詢條件。

■ 新增例外交換機

按下新增 鈕進行例外交換機手動新增。

■ 指定交換機: 請選擇要新增的例外交換機

■ 新增例外 Port 號: 請輸入要加入的例外介面清單

2.3 Flow 設備

此選項的功能主要在於執行 Flow 輸出設備的新增、已管理之設備的編輯及新增、管理 Flow 路由器(Router)及路由器介面。 由於 Flow 輸出設備通常為網路中擔任重要角色的設備，為強化設備管理，新增 Flow 設備時，會要求輸入 SNMP 相關訊息，以進行 SNMP 設備狀態的監控，並在加入 Flow 設備進行管理的同時也將新增的 Flow 設備新增於 SNMP 設備列表中。因此若要新增進行管理的設備為 Flow 設備，請優先由 Flow 設備管理頁面進行添加。考慮到用戶一開始對報表的操作可能不熟悉，在新增 Flow 設備後，將產生預設的 Top-N 報表，分時監控報表，及分時監控報表群組供用戶編輯使用。

Flow

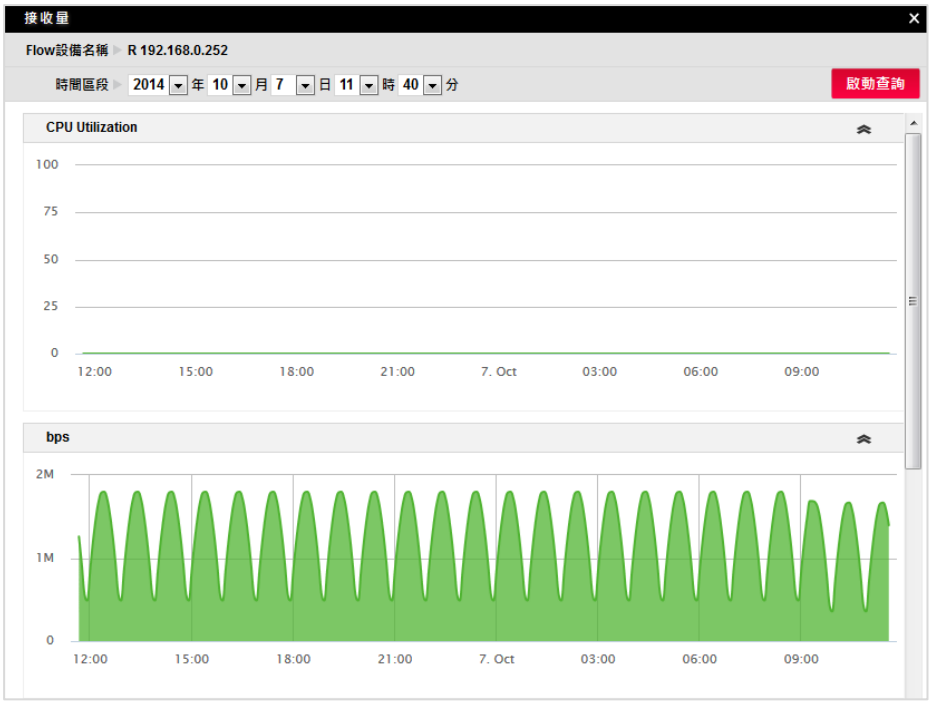
Flow 設備列表

列出所有已管理的 Flow 設備相關資訊。

列表欄位說明如下：

- 操作：點擊 圖示，以編輯該筆 Flow 設備，包括更改「Flow 設備名稱」及「Read/Write Community」。點擊 圖示，則刪除該 Flow 設備(注意，設備刪除後資料將一併刪除，無法回復。移除設備時，請務必三思)。
- 區域：此設備在 SNMP 樹狀圖中所在的位置名稱，方便使用者立即瞭解該設備的地理位置。
- Flow 設備名稱：為使用者自行定義的 Flow 設備名稱，供使用者方便閱讀與辨識用。
- Flow 設備 IP：顯示該 Flow 設備 IP。N-Reporter 接收來自此 IP 的 Flow 流量資料，並列出所屬介面名稱。此 IP 亦為該設備在系統內唯一的識別資訊。
- Flow 設備描述：透過 SNMP Polling 取得 Flow 設備描述。
- Model: 選用交換機的廠牌，如 Cisco。
- 監看設備: 是否啟動 SNMP 監看設備狀態，除了繪製 CPU/Memory 使用率曲線圖之外，在使用率超過門檻值時能即時發送告警。
- 加入時間：顯示該 Flow 設備與 N-Reporter 開始連結的時間。

■ 接收量：點擊 圖示顯示 Flow 設備的接收量曲線圖及 CPU/Memory 使用率。



按鈕操作

■ 按下 鈕，彈出新增或編輯 Flow 設備視窗(如下圖)。依序選擇設備所在的「區域」，輸入「Flow 設備名稱」與「Flow 設備描述」，為了顯示正確，N-Reporter 不接受 Flow 設備名稱重覆，依設備本身所設置的取樣率選擇或輸入「取樣率」。輸入正確的 Community 後，N-Reporter 會自動擷取所屬的介面資訊。

■ N-Reporter 提供透過 SNMP 擷取路由器 CPU/Memory 使用率的功能，除了繪製 CPU/Memory 使用率

曲線圖之外，在使用率超過門檻值時還能發送告警。指定監看設備(監看樣版)用來指定套用門檻值。為了使 SNMP 能正確運作，選擇適當的「Model」可使 N-Reporter 套用正確的 SNMP OID，預設 Model 為 Cisco。勾選「此為交換機」時，則可開啓 IP 對應 MAC Polling 的功能。

N-Reporter 不會限制新增的 Flow 設備總數，Flow Module License 管控系統每秒可接收 Flow 數，欲知該數值請參閱「系統管理➔系統資訊➔可處理 Flow 限速(flow/sec)」。

2.4 介面列表

此功能主要管理介面設定，以及查看介面狀態圖表。

介面列表

■ 搜尋列

針對主機列表中來搜尋特定的介面，可輸入介面名稱(部份或全部)，按下鈕進行搜尋。按下鈕，可以清除輸入的搜尋字串。

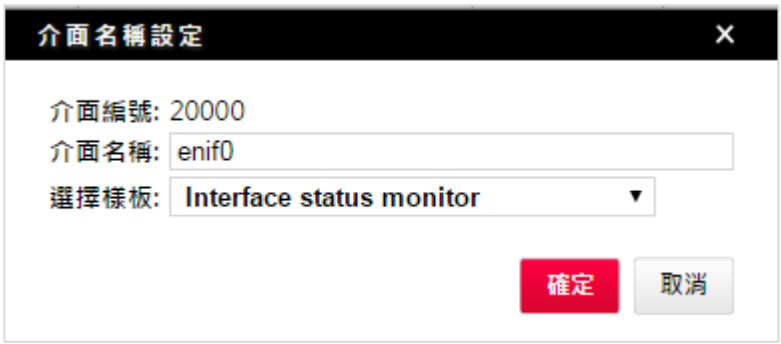
也可以指定設備，列出該設備的所有介面資訊，也可以點選來重新抓取某設備的介面資訊。

■ 介面列表顯示目前所有管理的介面相關資訊。

操作	瀏覽	狀態	設備名稱	介面名稱	介面編號	監控設定	ifspeed	iftype	ifdesc	ifalias
			ZyXEL 192.168.2.252	enif0	20000	Interface status monitor		6(ethernet-csmacd)	enif0	
			ZyXEL 192.168.2.252	swp07	8	Interface status monitor	100M	6(ethernet-csmacd)	swp07	
			ZyXEL 192.168.2.252	swif2	20002			6(ethernet-csmacd)	swif2	
			ZyXEL 192.168.2.252	cmif0	20003			6(ethernet-csmacd)	cmif0	
			ZyXEL 192.168.2.252	swp01	2		100M	6(ethernet-csmacd)	swp01	
			ZyXEL 192.168.2.252	swp03	4		1G	6(ethernet-csmacd)	swp03	
			ZyXEL 192.168.2.252	swp04	5		100M	6(ethernet-csmacd)	swp04	
			ZyXEL 192.168.2.252	swp05	6		1G	6(ethernet-csmacd)	swp05	
			ZyXEL 192.168.2.252	swp06	7		100M	6(ethernet-csmacd)	swp06	

列表欄位說明：

(1) 操作：點擊編輯圖示，可更改「介面名稱」及「告警樣版」

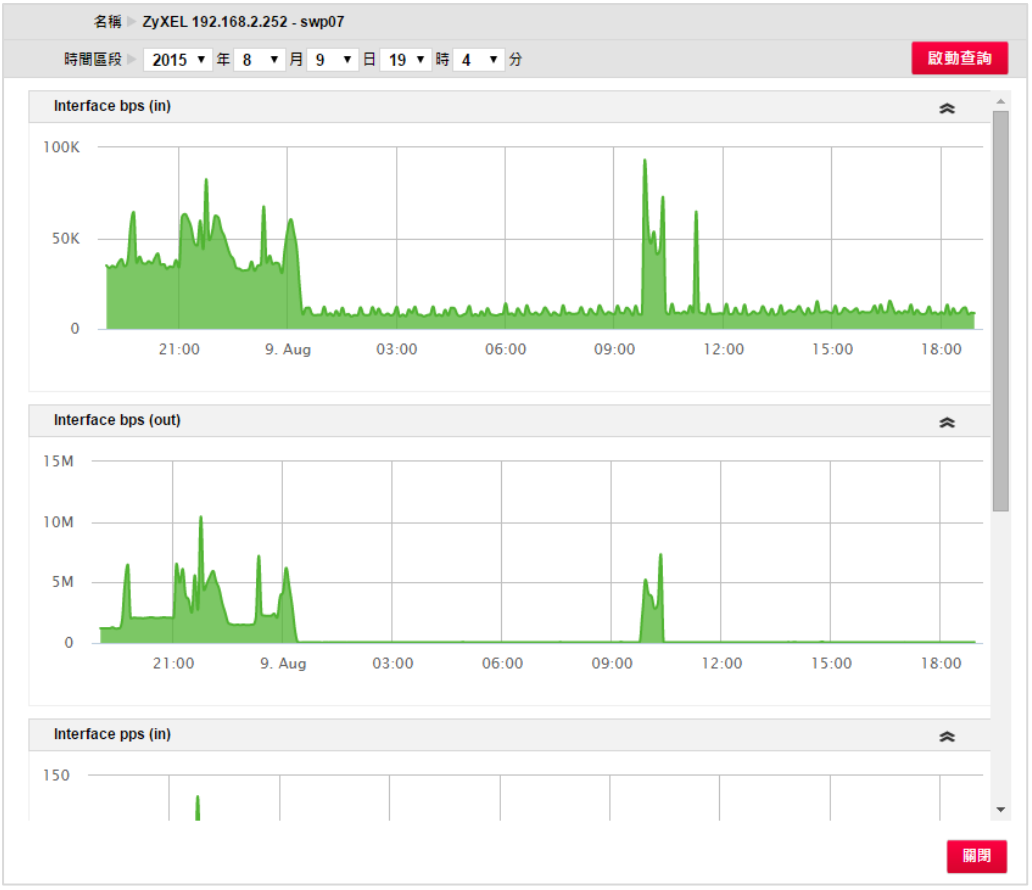


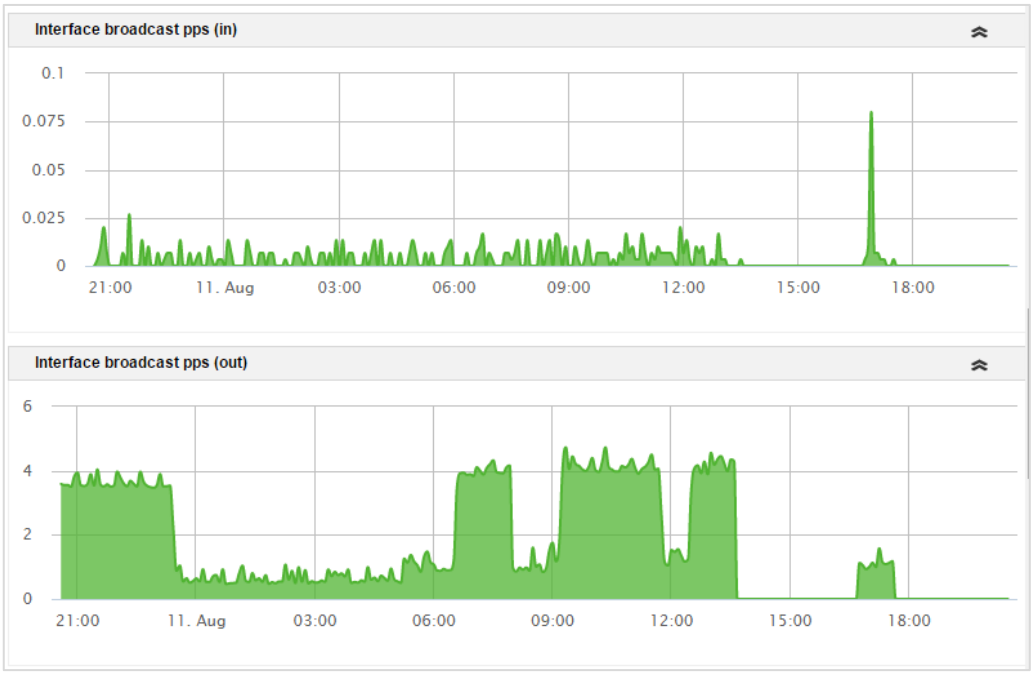
(2) 瀏覽：點擊瀏覽圖示，可以查看介面狀態圖表。必須套用告警樣版並且勾選監控項目，才有相對的圖表。

包含 Interface bps in, bps out, pps in , pps out

Interface broadcast pps in, broadcast pps out

Interface Drop packet in/out, Error packet in/out 等





(3) 設備名稱：所屬設備名稱

(4) 介面編號：SNMP 所抓取的介面編號

(5) 監控設定：所指定的介面告警樣版

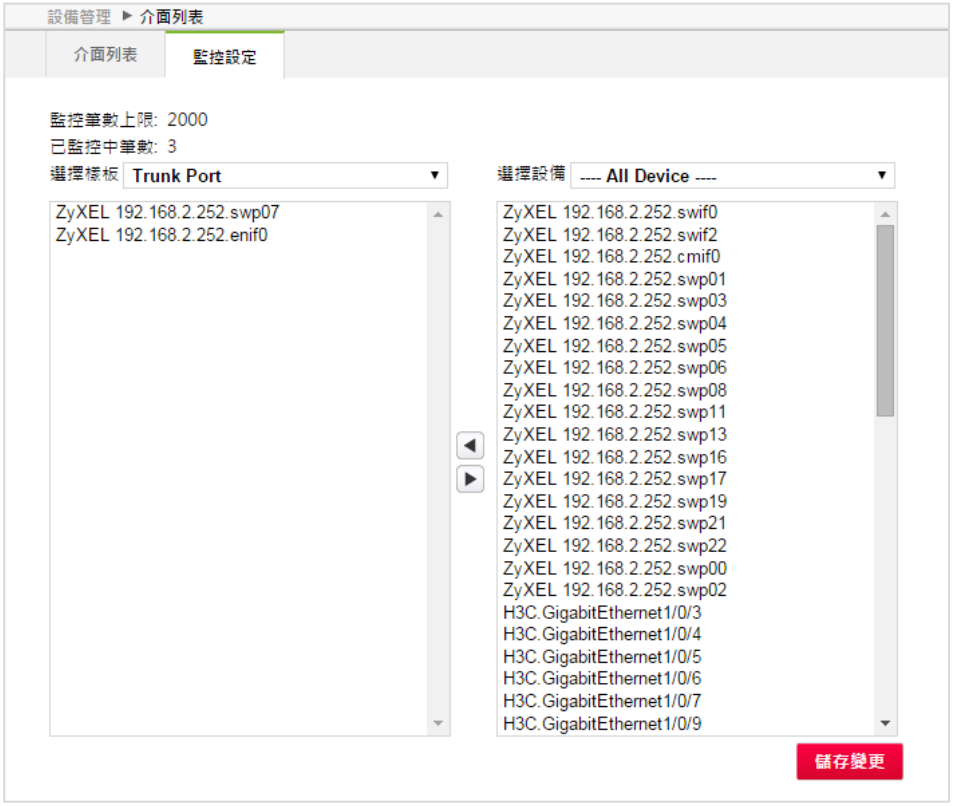
(6) Ifspeed：介面連線速度

(7) Iftype：介面種類

(8) Ifdesc：介面描述

監控設定

此功能提供介面告警樣版套用的查看與批次設定功能。



■ 項目功能說明

(1) 監控筆數上限：系統允許啟動監控的介面數

(2) 已監控中筆數：已啟動的監控介面數

(3) 選擇樣版：可選用於告警樣板中設置的介面告警樣板，並用來套用於被選擇至本欄下方列表的介面以進行監控。

(4) 選擇設備：可選擇已加入監控的 SNMP 設備，選擇設備後，將於本欄下方列表顯示該設備目前可選入進行樣板監控套用的介面列表；預設選擇 All Device，代表顯示所有可進行樣板套用的介面，供使用者選擇。

(5) 已套用樣板列表(選擇樣版欄位下方列表)：可查看目前選擇的樣板所套用的介面列表。於列表中點選介面名稱並按下 ▶ 鍵，可將所選擇的設備由目前選擇的介面監控樣板中移除，並加入可選介面列表中(選擇設備欄位下方列表)。可按住鍵盤上的 Ctrl 鍵，並由滑鼠點選設備進行多選以進行批次移除。

(6) 可套用樣板列表(選擇設備欄位下方列表)，可查看目前選擇的設備上，可被套用於介面監控樣板的介面於列表中。於列表中點選介面名稱並按下 ◀ 鍵，可將所選擇的設備加入目前選擇的介面監控樣板中，並由可選介面列表中移除。可按住鍵盤上的 Ctrl 鍵，並由滑鼠點選設備進行多選以進行批次套用。

當設定完成後，請點選 儲存變更 保留該樣版的設定

注意: 切換樣版前請確認是否已儲存變更，切換樣版時將放棄所有未儲存之設定。

2.5 主 機

針對內網的主機行為進行監控，包含利用 Flow 資料進行 Web 主機行為分析。

Flow

Web

在購買 Flow Module 後，系統會在設備管理項下增加「主機」>>「Web」選項。

利用收集到的 NetFlow/sFlow 資料，N-Reporter 會進行針對 Web 主機的行為分析及異常的偵測，並提供自動偵測網路中 Web 主機的功能。

此功能主要在於 Web 主機設備的新增、編輯及相關設定。

■ 搜尋列

針對主機列表中來搜尋特定的 Web 主機，可輸入主機名稱或 IP，按下 鈕進行搜尋。按下 鈕，清除所輸入的查詢條件。

■ 新增 Web 主機

按下 鈕進行 Web 設備手動新增。

(1) 區域: 指定在 Tree View 中所屬的區域，新增及管理區域請參考『2.2 SNMP 監控設備』章節說明。

(2) 名稱: 輸入可識別的 Web 主機名稱

(3) IP: 輸入單一 IP 或網段，例如 192.168.100.0/24。點選 可將輸入 IP 或網段加入列表中，點選確定 鈕完成設定。

■ 設備列表

顯示目前所有管理的 Web 主機相關資訊。

操作	區域	名稱	IP	最近修改時間	流量圖
	Root	10.1.100.1	10.1.100.1	2015-08-11 16:19:46.518396	
	Factory A	192.168.2.71	192.168.2.71	2015-08-11 16:19:51.848901	
	Factory A	192.168.2.79	192.168.2.79	2015-08-11 16:19:56.409094	
	Factory B	192.168.3.1	192.168.3.1	2015-08-11 16:20:00.710089	
	Factory B	192.168.3.2	192.168.3.2	2015-08-11 16:20:05.302275	
	Factory B	192.168.3.3	192.168.3.3	2015-08-11 16:20:10.719691	
	Factory B	192.168.3.4	192.168.3.4	2015-08-11 16:20:20.379161	
	Factory B	192.168.3.5	192.168.3.5	2015-08-11 16:20:28.578885	

列表欄位說明：

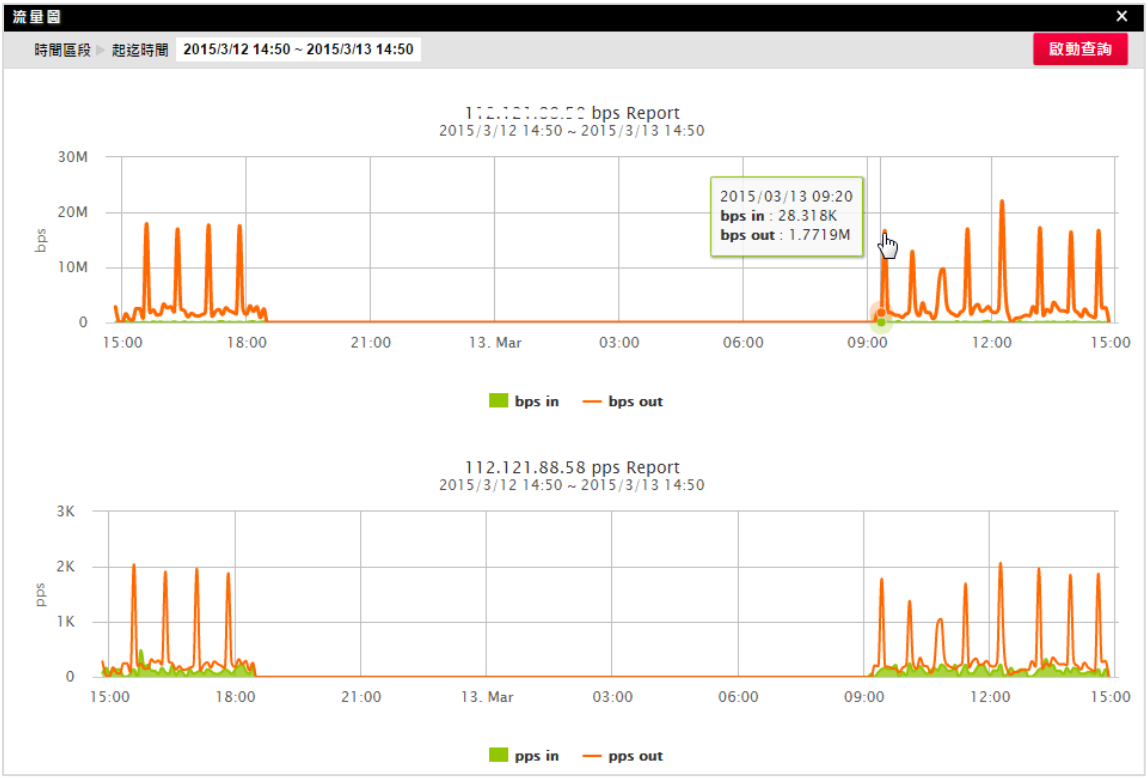
(1) 操作：點擊 圖示，可更改「名稱」及「IP」項目。點擊 圖示，則刪除該 Web 主機。

(2) 名稱：使用者自行定義的 Web 主機名稱，以供使用者方便閱讀與辨識。

(3) IP：顯示該設備所使用的 IP Address。

(4) 最近修改時間：顯示該筆項目最近一次異動的時間。

(5) 流量圖：點擊 圖示，彈出視窗顯示此 Web 主機 pps in/out 及 bps in/out 分時曲線圖。使用者可任意選擇所需的起迄時間進行查詢。滑鼠移至曲線圖任一特定點(如下圖)，系統會顯示該點 pps in/out 及 bps in/out 之流量及時間，若點擊該特定點，則會把該 Web 主機資訊帶入 Top N 報表進行更詳細的追查，其 Drill-Down 查詢功能，可參閱 4.1 Top N 報表章節。

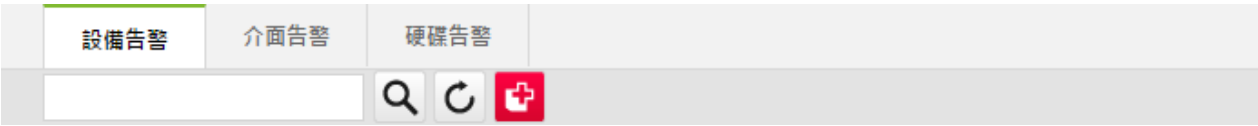


2.6 告警樣板

針對 SNMP 設備監控時異常發送告警的設定，可以針對設備類型(如 Core Switch 或 Edge Switch) 或介面類型(Trunk Port、Line Port 或 WAN Port 等)或硬碟類型(Host)自訂多組不同的設定。修改告警樣版時也能即時套用新設定到所指定的設備、介面及硬碟，提供更有效率的管理。

設備告警

設定「Flow 設備」及「SNMP 監控設備」及「SNMP 主機」的 CPU/Memory 使用率門檻值的告警樣版，可在編輯設備時套用所設定的告警樣版。



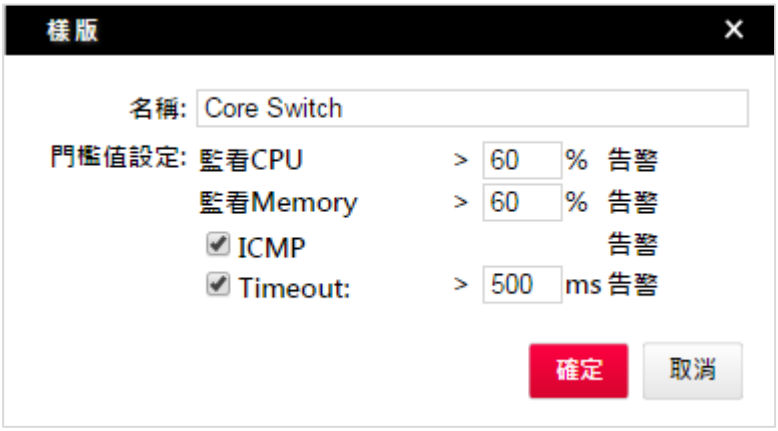
■ 搜尋列

針對告警樣版列表來搜尋特定的樣版設定，可輸入樣版名稱(部份或是全部)，按下 鈕進行搜尋。

按下 鈕，清除所輸入的查詢條件。

■ 新增設備告警樣版

按下新增鈕進行告警樣版手動新增。



(1) 名稱: 告警樣版的識別名稱

(2) 門檻值設定: 可輸入 CPU/Memory 使用率的門檻值，當設備運作使用率超過所輸入的門檻值時發出警示。若只需監控 CPU 狀態，請在 Memory 門檻值處保留空白即可。同時提供 CPU/Memory 使用率分時圖，可在設備列表中進行查看，操作請參考『2.2 SNMP 監控設備』說明。

(3) 勾選 ICMP 告警時，Timeout 值的設定欄位將會顯示，以供設定 Ping Timeout 的時間。系統會在連續 3 次 Ping 設備都未收到回應時，或是回應時間大於所設定的 Timeout 值時，會發送 ICMP 告警

■ 告警樣版列表

顯示目前所有定義的告警樣版列表。

操作	名稱	監看CPU	監看Memory	監看ICMP	建立時間
	Default CPU(50) on, Memory Off, Icmp On	50%		On	2015/07/09 12:10:34
	Core Switch	60%	60%	On , 500 ms	2015/08/12 10:43:00
	Edge Switch	80%	80%	On , 500 ms	2015/08/12 10:43:15

列表欄位說明：

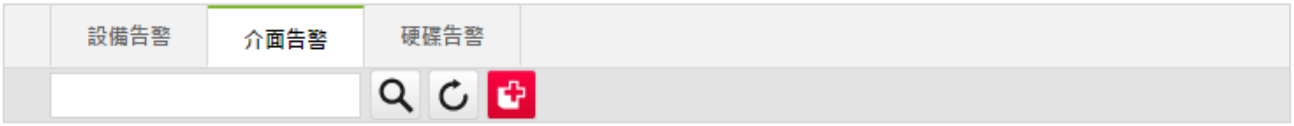
(1) 操作：點擊編輯圖示，可更改「告警樣版」設定項目。點擊刪除圖示，則刪除該筆告警樣版。

(2) 監看 CPU、監看 CPU、監看 ICMP: 門檻值的設定，及是否啟動該項目監控

(3) 建立時間: 告警樣版的建立時間

介面告警

設定「Flow 設備」及「SNMP 監控設備」及「SNMP 主機」的介面監控及告警項目樣版，可在編輯設備時套用所設定的告警樣版。



■ 搜尋列

針對告警樣版列表來搜尋特定的樣版設定，可輸入樣版名稱(部份或是全部)，按下鈕進行搜尋。

按下鈕，清除所輸入的查詢條件。

■ 新增介面告警樣版

按下新增鈕進行告警樣版手動新增。

(1) 名稱: 告警樣版的識別名稱

(2) 介面監控: 監控介面的運作狀況，當 Interface Down 時告警，預設勾選

(3) 門檻值設定: 提供針對介面頻寬使用率、封包數、廣播封包數、封包丟棄數及封包錯誤數設定門檻值，當超過門檻值時發出警示。項目勾選同時提供分時圖，可在介面列表中進行查看，操作請參考『2.4 介面列表』說明。

■ 告警樣版列表

顯示目前所有定義的告警樣版列表。

操作	名稱	介面監控	使用率(%)		封包(pps)		廣播封包(pps)		封包丟棄(Packets)		封包錯誤(Packets)		建立時間
			流入	流出	流入	流出	流入	流出	流入	流出	流入	流出	
	Interface status monitor	Yes	-	-	-	-	-	-	-	-	-	-	2015/07/09 12:10:38
	Trunk Port	Yes	90%	90%	100 K pps	10 K pps	10 K pps	10 K pps	0 packet	0 packet	0 packet	0 packet	2015/07/10 11:21:07

列表欄位說明：

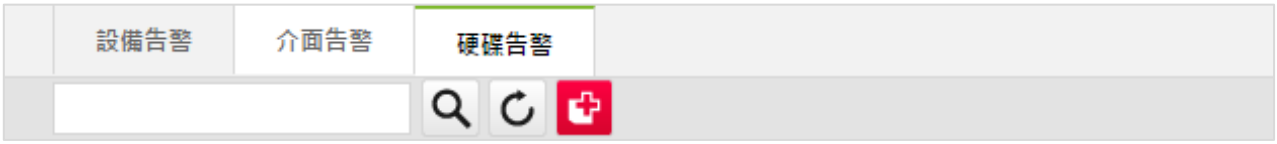
(1) 操作：點擊編輯圖示，可更改「告警樣版」設定項目。點擊刪除圖示，則刪除該筆告警樣版。

(2) 使用率、封包、廣播封包、封包丟棄及封包錯誤: 門檻值的設定，及是否啟動該項目監控

(3) 建立時間: 告警樣版的建立時間

硬碟告警

設定「SNMP 監控設備」其設備種類為 Host 的硬碟使用率門檻值的告警樣版，可在編輯設備時套用所設定的告警樣版。



■ 搜尋列

針對告警樣版列表來搜尋特定的樣版設定，可輸入樣版名稱(部份或是全部)，按下 鈕進行搜尋。

按下 鈕，清除所輸入的查詢條件。

■ 新增設備告警樣版

按下新增鈕 進行告警樣版手動新增。

(1) 名稱: 告警樣版的識別名稱

(2) 門檻值設定: 可輸入硬碟使用率的門檻值，當硬碟使用率超過所輸入的門檻值時發出警示。同時提供硬碟使用率分時圖，可在設備列表中進行查看，操作請參考『2.2 SNMP 監控設備』說明。

■ 告警樣版列表

顯示目前所有定義的告警樣版列表。

操作	名稱 ▲	硬碟使用率	建立時間
	硬碟監控(over 95)	95%	2016/06/30 16:14:42

列表欄位說明：

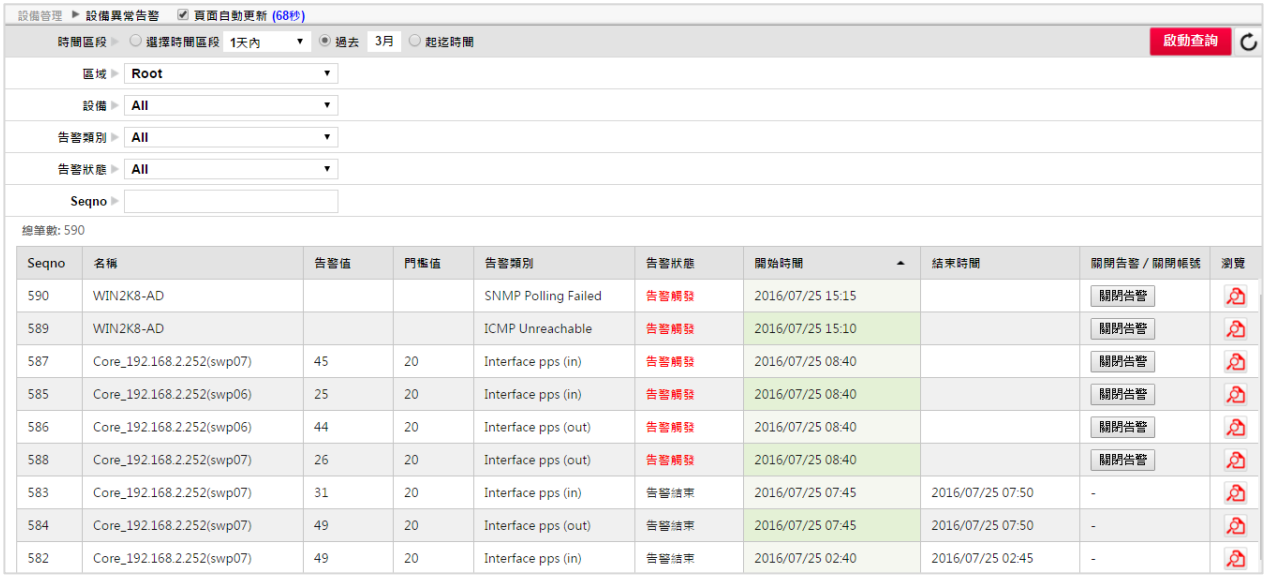
(1) 操作：點擊編輯 圖示，可更改「告警樣版」設定項目。點擊刪除 圖示，則刪除該筆告警樣版。

(2) 硬碟使用率: 門檻值的設定，及是否啟動該項目監控

(3) 建立時間: 告警樣版的建立時間

2.7 設備異常告警

在網路設備有 CPU/Memory 使用率超過門檻值時，通常表示此設備已經有運作異常的徵兆，系統會發送異常告警，讓使用者在網路設備異常影響網路之前，先一步進行處理。



Seqno	名稱	告警值	門檻值	告警類別	告警狀態	開始時間	結束時間	關閉告警 / 關閉帳號	瀏覽
590	WIN2K8-AD			SNMP Polling Failed	告警觸發	2016/07/25 15:15		關閉告警	
589	WIN2K8-AD			ICMP Unreachable	告警觸發	2016/07/25 15:10		關閉告警	
587	Core_192.168.2.252(swp07)	45	20	Interface pps (in)	告警觸發	2016/07/25 08:40		關閉告警	
585	Core_192.168.2.252(swp06)	25	20	Interface pps (in)	告警觸發	2016/07/25 08:40		關閉告警	
586	Core_192.168.2.252(swp06)	44	20	Interface pps (out)	告警觸發	2016/07/25 08:40		關閉告警	
588	Core_192.168.2.252(swp07)	26	20	Interface pps (out)	告警觸發	2016/07/25 08:40		關閉告警	
583	Core_192.168.2.252(swp07)	31	20	Interface pps (in)	告警結束	2016/07/25 07:45	2016/07/25 07:50	-	
584	Core_192.168.2.252(swp07)	49	20	Interface pps (out)	告警結束	2016/07/25 07:45	2016/07/25 07:50	-	
582	Core_192.168.2.252(swp07)	49	20	Interface pps (in)	告警結束	2016/07/25 02:40	2016/07/25 02:45	-	

告警的過濾條件如下

- 區域：以 Treeview 上的區域為條件進行過濾
- 設備：指定單一設備來查詢設備相關的告警
- 告警類別：指定只查詢某類別告警，例如設備類型的告警(如 CPU、ICMP 等) 或介面類型的告警 (如 Interface Utilization 等)
- 告警狀態：指定以「告警觸發」、「告警結束」來過濾告警
- Seqno：可以輸入告警 Seqno 來查詢某特定告警

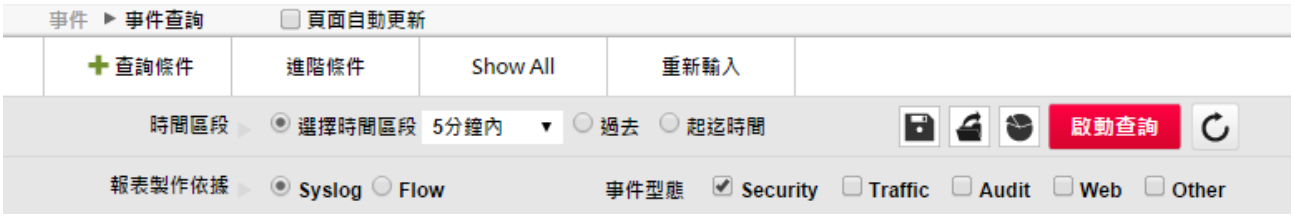
在告警列表中，點選「關閉告警」按鈕可以手動關閉某筆告警，右側  可以查看告警相關的曲線圖(如 CPU/Memory 使用率或介面使用率等)

Chapter 3 事件

在此章節會介紹如何使用本系統的智慧型查詢功能。運用邏輯運算概念，能讓使用者完成各式各樣條件下的查詢工作。

3.1 事件查詢

此選項的功能主要在於對事件下的過濾條件，並依所下的條件來列表。



3.1.1 事件過濾設定

頁面自動更新

當勾選「頁面自動更新」則會以每 2 分鐘(120 秒)刷新此頁面。

畫面快捷

點選畫面查詢條件右側鈕或鈕，可展開或隱藏目前所查詢的事件過濾條件。

查詢條件

點選「查詢條件」，視窗會顯示常用條件，滑鼠移至欲選擇的條件選項，點擊條件選項，即可設定該條件過濾。

進階條件

點選「進階條件」，視窗會顯示進階條件，滑鼠移至欲選擇的條件選項，點擊條件選項，即可設定該條件過濾。

Show All

點選「Show All」即會依照目前所點選的「查詢依據」展開所有相關查詢條件。

重新輸入

清空所有輸入的條件內容。

時間區段

系統提供三種查詢時間區段方式：

(1) 選擇時間區段：從下拉式選項中選擇系統預先定義好的時間區段。

(2) 過去：如下圖，填寫欲查詢的「小時」、「天」、「週」、「月」數字。

(3) 起迄時間：請選擇「起始時間」與「結束時間」。

刪除已選擇條件

點選條件列右方 X ，即可移除設定。

報表製作依據

■ Syslog：點選 Syslog 時，系統會以 IPS 的資訊安全 Syslog 資料為主體進行查詢動作，允許以事件關鍵字、IP、Port、等級等條件搜尋，列出符合條件的最近 10,000 筆資料。

查詢條件有「事件關鍵字」、「使用者名稱」、「Policy ID」、「Session ID」、「IP 過濾」、「Port 過

濾」、「區域過濾」、「介面過濾」、「流量過濾」、「等級」、「動作」及「設備」下拉選項可供使用者設定。

Flow

■ Flow：點選 Flow 時，系統會以 Flow 資料為主體進行查詢動作，允許以 IP、Port 等條件搜尋，列出符合條件的最近 10,000 筆資料。

查詢條件有「使用者名稱」、「IP 過濾」、「Port 過濾」、「區域過濾」、「介面過濾」、「流量過濾」及「設備」下拉選項可供使用者設定。

1. 為增進系統事件查詢、報表呈現效能及延長資料可儲存空間，進而提供好用的 Flow 以及 Syslog 交叉比對分析(Correlation)功能，Traffic 類別的 Syslog 資料(多半由 Firewall 所提供)，將在申裝 Flow Module 後改由 Flow Module 進行接收、儲存以及運用。強烈建議接收取巨量 Traffic 資料的使用者應購買 Flow Module。

2. 預設的查詢依據及各種查詢依據要呈現的欄位，請在「系統管理➔偏好設定」中定義。

▶ 事件型態

■ 本選項需於「報表製作依據」中點選「Syslog」方可使用。

■ 勾選欲查詢的 Syslog 事件型態(可多選)。

■ 全部不勾選表示將查詢所有型態的事件資料(系統預設選項)。

若欲定義預設事件型態，請在「系統管理➔偏好設定」中設定。

▶ 按鈕操作

■ 啟動查詢鈕：系統會依據使用者在事件過濾設定的各種過濾條件來搜尋符合的事件並呈現於下方事件列表中。

■ 鈕：清空所有輸入的條件內容。

■ 「儲存查詢條件」鈕：彈出儲存查詢條件視窗，請輸入一個容易辨識的查詢條件名稱，按下 確定 鈕，系統會把使用者在事件過濾設定的各種過濾條件儲存起來，方便使用者日後欲進行相同條件查詢時，不需再重新輸入過濾參數。使用者可在「事件➔已儲存查詢條件」的已儲存查詢條件列表中找到方才儲存的查詢條件。儲存的查詢條件包含選取的時間範圍，非

必要，建議不儲存起迄時間條件。

- 若要系統定期寄送事件(Off-line 形式離線事件)，使用者可依照實際需求逐一設定事件寄送條件。

  (1) 輸入查詢條件名稱：請輸入一個容易辨識的名稱(如：嚴重資安事件)。

  (2) 寄送型態：告知系統要自動寄送離線事件報表的週期排程(可複選)。其中 1 小時報表為每小時寄送前 1 小時(如：9：00 ~ 9：59)的離線事件 1 次；24 小時報表為每天寄送前 1 天(00：00 ~ 23：59)的離線事件 1 次。

  (3) E-Mail 群組:下拉式選項供使用者選取預先定義的 E-Mail 群組(請參考「系統管理➔系統通報設定➔ 建立 E-Mail 群組」章節)。

  (4) 寄送欄位：請選擇事件欄位(如: 時間、等級、事件、來源 IP...等)

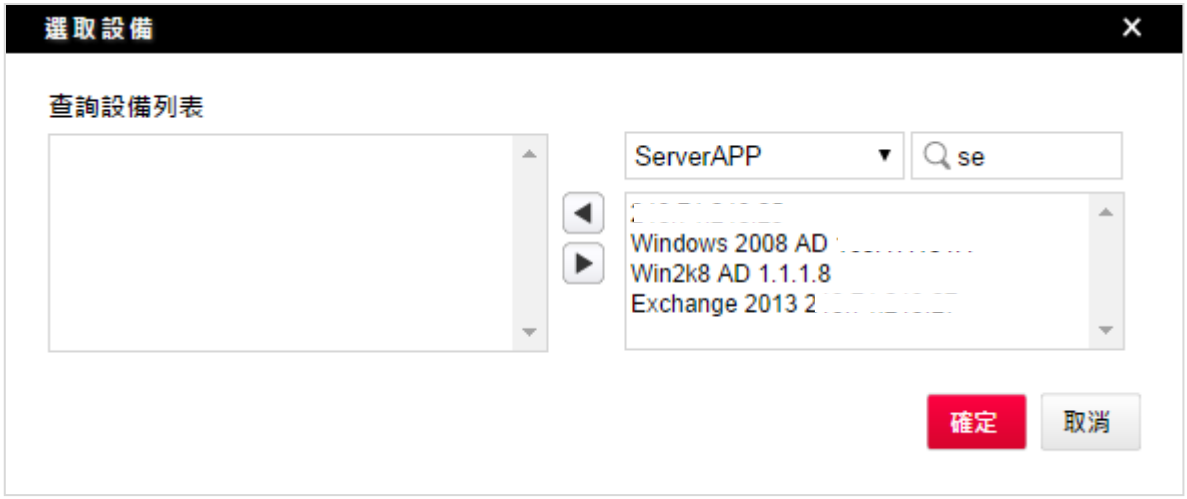
- 「資料輸出」  鈕：彈出匯出事件列表視窗(如下圖所示)，使用者可選擇 PDF、CSV、XML 格式將查詢到的事件列表輸出。

- 「繪製報表」  鈕:則會將查詢到的事件列表透過「Top N 報表」功能加以統計並製作成 Top N 報表，讓使用者不需逐條檢視事件即可得知統計結果。

3.1.2 常用查詢條件說明

設備

- 全部不勾選表示將查詢來自所有設備的 Syslog 或 Flow 資料(系統預設選項)。
- 點選設備格窗或「選取設備」圖示，彈出「選取設備」視窗，在視窗右方提供搜尋功能。可輸入 Syslog 設備所屬資料夾名稱(全部或是部分)作為過濾依據，搜尋結果將呈現在左側的下拉式選項中，以簡化找尋所需條件的流程。
- 在視窗右方點選欲查詢的設備，按下◀鈕，將設備加入左方的「查詢設備列表」(點選時同時按住 Ctrl 鍵，可進行多選，以進行批次處理)；按下▶鈕，則把設備移出「查詢設備列表」。按下 確定 鈕完成設備選取動作，已選取的設備會呈現在設備條件列上。



Syslog

事件關鍵字

- 輸入欲查詢的事件標題字串(全部或是部分)。
- 在字串前輸入「+」，表示欲查詢該字串(邏輯運算中的 OR)；在字串前輸入「!」，表示欲排除該字串(邏輯運算中的 NOT)；系統允許同時輸入多筆「+」與「!」作邏輯運算。

【範例】SQL!MS+P2P+Spyware 表示欲查詢事件標題中含有 SQL、P2P 及 Spyware 字串的事件，但是排除含有 MS 字串的事件。

IP 過濾

- 同時判定來源與目的 IP：使用者可以分別指定要查詢的來源 IP 及目的 IP，系統會過濾符合使用者指定的來源 IP 及目的 IP 的事件(如：來源 IP 設定為 192.168.1.0/24，目的 IP 設定為 Server 區，則表示欲查詢從 192.168.1.0/24 連線到 Server 區的所有事件)。

  點選「同時判定來源與目的 IP」選項後，畫面將向右展開「來源 IP」與「目的 IP」格窗(如下圖所示)，點選格窗最右方箭頭標誌可將格窗收回。

以滑鼠點選「來源 IP」與「目的 IP」任一格窗，彈出「IP 網段過濾條件」視窗，

輸入方式如下：

(1) 單一 IP 或網段：請輸入 CIRD 格式的 IP 條件(如：192.168.1.0/24)。

(2) IP 範圍：請輸入 IP 區間。

(3) 名稱解析：提供下拉式選項供使用者選取預先定義的 IP 條件(請參考「系統管理➔名稱解析」章節)。右方則提供名稱解析搜尋功能，可輸入網段名稱(全部或是部分)作為過濾依據，搜尋結果將呈現在左側的下拉式選項中，以簡化在大量名稱解析資料中找尋所需條件的流程。

各欄位設定完後，按下鈕，將上述 IP 條件加入條件列表中，可加入多筆 IP 過濾條件(邏輯運算中的 OR)。按下鈕，則會排除上述 IP 條件(邏輯運算中的 NOT)。點選 IP 條件列表中的任一筆資料按下鈕或鈕，可以執行該筆 IP 條件的修改與刪除動作。若使用「名稱解析」作為 IP 過濾條件時，則不能進行編輯動作，只能移除。按下 確定 鈕完成 IP 過濾條件的輸入動作。

■ 判定來源或目的 IP：使用者可以針對特定 IP 作為事件過濾條件，不論該特定 IP 是出現在來源端或是目的端，系統都會呈現出來(如：IP 設定為台北辦公室，則表示無論事件的來源端是台北辦公室或是目的端是台北辦公室，系統都會查找出來。如果 IP 設定為排除[!]192.168.1.0/24，則表示要濾掉所有從 192.168.1.0/24 到 192.168.1.0/24 的事件，此用法是在查詢事件時，不需要看到某網段內對內的事件)。

點選「判定來源或目的 IP」選項後，畫面將向右展開「IP」格窗(如下圖)，點選格窗最右方箭頭標誌可將格窗收回。

以滑鼠點選「IP」格窗，彈出「IP 網段過濾條件」視窗，使用者可在視窗中進行條件設定(作法請參考「IP 過濾➔同時判定來源與目的 IP」)。

Port 過濾

- 同時判定來源與目的 Port：使用者可以分別指定要查詢的來源 Port 及目的 Port，系統會過濾符合使用者指定的來源 Port 及目的 Port 的事件(如：來源 Port 設定為 TCP:80，目的 Port 設定為 TCP:5335，則表示欲查詢從 TCP:80 到 TCP:5335 的所有事件)。

  點選「同時判定來源與目的 Port」選項後，畫面將向右展開「來源 Port」與「目的 Port」格窗(如下圖)，點選格窗最右方箭頭標誌可將格窗收回。

  以滑鼠點選「來源 Port」與「目的 Port」任一格窗，彈出「Port 過濾」視窗(如下圖)，輸入方式如

下：

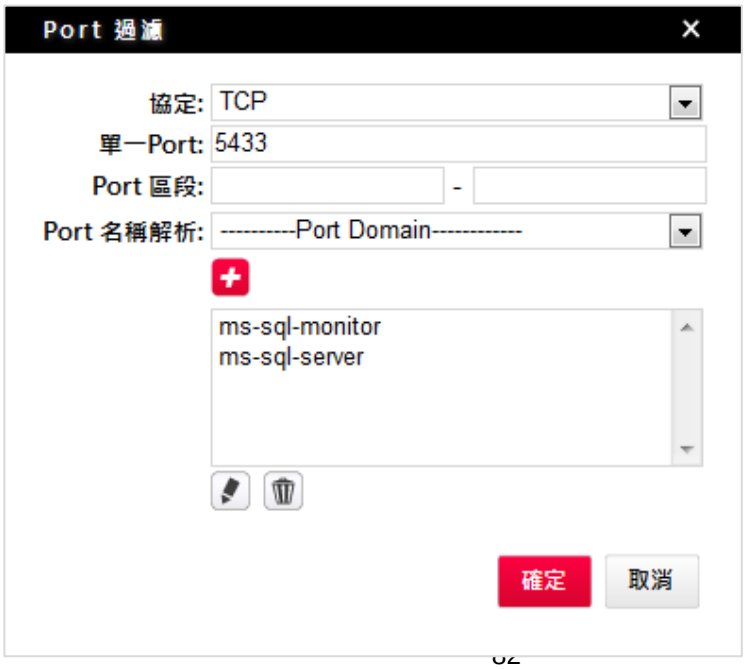
(1) 協定：下拉式視窗，請選擇 Any、TCP、UDP 或 ICMP。

(2) 單一 Port：請輸入單一 Port 號。

(3) Port 區段：請輸入連續 Port 區間之起迄 Port 號。

(4) Port 名稱解析：提供下拉式選單供使用者選取預先定義的 Port 條件

(請參考「系統管理➔Port 名稱解析」章節)。



各欄位設定完後，按下鈕，將上述 Port 條件加入條件列表中，可加入多筆 Port 過濾條件(邏輯運算中的 OR)。點選 Port 條件列表中的任一筆資料按下鈕或鈕，可以執行該筆 Port 條件的修改與刪除動作。按下 確定鈕完成 Port 過濾條件的輸入動作。

- 判定來源或目的 Port：使用者可以針對特定 Port 作為事件過濾條件，不論該特定 Port 是出現在來源端或是目的端，系統都會呈現出來(如：Port 設定為 TCP:80，則表示無論事件的來源端是 TCP:80 或是目的端是 TCP:80，系統都會查找出來)。

  點選「判定來源或目的 Port」選項後，畫面將向右展開「Port」格窗(如下圖)，點選格窗最右方箭頭標誌可將格窗收回。

  以滑鼠點選「Port」格窗，彈出「Port 過濾」視窗，使用者可在視窗中進行條件設定(作法請參考上述「同時判定來源與目的 Port」)。

Syslog ▶ 動作

- 勾選「允許」表示 Permit、Allow、Trust、Pass 或 Monitor 等意義。
- 勾選「阻擋」表示 Block 或 Deny 等意義。
- 全部不勾選表示將查詢所有動作的事件資料(系統預設選項)。

Syslog ▶ 等級

- 勾選欲查詢的事件等級(可多選)。
- 全部不勾選表示將查詢所有等級的事件資料(系統預設選項)。

「動作」、「等級」條件需於「報表製作依據」中點選「Syslog」方可使用。

3.1.3 進階查詢條件說明

Syslog 表示僅供選填syslog依據時查詢；Flow 表示僅供選填Flow依據時查詢。

Syslog 應用服務

- 資安設備判別出使用者的應用服務時會送出此資訊，如「YouTube」、「Netbios」等。
- 輸入欲查詢的應用服務標題字串（全部或是部分）。
- 在字串前輸入「+」，表示欲查詢該字串（邏輯運算中的 OR)；在字串前輸入「!」，表示欲排除該字串 (邏輯運算中的 NOT)；系統允許同時輸入多筆「+」與「!」作邏輯運算。

使用者名稱

- 將同時過濾找出符合「來源使用者」、「目的使用者」、「Audit User」等欄位的事件。
- 在 IP 動態分配的環境中，搭配 Windows AD 的 LOG，可以用「使用者名稱」為條件來查詢流量及資安事件。
- 輸入欲查詢的使用者名稱字串，愈完整的名稱字串，愈能找出符合的結果。可勾選 Full Match 以查找和輸入條件完全符合的使用者。
- 不輸入表示查詢所有使用者名稱的事件 (系統預設選項)。

時間範圍

使用者能指定查詢每日多個時間區段或者起迄時間。

【範 例】查詢一週內上班時段事件，時間範圍設定 9:00~12:00，13:00~18:00。

Syslog Policy ID

- 以防火牆允許 / 阻擋的 Policy ID 作為過濾條件。
- 輸入欲查詢的 Policy ID 字串(全部或是部分)。
- 在字串前輸入「+」，表示欲查詢該字串(邏輯運算中的 OR)；可同時輸入多筆「+」作邏輯運算；在字串前輸入「!」，表示欲排除該字串（邏輯運算中的 NOT)。系統允許同時輸入多筆「+」與「!」作邏輯運算。
- 不輸入表示查詢所有 Policy ID 的事件(系統預設選項)。

【範 例】allow_web+deny_stock 表示查詢所有 Policy ID 包含 allow_web 或 deny_stock 的事件。

Protocol

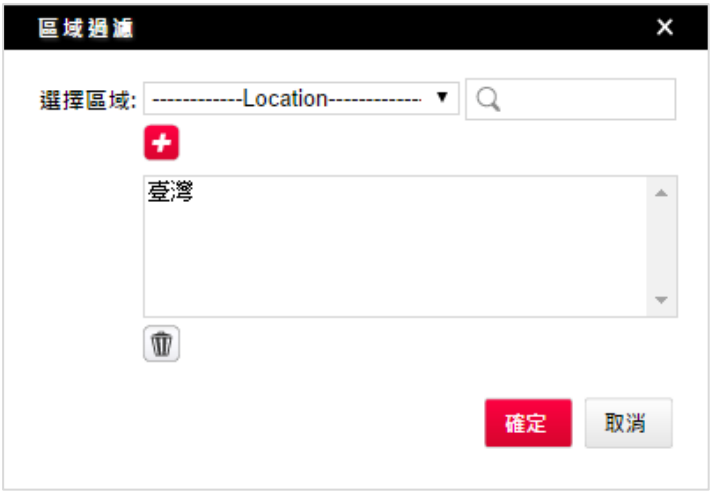
指定網路協定 Protocol 為過濾條件，請選取下拉式選單指定 Protocol，不選取 Protocol 表示查詢所有 Protocol 的事件。

區域過濾

- 同時判定來源與目的區域：使用者可以分別指定要查詢的來源區域及目的區域，系統會過濾符合使用者指定的來源區域及目的區域的事件(如：來源區域設定為臺灣，目的區域設定為香港，則表示欲查詢從臺灣到香港的所有事件)。

  點選「同時判定來源與目的區域」選項後，畫面將向右展開「來源區域」與「目的區域」格窗(如下圖)，點選格窗最右方箭頭標誌可將格窗收回。

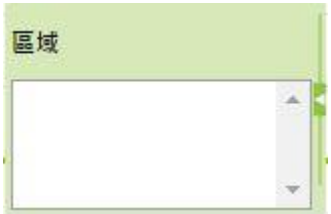
  以滑鼠點選「來源區域」與「目的區域」任一格窗，彈出「區域過濾」視窗(如下圖)。



  系統提供下拉式選單供使用者選擇欲查詢的區域名稱。右方則提供區域搜尋功能，可輸入區域名稱(全部或是部分)或國名縮寫(如：輸入 臺灣 或 tw)作為過濾依據，搜尋結果將呈現在左側的下拉式選單中，以簡化在大量區域資料中找尋所需條件的流程。按下  鈕，將上述區域條件加入條件列表中，可加入多筆區域過濾條件(邏輯運算中的 OR)。點選區域條件列表中的任一筆資料按下  鈕，可以執行該筆區域條件的刪除動作。按下確定鈕完成區域過濾條件的輸入動作。

- 判定來源或目的區域：使用者可以針對特定區域作為事件過濾條件，不論該特定區域是出現在來源端或是目的端，系統都會呈現出來(如：區域設定為臺灣，則表示無論事件的來源端是臺灣或是目的端是臺灣，系統都會查找出來)。

  點選「判定來源或目的區域」選項後，畫面將向右展開「區域」格窗(如下圖)，點選格窗最右方箭頭標誌可將格窗收回。



回目錄

以滑鼠點選「區域」格窗，彈出「區域過濾」視窗，使用者可在視窗中進行條件設定(作法請參考上述「同時判定來源與目的區域」)。

流量過濾

- 勾選「總流量(bytes)」，可以找出總流量大於、小於或等於使用者所設定流量的 Syslog/Flow 資料。
- 勾選「總封包數(packets)」，可以找出總封包數大於、小於或等於使用者所設定封包數的 Syslog/Flow 資料。

封包大小

指定封包大小，通常用來查詢海量小封包攻擊行為(<64byte)，或是鎖定特定封包大小的攻擊行為。

Syslog

主機名稱

- 查詢來源主機名稱及目的主機名稱。系統可以透過 DNS 方式或 Netbios 方式來取得內部 IP 的主機名稱，請在「偏好設定」的「主機名稱」中設定。
- 輸入欲查詢的使用者名稱字串 (全部或是部分)。可勾選 Full Match 以查找和輸入條件完全符合的項目。
- 在字串前輸入「+」，表示欲查詢該字串 (邏輯運算中的 OR)；在字串前輸入「!」， 表示欲排除該字串 (邏輯運算中的 NOT)；系統允許同時輸入多筆「+」與「!」作邏輯運算。
- 不輸入表示查詢所有主機名稱的事件 (系統預設選項)。

【 範 例 】 webportal+database 表示查詢所有主機名稱包含 webportal 或 database 的事件。

Syslog

寄件者

- 適用於過濾郵件主機或 Spam Mail LOG 中的寄件者。
- 不輸入表示查詢所有寄件者的事件 (系統預設選項)。
- 在字串前輸入「+」，表示欲查詢該字串 (邏輯運算中的 OR)；在字串前輸入「!」， 表示欲排除該字串 (邏輯運算中的 NOT)；系統允許同時輸入多筆「+」與「!」作邏輯運算。

Syslog

收件者

- 適用於過濾郵件主機或 Spam Mail LOG 中的收件者。
- 不輸入表示查詢所有收件者的事件 (系統預設選項)。
- 在字串前輸入「+」，表示欲查詢該字串 (邏輯運算中的 OR)；在字串前輸入「!」， 表示欲排除該字串 (邏輯運算中的 NOT)；系統允許同時輸入多筆「+」與「!」作邏輯運算。

Syslog

MAC

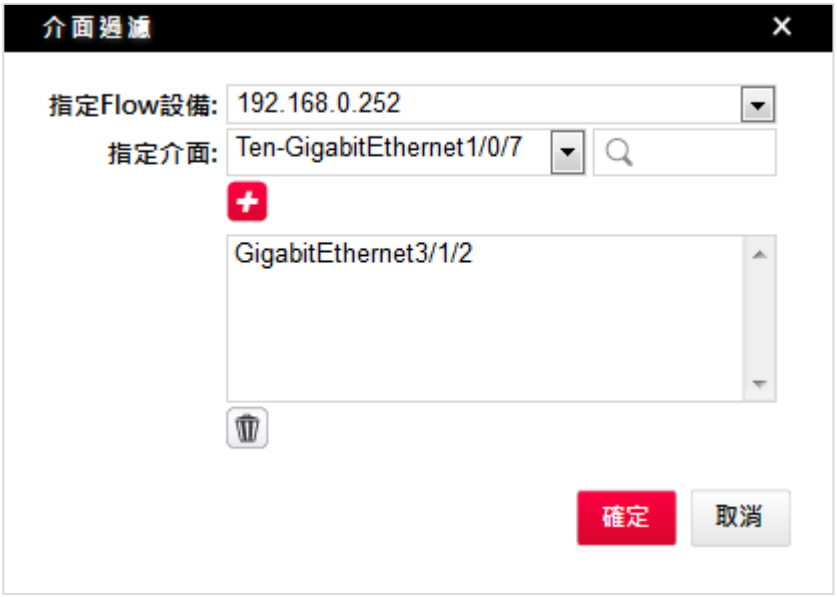
- 指定要查詢的完整 MAC 資訊，例如 98:e7:9a:2c:00:00。
- 不輸入表示查詢所有 MAC 的事件 (系統預設選項)。

介面過濾

- 同時判定流入與流出介面：使用者可以分別指定要查詢的流入介面及流出介面，系統會過濾符合使用者指定的流入介面及流出介面的事件。

  點選「同時判定流入與流出介面」選項後，畫面將向右展開「流入介面」與「流出介面」格窗(如下圖)，點選格窗最右方箭頭標誌可將格窗收回。

- 「報表製作依據」中點選**「Flow」**選項時，以滑鼠點選「流入介面」與「流出介面」任一格窗，彈出「介面過濾」視窗(如下圖)。



輸入方式如下：

(1) 指定 Flow 設備：下拉式視窗，請選擇欲查詢的 Flow 設備。

(2) 指定介面：下拉式視窗，請選擇欲查詢的介面。右方則提供介面搜尋功能，可輸入介面名稱(全部或是部分)。

各欄位設定完後，按下  鈕，將上述介面條件加入條件列表中，可加入多筆介面過濾條件(邏輯運算中的 OR)。點選介面條件列表中的任一筆資料按下  鈕，可以執行該筆介面條件的刪除動作。按下 確定 鈕完成介面過濾條件的輸入動作。

Syslog ■ 「報表製作依據」中點選「**Syslog**」選項時，以滑鼠點選「流入介面」與「流出介面」任一格窗，彈出「介面過濾」視窗(如下圖所示)。

請在「介面名稱關鍵字」欄輸入欲查詢的介面名稱(部份或全部)，按下鈕，將上述介面條件加入條件列表中，可加入多筆介面過濾條件(邏輯運算中的 OR)。點選介面條件列表中的任一筆資料按下鈕，可以執行該筆介面條件的刪除動作。按下 確定 鈕完成介面過濾條件的輸入動作。

■ 判定流入或流出介面：使用者可以針對特定介面作為事件過濾條件，不論該特定介面是出現在流入端或是流出端，系統都會呈現出來。

點選「判定流入或流出介面」選項後，畫面將向右展開「介面」格窗(如下圖)，點選格窗最右方箭頭標誌可將格窗收回。

以滑鼠點選「介面」格窗，彈出「介面過濾」視窗，使用者可在視窗中進行條件設定(作法請參考上述「同時判定流入與流出介面」)。

1.「介面過濾」視窗的「指定 Flow 設備」及「指定介面」選項，需於「報表製作依據」中點選「Flow」方可使用。

2.「介面過濾」視窗的「介面名稱關鍵字」選項，需於「報表製作依據」中點選「Syslog」方可使用。

Syslog ▶ **路徑**

■ 指定要查詢的路徑資訊(全部或部份)

■ 不輸入表示查詢所有路徑的事件 (系統預設選項)。

■ 在字串前輸入「+」，表示欲查詢該字串 (邏輯運算中的 OR)；在字串前輸入「!」， 表示欲排除該

字串 (邏輯運算中的 NOT)；系統允許同時輸入多筆「+」與「!」作邏輯運算。

Syslog

作業系統

- 指定要查詢的作業系統資訊(全部或部份)
- 不輸入表示查詢所有作業系統的事件 (系統預設選項)。
- 在字串前輸入「+」，表示欲查詢該字串 (邏輯運算中的 OR)；在字串前輸入「!」， 表示欲排除該字串 (邏輯運算中的 NOT)；系統允許同時輸入多筆「+」與「!」作邏輯運算。

Syslog

分類

- 指定要查詢的類型資訊(全部或部份)
- 不輸入表示查詢所有類型的事件 (系統預設選項)。
- 在字串前輸入「+」，表示欲查詢該字串 (邏輯運算中的 OR)；在字串前輸入「!」， 表示欲排除該字串 (邏輯運算中的 NOT)；系統允許同時輸入多筆「+」與「!」作邏輯運算。

Syslog

狀態

- 指定要查詢的狀態資訊(全部或部份)
- 不輸入表示查詢所有狀態的事件 (系統預設選項)。
- 在字串前輸入「+」，表示欲查詢該字串 (邏輯運算中的 OR)；在字串前輸入「!」， 表示欲排除該字串 (邏輯運算中的 NOT)；系統允許同時輸入多筆「+」與「!」作邏輯運算。

Syslog

無線基地台

- 指定要查詢的無線基地台名稱(全部或部份)
- 不輸入表示查詢所有狀態的事件 (系統預設選項)。
- 在字串前輸入「+」，表示欲查詢該字串 (邏輯運算中的 OR)；在字串前輸入「!」， 表示欲排除該字串 (邏輯運算中的 NOT)；系統允許同時輸入多筆「+」與「!」作邏輯運算。

Syslog

AP SSID

- 指定要查詢的完整 AP SSID
- 不輸入表示查詢所有 AP SSID 的事件 (系統預設選項)。

Syslog

Session ID

- 以 Session ID 作為過濾條件。
- 輸入欲查詢的 Session ID 字串(請輸入完整 Session ID)。
- 不輸入表示查詢所有 Session ID 的事件(系統預設選項)。

Syslog

回應時間

使用者可以指定回應時間(單位是 msec)，系統會過濾符合使用者指定的回應時間範圍的事件。

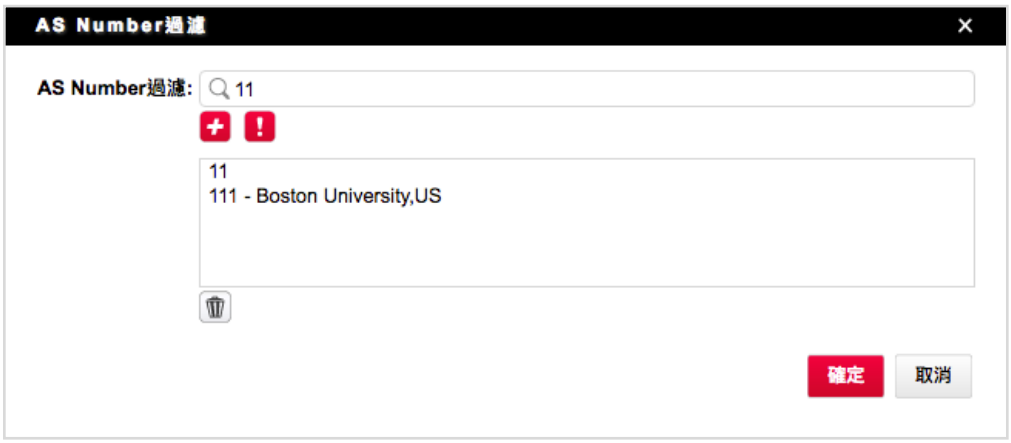
Flow

AS Number 過濾

■ 同時判定來源目的 AS Number： 使用者可以分別指定來源 AS 及目的 AS，系統會過濾符合使用者指定來源 AS 及目的 AS 的事件。(如 ： 來源 AS 設定為 111 - Boston University,US，目的 AS 設定為 5554 - Integra Zrt.,HU，則表示欲查詢從來源 AS 111 到目的 AS 5554 的所有事件)。點選「同時判定來源與目的 AS Number」選項後，畫面將向右展開「來源 AS」與「目的 AS」格窗 (如下圖)，點選格窗最右方箭頭標誌可將格窗收回。

以滑鼠點選「來源 AS」與「目的 AS」任一格窗，彈出「AS Number 過濾」視窗 (如下圖)， 輸入方式如下：

■ AS Number 過濾：請輸入要過濾的 AS Number 條件(可輸入部分或全部的關鍵字如 11 或 111 - Boston University,US)。

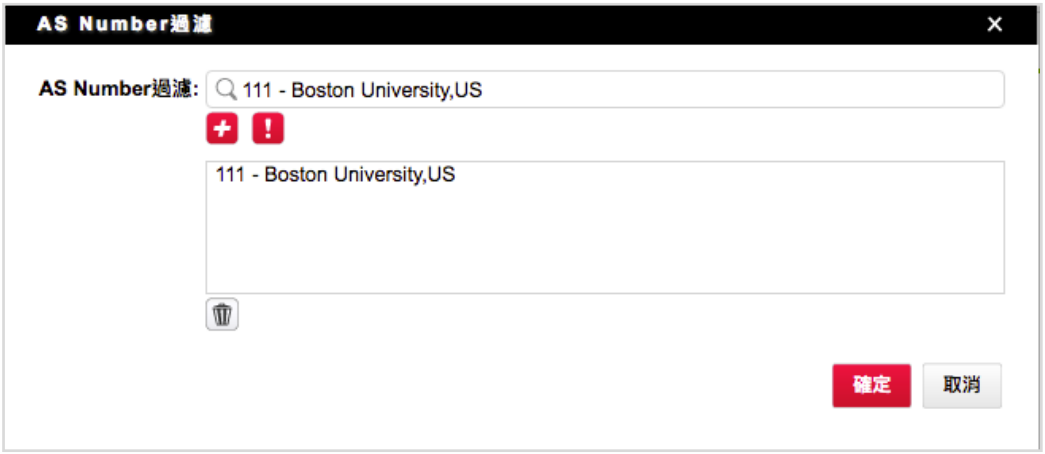


各欄位設定完後，按下 鈕，將上述 AS Number 條件加入條件列表中，可加入多筆 AS Number 過濾條件 (邏輯運算中的 OR) 按下 鈕，則會排除上述 AS Number 條件 (邏輯運算中的 NOT)。

點選 AS Number 條件列表中的任一筆資料按下 鈕，可以執行該筆 AS Number 條件的修改與刪除動作。

按下 確定 鈕完成 AS Number 過濾條件的輸入動作。

- 判定來源或目的 AS Number： 使用者可以針對特定 AS Number 作為事件過濾條件，不論該特定 AS Number 是出現在來源端或是目的端，系統都會呈現出來（ 如：AS Number 設定為 111 - Boston University,US，則表示無論事件的來源端是 111 - Boston University,US 或是目的端是 111 - Boston University,US，系統都會查找出來。 如果 AS Number 設定為排除 [!] 111 - Boston University,US，則表示要濾掉所有從 AS Number=111 - Boston University,US 到 AS Number =111 - Boston University,US 的事件。 點選「判定來源或目的 AS Number」選項後，畫面將向右展開「AS Number 過濾」格窗（ 如下圖 ），點選格窗最右方箭頭標誌可將格窗收回。



- 以滑鼠點選「AS Number 過濾」格窗，彈出「AS Number 過濾」視窗，使用者可在視窗中進行條件設定（ 作法請參考上述「AS Number 過濾 ➔ 同時判定來源與目的 AS Number」）。

Flow ▶ TCP Flags

- TCP Flags：可勾選 URG|ACK|PSH|RST|SYN|FIN 等 TCP Flag 欲進行搜尋 TCP 的 Flow 資訊中含有所勾選的 Flag 的 Flow 資料並列表，單獨勾選不會排除該 Flow 資訊含有其他未勾選 Flag 的 Flow 資料。
- Mask : 同樣可勾選 URG|ACK|PSH|RST|SYN|FIN 等 TCP Flag，主要目的是用來進行排除結果中含有其他 Flag 時，可利用來排除同時具有其他 TCP Flag 的資料，例如希望只看到有 TCP ACK 的 Flow 資料，在選擇了 TCP ACK Flag 查詢之後，看到的 Flow 資料看到含有 TCP ACK|PSH Flag，想將 TCP PSH Flag 從查詢結果中剔除，可勾選 Mask TCP PSH Flag 後再進行詢，結果則會呈現僅有 TCP ACK Flag 的 Flow 資料。

3.1.4 事件列表

事件列表

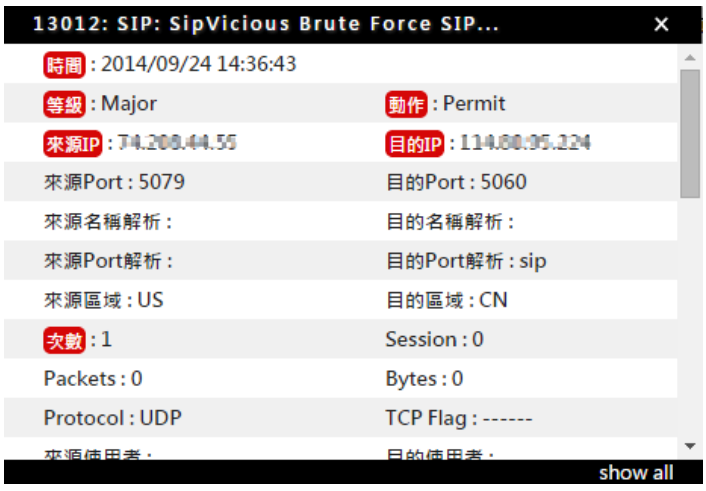
時間	事件	來源IP	來源Port	來源名稱解析	來源區域	目的IP	目的Port	目的名稱解析	目的區域	來源MAC	Protocol
2014/09/24 14:36:43	13012: SIP: SipVicious Brute Force SIP Tool	74.208.44.55	5079		US	114.80.95.227	5060		CN		UDP
2014/09/24 14:36:43	13012: SIP: SipVicious Brute Force SIP Tool	74.208.44.55	5079		US	114.80.95.226	5060		CN		UDP
2014/09/24 14:36:43	13012: SIP: SipVicious Brute Force SIP Tool	74.208.44.55	5079		US	114.80.95.224	5060		CN		UDP
2014/09/24 14:36:43	13012: SIP: SipVicious Brute Force SIP Tool	74.208.44.55	5079		US	114.80.95.227	5060		CN		UDP

- 事件列表之欄位包含：「事件」、「設備」、「等級」、「時間」、「來源 IP」、「來源 Port」、「目的 IP」、「目的 Port」、「來源名稱解析」、「目的名稱解析」、「來源區域」、「目的區域」、「動作」、「次數」、「事件型態」、「Packets」、「Bytes」、「Protocol」、「NAT 來源 IP」、「NAT 來源 Port」、「NAT 目的 IP」、「NAT 目的 Port」、「流入介面」、「流出介面」、「Policy ID」、「Session ID」、「來源 IP 所在交換機/介面」、「目的 IP 所在交換機/介面」、「Session」。
- 使用者可依據閱讀喜好搬移欄位的相對位置，將滑鼠移至欲搬移的事件列表表頭任一項目標題，按住左鍵後拖曳至任意位置。

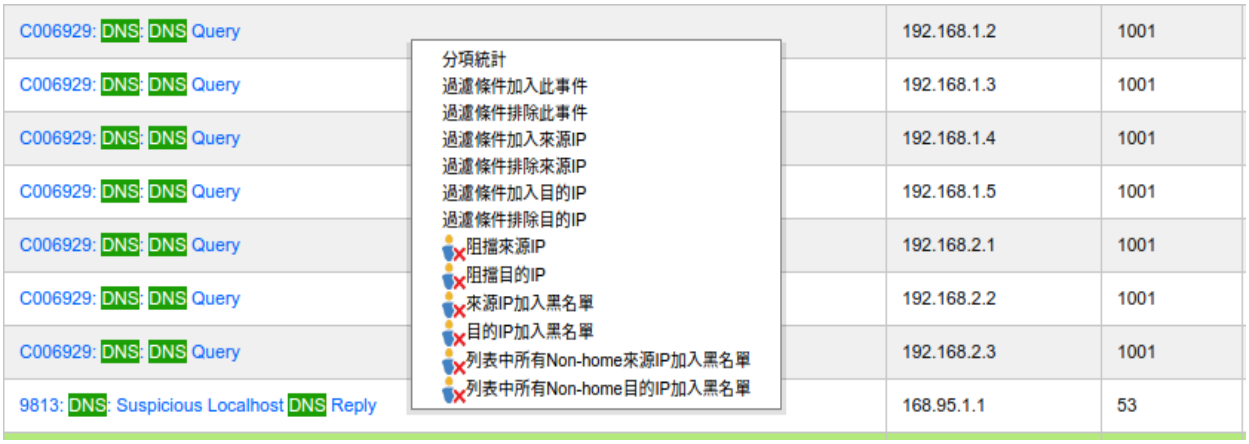
Action

「來源 IP 所屬交換機/介面」及「目的 IP 所屬交換機/介面」等訊息，僅於交換機設定 IP/MAC 對應後提供。

點選「事件」欄位裡的事件名稱，系統會另彈一新視窗(如下圖)，顯示事件的詳細說明(並非每一個事件都有進階查詢內容，需視 Syslog 設備原廠的支援程度而定)。



管理者可在事件列表上點擊右鍵，彈出快捷功能表。(如下圖)



- 分項統計：點選分項統計，彈出選擇分項統計欄位視窗(如下圖)，可以選定單個或最多 3 個項目進行分項統計(Aggregation 運算)，例如：依「設備」、「事件」、「等級」、「來源 IP」、「來源區域」、「來源 Port」、「目的 IP」、「目的區域」、「目的 Port」、「來源名稱解析」、「目的名稱解析」、「動作」及「Policy ID」等 13 個特定欄位進行分項統計，系統會將所查詢出的事件再根據選取的分項進行 Hit Count/Session/Packet/Byte 加總，以方便使用者閱讀。

舉例來說，若選擇以「設備」進行分項統計，則顯示的結果是將各設備的 Hit Count/Session/Packet/Byte 加總顯示出來。如此可以幫助用戶瞭解目前事件量最多的設備是哪個，耗用最多頻寬的設備是哪個。

- 過濾條件加入此事件：表示要將該事件加到事件過濾設定的「事件關鍵字」中，作為下次搜尋的過濾條件之一，使用者無須手動輸入字串。
- 過濾條件排除此事件：表示要將該事件在事件過濾設定的「事件關鍵字」中設定為「!」排除，並作為下次搜尋的過濾條件之一，使用者無須手動輸入字串。
- 過濾條件加入來源 IP：表示要將該事件的來源 IP 加到事件過濾設定的「IP 過濾➔同時判定來源與目的 IP」選項中的「來源 IP」格窗，作為下次搜尋的過濾條件之一，使用者無須手動輸入 IP。
- 過濾條件排除來源 IP：表示要將該事件的來源 IP 在事件過濾設定的「IP 過濾➔同時判定來源與目的 IP」選項中的「來源 IP」格窗中設定為「!」排除，並作為下次搜尋的過濾條件之一，使用者無須手動輸入 IP。
- 過濾條件加入目的 IP：表示要將該事件的目的 IP 加到事件過濾設定的「IP 過濾➔同時判定來源與目的 IP」選項中的「目的 IP」格窗，作為下次搜尋的過濾條件之一，使用者無須手動輸入 IP。
- 過濾條件排除目的 IP：表示要將該事件的目的 IP 在事件過濾設定的「IP 過濾➔同時判定來源與目的 IP」選項中的「目的 IP」格窗中設定為「!」排除，並作為下次搜尋的過濾條件之一，使用者無須手動輸入 IP。

Flow ■ 阻擋來源 IP：針對該事件的來源 IP 進行阻擋。IP 阻擋指令可下達至 N-Reporter 能支援的 L2 Switch 或是 Syslog 設備上。概括論之，內網 IP 的阻擋工作會交由 L2 Switch 執行；而來自外網的惡意 IP 則交由 Syslog 設備(通常是 Firewall 或是 IPS)執行。點選阻擋來源 IP，彈出 IP 阻擋視窗(如下圖所示)，使用者可設定阻擋時間的長短。此外，若欲查詢 IP 阻擋列表則需瀏覽「報表➔IP 阻擋列表」。

Action ■ 阻擋目的 IP：針對該事件的目的 IP 進行阻擋。IP 阻擋指令可下達至 N-Reporter 能支援的 L2 Switch 或是 Syslog 設備上。

Action ■ 來源 IP 加入黑名單：將來源 IP 加入黑名單進行批次阻擋，可指定自動復原週期。

目前僅 Action 支援列表中所列出的設備支援此功能

Action ■ 目的 IP 加入黑名單：將目的 IP 加入黑名單進行批次阻擋，可指定自動復原週期。

目前僅 Tipping Point SMS 支援此功能

- 列表中所有 Non-home 來源 IP 加入黑名單：將非屬於已定義於 home 內的 IP 之來源 IP 全部加入黑名單進行批次阻擋，並可設置自動復原的時間，如下圖所示。。

> 目前僅 Tipping Point SMS 支援此功能

- 列表中所有 Non-home 目的 IP 加入黑名單：將非屬於已定義於 home 內的 IP 之目的 IP 全部加入黑名單進行批次阻擋，並可設置自動復原的時間，如下圖所示。

> 目前僅 Tipping Point SMS 支援此功能

3.2 已儲存查詢條件

此選項的功能主要在於對已儲存之事件查詢條件進行編輯與刪除動作。

已儲存查詢條件搜尋

搜尋特定的已儲存查詢條件，可輸入查詢條件名稱(全部或是部份)，按下鈕，針對「查詢條件名稱」欄位進行搜尋。按下鈕，可以清除輸入的搜尋字串。

已儲存查詢條件列表

操作	查詢條件名稱	查詢依據	寄送型態	查詢建立時間	最近修改時間	事件下載
	AP status	Syslog		2016/07/19 15:34	2016/07/20 15:29	
	All Syslog	Syslog		2016/07/25 18:26	2016/07/26 14:07	
	IIS response time 128 to 804	Syslog	日報表	2016/07/01 13:45	2016/07/01 13:46	
	as number is 1 or 2	Flow	日報表	2016/06/30 13:44	2016/07/01 16:04	
	flow ip is 192.168.1.1	Flow	日報表	2016/06/30 13:54	2016/07/01 16:04	
	imperva severity is medium(map to minor)	Syslog	日報表	2016/07/01 09:53	2016/07/01 17:47	
	syslog src host 2001::ffff:c0a8:104	Syslog	日報表	2016/07/01 15:34		
	嚴重資安事件	Syslog	時報表, 日報表	2016/07/26 14:05		

- 操作：點擊圖示，系統會將頁面轉至「事件➔事件查詢」，並自動載入該筆已儲存的所有過濾參數進行事件搜尋動作。點擊圖示，則刪除該筆查詢條件。
- 查詢條件名稱：為使用者自行定義的查詢條件名稱，供使用者方便閱讀與辨識用。
- 寄送型態：顯示自動寄送離線事件為何種型態(如：時報表或日報表)
- 查詢依據：顯示該筆儲存條件為何種查詢依據。
- 查詢建立時間：顯示該筆查詢條件建立的時間。
- 最近修改時間：顯示該筆查詢條件最近一次修改的時間。

  點選「查詢條件名稱」欄任一名稱，系統會將頁面轉至「事件➔事件查詢」，並自動載入該筆已儲存的所有過濾參數進行事件搜尋動作。當頁面轉至「事件➔事件查詢」時，可再次設定事件過濾條件，設定完成後，可按「儲存查詢條件」鈕，來覆蓋原本已存查詢條件或按「另存查詢條件」鈕，來另存一個新的查詢條件。
- 事件下載：點選「事件下載」鈕，將彈出「事件下載」視窗(如下圖所示)。使用者可選擇起始時間及結束時間，然後按下「下載」鈕即可下載 TXT 格式之離線事件。

事件下載鈕，在「儲存查詢條件」時，需指定至少一個「寄送欄位」才會出現，若未指定「寄送欄位」則不顯示。

Chapter 4 報表

N-Reporter 不僅是一個效能優異且功能完整的報表產生器，在許多真實案例的應用上，N-Reporter 的自動學習與異常突增發覺能力更是使用者在維運網路與進行除錯時非常倚賴的分析工具。

在此章節會介紹「報表」下之子功能：「Top N」、「分時報表」、「趨勢報表」、「IP 阻擋列表」、「事件數量統計」及「Flow 專屬報表」等豐富、多樣、動態顯示的報表。在這些報表功能中，系統同樣支援事件功能中所運用的邏輯運算概念，讓報表製作更貼近使用者的真實所需。

4.1 Top N 報表

此選項的功能主要在依使用者所定義的複合式條件來製作出排行報表，可讓使用者迅速掌握網路環境中發生最多量的資安問題、流量最大的 IP 排行，甚至可以監看在一週內某個特定攻擊事件的軌跡。資安 Syslog 搭配 Flow 模組，可讓使用者從各種不同的角度分析問題，以迅速掌握並排除問題。除線上輸入參數即時製作報表之外，使用者也可以定義排程，讓 N-Reporter 自動產生離線報表(Off-line Report)並寄發給指定收件者。

4.1.1 Top N 報表製作設定

查詢條件設定方式請參考【事件】3-1 章節。

TOP N

- 本選項於「報表製作依據」中點選「Syslog」、「Flow」方可使用。
- 製作報表時可以輸入欲排行的數量，最多允許輸入 1000，預設列出排行前 100 名。

報表形式

- 本選項於「報表製作依據」中點選「Syslog」、「Flow」方可使用。
- 系統提供「圓餅圖」、「長條圖」、「曲線圖」等三種圖表型式。「圓餅圖」與「長條圖」適合繪製 Top N 排名報表。「曲線圖」適合繪製長時間流量報表，選擇繪製「曲線圖」時，將不參考「排序依據」及「Top N」的設定。

排序依據

製作報表時可以依據「事件」、「來源 IP」、「目的 IP」、「等級」、「來源區域」、「目的區域」、「來源名稱解析」、「目的名稱解析」、「來源 Port」、「目的 Port」、「來源 Port 解析」、「目的 Port 解析」、「Policy ID」、「來源使用者」、「目的使用者」、「設備」、「動作」、「事件型態」、「Protocol」、「NAT 來源 IP」、「NAT 目的 IP」、「NAT 來源 Port」、「NAT 目的 Port」、「流入介面」、「流出介面」、「TCP Flag」、「狀態」、「目的主機名稱」、「路徑」、「來源主機名稱」、「平均封包大小」、「來源 MAC」、「目的 MAC」、「應用服務」、「AP SSID」、「無線基地台」、「Audit User」、「作業系統」、「寄件者」、「收件者」、「分類」等參數進行統計。

上述參數只允許任選 8 項作為排序依據。

例如：想得知網路環境中每種應用的排行，可以依「目的 Port 解析」進行排序；想要得知 AD 使用者使用網路或資安現況，也可以依「來源使用者」或「目的使用者」進行排序。

排序數值

- 選擇製作報表時是以「Hit Count」、「Session」、「Packet」或「Byte」為根據進行排序。
- 選擇比對圖為「不顯示」、「Hit Count」、「Session」、「Packet」或「Byte」。

  在 N-Reporter 有同時接收資訊安全設備 LOG 以及流量 LOG(防火牆 Traffic 或 Flow) 時，可以同時繪出關聯 Top N 報表，例如顯示資訊安全事件所佔用的頻寬資訊等。
- 勾選其數值顯示為「Hit Count」、「Session」、「Packet」或「Byte」(可多選)，用來規範 Top N 下方表格的欄位顯示。

事件關鍵字

- 當勾選「關鍵字符合即當作特定事件」後，系統會將符合所輸入的關鍵字做出統計結果。

當勾選「關鍵字符合即當作特定事件」後，建議排序依據只選「事件」一項即可。

【範例】在「事件關鍵字欄位」中輸入 BitTorrent+P2P+ICMP 並且勾選「關鍵字符合即當作特定事件」後啟動查詢，系統會將所欲查詢事件標題中含有 BitTorrent、P2P 及 ICMP 字串的當成事件統計出來如下圖。

NO.	事件	Hit Count	Sessions	Packets	Bytes	流量圖
1	P2P	803.1K	86.4K	1M	31.1M	
2	BitTorrent	196.2K	1.6K	96.4K	924.7K	
3	ICMP	88.5K	0	0	0	

按鈕操作

按下 啟動查詢 鈕，系統會依據使用者在報表製作設定中定義的各種條件搜尋符合的事件或是進行統計與排序 Flow 資料工作，執行結果以圖形與表格的形式呈現於畫面下方。按下 鈕，則會清空所有輸入的條件內容。若要系統定期寄送報表(Off-line 形式離線報表)，按下「儲存報表」 鈕，彈出儲存報表視窗(如下圖)，使用者可依照實際需求逐一設定報表寄送條件。

- 輸入報表名稱：請輸入一個容易辨識的名稱(如：總部資安事件日報表、宿舍流量日報表等)。
- 定義工作時段 : 定義要納入報表計算的時段，如果使用者希望列出例如早上 8 點到下午 6 點的日報表，可自行定義工作時間區段。

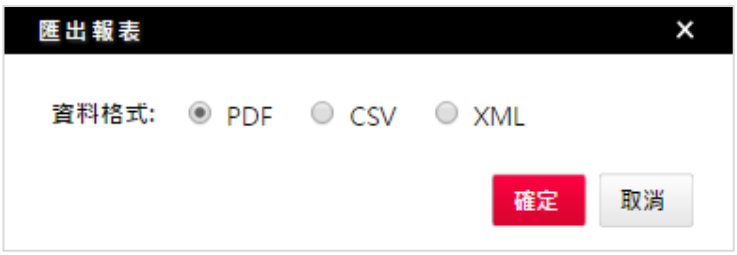
- 定義工作日：非工作日的事件或是 Flow 資料將不納入統計，如：工作日是周一至周五，則周六與周日所發生的事件與 Flow Data 都不會產生報表，而日報表也僅在周二至周六寄送(即在隔天的指定時間寄送前一天的報表)。若報表所選擇的時段資料量大時，報表可能延連發送。
- 報表型態：則是告知系統要自動產生報表的週期排程(可複選)。其中半月報的寄送時間固定為每月 1 日及 16 日；月報為每月 1 日；季報的寄送時間固定為 1/1、4/1、7/1 及 10/1；半年報為 1/1 及 7/1；年報是每年 1/1。

  計算區段以設定當時為起點，如勾選月報表後，當月月報並不會從當月 1 日開始製作報表，而是從報表設定日起算，隔月則會從當月 1 日起算

- 報表寄送時間：定義這份報表寄送的時間。
- E-Mail 群組：下拉式選項供使用者選取預先定義的 E-Mail 群組(請參考「系統管理➔系統通報設定　建立 E-Mail 群組」章節)。
- 資料格式：定義爾後這份報表要用 HTML、PDF、CSV 或 XML 格式寄送(可複選)。

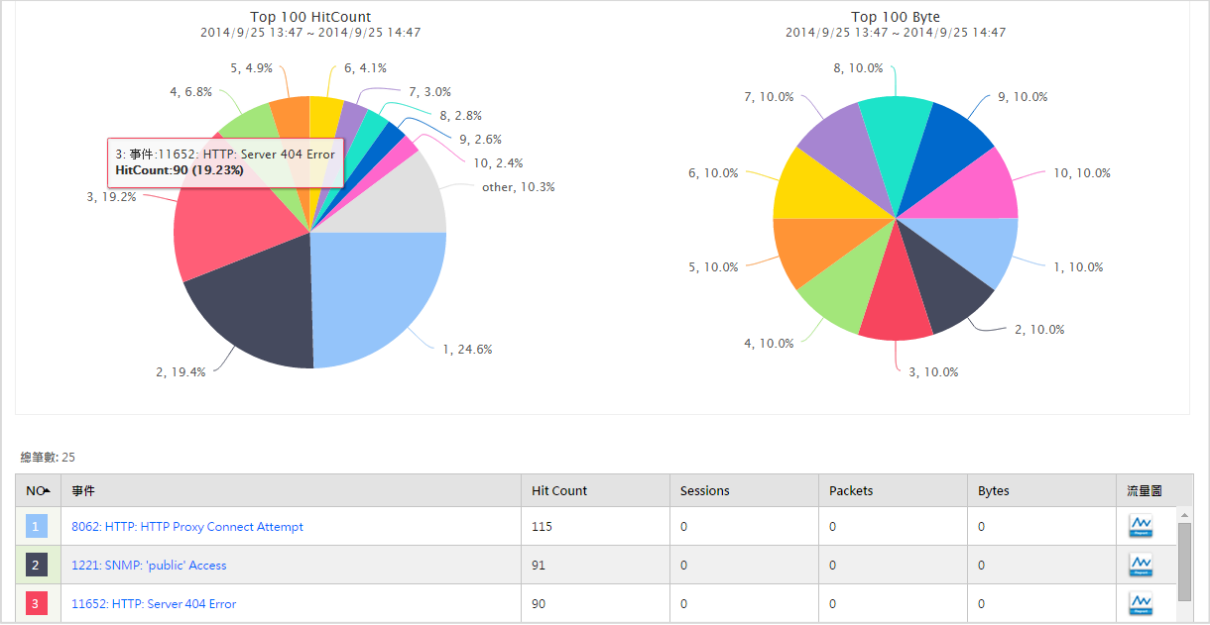
  各欄位設定完後，按下 確定 鈕，系統會把使用者定的各種設定儲存起來，使用者可在「報表➔Top N➔已儲存報表」的已儲存報表列表中找到儲存的報表。

  按下「資料輸出」  鈕，彈出匯出報表視窗(如下圖)，使用者可選擇 PDF、CSV、XML 格式將所製作 Top N 報表輸出。按下 確定 鈕後一段時間(所選擇的時段中之資料量不同，等待的時間可能會有所不同)，將會開始下載。



報表列表

報表執行結果會以圖形與表格的形式呈現。(如下圖)



將滑鼠移動到報表圓餅圖之特定區塊，系統會顯示此區塊相關訊息，再點選圖此區塊或是下方表格中的事件內容，N-Reporter 會彈出「事件」視窗，其呈現該區塊詳細的事件列表。系統提供 Drill-down 查詢功能，使用者可再進一步深入分析(詳細事件操作功能，請參考「事件➔事件查詢」章節)。

Flow

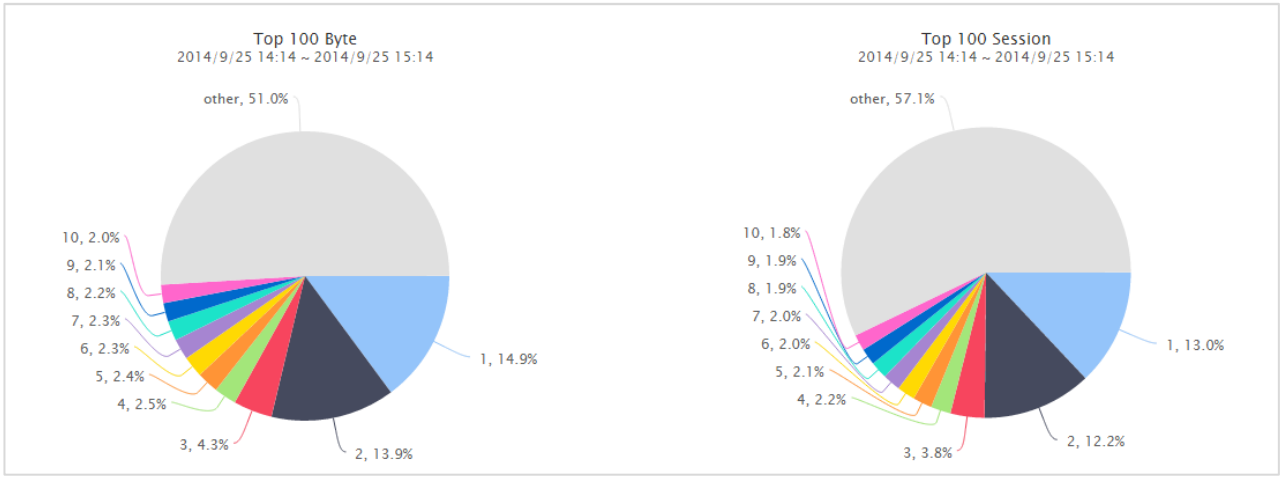
將蒐集到的 Syslog 資料(通常是具有第七層使用者行為的訊息)與 Flow 資料(含有第三層與第四層的 Packets/Bytes 等頻寬用量數值)做交叉比對分析(Correlation)是 N-Reporter 的主要應用之一。如：使用者如果發現網路中有 P2P 的行為(來自 Syslog Data)， N-Reporter 的交叉比對功能可以得知這些 P2P 流量有多少(Packets/Bytes，來自 Flow Data)；從另一個角度來看，當某一個 IP 或是網段佔用大量頻寬時(來自 Flow Data)，使用者也可透過 N-Reporter 的交叉比對功能得知這個 IP 或是網段到底在執行什麼樣的應用程式(來自 Syslog Data)導致巨量消耗網路資源的情況。

Syslog

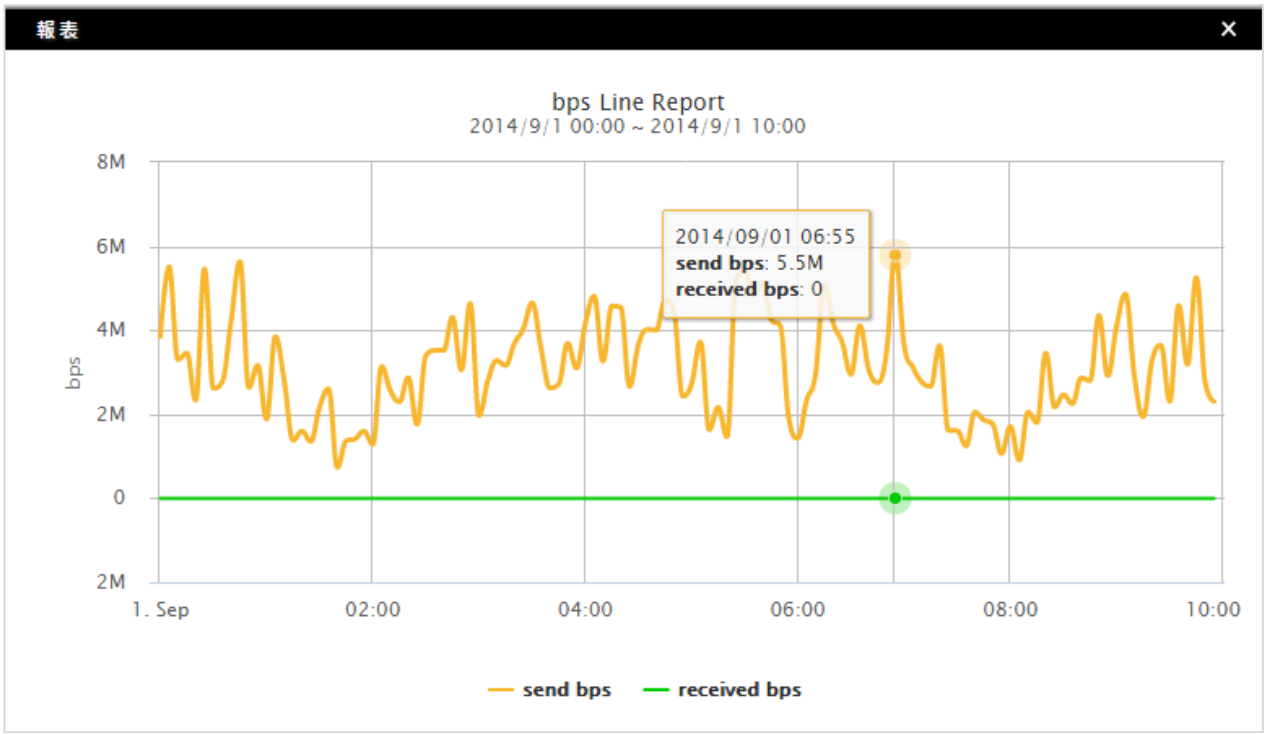
在「報表製作依據」中點選 Syslog，則以 Syslog 資料為主進行排序，再根據 Syslog 的排序結果(事件 Hit Count 最高的排名第一，次高排第二，以此類推)交叉比對這些 Top N 事件所使用的 Packets/Bytes 數，因此報表製作的結果會呈現兩張圖，左方為主要圖形，是根據 Syslog Data 所計算出來的 Top N 事件排行，單位為 Hit Count 數；而右方則為輔助圖，讓使用者了解左邊主圖中的每一個事件到底傳送了多少 Packets/Bytes，占所有事件流量多少的百分比。

Flow

在「報表製作依據」中點選 Flow，則以 Flow 資料為主進行排序後，再根據 Flow 用量的排序結果(Bytes 數最高的排名第一，次高排第二，以此類推)交叉比對這些 Top N IP 所產生的事件數，因此報表製作的結果會呈現兩張圖，左方為主要圖形，是根據 Flow Data 所計算出來的 Top N IP 排行，單位為 Byte 數；而右方則為輔助圖，讓使用者了解左邊主圖中的每一個高用量 IP 到底產生多少事件，占所有事件多少百分比。



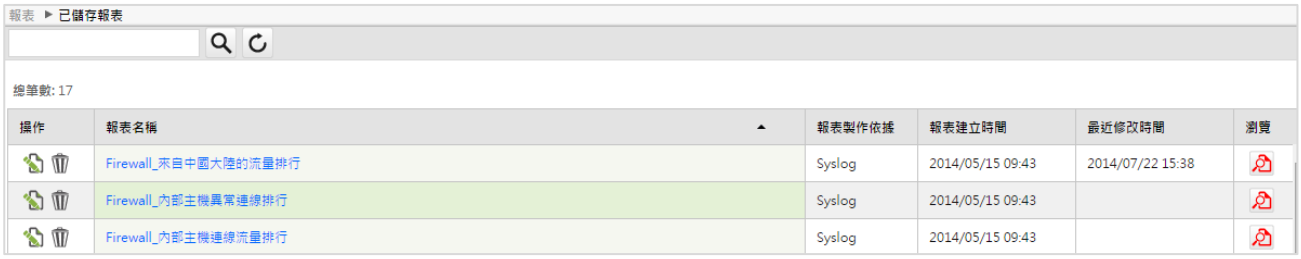
Syslog 事件一定可以從 Flow Data 中計算比對出使用的 Packets/Bytes 量；但不是每一筆 Flow 資料都可以找到相對應的 Syslog 事件，端看使用者環境中的 Syslog 設備能否產生夠豐富的事件資料。



以 Syslog 為基礎所製作而成的 Top N 排序報表，使用者可以點選表格右方 圖示，查看該事件的流量分時圖。將滑鼠移至流量分時之特定點(如上圖箭頭所指)，系統會顯示 pps / bps 的數量及精確時間。

4.1.2 已儲存報表

此選項的功能主要在於對已儲存之報表進行條件編輯與刪除動作，亦可在此處隨時查閱報表的歷史紀錄。



已儲存報表搜尋

搜尋特定的已儲存報表，可輸入報表名稱(全部或是部份)，按下 鈕進行搜尋。按下 鈕，可以清除輸入的搜尋字串。

已儲存報表列表

列表欄位說明如下：

- 操作：點擊 圖示，系統會載入該筆已儲存的參數設定，使用者可在此頁面修改參數，當使用者修改完報表參數條件後，可按「儲存報表」 鈕，來覆蓋原本已存參數條件或按「另存報表」 鈕，來另存一個新的參數條件。點擊 圖示，則刪除該筆報表。
- 報表名稱：為使用者自行定義的報表名稱，供使用者方便閱讀與辨識用。
- 報表製作依據：顯示該筆報表為何種製作依據。
- 報表建立時間：顯示該筆報表建立的時間。
- 最近修改時間：顯示該筆報表最近一次修改的時間。
- 瀏覽：點選 圖示，可查閱該報表歷史記錄。

報表歷史紀錄查詢

- 查詢功能：

使用者可以在此找到系統過去為該已儲存報表所製作的每份報表，輸入欲查閱報表的時間區段，系統提供三種查詢時間區段方式：

(1) 選擇時間區段：從下拉式選項中選擇系統預先定義好的時間區段。

(2) 過去：填寫欲查詢的「小時」、「天」、「週」、「月」數字，系統預設值為過去 30 天。

(3) 起迄時間：請輸入「起始時間」與「結束時間」。

按下 啟動查詢 鈕後，該儲存報表於使用者所定義的時間區段內所有歷史紀錄都將呈現於下方「查

詢結果列表」中。按下  鈕，則回復系統預設時間值。

■ 查詢結果列表說明：

(1) 操作：點擊  圖示，為刪除該筆報表歷史記錄。

(2) 報表名稱：為使用者自行定義的報表名稱，供使用者方便閱讀與辨識用。

(3) 報表型態：顯示該筆報表的製作週期。

(4) 報表起始時間：顯示該筆報表統計的起始時間。

(5) 報表結束時間：顯示該筆報表統計的結束時間。

(6) 瀏覽：點選  圖示，可線上呈現報表內容，如同於「Top N 報表」功能中製作報表的結果。

(7) 下載報表：則是採離線方式下載該報表的結果，可選擇 PDF  、CSV  及 XML  格式。

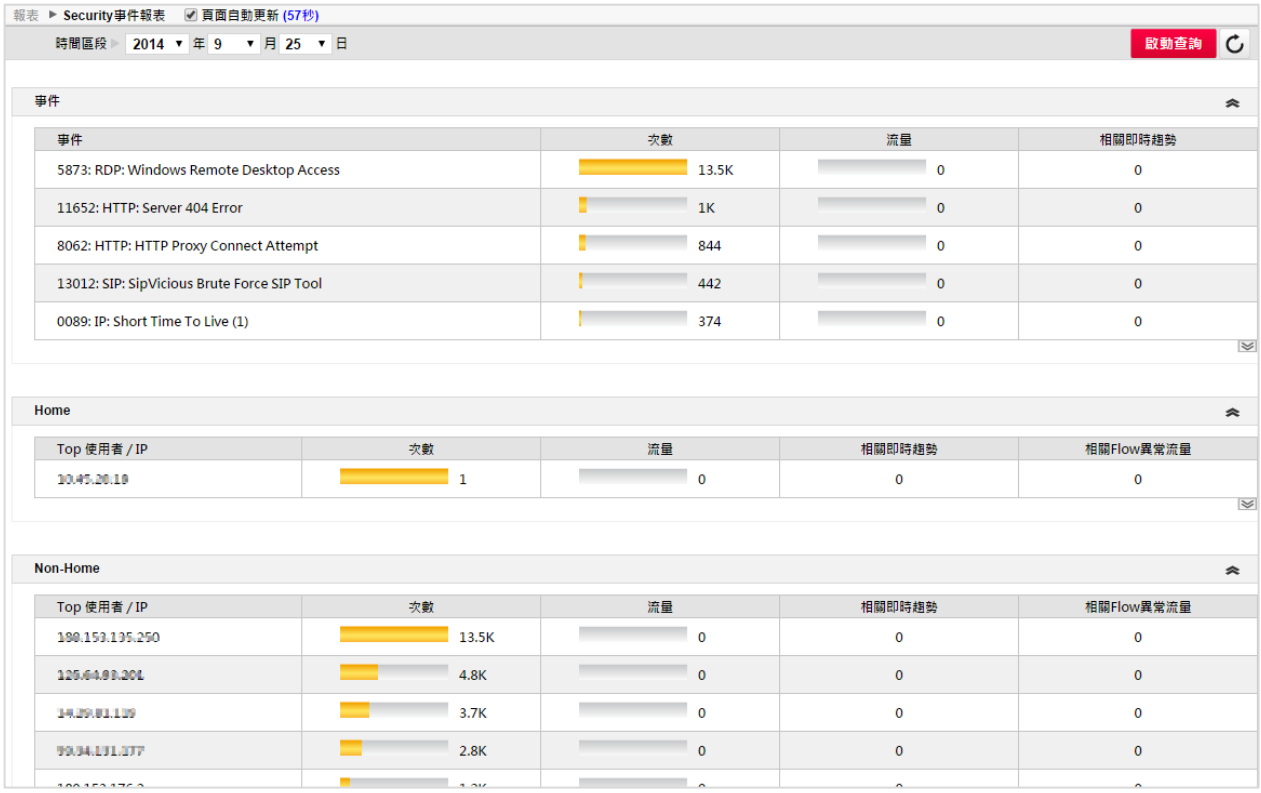
4.2 加值報表

N-Reporter 在收集各式 LOG 之後，會進行主動分析，並列出最需注意的項目，包括分析網路資安流量現況的資安報表，以及主機入侵分析的異常登入行為報表。

4.2.1 Security 事件報表

收集使用者各種網路設備的資料，包含資安 Syslog(如 IPS)或流量資料(如 Router Netflow 或防火牆 Traffic)，資安報表每日整理、萃取次數最多的前 30 筆事件及引發最多資安事件的 IP，並同時列出所佔用的流量。

選擇一時間區段，按下 啟動查詢 鈕，可查閱該時段的資安報表。按 鈕，回復成目前時間。

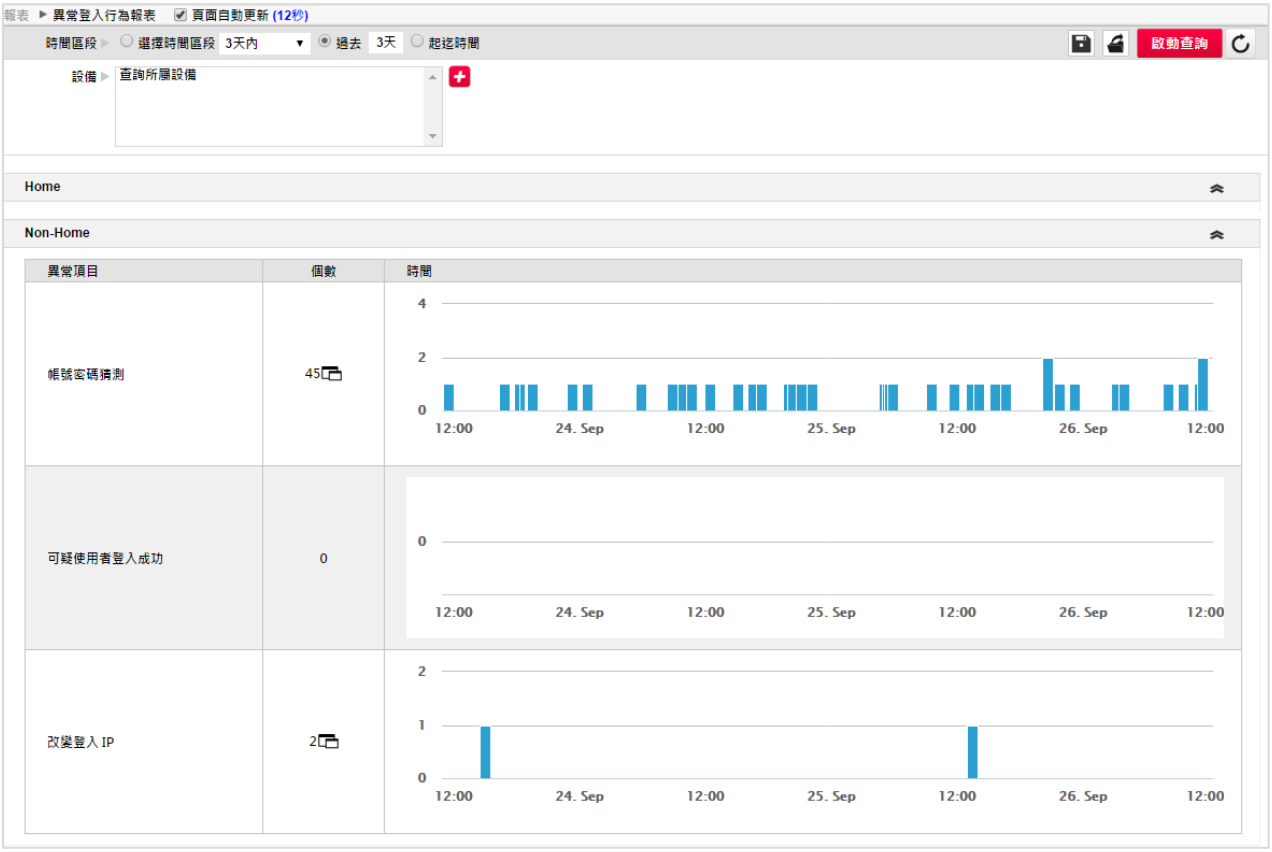


預設列出 5 筆資料，點擊 圖箭頭指標可列出所有 30 筆項目。

資安報表共分三大類「資安事件排行」、「內部 IP 排行」以及「外部 IP 排行」，可以看出整個網路環境中發生次數最多的資安事件，並同時可得知這些資安事件所佔用的流量，以及是否引發即時趨勢。

Server 4.2.2 異常登入行為報表

面對數量龐大的伺服器及海量的稽核資料 (Log)，使用者該如何在面臨駭客威脅時能快速反應。N-Reporter 幫您分析出最需關注的項目。



■ 異常登入行為報表共分二大類「內部 IP 排行」以及「外部 IP 排行」，其包含以下種類：

(1) 帳號密碼猜測：針對登入失敗的 Log，列出所有進行帳號密碼猜測行為的可疑 IP 列表。

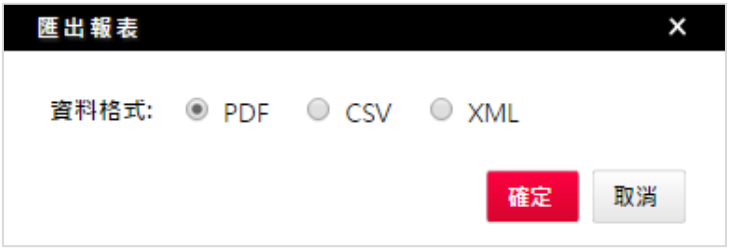
(2) 可疑 IP 登入成功：曾經列為可疑 IP 的觀察對象，最後此可疑 IP 登入成功，可能表示攻擊者已成功登入主機，必須特別加以關注。

(3) 改變登入 IP：雖然使用者的帳號密碼認證成功，但是卻是使用與平常不同的 IP 或網段，可能表示攻擊者已成功登入主機，必須特別關注加以確認。

■ 選擇設備，在設備框中，可選擇欲查詢的設備，若未選擇，則系統預設為查詢所屬設備，即全部設備。

■ 選擇一時間區段，按下 啟動查詢 鈕，可查閱該時段的異常登入行為報表，按 鈕可回復成目前時間。

■ 按 ，系統將彈出「匯出報表」視窗，使用者可以選擇 PDF、CSV、XML 格式，並將查詢得到的列表內容輸出並下載回操作端主機。



■ 按鈕，系統將彈出「儲存設定」視窗，並進行以下設定：

(1) 離線報表設定：可以勾選定期產生日報表、週報表及月報表，並設定寄送的資料格式 (HTML/PDF/CSV/XML)。

(2) 寄送即時告警：設定當發生哪些異常事件時應寄送告警 E-mail

(3) 密碼錯誤次數: 短時間內的累積密碼錯誤次數達設值時，就判定為帳號密碼猜測，預設值為 5 次。

(4) 非法使用者錯誤次數: 短時間內的累積帳號錯誤次數達設值時，判定為帳號密碼猜測，預設值為 3 次。

(5) 改變登入 IP: 設定當有跨區域登入的判斷精準度。以 IPv4 為例，設定值 24 表示 subnet prefix 為 24，即為 netmask 255.255.255.0 也就是當某個使用者前後兩次成功登入 IP 被判定為不同網段時，例如 192.168.100.10 及 192.168.120.50 時，將會視為異常並發送告警。

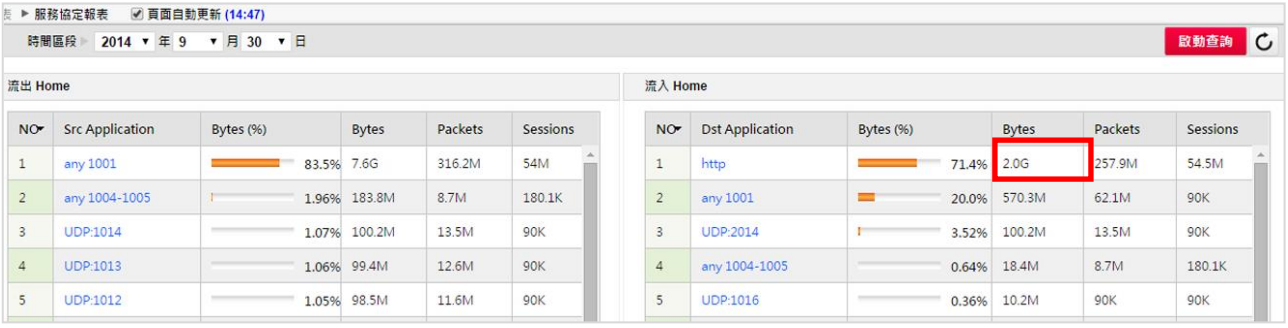
(6) 收件者設定: 指定 E-mail 群組: 指定收件者的 E-mail 群組，請在「系統管理➔告警通報設定」中設定。

(7) 通報週期: 告警發生時將累計一段時間後寄出，避免狀況發生時有過多的告警 E-Mail 送出，可以依使用者對告警處理反應時間來修改，預設為 10 分鐘。™

Flow

4.2.3 服務協定報表

服務協定報表會依據 Flow 或是 Firewall Traffic 等流量資料，提供針對「Port」及「Port 名稱解析」來進行流量排行，使用者可以針對有疑慮的特定 Port 流量進行追查。



NO	Src Application	Bytes (%)	Bytes	Packets	Sessions
1	any 1001	83.5%	7.6G	316.2M	54M
2	any 1004-1005	1.96%	183.8M	8.7M	180.1K
3	UDP:1014	1.07%	100.2M	13.5M	90K
4	UDP:1013	1.06%	99.4M	12.6M	90K
5	UDP:1012	1.05%	98.5M	11.6M	90K

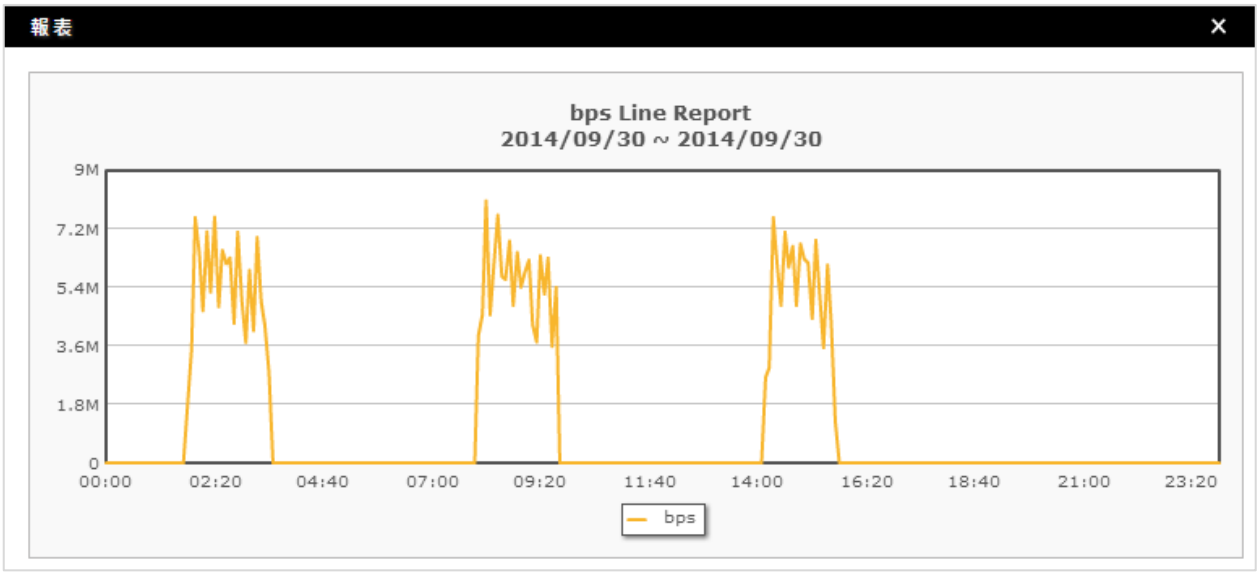
NO	Dst Application	Bytes (%)	Bytes	Packets	Sessions
1	http	71.4%	2.0G	257.9M	54.5M
2	any 1001	20.0%	570.3M	62.1M	90K
3	UDP:2014	3.52%	100.2M	13.5M	90K
4	any 1004-1005	0.64%	18.4M	8.7M	180.1K
5	UDP:1016	0.36%	10.2M	90K	90K

時間區段可以指定查詢的日期，預設查詢今日的服務協定流量排行，指定想查詢的日期後，再點選 啟動查詢 即可，點選右方 鈕 可以將日期回復到今日。

上圖紅框所指透過 HTTP 的流入流量高達 2G 有可疑，就可以直接點擊 http 來找出所有採用 HTTP 來下載的 IP。

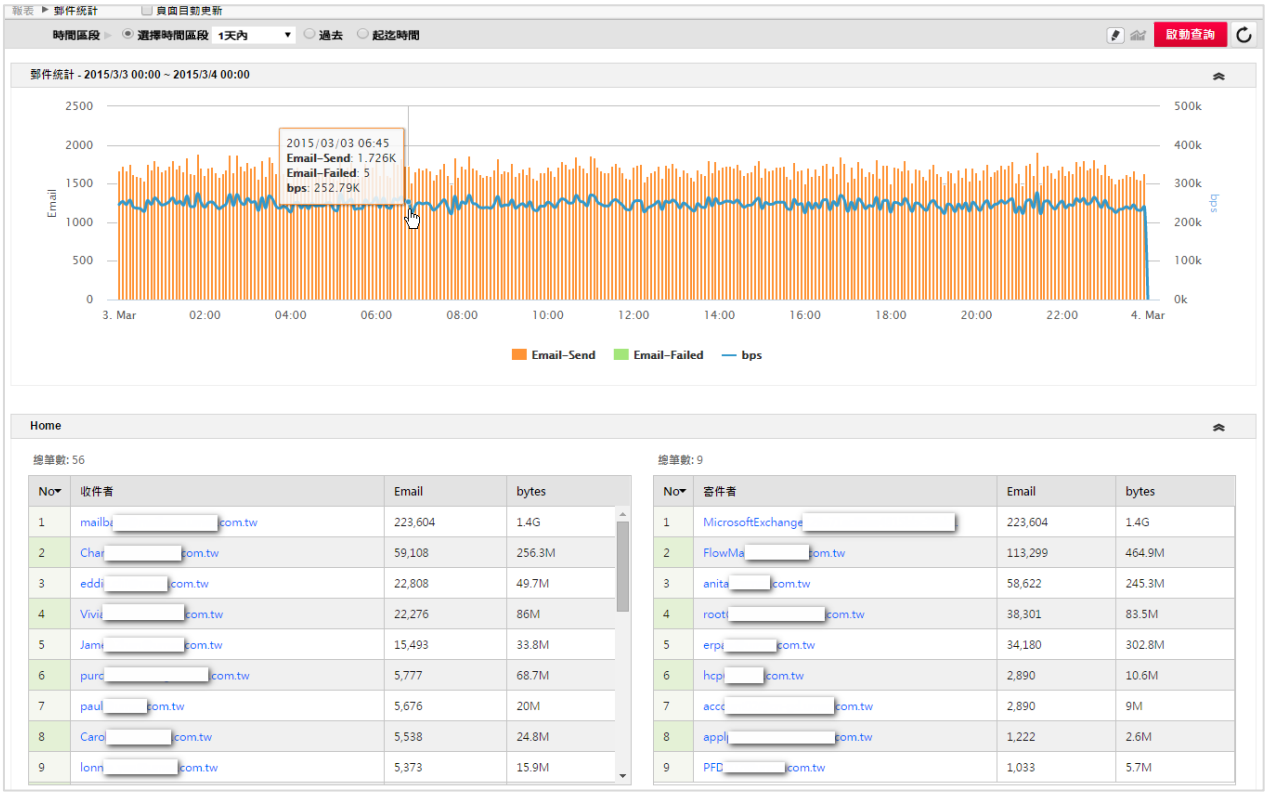
NO	目的IP	Bytes(%)	Bytes	Packets	Sessions	Hit Count	流量圖
1	192.168.0.1	49.9%	1.8G	233.8M	34.5M	0	
2	60.0.0.1	49.9%	1.8G	233.8M	34.5M	0	
3	192.168.3.6	0.05%	1.9M	1.4M	115.8K	928	
4	192.168.3.4	0.03%	1M	463.3K	57.9K	928	
5	192.168.3.2	0.03%	1M	231.6K	57.9K	928	
6	192.168.3.1	0.02%	926.6K	115.8K	57.9K	928	

針對所列出的異常 IP，點選右側 圖示繪製流量圖。



4.2.4 郵件統計

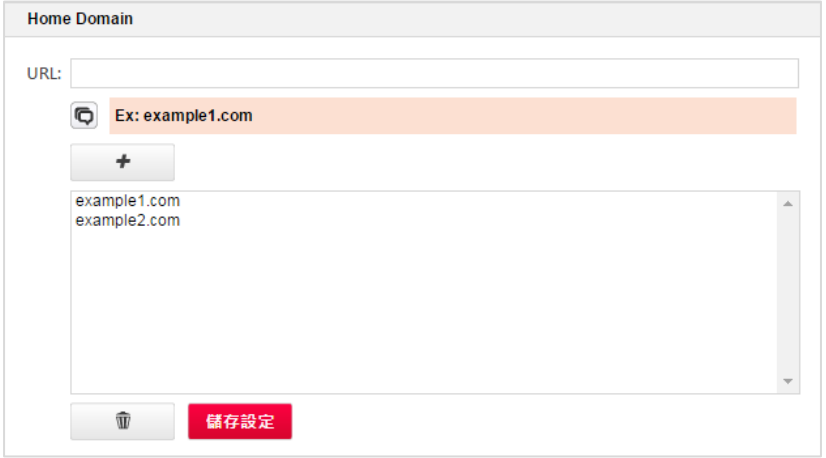
針對 Windows Server 上的 Exchange Server 郵件收送狀況進行分析，讓管理者可以了解所管轄郵件主機的寄件收件分時圖、流量圖及使用者排行等，並在帳號被入侵用於垃圾信寄送時能即時察覺及鎖定。



由上方的分時圖可以看出過去 24 小時的寄件及收件狀況(數值對應左側座標)，及頻寬使用的流量圖(數值對應右側座標)，當有異常突增能即時察覺。

下方的排行會針對內部郵件(Home)及外部郵件(Non-Home)進行次數排行，企業使用的網域名稱可以在點下 圖示進行設置。點選列表中的有異常大量的收件者或寄件者資訊，可以進一步追查該收件者或寄件者的相關郵件 LOG。

■ 設定企業使用的網域名稱，讓管理者可以了解所管轄郵件主機的寄件收件分時圖、流量圖及使用者排行等資訊。點擊 + 鈕，將 URL 輸入的內容加入列表；選取任一 URL 項目並點擊 鈕則將其由列長中移除。編輯完成後按 儲存設定 鈕儲存設定。



■ 郵件異常告警設定，在點下  圖示後，可進行設定。

(1) 寄件者寄信超過：可設定當單一寄件者在 5 分鐘之內寄信超過指定信件量的郵件時進行告警。

(2) 收件者收信超過：單一收件者在 5 分鐘之內收到超過指定信件量的郵件時進行告警。

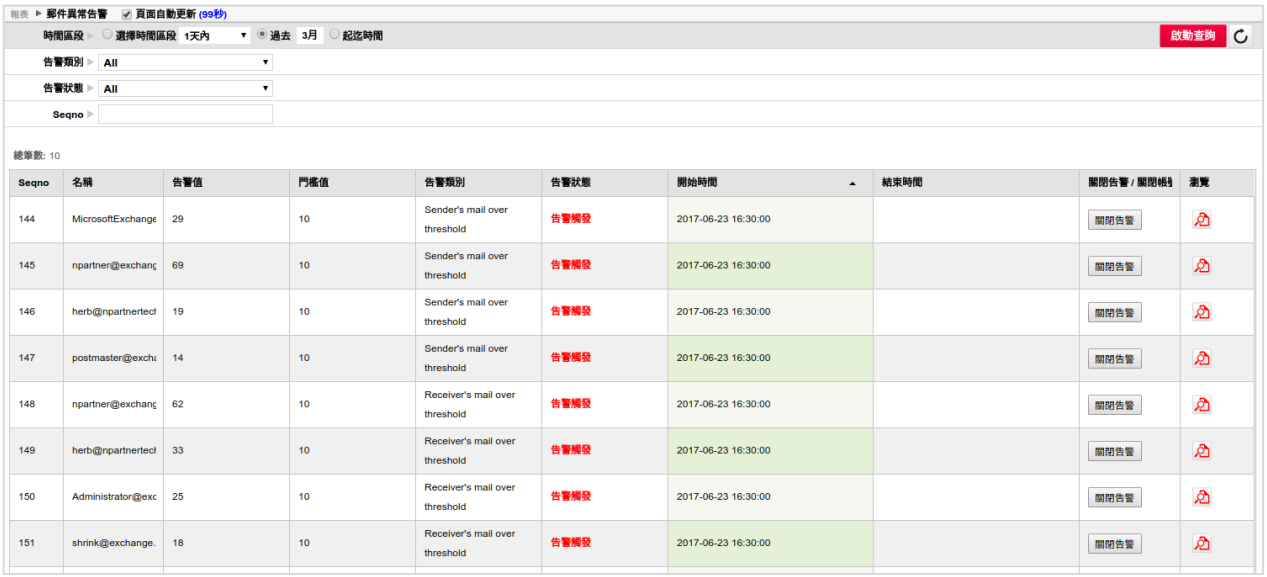
(3) 內部不存在的收件者：5 分鐘之內收到寄給內部不存在的收件者，超過指定信件量時進行告警。

(4) E-mail 群組: 指定收件者的 E-mail 群組，請在「系統管理➔告警通報設定」中設定。

(5) E-Mail 通報週期：通報週期: 告警發生時將累計一段時間後寄出，避免狀況發生時有過多的告警 E-Mail 送出，可以依使用者對告警處理反應時間來修改，預設為 10 分鐘。

4.2.5 郵件異常告警

郵件異常告警顯示當前是否有需要關注的郵件活動，可觀察到經過郵件異常告警設置的條件觸發的郵件告警事件，幫助管理者快速掌握問題的方向



■ 查詢功能：

使用者可以在此找到系統過去所發出的郵件異常告警，輸入欲查閱郵件告警的時間區段，系統提供三種查詢時間區段方式：

(1) 選擇時間區段：從下拉式選項中選擇系統預先定義好的時間區段。

(2) 過去：填寫欲查詢的「小時」、「天」、「週」、「月」數字，系統預設值為過去 3 個月。

(3) 起迄時間：請輸入「起始時間」與「結束時間」。

(4) 告警類別：可選擇欲查詢的告警類別，「Sender's mail over threshold」為寄件者在 5 分鐘內寄信超過指定的信件量。「Receiver's mail over threshold」為收信者 5 分鐘內收到超過指定數量的來信。「Recipient not found(Sender)」為寄信者指定的收件者郵件帳號不存在的信件，在 5 分鐘內超過指定的信件量。「All」為全部顯示。

(5) 告警狀態：可選擇欲查詢的告警狀態為「告警觸發」或是「告警結束」，「All」為全部顯示。

(6) Seqno：可指定查詢告警編號。

按下 啟動查詢 鈕後，該郵件異常告警於使用者所定義的時間區段內所有歷史紀錄都將呈現於下方列表中。按下  鈕，則回復系統預設查詢條件值。

■ 查詢結果列表說明：

(1) Seqno：顯示該項目的告警編號。

(2) 名稱：為該郵件告警項目的名稱，通常命名的規則為的告警目標之郵件帳號。

(3) 告警值：顯示該筆郵件告警在觸發告警時的數值。

(4) 門檻值：顯示該筆郵件告警在觸發告警時的門檻值。

(5) 告警類別：顯示該筆郵件告警在觸發告警時的類別。「Sender's mail over threshold」為寄件者在 5 分鐘內寄信超過指定的信件量。「Receiver's mail over threshold」為收信者 5 分鐘內收到超過指定數量的來信。「Recipient not found(Sender)」為寄信者指定的收件者郵件帳號不存在的信件，在 5 分鐘內超過指定的信件量。

(6) 告警狀態：顯示該筆郵件告警目前的狀態為「告警觸發」或是「告警結束」。「告警觸發」為當時告警可能持續發生或正在發生，「告警結束」為告警已被管理者關閉。

(7) 開始時間：為該筆郵件告警在觸發告警時的時間。

(8) 結束時間：為該筆郵件告警被管理者關閉的時間。

(9) 關閉告警：顯示該筆郵件告警可否被關閉，如可被關閉則顯示 關閉告警 鈕。

(10) 瀏覽：點選  圖示，可線上呈現該事件內容，如同於「事件查詢」功能中製作報表的結果，可供管理者再深入追查問題。

4.3 分時監控報表

提供使用者定義專屬的資安監控計劃，在監控值超過所設定的門檻值時能即時以 E-mail 方式通報，提供 24 小時不間斷監控。

4.3.1 訂製分時監控報表

查詢條件的設定方式，請參考「3.1.1 事件過濾設定」章節說明。

此選項的功能主要在讓使用者可以針對特定條件進行長期監控，其與事件及 Top N 報表相同，允許定義複雜的過濾條件，並可針對發生次數及流量設定 Red / Yellow 門檻值，並在監控值高於門檻值時，立即寄發警示通知於系統收件者。

如：可定義「A 棟大樓」的「Bit-torrent」事件所使用的流量「超過 60MB/s」或是「伺服器區」的「Login Fail」次數「超過每秒 10 次」等的長期追蹤條件，N-Reporter 將在超過門檻值發生時發出警示，並繪製此事件長時間的發生次數與流量報表，以提供各階層的管理與決策參考。

按鈕操作

- 按下「啟動查詢」鈕，系統會依據使用者在報表製作設定中定義的各種條件搜尋符合的事件或是進行統計與排序 Flow 資料工作，執行結果以圖形與表格的形式呈現於畫面下方。按下 鈕，則會清空所有輸入的條件內容。
- 按下「儲存報表」鈕，彈出訂製分時報表視窗(如下圖)，使用者可依照實際需求逐一設定參數值：

(1) 分時報表名稱：請輸入一個容易辨識的名稱(如：總部資安事件日報表、宿舍流量日報表等)。

(2) Hit Count/Sec 門檻值：允許設定 Red/Yellow 兩個門檻值，用以定義警示的嚴重程度。當 Syslog Hit

Count 值超過門檻值時，系統會發送警示 E-mail(收件者請參考「系統管理➔網路參數設定➔SMTP 認證帳號」的收件者列表)。由於統計方式為每 5 分鐘計算，因此門檻值的計算方式將以 Hit Count 值/300 秒的方式計算。若要設置特定事件發生單次就告警，則此設定值需小於 0.003(建議 0.001)。

(3) Session/Sec 門檻值：允許設定 Red/Yellow 兩個門檻值，用以定義警示的嚴重程度。當 Flow Session 值超過門檻值時發送警示 E-mail。由於統計方式為每 5 分鐘計算，因此門檻值的計算方式將以 Session 值/300 秒的方式計算。

(4) pps 門檻值：允許設定 Red/Yellow 兩個門檻值，用以定義警示的嚴重程度。當 pps 值超過門檻值時發送警示 E-mail。

(5) bps 門檻值：允許設定 Red/Yellow 兩個門檻值，用以定義警示的嚴重程度。當 bps 值超過門檻值時發送警示 E-mail。

(6) E-Mail 群組：下拉式選項供使用者選取預先定義的 E-Mail 群組(請參考「系統管理 系統通報設定 建立 E-Mail 群組」章節)。

(7) E-Mail 通報週期：選擇通報的發送週期。

(8) 離線報表型態：可以勾選定期產生日報表、週報表及月報表。

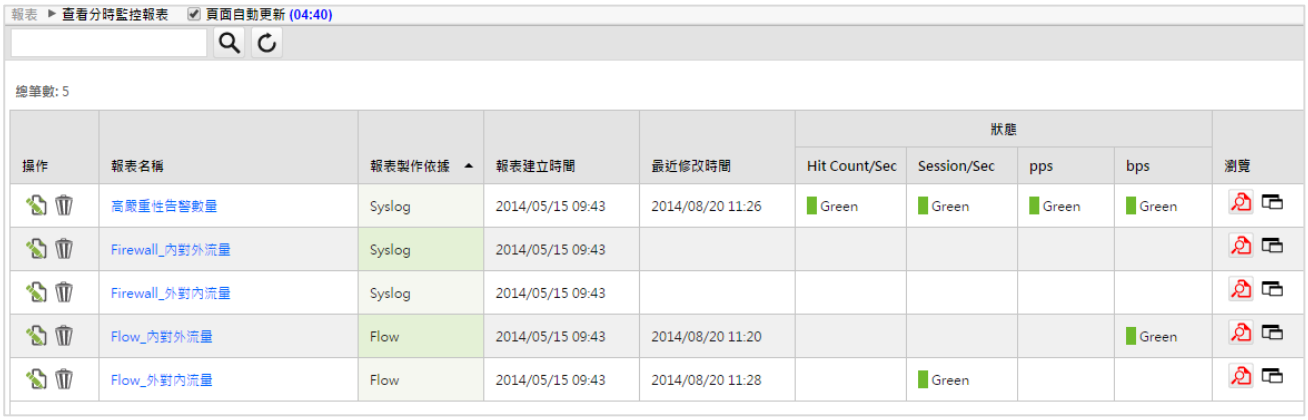
(9) E-mail 群組: 指定收件者的 E-mail 群組，請在「系統管理➔告警通報設定」中設定。

按下 »進階 或 «簡易 按鍵可切換進階告警設定模式及簡易告警模式，進階告警模式可設定預警(Yellow)閥值。

上述參數設定完成後，按下 確定 鈕，系統會把使用者設定的各種參數條件儲存起來。使用者可在「報表➔分時報表➔查看分時報表」中找到方才儲存的報表。按下 ↻ 鈕，則會清空所有輸入的條件內容。

4.3.2 查看分時監控報表

此選項的功能主要在於對已儲存之分時報表進行條件編輯與刪除動作。



已儲存分時報表搜尋

搜尋特定的已儲存報表，可輸入報表名稱(全部或是部份)，按下鈕進行搜尋。按下鈕，可以清除輸入的搜尋字串。

查看分時報表列表

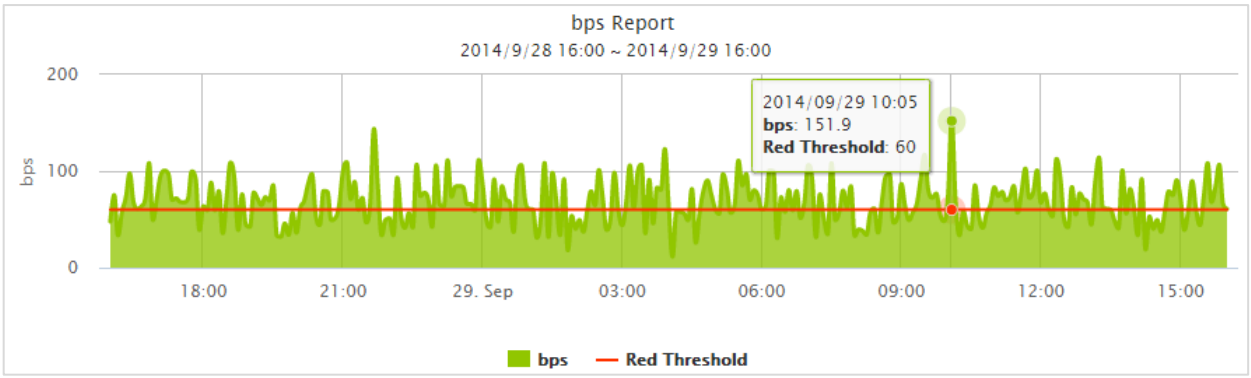
欄位說明如下：

- 操作：點擊圖示，系統會將頁面轉至「報表➔分時報表➔訂製分時報表」，並自動載入該筆已儲存的參數設定，此時可再次設定分時報表參數條件，設定完成後，可按「儲存報表」鈕，來覆蓋原本已存參數條件或按「另存查詢條件」鈕，來另存一個新的參數條件。點擊圖示，則刪除該筆分時報表。
- 報表名稱：為使用者自行定義的分時報表名稱，供使用者方便閱讀與辨識用。
- 報表製作依據：顯示該筆分時報表為以 Syslog 或是 Flow 作為製作依據。
- 報表建立時間：顯示該筆分時報表建立的時間。
- 最近修改時間：顯示該筆分時報表最近一次修改的時間。
- 狀態：系統共分為四類型的門檻值。
  - (1) Hit Count/Sec：表示每秒 Syslog 發生次數。
  - (2) Session/Sec：表示每秒的 Flow Session 數。
  - (3) pps：Packets per second，表示每秒的 Flow Packet 數。
  - (4) bps：Bits per second，表示每秒的 Flow Bits 數。
- 狀態：
  - (1) Green：數值低於 Yellow 門檻值，通常表示運作正常。
  - (2) Yellow：數值高於 Yellow 門檻值，但未超過 Red 門檻值，表示已發生問題需注意但仍算運作正常。
  - (3) Red：數值高於 Red 門檻值，通常表示可能已發生嚴重問題需特別注意。

若您持續收到 Yellow 或 Red 的通報，或大量狀態切換的通報，表示您所定義的門檻值不恰當需要再檢視。

■ 瀏覽：點  選鈕，彈出分時報表曲線圖，會依使用者所定義的報表製作依據呈現。Syslog、Server/App、Other 等條件，會繪製 Hit Count 分時曲線圖；Flow 會分別繪製 Session、Packet(pps)及 Bits(bps)分時曲線圖。頁面會列出 Hit Count、Session、Packets 及 Byts 在該時間內的總量，並計算出該時間內屬於 Yellow 及 Red 的時間比例。點選  鈕，系統會另開一新視窗顯示分時報表曲線圖，勾選「頁面自動更新」，其頁面會每 5 分鐘刷新一次。

使用者可輸入欲調閱分時報表的起迄時間區段，按 啟動查詢 鈕執行查詢。滑鼠移至頁面上其一曲線圖之特定點，系統會顯示事件發生量及精確時間，此時再點此特定點，系統會另開一「事件」視窗，其呈現該特定點詳細的事件列表。系統提供 Drill-down 查詢功能，使用者可再進一步深入分析(詳細事件操作功能，請參考「事件➔事件查詢」章節)。

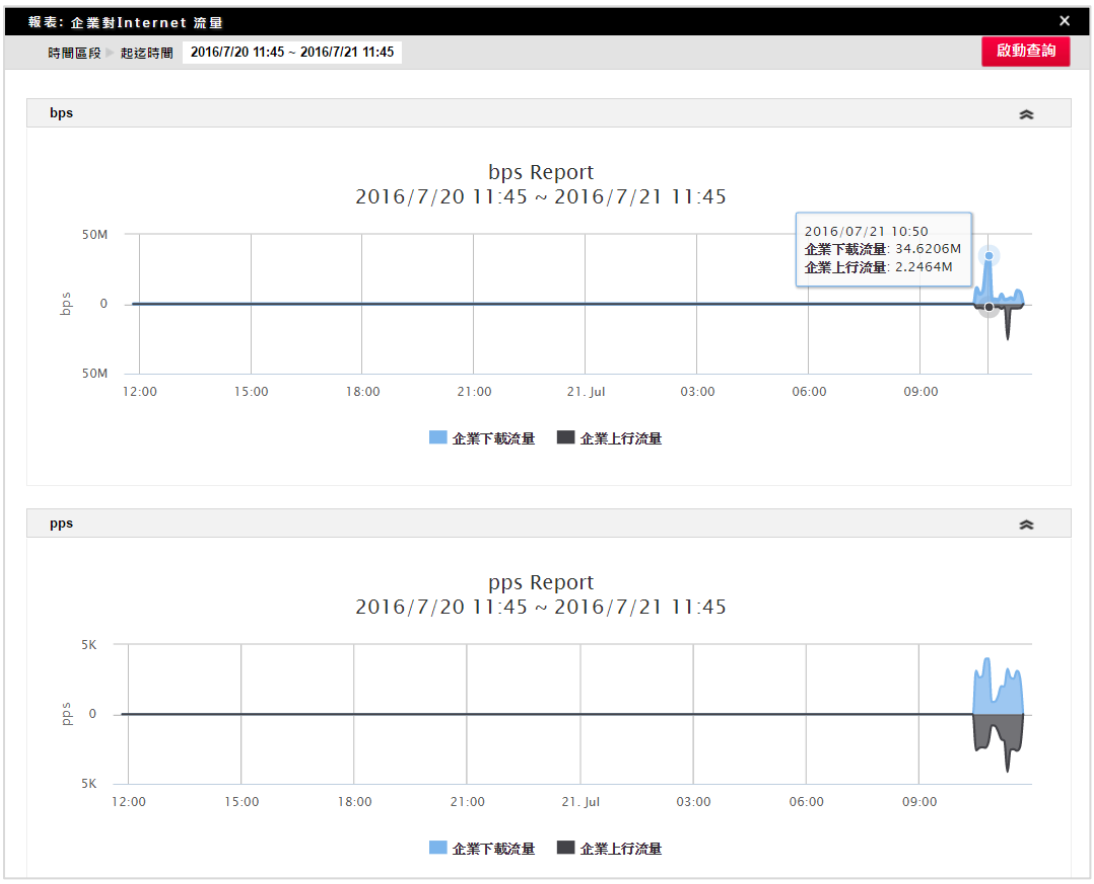


4.3.3 分時監控報表群組

提供使用者將多個分時監控報表指定為群組，讓多個分時監控報表的數值得以相互比較，或提供使用者定義任意條件的流入/流出流量圖。

列表欄位定義

- 操作：點選「分時監控報表群組」條件列表中的任一筆資料按下鈕及鈕，可以執行該筆報表的修改與刪除動作。
- 報表名稱：群組報表名稱。
- 報表製作依據：分時監控報表的資料來源。
- 報表建立時間：報表的建立時間。
- 最後修改時間：最後編輯報表設定的時間。
- 瀏覽：點選即可在視窗內瀏覽分時報表群組的 T 型圖，如下圖。點選則會另開視窗提供長時間監看，每 5 分鐘自動更新報表。



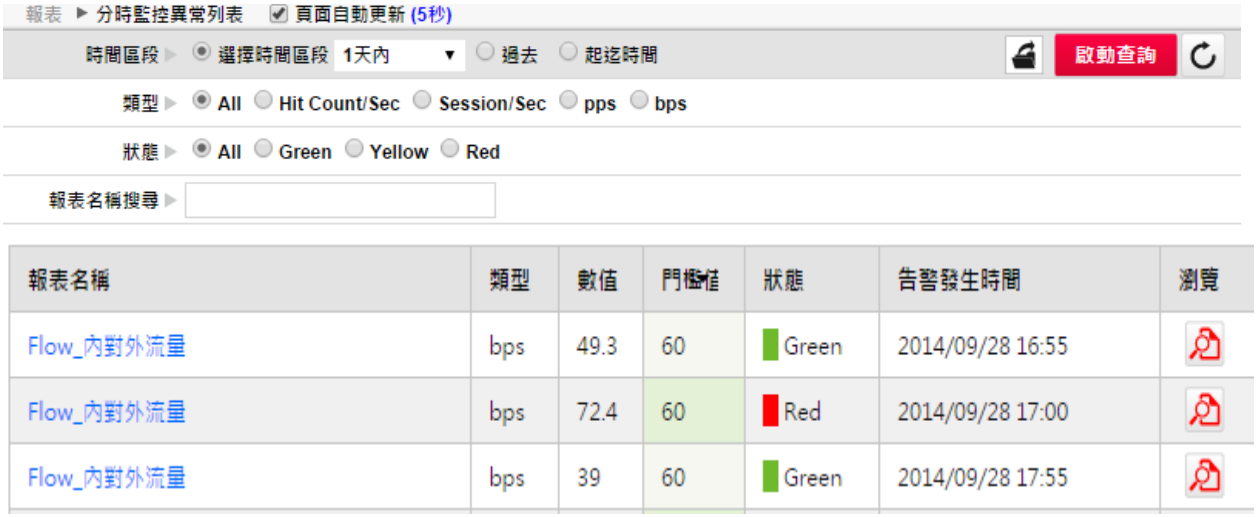
按鈕操作

在搜尋列可以輸入分時監控報表群組名稱 (全部或是部份) 來進行過濾，例如輸入 “人事” 可以找到人事部門的相關報表群組。按下  按鈕，彈出新增分時監控報表群組視窗 (如下圖)。

- 名稱：請輸入群組報表名稱。
- 類型：指定資料來源為 Syslog 或 Flow，系統僅能將同一種類型的分時監控報表加入群組進行數值比對。
- In：新增位於群組報表 T 型圖上方的報表，會依勾選的「類型」列出同一類型的分時監控報表。
- Out：新增位於群組報表 T 型圖下方的報表。

4.3.4 分時監控異常列表

此選項的功能主要在於對已儲存之分時報表所發送的警示進行搜尋。



報表查詢與輸出

提供以下三種查詢功能，在輸入搜尋條件後，按 啟動查詢 鈕，執行查詢動作。按鈕 可清除所輸入的搜尋條件。按下 鈕，可將查詢結果輸出為 PDF、CSV 或 XML 檔案。

- 報表名稱搜尋：搜尋特定的已儲存分時報表，請輸入報表名稱(全部或是部分)。
- 類型：點選某一類型，可以僅列出某種類型的警示。
- 狀態：點選某一狀態，可以僅列出某種狀態的警示。
- 查詢時間區段：點選「選擇時間區段」、「過去」或「起迄時間」的時間區段進行查詢。

報表列表

點選列表表頭任一項目標題，系統會根據該項目進行遞增排序與遞減排序(如下圖紅框所示)。

列表欄位說明如下：

- 報表名稱：為使用者自行定義的分時報表名稱，供使用者方便閱讀與辨識用。
- 類型：顯示該警示的狀態是屬於 Hit Count/Sec、Session/Sec、pps 或 bps。
- 數值：顯示該警示當時的數值。
- 門檻值：顯示該警示狀態改變時的門檻值。
- 狀態：顯示所訂製的分時報表的數值與門檻值的關係，共分為以下狀態：

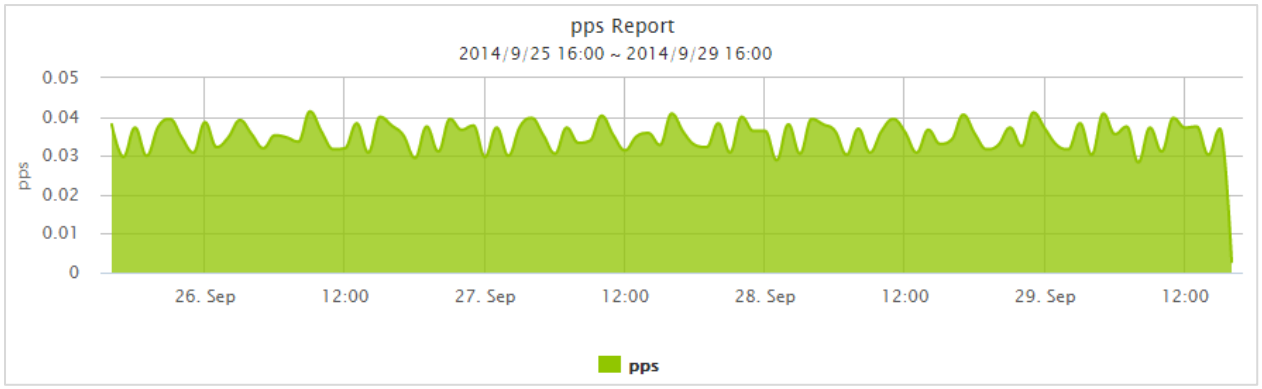
(1) Green：數值低於 Yellow 門檻值，通常表示運作正常。

(2) Yellow：數值高於 Yellow 門檻值，但未超過 Red 門檻值，通常表示已發生問題需　注意但仍算運作正常。

(3) Red：數值高於 Red 門檻值，通常表示可能已發生嚴重問題需特別注意。

若您持續收到 Yellow 或 Red 的通報，或大量狀態切換的通報，表示您所定義的門檻值不恰當需要再檢視。

- 告警發生時間：顯示警示狀態改變發生的時間。
- 瀏覽：點選  鈕，彈出分時報表曲線圖，會自動繪出警示發生前 1 小時的曲線圖。Syslog、Server/App、Other 會繪製 Hit Count 分時曲線圖；Flow 會分別繪製 Session、Packet(pps)及 Bits(bps)分時曲線圖。頁面會列出 Hit Count、Session、Packets 及 Byts 在該時間內的總量，並計算出該時間內屬於 Yellow 及 Red 的時間比例。



若 Red 或 Yellow 所佔的時間比例很高(例如 Yellow 80%或 Red 30%)，表示網路長時間處於不良狀況，而非一時的突發，必須特別注意。

使用者可輸入欲調閱分時報表的起迄時間區段，按 啟動查詢 鈕執行查詢。將滑鼠移至頁面上其一曲線圖之特定點，系統會顯示事件發生量及精確時間，此時再點此特定點，系統會另開一「事件」視窗，其呈現該特定點詳細的事件列表。系統提供 Drill-down 查詢功能，使用者可再進一步深入分析(詳細事件操作功能，請參考「事件➔事件查詢」章節)。

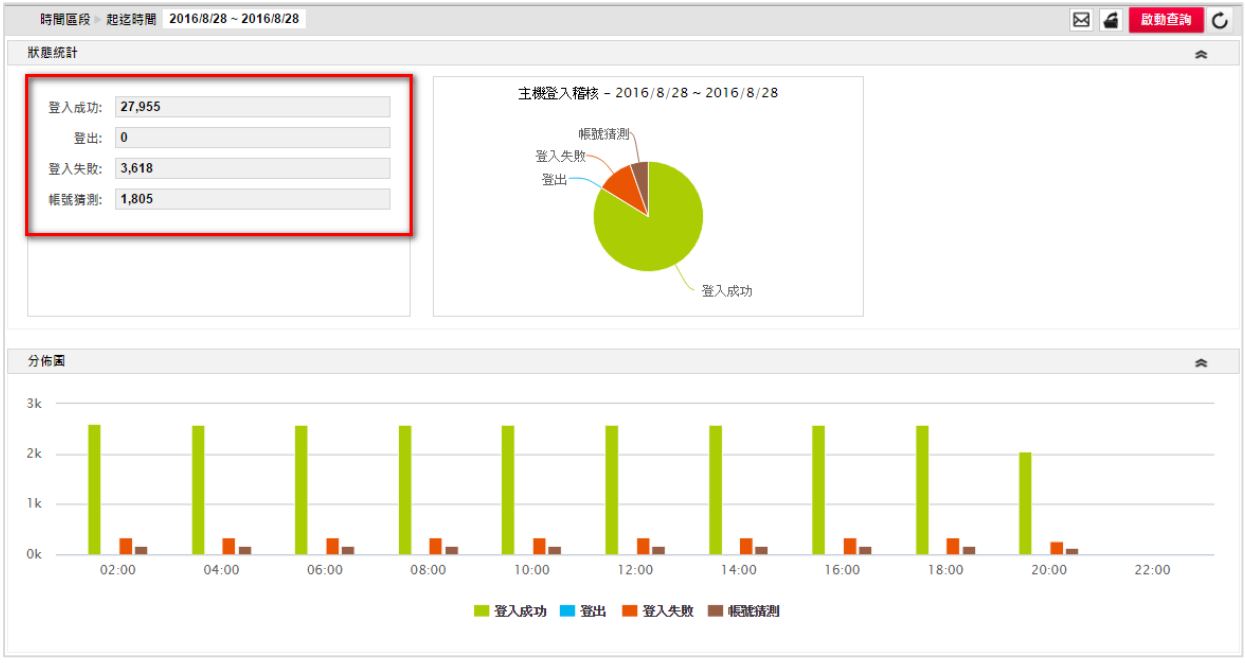
4.4 稽核報表

「伺服器稽核」功能可以分析蒐集來的系統伺服器主機 Log，讓您迅速掌握伺服器異常登錄、存取及執行的狀況，以進一步排除資安問題。N-Reporter 針對「主機登入稽核」、「Windows 檔案分享」、「Oracle」、「MySQL」、「PostgreSQL」、「MS SQL Server」等資料庫稽核，讓使用者快速掌握是否發生資安狀況。

Server 4.4.1 伺服器稽核

此選項的功能中，N-Reporter 預設提供使用者「主機登入稽核」、「Windows 檔案分享」、「Oracle 登入稽核」、「MySQL 登入稽核」及「PostgreSQL 登入稽核」等稽核報表。

■ 點選「查詢條件名稱」欄位的「主機登入稽核」或瀏覽圖示，可進一步查詢相關資訊。



紅框處會列出整個網路所有主機的各項目加總數值。

(1) 登入成功：使用正確帳號密碼登入。

(2) 登出：離開系統。

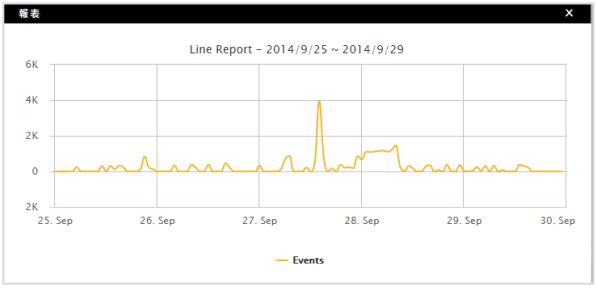
(3) 登入失敗：代表帳號輸入正確，但密碼輸入錯誤。(發生大量時，很有可能就是入侵的警訊。)

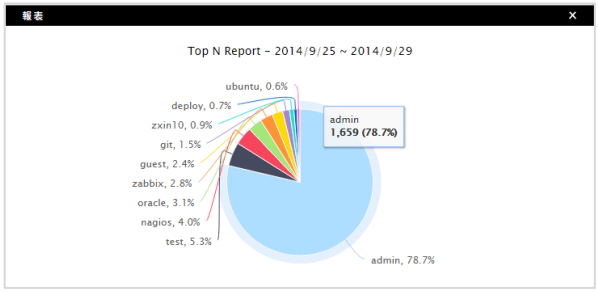
(4) 帳號猜測：任意的猜測主機的帳號密碼。(發生大量時，很有可能就是入侵的警訊。)

設備名稱	登入成功	登出	登入失敗	帳號猜測
210.71.213.25	6 (0%)	5 (0%)	28733 (64%)	16086 (35.8%)
Win_AD_140.131.164.200	381 (4.2%)		1237 (13.6%)	7415 (82%)

上方列表可顯示每部主機各別的數值，可快速得知整體網路狀況，也可以進一步了解這些狀況是發生於哪些主機上。

■ 點選列表中異常數量的  圖示，可以選擇依「使用者帳號」或是「用戶端 IP」進行排序，選擇曲線圖或圓餅圖可以畫出猜測行為，以了解問題發生的時間區段(如下圖)。





當某個使用者帳號被大量猜測密碼時，請特別注意此帳號的密碼是否被設置得太過於簡單。而當某個用戶端 IP 大量的進行猜測時，表示此部電腦可能遭受到木馬威脅，此時可以透過「事件」的阻擋功能將這些 IP 阻擋於網路之外。

■ 按  鈕，系統將彈出「離線報表設定」視窗，並進行以下設定：

(1) 報表名稱：顯示目前所點選的報表。

(2) 報表型態：可以勾選定期產生日報表、週報表及月報表。

(3) E-Mail 群組：下拉式選項供使用者選取預先定義的 E-Mail 群組

(請參考「系統管理➔系統通報設定➔建立 E-Mail 群組」章節)。

(4) 資料格式：設定寄送的資料格式(HTML/PDF/CSV/XML)。

■ 按  鈕，系統將彈出「匯出報表」視窗，使用者可以選擇 PDF、CSV、XML 格式，並將查詢得到的列表內容輸出。

4.4.2 法規報表

針對個資法需求，以及滿足國際法規如 HIPPA、SOX，N-Reporter 提供主機稽核的法規報表。

在法規報表頁面，可以依選取的日期提供以下報表:

■ 時間區段

時間區段可以指定起迄日期，預設查詢近兩日的統計資料，可依需求調整為某月份(例如 3/1~3/31)或是某一季(例如 1/1~3/31)來產生法規報表。

■ 使用者活動紀錄

使用者活動紀錄

總筆數: 6

設備名稱	登入	登出	登入失敗
PostgreSQL 1.1.1.7	8592 (28.5%)	8592 (28.5%)	12888 (42.8%)
Oracle 1.1.1.6	11454 (44.4%)	7160 (27.7%)	7160 (27.7%)
My SQL 1.1.1.5	5720 (66.6%)		2860 (33.3%)
Linux 1.1.1.3	2842 (40%)	1420 (19.9%)	2840 (39.9%)
MS SQL 1.1.1.4	1430 (33.3%)		2860 (66.6%)
Win2k3 cht 192.168.2.71	8 (53.3%)	6 (40%)	1 (6.6%)

■ 物件存取報表

物件存取報表

總筆數: 3

設備名稱	檔案讀取	檔案修改	檔案刪除	讀取錯誤	其它
Win2k8 AD DC cht 192.168.2.80					1430 (100%)
Win2k3 AD DC 192.168.2.70					1428 (100%)
Win2k3 cht 192.168.2.71	8 (33.3%)	16 (66.6%)			

■ 系統事件報表

系統事件報表

總筆數: 2

設備名稱	開機	關機	程序起動	程序關閉	其它
Win2k8 AD DC cht 192.168.2.80	1430 (20%)	1430 (20%)	1430 (20%)	1430 (20%)	1430 (20%)
Win2k3 AD DC 192.168.2.70	1427 (20%)	1427 (20%)	1427 (20%)	1427 (20%)	1427 (20%)

■ 追蹤帳戶管理的變更

追蹤帳戶管理的變更

總筆數: 2

設備名稱	建立使用者	刪除使用者	變更使用者密碼
Win2k8 AD DC cht 192.168.2.80	1430 (24.8%)	1430 (24.8%)	2904 (50.3%)
Win2k3 AD DC 192.168.2.70	1427 (25%)	1427 (25%)	2854 (50%)

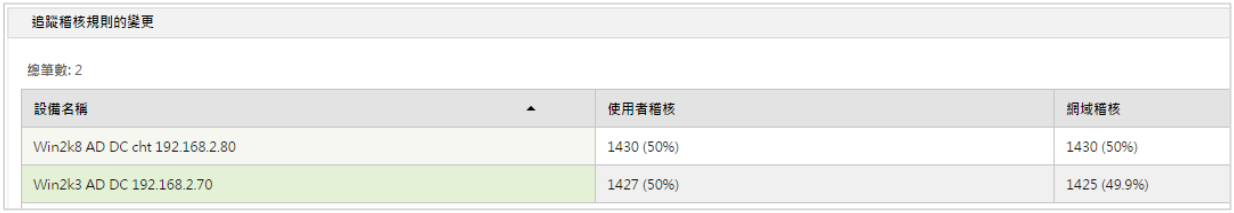
■ 追蹤使用者群組的變更

追蹤使用者群組的變更

總筆數: 2

設備名稱	建立群組	變更群組	刪除群組
Win2k8 AD DC cht 192.168.2.80	2860 (50%)	1430 (25%)	1430 (25%)
Win2k3 AD DC 192.168.2.70	2854 (50%)	1427 (25%)	1427 (25%)

■ 追蹤稽核規則的變更



點選離線報表設定可以進行法規報表的日週月報的建立，並指定 E-Mail 群組及資料格式。 也可以直接點選資料匯出直接產生 PDF 的法規報表。

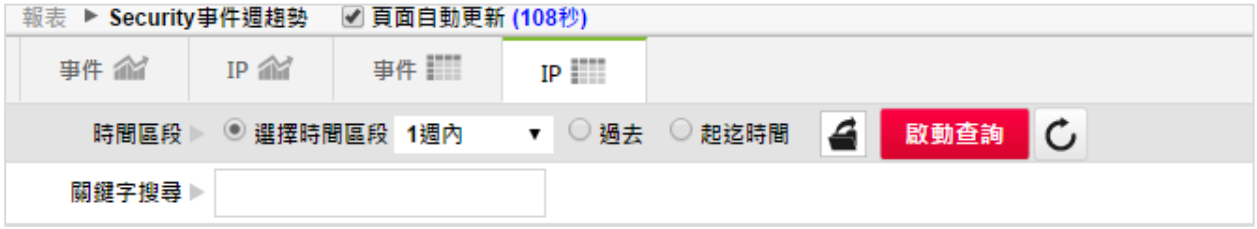
4.5 趨勢分析

「趨勢報表」是 N-Reporter 的主要應用之一。N-Reporter 內建的動態演算法則能根據蒐集到的 Syslog Data 與 Flow Data，歸納出事件行為與流量行為的歷史軌跡，自動找出任何次數(Hit Count)/Bytes 數或是 Packets 數出現異常突增的事件、來源 IP(通常是攻擊端)以及目的 IP(通常是被攻擊端)後，發送告警給使用者。N-Reporter 將持續追蹤這些出現異常的事件與 IP 並且呈現分析結果於趨勢報表功能中。使用者無需設定任何門檻值(Threshold)即可充分掌握網路環境裡值得注意的變化，讓維運網路工作顯得更輕鬆容易。

4.5.1 Security 事件週趨勢

統計所有事件、來源與目的 IP 過去一週的平均值後，再比對今日的資料，自動分析出 Hit Count 次數突增的事件、來源 IP 與目的 IP，協助使用者掌握以週為觀點的資安與網路異常使用趨勢變化。

Syslog 週趨勢分析查詢與輸出

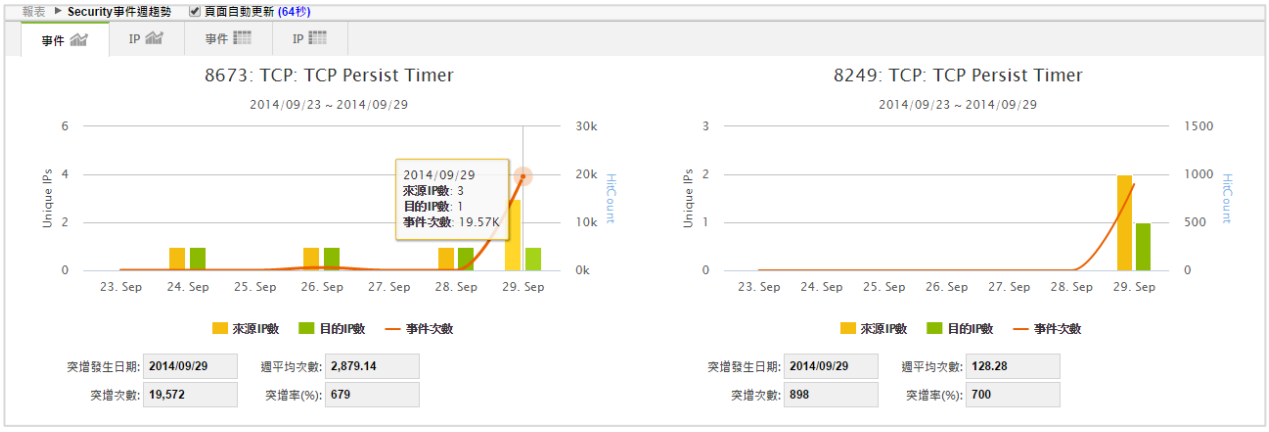


- **事件趨勢圖-根據事件**：採用趨勢圖型，列出當日事件 Hit Count 值高於過去一週平均者，最多可呈現 8 個趨勢升高的事件。
- **IP 趨勢圖-根據 IP**：採用趨勢圖型，列出當日事件 Hit Count 值高於過去一週平均的來源 IP 及目的 IP，最多可呈現 8 個趨勢升高的來源 IP 及目的 IP。
- **事件趨勢表-根據事件**：採用表格方式，列出當日事件 Hit Count 值高於過去一週平均者。
- **IP 趨勢表-根據 IP**：採用表格方式，列出當日事件 Hit Count 值高於過去一週平均的來源 IP 及目的 IP。

> 選擇「趨勢表-根據事件」或「趨勢表-根據 IP」項目，系統會出現關鍵字搜尋及查詢時間區段功能，使用者可依據需求查詢特定時段內的特定事件、IP 等。

- **「關鍵字搜尋」**可以輸入事件名稱、來源 IP 或目的 IP 進行過濾。
- **「查詢時間區段」**可點「選擇時間區段」、「過去」或「起迄時間」的時間區段進行查詢。在輸入搜尋條件後，按 啟動查詢 鈕，執行查詢動作。按鈕，可清除所輸入的搜尋條件。按下鈕，可將查詢結果輸出為 PDF、CSV 或 XML 檔案。

趨勢圖操作



- 左縱軸表示 IP 數，顯示照造成此事件的來源 IP(橘色柱狀棒)與目的 IP(綠色柱狀棒)各是多少個。
- 右縱軸表示事件數。
- 水平橫軸表示時間。
- 將滑鼠移到線上可顯示來源 IP 數、目的 IP 數、事件次數。
- 趨勢圖說明項目如下：
  (1) 突增發生日期：為該突增情況發生的時間點。
  (2) 突增次數：為該突增事件的 Hit Count 數、突增來源 IP 所造成的 Hit Count 數或該突增目的 IP 接收到的 Hit Count 數。
  (3) 週平均次數：過去一週的平均 Hit Count 數。
  (4) 突增率(%)：(突增次數 / 週平均次數)×100。
- 點選趨勢圖，系統會另開一「事件」視窗，其呈現趨勢圖詳細的事件列表。
- 系統提供 Drill-down 查詢功能，使用者可再進一步深入分析(詳細事件操作功能，請參考「事件➔事件查詢」章節)。

趨勢表操作

- 選擇「趨勢表-根據 IP」項目，趨勢表的列表呈現方式將分為兩表：「內部網段(Home)」與「非內部網段(Non-Home)」。

■ 如果突增的來源 IP 或目的 IP 是落在使用者所定義的 Home 網段中，則系統將會把該來源 IP 或目的 IP 放在「內部網段(Home)」的表格中。

(Home 網段定義請參考「系統管理➔名稱解析」章節)

■ 「內部網段(Home)」與「非內部網段(Non-Home)」的分類方式，可以讓使用者優先關注在內部網段發生異常突增的 IP，而不需在一堆 IP 資料中慢慢查找，爭取除錯時效。

如：組織內部有一台 PC 突然發送大量的事件(可能遭植入惡意控制程式並從組織內部發動攻擊)，使用者可以很快地在來源 IP 的 Home 網段中看見這台 PC，以進行必要的後續處置。

(1) 事件 / 來源 IP / 目的 IP：顯示發生突增異常的事件名稱 / 來源 IP / 目的 IP。使用者可以點選該項目中的事件名稱 / 來源 IP / 目的 IP 作 Drill Down 細部查詢，系統會另開一「事件」視窗，其呈現該事件 / 來源 IP / 目的 IP 發生突增當天的詳細內容，使用者可再進一步深入分析(詳細事件操作功能，請參考「事件➔事件查詢」章節)。

(2) 突增發生日期：為該突增情況發生的時間點。

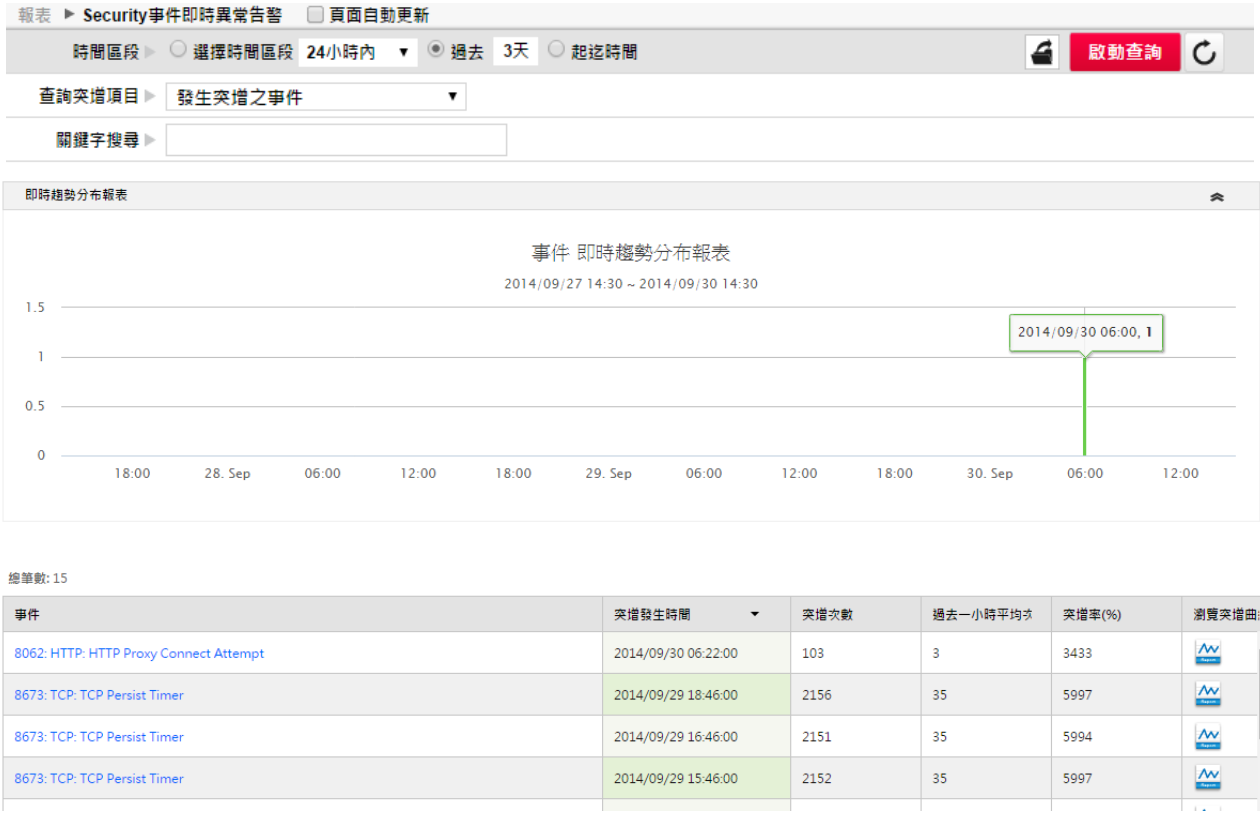
(3) 突增次數：為該突增事件的 Hit Count 數、突增來源 IP 所造成的 Hit Count 數或該突增目的 IP 接收到的 Hit Count 數。

(4) 週平均次數：過去一週的平均 Hit Count 數。

(5) 突增率(%)：(突增次數 / 週平均次數)×100。

4.5.2 Security 事件即時異常告警

根據最近一小時的歷史資料自動分析出事件數(Hit Count)突增的事件、來源 IP 與目的 IP，協助使用者即時掌握資安與網路異常使用的趨勢變化。



Syslog 即時趨勢報表查詢與輸出

提供以下三種查詢功能，在輸入搜尋條件後，按 啟動查詢 鈕，系統將繪製出即時趨勢分佈圖及報表。按 鈕，可清除所輸入的搜尋條件。按下 鈕，可將查詢結果輸出為 PDF、CSV 或 XML 檔案。

- 查詢時間區段：點選「選擇時間區段」、「過去」或「起迄時間」的時間區段進行查詢。
- 查詢突增之項目：
  (1) 發生突增之事件：列出哪些事件的瞬間 Hit Count 值高於過去一小時平均值。
  (2) 發生突增之來源 IP：列出哪些來源 IP 瞬間造成高於過去一小時平均值的事件數，這些來源 IP 很可能是惡意攻擊者。
  (3) 發生突增之目的 IP：列出哪些目的 IP 瞬間接收到高於過去一小時平均值的事件數，這些目的 IP 很可能正遭受到惡意攻擊中。
- 關鍵字搜尋：可以輸入事件名稱、來源 IP 或目的 IP 進行過濾(全部或是部份)。

Syslog 即時趨勢分佈報表

將滑鼠移至柱狀棒上，會顯現該時間點共發生幾次突增現象。

時間軸的定義端看使用者所選擇的時間區段長短。

Syslog 即時趨勢報表列表

- 「查詢突增之項目」下拉選單中選擇「發生突增之來源 IP」或「發生突增之目的 IP」項目，列表呈現方式將分為兩表：「內部網段(Home)」與「非內部網段(Non-Home)」。
- 如果突增的來源 IP 或目的 IP 是落在使用者所定義的 Home 網段中，則系統將會把該來源 IP 或目的 IP 放在「內部網段(Home)」的表格中。

  (Home 網段定義請參考「系統管理➔名稱解析」章節)
- 為了增加 IP 判讀的方便性，N-Reporter 會試圖解譯出 IP 所代表的名稱解析或主機名稱，用括號的方式標注在 IP 之後。
- 「內部網段(Home)」與「非內部網段(Non-Home)」的分類方式，可以讓使用者優先關注在內部網段發生異常突增的 IP，而不需在一堆 IP 資料中慢慢查找，爭取除錯時效。如：組織內部有一台伺服器突然收到大量的流量，使用者可以很快地在目的 IP 的 Home 網段中看見這台伺服器，進一步找到攻擊來源，以進行必要的後續處置。
- 欄位說明如下：

  (1) 事件 / 來源 IP / 目的 IP：顯示發生突增異常的事件名稱 / 來源 IP / 目的 IP。使用者可以點選該項目中的事件名稱 / 來源 IP / 目的 IP 作 Drill Down 細部查詢，系統會另開一「事件」視窗，其呈現該事件 / 來源 IP / 目的 IP 的詳細行為內容，使用者可再進一步深入分析造成這次突增異常的原因。

  (詳細事件操作功能，請參考「事件　事件查詢」章節)

  (2) 突增發生時間：為該突增情況發生的時間點。

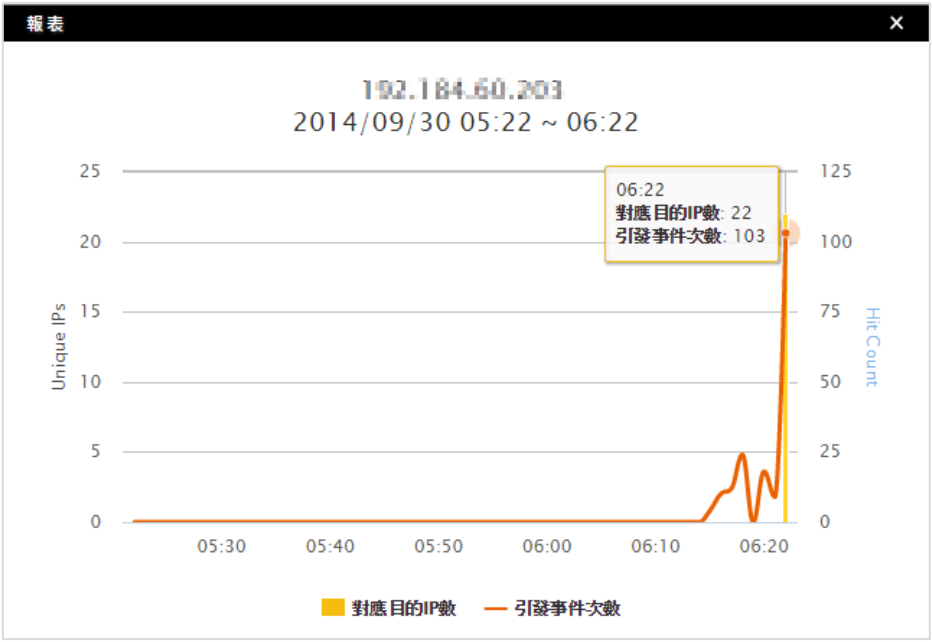
  (3) 突增次數：為該突增事件瞬間的 Hit Count 數、突增來源 IP 所造成瞬間的 Hit Count 數或該突增目的 IP 接收到瞬間的 Hit Count 數。

  (4) 過去一小時平均次數：過去一小時的平均 Hit Count 數。

  (5) 突增率(%)：(突增次數 / 過去一小時平均次數)×100。

  (6) 瀏覽突增曲線：點選  鈕可查看該項目的「即時趨勢圖」。點選趨勢圖，系統會另開一「事件」視窗，其呈現趨勢圖詳細的事件列表。系統提供 Drill-down 查詢功能，使用者可再進一步深入分析。

詳細事件操作功能，請參考「事件➔事件查詢」章節)



實際運用流程：

1.使用者收到系統發送的異常突增告警信件。

2.登入系統，查閱「Syslog 即時趨勢報表」，找到該筆異常事件或是 IP 資料。

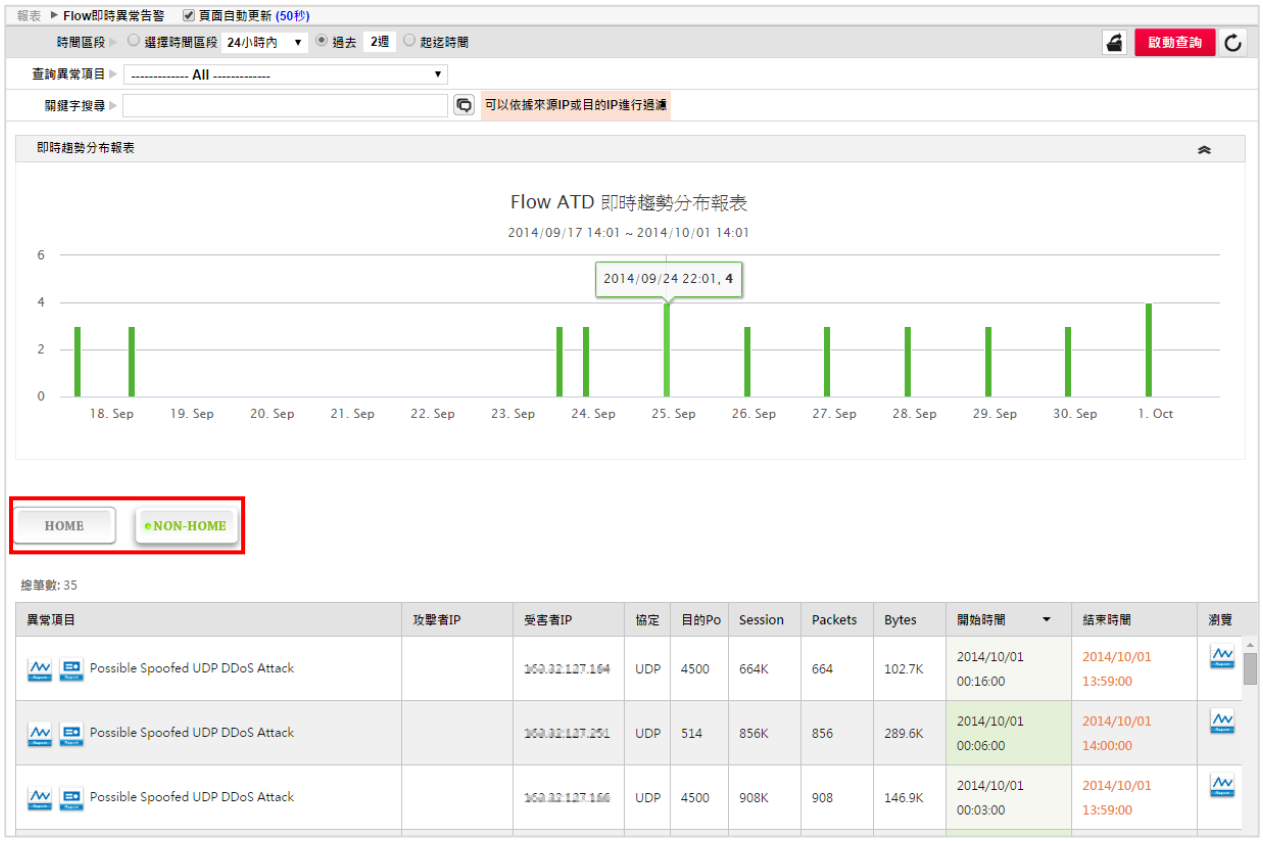
3.Drill Down 查詢詳細與該事件或是 IP 相關的行為內容並搜尋出造成這次事件的來源 IP 群。

4.在事件列表按滑鼠右鍵使用 Action Module 進行惡意來源 IP 的阻擋，以排除網路的異常狀況。

Flow

4.5.3 Flow 即時異常告警

在「Flow 異常流量報表」功能中，系統會根據最近一小時的歷史資料自動分析出該注意的攻擊行為，協助使用者即時掌握資安與網路異常使用的趨勢變化。



Flow 異常流量報表查詢與輸出

提供以下三種查詢功能，在輸入搜尋條件後，按 啟動查詢 鈕，系統將繪製出即時趨勢分佈圖及報表。按 鈕，可清除所輸入的搜尋條件。按下 鈕，可將查詢結果輸出為 PDF、CSV 或 XML 檔案。

- 查詢時間區段：點選「選擇時間區段」、「過去」或「起迄時間」的時間區段進行查詢。
- 查詢突增項目：系統提供 20 種攻擊行為分析。

(1) UDP Port Scan
(2) TCP SYN Port Scan
(3) Host Scan
(4) TCP SYN Host Scan
(5) SQL Server Host Scan
(6) MySQL Host Scan
(7) Possible Spoofed UDP DDoS Attack
(8) Possible Spoofed TCP SYN DDoS Attack
(9) Possible Spoofed TCP SYN/ACK DDoS Attack
(10) Possible Spoofed TCP FIN/ACK DDoS Attack
(11) Possible Spoofed TCP Rst DDos Attack
(12) Possible Spoofed TCP NULL Flag Attack
(13) Possible Spoofed ICMP DDoS Attack
(14) Land Attack
(15) Burst pps on Source Port
(16) Burst pps on Destination Port
(17) Burst bps on Source Port
(18) Burst bps on Destination Port
(19) Burst Session on Source
(20) Burst Session on Destination

(門檻值及監控狀態可在「系統管理➔偏好設定➔異常流量」中作設定)

- 關鍵字搜尋：可依據來源 IP 或目的 IP 進行過濾(全部或是部份)。

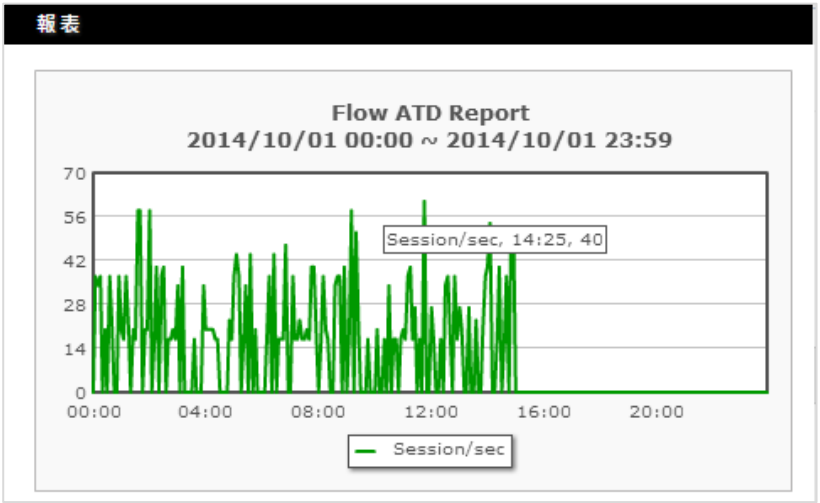
「即時趨勢分佈報表-趨勢圖」

將滑鼠移到柱狀棒上，可顯示確切的時間點、定義的時間區段。每根柱狀棒表示該時間點共發生幾次突增現象，時間點的定義端看使用者所選擇的時間區間長短。

「即時趨勢分佈報表-趨勢表」

列表欄位說明如下：

- 列表呈現方式將分為兩種：「內部網段(Home)」與「非內部網段(Non-Home)」(如上圖紅色框處)，如果突增的來源 IP 或是目的 IP 位在使用者定義的 Home 網段(「系統管理➔名稱解析」下可以定義 Home 網段)，則系統會將該來源 IP 或是目的 IP 放在「內部網段(Home)」表格中。這樣的分類可以讓使用者優先關注發生在內部的異常行為，不需在一堆 IP 資料中慢慢查找，爭取除錯時效。例如：組織內部有一個伺服器突然受到大量的 Port 掃描攻擊，使用者可以很快在目的 IP 的 Home 網段中看見這部伺服器，以進行必要的處置行為。
- 「異常項目」：顯示異常項目。
- 「攻擊者 IP」/「受害者 IP」：顯示發生異常行為的攻擊者 IP/受害者 IP。點選該項目中的攻擊者 IP/受害者 IP，系統會轉至「事件」功能呈現該 IP 當時的詳細事件列表，系統有提供 Drill-down 功能，供管理者進一步深入分析。
- 「協定」、「來源 Port」、「目的 Port」：協助管理者瞭解到該事件是相對應到哪個應用，以快速決定對策。
- 「Session」、「Packet」、「Byte」：該異常行為所造成的瞬間 Session 數、Bytes 數及 Packets 數。
- 「開始時間」、「結束時間」：顯示異常情況發生的時間。
- 「瀏覽」：可查看該項目的流量曲線圖(如下圖)。



實際運用流程：

1.使用者收到系統發送的異常流量的告警信件。

2.登入系統，查閱「Flow 異常流量報表」，找到該筆異常 IP。

3.Drill Down 查詢詳細與該 IP 相關的當下 Flow 通聯資料，搜尋出造成這次事件的來源 IP 群。

4.在事件列表按滑鼠右鍵使用 Action Module 進行惡意來源 IP 的阻擋，排除網路的異常狀況。

4.6 異常 IP 阻擋

在此章節會介紹「異常 IP 阻擋」下之子功能：「IP 阻擋列表」、「訂製自動阻擋」等各項設定。

Action

4.6.1 IP 阻擋列表

此選項的功能中，使用者透過 Action 執行 IP 阻擋動作之後，系統會將 IP 阻擋過程記錄下來，使用者可在「IP 阻擋列表」查閱阻擋訊息及提供手動復原機制(IP 恢復通行)。

IP 阻擋指令可下達至 N-Reporter 能支援的 L2 Switch 或是 Syslog 設備上。

訂製手動阻擋

按下鈕，彈出 IP 阻擋視窗(如下圖所示)，使用者可設定阻擋時間的長短。

阻擋 IP 查詢與輸出

提供以下三種查詢功能，在輸入搜尋條件後，按 啟動查詢 鈕，執行查詢動作。按鈕，可清除所輸入的搜尋條件。按下鈕，可將查詢結果輸出為 PDF、CSV 或 XML 檔案。

- 時間區段：點選「選擇時間區段」、「過去」或「起訖時間」的時間區段進行查詢。點選「全部資料」則列出全部 IP 阻擋訊息。
- 資料來源：選擇查詢目前阻擋中的資料或者歷史阻擋資料。
- 阻擋狀態：選擇欲查詢的阻擋狀態。

(1) 全部：表示欲查詢全部的資料。

(2) 阻擋中：表示欲查詢目前正在執行阻擋的 IP 資料。

(3) 已復原：表示欲查詢曾經阻擋過但是已經恢復連線的 IP 資料。

■ 阻擋 IP 搜尋：搜尋特定的遭阻擋的 IP。請輸入字串或是 IP(全部或是部份)，以針對「阻擋 IP」、「執行阻擋設備名稱」或「執行阻擋設備 IP」欄位進行搜尋。

由事件列表進行阻擋

■ 在事件列表中點擊滑鼠右鍵，可呼叫出操作清單，操作清單上可選擇「阻擋來源 IP」、「阻擋/A10 保護目的 IP」，直接進行所選項目上的 IP 進行阻擋。

選擇進行阻擋的設備種類及設備及自動復原週期，按下確定即可進行阻擋。

IP 阻擋列表

阻擋IP/MAC	執行阻擋設備名稱	阻擋類別	阻擋狀態	阻擋時間	復原時間	自動復原週期(min)
192.168.200.254	TP 192.168.2.77	IPS/Firewall(手動阻擋)	已阻擋	2014/10/01 17:30:00		60
111.111.111.111	TP 192.168.10.14, TP 192.168.2.77	IPS/Firewall(手動阻擋)	已復原	2014/10/01 17:30:00	2014/10/08 08:00:00	
192.168.100.124	TP 192.168.2.77, TP 192.168.10.14	IPS/Firewall(手動阻擋)	已阻擋	2014/10/01 17:20:00		60
192.168.100.123	TP 192.168.2.77, TP 192.168.10.14	IPS/Firewall(手動阻擋)	已阻擋	2014/10/01 17:00:00		60

列表欄位說明：

■ 阻擋 IP：顯示哪個 IP 遭到使用者的阻擋。

■ 執行阻擋設備名稱：顯示使用哪個設備執行阻擋工作。概括論之，內網 IP 的阻擋工作會交由 L2 Switch

執行，而來自外網的惡意 IP 則交由 Syslog 設備(通常是 Firewall 或是 IPS)執行。

- 阻擋狀態：顯示該阻擋 IP 目前是「阻擋中」或「已復原」的阻擋狀態。
- 阻擋時間：顯示使用者在哪個時間點執行阻擋動作。
- 復原時間：顯示使用者在哪個時間點停止阻擋動作以恢復該 IP 的連線。
- 自動復原週期：顯示使用者在執行阻擋指令時所預定的阻擋週期，當這個時間到達後，系統會自動將阻擋指令從執行阻擋設備中移除，恢復該 IP 的連線。

使用者可以視需求手動恢復阻擋 IP 的連線，不一定要等到自動復原週期時間過後，再由系統自動解除之。勾選表格左方的核取方塊(可多選同時釋放多筆 IP)，按下畫面右上方的 復原 IP 阻擋 鈕，即可以進行手動復原。

Action 4.6.2 訂製自動阻擋

此選項的功能主要在讓使用者可以針對特定條件進行自動阻擋，當達到所設定的阻擋條件時，立即執行阻擋並寄發警示通知於系統收件者，最多允許使用者訂定 64 筆自動阻擋。

訂製自動阻擋的過濾條件和事件查詢的操作方式相同，請參考「事件➔事件查詢」章節。設定完過濾條件後，按下  鈕後會彈出阻擋條件的設置，依照「報表製作依據」為 Syslog 或是 Flow 時，在阻擋的條件上會有此許的不同。

阻擋條件根據 Syslog

- 名稱：請輸入一個容易辨識的名稱字串。
- 執行週期：請選擇欲執行週期。
- 門檻值：請輸入欲警示的門檻值，在根據 Syslog 則為 Hit count/Sec。
- 選擇阻擋對象：選擇欲阻擋的「來源 IP」或「目的 IP」。
- 自動阻擋：選擇「自動阻擋並發送告警」或「僅發送告警」。
- 阻擋設備：選擇欲執行阻擋的 IPS 設備。
- 自動復原週期：選擇在執行阻擋指令所預定的阻擋週期後，系統會自動在時間點內停止阻擋動作以恢復該 IP 的連線。
- E-mail 群組(報表收件者)：下拉式選項供使用者選取預先定義的 E-Mail 群組(請參考「系統管理➔系統通報設定➔建立 E-Mail 群組」章節)。
- E-Mail 通報週期：選擇通報的發送週期。

阻擋條件根據 Flow

- 門檻值：請輸入欲警示的門檻值，在過濾條件根據 Flow 時為 pps 單位及 bps 單位可選擇為 ”” (bps)、K(bps)、M(bps)、G(bps)。

若欲修改訂製自動阻擋相關資訊，請在「已儲存自動阻擋」列表中該項目的「操作」欄位，點擊欲修改項目圖示，則可編輯所選訂製自動阻擋相關資訊。若欲刪除訂製自動阻擋，則點擊圖示，系統則會刪除該訂製自動阻擋。

已儲存自動阻擋

顯示目前系統訂製自動阻擋相關資訊。點選列表表頭任一項目標題，系統會根據該項目進行遞增排序與遞減排序。

列表欄位說明如下：

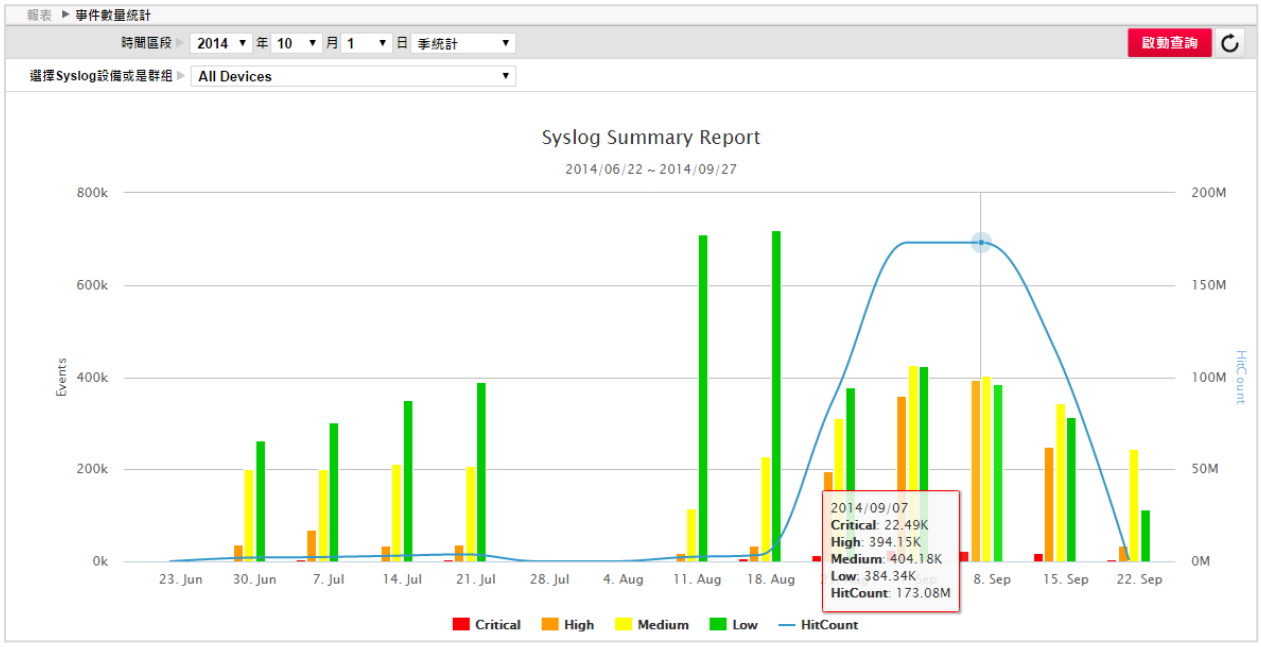
- 名稱：顯示訂製自動阻擋對應中的名稱部分。
- 事件關鍵字：表示欲阻擋含有此事件關鍵字之事件。
- 執行週期：顯示該項目執行週期。
- 門檻值：定義警示的嚴重程度。
- 阻擋來源目的 IP：顯示阻擋「All」、「來源 IP」或「目的 IP」。
- 自動阻擋：顯示當達到所設定的阻擋條件時，系統將「自動阻擋並發送告警」或「僅發送告警」。

按鈕操作

按下按鈕，則跳轉至訂製自動阻擋視窗。

4.7 事件數量統計

此選項的功能主要在於統計過去一季或是一年裡 Syslog 事件的消長變化，藉此協助使用者了解網路維運與資安防護工作的成效。



事件數量統計查詢

提供以下兩種查詢功能，在輸入搜尋條件後，按 啟動查詢 鈕，執行查詢動作。按鈕，可清除所輸入的搜尋條件。

- 查詢時間區段：請選擇欲查詢時間區段及兩種統計方式。

  (1) 季統計：根據輸入時間的當天往前推算一季，每一個時間點代表一週。

  (2) 年統計：根據輸入時間的當天往前推算一年，每一個時間點代表一個月。

- 選擇 Syslog 設備或是群組：下拉選項中會列出系統所有控管的 Syslog 設備，以及存放這些 Syslog 設備的資料夾，方便使用者針對特定的 Syslog 設備或資料夾來查詢事件統計結果。

> 「All Devices」選項包含所有 Syslog 設備，其為系統預設值。

事件數量統計圖操作

- 數量統計圖的左縱軸表示事件總數，系統使用不同顏色的柱狀棒表示不同嚴重等級的 Syslog 事件總數。將滑鼠移到柱狀棒上可顯示確切的 Syslog 事件總數。
- 數量統計圖的右縱軸表示 Hit Count 數，將滑鼠移到藍色曲線圖上可顯示確切的 Hit Count 數。
- 數量統計圖的水平橫軸表示時間。如為查詢「季統計」數量統計圖，則每一個單位時間點代表一週。如為查詢「年統計」數量統計圖，則每一個單位時間點代表一個月。

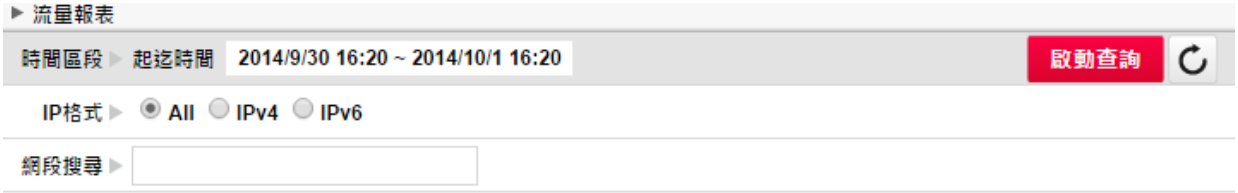
Flow 4.8 Flow 專屬報表

在購買 Flow Module 後，系統會在報表選單項下增加「Flow 專屬報表」選項。

Flow 4.8.1 流量報表

此選項的功能中，N-Reporter 提供 Flow 網段每日固定流量報表。

流量報表查詢



提供以下三種查詢功能，在輸入搜尋條件後，按 啟動查詢 鈕，執行查詢動作。按鈕，可清除所輸入的搜尋條件。

- 時間區段：請選擇欲查詢時間區段。預設為當下時間回推 24 小時內之流量資料。
- IP 格式：選擇「All」、「IPv4」或「IPv6」來列出相關項目。
- 網段搜尋：請輸入網段名稱(全部或是部份)進行過濾。

流量報表列表

	流入量		流出量		
網段名稱	Packets	Bytes	Packets	Bytes	流量圖
第三大樓	156.1M	152.6G	126.7M	43.2G	
財務部	52.7M	65.8G	52.7M	65.8	
主機群組	26.2M	1.2G	41.2M	59.5G	

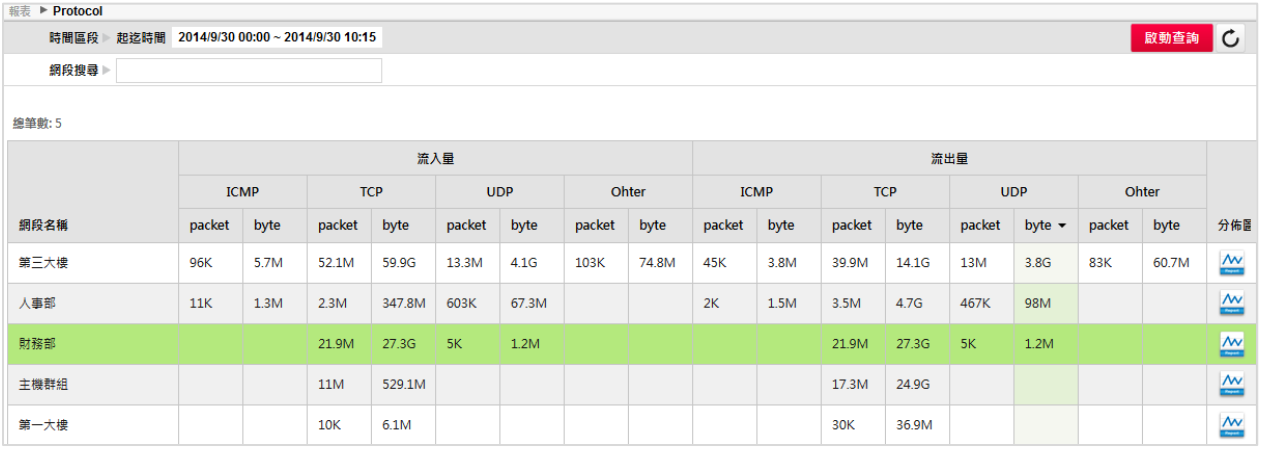
過濾來源名稱解析
過濾目的名稱解析

- 使用者可點選欲查看之網段名稱，系統會將頁面轉至「報表➔Top N➔Top N 報表」，並載入相關條件並顯示該網段在所選時間的事件 Top 100 排行，使用者可再進一步的查詢。
- 使用者可在流量報表列表上點擊右鍵，彈出右鍵功能選單，使用者可以將選定的網段當成「過濾來源名稱解析」或「過濾目的名稱解析」條件，帶到「報表➔Top N➔Top N 報表」並顯示該網段在所選時間的事件 Top 100 排行，使用者可再進一步的查詢。
- 點選鈕，彈出分時報表曲線圖，系統會在頁面下方顯示該報表所選時間的「網段流量圖」，包含流入 bps、流出 bps、流入 pps 及流出 pps 分時圖。將滑鼠移至頁面上其一曲線圖之特定點(如下圖)，會顯示流量值。

Flow

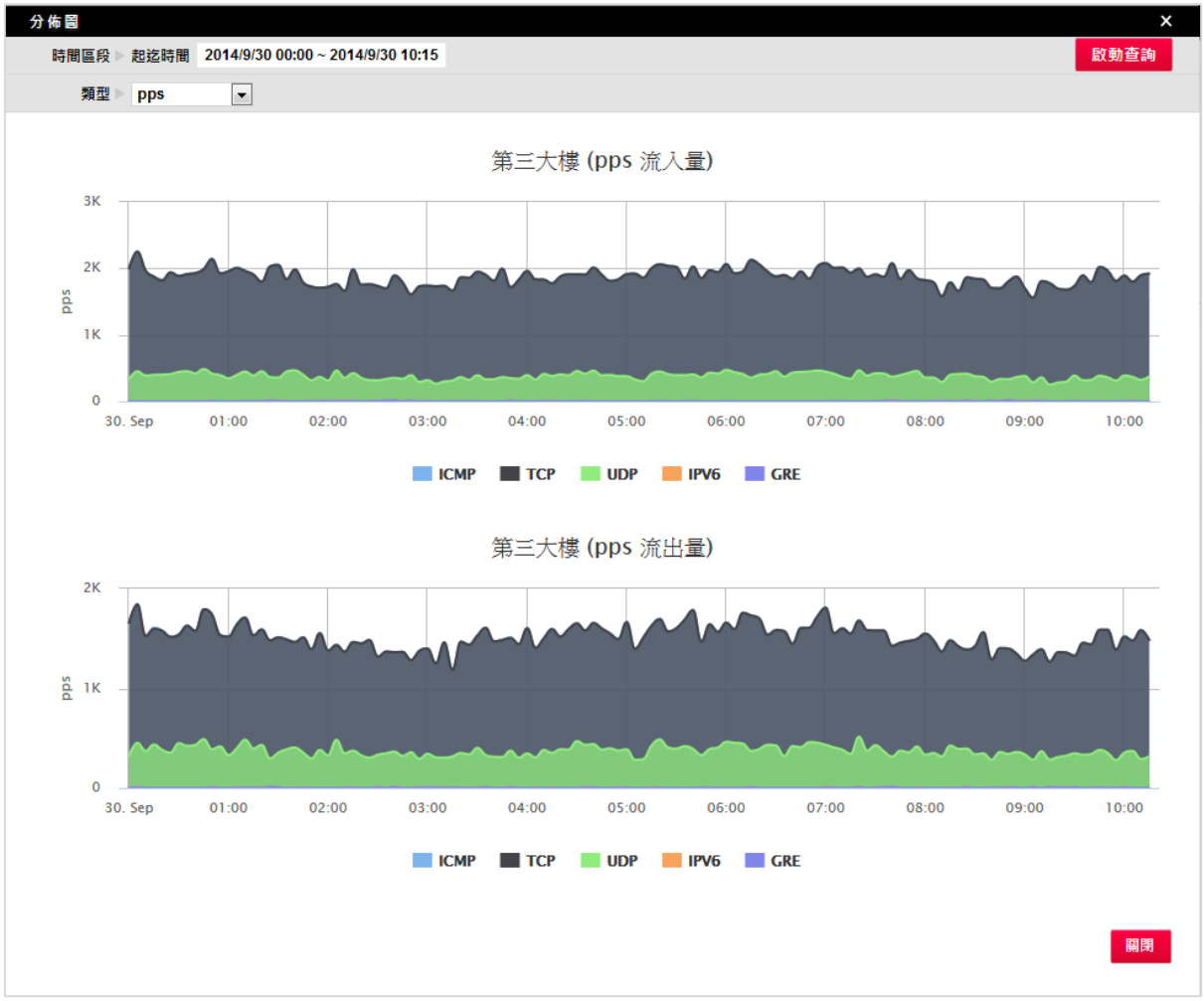
4.8.2 Protocol

Protocol 報表會依據 Flow 或是 Firewall Traffic 等流量資料，提供各網段中的 ICMP、TCP、UDP 等協定所佔用的流量累計，並提供各網段的 Protocol 分佈圖。

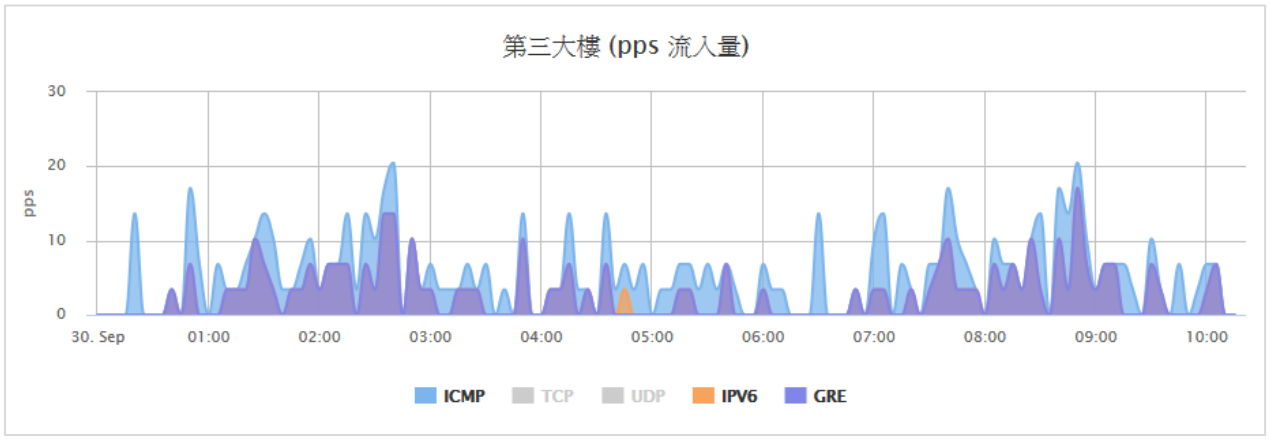


網段名稱	流入量								流出量								分佈圖
	ICMP		TCP		UDP		Ohter		ICMP		TCP		UDP		Ohter		
	packet	byte	packet	byte	packet	byte	packet	byte	packet	byte	packet	byte	packet	byte	packet	byte	
第三大樓	96K	5.7M	52.1M	59.9G	13.3M	4.1G	103K	74.8M	45K	3.8M	39.9M	14.1G	13M	3.8G	83K	60.7M	
人事部	11K	1.3M	2.3M	347.8M	603K	67.3M			2K	1.5M	3.5M	4.7G	467K	98M			
財務部			21.9M	27.3G	5K	1.2M					21.9M	27.3G	5K	1.2M			
主機群組			11M	529.1M							17.3M	24.9G					
第一大樓			10K	6.1M							30K	36.9M					

- 時間區段可以指定起迄時間，預設為當下時間回推 24 小時內之流量資料。
- 網段搜尋可以指定網段名稱(全部或部份)進行網段過濾。條件設定完成後，點選 啟動查詢 可以進行查詢，點選右方 鈕 可以清除所有已輸入的查詢條件。點選 可以查看網段的 Protocol 流量分佈圖。

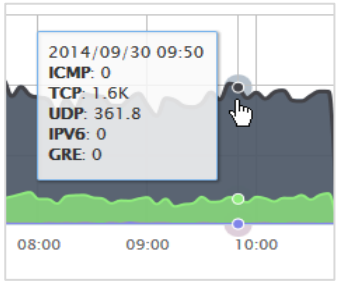


在視窗中的時間區段可以調整起迄時間，類型則可以指定繪製的資料是 bps(bits per second)或 pps(packets per second)。點選下方圖例可以暫時隱藏某些協定，例如上例中想到看出 TCP/UDP 以外的比例分佈，點選下方 TCP 與 UDP 圖示後即可得到下圖。



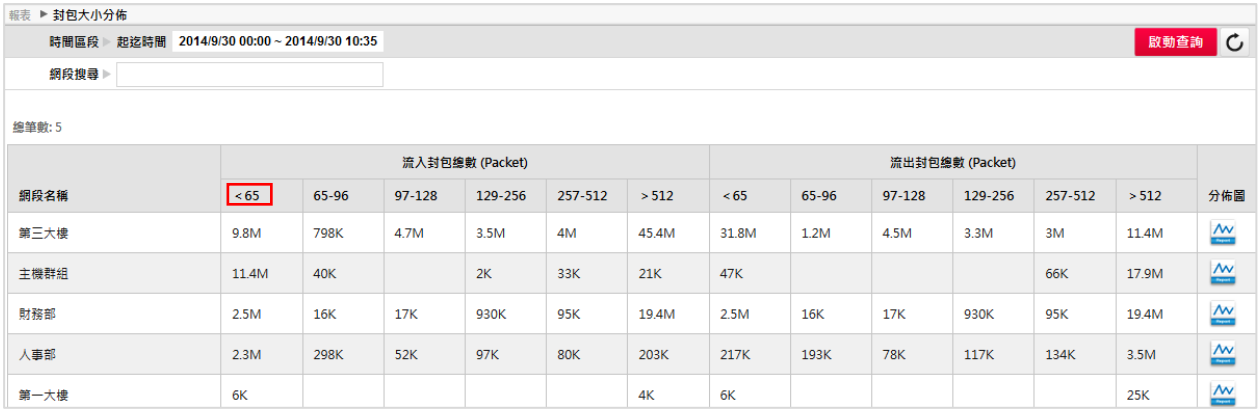
針對流量圖上有異常發生的時間點，點選後可以跳到 Top N 追查異常 IP 列表，進行進一步的鎖定及排除。

滑鼠移到流量圖上會列出該時間的流量數值。



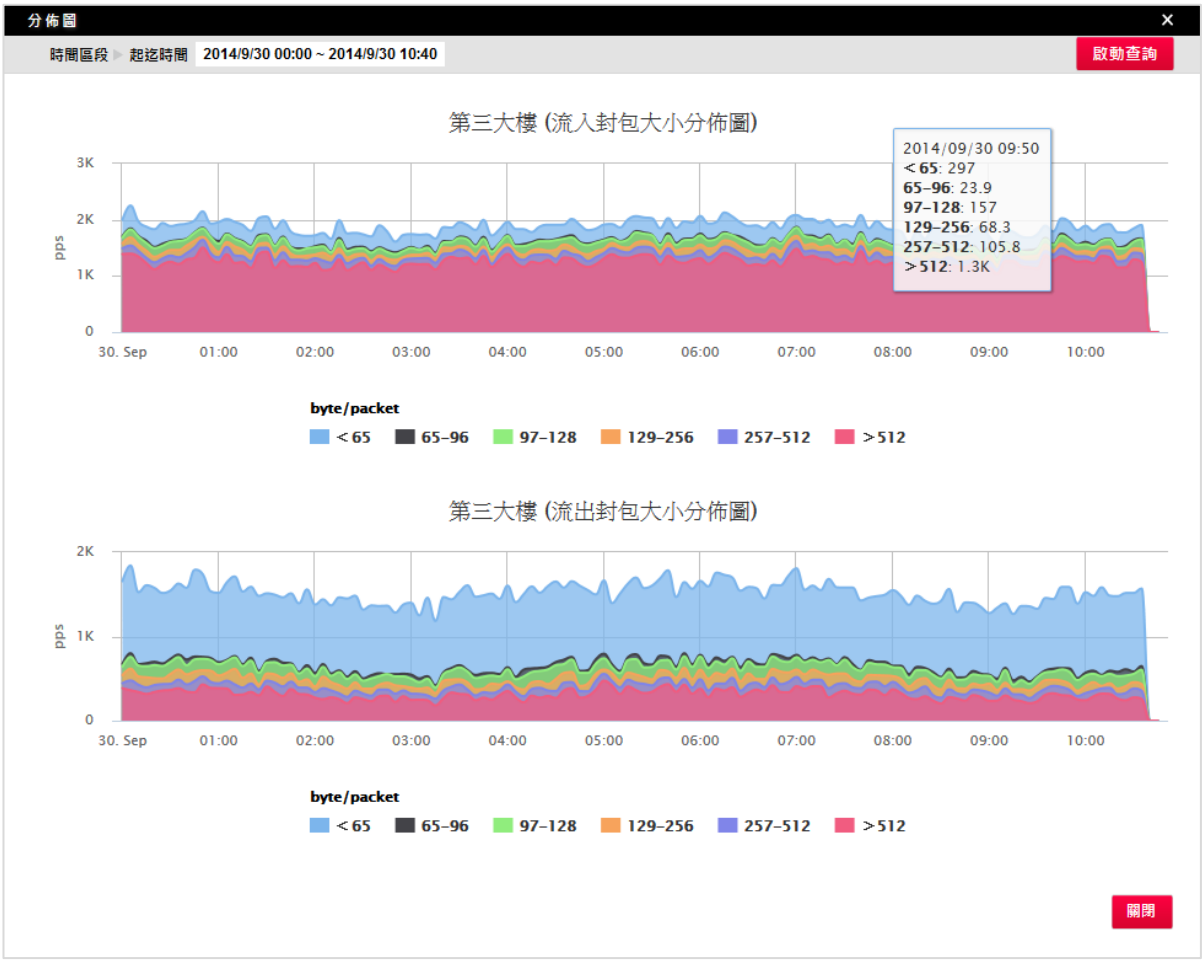
Flow

4.8.3 封包大小分佈

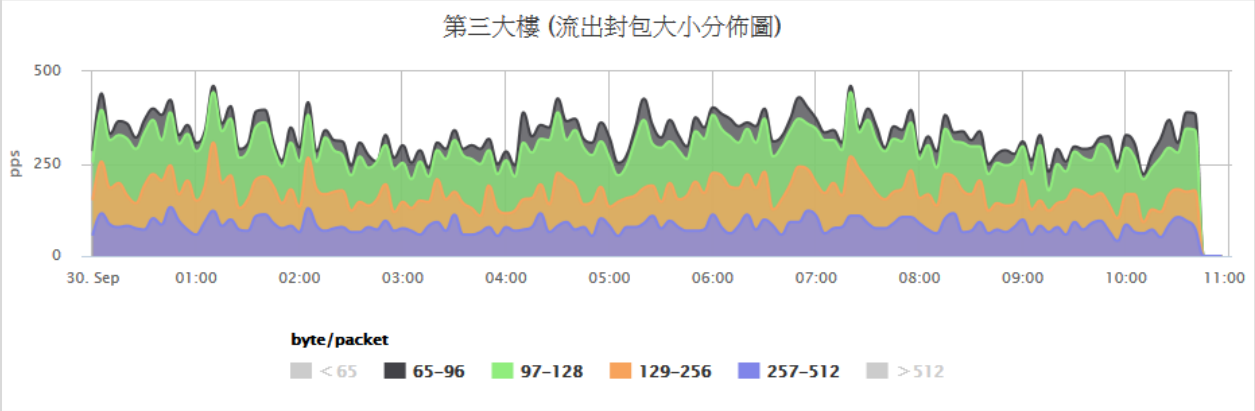


網段名稱	流入封包總數 (Packet)						流出封包總數 (Packet)						分佈圖
	< 65	65-96	97-128	129-256	257-512	> 512	< 65	65-96	97-128	129-256	257-512	> 512	
第三大樓	9.8M	798K	4.7M	3.5M	4M	45.4M	31.8M	1.2M	4.5M	3.3M	3M	11.4M	
主機群組	11.4M	40K		2K	33K	21K	47K				66K	17.9M	
財務部	2.5M	16K	17K	930K	95K	19.4M	2.5M	16K	17K	930K	95K	19.4M	
人事部	2.3M	298K	52K	97K	80K	203K	217K	193K	78K	117K	134K	3.5M	
第一大樓	6K					4K	6K					25K	

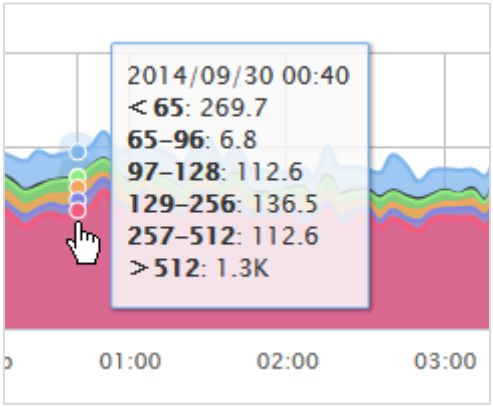
- 封包大小分佈報表會依據 Flow 或是 Firewall Traffic 等流量資料，提供各網段中的各種封包大小所佔用的流量累計，並提供各網段的封包大小分佈圖。
- 時間區段可以指定起迄時間，預設為當下時間回推 24 小時內之流量資料。網段搜尋可以指定網段名稱(全部或部份)進行網段過濾。條件設定完成後，點選 啟動查詢 可以進行查詢，點選右方 鈕 可以清除所有已輸入的查詢條件。
- 查出的結果可以點選表格標題進行排序，如上例中點選「流出封包總數 <65」(紅框部份),可依此數值由小至大進行排序，再點選一次可改為由大至小進行排序。點選各網段右方分佈圖 可以查看網段的封包大小流量分佈圖。



在視窗中的時間區段可以再調整起迄時間。點選下方圖例可以暫時隱藏某些封包大小，例如上例中想到看出<65 及>512 以外的比例分佈，點選下方<65 及>512 圖示後即可得到下圖。



針對流量圖上有異常發生的時間點，點選後可以跳到 Top N 追查異常 IP 列表，進行進一步的鎖定及排除。滑鼠移到流量圖上會列出該時間的流量數值。



Flow 4.8.4 交叉分析

此選項的功能中，N-Reporter 提供 Flow 網段交互間流量分析。

網段名稱	流入總量(Bytes)	流入總封包數	流出總量(Bytes)	流出總封包數
第三大樓	25.06G	43.97M	25.06G	43.97M
主機群組	37.41G	25.26M	781.14M	16.05M
人事部	11.00G	8.33M	427.28M	5.84M
Home	0	0	30.43M	172.03K
第一大樓	12.61M	16.38K	6.14M	4.09K

交叉分析查詢

提供以下三種查詢功能，在輸入搜尋條件後，按 啟動查詢 鈕，執行查詢動作。按 鈕，可清除所輸入的搜尋條件。

- 查詢時間區段：請選擇欲查詢時間區段。預設為當下時間回推 24 小時內之流量資料。
- IP 格式：選擇「All」、「IPv4」或「IPv6」來列出相關項目。
- 請選擇網段：請選擇欲查詢的網段。

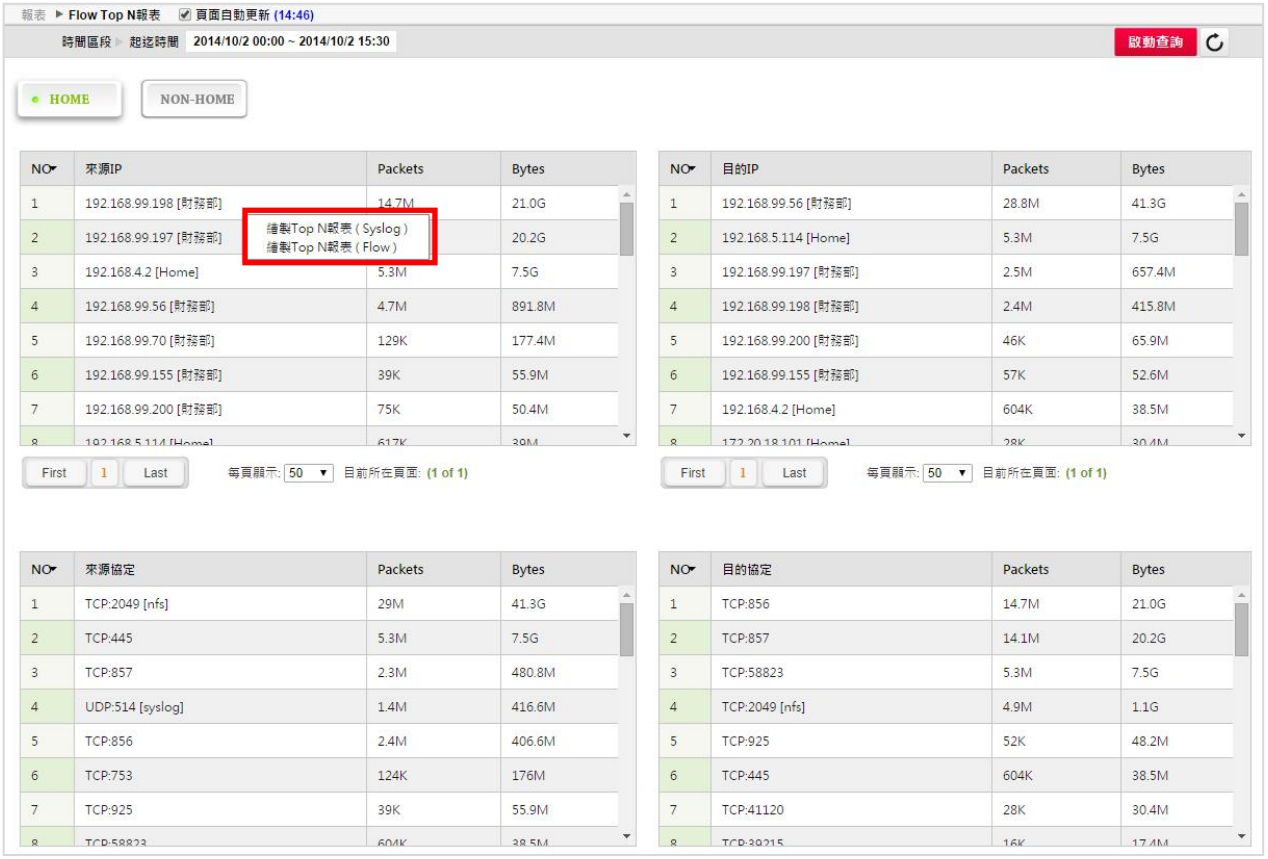
交叉分析列表

預設排序為「流入總量 + 流出總量」的總和。

Flow

4.8.5 Flow Top N 報表

此選項的功能中，N-Reporter 提供 Flow 網段的流量排行。



頁面自動更新

當勾選「頁面自動更新」則會以每 15 分鐘刷新此頁面。

查詢時間區段

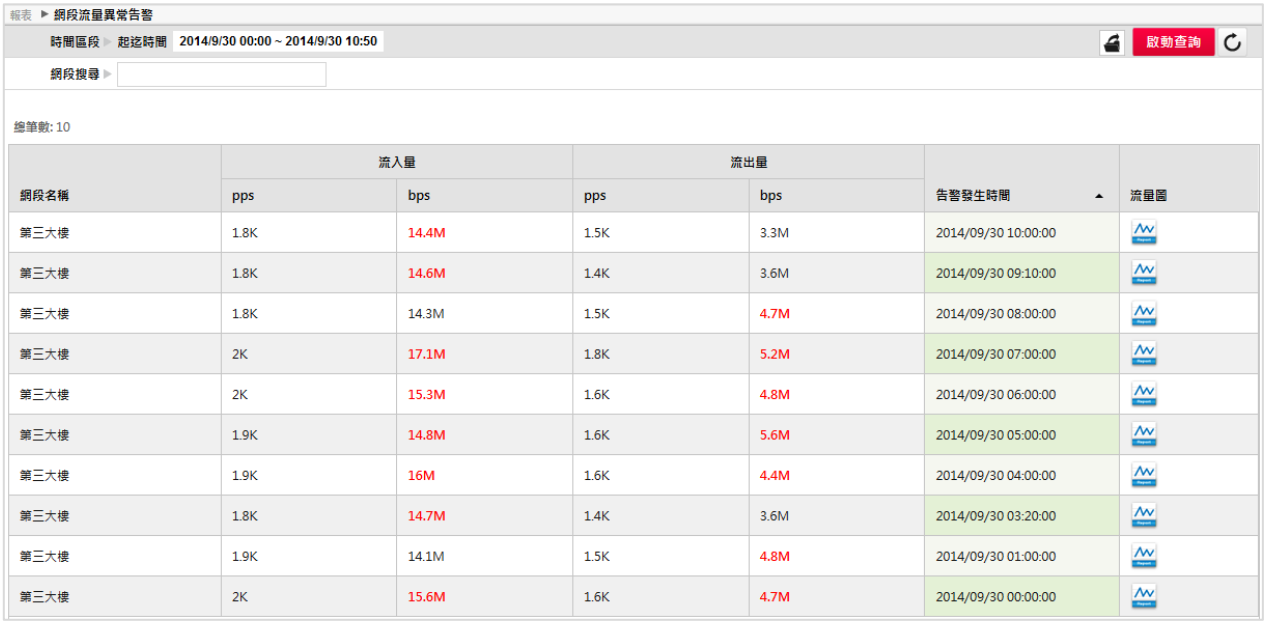
輸入起始時間與結束時間後，按 啟動查詢 鈕，執行查詢動作，其分別依據「內部網段(Home)」與「非內部網段(Non-Home)」的「來源 IP」 / 「目的 IP」 / 「來源協定」 / 「目的協定」進行排序。按鈕，可清除所輸入的搜尋條件。

來源 IP / 目的 IP / 來源協定 / 目的協定列表

使用者可在列表上點擊右鍵，彈出右鍵功能選單(如上圖所示)，使用者可以將選定的項目來「繪製 Top N 報表(Syslog)」或「繪製 Top N 報表(Flow)」，點選欲查看之項目，系統會將頁面轉至「報表➔Top N➔Top N 報表」，並載入相關條件並顯示該項目在所選時間的事件 Top 100 排行，使用者可再進一步的查詢。

Flow 4.8.6 網段流量異常告警

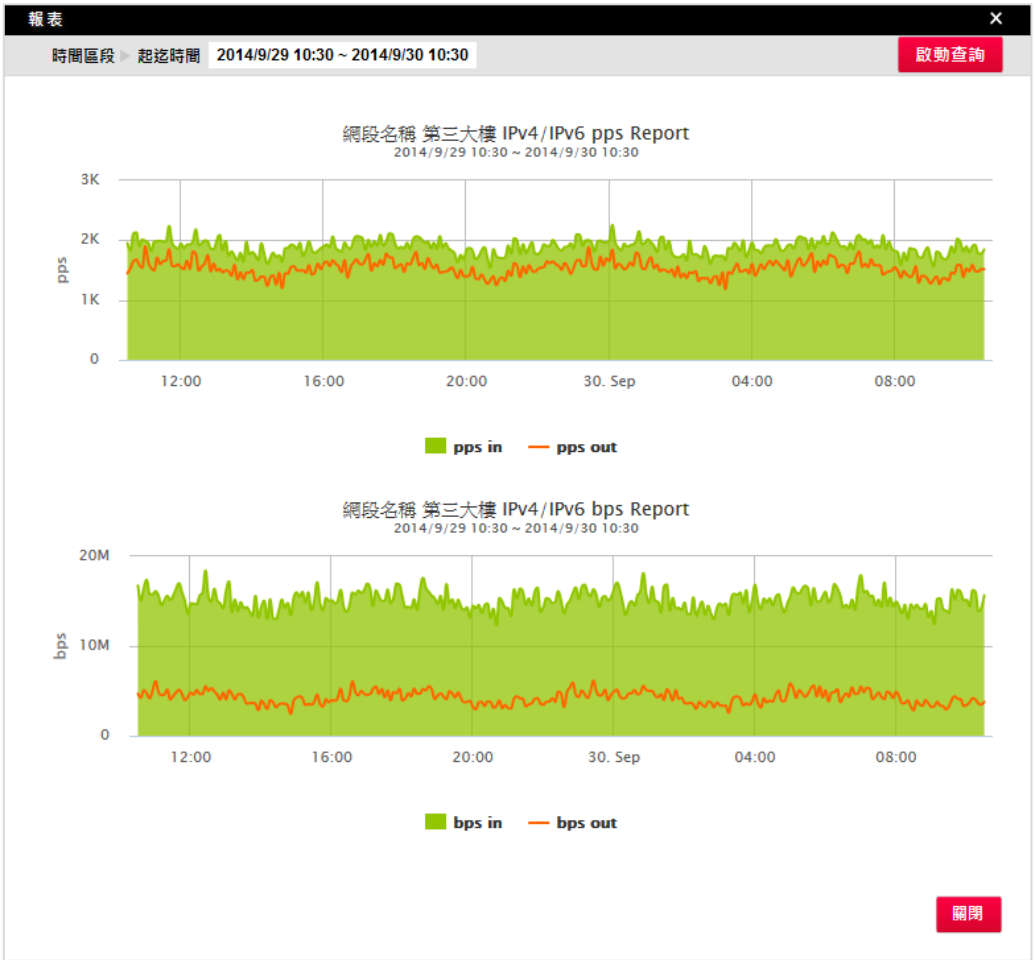
網段流量異常告警的啟動及設定，請參考「系統管理」➔「名稱解析」章節，系統提供動態門檻值的概念，自動依據各網段過去的流量，推估出適當的門檻值，在網段的流量(bps/pps)有突增時發出警示。



網段名稱	流入量 pps	流入量 bps	流出量 pps	流出量 bps	告警發生時間	流量圖
第三大樓	1.8K	14.4M	1.5K	3.3M	2014/09/30 10:00:00	
第三大樓	1.8K	14.6M	1.4K	3.6M	2014/09/30 09:10:00	
第三大樓	1.8K	14.3M	1.5K	4.7M	2014/09/30 08:00:00	
第三大樓	2K	17.1M	1.8K	5.2M	2014/09/30 07:00:00	
第三大樓	2K	15.3M	1.6K	4.8M	2014/09/30 06:00:00	
第三大樓	1.9K	14.8M	1.6K	5.6M	2014/09/30 05:00:00	
第三大樓	1.9K	16M	1.6K	4.4M	2014/09/30 04:00:00	
第三大樓	1.8K	14.7M	1.4K	3.6M	2014/09/30 03:20:00	
第三大樓	1.9K	14.1M	1.5K	4.8M	2014/09/30 01:00:00	
第三大樓	2K	15.6M	1.6K	4.7M	2014/09/30 00:00:00	

點選右側流量圖 可以查看近 24 小時的流量狀況

在視窗中的時間區段可以再調整起迄時間。例如本例中將時間拉長為一週時就可看出流量突增狀況，可以明顯看出是在哪天發生，直接點選流量圖上異常的時間點，可以跳至 Top N 報表進一步追查異常 IP。



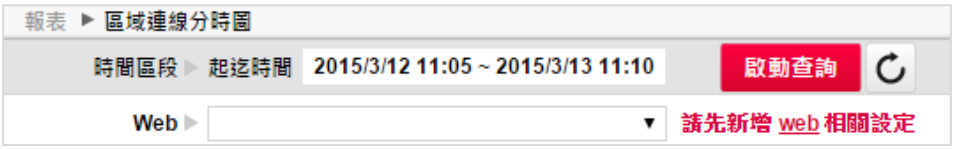
Flow

4.9 Web 專屬報表

利用收集到的 NetFlow/sFlow 資料，N-Reporter 會進行針對 Web 主機的行為分析及異常的偵測，包含針對國家或區域的流量分析，以及該 Web 主機非 HTTP/HTTPS(80/443) 的流量分析。

4.9.1 區域連線分時圖

根據使用者所訂定的時間區段來提供各區域的連線分時資訊。



時間區段

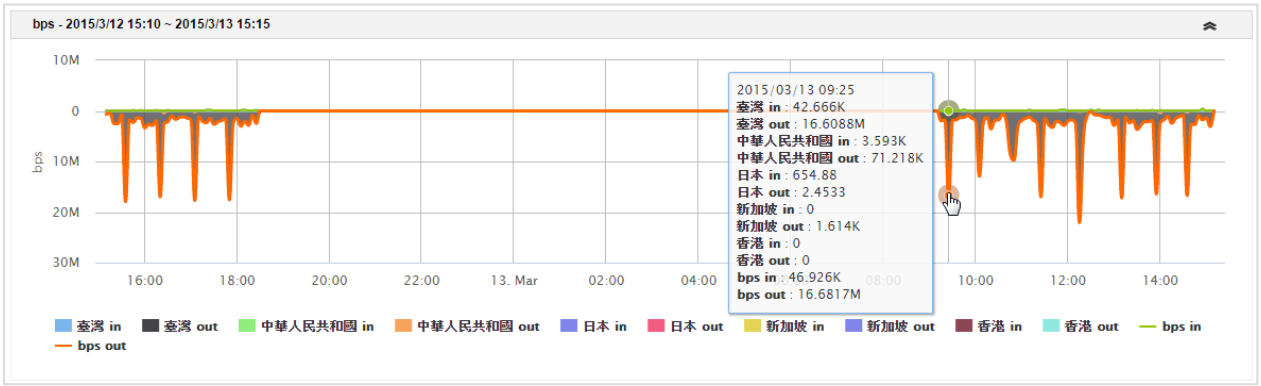
時間區段可以指定起迄時間，預設查詢 24 小時內的統計資料。

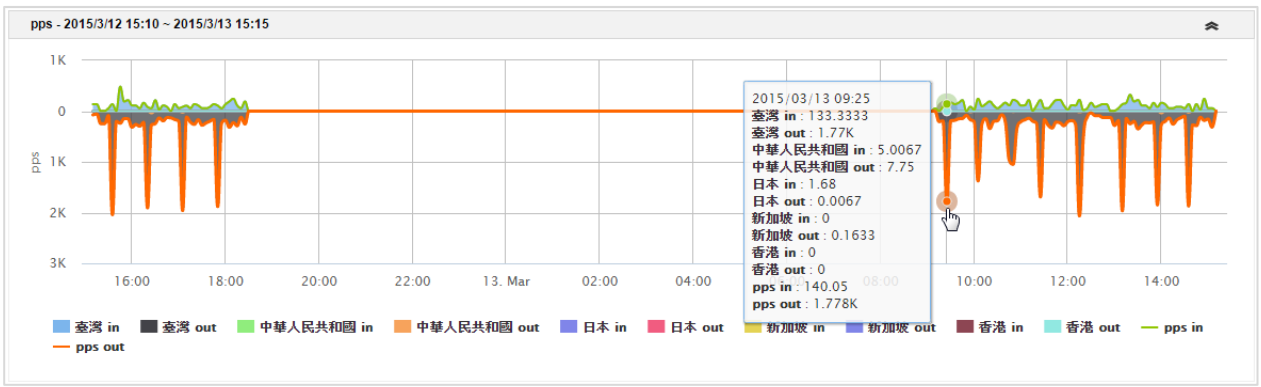
Web

可以指定任一 Web 主機進行資料查詢，若未新增任一 Web 主機，系統將導引使用者在「設備管理➔主機」中進行 Web 主機相關設定，請參考 2.5 章節。

bps/pps 分時圖

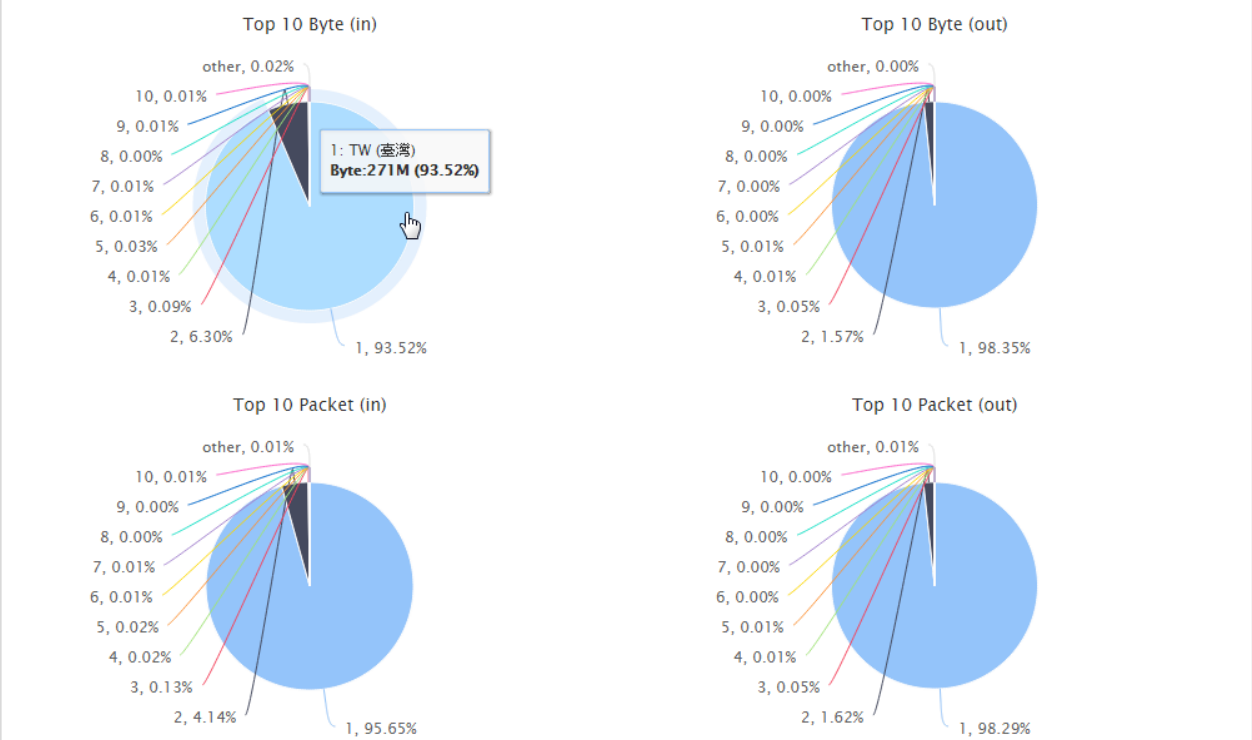
顯示此 Web 主機各區域之 bps in/out 或 pps in/out 分時曲線圖。使用者可任意選擇所需的起迄時間來進行查詢。滑鼠移至曲線圖任一特定點(如上圖)，系統會顯示該點各區域之 bps in/out 或 pps in/out 流量及時間，若點擊該特定點，則會把該特定點資訊帶入 Top N 報表進行更詳細的追查，其 Drill-Down 查詢功能，可參閱 4.1 Top N 報表章節。





Top N

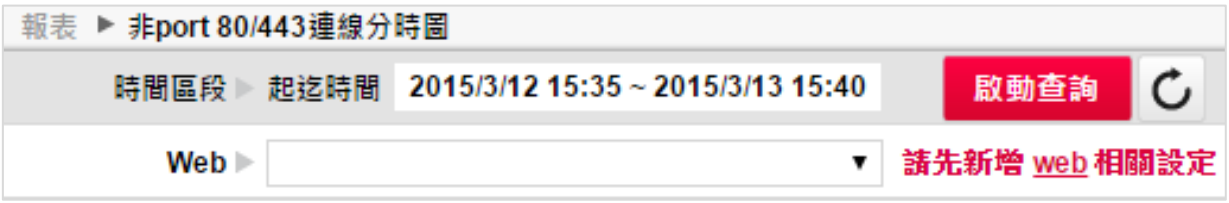
顯示此 Web 主機下，其區域之 Top 10 Byte in/out 及 Top 10 Packet in/out 圖餅圖和各區域排行表。滑鼠移至圖餅圖任一區塊(如上圖)，系統會顯示該點區域之 Byte 或 Packet 流量，若點擊特定區域，則會把其資訊帶入 Top N 報表進行更詳細的追查，其 Drill-Down 查詢功能，可參閱 4.1 Top N 報表章節。



NO	區域	流入量		流出量	
		Packets	Bytes	Packets	Bytes
1	TW (臺灣)	3.5M	271M	11.9M	13.5G
2	CN (中華人民共和國)	156.8K	18.2M	200.5K	220.5M
3	JP (日本)	4.9K	259.5K	5.9K	7.7M
4	SG (新加坡)	724	36.7K	1.1K	1.6M
5	HK (香港)	897	85.5K	1.2K	1.1M

4.9.2 非 port 80/443 連線分時圖

根據使用者所訂定的時間區段來提供非 port 80/443 的連線分時資訊。



時間區段

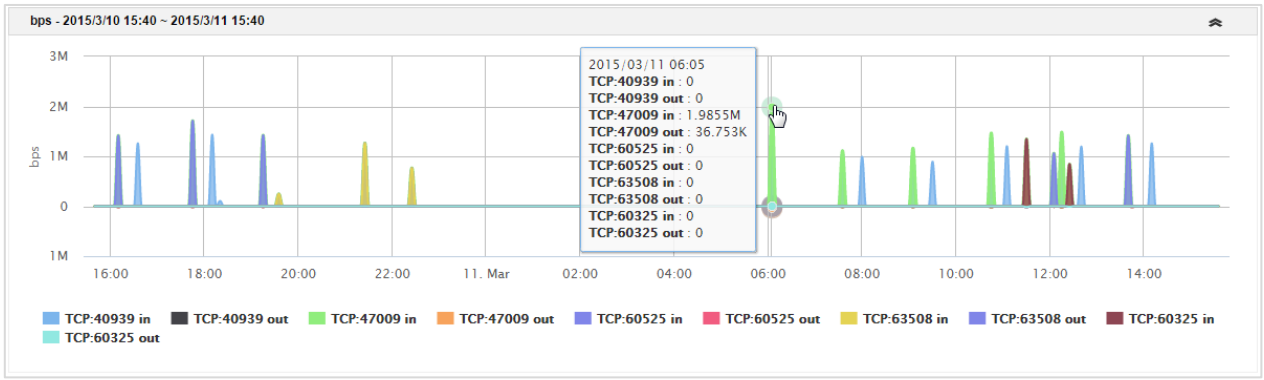
時間區段可以指定起迄時間，預設查詢 24 小時內的統計資料。

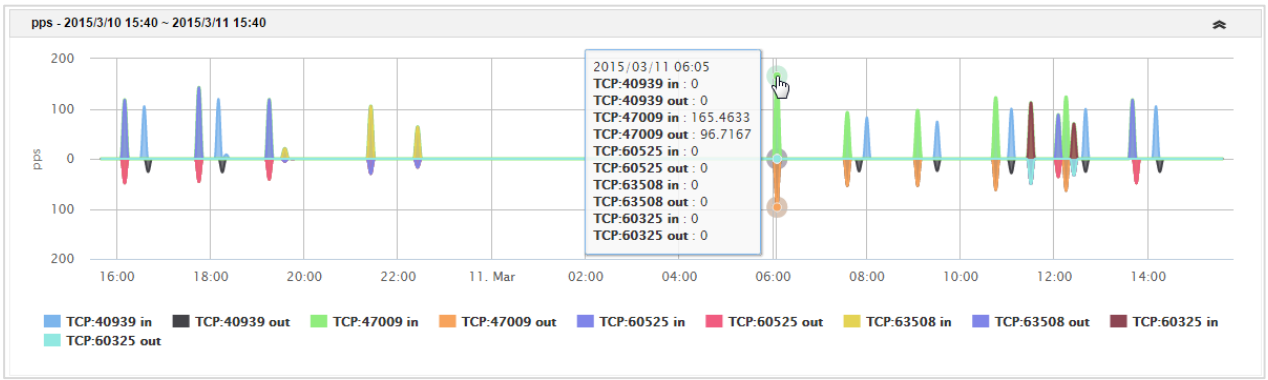
Web

可以指定任一 Web 主機進行資料查詢，若未新增任一 Web 主機，系統將導引使用者在「設備管理➔主機」中進行 Web 主機相關設定，請參考 2.5 章節。

bps/pps 分時圖

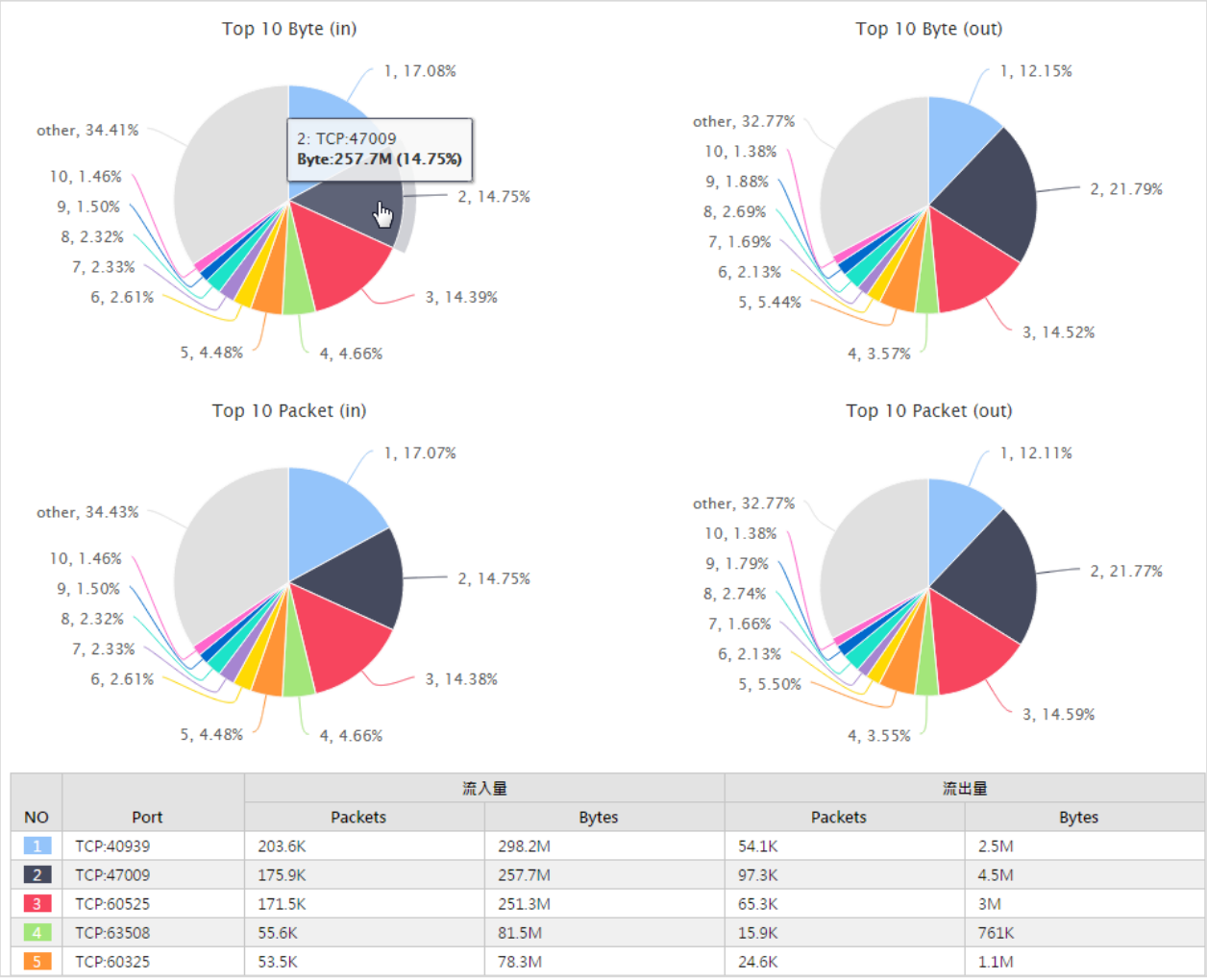
顯示此 Web 主機各非 80/443 port 之 bps in/out 或 pps in/out 分時曲線圖。使用者可任意選擇所需的起迄時間來進行查詢。滑鼠移至曲線圖任一特定點(如上圖)，系統會顯示該點之 bps in/out 或 pps in/out 流量及時間，若點擊該特定點，則會把該特定點資訊帶入 Top N 報表進行更詳細的追查，其 Drill-Down 查詢功能，可參閱 4.1 Top N 報表章節。





Top N

顯示此Web主機下，其非80/443 port 之Top 10 Byte in/out及Top 10 Packet in/out圖餅圖和各非80/443 port排行表。滑鼠移至圖餅圖任一區塊(如上圖)，系統會顯示該點 port 之 Byte 或 Packet 流量，若點擊特定區塊，則會把其資訊帶入 Top N 報表進行更詳細的追查，其 Drill-Down 查詢功能，可參閱 4.1 Top N 報表章節。



NO	Port	流入量		流出量	
		Packets	Bytes	Packets	Bytes
1	TCP:40939	203.6K	298.2M	54.1K	2.5M
2	TCP:47009	175.9K	257.7M	97.3K	4.5M
3	TCP:60525	171.5K	251.3M	65.3K	3M
4	TCP:63508	55.6K	81.5M	15.9K	761K
5	TCP:60325	53.5K	78.3M	24.6K	1.1M

採購與銷售合作：sales@npartnertech.com

技術諮詢：support@npartnertech.com