Curelan Data Sheet

Flowviewer 網路流量分析系統

主功能：防止駭客入侵及防止駭客攻擊

Flowviewer FM-1500A / FM-800A Configuration：Inline Mode

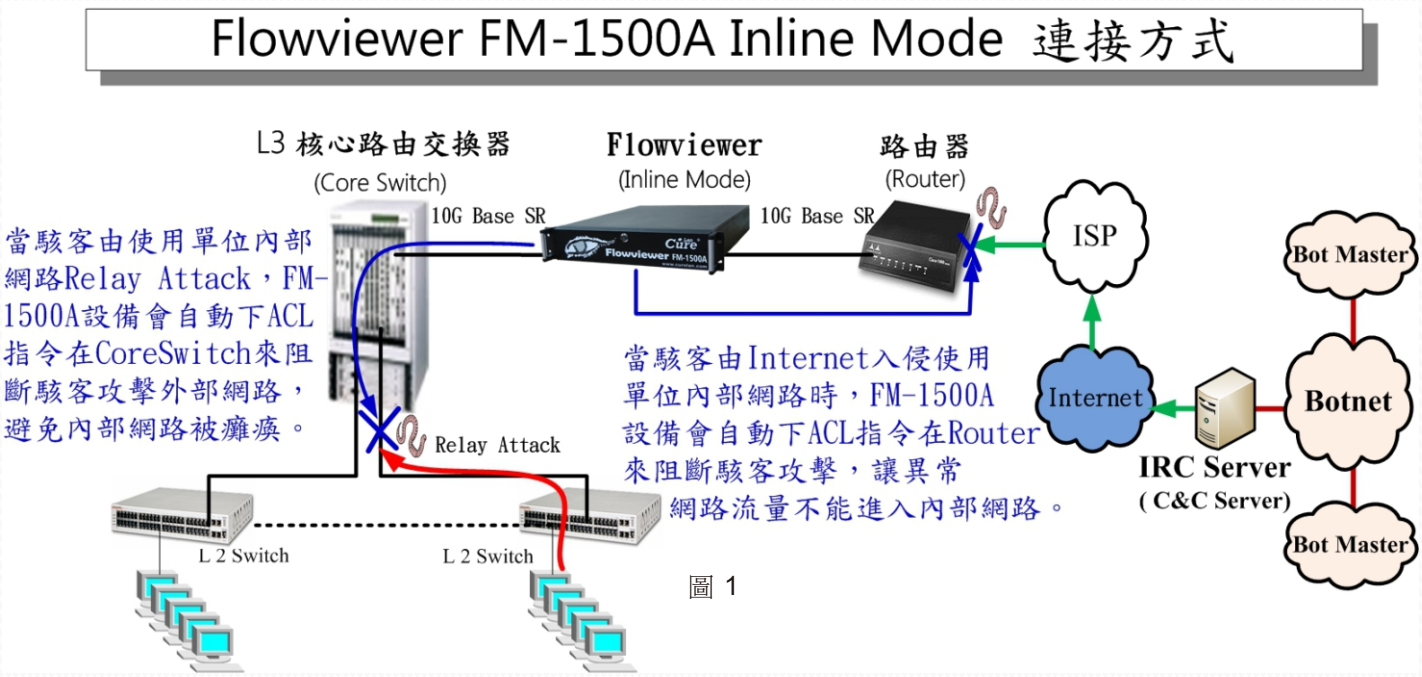

圖 1

＊FM-800A 1G 方案；FM-1500A 10 G 方案

圖 2

P.S. Flowviewer 有 2 種方式可以自動阻擋駭客攻擊

1.Flowveiwer 設備本身可以自動阻擋駭客攻擊

2.Flowviewer 可以自動在L3核心路由器下ACL指令來阻擋駭客的攻擊

駭客在檔案伺服器中竊取機密資料，FM-1500A/800A 有方案：

沒有任一個網路防護產品可以阻擋所有駭客的入侵並植入木馬程式，例如，木馬程式依附在P2P、APP及網路釣魚程式中是所有防護設備偵測不到的，這些方式是無解。幸運的是，伺服器並不會自動地收發信件或使用 P2P、APP 下載任何檔案；因此上述的駭客入侵行為都僅限於個人電腦。例如；網路新聞曾經報導東歐駭客集團曾經透過 Facebook 員工下載APP軟體並成功植入木馬程式來竊取 Facebook 的使用者資料，我們來分析這個事件，被駭客植入木馬程式的 Facebook 員工的電腦並沒有 Facebook 使用者的資料，這些使用者的資料一定是放置在 Database 伺服器，而駭客如何竊取這些資料呢？ 方案很簡單，駭客會再透過內部網路的入侵方式來竊取使用者資料，也就是內對內入侵，而市場上防護駭客入侵設備都放置在 Inline Mode 自然偵測不到駭客內對內入侵。Flowviewer 設備雖然放置在 Inline Mode 但是 Flowviewer 設備可以同時接收Netflow 或 Sflow，並且是接收 1：1 抽樣資料來偵測駭客的內對內入侵。大多的駭客入侵電腦後都是使用內對內入侵，直到他們找出伺服器 Ip來竊取機密文件。

大部份的內對內入侵都是透過 RDP 來執行，而 RDP 密碼猜測入侵攻擊的偵測功能正是 FM-1500A/FM-800A 的獨家功能。而 FM-1500A/FM-800A 可以偵測到並可以自動下ACLs指令給 Layer3 核心路由器來防止內對內入侵。如下圖所示：遭受到RDP攻擊的報告中指出第 3，5，6 及第 7 個 IP 正遭受內對內入侵。一般內部網路電腦使用(IP)不可能同時間對 10 台電腦連線，或許你會說網路管理者有可能發生這個現象，沒有錯，有可能發生，但是 Flowviewer 設備不是偵測到一個 IP 對多台電腦連線就判定是非法入侵，非法入侵一定是要猜測對方的密碼，合法登入不需要猜測對方的密碼。

圖 3　　我們可以看到紅色框線中，有一個內部的來源IP在同一時間中入侵其它的 10 個內部IP。

駭客的入侵方式：駭客會使用入侵程式在Internet進行；對任何使用單位入侵，也就是外對內入侵

- Port Scanning 通訊埠掃描
- SSH 密碼猜測入侵攻擊
- RDP 密碼猜測入侵攻擊
- P2P、APP、網路釣魚程式(Spear phishing)、Microsoft、PHP 及 C++ 等有未知的安全漏洞，而這個方式只有老練的駭客會找到。然而，這是無法可解的，除非業者自行找出這漏洞並修正這個問題。駭客透過這些管道入侵到使用單位的個人電腦，一定再會透過內對內入侵找到伺服器才能竊取機密文

解決方式：Flowveiwer FM-1500A/FM-800A 提供 Port Scan、SSH 及 RDP 偵測並可以自動阻擋功能。

IPS (Intrusion Prevention System) 的盲點

IPS防止駭客入侵方式是使用 Signature 技術，也就是使用 Pattern (特徵碼)方式來分析比對並過濾所經過此設備的網路封包(packet)，所以此設備需要定期更新 Pattern(特徵碼)。

IPS防止駭客攻擊(DDoS)方式是使用門檻設定功能(threshold)技術，就是設定每一個IP，每秒累積封包(Packet)的次數，也就是數(count)每一個IP所累積的session，例；udp_src_session、udp_dst_session等，此功能容易把正常封包(Packet)誤判為異常(anomaly)封包(Packet)，因為語音(Voice)、多媒體(Media Stream)、DNS(Domain Name System)、NTP(Network Time Protocol)等都是使用UDP封包(Packet)。

Flowveiwer FM-1500A/FM-800A 主要技術

Flowviewer 設備採用自行開發的數學演算法，可以快速收集 NetFlow 或 Sflow 並且加以歸類及分析每一筆IP，來判斷異常(anomaly) 封包(Packet)。很多廠商都朝這方面來開發產品成效都很差，主要是都採用資料庫的架構來收集 IP，例： MySQL、Oracle 等資料庫，這些資料庫是很好產品但是用不對方向，因為收集網路(Network) 的 IP 資料可能在 1 小時就有十幾億筆 IP 資料，所以效能都不佳。接收 NetFlow 或 Sflow 來收集 IP 並判斷網路異常，並不是我們發現，這在 IEEE 論文有很多人都有發表，只是我們開發出數學演算法，可以很快速在同一時間將相同來源及目的 IP 歸納整理在一起，所以我們稱此種方式是 IP NBAD (Network Behavior Anomaly Detection)，因為 Flowviewer 設備是收集IP來分析駭客入侵及攻擊所以不需要更新 Pattern(特徵碼)，也不是採用門檻設定功能(threshold) 技術來偵測 DDoS 攻擊，不會有常常有誤判情況造成使用單位困擾。Flowviewer 設備是採用收集 IP 技術不須要分析網路封包來判斷 DDoS 的種類，例；TCP SYN ACK flood、TCP FIN、TCP REST、TCP Fragment 等等。

Flowviewer 設備採用收集IP技術說明，設備是接收 NetFlow 或 Sflow 內容包括， Source IP address、Destination IP address、Time duration、Transport protocol port number、 protocol、Flow (Session)、Packets 及 Traffic by each IP address。

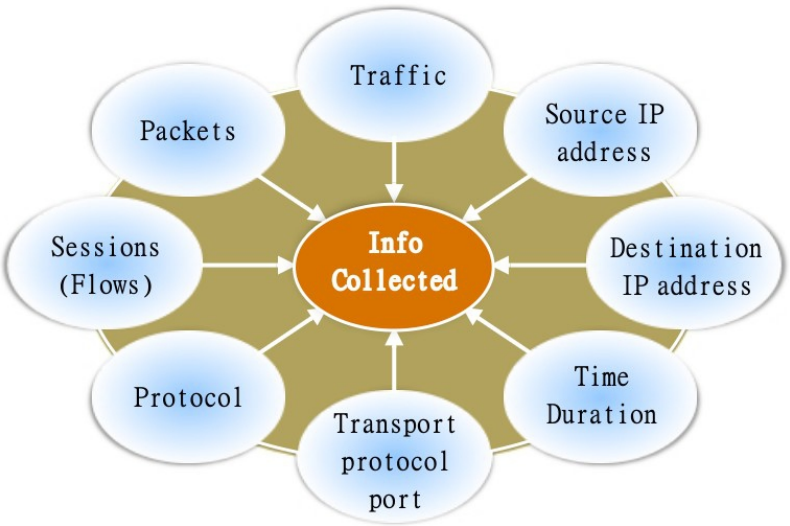

圖 4

IEEE有這方面的文章發表

FM-800A／FM-1500A ➡ NBA(Network Behavior Analysis) 進化 ➡ IP NBAD(Network Behavior Anomaly Detection) ➡ 收集每IP來分析網路(Network)異常(anomaly)封包(Packet) 。

解決方式: Flowveiwer FM-1500A/FM-800A提供防止駭客攻擊功能(DDOS)：UDP Flood Attacks、DOS Attacks、DNS Attacks、NTP Attacks等偵測功能並可以自動阻擋功能。

駭客攻擊癱瘓方式

1. The Amount of Traffic (大量網路流量攻擊)：

駭客會使用巨大異常網路流量來佔據網路頻寬導致正常網路流量受到擠壓而導致網路癱瘓。

2. A Number of Sessions(大量網路Sessions攻擊)：

駭客會使用巨大網路 Sessions，所經過網路設備都會產生設備的 CPU 損耗過高導致癱瘓網路。

以實際例子來說明駭客攻擊方式

UDP Flood Attack

真實案例，UDP通訊協定是沒有連線數(Sessions) 觀念(TCP才有連線數觀念)。但是，駭客運用”跳Port Number”的觀念來產生連線數(Sessions)，如下圖，駭客假借 140.xxx.xxx.197 來攻擊對外 IP，產生 40.72 GB 網路流量及2,390,917 Flows (Sessions)，被假借(Relay) 的使用單位一樣被癱瘓內部網路，但是，有 Flowviewer 設備會自動偵測攻擊 IP 並阻斷，避免網路癱瘓。

圖 5

我們 zoom In (點入) 2,390,917 Flows(Sessions)來看內容細節，如圖示：Source Port 相隔每一個 Port 都不一樣，同樣 Destination Port 相隔每一個 Port 也都不一樣，駭客就是使用跳 Port Number 的觀念來產生連線數(Sessions)，駭客也可以固定 Source Port 是123 Port Number 而Destination Port 相隔每一個 Port 都不一樣也可以是一樣(如果攻擊是 80 Port 當場是一樣)，這就是 NTP Attack，以此推論 DNS Attack。

No.	Src IP	Src Port	Dst IP	Dst Port	Time duration	Protocol	Packets	
1	140 197	4825	188.40.129.201	11268	2014-05-27 04:54:57 --> 2014-05-27 04:54:57	UDP	1	1.46 KB (1,500)
2	140 197	4796	188.40.129.201	18142	2014-05-27 04:54:57 --> 2014-05-27 04:54:57	UDP	1	1.46 KB (1,500)
3	140 197	4799	188.40.129.201	30463	2014-05-27 04:54:57 --> 2014-05-27 04:54:57	UDP	1	1.46 KB (1,500)
4	140 197	4829	188.40.129.201	13292	2014-05-27 04:54:57 --> 2014-05-27 04:54:57	UDP	1	1.46 KB (1,500)
5	140 197	4851	188.40.129.201	24937	2014-05-27 04:54:57 --> 2014-05-27 04:54:57	UDP	1	1.46 KB (1,500)
6	140 197	4850	188.40.129.201	28953	2014-05-27 04:54:57 --> 2014-05-27 04:54:57	UDP	1	1.46 KB (1,500)
7	140 197	4841	188.40.129.201	1972	2014-05-27 04:54:57 --> 2014-05-27 04:54:57	UDP	1	1.46 KB (1,500)
8	140 197	4859	188.40.129.201	1974	2014-05-27 04:54:57 --> 2014-05-27 04:54:57	UDP	1	1.46 KB (1,500)
9	140 197	4867	188.40.129.201	18933	2014-05-27 04:54:57 --> 2014-05-27 04:54:57	UDP	1	1.46 KB (1,500)
10	140 197	4860	188.40.129.201	30567	2014-05-27 04:54:57 --> 2014-05-27 04:54:57	UDP	1	1.46 KB (1,500)
11	140 197	4870	188.40.129.201	32532	2014-05-27 04:54:57 --> 2014-05-27 04:54:57	UDP	1	1.46 KB (1,500)
12	140 197	4872	188.40.129.201	17361	2014-05-27 04:54:57 --> 2014-05-27 04:54:57	UDP	1	1.46 KB (1,500)
13	140 197	4854	188.40.129.201	8048	2014-05-27 04:54:57 --> 2014-05-27 04:54:57	UDP	1	1.46 KB (1,500)
14	140 197	4865	188.40.129.201	13940	2014-05-27 04:54:57 --> 2014-05-27 04:54:57	UDP	1	1.46 KB (1,500)
15	140 197	4862	188.40.129.201	6477	2014-05-27 04:54:57 --> 2014-05-27 04:54:57	UDP	1	1.46 KB (1,500)
16	140 197	4853	188.40.129.201	9064	2014-05-27 04:54:57 --> 2014-05-27 04:54:57	UDP	1	1.46 KB (1,500)
17	140 197	4846	188.40.129.201	2871	2014-05-27 04:54:57 --> 2014-05-27 04:54:57	UDP	1	1.46 KB (1,500)
18	140 197	4844	188.40.129.201	17302	2014-05-27 04:54:57 --> 2014-05-27 04:54:57	UDP	1	1.46 KB (1,500)
19	140 197	4848	188.40.129.201	28459	2014-05-27 04:54:57 --> 2014-05-27 04:54:57	UDP	1	1.46 KB (1,500)
20	140 197	4858	188.40.129.201	15264	2014-05-27 04:54:57 --> 2014-05-27 04:54:57	UDP	1	1.46 KB (1,500)
21	140 197	4863	188.40.129.201	12329	2014-05-27 04:54:57 --> 2014-05-27 04:54:57	UDP	1	1.46 KB (1,500)
22	140 197	4864	188.40.129.201	26468	2014-05-27 04:54:57 --> 2014-05-27 04:54:57	UDP	1	1.46 KB (1,500)
23	140 197	4877	188.40.129.201	10963	2014-05-27 04:54:57 --> 2014-05-27 04:54:57	UDP	1	1.46 KB (1,500)
24	140 197	4875	188.40.129.201	1759	2014-05-27 04:54:57 --> 2014-05-27 04:54:57	UDP	1	1.46 KB (1,500)
25	140 197	4886	188.40.129.201	10891	2014-05-27 04:54:57 --> 2014-05-27 04:54:57	UDP	1	1.46 KB (1,500)
26	140 197	4878	188.40.129.201	6895	2014-05-27 04:54:57 --> 2014-05-27 04:54:57	UDP	1	1.46 KB (1,500)
27	140 197	4887	188.40.129.201	3486	2014-05-27 04:54:57 --> 2014-05-27 04:54:57	UDP	1	1.46 KB (1,500)
28	140 197	4889	188.40.129.201	9236	2014-05-27 04:54:57 --> 2014-05-27 04:54:57	UDP	1	1.46 KB (1,500)
29	140 197	1260	188.40.129.201	24567	2014-05-27 04:54:17 --> 2014-05-27 04:54:57	UDP	2	2.93 KB (3,000)
30	140 197	4894	188.40.129.201	19868	2014-05-27 04:54:57 --> 2014-05-27 04:54:57	UDP	1	1.46 KB (1,500)

圖 6

DOS Attack

真實案例，如圖所示，140.XXX.XXX.174 是使用 DOS 來攻擊 113.107.174.140。產生 105.44GB 網路流量及 53,706,960 Flows(Sessions)。

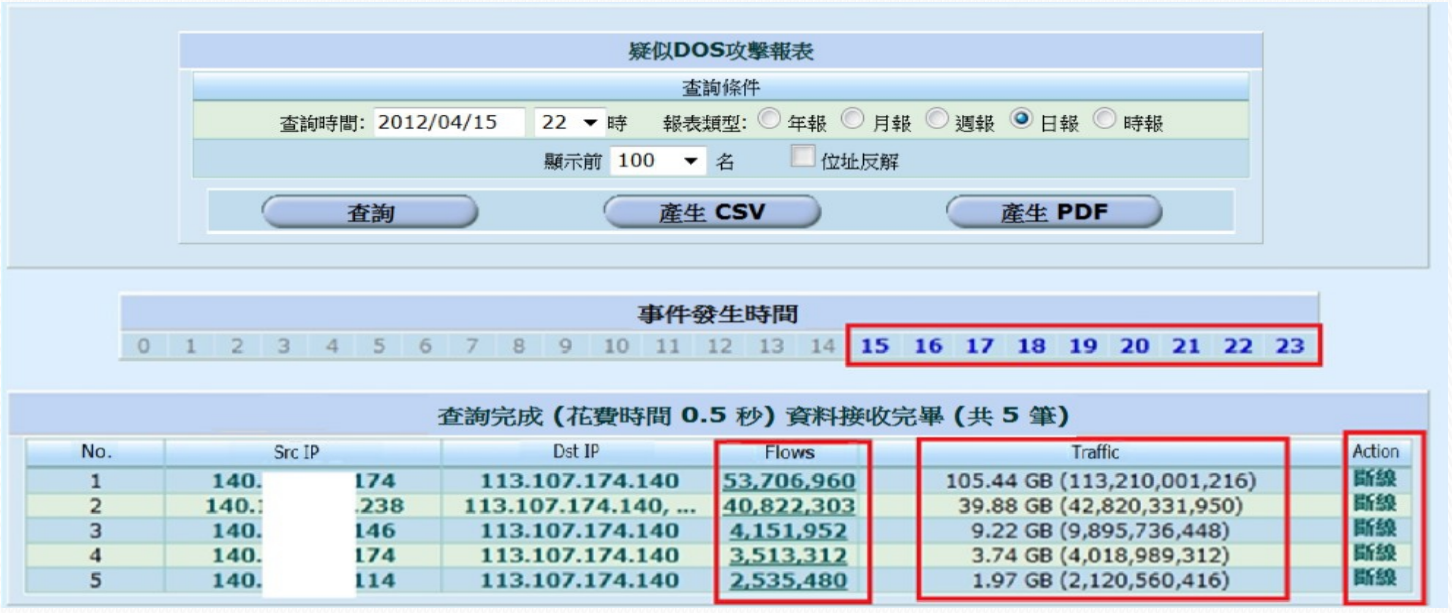

圖 7

NTP reflection Attacks

真實案例，如圖所示，駭客藉由連接埠 123 來放置 140.XXX.XXX.2 來攻擊 192.99.18.64; 這就是 NTP 反射攻擊。

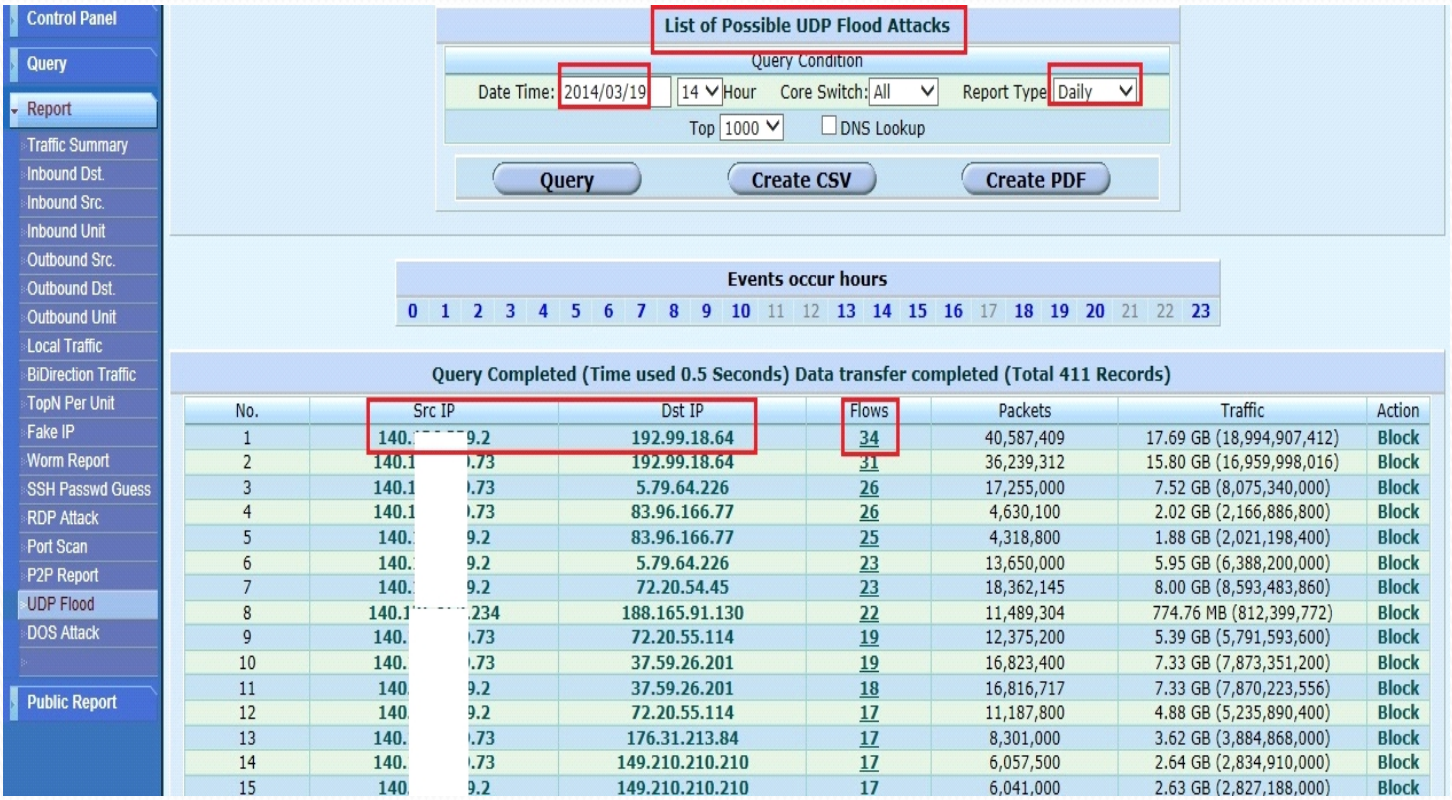

圖 8

我們 zoom In(點入) 34 Flows(Sessions) 來看內容細節，如圖示，Source Port 是123 Port Number 而 Destination Port 是 80 Port，這就是駭客借 NTP Attacks 來攻擊外部網站。

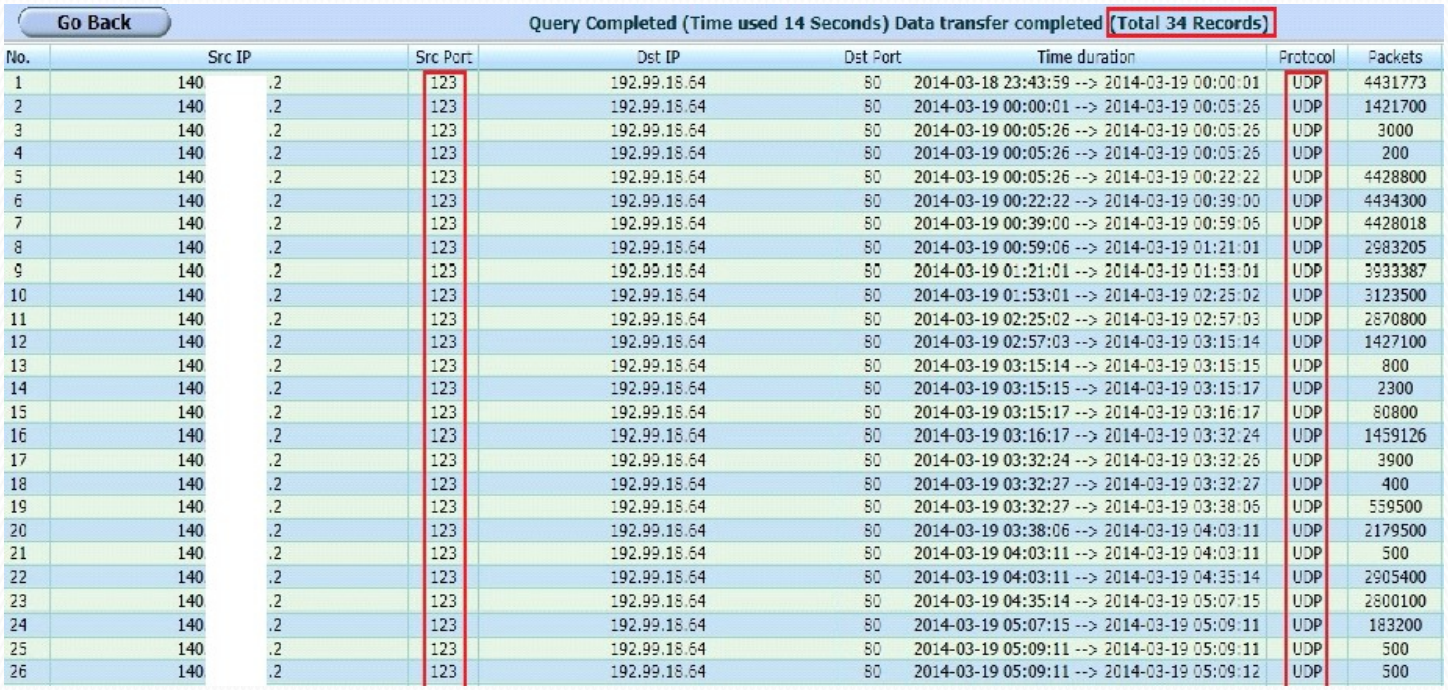

圖 9

產品主要功能(FM-1500A/800A)

- 本設備可於網路中任一節點，同時具備接收 sFlow 及 Netflow 之功能。
- 設備系統提供中文化整合性Web使用者介面，管理者可遠端以瀏覽器進入管理畫面管理所有功能，且提供管理者帳號、密碼之設定功能。
- 系統設備可同時對 L3 Switch 下 ACL 指令，最多 10 台 L3 Switch 來阻斷被攻擊之IP。需搭配適用 Layer 3 之網路設備(Cisco, Foundry, Alcatel, Extreme)。
- 提供異常流量分佈圖，顯示每個小時裡有發生哪些網路攻擊行為，有發生攻擊行為事件時會以顏色做區分顯示，亦可直接點選發生的時間點後自動導入報表做詳細的查詢，方便網路管理者做管理，不須再一一到各個攻擊報表作查詢。
- 提供阻斷鎖定被蠕蟲攻擊之IP功能並可設定所需阻斷之時間，且提供Mail通知管理者之機制，並提供白名單即發生蠕蟲攻擊時不想被阻斷之IP。
- 提供偵測 Port Scan 埠掃描之功能(NBAD)，提供可本機或下ACL到Core Switch自動阻斷攻擊來源IP並可設定所需阻斷之時間。
- 提供偵測SSH(Secure Shell) 及 RDP(Remote Desktop Protocol) 密碼猜測攻擊之功能(NBAD)，提供可本機或下ACL到Core Switch自動阻斷攻擊來源IP並可設定所需阻斷之時間。
- 提供偵測 DOS(Denial of Service) Attack、UDP Flood、DNS(Domain Naming System) Attack、NTP (Network Time Protocol) Attack攻擊偵測功能 (NBAD)，可設定之阻斷模式：阻斷攻擊來源為內部 IP、阻斷攻擊來源為外部 IP、內外部IP同時阻斷等三種模式。
- 提供動態查詢分析可任自行定義時間區段(年、月、日、時、分) 間來查詢歷史犯罪記錄，並提供連線數點選進入顯示詳細資料。
- 提供即時流量報表及網路流量控制功能可分別針對 IPv4 和 IPv6 協定。

產品標準功能比較表

Flowviewer Type	FM-800A	FM-1500A
Quota Management function and current traffic monitor	Yes	Yes
Netflow or sFlow traffic report	Yes	Yes
Worm Detection(NBAD)	Yes	Yes
Automatic block infected Ips from L3 Switch by ACL	Yes	Yes
SSH Password Guess Attacks Report	Yes	Yes
RDP Attack Report	Yes	Yes
Automatic block SSH Password Guess Attacks	Yes	Yes
Automatic block RDP Attacks	Yes	Yes
UDP Flood Attack Detection and DOS Attack Report	Yes	Yes
Automatic block UDP Flood Attack and DOS Attack Detection	Yes	Yes
Public Report(Hyperlinks)	Yes	Yes
DNS Attack Report	Yes	Yes
NTP Attack Report	Yes	Yes
Report of the statistical attack source	Yes	Yes

系統規格

Flowviewer 設備：所有型號均使用相同的2U機架高度。

功能	描述
物理尺寸	Chassis: 2U rack height Height: 3.45 inches (8.67 cm) Width: 17.4 inches (43.53 cm) Depth: 24 inches (61 cm) Weight: 41 lbs. (18.5 kg)
環境	Temperature, operating: 50º to 95ºF (10º to 35ºC) Temperature, non-operating: -40º to 158ºF (-40º to 70ºC) Humidity, non-operating: 95% Operating humidity: 5-85% Non-condensing at temperatures: 73º to 104ºF (23º to 40ºC)
操作系統	Embedded Linux operating system
管理方式	Web UI, role-based management
管理介面	1 x 10/100/1000 Base TX
網路架構 (Availability)	Inline mode
平均故障時間 (MTBF)	5 years
法規依從	Complies with RoHS Directive 2002/95/EC
網路使用介面	Supports language: English, Traditional Chinese
網路通量	Up to 1Gbps (FM-800A) ； Up to 10Gbps (FM-1500A)
受保護端點數	Unlimited
延遲時間	Less than 85 microseconds
報表	Real-time and historic traffic reporting; SSH password guess attacks reporting; RDP attack reporting; UDP flood attacks reporting; DOS attacks reporting; Worm attacks reporting; Port scan reporting; DNS attacks reporting; NTP attacks reporting
模式	Inline, Receive Netflow; Inline, Generate Netflow itself; Listen, Receive Netflow; Listen, Generate Netflow itself
即時更新	We do NOT use Signature database so we do not need to update it.
通知	E-mail

	FM-800A	FM-1500A
記憶體	16 GB	32GB
硬碟	• 1 x 60 GB SSD drives • 2 x 3 TB STAT drives in RAID 1	• 1 x 60 GB SSD drives • 2 x 3 TB STAT drives in RAID 1
電源供應器	• 1 x AC power supplies; 520W max continuous output	• 1 x AC power supplies; 520W max continuous output
網路卡介面	• 2 x 10/100/1000 Base TX • 2 x Gigabit Ethernet 1000BASE：SX, 850 nm	• 2 x 10/100/1000 Base TX • 2 x Gigabit Ethernet 1000BASE：SX, 850 nm • 2 x 10 Gigabit Ethernet：SR Fiber
網路 Bypass	• Integrated hardware bypass • Internal “software” bypass to pass traffic without inspection	• Integrated hardware bypass • Internal “software” bypass to pass traffic without inspection

CureLan Technology Co., Ltd 治科資訊股份有限公司

地址：高雄市三民區九如二路255號15樓之一

電話：07-311-5186

傳真：07-311-5178

www.curelan.com