N-Partner

建構新一代的智慧 IT 維運方式

整合網管、流量分析與資安技術

(SNMP、Flow、Syslog)

(06-01-01-005) 2015/08/17

目錄

連絡資訊

N-Partner 公司連絡方式：

TEL: +886-4-23752865

FAX: +886-4-23757458

有關技術問題請洽：

Email: support@npartnertech.com

Skype：support@npartnertech.com

有關業務相關問題請洽：

Email: sales@npartnertech.com

一、三大網管技術- SNMP Monitoring, Flow Analysis and Syslog Correlation

1-1 三大技術用途

✧ **SNMP (Simple Network management Protocol)**

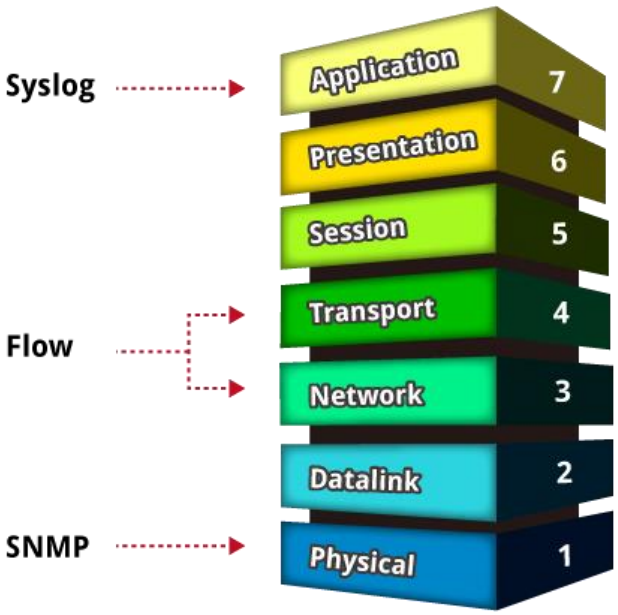
主要用途是對於設備的健康狀態(CPU/Memory/溫度/風扇/Interface UP and Down 等)進行監測。網路服務能正常運作，第一個關鍵就是所有佈署於網路的設備要能保持健康。透過 SNMP 協定採集設備端的硬體參數用以得知設備的健康狀態。

✧ **Flow (NetFlow, sFlow)**

Flow 的用途則是了解關於網路用量的訊息，諸如某個用戶端 IP 發送了多少封包(Packet)、總共傳送了的少 Bytes？某個伺服器接收了多少連線(Session)請求、回應了多少封包與多少 Bytes？某個應用(ex: TCP 80)佔據多少頻寬等。藉由 Flow 訊息的分析能夠了解人們使用網路關於量大量小的問題。Flow 訊息涵蓋 OSI 定義中的 Layer 3 與 Layer 4。

✧ **Syslog**

隨著資安意識的逐漸普及與提升，有越來越多的組織佈署了安全防禦設備或是上網行為管控機制，針對封包裡第七層(Application)的內容進行檢查與分析。這些七層的訊息除了能幫助 IT 人員得知組織中所發生的資安威脅事件之外，對於人員的網路使用行為(ex: P2P 下載、使用通訊軟體、瀏覽哪些網站等)也可以有更完整的了解。現今大多數的網路與資安設備、電腦作業系統都已支援透過 syslog 協議的方式將日誌輸出，IT 管理人員則透過日誌收集與分析的方式掌握網路使用行為以及跟資安相關的事件。Syslog 訊息涵蓋 OSI 定義中的 Layer 7。



圖一、三大技術的 OSI 涵蓋領域

1-2 為什麼需要整合分析？

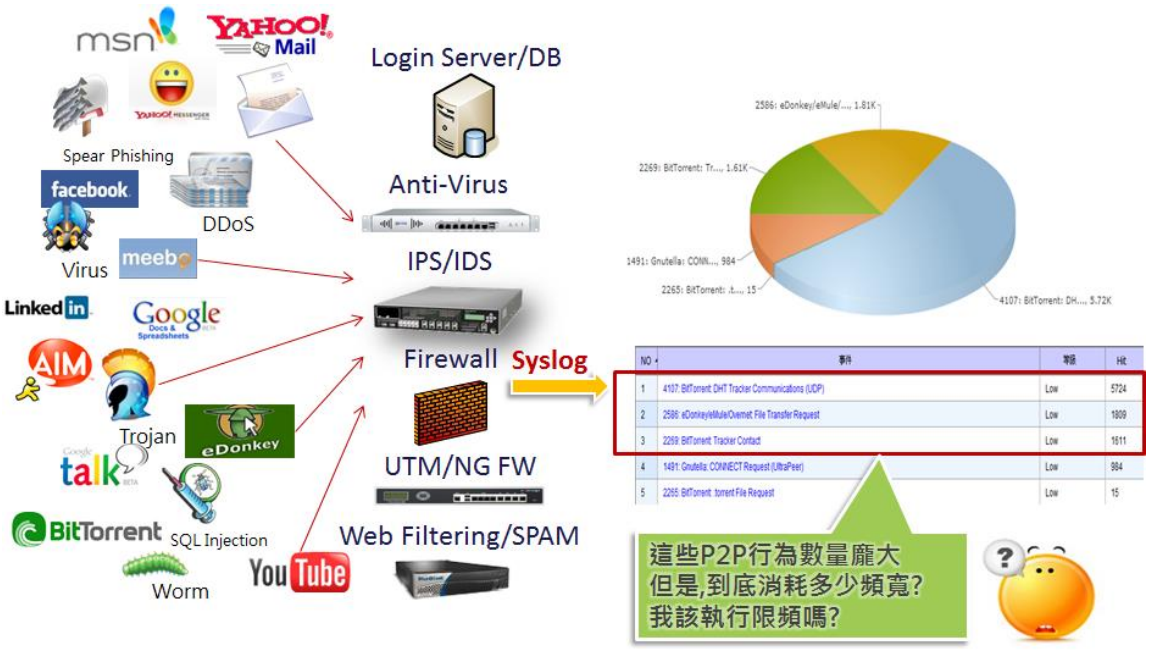
當網路發生傳輸問題或是伺服器的服務出現異常狀況時，技術人員執行除錯，通常第一步驟是去了解網路設備或是伺服器的健康狀態，接著從網路層面查找可疑的 IP，再去比對資安設備與伺服器的日誌，費時費力卻不一定能找到肇致障礙的根源。此外，隨著組織內網路架構逐漸龐大，採購設備的品牌也越來越多樣，無形間也就提升了維運與除錯的難度。

為什麼組織裡的防火牆與路由器 CPU 會突然升高導致網路緩慢?為什麼頻寬需求不斷飆升？到底是什麼樣的應用、哪些使用者以及哪些電腦佔據了網路資源？人員無法上網到底是網路問題還是資安事件造成的？

許多技術人員為了確保 IT 系統運作無虞，採購各種網管與分析工具卻達不到預期的成效。主要的原因就是三大網管技術間沒有加以有效的整合。

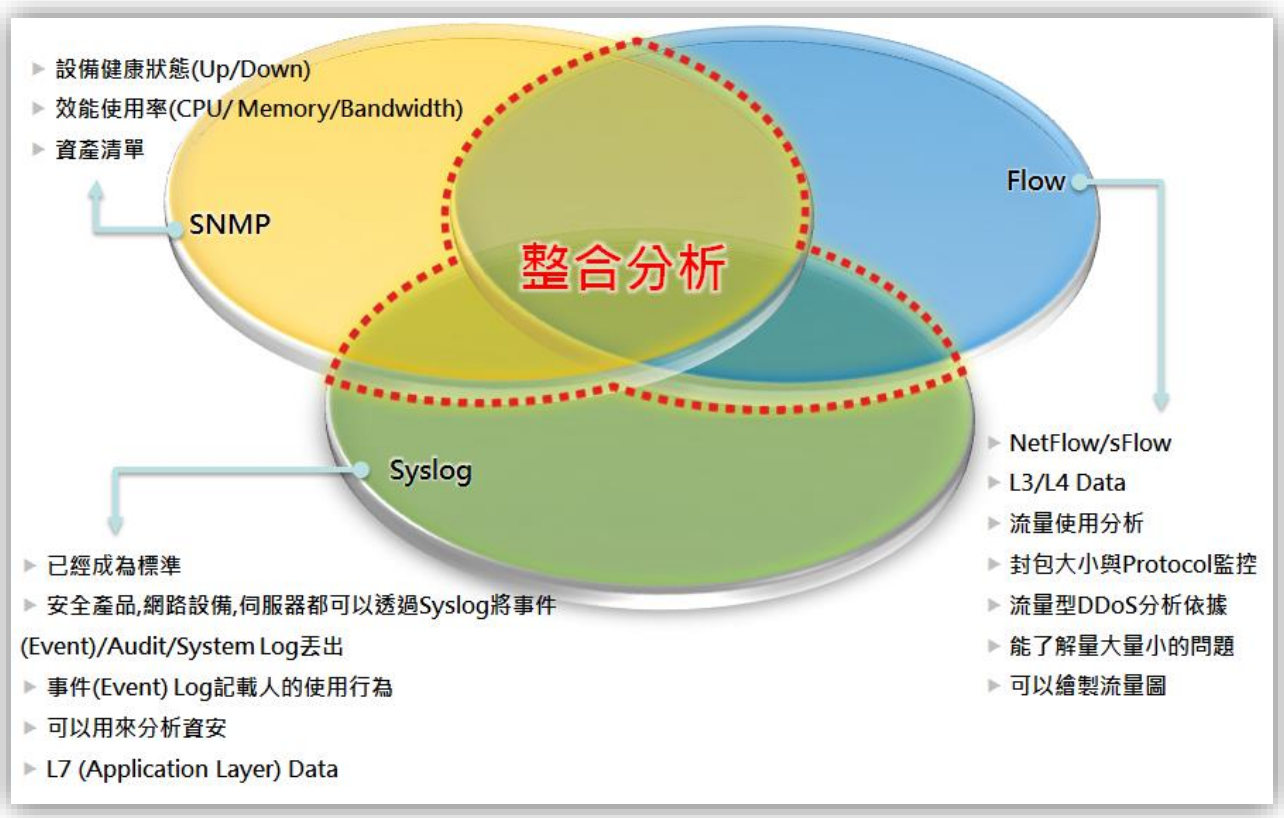
在大多數的情況下，網路設備 CPU 之所以衝高通常是因為必須處理瞬間流經的巨量封包。使用 SNMP 監控技術的網管工具只能偵測到 CPU 升高的狀況，卻無法告知是哪些 IP 發出巨量封包才造成設備的效能負擔。IT 管理者必須使用另一套管理工具-Flow 分析軟體自行找出可疑的 IP 地址。然而，就算知道了 IP 地址，如果組織龐大，想要進一步了解這些 IP 在哪個實體位置(ex: 哪個 Switch 的哪個 Port)？是哪個使用者正在操作這部電腦？而又是甚麼樣的 Application 讓這些 IP 發送出這麼大量的封包？是電腦被植入了 Malware 嗎？這些問題的答案還是只能再從 SNMP 或是 Syslog 日誌去慢慢拼湊蛛絲馬跡。

圖二、Flow 統計無法告知真正的網路使用行為



圖三、透過 Syslog 得知的事件無法告知該種應用對網路資源消耗的輕重

將三大網管技術加以整合是建構新一代 IT 維運方式必要的做法。因為每種技術各有專長也都有不足之處。整合得當將有助於 IT 人員窺知網路活動的全貌。



圖四、三大網管技術的涵蓋工作與整合

1-3 Flow 與 Syslog 的關聯

Flow 記錄兩個 IP 之間的傳輸用量統計，資料內容帶有 Source IP、Source Port、Destination IP、Destination Port、Protocol、Packet、Byte 等。而 Syslog 日誌主要是說明發生了甚麼事件，資料內容包括事件名稱與說明、Source IP、Source Port、Destination IP、Destination Port、Protocol、事件發生次數(Hit Count)等。要將 Flow 與 Syslog 關聯在一起可以使用 5 Tuples 比對方式執行 : 單位時間裡(通常是 1 分鐘內) Source IP、Source Port、Destination IP、Destination Port、Protocol 這 5 個參數相同者可以視為同一連線行為。下圖為說明案例：

圖五、Flow 與 Syslog 關聯整合

從資安設備的 Syslog 日誌得知某 IP 正在發起巨量的 DNS 查詢，透過 5 Tuples 方式比對同時間的 Flow 資料可以知道這樣的 DNS 查詢行為共傳送了多少封包，佔去多少頻寬資源。此外，整合登入機制的日誌(ex: AD)則能夠將該 IP 的使用者名字比對出來。最後如果還能夠整合 SNMP，就會知道這個 IP 連接在組織裡哪個 Switch 的哪個 Port 底下。一張整合三種技術的關聯表格可以清楚呈現所有網路使用訊息給 IT 管理人員，省去人工比對查找所耗費的時間。

1-4 三大技術整合分析案例

✧ 案例一：從 Flow 分析發現異常，Syslog 訊息告知攻擊的手法

這是針對一個電子商務網站所進行的監控。從流量分析(Flow Analysis)中發現有一種特定大小的封包(Packet Size=129-256 Bytes)是異於多數人訪問網站時所傳送的封包大小，正在某個時刻突然開始活動。

從 Flow 資料能夠得知發送這種封包的來源 IP，根據前節(1-3)所述，使用 5 Tuples 比對方式後就能夠比對出這種異於其他瀏覽行為的封包其實是在進行針對 OpenSSL 漏洞的入侵行為。接下來的動作將是把這個不友善的來源 IP 阻擋下來。

事件	來源IP	來源Port	來源區域	目的IP	目的Port	目的IP名稱解析	次數
16538: TCP: OpenSSL ClientHello Message	121.15.2.177	4885	CN	[redacted]	443	[redacted]	85
16270: TLS: OpenSSL ChangeCipherSpec Request	121.15.2.177	4885	CN	[redacted]	443	[redacted]	79
16270: TLS: OpenSSL ChangeCipherSpec Request	121.15.2.177	4706	CN	[redacted]	443	[redacted]	36
16538: TCP: OpenSSL ClientHello Message	121.15.2.177	4706	CN	[redacted]	443	[redacted]	36
16270: TLS: OpenSSL ChangeCipherSpec Request	121.15.2.177	5003	CN	[redacted]	443	[redacted]	11
16538: TCP: OpenSSL ClientHello Message	121.15.2.177	5003	CN	[redacted]	443	[redacted]	11
16270: TLS: OpenSSL ChangeCipherSpec Request	121.15.2.177	5221	CN	[redacted]	443	[redacted]	3
16538: TCP: OpenSSL ClientHello Message	121.15.2.177	5221	CN	[redacted]	443	[redacted]	3
16270: TLS: OpenSSL ChangeCipherSpec Request	121.15.2.177	5112	CN	[redacted]	443	[redacted]	2
16538: TCP: OpenSSL ClientHello Message	121.15.2.177	5112	CN	[redacted]	443	[redacted]	2

圖六、Flow 分析發覺異常來源 IP，Syslog 日誌提供更清楚的入侵行為說明

✧ 案例二：DNS 放大攻擊耗損頻寬資源- 從 Syslog 事件比對 Flow 後計算出頻寬的損耗量

DNS 攻擊有越來越普及的趨勢，主要原因是方法簡單、有效而且難以防禦。DNS 攻擊的種類繁多，其中一種稱為 DNS Amplification 的 DNS 放大攻擊，發動後可以產生巨量 DNS 回應流(DNS Response)，導致頻寬資源的無謂耗損。此外，DNS 放大攻擊往往搭配 IP Spoofing 手法，藉由將發送來源 IP 竄改成欲攻擊端 IP 的方式，引導巨量 DNS 回應流癱瘓欲攻擊端。

然而，DNS 放大攻擊如此頻繁，到底甚麼時候；或是要多大的攻擊量才值得 IT 管理人員必須要關注並且立即採取防禦作為？再者，DNS 放大攻擊目標是造成頻寬資源的損耗，那麼要如何知道 DNS 放大攻擊(Syslog，事件)出現後到底吃掉多少頻寬(Flow，流

量)？圖五中的案例給了我們答案：

左上圖告警了當 DNS 放大攻擊事件出現值得注意的異常突增(3/9 11:03，蒐集來自 IPS 防禦系統的日誌)，對比左下方的流量圖(蒐集 Flow 資料後繪製 DNS 對外送出的流量圖)，得知同一時間 DNS 對外發出的流量隨即跟著爆增。關聯 Syslog 日誌與 Flow 資料更能幫助 IT 管理人員了解各種事件對於頻寬資源的影響。

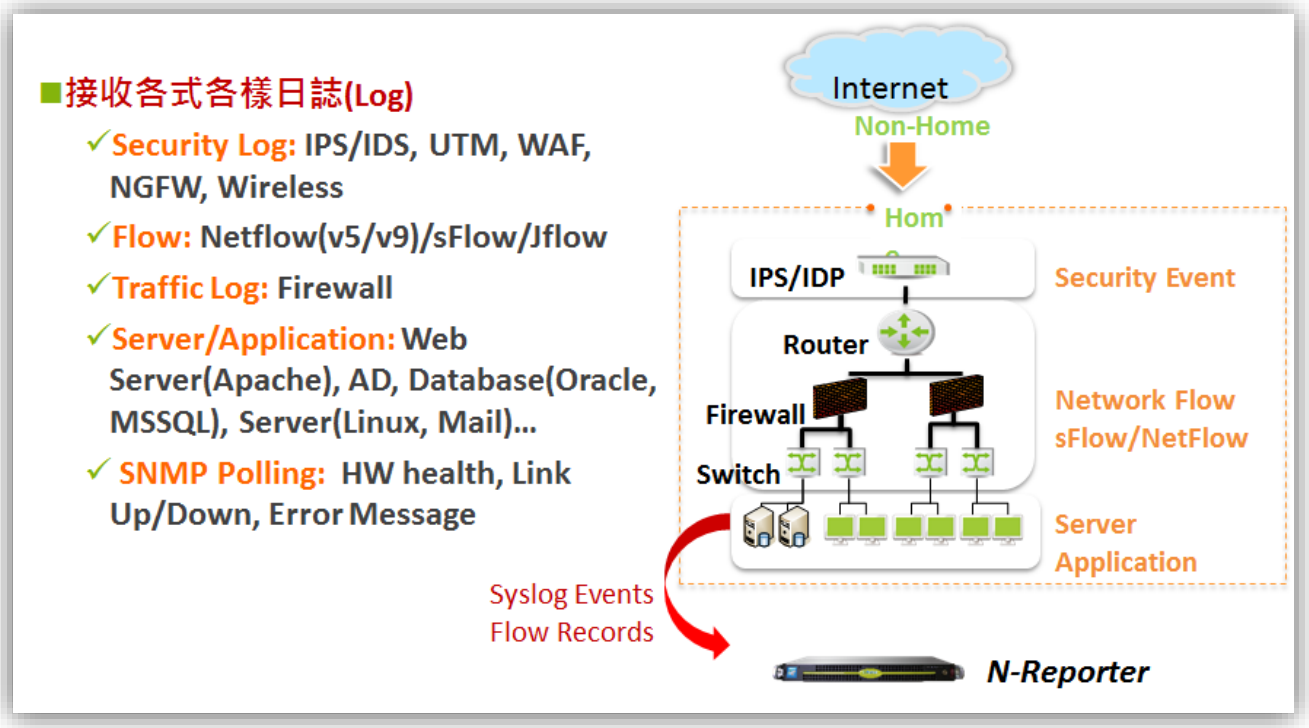
事件	來源IP	來源區域	目的IP	目的Port	目的IP名稱解析	次數
13019: DNS: DNS ANY Response	50.87.225.135	US	[redacted]	53	[redacted]	13,059
13019: DNS: DNS ANY Response	113.28.162.189	HK		53		6,965
13019: DNS: DNS ANY Response	71.120.142.229	US		53		6,783
13019: DNS: DNS ANY Response	113.28.163.227	HK		53		4,815
13019: DNS: DNS ANY Response	69.27.199.74	US		53		3,357
13019: DNS: DNS ANY Response	68.41.37.35	US		53		3,122
13019: DNS: DNS ANY Response	63.141.198.179			53		2,633
13019: DNS: DNS ANY Response	113.28.162.147	HK		53		2,006
13019: DNS: DNS ANY Response	63.141.198.217			53		1,801
13019: DNS: DNS ANY Response	104.255.76.117			53		1,136

圖七、從 Syslog 日誌分析發覺突增的攻擊事件，比對 Flow 資料得知該事件消耗多少頻寬

二、資料的採集(Data Collection)與大數據(Big Data)處理效能

2-1 SNMP、Flow 與 Syslog 資料採集的方式

如果想要達到前一章節所述的成果，對下轄網路狀態、人員的使用行為與資安事件狀態清楚掌握並相互關聯，首要工作就是做到完整的 SNMP、Flow 與 Syslog 資料採集。檢視網路環境中的設備，包括網路基礎設備(Router/Switch/Wireless/Load Balancer)、安全設備(Firewall/UTM/IPS/WAF/Web Filtering/Spam)、伺服器，逐一設定 Flow 與 Syslog 輸出。

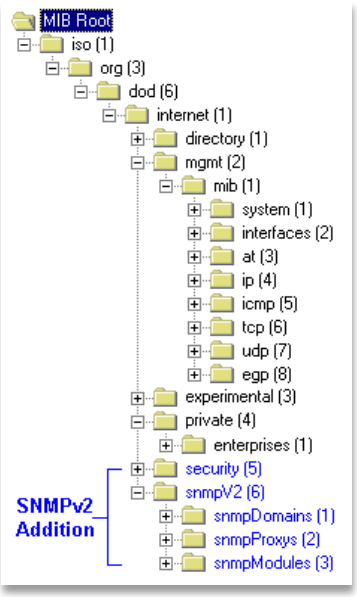


圖八、完整採集 SNMP、Flow 與 Syslog

✧ SNMP (Simple Network management Protocol) Polling

依循 SNMP v1/v2/v3 協議的設備會將各種硬體狀態數值(以不同 Object ID, OID 標示)儲存成樹狀 MIB file (Management Information Base)，外部管理軟體可以定時透過 SNMP 協定採集設備的 MIB 參數用以得知設備的健康狀態。

右圖是 MIB Tree。



✧ Flow (NetFlow, sFlow) Records Export

現今大多數品牌的 Router/Switch 都支援 Flow 丟出(Flow Export)功能。以下是 Cisco 設定 NetFlow 丟出的 CLI 命令範例： (Google search: Cisco NetFlow Configuration)

	Command	Purpose
Step 1	Router(config)# **interface** *type slot*/*port-adapter*/*port* (Cisco 7500 series routers) or Router(config)# **interface** *type slot*/*port*(Cisco 7200 series routers)	Specifies the interface, and enter interface configuration mode.
Step 2	Router(config-if)# **ip route-cache flow**	Enables NetFlow for IP routing.

To export NetFlow cache entries to a workstation when a flow expires, use the following command in global configuration mode:

Command	Purpose
Router(config)# ip flow-export ip-address udp-port	Configures the router to export NetFlow cache entries to a workstation.

To confirm data export, use the following command in EXEC mode:

Command	Purpose
Router# show ip flow export	Displays the statistics for the data export including the main cache and all other enabled caches.

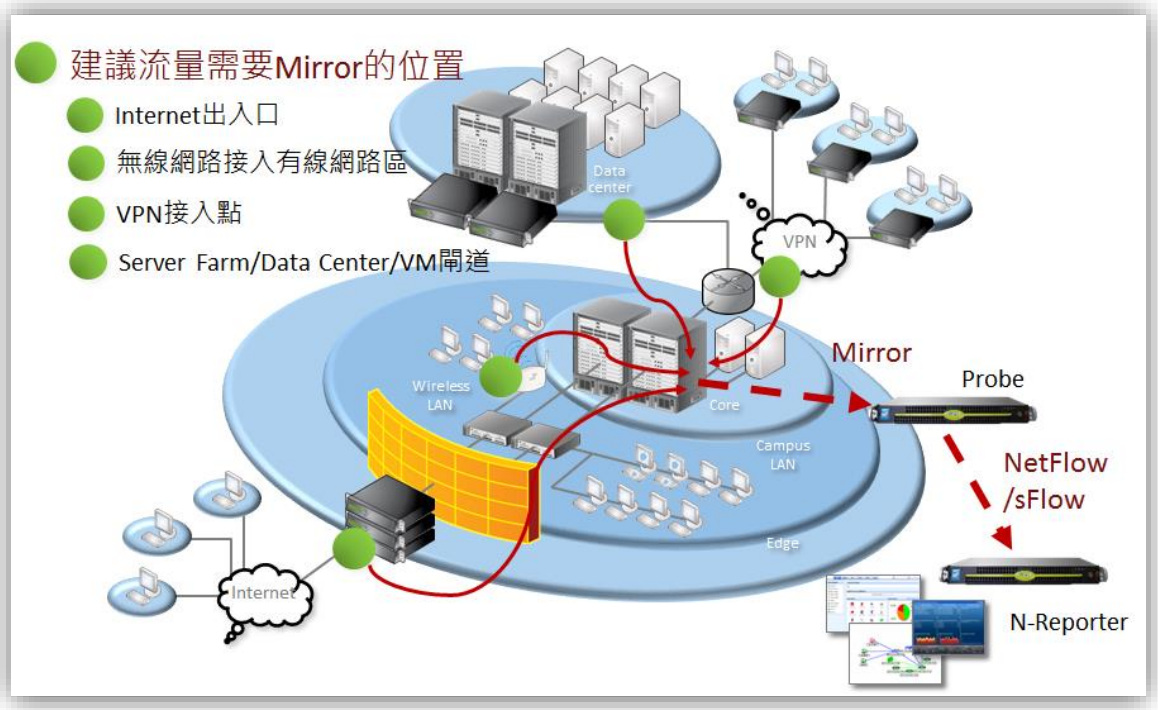
各家網路設備的 Flow 輸出設定方式並不相同，除了 Cisco 之外的廠商多數支援另一種稱為 sFlow 的格式，但是用途是相同的，就是記載流經設備的流量訊息。

來源IP	來源Port	目的IP	目的Port	Session	Packets	Bytes	Protocol	流入介面	流出介面
210.61.17.116	222	163.32.56.52	54335	1,024	1K	100K	TCP	Ten-GigabitEthernet2/7/0/5	Ten-GigabitEthernet2/0/0/1
163.28.130.14	443	163.32.78.56	1982	1,024	1K	1.41M	TCP	Ten-GigabitEthernet2/7/0/5	Ten-GigabitEthernet2/0/0/1
210.61.248.235	443	163.32.161.140	27334	1,024	1K	1.46M	TCP	Ten-GigabitEthernet1/7/0/5	Ten-GigabitEthernet1/7/0/1
163.32.74.24	80	101.12.32.82	14693	1,024	1K	1.4M	TCP	Ten-GigabitEthernet2/0/0/1	Ten-GigabitEthernet2/7/0/5
163.16.242.155	62107	163.28.130.13	443	1,024	1K	52K	TCP	Ten-GigabitEthernet2/0/0/13	Ten-GigabitEthernet1/7/0/5
163.32.211.9	80	118.160.184.38	57870	1,024	1K	1.45M	TCP	Ten-GigabitEthernet2/0/0/1	Ten-GigabitEthernet2/7/0/5
210.61.17.116	222	163.32.56.52	54335	1,024	1K	484K	TCP	Ten-GigabitEthernet2/7/0/5	Ten-GigabitEthernet2/0/0/1
210.61.17.116	222	163.32.56.52	54335	1,024	1K	164K	TCP	Ten-GigabitEthernet2/7/0/5	Ten-GigabitEthernet2/0/0/1
163.28.130.14	443	163.32.78.56	1982	1,024	1K	1.41M	TCP	Ten-GigabitEthernet2/7/0/5	Ten-GigabitEthernet2/0/0/1

圖九、Flow Records 內容

許多 IT 人員對於在 Core Router/Core Switch 啟動 Flow 存有效能受影響的疑慮。多數的網路設備在丟 Flow 時可以設定成取樣(Sampling)模式，以減少設備的效能負擔。不過，取樣模式會導致流量計算準確度失真的問題。部份高端的 Router/Switch 則支援加購專用的 Flow 卡用以專責執行 Flow 的轉換與丟出工作。

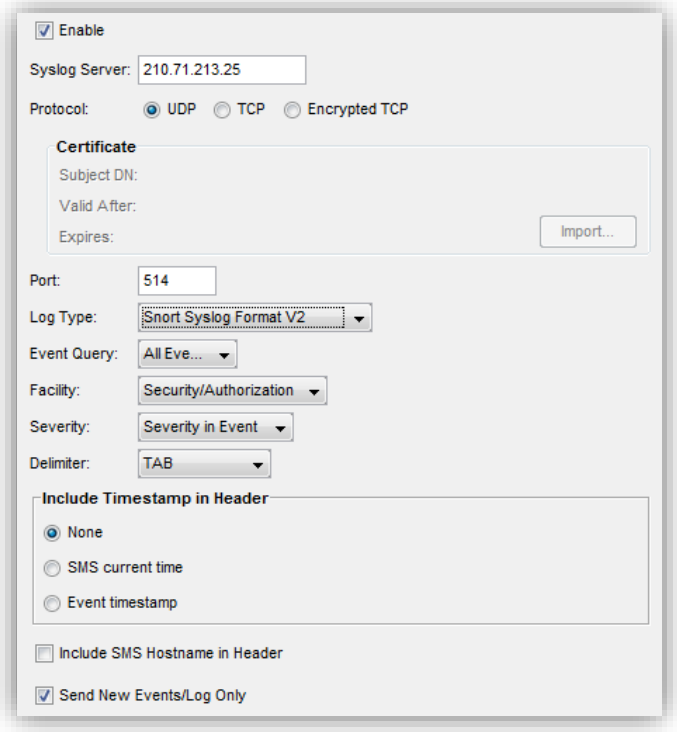
除了上述讓 Router/Switch 自己產生 Flow 資料的方式之外，市面上還有另一種普及的方案叫做探針採樣(Probe)，作法是將網路流量藉由鏡射(Mirror)的設定複製一份到外部的 Probe，由 Probe 代替 Router/Switch 把實際流量轉成 NetFlow 或 sFlow 格式後再丟到分析軟體，好處是不需佔用 Router/Switch 的運算資源，只是需要額外的預算採購 Probe。



圖十、建議流量需要 Mirror 的位置

✧ **Syslog Events Export**

使用 Syslog 方式將事件日誌(Event)丟出最為分析或是稽核備查之用已經非常普及，包括網路設備、安全設備、伺服器(OS、Application)都已能支援 Syslog。然而，Syslog 丟出的設定並不相同，日誌的格式也都不一樣，因此接收端的軟體需要能夠辨識與讀懂不同型態的日誌，並且正規化(Normalization)，才能做分析。



圖十一、Syslog 輸出設定範例

伺服器 Syslog 丟出設定可參考此網站 http://www.npartnertech.com/Support.html

原始的LOG難以閱讀！

```
        Facility auth (4), Severity error (3)
        Msg: Jun  5 22:50:01 163.15.40.248 BLK\011v4\01120110605T225001-0480\011"TF-TP600E"/163.15.40.248\0115665682\0112\011
Block\011Low\011b507ac3d-298d-11de-8256-000799a161c7\011"7120: TCP: Segment Overlap With Different Data, e.g., Fragroute"\011
"7120: TCP: Segment Overlap With Different Data, e.g., Fragroute"\011tcp\011" "\01160.0.0.3:60003\011192.168.1.3:1003\0112011
0605T224901-0480\01113\011" "\0110\0113B-3A
10:42:10.687311 IP (tos 0x0, ttl 64, id 1, offset 0, flags [none], proto UDP (17), length 354) 192.168.0.251.27531 > 192.168.
2.88.514: SYSLOG, length: 326
        Facility auth (4), Severity error (3)
        Msg: Jun  5 22:50:01 163.15.40.248 BLK\011v4\01120110605T225001-0480\011"TF-TP600E"/163.15.40.248\0115665682\0112\011
Block\011Major\011b507ac3d-298d-11de-8256-000799a161c7\011"7121: TCP: Header Length Invalid, e.g., Fragroute"\011"7121: TCP:
Header Length Invalid, e.g., Fragroute"\011tcp\011" "\011192.168.1.4:1004\01160.0.0.4:60004\01120110605T224901-0480\01114\011
" "\0110\0114A-4B
10:42:10.687336 IP (tos 0x0, ttl 64, id 1, offset 0, flags [none], proto UDP (17), length 354) 192.168.0.251.27531 > 192.168.
2.88.514: SYSLOG, length: 326
```

正規化後的LOG才能提供可分析的資訊！

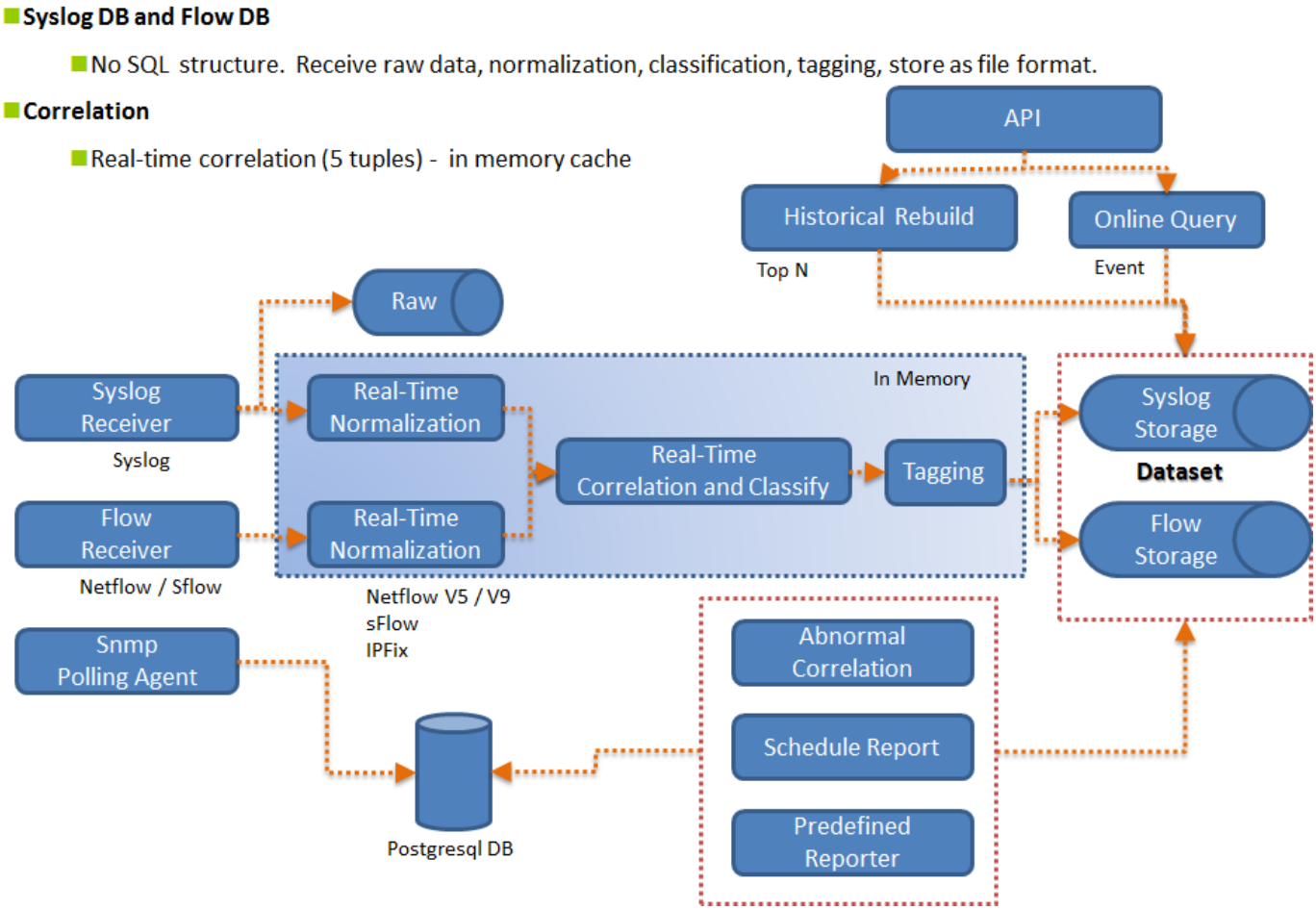
事件	來源IP	來源Port	來源區域	目的IP	目的Port	目的區域	次數
5601: SSH: SSH Login Attempt Client Request	110.45.139.40	34695	KR	203.72.197.204	22	TW	557
5601: SSH: SSH Login Attempt Client Request	110.45.139.40	46597	KR	203.72.197.138	22	TW	146
5601: SSH: SSH Login Attempt Client Request	110.45.139.40	47867	KR	203.72.122.185	22	TW	122
13608: TCP: PDF Containing FlateDecode Filter	163.32.250.179	80	TW	66.249.79.136	52619	US	76
13019: DNS: DNS ANY Response	163.16.40.2	60396	TW	163.16.1.12	53	TW	57
11349: HTTP: Default Page Request (ONLY enable when under DoS attack)	2001:288:8201:1:216:e6ff:	38126		2001:288:8401:0:163:16:	80		41
11349: HTTP: Default Page Request (ONLY enable when under DoS attack)	2001:288:8201:1:216:e6ff:	38126		2001:288:8401:0:163:16:	80		41
Black List 111.111.111.111	163.32.89.118	8433	TW	111.111.111.111	80	JP	40
13019: DNS: DNS ANY Response	163.32.48.1	53712	TW	163.28.136.2	53	TW	34

圖十二、Syslog 日誌正規化後才容易讀懂並進行統計與分析

2-2 蒐集大數據(Big Data)後的處理效能相當重要

將下轄網路裡的 SNMP、Flow 與 Syslog 資料集中蒐集的目的是為了可以完整呈現網路真實的使用現況，協助網路維運以及除錯，進而提供 IT 人員未來執行網路優化和擴容計畫時的確切可行方向。只是這麼龐大的數據資料處理起來並不容易，更何況 SNMP、Flow 與 Syslog 的資料屬性與內容迥異，要相互關聯起來；又要做到即時，確實需要非常高效能的邏輯處理能力。從資料的接收(Receive)、分類(Classify)、標記(Tagging)、儲存(Store)、搜尋(Search)、讀取(Read)、統計(Statistic)、人工智慧分析(AI Analysis)、告警(Alert)到報告(Reporting)以及記錄(Audit)的每個環節都必須緊密連結並有效運用運算資源。

我們用下方資料處理流程圖說明如何做到高效能的處理大數據：Syslog 與 Flow 資料接收進來後存放入記憶體中執行正規化(Normalization)拆解，接著根據 5 Tuples 原理進行關聯比對(Correlation)，加註標記(tagging)後離開記憶體以檔案的形式放入儲存空間等待後續的查詢與統計命令。



圖十三、大數據處理流程

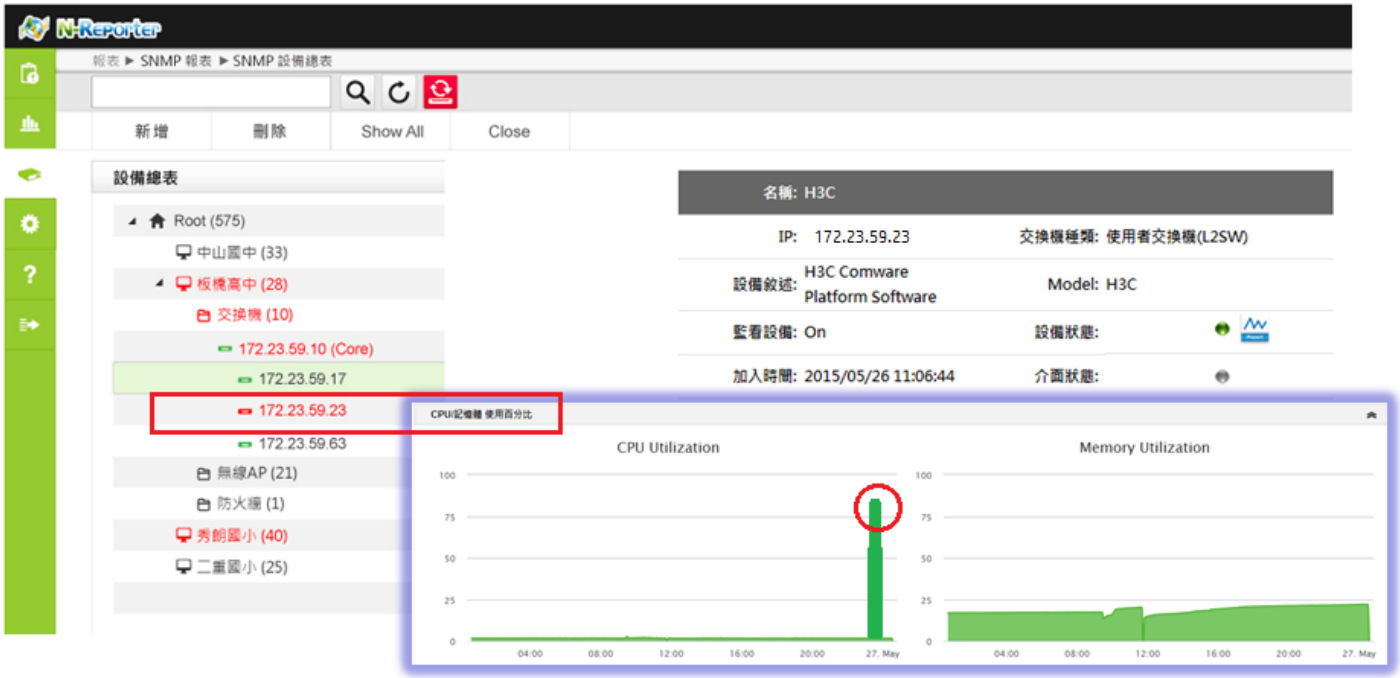
為了做到快速查詢，現今許多技術已經摒棄傳統的 SQL 架構改採檔案儲存(No SQL)。然而，檔案儲存後要能快速而精準的找到，清楚標記的工作是關鍵。整個資料處理的過程可以想成餐廳上菜的步驟，餐廳上菜速度要快，通常是預先將食材處理成半成品後，再依據客戶下的訂單內容組合烹煮。請看下表的對應說明：

	餐廳上菜的流程	大數據處理流程
步驟 1 **Normalization**	食材進來後必須先做處理，洗滌、切去不需要的部分、生食熟食分類	將接收到的 Flow 以及 syslog 資料進行正規化處理
步驟 2 **Correlation**	把幾個會烹調在一起經上一步驟處理過後的食材進行初步的烹調	正規化後的資料根據 5 Tuples 原則關聯在一起
步驟 3 **Tagging & Store**	將初步烹調後的半成品暫放在適當的地點，食物架或是冷藏。註記半成品品名與存放地點	在以檔案型態存入 Storage 前先做各種標記：時間、屬性(Attribute)、重要級別、自編序號、存放位置等
步驟 4 **Search & Report**	客人下單後將幾個半成品分別從儲存地方取出，依據客人的口味要求進行烹調，上菜	使用者下達查詢或是 TOP N 統計報表製作指令，系統將根據指令的條件分別抓取檔案進行整合演算，輸出結果

三、以人組織為基準的 SNMP 設備狀態監控、Flow 流量分析、日誌事件統計

3-1 全新 UI 設計概念，連結組織與設備關係的樹狀結構拓撲

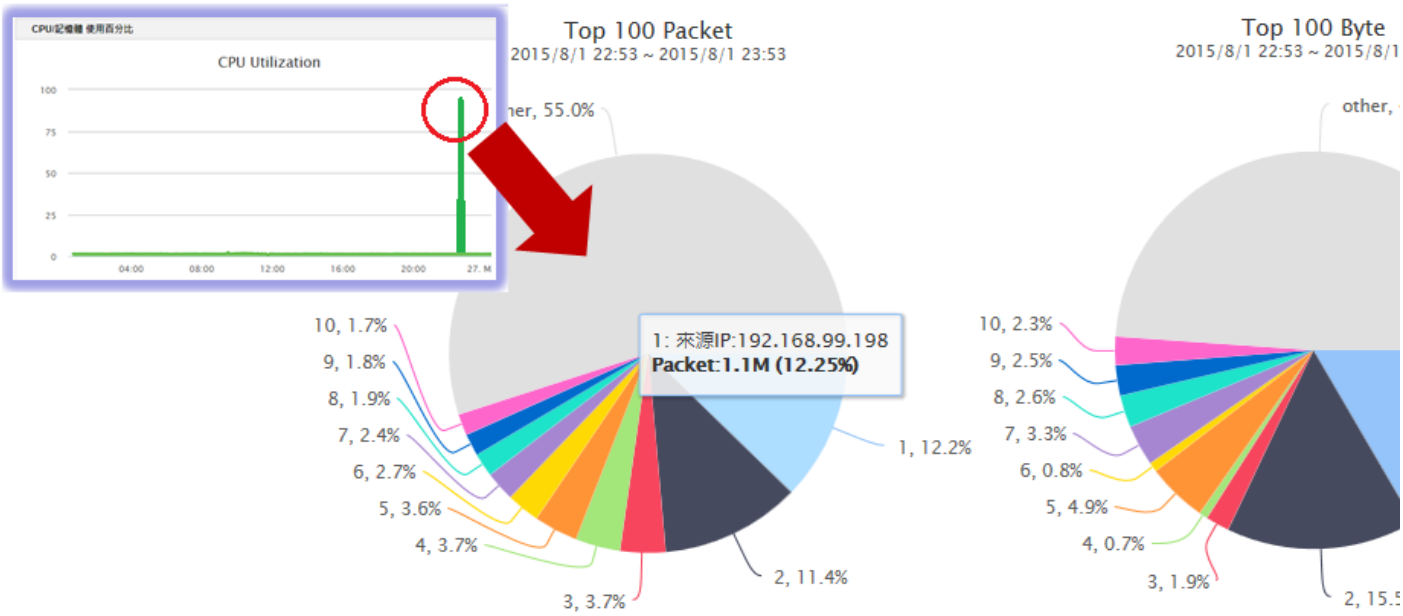
傳統網管軟體所使用的拓撲圖功能在大型網路架構下相當不容易繪製。管理者往往需要在好幾個畫面之間切換或是使用縮放功能才有辦法定位到欲查閱的設備。新的拓撲設計概念則強調人的組織與設備間的關聯性，採用樹狀分層結構(Tree View)將人組織間的主從關係以類似 Windows 檔案總管資料匣的模式建立妥後，再將佈署於各組織裡網路設備：諸如路由器與交換機新增於所屬組織的資料匣中。網路設備也可以階層關聯化，交換機依據實際環境中 Core-Distribution-Access Layer 的佈署結構呈現於組織資料匣內。最後，將需要監控健康狀態的伺服主機連接在交換機之下，完成樹狀拓撲。樹狀拓撲可以將資料匣收合，因此即使是數十個或是數百廠區、校區、外點單位；數百甚至數千網路設備與伺服器的 IT 規模也能輕易收納於一個螢幕畫面中。透過 SNMP 定時取得設備的健康狀態參數，監控時若發現某設備出現異常的情況，該設備所屬上層資料匣就會以警示燈號顯示告警，此時管理人員只要用滑鼠點擊展開這個警示燈號亮起的資料匣就能夠立即找到發生健康狀態異常之設備，以及這個設備所有的 SNMP 監控訊息與使用率圖形。對網路管理人員來說，能即時掌握出現異常設備所在的組織位置，就可以快速回應來自該組織的報修請求，並於最短時間內進入下一階段的除錯工作。



圖十四、連結人組織與設備關係的樹狀結構拓撲

3-2 SNMP 監控發現異常，關聯 Flow 流量與日誌訊息找出障礙根源

當 IT 人員從網管工具得知一個報警後，諸如某路由器的 CPU 使用率(Utilization)超過 90%，接下來的工作就是盡速執行除錯檢查。傳統使用 SNMP 監控設備健康狀態的網管工具只能做到異常通報，但是無法釐清之所以導致設備運作異常的根本原因為何。現今的情況是：網路發生障礙有很大的比例其實與安全事件相關，突發巨量的小封包在網路裡無預警流竄就非常容易讓網路設備超載進而癱瘓網路服務。新一代的網路維運方案能夠在偵測到設備使用率有異常生高的情況時，主動切換到 Flow 分析模式，找出當下是否有任何 IP 正在產生巨量流或是封包數，關聯 SNMP 監控與 Flow 分析兩種技術，即刻查出導致網路設備異常的來源 IP，IT 人員就能進行後續的處置作為，在最短的時間內恢復網路的正常運作。



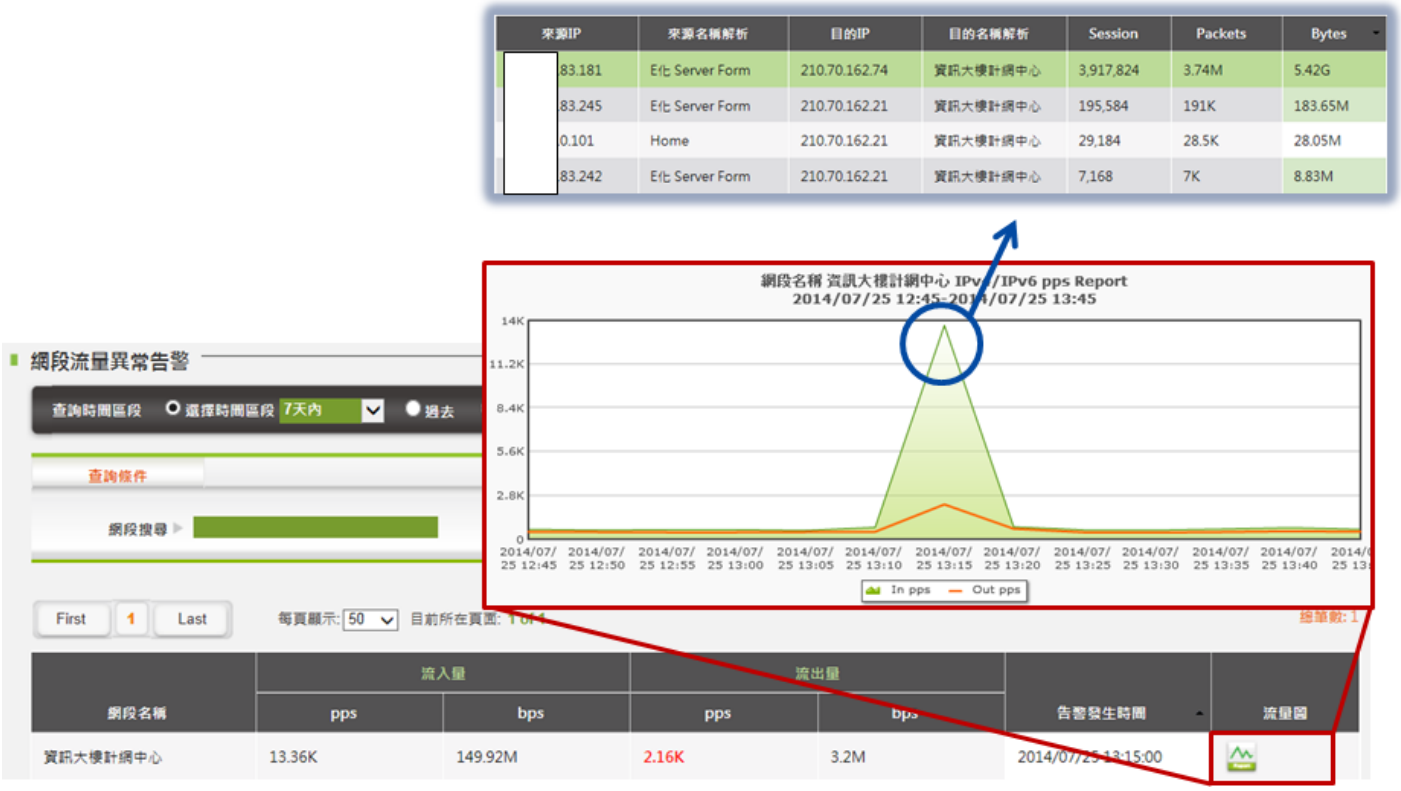
圖十五、設備使用率異常時關聯 Flow 分析即時找出發送來源

3-3 以人的組織為依據進行流量分析與用量圖繪製

將整個網路架構細分成幾個區塊分別進行使用行為監控會是一個有效管理網路的方式。細分的依據最好是根據實際的組織架構：一廠、二廠…；一樓、二樓…；工程部、行銷部、無線網路區段…；台北辦公室、台中生產中心…；數據中心、教學大樓、宿舍…DNS、Web、Mail Server…等概念來進行分區分段的流量監控與分析，並繪製流量報表。IT 人員可以用設定門檻值的方式讓超過用量的單位發出告警，新一代的智慧系統還能做到藉由學習各組織歷史用量的方式自動建立動態 Base Line 後比對當下數據，主動針對出現異常爆量的組織發出告警。IT 管理人員可以一目了然所有下轄組織的流量使用動態，揮別過去被

動接收報修通知後才開始進行流量監控以及除錯分析舊法與時間浪費，新一代的智慧系統已經將哪個單位有異常？是這個單位裡的哪些 IP、哪些人因為不當使用而造成整個網路發生障礙的答案即時告訴 IT 管理者，可以直接對問題目標採取處置作為，恢復網路正常運作。

圖十六、以人組織作為 Flow 分析的基礎單位，用 CIO 觀點隨時掌握發生異常用量的組織



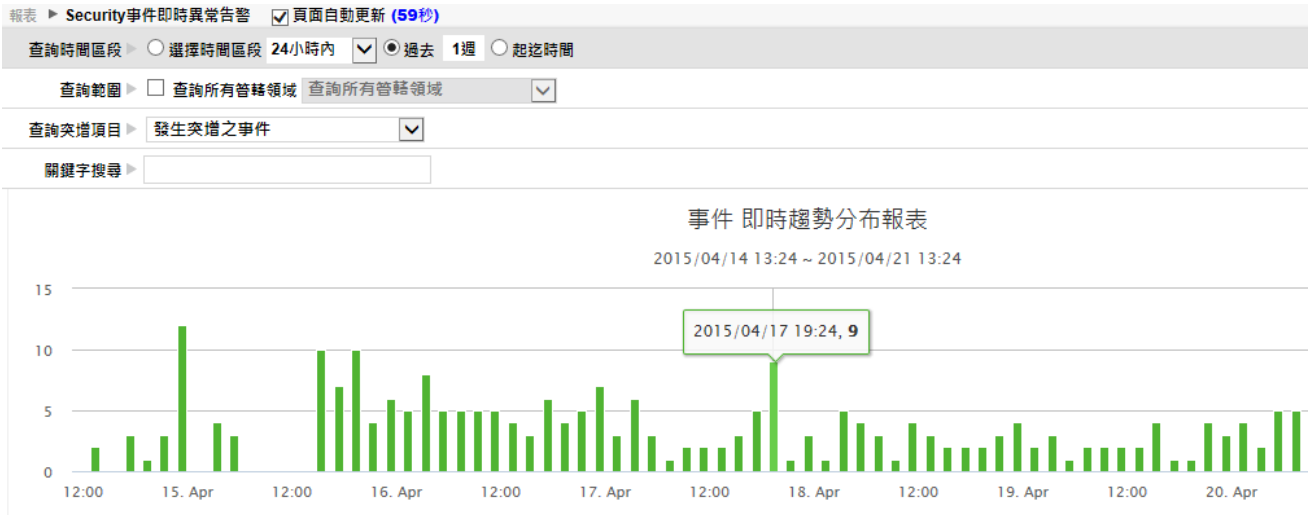
圖十七、針對發生流量異常的組織進行 Drill Down 分析找出問題來源 IP/使用者名稱/所在位置

四、 自動學習與即時發現異常

4-1 掌握全域裡下轄每個組織的網路與安全事件即時動態

其實對於 IT 管理人員來說並不是需要非常多的所謂智慧分析 Use Case，主要原因是產業不同、組織不同或是網路使用政策不同等因素讓許多 Use Case 是無法通用的，就算買了昂貴的網管或是日誌分析工具，IT 人員仍然必須要花不少時間將自己管理與除錯 Know-How 逐一寫成分析規則(Rule)後拆解日誌才可能有實質的幫助。不只如此，隨著環境與種種使用條件的改變，寫好的 Use case 也是需要持續修改才能減少錯報問題。還有一個更棘手的問題跟如何量化有關：如何為每一個 Use case 監控條件定義適當的門檻值(Threshold)用以驅動告警機制是非常困難的。舉例來說：針對一個組織流量使用，超過多少流量或是 Packet 數算多？同一台伺服器，到底多少的連線數算多？對於同一個資安事件，到底發生多少次數算是嚴重？再者，平日與周末、白天與夜晚、甚至不同的每一個小時該如何定義門檻值？

N-Cloud 運用人工智慧所開發的趨勢演算法則能根據蒐集到的 Syslog/ Flow 歷史資料，自動學習建立每個 IP 用量以及每種事件行為合理的 Base Line，持續比對每一分鐘進來的 Syslog/Flow 數據，即時發覺事件次數(Hit Count)、流量 Packet 數或是 Byte 數異常突增的事件、來源 IP(通常是攻擊端)以及目的 IP(通常是被攻擊端)。N-Cloud 維運平台會呈現分析結果於趨勢報表功能中，並將發生異常突增的內容主動寄發通知郵件給相關的網管老師，以利於第一時間處置網路中的的異常狀況。爾後網管老師無需為所轄各單位或是 IP 猜測合理的 Threshold 值，N-Cloud 的 Behavior Base 偵測與分析功能即可充分掌握網路環境裡值得注意的變化，讓維運工作變得更輕鬆容易



圖十八、根據歷史數據自動學習建立動態 Base Line 後比對每一當下狀態，即時發覺異常

4-2 Any-to-Any 的分析

IT 人員執行維運工作大都有同樣的困擾，那就是如何在第一時間就可以知道障礙發生了？發生在何處？根源是甚麼？

其實要得到上述問題答案的關鍵就在於對異常的確實掌握，諸如：下午四點的時候 DNS 伺服器的查詢突然爆量了；組織裡某個 IP 發出比平常多十倍的連線數到國外；凌晨兩點 Botnet 開始活動；DDoS 攻擊瞬間癱瘓了我們的頻寬與服務等等。解法就是掌握異常，問題是又該如何對每個目標定義異常的標準？在前個章節 4-1 我們闡述了根據歷史數據自動學習並針對每個日誌事件、每個服務、甚至每個 IP 建立自己專屬的動態 Base Line，就能夠比對每一刻的數據是否超標最近期的 Base Line，達到掌握異常的目的。理論上是這樣做沒有錯，問題是在執行這個工作的過程中有一個技術瓶頸必須突破，就是如何能同時監控這麼多的目標？試想在一個真實環境中，如果產生的日誌內容超過十萬種，那等於要建立十萬個監控分析條件，分別計算動態 Base Line。更大的監控量體是 IP 與流量，如果要準確計算 DDoS 攻擊，那就必須針對每個進出的 IP 都開一個記憶體空間 Queue 累加這個 IP 所傳送的流量，然而在有限的記憶體條件下，這個需求幾無達成的可能。因此，現在的網管或是流量分析方案採用的取代方式是：IT 人員必須事先定義要監控的目標，例如把 DNS 的 IP 設定為監控模式，再針對這個 IP 的流量行為進行數據累加與分析的工作。這種方式又會回到 IT 人員如何全面並即時掌握障礙發生的老問題：要將哪個 IP 或是事件放入監控條件？因為我們根本無法預先知道哪個 IP 或是事件會發生異常。

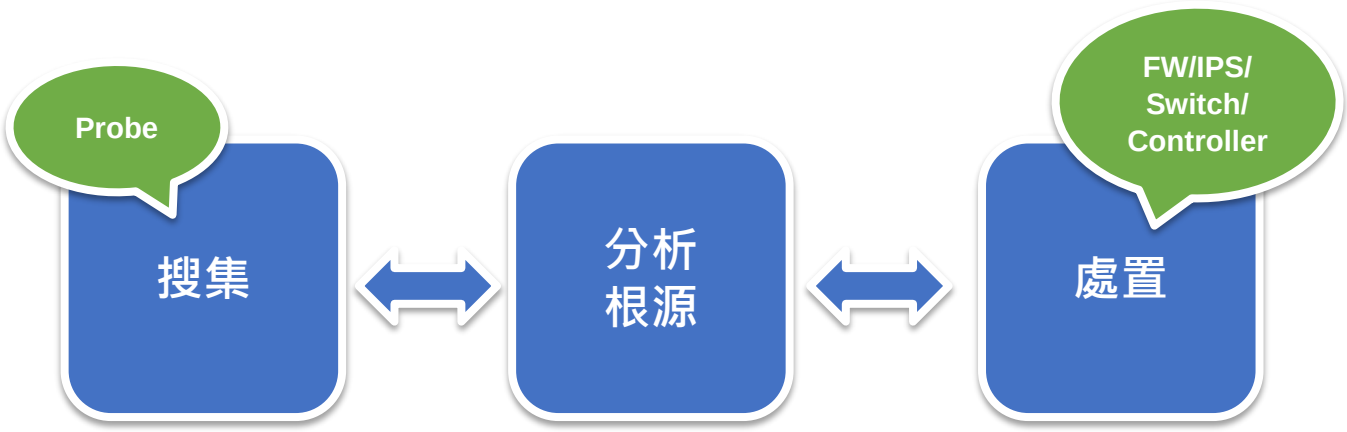
要做到不預設監控條件的 Any-to Any 分析就要改變固定 Queuing 的概念。每 15 秒鐘做一次 TOP N 排序掃描，把有限的記憶體空間留給正在 Active 的 IP 與事件，配合 Priority

的排隊順序規則，如果這個 15 秒某個 IP 沒有流量，不是直接從記憶體中刪除，而是逐次降低序位，下一個 15 秒有量了就提高序位；還是沒有量繼續將低，直到離開記憶體空間，如此就能做到 Any-to-Any 的分析。N-Partner 公司生產的 N-Reporter/N-Cloud 維運平台能在電信環境中即時分析到 DDoS 攻擊的來源就是善用了原理，大量縮短 IT 人員排除障礙的困難度。

4-3 區域聯防的實踐

有許多案例是：網路裡經常出現因為校園師生或是政府與企業僱員的電腦遭入侵成為殭屍電腦(Botnet)，在接收控制駭客的攻擊指令後往 Internet 發送巨量封包而導致網路頻寬遭耗盡癱瘓的災害事件。此外，對許多經營網站服務的組織來說，即時阻斷來自外網的攻擊更是確保服務不中斷的必備手段。IT 部門執行整個障礙的處理過程分成三個主要階段：

- ✧ **蒐集資料：**包括接收 Flow 與 Log 數據，從 Mirror Traffic 抓取需要的內容等
- ✧ **分析障礙根源：**將蒐集來的資料進行分析，新一代的管理系統必須能夠做到關聯各種類型數據(SNMP/Flow/Syslog)、學習歷史數據建立動態 Base Line、即時發現異常並告警、大數據處理效能以及內建人工分析智慧等
- ✧ **進行處置作為：**迅速阻擋異常來源，恢復網路服務的正常運作



圖十九、障礙處理三流程

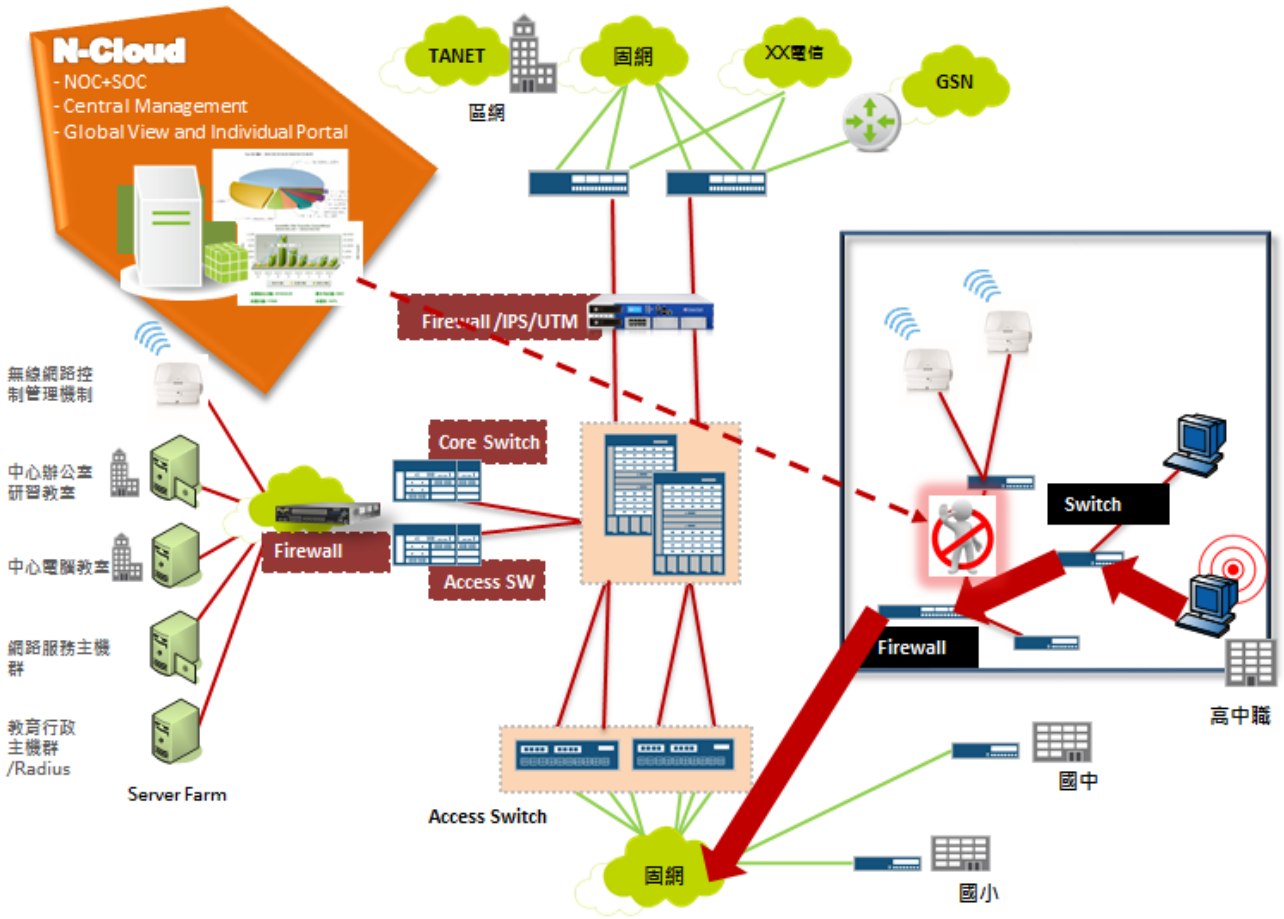
區域聯防的概念就是要能夠結合分析系統與防禦設備，將惡意的攻擊來源在最快的時間內找出，再交由距離攻擊來源最近的設備(例如：IPS/FW/Switch/Router 等)進行阻擋隔離，發生的異常障礙才能消弭，或是至少能夠大幅降低危害。如果攻擊來源位於內網，透過 L3 Switch 比對出該攻擊來源 IP 的 MAC，再詢問下轄所有 L2 Switch 這個 MAC 的所在實體 Interface，IT 人員就能快速定位這個攻擊來源是在哪個 Switch 的哪個 Interface 底下，進行聯防處置。如果攻擊來源是外網，則直接下達封鎖命令於聯外的 Gateway 設備上。

✧ **分述區域聯防實施步驟如下：**(以 N-Partner 公司生產的 N-Reporter/N-Cloud 維運平台為例)

步驟 1- N-Reporter 平台持續蒐集 IPS/FW 的資安事件日誌、交換機所吐出的 Flow 訊息

步驟 2- N-Reporter 系統內建人工智慧數值分析演算法，能根據過去一小時的流量歷史紀錄模擬出合理的流量預測值用以比對每一分鐘的即時流量數據與安全事件次數，主動查覺異常後找出造成異常流量行為的來源 IP 資訊

步驟 3- 根據上步驟所得知的 IP 資訊進階查詢出其所在 Switch 與 Interface Port，IT 人員就能夠手動下達 IP 封鎖指令給距離攻擊來源最近的 IPS/FW/交換機設備，將造成流量異常的來源予以隔離，避免網路災害擴大



圖二十、N-Reporter/N-Cloud 與 IPS/FW/Switch 整合執行區域聯防

五、整合 SNMP、Flow 與 Syslog 技術，建構新一代 IT 智慧維運方式

5-1 IT 維運的現況與問題

隨著組織營運與服務規模的成長，內部系統 IT 化的進程越來越快速。企業或是大多數非營利組織對 IT 系統運作的穩定性和品質要求也跟隨著不斷提升。而 IT 部門所面對到共同的管理難題不外乎是因為採購的軟硬體設備日益增多卻只能各自獨立維運，在管理上缺乏連結，不但無法發揮 1+1>2 的效益，反而增加了除錯的困難。現實的狀況都是當問題發生，影響了服務或是生產，IT 部門才開始在眾多系統中執行人工除錯，憑恃個人經驗試圖拼湊各系統的片面訊息，查找或是定位問題的根源，平時的工作幾乎都耗費在各種臨時除錯，成效卻不佳。下方列舉一些常常出現在 IT 人員心中的疑問。

- ✧ **人員反映有些郵件收不到也寄不出，真的是郵件伺服器的問題嗎？**

  現今全球有許多安全組織藉由郵件寄送內容的監控方式定義 Mail SPAM 清單，組織內部的電腦遭到駭客的入侵與擅用，寄送大量垃圾郵件或是廣告信函，組織所屬的郵件網域很容易被列入 Mail SPAM 黑名單中導致信件無法收發的問題。

  解決的作法是：學習並記錄組織內每位人員平時的寄件行為與信件數量，一旦發覺有異於平常量的發送活動應立即告警，IT 人員就可以即時阻絕。除了對郵件伺服器日誌的監控(Syslog)，也要透過流量分析的方式(Flow 分析)觀察 SMTP Port25 的用量變化輔助，才能全方位掌握垃圾郵件的問題。

- ✧ **網路異常緩慢時該如何即時知道原因？**

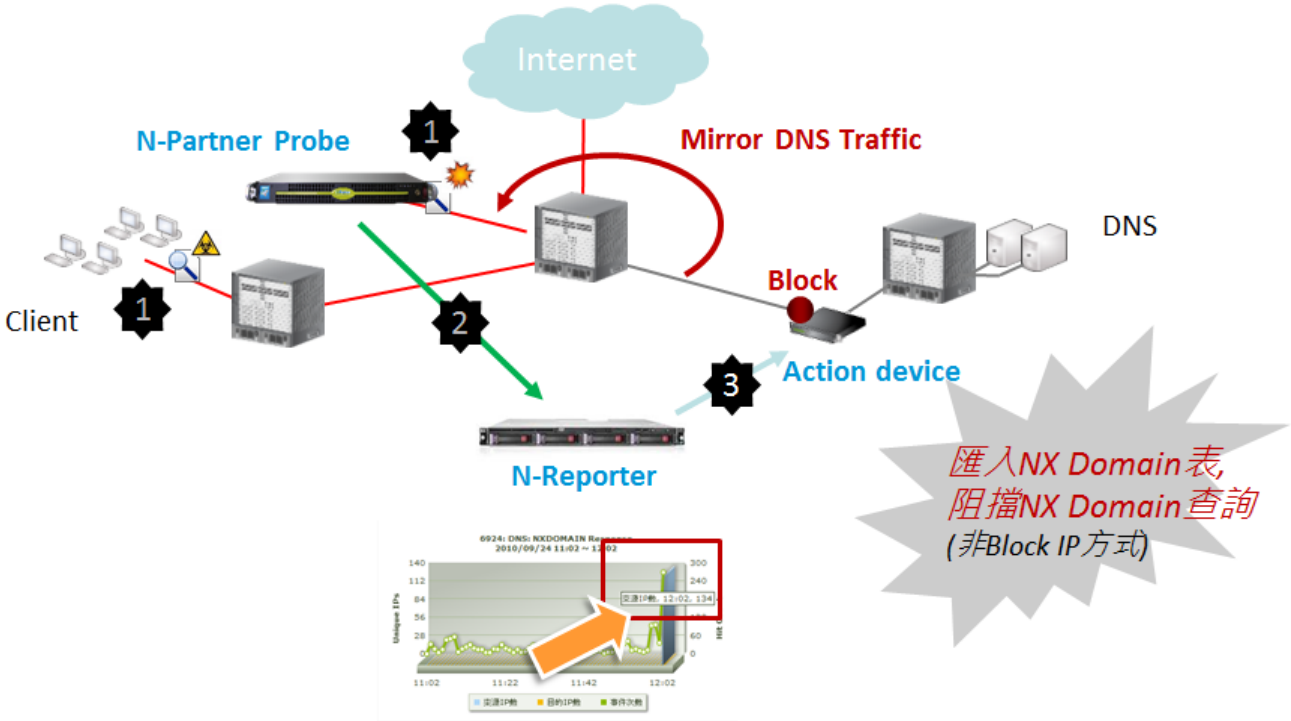
  解決的作法是：監控所有網路設備(Router/Switch/FW)的健康狀態(使用 SNMP 技術)，CPU 出現異常升高的情況，根據封包大小(Packet Size)分類分析哪些 IP 發送異常量的封包(使用 Flow 分析)。如果來源是外部，阻擋於外部防禦設備；如果來自於內網，定位 IP 在哪台 Switch 的哪個實體介面上(使用 SNMP 技術)，進行隔離。某些情況下網路設備的 CPU 並無異常，只是出現了巨大流量佔據有限的頻寬資源所造成網路壅塞。透過 Flow 分析自動學習每個 IP 歷史用量的技術可以即時掌握發送異常巨量的來源 IP。

- ✧ **無法瀏覽外部網站，或是客戶反映無法瀏覽我們的網站，甚麼原因？**

  這類的問題通常與 DNS 無法正常解析有關。

  解決的作法是：了解 DNS 的攻擊手法、提升 DNS 防禦能力並監控所有 DNS 的訪問行為，從中分辨出正常的 DNS 查詢或是惡意的破壞行為(使用 Probe 探聽與 Flow 分析技術)，透過聯防機制讓佈署的 DNS 防禦設備知道何時該阻擋甚麼樣 DNS 查詢行為。

- *1. Mirror DNS流量可得知哪些查詢的Domain是不存在的(NX Domain)*
- *2. 進行NX Domain的統計與即時爆量分析*
- *3. 將NX Domain匯入佈署於DNS前方的防預設備進行阻擋*



圖二十一、NX Domain 防禦架構與流程

✧ **私接無線 AP 廣播 DHCP 造成 IP 衝突**

市面上有些無線產品能夠偵測到非授權的無線訊號，透過 Syslog 將相關的日誌發送出來。發現這類的日誌出現時必須發送告警。日誌訊息帶有 AP 的名稱與 MAC，方便 IT 管理人員縮小找尋私接 AP 的範圍。

✧ **如何即時知道底層交換機 Broadcast 風暴正要開始爆發？**

解決的作法是：使用 SNMP Polling 佈署於底層(Access Layer)或是往上提一層(Distribution Layer)的 L2 交換機，統計與分析 Broadcast 封包數量，當 Broadcast 出現異常突增時需主動告警並定位發生於哪部或是哪幾部交換機。

✧ **網站遭入侵與重要資料外洩該如何處理或是防範？**

該佈署的安全防禦產品諸如 IPS、WAF、Anti-Virus、APT、Web Filtering、DLP 等都採購了，負責資安的人員卻無法百分之百確信安全已經無虞。另一個嚴峻的問題是：入侵與攻擊的手段日新月異，組織到底面臨何種威脅？而又該如何在已經購買的資安防禦設備上調整防禦策略，才能發揮最大的功效？

解決的作法是：除了針對資安設備所產生的事件日誌進行分析之外，亦須了解 Flow 資料所代表意義。由於防禦技術對未知攻擊手法辨識能力的限制，有許多方法可以規避

安全設備的檢查。然而凡走過還是會留下痕跡，Flow 紀錄往往提供了最佳的證據。駭客入侵網站或是試圖竊取資料的連線舉動勢必與一般人的瀏覽行為大不相同，可能是封包大小或是發送的速率迥異。只要透過精準的流量學習計算，取大數原則，就能發覺異常訪問的來源 IP。側錄該 IP 連線行為的封包，交由資安協力廠商研究有無既有的防禦規則能有效辨識，或是新開發防禦特徵，最後調整防禦策略，避免同樣的攻擊行為能再次穿越防禦網。

✧ **我們的網站來自全球各國的瀏覽統計，善意或是惡意？**

解決的作法是：採集 Flow 資料根據 IP 的所屬國家進行流量排行統計。透過長時間的學習，發覺瀏覽量異常(排名大幅上升)的國家，接著 Drill Down 細查是哪些 IP 傳送了大量。亦或是平時連線數非常少的甚至沒有的國家竟然出現了連線流量，這樣的情況發生時就需要進一步的分析與監控。

✧ **如何知道各部門的網路使用量?用量這麼大是甚麼樣的服務佔用了？**

解決的作法是：採集 Flow 資料根據 IP 的所屬部門繪製流量圖。得知每個部門的網路使用流量之後，再根據不同的服務(ex: HTTP/HTTPS/FTP/SMTP/TCP/UDP/ICMP 等)統計排行，藉此得知每個部門各種服務的用量分布。

✧ **DDoS 癱瘓了 IT 服務，有甚麼解決之道？**

DDoS 的攻擊模式相當多樣，而且常常是多種模式針對一個目標同時發動攻擊，導致防禦手段佈署的困難。

解決的作法是：消弭或是減弱 DDoS 攻擊必須像濾水的原理一樣，從大石頭、小石頭、碎石、細砂到薄膜一層一層過濾。除非攻擊量龐大到必須由電信端協助處理(清洗中心概念，將攻擊量分散到多個電信機房分別過濾)，大多數的 DDoS 問題皆可以透過下表所列步驟得到改善：

Step	Purpose	Method
1	管控 UDP/ICMP	1. 確認各段網路是否需要 UDP/ICMP 2. 建立阻擋例外清單
2	阻擋 TCP SYN Flooding	啟動 SYN Proxy/Cookie 防禦機制
3	阻擋全球已知惡意 IP	善用資安組織發佈的 Reputation 資料
4	建立自己的黑名單	1. 建立 IP 黑名單 2. 建立 Domain 黑名單
5	過濾發送過多封包之來源 IP	1. 依據服務的正常連線中,Client 端會發出到伺服器的封包數做為 Threshold 設定依據 2. 過濾超過 Threshold 的來源 IP

6	即時偵測出網軍攻擊發動時間與來源 IP	1. 使用 Flow 分析 2. 能經過前述步驟穿透的都是在 Threshold 以內的"看似正常來源" 3. Flow 可以發現集結眾多"看似正常來源"IP 卻同時發動連線請求而造成產生巨量的攻擊模式
7	消弭 Application 層次的 DDoS	針對七層行為的日誌做分析(EX:密碼猜測,網站巨量瀏覽,搭配 Syslog 日誌分析)，阻擋發動七層型態攻擊的異常來源 IP

上表步驟 1-2 是為了減少 IP Spoof 的攻擊量，施作得當，可以預期能通過的大多數是真實 IP，爾後進行 IP 阻擋的時候才不會產生誤擋或是阻擋無效的問題。步驟 3-4 是為了阻斷已知有問題的 IP 與 Domain。步驟 5 是處理一個 IP 打大量的攻擊型態；步驟 6 則是要處理一群打出小量的 IP(規避步驟 5 的防禦作為)集結起來的攻擊方式；步驟 7 是專門處理第七層的 DDoS 攻擊方法，因為經過步驟 5-6 的過濾後應該鮮少有量大的情況存在，大都只剩七層類行的攻擊。這部分光靠 Flow 不能妥善處理，必須搭配 Syslog 日誌。

✧ **內部人員無法登入網域使用內部 IT 資源，障礙原因為何？**

如果組織的 AD 系統設有輸入密碼錯誤達 N 次後將該帳號鎖定的機制，往往會出現冒用他人帳號進行密碼猜測，導致無辜被冒用者因帳號被鎖定而無法登入組織網域執行工作的問題。

解決的作法是：把 AD 的鎖定機制取消並不是一個好的做法，應該是要針對 AD 登入錯誤的日誌進行分析(Syslog)，發現密碼猜測行為；更甚者某帳號在密碼輸入錯誤多次後隨即出現登入成功的訊息(表示有可能猜測成功)都應該即刻告警。定位發動猜測的來源 IP 位置進行隔離(SNMP)。

✧ **我有這麼多系統日誌要監控，能減少人工的處理負擔嗎？**

解決的作法是：選擇處理效能優異的產品，集中蒐集所有系統日誌(Syslog)，輸入日誌中需要被監控與觸發告警的關鍵字，當事件數超過(突增)或是低於(突減)預設的門檻值時馬上發出告警。

✧ **下轄網路這麼龐大；這麼多人使用網路，我能即時知道哪個 IP 發生了異常？誰正在用這個 IP？這個 IP 在哪個實體位置？**

異常的定義就是易於平常。問題的關鍵在如何學習每個 IP 的網路使用狀態，才能建立每個 IP 各別的 Baseline。有了 Baseline 之後才能逐一分鐘比對當下的使用狀態是否與這個 Baseline 間出現了巨大的乖離情況，視為異常，進而主動告警。IP 的網路使用狀態包括 Flow 用量分析以及七層行為(由 Syslog 內容得知)，也就是說，異常監控應

該包含網路使用量的異常(ex:發送多於平時數倍甚至數十倍以上的封包)與行為異常(ex:一分鐘內進行超過 50 次以上的帳號密碼登入動作)。

解決的作法是：整合 AD 的登入記錄，將出現異常網路使用行為的 IP 轉換成 AD 網域登入名，協助 IT 管理人員與主管部門知曉該 IP 的使用者。使用 SNMP polling L3 交換機，查詢異常 IP 的 MAC 資訊，接著 polling 組織裡的底層 L2 交換機，詢問這個 MAC 是連接在哪個交換機的哪個實體埠，就可以得知這個異常 IP 所在的實體位置。

✧ **資安事件這麼多，每個時間點應該要優先處理的事件是甚麼？**

安全防禦的作法從處置方式來看主要分成兩種：經判斷為嚴重等級危害而且幾無誤判可能的事件，多數會採取在第一時間發現時就予以阻擋(Block)；另一種情況是，在事件出現的當下並無法立即判定是否為攻擊或是惡意威脅，需要持續觀察一段時間再做判斷者，通常處置方式會是先放行(Permit)，DDoS 攻擊就屬此類。能夠阻擋的對 IT 人員來說其實簡單，就是事後看統計報告。然而對於必需暫時放行的事件就要保持警戒，當威脅確認或是攻擊突增超量時，必須將處置行為從放行立即修改成阻擋模式，以避免災害擴大。

解決的作法是：採自動學習方式為每個接收到的事件(Syslog)建立 Baseline，逐一分鐘比對事件當下的次數(Hit Count)是否與這個 Baseline 間出現了巨大的乖離情況：，視為異常，進而主動告警。告警的內容包括突增事件、突增次數、發動該事件的來源 IP 與接收該事件的目的 IP、發生時間等。

✧ **如何呈現 IT 維運的績效？如何根據 IT 現況精準訂定未來調整與優化的需求？**

依據部門組織分別製作資安事件統計報表，逐月檢視各部門安全事件的次數是上升或是下降；嚴重等級的事件是上升或是下降。要換購新的防火牆或是網路設備前已確認是正常使用下效能不足而不是因為人員不正當使用(或是電腦中毒或是遭受攻擊)導致 CPU 非合理的升高。要加購安全設備是因為從長期的 Flow 分析中得知我們的網站常常遭受非正常瀏覽行為的危害；是因為內部常有 IP 非人為操作的發送大量，在非工作時段連線到與組織幾無往來的國家。運行在伺服器上的服務效能不足如果是攻擊行為所造成的，那就應該規劃安全防禦機制過濾惡意流量而不只是盲目的添購伺服器。頻寬不足如果是因位人員使用會消耗大量頻寬資源的應用(ex: P2P)所造成，那麼網路優化的作為應該是訂定網路使用規範而不是申請預算採購更多的頻寬服務。

解決的作法是：必須善用 SNMP、Flow 與 Syslog 的分析技術，確實了解設備的健康、網路的活動與安全的狀況後才能訂定最適當的 IT 優化做法與未來擴建計劃，避免預算用在錯誤的投資上造成不必要的浪費。

5-2 採用 N-Partner 公司開發之 N-Reporter/N-Cloud 建構新一代 IT 智慧維運方式後的預期效益

- ✧ **跨設備廠牌蒐集，將所有採購的 IT 資源集中在一個維運平台上並加以運用**
- ✧ **全新 NOC+SOC 營運概念，在一個平台上完美整合三大網管技術(SNMP、Flow、Syslog)數據，透過彼此關聯交叉分析，協助 IT 人員充分掌握組織內的設備健康狀態、網路使用情況與資安威脅風險**
- ✧ **讓負責不同工作的 IT 人員可以在同一個平台上分享屬於自己管理範疇的數據，各單位間協同運作有助於障礙根源的快速排除**
- ✧ **CIO 擁有完整且即時的監控與統計訊息(Global View)，即使管理的組織規模龐大(如：跨國企業、電信服務商、政府與教育網等)，也能夠精準掌握下轄各分支單位的網路使用與資安狀態**
- ✧ **嶄新樹狀目錄收合管理概念，以人的組織為資料夾，資料夾裡再收容佈署於該組織的網路設備以及伺服器，可將全域 IT 設備收合在一個螢幕畫面裡。任何設備出現健康異常時，其所屬的組織資料夾會以燈號警示，IT 人員在收到告警後只要點擊該組織資料夾就可展開並且看見出現異常的設備，在最短的時間裡排除障礙**
- ✧ **以人的組織為分析單位繪製各種流量圖形，包括 Protocol 分布、封包大小分佈、Packet per Second、Bit per Second 等。Drill Down 功能讓 IT 人員可以非常直覺的從圖形的任一時間點查詢流量詳細內容**
- ✧ **採用 Any-to-Any 大數據分析技術，能夠學習每個 IP、每個事件的歷史使用數據，自動建立動態 Base Line 後比對即時狀態，主動發覺異常後發送告警。IT 人員只要將流量 Flow 與日誌(Log)導入 N-Reporter/N-Cloud 維運平台，就能輕易得知組織裡有哪些 IP、事件或是伺服器出現異常的狀況，快速定位問題根源後於最短時間恢復網路服務障常運作**
- ✧ **親和的使用者介面設計，無需耗時學習即可上手。擁有非常彈性的報表製作功能，允許 IT 人員依據各種實際需求客製報表，亦支援多種 Compliance 報表的自動生成**
- ✧ **N-Cloud 採用雲架構，是專為大型網路環境的管理需求而開發的系統。採用多租戶 Multi-Tenant 的管理架構，中心端可以瀏覽全域狀態而各分支機構無須自建管理系統就能採用分享 N-Cloud 的方式查閱屬於自己的 SNMP/Flow/Syslog 分析訊息並製作自己的統計報表**
- ✧ **搭配部分品牌 FW/IPS/Switch 進行端點聯防，即時阻擋攻擊來源 IP，快速恢復網路運作**
- ✧ **提升 IT 服務的除錯能力就等於提升組織的生產效率**

N-Partner 公司簡介

新夥伴科技股份有限公司(N-Partner Technology Ltd. Co.)成立於 2011 年，是一個專長於高效能大數據蒐集(Big Data)、人工智慧分析技術(AI and Abnormal Analysis)的研發團隊，總部位於台灣台中市。核心成員均擁有超過 15 年的電信等級網路維運以及軟體開發經驗，集合網路、資安、作業系統與 Kernel、電腦硬體與虛擬機、C 語言、PHP/Java、資料庫、大數據處理與雲架構、美術與設計等各領域專長的人才。

由 N-Partner 公司所開發的 N-Reporter 以及 N-Cloud 雙產品線為當前全球唯一能夠完美整合 SNMP、Flow 與 Syslog 三種主流網管和資安事件分析技術的 IT 維運系統，領先的技術包括：Any-to-Any 分析，能針對各個日誌事件與所有 IP 進行歷史行為自動學習進而建立動態基準，用以發覺異常並即時告警；關聯 SNMP、Flow 與 Syslog 三種數據，提供 IT 管理者清楚的障礙除錯依據等。此外，N-Cloud 維運平台更運用了雲架構來提供高處理效能、幾無限制的延展性以及萬人同時操作使用的能力，是世界上第一個商轉的 NOC/SOC 合一 SaaS 服務，已經獲得多家大型教育網、跨國企業與電信公司採用做為網路與資安的維運平台。在 2015 年之前，N-Partner 公司的商業版圖已經橫跨兩岸三地，並逐步拓展至南亞。

N-Partner

採購與銷售合作：sales@npartnertech.com
技術諮詢：support@npartnertech.com
更多產品資訊：www.npartnertech.com