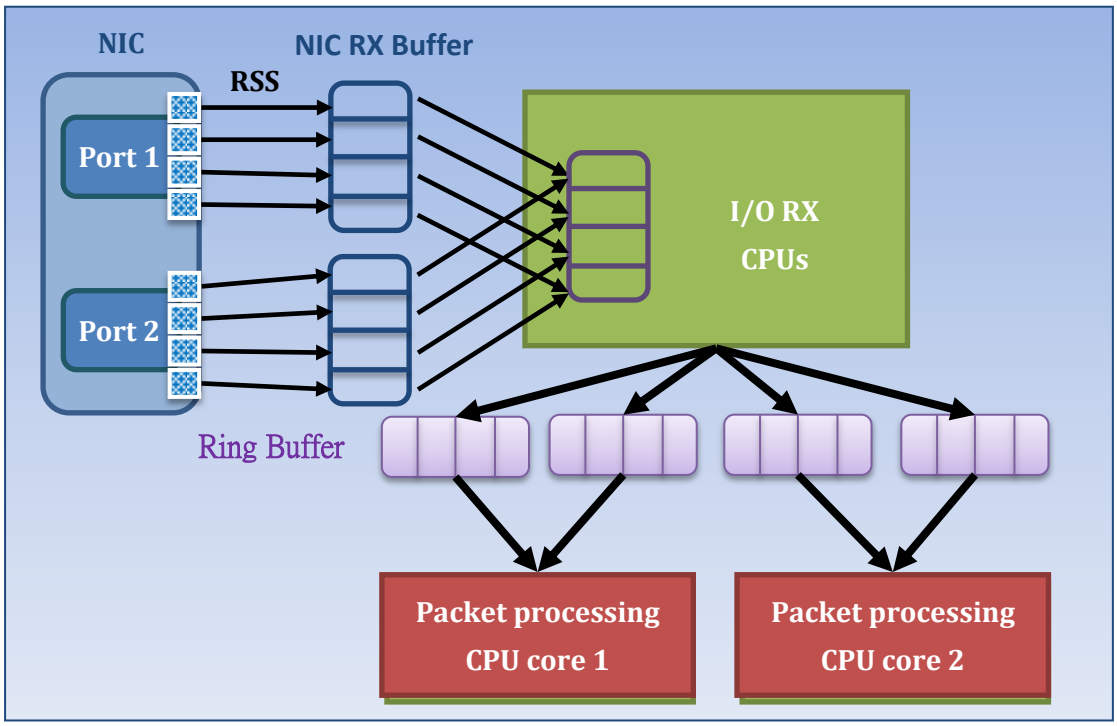
Flowviewer 產品特色與優點

原理

Flowviewer 採用具備 auto-bypass 功能之網路卡與優化後的系統。系統搭載由本公司獨立開發的異常偵測系統，包含能快速辨別異常流量（駭客入侵與攻擊）的特殊演算法與能快速收集網卡上封包的驅動程式，透過多線程/執行序（multi-thread）的方式可迅速收集封包；利用多核心處理的概念來提升整體處理效率，可在本機端或是透過 ACL (Access Control List) 在核心路由交換器(目前支援的廠牌有 Alcatel、Cisco、Foundry、Extreme)，阻斷惡意流量。由於軟、硬體搭配得宜，Flowviewer 並不會像市面上 IPS(Intrusion Prevention System)設備，在面對頻寬消耗型或是資源消耗型的攻擊便發生硬體故障的問題。

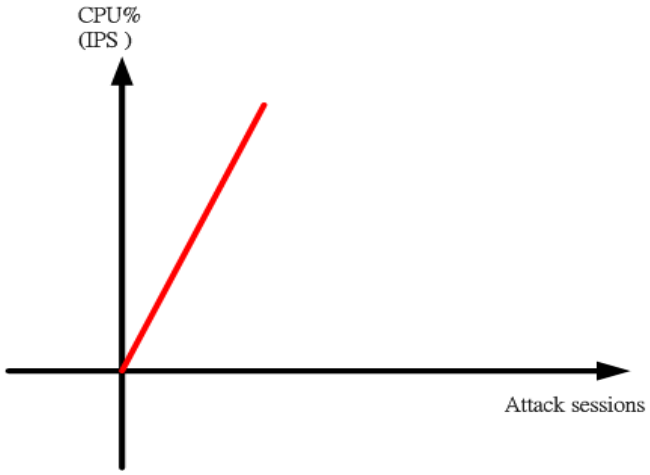


圖一　利用多核心及多執行序方式提升處理封包效率

Flowviewer 設備與 IPS(Intrusion Prevention System)設備之技術的比較

IPS 設備之技術採用深層檢測（deep packet inspection），此技術必須要過濾經過此設備上多數封包才能準確比對特徵碼（Signature）提高防止駭客入侵的準確率，此技術的架構一定是採用有 session 原理。此設備另一項功能防禦值（Threshold）是計算經過設備上每秒有多少封包及 sessions 數，防禦值（Threshold）由使用單位自行設定，此技術相同是採用有 session 原理。

採用有 session 原理的缺點，當使用單位遇到駭客 DDoS 攻擊時產生巨大 sessions 數經過 IPS 設備會導致此設備 CPU 使用率滿載讓設備當機，雖然 IPS 設備廠商宣稱是採用 ASIC 晶片技術，但是 ASIC 晶片也是屬於 CPU 的種類。不相信此說法的人可以拿任何一種廠牌的 IPS 設備來實驗，以軟體模擬 DDoS 攻擊製造大量 Flow（Session）攻擊 IPS 設備，觀察設備的 CPU 使用率跟 Flow（Session）攻擊數的比率情況，也就是 X 軸是 Flow(Session)攻擊數，Y 軸是設備的 CPU 使用率，並繪出座標圖。如果數據做的越多，應該是趨近直線，成線性關係也就是正比，再從二度空間推到三度空間，當 Z 軸是時間，在何時 IPS 設備會當機？



圖二　　攻擊 session 數與 IPS CPU 使用率比例示意圖

Flowviewer 設備是採用 non session 原理，為何可以達到 non session 架構？設備是接收取樣率 1:1 的 Netflow（或 sFlow）資料所以可以達到 non session 架構，藉由分析來源位址、目的位址、通訊協定、通訊埠號、封包數、傳輸量大小等資料來找出異常流量。如同大數據採用的全樣本原理，我們相信唯有利用大量的流量數據資料，並針對個別 IP 去進行分析，方得精準找出其行為規律性。在 IEEE 的論文期刊中也都可以看到有人發表與這項技術原理相關的文章。因此，我們誠摯建議客戶將 1:1 的 Netflow 資料轉送至 Flowviewer 進行分析，透過全部數據樣本的解析，便可精確判斷出哪些是屬於異常流量。雖然透過分析全部數據資料來作辨識是最完善的解決方案，然而在實務上，設備能不能接受海量的數據卻成了另一個問題，這就是此技術無法產品化真正原因，Flowviewer 設備採用自行開發的數學演算法與判別式，還有就是透過分析完整的流量資料，才能突破此技術的瓶頸。以我們的實際經驗來說，某 A 廠牌字母開頭的設備僅能接受取樣率 1:1000 的 Netflow。換句話說，就是從一百萬個封包中只取樣一千個出來做樣本分析，這樣的話又怎麼能精準判別出來呢？這表示有設備廠商是認同此技術，只是無法克服此技術的瓶頸。

Flowviewer 設備上有一項功能可以阻斷 Domain Name，使用單位只要將想封鎖的 Domain Name 輸入設備上即可，此功能的技術的確要分析經過設備上的封包，但是此技術只要分析 1 個封包就可以判斷出 Domain Name，不需要使用深層檢測（deep packet inspection）技術，所以可以達到 non session 的技術。

IPS 這類採用 session 的設備在阻斷時，同樣是要使用深層檢測的技術去分析流經設備的封包，因此在面對大量封包時，必定會大量消耗 CPU 等硬體資源，進而導致設備當機；而 Flowviewer 採用 non session 技術，因此不必擔心大量異常流量消耗硬體資源的問題，當然也不會因此而引發當機的問題。

實際案件說明

台灣新北市某知名私立大學因為某些原因被駭客以 DDoS 攻擊導致全校網路癱瘓，台灣電視新聞及網路新聞都有報導，駭客還透過網路發佈在哪一天要發動第二次攻擊，剛好此學校有購買 Flowviewer 設備所以網路管理者跟我們抱怨為什麼購買 Flowviewer 設備，還會造成網路癱瘓？我們來分析原因，此學校的網路設備架構是 Router 放置在最出口端，接著對內設備有 IPS 設備、Flowviewer 設備、Core Switch 設備，在學校網路癱瘓的時間 Core Switch 設備並沒有當機而且 Netflow 資料還有傳送到 Flowviewer 設備上，在從 Flowviewer 設備上有看到 IP 資料只是資料內容只有內對內的 IP 資料，並沒有內對外及外對內的 IP 資料，這表示 Flowviewer 設備也沒有當機，等於說明 Router 跟 IPS 設備有一台設備當機而導致全校網路對外癱瘓，Flowviewer 設備是每 5 分鐘收集一次 Netflow 資料後，在下 1 秒內以數學演算法快速分析判斷出攻擊的 IP 並且直接在設備上阻斷攻擊的 IP，而 IPS 設備竟然不到 5 分 1 秒內就當機導致全校對外網路癱瘓，我們不相信 Router 會在 5 分 1 秒內就當機，經過我們分析給網路管理者了解，而且駭客還會發動第二次攻擊，建議網路管理者將 IPS 設備卸下讓 Flowviewer 設備來判斷駭客攻擊並自動阻斷來攻擊的 IP，結果駭客還是有發動第二次攻擊而 Flowviewer 設備也順利阻斷來攻擊的 IP，否則駭客又要在網路發佈另一次的攻擊。網路管理者將 IPS 設備卸下就沒有將 IPS 設備再上線。所以你們可以模擬駭客使用大量 sessions 攻擊 IPS 設備，跟上述座標圖是否相同？

IPS (Intrusion Prevention System) / IDS (Intrusion Detection System) 設備是採用特徵碼（signature）方式去進行比對、過濾的。除了需要定期更新特徵碼外，在面對未知型的攻擊與入侵/零時差攻擊時，這樣的設備也難以在第一時間防護網路安全。駭客使用機器人程式在雲端網路對使用單位網路進行入侵每兩、三天就會變更使用的特徵碼，**事實上實際的說法是駭客使用入侵程式，而此入侵程式就是在對使用單位的網路進行猜測密碼的動作，如果成功就可植入木馬程式成為駭客的殭屍網路(botnet)，駭客也會針對特定埠號（Port number）來進行猜測密碼的動作，因為某些特定埠號比較容易進行內對內入侵**，再擴大殭屍網路(botnet)，而 IPS 設備就是收集這些機器人程式的特徵碼來過濾，防止駭客的入侵程式到使用單位的網路來猜測密碼的動作，駭客也會從內對內入侵來竊取軍事/商業機密資料。例：facebook 被竊取使用者資料，美國的資訊安全專家完全沒有分析到駭客是如何使用內對內入侵方式，都只探討駭客是如何找到軟體漏洞，最後結論是 facebook 員工下載 app software 讓駭客成功入侵到 facebook 內部網路然後成功竊取使用者資料，facebook 員工的電腦有 facebook 使用者的資料嗎？當然沒有，駭客一定是使用最新木馬程式進行內對內入侵並成功躲避保護 server farm 的 IPS 設備，駭客使用的木馬程式是最新程式在 IPS 設備的資料庫當然沒有，所以很容易躲避偵測並成功竊取使用者資料。如果我所敘述的觀念不是事實，那麼為什麼美國在 2017 年又會發生 Equifax 公司的使用者資料被竊取的事件？我猜想 2015 年 Hello Kitty 網站被駭，造成 330 萬用戶資料被竊，駭客也是使用此種方式。如果你是駭客知道這種方式可以成功竊取資料一定會使用此方式，而且駭客寫最新的木馬程式並不難；至於軍事/商業間諜也一定會採用新型的特徵碼去進行入侵行為，因此採用特徵碼的設備對於這類未知特徵的攻擊與入侵是束手無策的。利用特徵碼的方式去比對、過濾並非是完全不好的，但是在面對資源消耗型的攻擊時，系統效能會因為異常大量的封包而耗費甚鉅，進而引發當機的問題，上述已經有用數學座標圖概念來說明當機現象。部分 IPS / IDS 設備採用門檻值（threshold）去辨別駭客攻擊，由於門檻值設定太低會造成嚴重誤判、造成管理者的額外負擔。因此管理者並不會將門檻值設定太低，作為代價的結果便是讓駭客有機可乘。

另一方面，絕大多數的 IPS / IDS 設備都聚焦於「內部網路對外部網路」與「外部網路對內部網路」的入侵與攻擊，對於「內部網路對內部網路」的入侵與攻擊是不太著重的。金融與軍事單位常為了防範外部網路入侵與攻擊，都會採用封閉的網路環境。但也因為採用封閉網路的關係，造成管理者往往忽視了內部入侵的嚴重性與威脅性。當 Flowviewer 的分析資料來源是採用 Netflow 時，其資料包含內部對傳的流量，因此 Flowviewer 可利用獨有的 inner intrusion 功能去分析出內部入侵(insider intrusion)。

Flowviewer 設備判斷駭客入侵及攻擊之 IP 規律性分析

我們也創造出相關的數學方程式來做為判斷駭客入侵及攻擊的規律性機制，再加上實際單位的使用經驗。因為使用單位會告知設備是否有誤判情況。如果有誤判發生，我們會修正判斷式，直到使用單位說沒有誤判情況發生為止。

$$S: f(T_n, P_{src\,n}, P_{dst\,n}) = 1$$

$$\because T_n \in \mathrm{R}$$

$$\Delta T_n = T_{n+1} - T_n,\ \Delta T_n > 0$$

$$P_{src\,n} \in \{p \mid 1024 \le p \le 65535,\ p \in \mathbb{N}\}$$

$$P_{dst\,n} \in \{p \mid 1 \le p \le 65535,\ p \in \mathbb{N}\}$$

$$(P_{src}{}^n, P_{dst}{}^n) \neq (P_{src\,n+1}, P_{dst}{}^{n+1})$$

$$\therefore \sum_n f(T_n, P_{src}{}^n, P_{dst}{}^n) = Sessions$$

S: *session*
$P_{src\,n}$: source port number
$P_{dst\,n}$: destination port number
T_n: some time

圖三　　利用數學公式作判別準則

關於上述方程式，我們的 Youtube 頻道有簡單的解說
https://www.youtube.com/watch?v=yX_wp2oedYM
裡面也有關於「Simulate hacker attack_ Top 6 ways of hack attacks and how to protect」的影片：https://www.youtube.com/watch?v=vKweWU82okI

實際案例

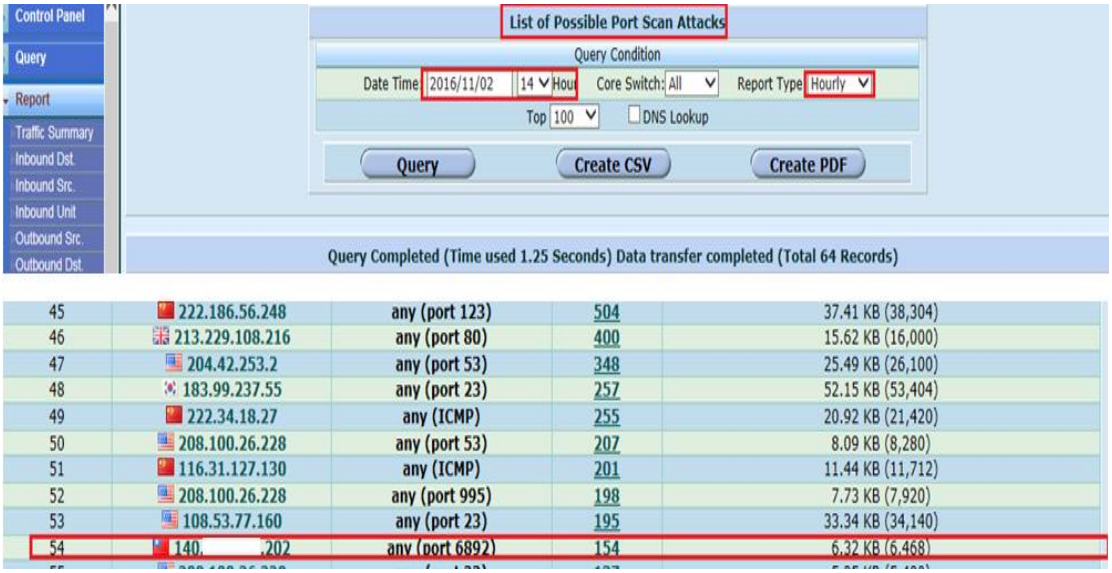
案例一：WannaCry 勒索病毒

2017 年 5 月該病毒於全球大規模傳播，利用微軟 SMB 協定中的數個漏洞進行主動傳播。透過利用漏洞，病毒可以獲得作業系統的特權，並隨機透過 445 或是 139 埠自我傳播，嘗試感染區域網路中其他設備。當時建議的應對防禦方式除了更新微軟釋出的更新檔外，就是建議透過防火牆關閉 445 埠。然而關閉 445 埠這個手段卻可能影響其他正常 Windows 共用完全停止工作，並且可能會影響其它應用程式的執行。我們觀察幾個部屬 Flowviewer 的單位後，發現在 5 月時透過 445 埠的入侵/攻擊行為有明顯的增加。這可以證明 Flowviewer 能確實抵禦該病毒主動傳播的行為。

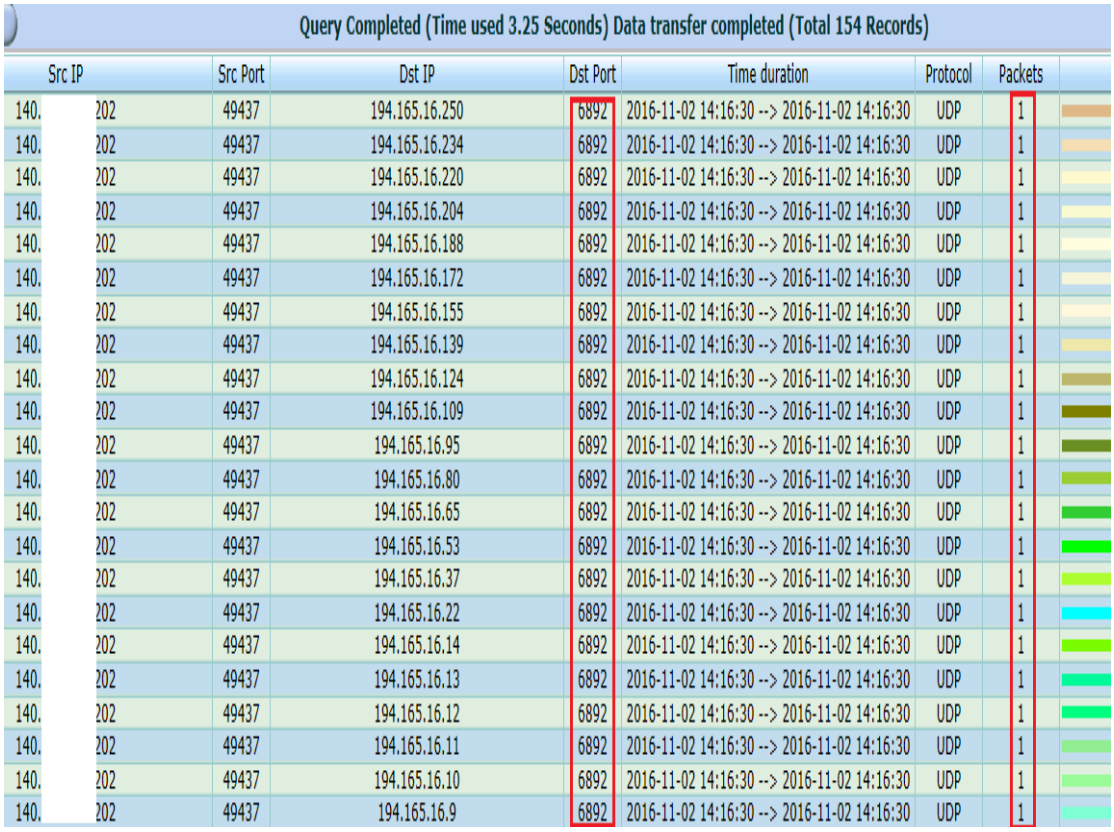
A 校		B 校	
日期	攻擊數量 / 每日	日期	攻擊數量 / 每日
2017/5/1	6	2017/5/1	69
2017/5/2	14	2017/5/2	75
2017/5/3	19	2017/5/3	82
2017/5/4	24	2017/5/4	80
2017/5/5	29	2017/5/5	84
2017/5/6	25	2017/5/6	118
2017/5/7	20	2017/5/7	60
2017/5/8	15	2017/5/8	85
2017/5/9	18	2017/5/9	61
2017/5/10	18	2017/5/10	83
2017/5/11	18	2017/5/11	75
2017/5/12	**309**	2017/5/12	**328**
2017/5/13	286	2017/5/13	278
2017/5/14	94	2017/5/14	140
5 月 12 日前每日平均攻擊數：19 個 5 月 12 日當日攻擊數：309 個		5 月 12 日前每日平均攻擊數：80 個 5 月 12 日當日攻擊數：328 個	

表一 A、B 兩單位於五月 1-14 日透過 445 埠進行入侵的 IP 數量統計

就算關閉 445 埠，WannaCry 這類的勒索軟體還是會從其他埠入侵。例：台灣嘉義縣某私立大學在 2016 年 11 月 2 日就發現有內部主機受到感染，通過 6892 埠對外進行大規模掃描的動作。圖四、五分別顯示 Flowiewer 當時偵測到的結果。由此案例可知，針對特定埠號去進行阻擋、防禦無法有效防止入侵與攻擊行為。



圖四　　11 月 2 日當日的 portscan 報表

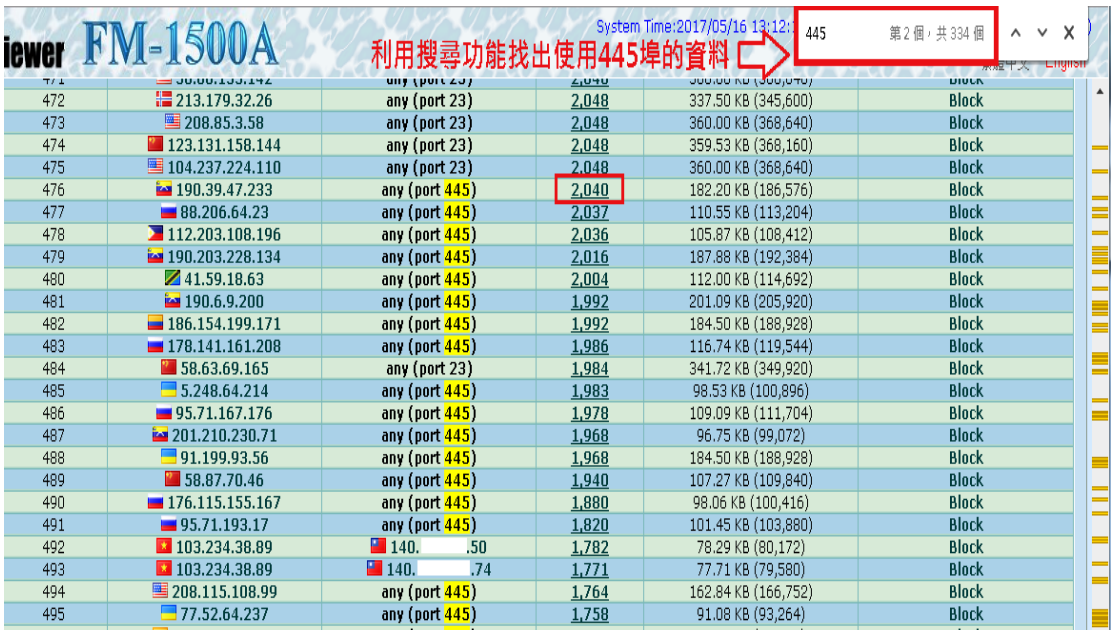


Query Completed (Time used 3.25 Seconds) Data transfer completed (Total 154 Records)

Src IP	Src Port	Dst IP	Dst Port	Time duration	Protocol	Packets
140. 202	49437	194.165.16.250	6892	2016-11-02 14:16:30 --> 2016-11-02 14:16:30	UDP	1
140. 202	49437	194.165.16.234	6892	2016-11-02 14:16:30 --> 2016-11-02 14:16:30	UDP	1
140. 202	49437	194.165.16.220	6892	2016-11-02 14:16:30 --> 2016-11-02 14:16:30	UDP	1
140. 202	49437	194.165.16.204	6892	2016-11-02 14:16:30 --> 2016-11-02 14:16:30	UDP	1
140. 202	49437	194.165.16.188	6892	2016-11-02 14:16:30 --> 2016-11-02 14:16:30	UDP	1
140. 202	49437	194.165.16.172	6892	2016-11-02 14:16:30 --> 2016-11-02 14:16:30	UDP	1
140. 202	49437	194.165.16.155	6892	2016-11-02 14:16:30 --> 2016-11-02 14:16:30	UDP	1
140. 202	49437	194.165.16.139	6892	2016-11-02 14:16:30 --> 2016-11-02 14:16:30	UDP	1
140. 202	49437	194.165.16.124	6892	2016-11-02 14:16:30 --> 2016-11-02 14:16:30	UDP	1
140. 202	49437	194.165.16.109	6892	2016-11-02 14:16:30 --> 2016-11-02 14:16:30	UDP	1
140. 202	49437	194.165.16.95	6892	2016-11-02 14:16:30 --> 2016-11-02 14:16:30	UDP	1
140. 202	49437	194.165.16.80	6892	2016-11-02 14:16:30 --> 2016-11-02 14:16:30	UDP	1
140. 202	49437	194.165.16.65	6892	2016-11-02 14:16:30 --> 2016-11-02 14:16:30	UDP	1
140. 202	49437	194.165.16.53	6892	2016-11-02 14:16:30 --> 2016-11-02 14:16:30	UDP	1
140. 202	49437	194.165.16.37	6892	2016-11-02 14:16:30 --> 2016-11-02 14:16:30	UDP	1
140. 202	49437	194.165.16.22	6892	2016-11-02 14:16:30 --> 2016-11-02 14:16:30	UDP	1
140. 202	49437	194.165.16.14	6892	2016-11-02 14:16:30 --> 2016-11-02 14:16:30	UDP	1
140. 202	49437	194.165.16.13	6892	2016-11-02 14:16:30 --> 2016-11-02 14:16:30	UDP	1
140. 202	49437	194.165.16.12	6892	2016-11-02 14:16:30 --> 2016-11-02 14:16:30	UDP	1
140. 202	49437	194.165.16.11	6892	2016-11-02 14:16:30 --> 2016-11-02 14:16:30	UDP	1
140. 202	49437	194.165.16.10	6892	2016-11-02 14:16:30 --> 2016-11-02 14:16:30	UDP	1
140. 202	49437	194.165.16.9	6892	2016-11-02 14:16:30 --> 2016-11-02 14:16:30	UDP	1

圖五　　針對受到感染設備發出入侵封包 zoom in 觀察結果

除了能夠自動偵測與阻斷入侵與攻擊，Flowviewer 也能夠提供相關報表。圖六、七分別為 B 校在 5 月 12 日當天的 portscan 報表與針對特定 IP(190.39.47.233) zoom in 的結果。



472	213.179.32.26	any (port 23)	2,048	337.50 KB (345,600)	Block
473	208.85.3.58	any (port 23)	2,048	360.00 KB (368,640)	Block
474	123.131.158.144	any (port 23)	2,048	359.53 KB (368,160)	Block
475	104.237.224.110	any (port 23)	2,048	360.00 KB (368,640)	Block
476	190.39.47.233	any (port 445)	2,040	182.20 KB (186,576)	Block
477	88.206.64.23	any (port 445)	2,037	110.55 KB (113,204)	Block
478	112.203.108.196	any (port 445)	2,036	105.87 KB (108,412)	Block
479	190.203.228.134	any (port 445)	2,016	187.88 KB (192,384)	Block
480	41.59.18.63	any (port 445)	2,004	112.00 KB (114,692)	Block
481	190.6.9.200	any (port 445)	1,992	201.09 KB (205,920)	Block
482	186.154.199.171	any (port 445)	1,992	184.50 KB (188,928)	Block
483	178.141.161.208	any (port 445)	1,986	116.74 KB (119,544)	Block
484	58.63.69.165	any (port 23)	1,984	341.72 KB (349,920)	Block
485	5.248.64.214	any (port 445)	1,983	98.53 KB (100,896)	Block
486	95.71.167.176	any (port 445)	1,978	109.09 KB (111,704)	Block
487	201.210.230.71	any (port 445)	1,968	96.75 KB (99,072)	Block
488	91.199.93.56	any (port 445)	1,968	184.50 KB (188,928)	Block
489	58.87.70.46	any (port 445)	1,940	107.27 KB (109,840)	Block
490	176.115.155.167	any (port 445)	1,880	98.06 KB (100,416)	Block
491	95.71.193.17	any (port 445)	1,820	101.45 KB (103,880)	Block
492	103.234.38.89	140. .50	1,782	78.29 KB (80,172)	Block
493	103.234.38.89	140. .74	1,771	77.71 KB (79,580)	Block
494	208.115.108.99	any (port 445)	1,764	162.84 KB (166,752)	Block
495	77.52.64.237	any (port 445)	1,758	91.08 KB (93,264)	Block

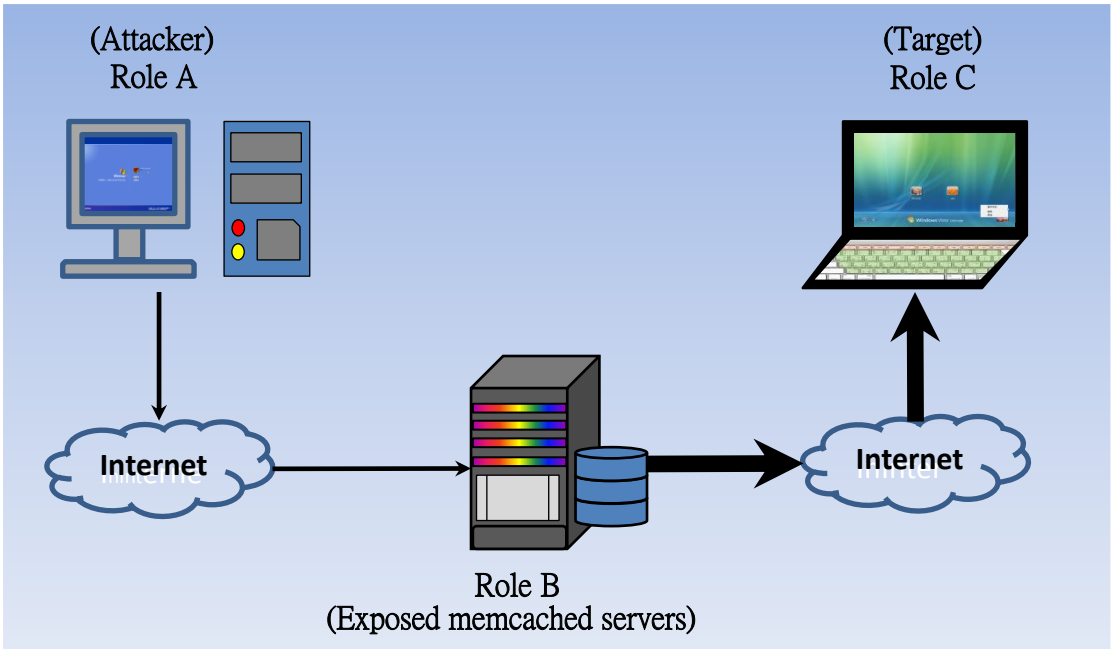
圖六　　5 月 12 日當日的 portscan 報表

No.	Src IP	Src Port	Dst IP	Dst Port	Time duration	Protocol
1	190.39.47.233	4417	140. .60	445	2017-05-11 23:55:01 --> 2017-05-11 23:55:04	TCP
2	190.39.47.233	1086	140. .61	445	2017-05-11 23:55:11 --> 2017-05-11 23:55:11	TCP
3	190.39.47.233	1457	140. .62	445	2017-05-11 23:55:13 --> 2017-05-11 23:55:16	TCP
4	190.39.47.233	1827	140. .63	445	2017-05-11 23:55:19 --> 2017-05-11 23:55:22	TCP
5	190.39.47.233	2194	140. .64	445	2017-05-11 23:55:25 --> 2017-05-11 23:55:28	TCP
6	190.39.47.233	2568	140. .65	445	2017-05-11 23:55:34 --> 2017-05-11 23:55:34	TCP
7	190.39.47.233	2943	140. .66	445	2017-05-11 23:55:38 --> 2017-05-11 23:55:41	TCP
8	190.39.47.233	3313	140. .67	445	2017-05-11 23:55:43 --> 2017-05-11 23:55:46	TCP
9	190.39.47.233	3683	140. .68	445	2017-05-11 23:55:49 --> 2017-05-11 23:55:52	TCP
10	190.39.47.233	4050	140. .69	445	2017-05-11 23:55:55 --> 2017-05-11 23:55:58	TCP
11	190.39.47.233	4422	140. .70	445	2017-05-11 23:56:01 --> 2017-05-11 23:56:04	TCP
12	190.39.47.233	2531	140. .95	445	2017-05-11 23:58:35 --> 2017-05-11 23:58:35	TCP
13	190.39.47.233	2902	140. .96	445	2017-05-11 23:58:40 --> 2017-05-11 23:58:40	TCP
14	190.39.47.233	3272	140. .97	445	2017-05-11 23:58:43 --> 2017-05-11 23:58:43	TCP
15	190.39.47.233	3642	140. .98	445	2017-05-11 23:58:53 --> 2017-05-11 23:58:53	TCP
16	190.39.47.233	4010	140. .99	445	2017-05-11 23:58:55 --> 2017-05-11 23:58:58	TCP
17	190.39.47.233	4379	140. .100	445	2017-05-11 23:59:02 --> 2017-05-11 23:59:04	TCP
18	190.39.47.233	4998	140. .101	445	2017-05-11 23:59:11 --> 2017-05-11 23:59:11	TCP
19	190.39.47.233	1399	140. .102	445	2017-05-11 23:59:17 --> 2017-05-11 23:59:17	TCP
20	190.39.47.233	1764	140. .103	445	2017-05-11 23:59:19 --> 2017-05-11 23:59:22	TCP
21	190.39.47.233	2138	140. .104	445	2017-05-11 23:59:26 --> 2017-05-11 23:59:29	TCP
22	190.39.47.233	2505	140. .105	445	2017-05-11 23:59:32 --> 2017-05-11 23:59:35	TCP
23	190.39.47.233	2878	140. .106	445	2017-05-11 23:59:38 --> 2017-05-11 23:59:40	TCP
24	190.39.47.233	3244	140. .107	445	2017-05-11 23:59:43 --> 2017-05-11 23:59:46	TCP
25	190.39.47.233	3615	140. .108	445	2017-05-11 23:59:50 --> 2017-05-11 23:59:52	TCP
26	190.39.47.233	3985	140. .109	445	2017-05-11 23:59:56 --> 2017-05-11 23:59:59	TCP
27	190.39.47.233	4353	140. .110	445	2017-05-12 00:00:01 --> 2017-05-12 00:00:04	TCP
28	190.39.47.233	4854	140. .111	445	2017-05-12 00:00:08 --> 2017-05-12 00:00:11	TCP
29	190.39.47.233	1352	140. .112	445	2017-05-12 00:00:13 --> 2017-05-12 00:00:16	TCP
30	190.39.47.233	1722	140. .113	445	2017-05-12 00:00:19 --> 2017-05-12 00:00:22	TCP
31	190.39.47.233	2095	140. .114	445	2017-05-12 00:00:26 --> 2017-05-12 00:00:29	TCP
32	190.39.47.233	2466	140. .115	445	2017-05-12 00:00:32 --> 2017-05-12 00:00:35	TCP
33	190.39.47.233	2631	140. .122	445	2017-05-12 00:00:34 --> 2017-05-12 00:00:37	TCP

圖七　　針對特定 IP(190.39.47.233) zoom in 觀察結果

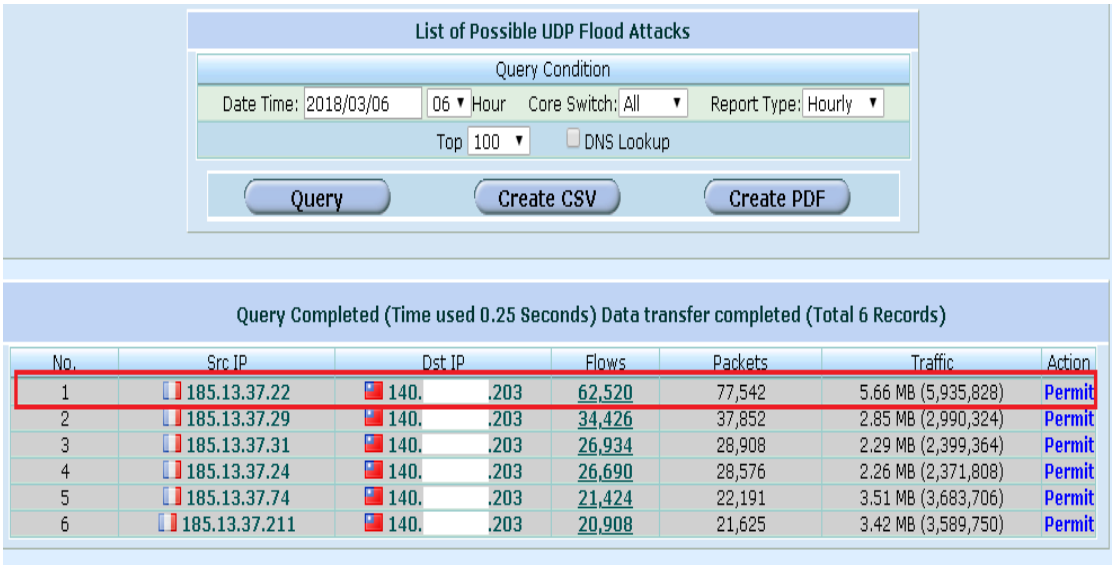
案例二：記憶體快取 DDoS 放大攻擊

2018 年 2 月時，某安全機構發現有透過 UDP 協定之 11211 埠產生記憶體快取 DDoS 放大攻擊（Memcached amplification attack），據指出其放大倍數高達 50000 倍以上，受害者包含開源碼（open-source）社群 GitHub 等多處，而當時湧入 GitHub 的流量最大值高達 1.35 Tbps，這也是自從 2016 之後看到最大的攻擊。在面對此種類型的攻擊，使用流量清洗之類防禦手段並無法阻止實體物理頻寬擁塞的問題，因此必須在網路架構的上一層（上游 ISP 或是區網中心）設備進行阻斷，方得有效控制。這個論點我們在 2017 年 9 月已於國外資訊安全雜誌：SECURITY 發表過相關廣告說明。這樣的處理方式是相當正確的，但如果能在持續放大攻擊前阻斷那就更好了。如下圖所示，角色 A 為發起攻擊的攻擊方，角色 B 為放大攻擊的角色，角色 C 為受害者。那麼有可能找到一個解決方案在 A、B 之間阻擋這樣惡意的流量嗎？答案是肯定的，在我們觀察部屬在某單位的 Flowviewer 之後，發現我們的演算法依舊適用於偵測尚未被放大的異常流量。透過 Flowviewer 的報表，也可以得知在五分鐘之內，其流量並不會迅速成長到 50000 倍以上。



圖八　　記憶體快取 DDoS 放大攻擊簡單示意圖

如圖九所示，從報表上可以看到 Flowviewer 可以偵測並阻擋這些惡意流量。此外，還可以藉由點擊連線數（Flows）來觀察相關詳細資料，如圖十。從該報表可以明顯看到該攻擊在 IP 行為上是有明顯規律性的。



圖九 記憶體快取 DDoS 放大攻擊會透過發送大量包含小傳輸量的封包

Go Back Query Completed (Time used 1.75 Seconds) Data transfer completed (Total 62520 Records)

No.	Src IP	Src Port	Dst IP	Dst Port	Time duration	Protocol	Packets	Traffic
1	185.13.37.22	58510	140. .203	11211	2018-03-06 06:37:01 --> 2018-03-06 06:37:02	UDP	1	166 Bytes
2	185.13.37.22	47773	140. .203	11211	2018-03-06 06:37:01 --> 2018-03-06 06:37:02	UDP	1	166 Bytes
3	185.13.37.22	27506	140. .203	11211	2018-03-06 06:37:01 --> 2018-03-06 06:37:02	UDP	1	166 Bytes
4	185.13.37.22	50669	140. .203	11211	2018-03-06 06:37:01 --> 2018-03-06 06:37:02	UDP	1	166 Bytes
5	185.13.37.22	33926	140. .203	11211	2018-03-06 06:37:01 --> 2018-03-06 06:37:02	UDP	1	166 Bytes

圖十　　zoom in 後可觀察到其規律性

結論

綜觀以上所述，可總結 Flowviewer 的優點包含：

1. 可依據網路環境彈性配置設備：設備提供四種模式給網路管理者選擇，管理者可以網路環境實際需求來配置設備。設備介面採人性化、直覺操作，可在短時間內熟悉系統操作。

2. 可與其他網路設備做配合，有效提升網路安全：偵測到惡意流量時，可依網路管理者選擇自動在本機進行阻斷或是利用 ACL 在核心交換器阻斷。

3. 利用分析 IP 行為辨別惡意流量：透過收集五分鐘內的流量資料，針對各 IP 去分析其流量的來源位址、目的位址、來源埠號、目的埠號、傳輸量、封包數、時間、傳輸協定等欄位，並利用本公司獨立開發之演算法判別，可針對 IP 行為辨別惡意流量。利用此方式可精準判別攻擊與入侵，也不須額外購買新的特徵碼。

4. 可提供詳細流量資料報表作為犯罪追查之證據：提供多樣化報表（包含流量與各類型攻擊/入侵報表）可供查詢，並提供動態查詢功能供管理者能快速檢索特定條件的流量資料。