中華民國第 53 屆中小學科學展覽會

作品說明書

高職組　電子、電機及資訊科

最佳團隊合作獎

091001

資安小尖兵

―網路超量連線預警偵測分析及探討

學校名稱：新北市立鶯歌高級工商職業學校

作者：	指導老師：
職二 徐銘峰	曾盛如
職二 謝靜篠	王振鴻
職二 李宛昀	

關鍵詞：超量連線、殭屍網路、入侵偵測

作品名稱

資安小尖兵－網路超量連線預警偵測分析及探討

摘要

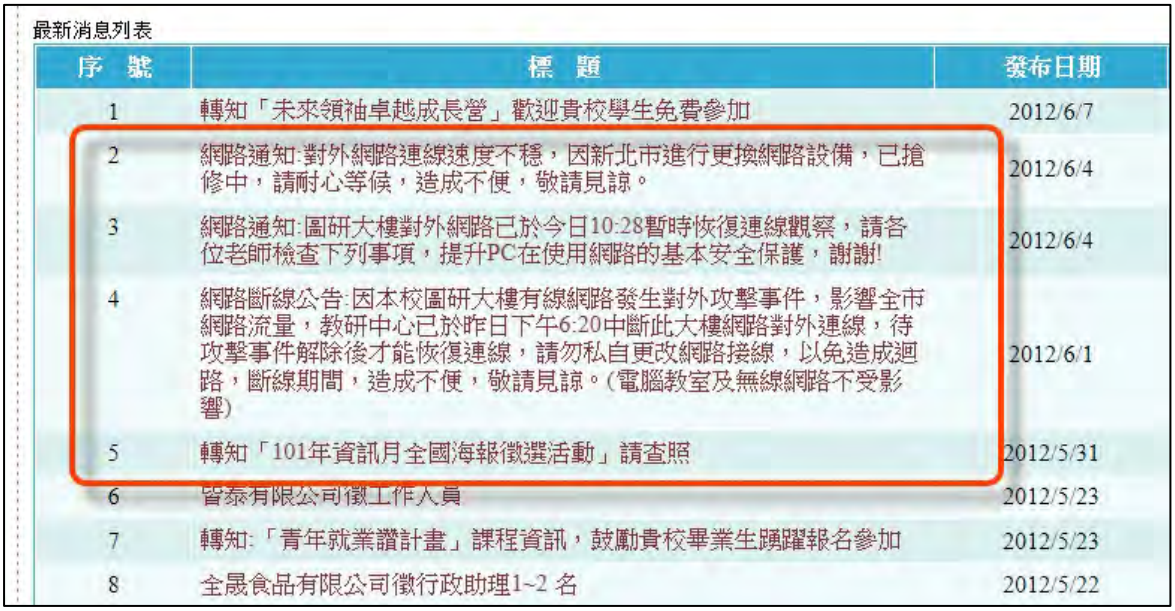
將**電腦網路**連線服務先分為不當入侵、一般需留意的服務，以防火牆篩選連線紀錄匯入資料庫，再進行統計、分析。對於外部**不當入侵**可立即放入警報項目，而內部**對等式網路**(P2P)或**電腦蠕蟲/殭屍網路**(Computer Worm/Botnet)若超過設定的上限值才列入警報項目，區域內電腦則以**警報觀察平面圖**立即觀測遭攻擊或故障電腦位置。

圖 1 - 網路超量連線預警偵測運作圖

網路管理時可利用警報資訊即時採取措施，對於超量網路連線異常可提早發現，達到**資安預警**，未知的網路異常在經過新的防火牆紀錄設定後，可快速加入統計，提升防制時效。

壹、研究動機

校園網路在運作時經常因為個人電腦的異常運作而影響整體網路的效能，因此如何即時找出異常運作的個人電腦對於網路管理有迫切的需求。在新北市教育網路曾經發生因為本校的網路異常對外攻擊，因而影響全市網路流量的例子（2012/5/31），本校圖研大樓也因此中斷連線 5 日，如下圖：



最新消息列表

序　號	標　題	發布日期
1	轉知「未來領袖卓越成長營」歡迎貴校學生免費參加	2012/6/7
2	網路通知:對外網路連線速度不穩，因新北市進行更換網路設備，已搶修中，請耐心等候，造成不便，敬請見諒。	2012/6/4
3	網路通知:圖研大樓對外網路已於今日10:28暫時恢復連線觀察，請各位老師檢查下列事項，提升PC在使用網路的基本安全保護，謝謝!	2012/6/4
4	網路斷線公告:因本校圖研大樓有線網路發生對外攻擊事件，影響全市網路流量，教研中心已於昨日下午6:20中斷此大樓網路對外連線，待攻擊事件解除後才能恢復連線，請勿私自更改網路接線，以免造成迴路，斷線期間，造成不便，敬請見諒。(電腦教室及無線網路不受影響)	2012/6/1
5	轉知「101年資訊月全國海報徵選活動」請查照	2012/5/31
6	皆泰有限公司徵工作人員	2012/5/23
7	轉知:「青年就業讚計畫」課程資訊，鼓勵貴校畢業生踴躍報名參加	2012/5/23
8	全晟食品有限公司徵行政助理1~2 名	2012/5/22

圖 2-本校圖研大樓造成新北市網路流量影響以致中斷連線

在教育經費日益拮据之下，資安分析設備通常價格不斐，後續定期韌體更新的服務收費驚人，並非一般學校所負擔得起，本次研究希望能以一般個人電腦建立資安偵測機制，加上客製化資訊建立(異常 IP 電腦位置)，可立即發揮協助校園內的網路管理功能，未來面對網路管理不再因即時資訊不足而束手無策。

貳、研究目的

因為想要做出自已的作品，所以這次實驗程式除了採用之 OS、PHP 為 Freeware 及部分小圖案（國旗、按鈕圖）取自網路，其它程式設計都以原創為目標，因此決定不參考其它程式或截取他人片段程式，採自行編寫全部程式，希望能將心中的構想實現，預定達成以下目的：

一、 網路防火牆建置與紀錄分析。

二、 網路各種傳輸模式探討。

三、 常見網路異常大量連線探討。

四、 資安偵測網路大量異常分析平台建立。

五、 資安偵測網路大量異常實驗成果。

六、 資安偵測預警所提升網路管理之成效分析比較。

參、研究設備及器材

一、 硬體設備

本次研究主題為網路超量封包紀錄之探討，是由伺服器分析後，所得到的資訊再由個人電腦瀏覽結果，因此所需的相關硬體如下：

硬體設備表			
項次	**設備或器材名稱**	**數量**	**規格**
1	中階伺服器	1	分析伺服器
2	低階伺服器	1	Pf 防火牆，資料庫
3	個人電腦	3	瀏覽、資料編寫
4	伺服器網路卡	2	橋接網路
5	Cat6 網路線	2	線路連接

表 1-硬體設備表

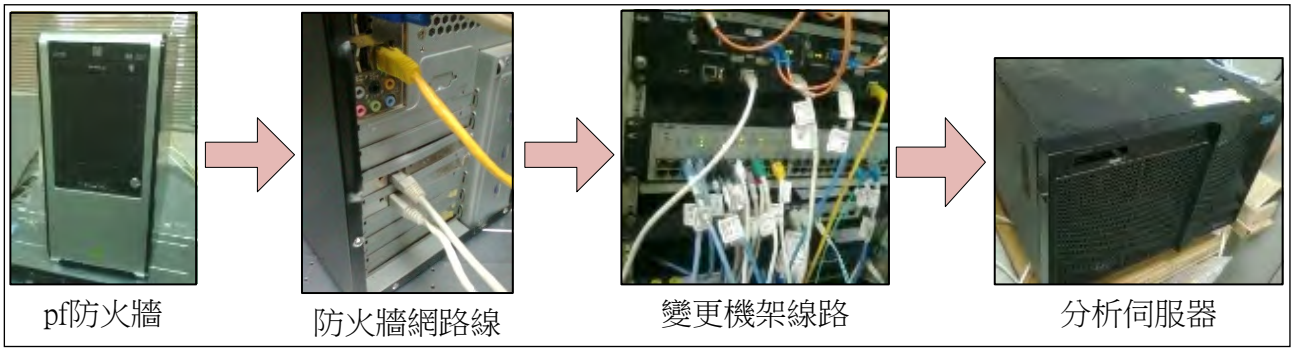


圖 3-硬體線路接線圖

二、 相關軟體

分析實驗主要是由 PHP 網頁程式來製作，所需**系統軟體**和**應用軟體**如下：

相關軟體表			
項次	**軟體名稱**	**數量**	**規格用途**
1	FreeBSD	2	Pf 防火牆
2	Windows7	2	個人電腦 OS
3	Ulead Photo Impact X3	2	影像處理
4	Adobe Dreamweaver CS6	2	PHP 網頁設計
5	Apache+PHP+MySQL	2	資料分析
6	Microsoft Visio 2010	2	圖形繪製
7	Microsoft Word 2010	2	文件製作
8	Microsoft Security Essentials	2	異常檢核
9	Wireshark	1	異常檢核驗證

表 2-相關軟體表

三、 分析實驗架構圖

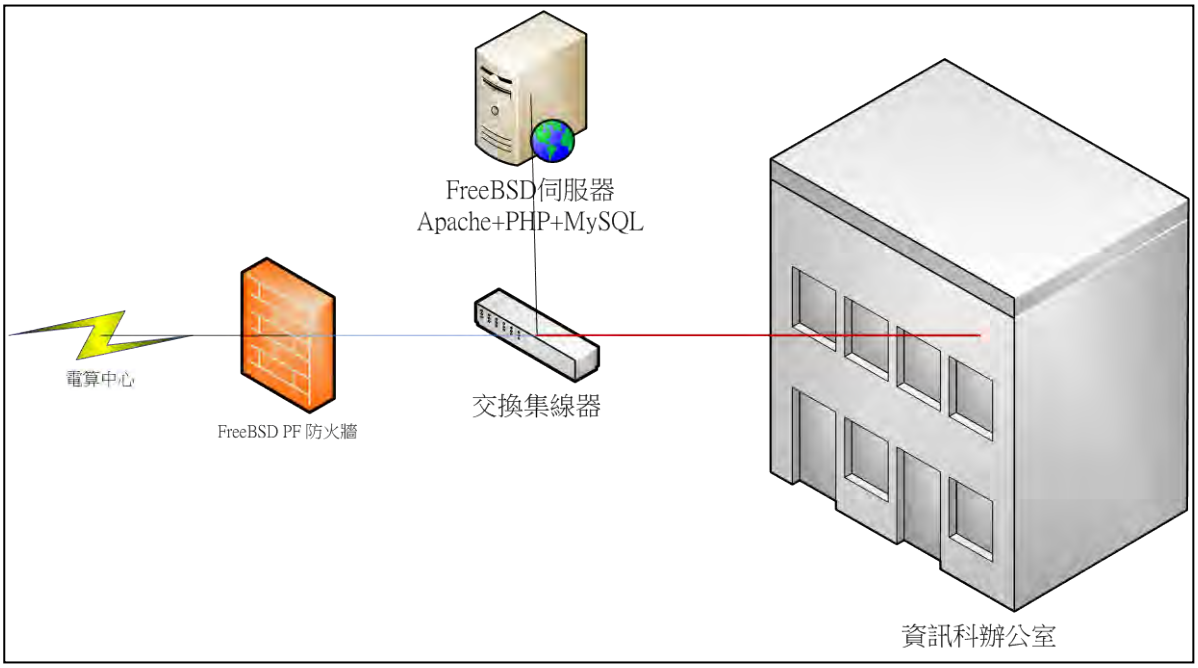


圖 4-網路分析實驗架構

肆、研究過程或方法

本次研究從電腦網路運作開始，探討各種常見網路大量連線異常，再架設防火牆，將**防火牆**紀錄分析統計，進而確定**演算法**編寫成警報程式。最後完成實驗成果分析，預定研究時間表如下：

超量網路連線預警偵測分析及探討研究進度表																									
	週次 / 項目	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
1	資料蒐集																									
2	研究設備																									
3	研究過程與方法																									
4	研究結果																									
5	討論、結論																									
6	參考資料																									
7	老師討論																									

表 3-超量網路連線預警偵測分析進度時間表

一、 網路運作模式探討

在 OSI 模型網路七層架構中取第四層**傳輸層**探討，TCP-IP **傳輸層**的協定主要為 UDP 與 TCP，傳輸的數量影響著網路效能，使用過量或異常所造成過量極易造成網路效能不彰。

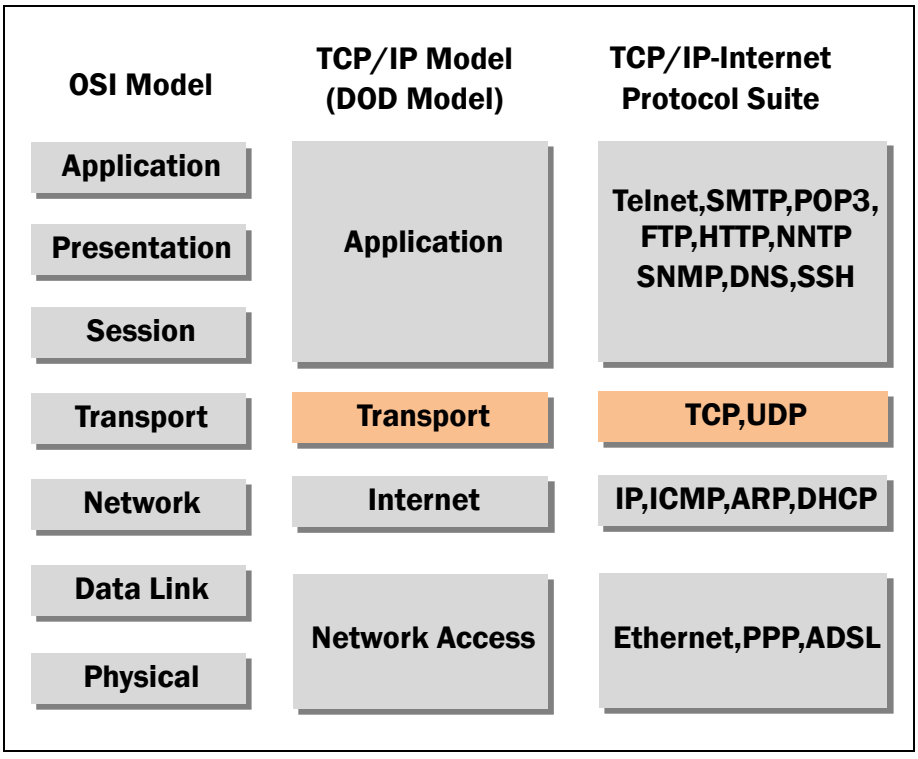


圖 5-TCP/IP DOD 模型中的**傳輸層**

二、 常見網路大量連線異常探討

(一) **對等式網路**(P2P)：主要是各對等電腦之間互相傳輸檔案或影片，在取得資料時有可能同一個檔案來自數十到數百電腦的來源，分割成不同的檔案片段，而且在接收的同時亦擔任伺服器(Server)的角色，把檔案片段分送給其他對等的電腦。

因此在規劃分析時要注意大量發送到對等電腦(大量不同 IP)的狀況，有很高的比例是屬於 P2P。

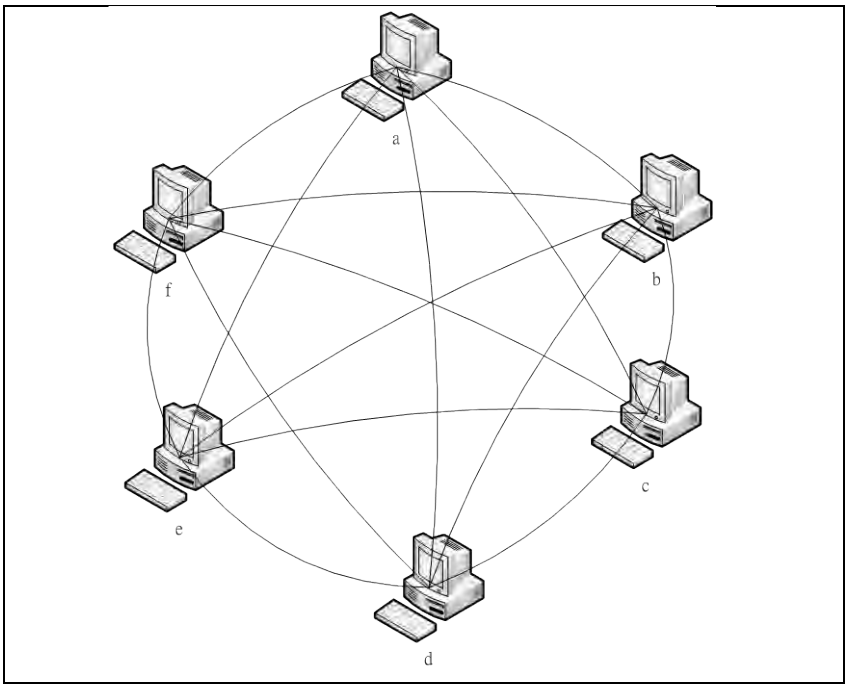


圖 6-**對等式網路**(P2P)

(二) **電腦蠕蟲**(Computer worm) ：具有在網路中自行散佈，並任意進行**阻斷式攻擊**(DDOS)的特性，分析時和 P2P 的不同點在於，封包的長度通常是 0 ，而 P2P 只有在 1024 以上埠口做 TCP ACK 時的封包長度是 0 。

(三) **殭屍網路**(Botnet)：特性與電腦蠕蟲大致類似，差別在於攻擊的對像在同一時段是固定的；分析時可將統一發動攻擊的 IP 歸類，來確認感染。

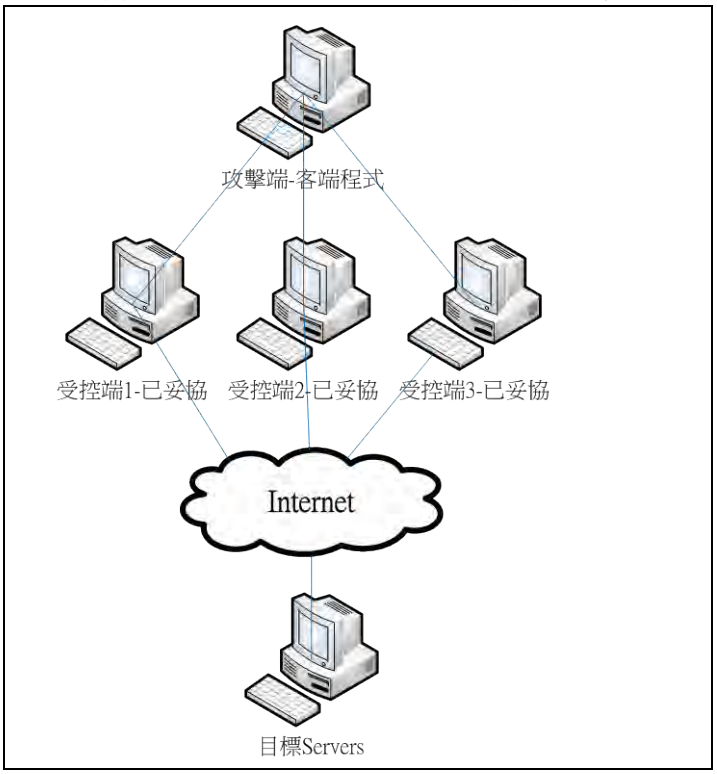


圖 7-殭屍網路運作(Botnet)

三、 建構分析平台

(一) 伺服器系統安裝

1. 安裝 FreeBSD 系統，並將 pf 加入系統核心。
2. 以學校現有伺服器 Apache+PHP+MySQL，加入個人帳號，以供資料分析及瀏覽程式平台。
3. 防火牆設定：網路運作 1024-65535 埠口，通常不做為**一般服務埠口**使用，因此排除 **0-1023 已知的服務埠口**，並以 1024-65535 為主要分析對象，防火牆也以 1024-65535 埠口為紀錄對象，在 IP 範圍也只以科內電腦為分析對象，採<u>正向列舉法</u>，至於其他 IP 或偽裝 IP 將被過濾排除。

```
pass in log quick on $ext_if inet proto tcp from any to $cc_net port $uk_ports flags S/SA modulate state
#紀錄 TCP->uknown port
pass in log quick on $ext_if inet proto udp from any to any port $wk_ports keep state
#紀錄 UDP->Well-known port
block in log quick on $ext_if inet proto udp from any to any port $uk_ports
#紀錄 UDP->uknown port
```

表 4-pf 防火牆 pf.conf 相關設定(pflog 紀錄部份)

(二) 圖表繪製與圖案設計

按鈕圖及代表 Logo 以 Ulead PhotoImpact 處理，IP 所屬國家之國旗，取自 Icon 網站，折線圖及圓形圖以 PHP 程式中 GD 函數自行繪製，同時在上方或下方加註執行時間資訊。

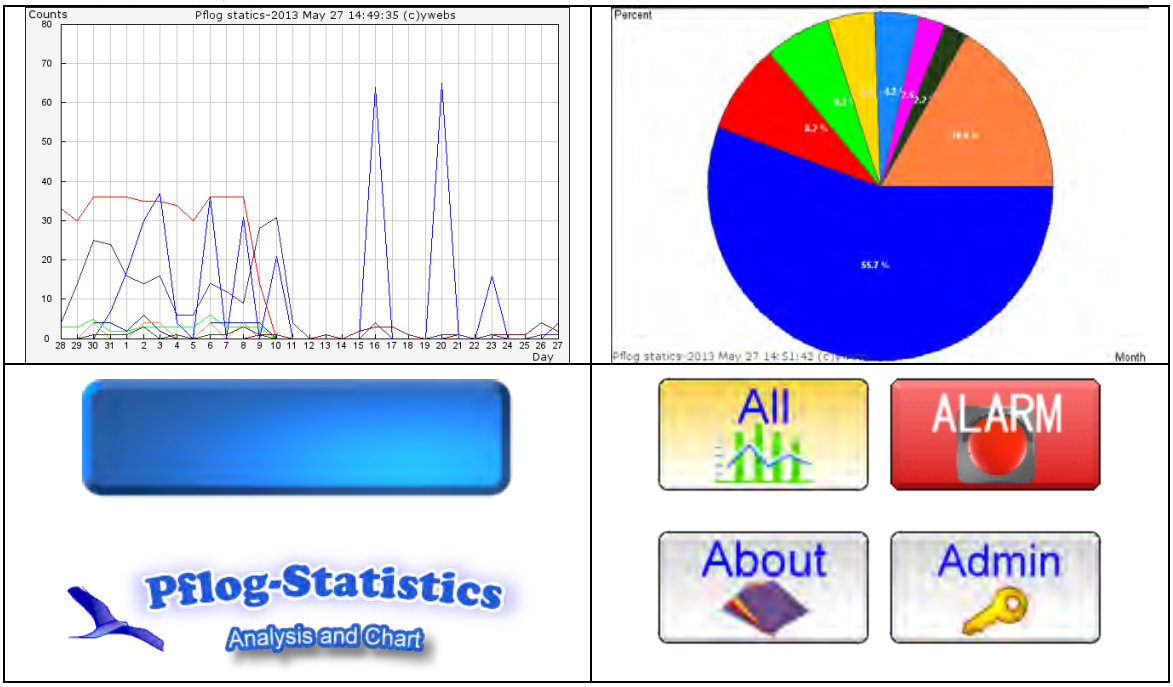


圖 9 各圖案設計與繪製

(三) 程式流程與演算法

以 PHP 語法完成所需程式，在登入網頁後可由各選單操作程式功能。為了考慮程式流通性，決定以英文介面來編寫。

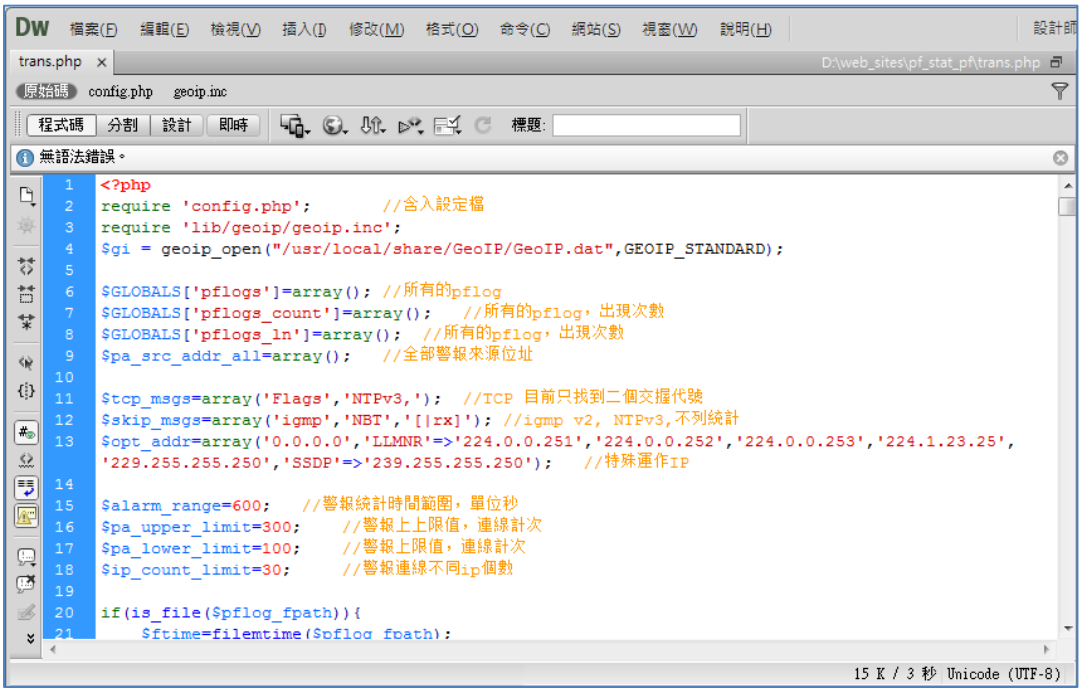


圖 8-PHP 程式編寫-匯入及警報程式

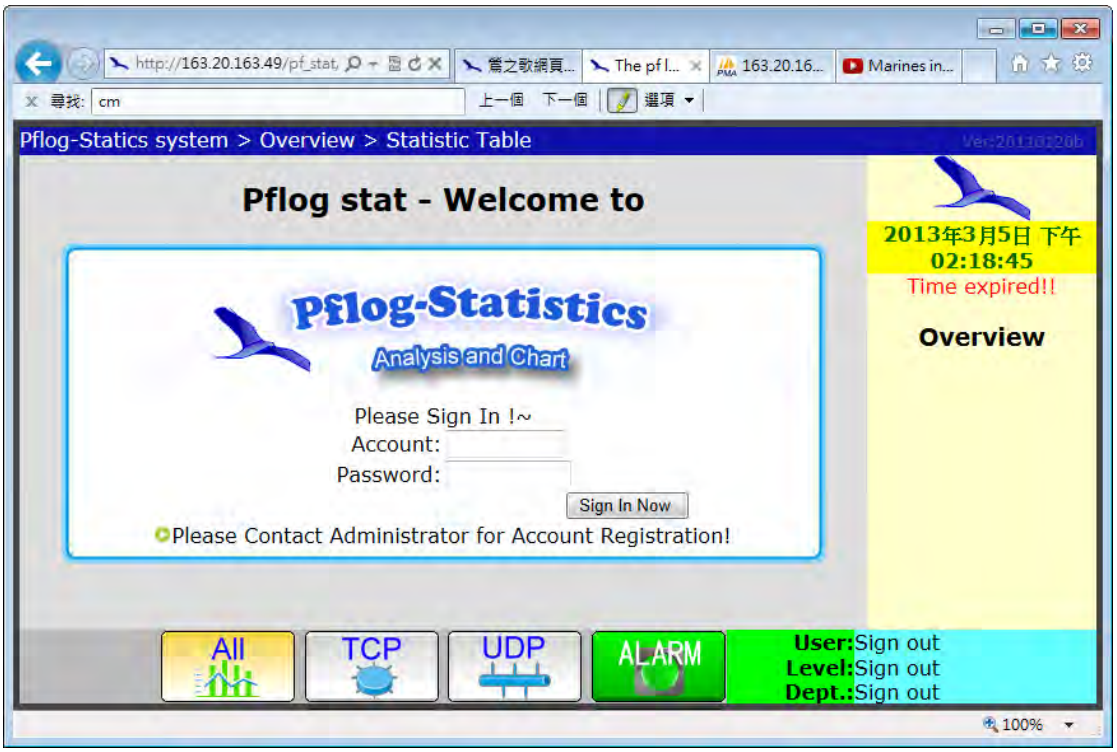


圖 9-紀錄分析網站登入畫面

編寫程式前必確立程式的演算法，以下以程式流程圖說明之：

1. 主網頁程式流程 ：

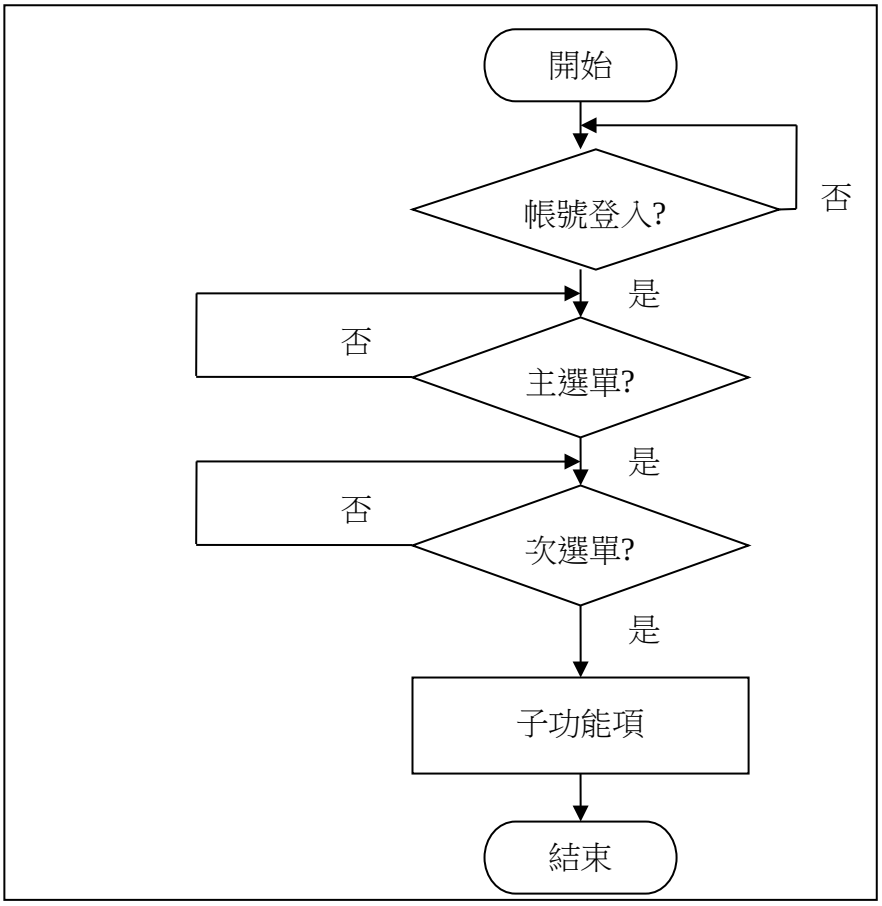


圖 10-主程式流程圖

2. **畫面**選單介紹：主選單按鈕，右方為次選單按鈕；下方為主選單按鈕。

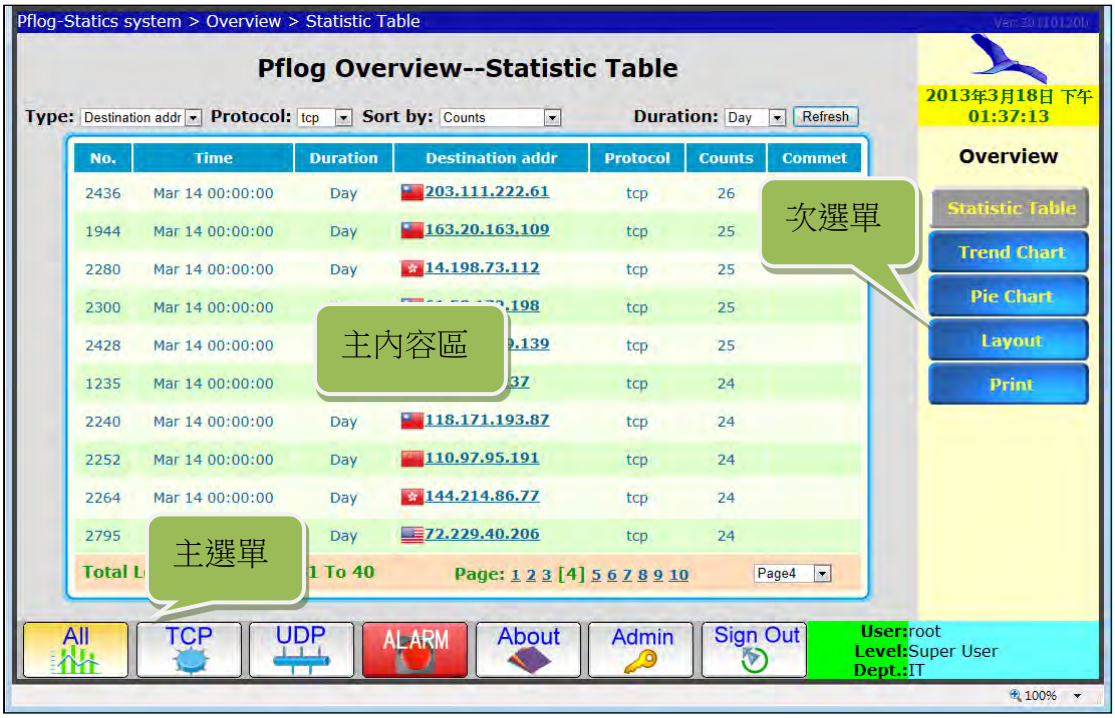


圖 11-主畫面選單介紹

3. 分析表輸出流程

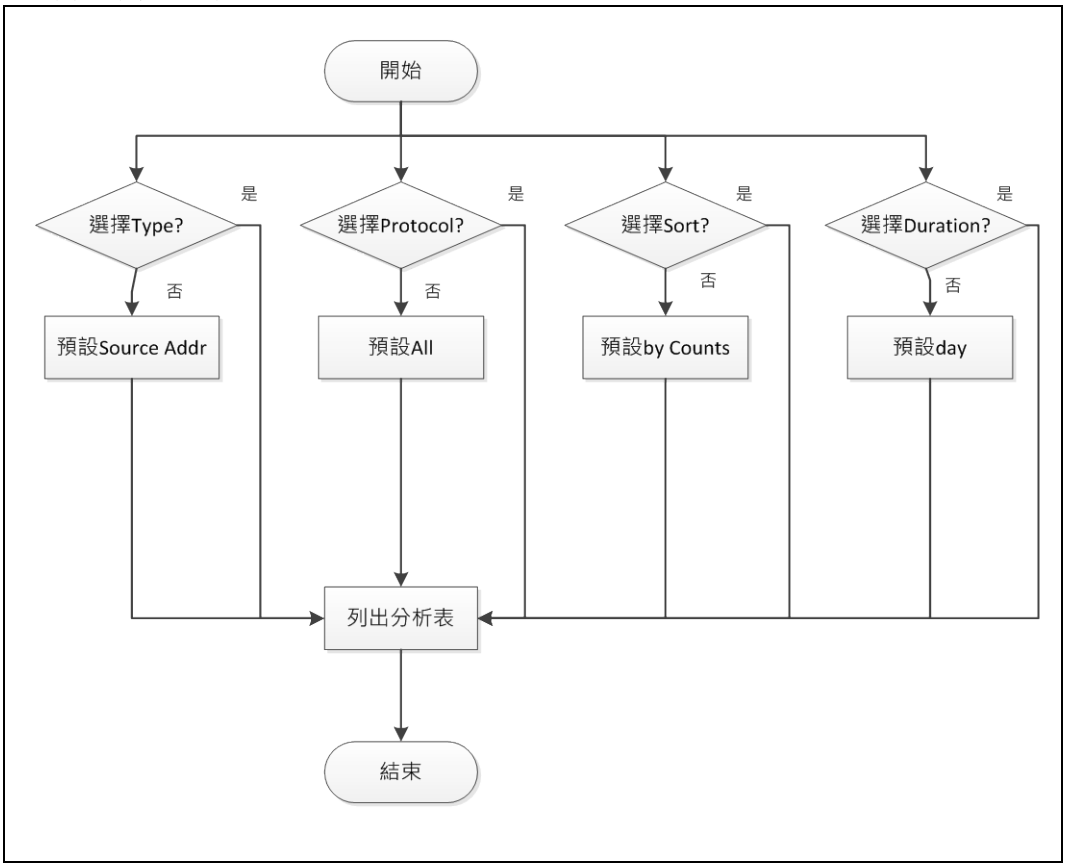


圖 12-分析表輸出流程圖

4. **防火牆**匯入及統計：透過系統排程 crontab，每 10 分鐘將 pflog 紀錄匯入，主要是以**空白字元**切割欄位，查詢指令說明 man pfctl，man pflog，找出每一欄之定義，以三方握手判斷為 TCP。

```
1339578055.102499 rule 37..16777216/0(match): block out on em0: 163.20.163.46.58029 > 224.0.0.252.5355: UDP, length 24
1339578055.113746 rule 37..16777216/0(match): block out on em0: 163.20.163.46.55921 > 224.0.0.252.5355: UDP, length 24
1339578055.123865 rule 37..16777216/0(match): block out on em0: 163.20.163.46.51834 > 224.0.0.252.5355: UDP, length 24
1339578055.136108 rule 37..16777216/0(match): block out on em0: 163.20.163.46.51437 > 224.0.0.252.5355: UDP, length 24
1339578055.146348 rule 37..16777216/0(match): block out on em0: 163.20.163.46.62521 > 224.0.0.252.5355: UDP, length 24
1339578055.294478 rule 11..16777216/0(match): block in on em0: 163.20.163.88.137 > 163.20.163.255.137: NBT UDP PACKET(137):
  QUERY; REQUEST; BROADCAST
1339578056.557532 rule 29..16777216/0(match): block out on em0: 163.20.163.35.137 > 163.20.163.255.137: NBT UDP
  PACKET(137): QUERY; REQUEST; BROADCAST
1339578057.324208 rule 37..16777216/0(match): block out on em0: 163.20.163.35.59319 > 224.0.0.252.5355: UDP, length 27
1339578057.431154 rule 37..16777216/0(match): block out on em0: 163.20.163.35.59319 > 224.0.0.252.5355: UDP, length 27
1339578059.162761 rule 29..16777216/0(match): block out on em0: 163.20.163.35.137 > 163.20.163.255.137: NBT UDP
  PACKET(137): QUERY; REQUEST; BROADCAST
1339578061.368852 rule 37..16777216/0(match): block out on em0: 163.20.163.31.20110 > 229.255.255.250.20110: UDP, length 83
1339578062.573266 rule 38..16777216/0(match): block out on em0: 163.20.163.31.59007 > 182.241.89.174.4411: Flags [S], seq
  1511517240, win 8192, options [mss 1460,nop,wscale 2,nop,nop,sackOK], length 0
1339578062.573392 rule 38..16777216/0(match): block out on em0: 163.20.163.31.59008 > 175.190.255.199.8080: Flags [S], seq
  3064329166, win 8192, options [mss 1460,nop,wscale 2,nop,nop,sackOK], length 0
1339578062.573398 rule 38..16777216/0(match): block out on em0: 163.20.163.31.59009 > 122.138.159.233.20100: Flags [S], seq
  1394610461, win 8192, options [mss 1460,nop,wscale 2,nop,nop,sackOK], length 0
1339578062.573516 rule 38..16777216/0(match): block out on em0: 163.20.163.31.59010 > 122.72.24.11.8080: Flags [S], seq
  756027366, win 8192, options [mss 1460,nop,wscale 2,nop,nop,sackOK], length 0
```

表 5-pflog 防火牆紀錄原始檔

(1) 匯入 **pflog** 原始檔，依各資料表各欄定義存放：

防火牆紀錄資料表												
編號	紀錄時間(微秒)	規則行	封鎖/放行	方向	介面	來源 IP	來源 Port	目的 IP	目的 Port	協定	次數	其他項
pl_id	pl_time	pl_rule	pl_action	pl_direct	pl_if	pl_src_addr	pl_src_port	pl_dst_addr	pl_dst_port	pl_proto	pl_count	pl_reason
1	1363131994.440217	33	1	1	em0	2736038777	1112	1876774285	40038	0	1	length0
2	1363132000.003976	33	1	1	em0	2736038687	56180	1249714045	5222	0	1	length0
3	1363132047.852354	33	1	1	em0	2736038777	1118	2735596250	3939	0	3	length0
4	1363132052.596841	33	1	1	em0	2736038773	60164	1136901070	5050	0	1	length0
5	1363132068.460351	33	1	1	em0	2736038773	60182	1136900797	5050	0	1	length0
6	1363132120.184468	33	1	1	em0	2736038687	49171	1249714045	5222	0	2	length0
7	1363132170.073283	33	1	1	em0	2736038880	61505	2736038705	25864	0	1	length0
8	1363132175.153073	33	1	1	em0	2736038880	61511	2736038705	15415	0	1	length0
9	1363132177.403386	33	1	1	em0	2736038880	61514	2736038705	56928	0	1	length0
10	1363132178.867907	33	1	1	em0	2736038880	61516	2736038705	59165	0	1	length0

表 6-**pflog 防火牆**紀錄資料表欄位(IP 已轉成**長整數**)

(2) 統計 pflog 紀錄，如超過警報上限值，則存入警報表，即發佈警報：

警報紀錄資料表									
警報類型	編號	警報 IP	協定	總次數	警報等級	警報單位	匯檔編號	解除	警報時間
pa_type	pa_id	pa_addr	pa_proto	pa_amount	pa_level	pa_dept_id	pa_pi_id	pa_en	pa_time
0	1	2736038880	0	21	0	1	55	0	1363132800
0	2	2736038741	0	131	0	1	62	0	1363136400
0	3	2736038741	0	167	0	1	63	0	1363136940
1	4	2736038774	1	107	0	1	78	0	1363144680
1	5	2736038774	1	124	0	1	79	0	1363145220
0	6	2736038773	0	101	0	1	99	0	1363152896
0	7	2736038757	0	133	0	1	99	0	1363153400
0	8	2736038757	0	165	0	1	100	0	1363153498
0	9	2736038757	0	136	0	1	101	0	1363154084
0	10	2736038757	0	101	0	1	102	0	1363154410

表 7-**pflog 警報**資料表欄位(IP 已轉成**長整數**)

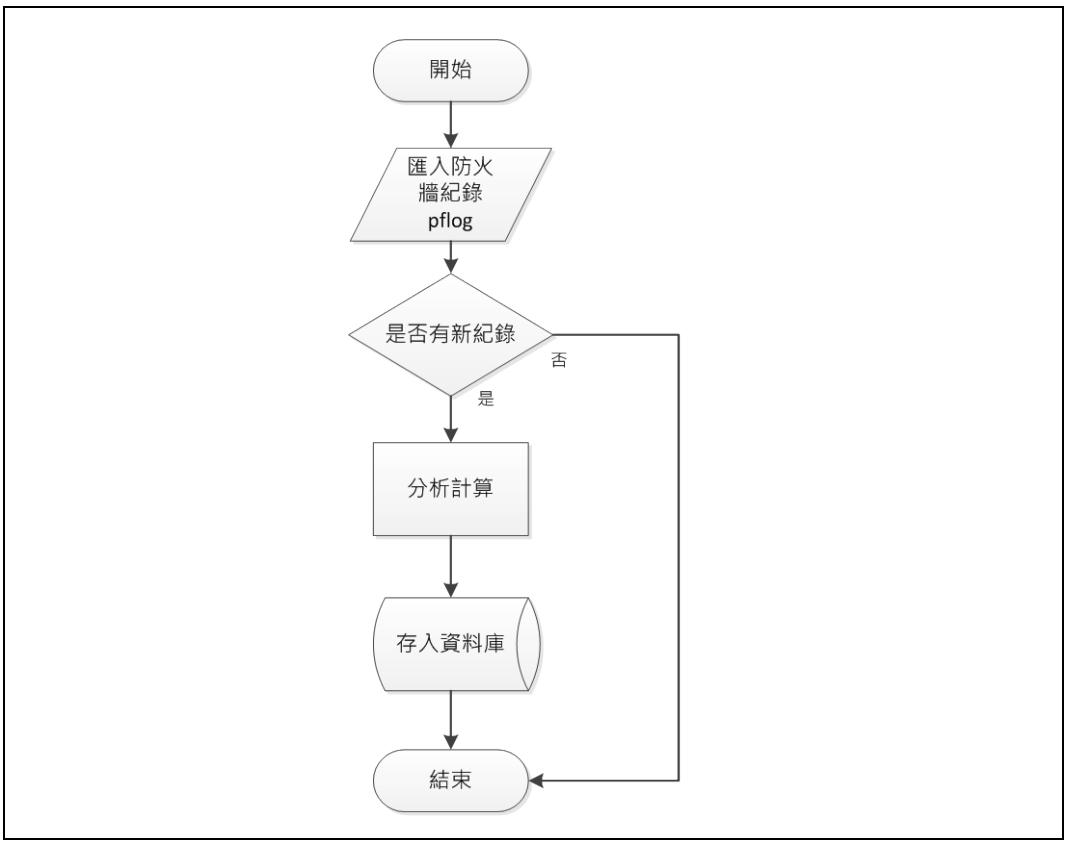


圖 13-防火牆匯入及統計流程圖

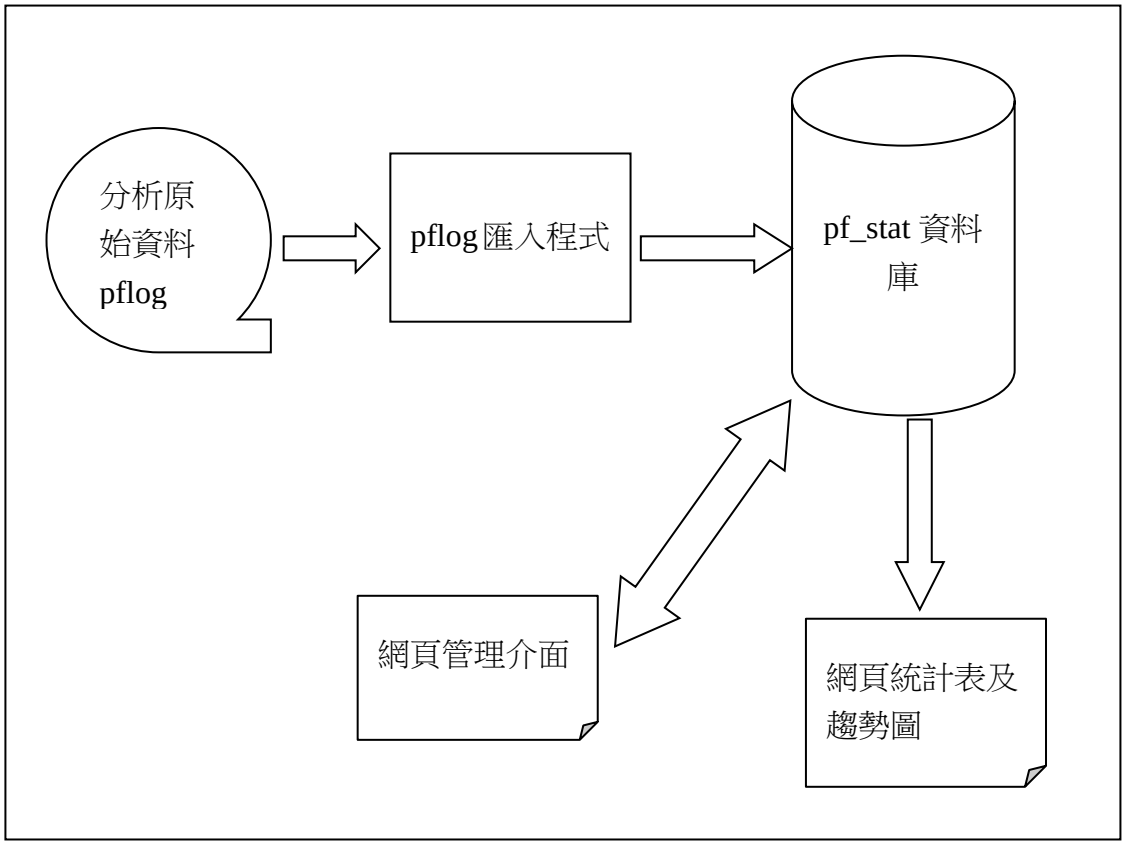


圖 14-防火牆匯入程序示意圖

1. 基本不當入侵偵測

網路運作埠口(port)有些服務屬於區域網路內部運作或是需要管理帳號密碼的服務，因此如果從外部連結內部這些埠口則屬於不正常運作或測試，可歸類為外部**不當入侵**，列舉具有風險的不當入侵埠口如下表：

編號	埠口(port)	用途	說明
1	22	ssh,sftp	安全外層及安全外層檔案傳輸協定
2	23	telnet	遠端登錄
3	25	smtp	簡易郵件傳輸協定
4	69	tftp	簡易檔案傳輸協定(常用於更新韌體)
5	137-139	netbios	網路基本輸入輸出系統(區網運作使用)
6	445	microsoft-ds	微軟網路芳鄰服務
7	593	http-rpc-epmap	交換目錄資訊
8	1433-1434	Microsoft-SQL	MSSQL Server and Monitor
9	3306	mysql	MySQL 資料庫交換 port
10	3389	rdp	微軟遠端桌面
11	4444	nv-video	影片播放

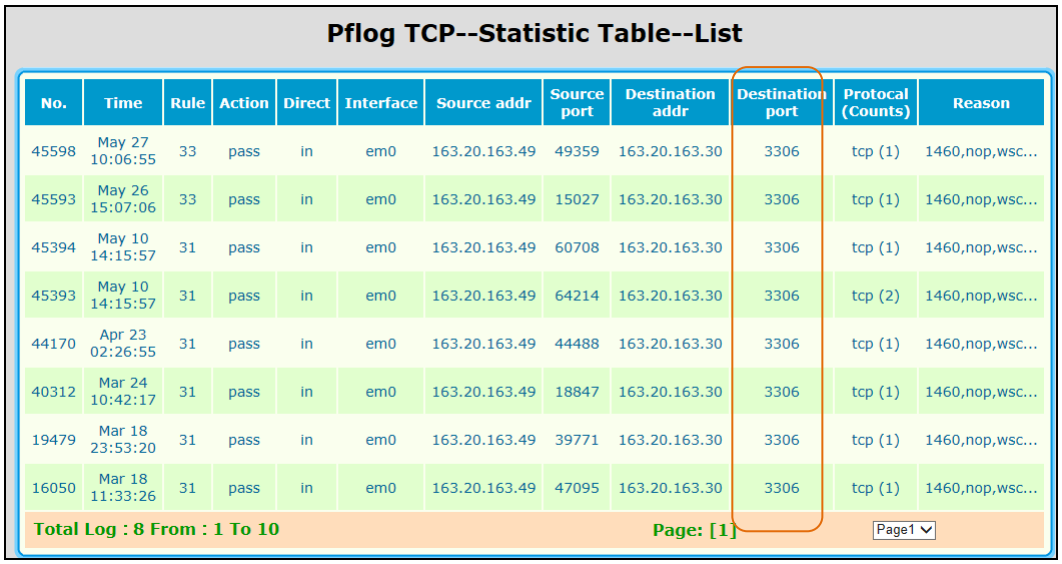
表 8 - 不當入侵偵測埠口

Pflog TCP--Statistic Table--List

No.	Time	Rule	Action	Direct	Interface	Source addr	Source port	Destination addr	Destination port	Protocal (Counts)	Reason
39914	Mar 23 14:43:28	31	pass	in	em0	42.96.174.109	1657	163.20.163.224	3389	tcp (10)	length0
39913	Mar 23 14:43:23	31	pass	in	em0	42.96.174.109	4949	163.20.163.224	3389	tcp (6)	length0
39912	Mar 23 14:39:33	31	pass	in	em0	42.96.174.109	2901	163.20.163.84	3389	tcp (1)	length0
39460	Mar 23 12:00:07	31	pass	in	em0	42.96.174.109	1955	163.20.163.224	3389	tcp (14)	length0
39282	Mar 23 08:29:17	31	pass	in	em0	42.96.174.109	6000	163.20.163.224	3389	tcp (1)	length0
39281	Mar 23 08:29:17	31	pass	in	em0	42.96.174.109	6000	163.20.163.170	3389	tcp (1)	length0
39280	Mar 23 08:29:17	31	pass	in	em0	42.96.174.109	6000	163.20.163.117	3389	tcp (1)	length0
39279	Mar 23 08:29:17	31	pass	in	em0	42.96.174.109	6000	163.20.163.83	3389	tcp (1)	length0
39278	Mar 23 08:29:17	31	pass	in	em0	42.96.174.109	6000	163.20.163.84	3389	tcp (1)	length0
39277	Mar 23 08:29:17	31	pass	in	em0	42.96.174.109	6000	163.20.163.41	3389	tcp (1)	length0

Total Log : 13 From : 1 To 10 Page: [1] 2 Page1

圖 15-不當入侵一例，3389(微軟遠端桌面)



Pflog TCP--Statistic Table--List

No.	Time	Rule	Action	Direct	Interface	Source addr	Source port	Destination addr	Destination port	Protocal (Counts)	Reason
45598	May 27 10:06:55	33	pass	in	em0	163.20.163.49	49359	163.20.163.30	3306	tcp (1)	1460,nop,wsc...
45593	May 26 15:07:06	33	pass	in	em0	163.20.163.49	15027	163.20.163.30	3306	tcp (1)	1460,nop,wsc...
45394	May 10 14:15:57	31	pass	in	em0	163.20.163.49	60708	163.20.163.30	3306	tcp (1)	1460,nop,wsc...
45393	May 10 14:15:57	31	pass	in	em0	163.20.163.49	64214	163.20.163.30	3306	tcp (2)	1460,nop,wsc...
44170	Apr 23 02:26:55	31	pass	in	em0	163.20.163.49	44488	163.20.163.30	3306	tcp (1)	1460,nop,wsc...
40312	Mar 24 10:42:17	31	pass	in	em0	163.20.163.49	18847	163.20.163.30	3306	tcp (1)	1460,nop,wsc...
19479	Mar 18 23:53:20	31	pass	in	em0	163.20.163.49	39771	163.20.163.30	3306	tcp (1)	1460,nop,wsc...
16050	Mar 18 11:33:26	31	pass	in	em0	163.20.163.49	47095	163.20.163.30	3306	tcp (1)	1460,nop,wsc...

Total Log : 8 From : 1 To 10 Page: [1] Page1

圖 16-不當入侵一例 2，3306(MySQL 資料庫交換 port)

2. 警報產生程式

警報產生程式為本次研究的重點項目，為加強時效每 9 分鐘由系統排程(crontab)匯入 pflog 檔；接著匯入程式先把可能的異常放入資料庫做為判別基本資料，等這次的紀錄都已匯入完成，再統計**個別 IP 於 10 分鐘內的總異常數**，比較原先設定好的上限值，如果有大於上限值即列入警報。

分析警報型態，如果目的 IP addr(Destination addr) 數目計算大於 20，將警報型能判斷為**對等式網路**(P2P)，否則判斷該 IP 電腦為感染**電腦蠕蟲**(Computer worm)或**殭屍網路**(Botnet)。

如果發生警報沒有適時處理，相同的 IP addr 會持續發生警報，因此需將相同的 IP 的警報合併加總，再另外處理成**一個 IP 只顯示一次**的統計表，操作上可由下拉選項選擇，**顯示最大的統計值**，或**顯示最新的統計值**。下圖為產生警報之流程。

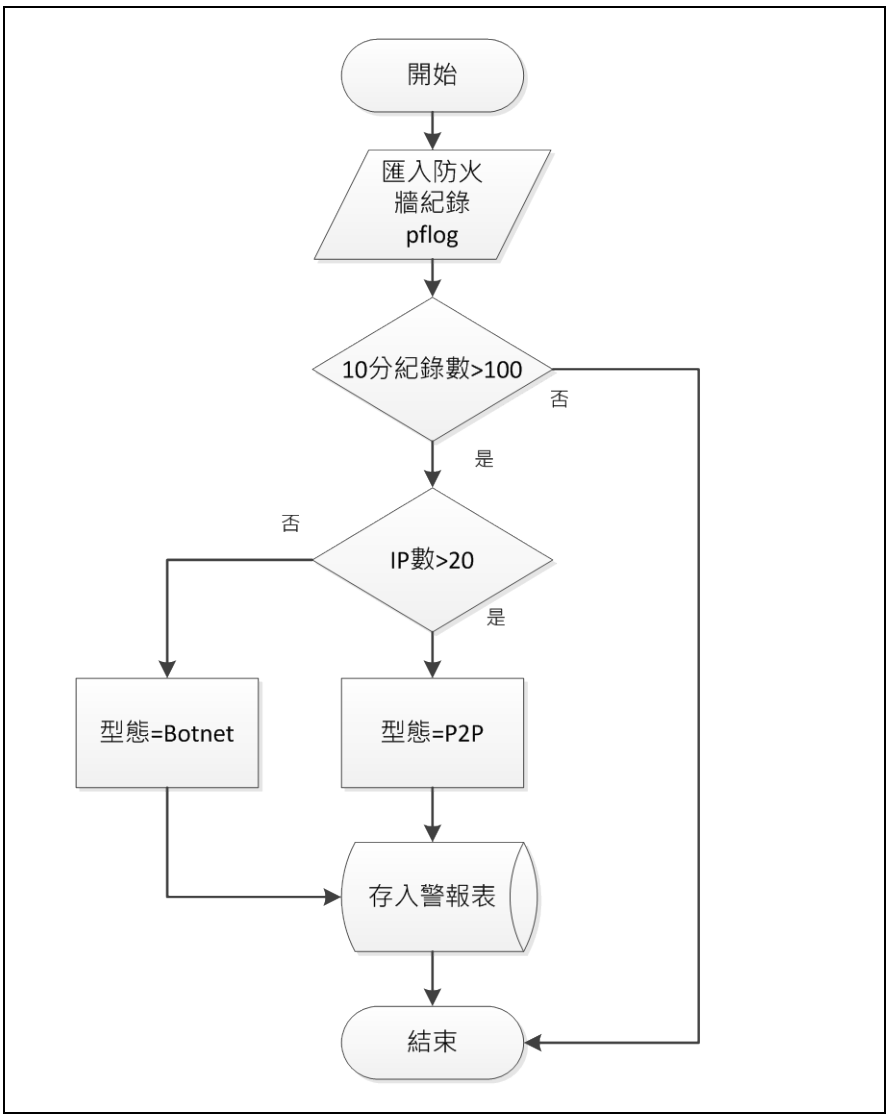


圖 15-警報產生程式流程圖

(1) 警報產生時的運作

A. 無警報時 Alarm 按鈕無閃爍

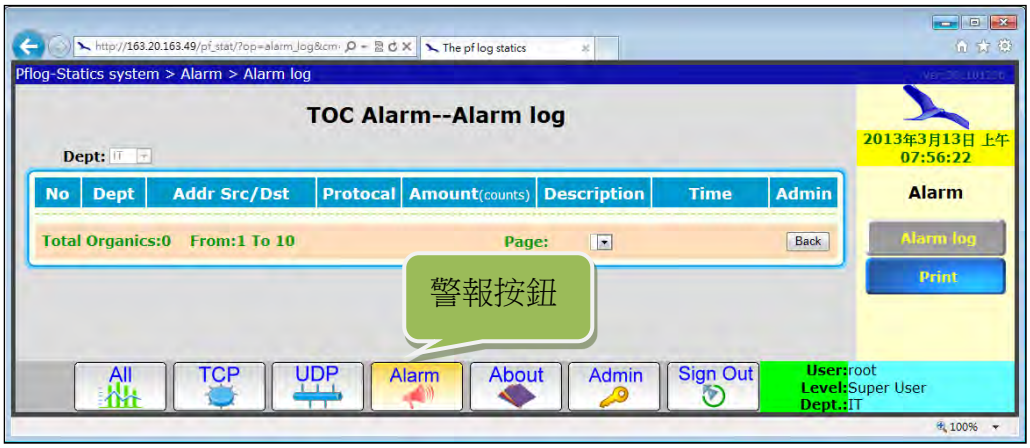


圖 16-無警報紀錄時顯示正常

B. 可能網路異常；發生警報，Alarm 按鈕紅綠閃爍，待解除(Recall)後恢復

圖 17-警報紀錄時顯示紅綠閃爍

C. 警報解除(Recall)，Alarm 按鈕停止閃爍

圖 18-警報解除恢復正常

3. 統計資訊

(1)異常紀錄數量排序表，每頁 10 筆

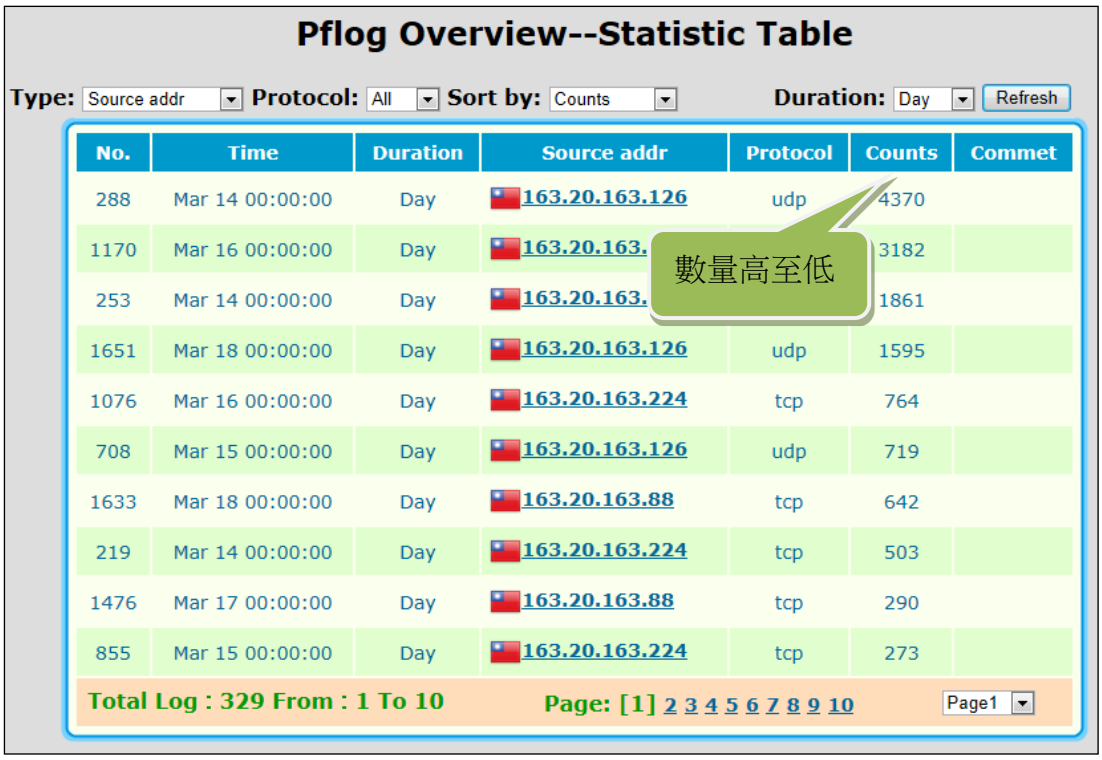


圖 19-異常紀錄數量排序表

(2)前 7 筆異常折線圖：最大刻度可彈性調整設定

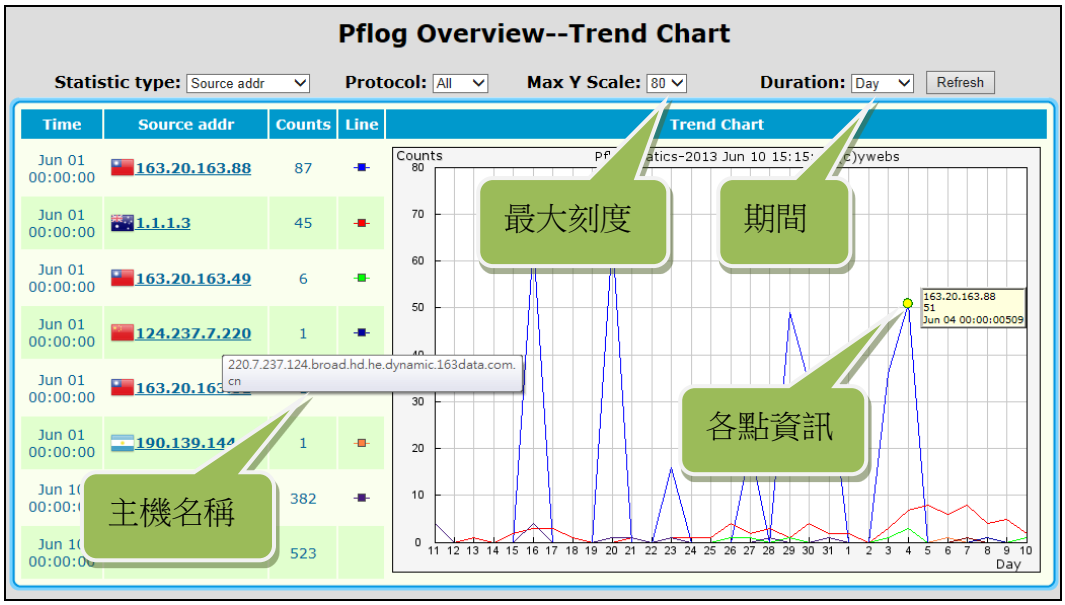


圖 20-前 7 筆異常折線圖

(3)前 7 筆異常圓形圖：

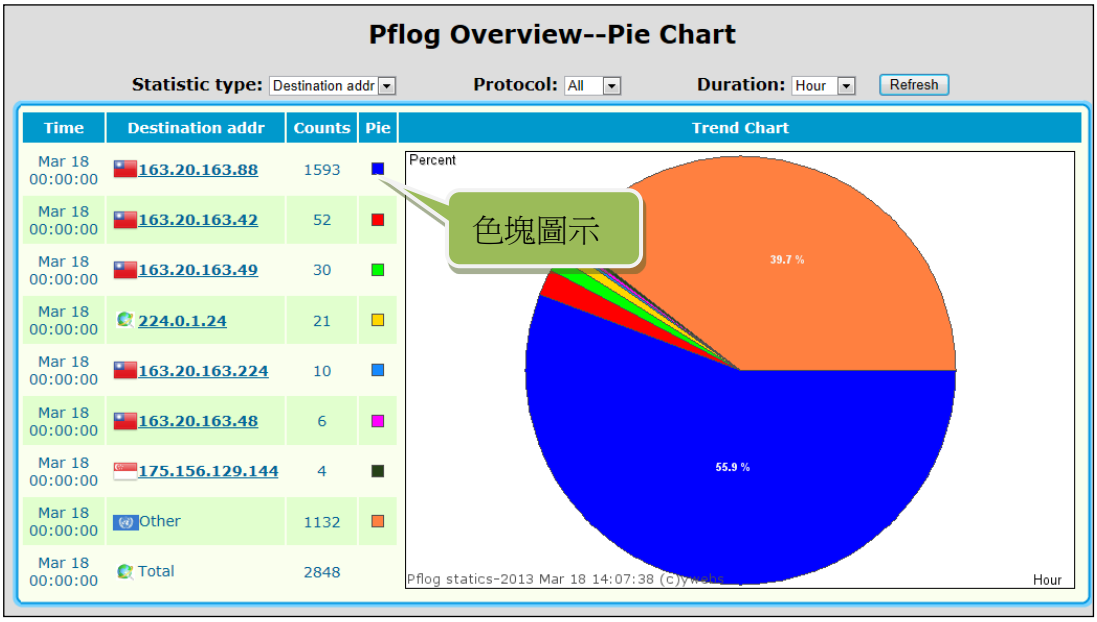
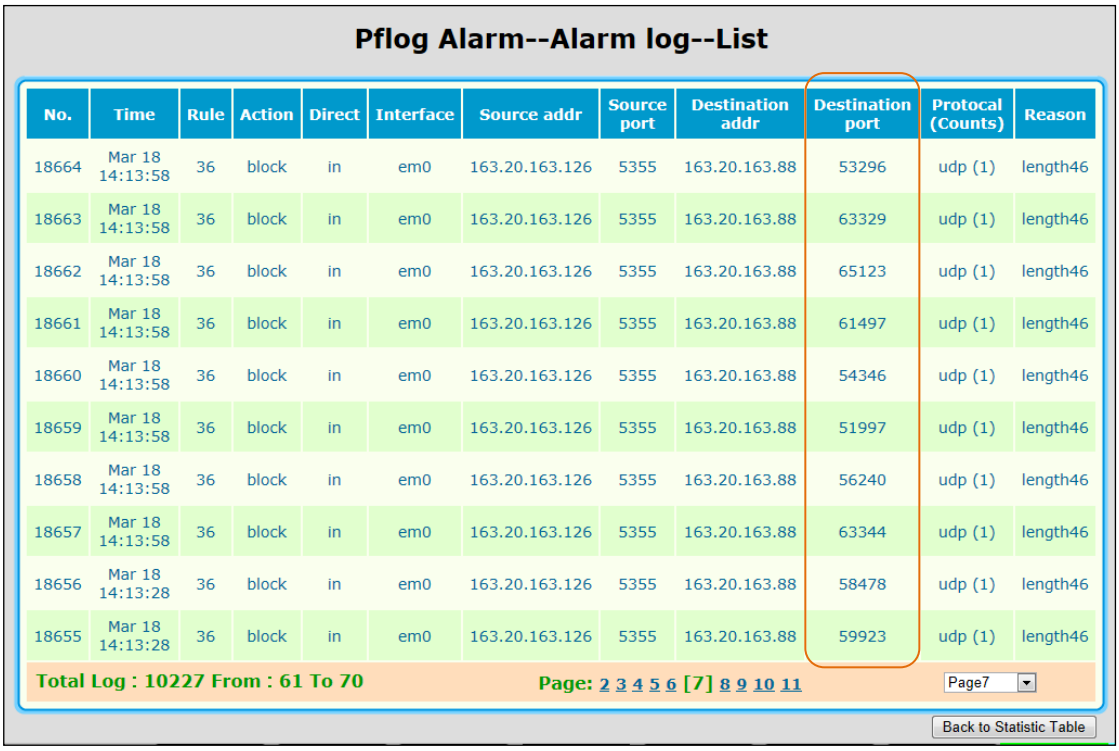


圖 21-前 7 筆異常圓形圖

4. 警報判別

(1)**電腦蠕蟲** Computer Worm 或**殭屍網路** Botnet：判斷上以大量不斷攻擊某IP，而且每次不同連接埠來偵測。



Pflog Alarm--Alarm log--List

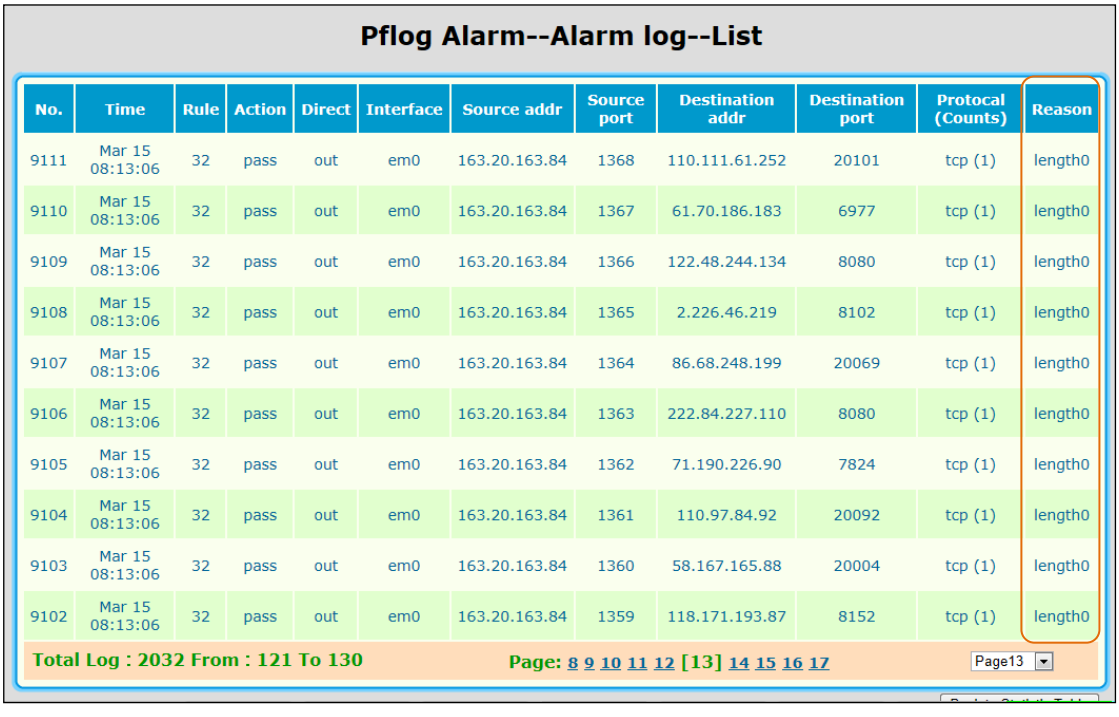
No.	Time	Rule	Action	Direct	Interface	Source addr	Source port	Destination addr	Destination port	Protocal (Counts)	Reason
18664	Mar 18 14:13:58	36	block	in	em0	163.20.163.126	5355	163.20.163.88	53296	udp (1)	length46
18663	Mar 18 14:13:58	36	block	in	em0	163.20.163.126	5355	163.20.163.88	63329	udp (1)	length46
18662	Mar 18 14:13:58	36	block	in	em0	163.20.163.126	5355	163.20.163.88	65123	udp (1)	length46
18661	Mar 18 14:13:58	36	block	in	em0	163.20.163.126	5355	163.20.163.88	61497	udp (1)	length46
18660	Mar 18 14:13:58	36	block	in	em0	163.20.163.126	5355	163.20.163.88	54346	udp (1)	length46
18659	Mar 18 14:13:58	36	block	in	em0	163.20.163.126	5355	163.20.163.88	51997	udp (1)	length46
18658	Mar 18 14:13:58	36	block	in	em0	163.20.163.126	5355	163.20.163.88	56240	udp (1)	length46
18657	Mar 18 14:13:58	36	block	in	em0	163.20.163.126	5355	163.20.163.88	63344	udp (1)	length46
18656	Mar 18 14:13:28	36	block	in	em0	163.20.163.126	5355	163.20.163.88	58478	udp (1)	length46
18655	Mar 18 14:13:28	36	block	in	em0	163.20.163.126	5355	163.20.163.88	59923	udp (1)	length46

Total Log : 10227 From : 61 To 70 Page: 2 3 4 5 6 [7] 8 9 10 11 Page7

Back to Statistic Table

圖 22-疑似電腦蠕蟲詳細列表

(2)**對等式網路** P2P(Internet TV,BT,...)：大量發送不同目標 IP，並且做 TCP ACK，特點為封包長度為”0”。



Pflog Alarm--Alarm log--List

No.	Time	Rule	Action	Direct	Interface	Source addr	Source port	Destination addr	Destination port	Protocal (Counts)	Reason
9111	Mar 15 08:13:06	32	pass	out	em0	163.20.163.84	1368	110.111.61.252	20101	tcp (1)	length0
9110	Mar 15 08:13:06	32	pass	out	em0	163.20.163.84	1367	61.70.186.183	6977	tcp (1)	length0
9109	Mar 15 08:13:06	32	pass	out	em0	163.20.163.84	1366	122.48.244.134	8080	tcp (1)	length0
9108	Mar 15 08:13:06	32	pass	out	em0	163.20.163.84	1365	2.226.46.219	8102	tcp (1)	length0
9107	Mar 15 08:13:06	32	pass	out	em0	163.20.163.84	1364	86.68.248.199	20069	tcp (1)	length0
9106	Mar 15 08:13:06	32	pass	out	em0	163.20.163.84	1363	222.84.227.110	8080	tcp (1)	length0
9105	Mar 15 08:13:06	32	pass	out	em0	163.20.163.84	1362	71.190.226.90	7824	tcp (1)	length0
9104	Mar 15 08:13:06	32	pass	out	em0	163.20.163.84	1361	110.97.84.92	20092	tcp (1)	length0
9103	Mar 15 08:13:06	32	pass	out	em0	163.20.163.84	1360	58.167.165.88	20004	tcp (1)	length0
9102	Mar 15 08:13:06	32	pass	out	em0	163.20.163.84	1359	118.171.193.87	8152	tcp (1)	length0

Total Log : 2032 From : 121 To 130 Page: 8 9 10 11 12 [13] 14 15 16 17 Page13

圖 23-P2P 其中一 IP 詳細列表

5. NetBios Name 及 Mac Address 查詢 ： 查詢目前在網域內**電腦名稱**及**網卡硬體位址** Mac Address，方便進一步聯繫追蹤，為避免 IP 變動及偽裝，可由管理頁的 NetBios 資訊再配合交換器設定，將 Mac Address 在 Layer2(第二層)進行封鎖。

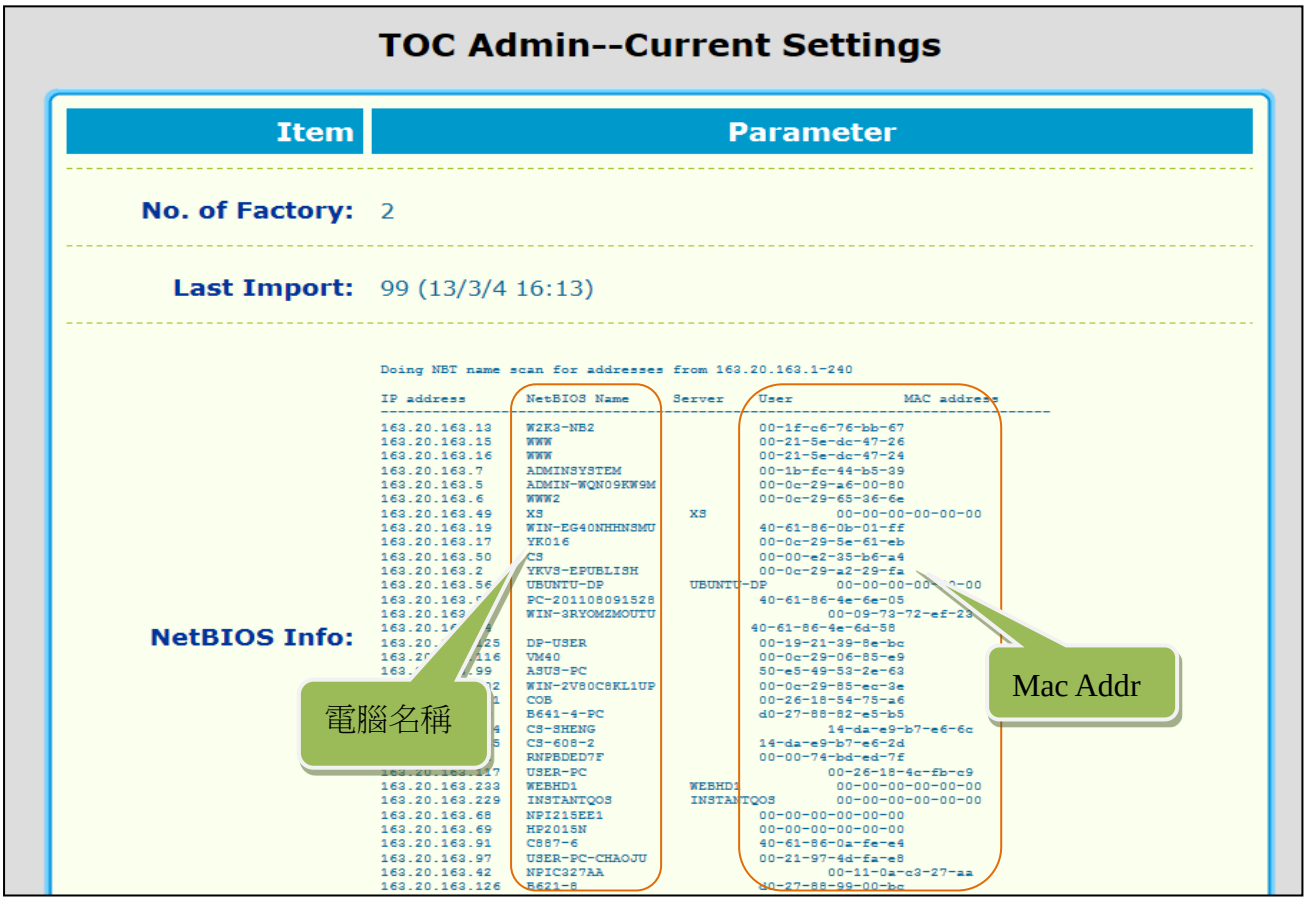


圖 24-NetBios Name 及 Mac Address

6. 特殊需排除連線：部份正常網路服務運作時，一樣會在短時間產生多次的連線，因此必需排除不列入警報統計，已先排除區域網路連線，其它正常大量連線分別討論如下：

(1) SSH，TCP 認可(ACK):

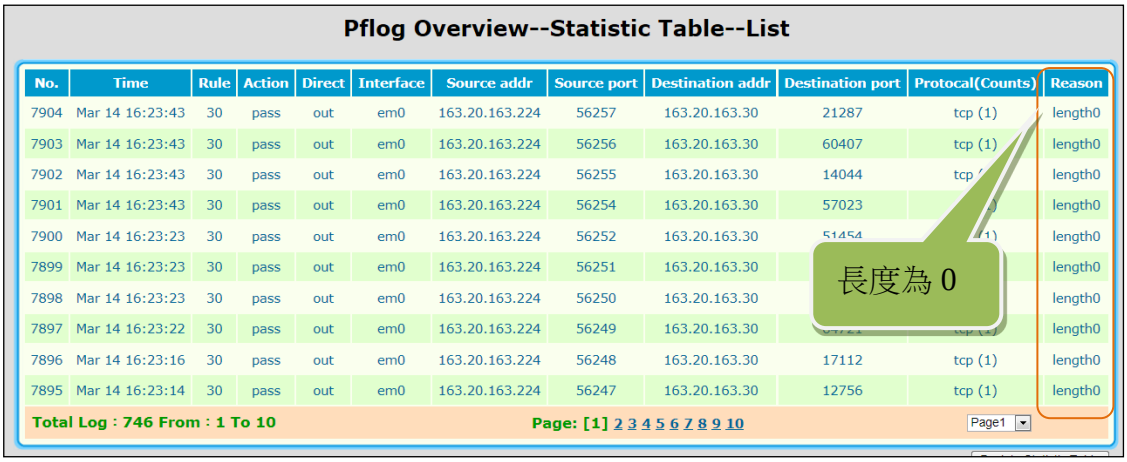


圖 25-SSH TCP 認可(ACK)

(2) 網路印表機 HP，TCP port 123->1230

Pflog Alarm--Alarm log--List

No.	Time	Rule	Action	Direct	Interface	Source addr	Source port	Destination addr	Destination port	Protocal(Counts)	Reason
8939	Mar 14 21:41:42	35	block	in	em0	163.20.163.57	123	163.20.163.42	1230	tcp (5)	length48
8936	Mar 14 21:41:25	35	block	in	em0	163.20.163.57	123	163.20.163.42	1230	tcp (6)	length48
8933	Mar 14 21:41:08	35	block	in	em0	163.20.163.57	123	163.20.163.42	1230	tcp (7)	length48
8930	Mar 14 21:40:50	35	block	in	em0	163.20.163.57	123	163.20.163.42	1230	tcp (8)	length48
8927	Mar 14 21:40:33	35	block	in	em0	163.20.163.57	123	163.20.163.42	1230	tcp (9)	length48
8924	Mar 14 21:40:16	35	block	in	em0	163.20.163.57	123	163.20.163.42	1230	tcp (10)	length48
8921	Mar 14 21:39:59	35	block	in	em0	163.20.163.57	123	163.20.163.42	1230	tcp (11)	length48
8918	Mar 14 21:39:42	35	block	in	em0	163.20.163.57	123	163.20.163.42	1230	tcp (12)	length48
8916	Mar 14 21:39:25	35	block	in	em0	163.20.163.57	123	163.20.163.42	1230	tcp (13)	length48
8911	Mar 14 21:21:11	35	block	in	em0	163.20.163.57	123	163.20.163.42	1230	tcp (77)	length48

Total Log : 54 From : 1 To 10　　Page: [1] 2 3 4 5 6　　Page1

Back to Statistic Table

圖 26-網路印表機 HP 紀錄

(四) 實驗檢核與回饋

以 user 電腦(近端)為進行實驗檢核，若偵測警報對像為近端電腦(圖 4 中**資訊科電腦**)，可進一步到電腦近端確認狀況，以**防毒軟體**及**封包過濾軟體** Wireshark 檢核確認。

下圖以 Microsoft Security Essentials 防毒軟體掃描的一個例子，可以提供警報統計後異常使用端回饋，做為判讀的正確性檢核的參考。

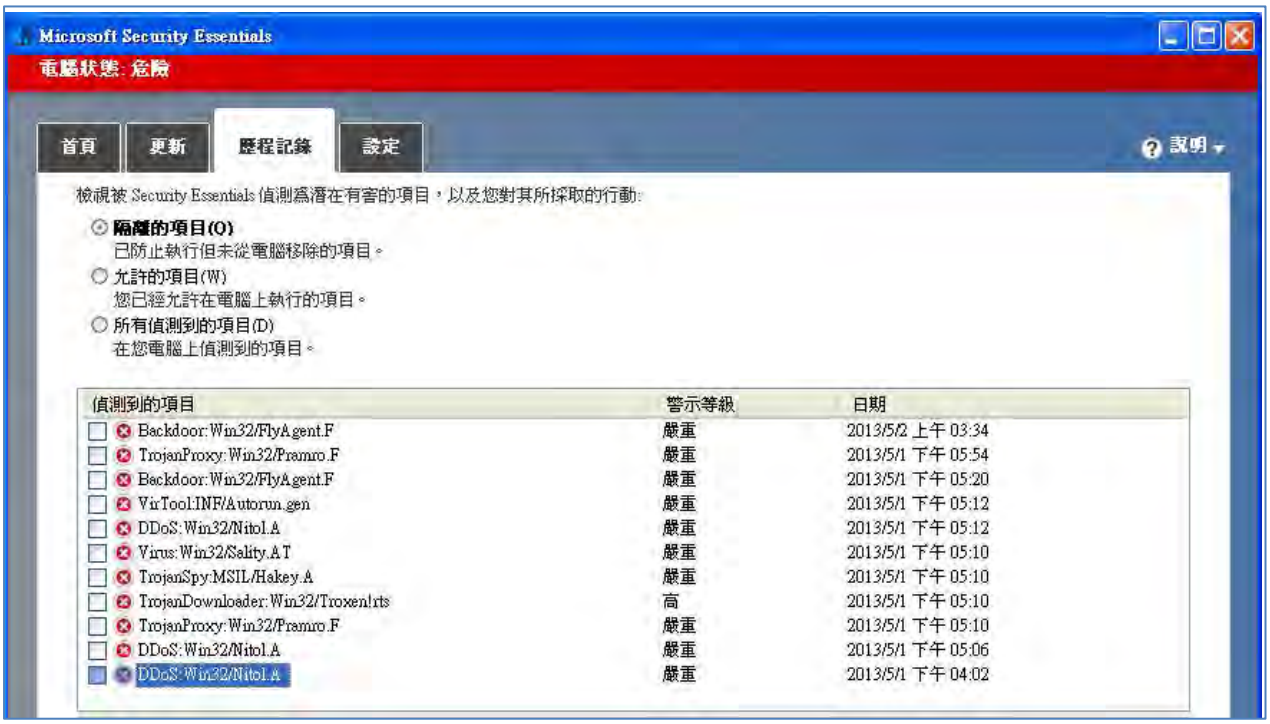


圖 27-防毒軟體掃描進行雙向檢核

封包過濾軟體 Wireshark 可選擇過濾其中一項規則或協定，如果能大略掌握可能的網路型危害，可針對該網路危害的特性設定過濾，來做為進一步查驗工具。但是如果在還沒有掌握異常的特性時，只能以全面性的監控封包，易因繁多的資料量，造成難以觀查出異常資料部份。

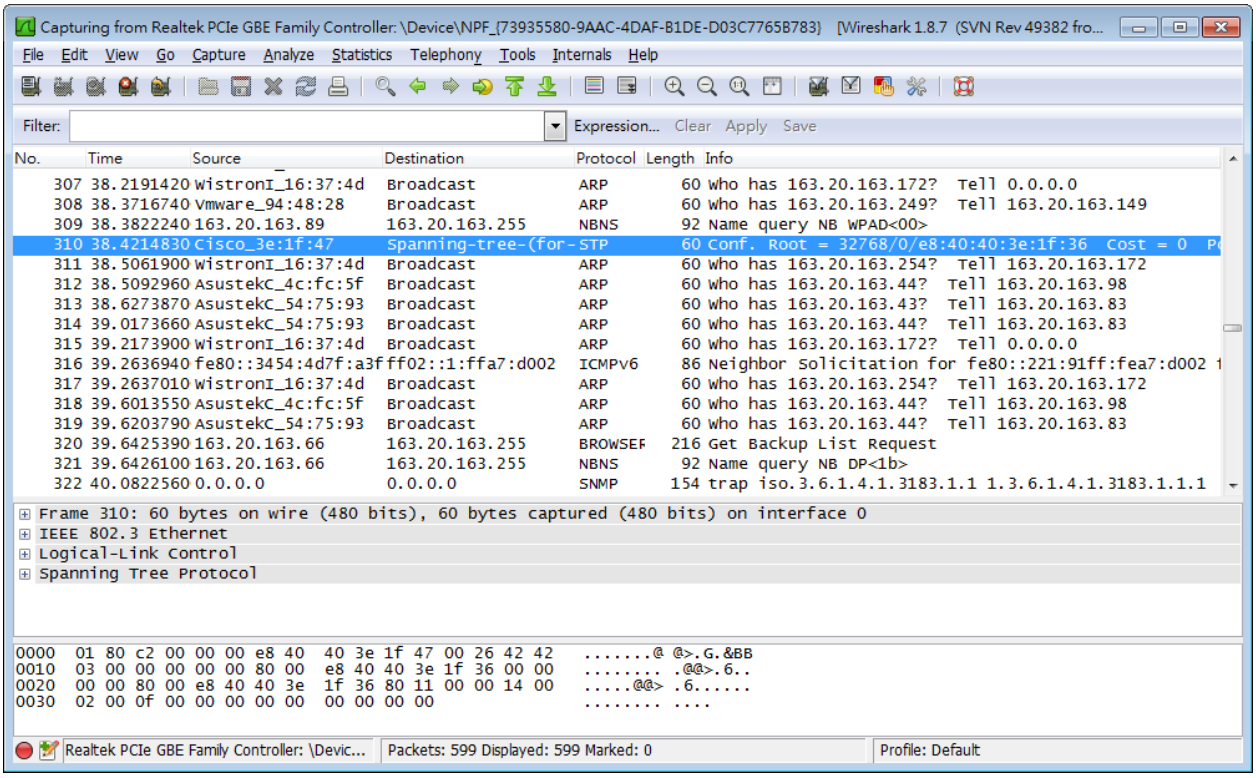


圖 26-Wireshark 封包過濾進行查驗檢核

伍、研究結果

警報紀錄表(Alarm log)對於符合異常的情況發出警報，但是在警報尚未排除時，相同的異常 IP 可能發生數次警報，因此在統計警報成效時，必須將重複 IP 先進行合併，警報值可以選擇輸出最大(Max)或最新值(Newer)，另外以**警報統計表**(Alarm stat)呈現：

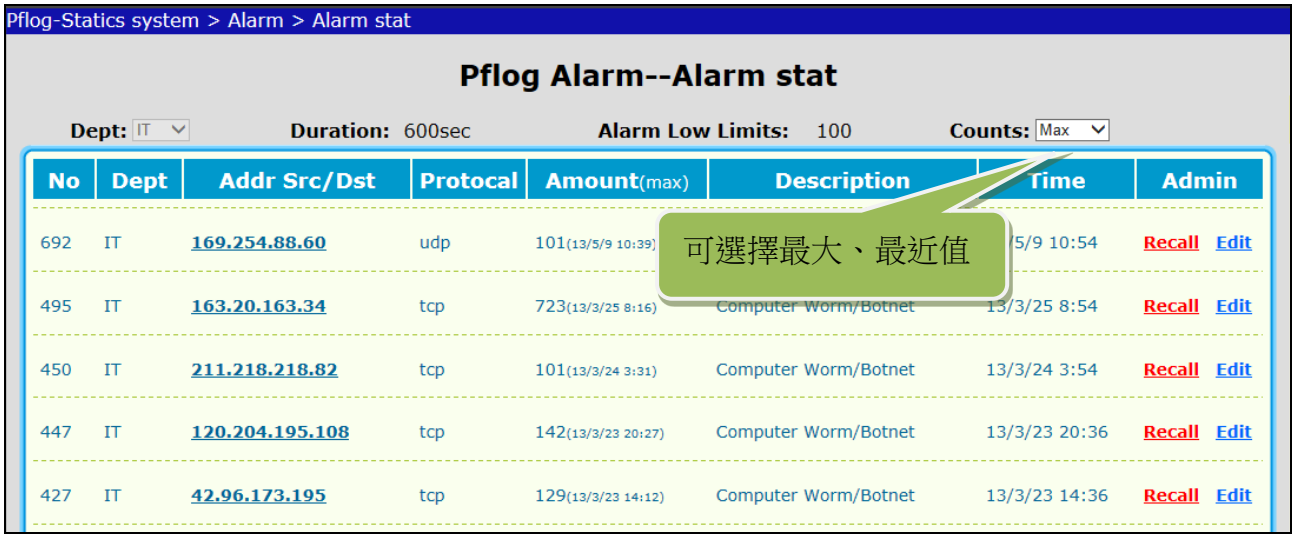
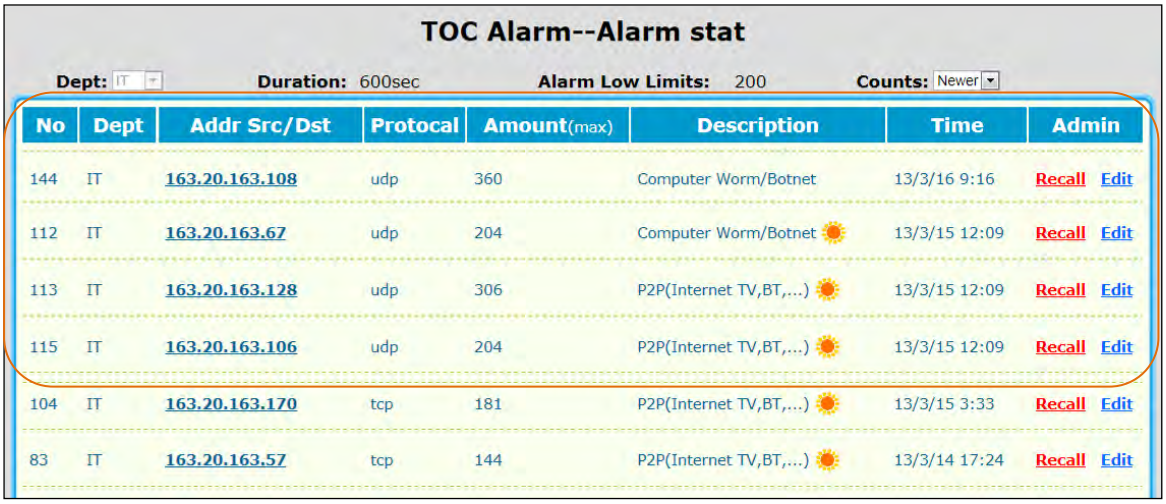


圖 28-警報統計表(IP 不重複)

一、 **警報實驗 1**，以下為警報分析設定

1. 分析期間：10 分鐘
2. 上限次數：200
3. 資料筆數：4



TOC Alarm--Alarm stat

Dept: IT Duration: 600sec Alarm Low Limits: 200 Counts: Newer

No	Dept	Addr Src/Dst	Protocal	Amount(max)	Description	Time	Admin
144	IT	163.20.163.108	udp	360	Computer Worm/Botnet	13/3/16 9:16	Recall Edit
112	IT	163.20.163.67	udp	204	Computer Worm/Botnet	13/3/15 12:09	Recall Edit
113	IT	163.20.163.128	udp	306	P2P(Internet TV,BT,...)	13/3/15 12:09	Recall Edit
115	IT	163.20.163.106	udp	204	P2P(Internet TV,BT,...)	13/3/15 12:09	Recall Edit
104	IT	163.20.163.170	tcp	181	P2P(Internet TV,BT,...)	13/3/15 3:33	Recall Edit
83	IT	163.20.163.57	tcp	144	P2P(Internet TV,BT,...)	13/3/14 17:24	Recall Edit

圖 29-實驗 1 警報統計表

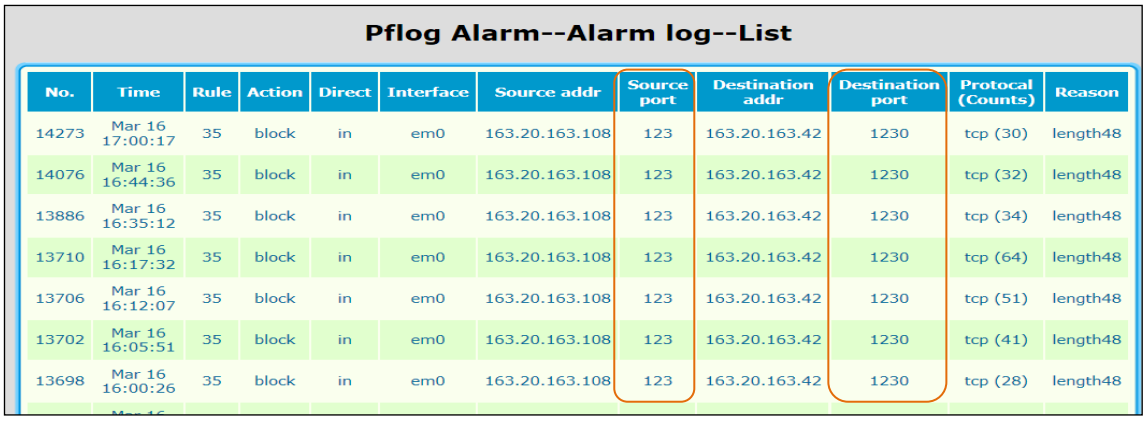
編號	來源 IP	協定類型	總數/時間	警報類型	正確	實際
1	163.20.163.108	udp	360	Worm/botnet	╳	print
2	163.20.163.67	tcp	204	Worm/botnet	○	botnet
3	163.20.163.128	udp	504	P2P	△	botnet
4	163.20.163.106	udp	204	Worm/botnet	○	botnet

警報正確率：75%

類型正確率：50%

4. 個別警報詳細分析：

(1) 163.20.163.108:連線 123->1230，為 HP 網路印表機運作，163.20.163.42 為本科 HP 5550C 網路印表機，另參照自 IP 分配表。IP 分配表另外可追踪警報位置。



Pflog Alarm--Alarm log--List

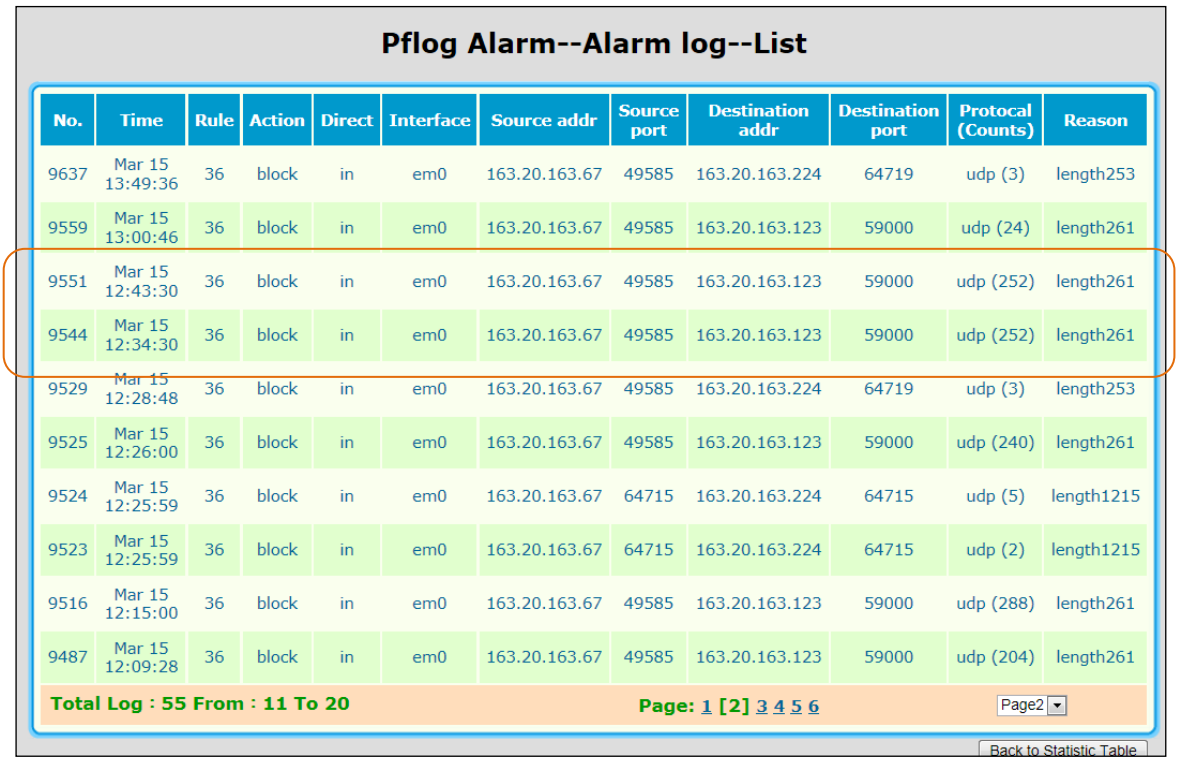
No.	Time	Rule	Action	Direct	Interface	Source addr	Source port	Destination addr	Destination port	Protocal (Counts)	Reason
14273	Mar 16 17:00:17	35	block	in	em0	163.20.163.108	123	163.20.163.42	1230	tcp (30)	length48
14076	Mar 16 16:44:36	35	block	in	em0	163.20.163.108	123	163.20.163.42	1230	tcp (32)	length48
13886	Mar 16 16:35:12	35	block	in	em0	163.20.163.108	123	163.20.163.42	1230	tcp (34)	length48
13710	Mar 16 16:17:32	35	block	in	em0	163.20.163.108	123	163.20.163.42	1230	tcp (64)	length48
13706	Mar 16 16:12:07	35	block	in	em0	163.20.163.108	123	163.20.163.42	1230	tcp (51)	length48
13702	Mar 16 16:05:51	35	block	in	em0	163.20.163.108	123	163.20.163.42	1230	tcp (41)	length48
13698	Mar 16 16:00:26	35	block	in	em0	163.20.163.108	123	163.20.163.42	1230	tcp (28)	length48

圖 30-網路印表機 HP 紀錄

資訊科 IP 分配表　　群組：CSD

IP	使用者	電腦名稱
163.20.163.30	曾老師	602B_自取名稱
163.20.163.31	鄭老師	608B_自取名稱
163.20.163.32	朱老師	604B_自取名稱
163.20.163.33	陳老師	607A_自取名稱
163.20.163.34	陳老師	606B_自取名稱
163.20.163.35	王老師	605A_自取名稱
163.20.163.36	盧老師	601A_自取名稱
163.20.163.37	褚老師	601B_自取名稱
163.20.163.38	林技士	603A_自取名稱
163.20.163.39	李老師	604A_自取名稱
163.20.163.40	林老師	606A_自取名稱
163.20.163.41	影印機-RICOH	
163.20.163.42	印表機-HP	
163.20.163.43	印表機-Epson	
163.20.163.44	影印機-Sharp	
163.20.163.45	翁老師	608A_自取名稱
163.20.163.46	劉老師	602A_自取名稱
163.20.163.47	科辦-Switch	
163.20.163.48	科辦-Switch	
163.20.163.49	機房-Server	
163.20.163.50	機房-Server	

表 8-資訊科 IP 分配表



Pflog Alarm--Alarm log--List

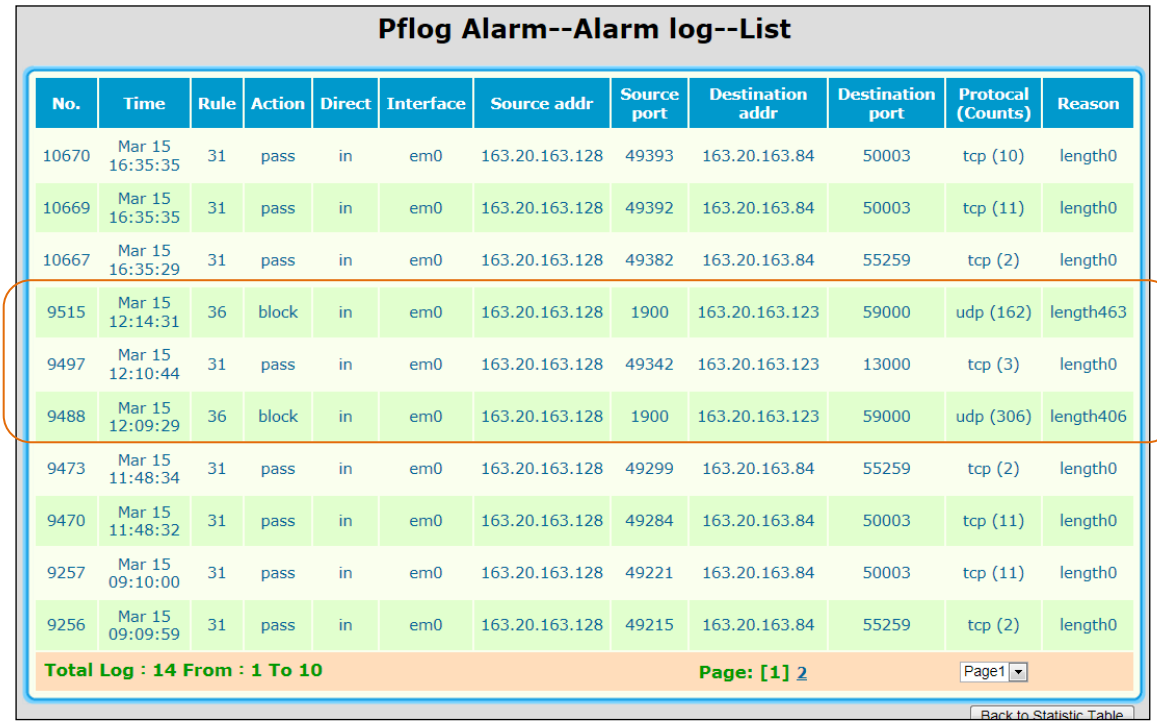
No.	Time	Rule	Action	Direct	Interface	Source addr	Source port	Destination addr	Destination port	Protocal (Counts)	Reason
9637	Mar 15 13:49:36	36	block	in	em0	163.20.163.67	49585	163.20.163.224	64719	udp (3)	length253
9559	Mar 15 13:00:46	36	block	in	em0	163.20.163.67	49585	163.20.163.123	59000	udp (24)	length261
9551	Mar 15 12:43:30	36	block	in	em0	163.20.163.67	49585	163.20.163.123	59000	udp (252)	length261
9544	Mar 15 12:34:30	36	block	in	em0	163.20.163.67	49585	163.20.163.123	59000	udp (252)	length261
9529	Mar 15 12:28:48	36	block	in	em0	163.20.163.67	49585	163.20.163.224	64719	udp (3)	length253
9525	Mar 15 12:26:00	36	block	in	em0	163.20.163.67	49585	163.20.163.123	59000	udp (240)	length261
9524	Mar 15 12:25:59	36	block	in	em0	163.20.163.67	64715	163.20.163.224	64715	udp (5)	length1215
9523	Mar 15 12:25:59	36	block	in	em0	163.20.163.67	64715	163.20.163.224	64715	udp (2)	length1215
9516	Mar 15 12:15:00	36	block	in	em0	163.20.163.67	49585	163.20.163.123	59000	udp (288)	length261
9487	Mar 15 12:09:28	36	block	in	em0	163.20.163.67	49585	163.20.163.123	59000	udp (204)	length261

Total Log : 55 From : 11 To 20 Page: 1 [2] 3 4 5 6 Page2

Back to Statistic Table

圖 31－**殭屍網路**(Botnet)紀錄，圈內紀錄有大量連線數

(2) 163.20.163.67：在同一時段內同時大量攻擊 163.20.163.123，參照上圖 Counts 大量連線時，為**殭屍網路**(Botnet)之特性。



Pflog Alarm--Alarm log--List

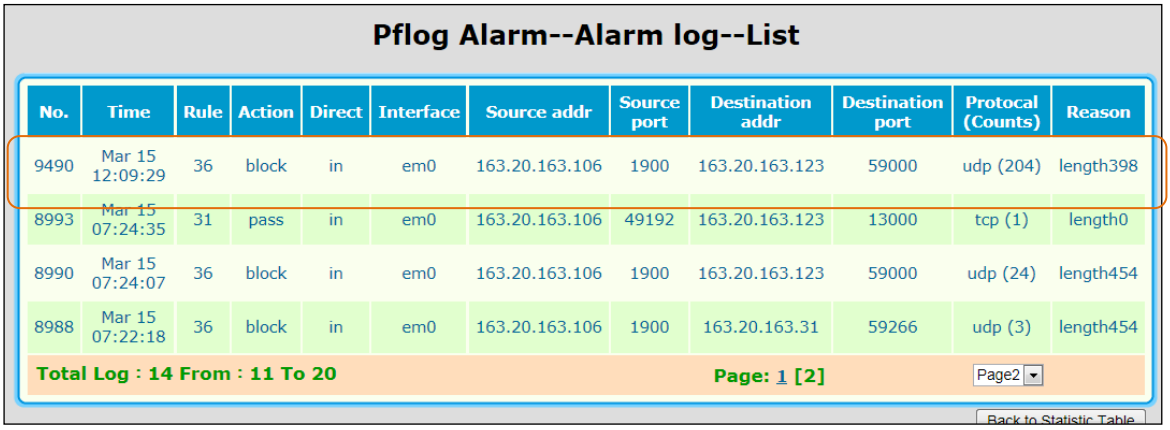
No.	Time	Rule	Action	Direct	Interface	Source addr	Source port	Destination addr	Destination port	Protocal (Counts)	Reason
10670	Mar 15 16:35:35	31	pass	in	em0	163.20.163.128	49393	163.20.163.84	50003	tcp (10)	length0
10669	Mar 15 16:35:35	31	pass	in	em0	163.20.163.128	49392	163.20.163.84	50003	tcp (11)	length0
10667	Mar 15 16:35:29	31	pass	in	em0	163.20.163.128	49382	163.20.163.84	55259	tcp (2)	length0
9515	Mar 15 12:14:31	36	block	in	em0	163.20.163.128	1900	163.20.163.123	59000	udp (162)	length463
9497	Mar 15 12:10:44	31	pass	in	em0	163.20.163.128	49342	163.20.163.123	13000	tcp (3)	length0
9488	Mar 15 12:09:29	36	block	in	em0	163.20.163.128	1900	163.20.163.123	59000	udp (306)	length406
9473	Mar 15 11:48:34	31	pass	in	em0	163.20.163.128	49299	163.20.163.84	55259	tcp (2)	length0
9470	Mar 15 11:48:32	31	pass	in	em0	163.20.163.128	49284	163.20.163.84	50003	tcp (11)	length0
9257	Mar 15 09:10:00	31	pass	in	em0	163.20.163.128	49221	163.20.163.84	50003	tcp (11)	length0
9256	Mar 15 09:09:59	31	pass	in	em0	163.20.163.128	49215	163.20.163.84	55259	tcp (2)	length0

Total Log : 14 From : 1 To 10 Page: [1] 2 Page1

Back to Statistic Table

圖 32-**殭屍網路**(Botnet)紀錄，圈內紀錄有大量連線數

(3) 163.20.163.128：在同一時段內同時大量攻擊 163.20.163.123，為**殭屍網路**(Botnet)之特性，與前述第 2 點相同。



Pflog Alarm--Alarm log--List

No.	Time	Rule	Action	Direct	Interface	Source addr	Source port	Destination addr	Destination port	Protocal (Counts)	Reason
9490	Mar 15 12:09:29	36	block	in	em0	163.20.163.106	1900	163.20.163.123	59000	udp (204)	length398
8993	Mar 15 07:24:35	31	pass	in	em0	163.20.163.106	49192	163.20.163.123	13000	tcp (1)	length0
8990	Mar 15 07:24:07	36	block	in	em0	163.20.163.106	1900	163.20.163.123	59000	udp (24)	length454
8988	Mar 15 07:22:18	36	block	in	em0	163.20.163.106	1900	163.20.163.31	59266	udp (3)	length454

Total Log : 14 From : 11 To 20 Page: 1 [2] Page2

Back to Statistic Table

圖 33-**殭屍網路**(Botnet)紀錄，圈內紀錄有大量連線數

(4) 163.20.163.106：在同一時段內同時大量攻擊 163.20.163.123，為**殭屍網路**(Botnet)之特性，與前述第 2 點相同。

二、**警報實驗 2**，以下為警報分析設定

1. 分析期間：10 分鐘
2. 上限次數：100
3. 資料筆數：134，詳如下表（重複 IP 不列）：

編號	來源 IP	協定類型	總數/時間	警報類型	正確	實際
1	163.20.163.126	udp	200	P2P	△	botnet
2	163.20.163.224	tcp	145	Worm/botnet	╳	ssh
3	163.20.163.67	udp	504	P2P	△	botnet
4	163.20.163.109	udp	1260	Worm/botnet	○	botnet
5	163.20.163.89	udp	744	Worm/botnet	○	botnet
6	163.20.163.67	udp	502	P2P	△	botnet
7	163.20.163.128	udp	468	P2P	△	botnet
8	163.20.163.106	udp	204	P2P	△	botnet
9	163.20.163.125	tcp	744	P2P	╳	print
10	163.20.163.94	udp	127	P2P	○	P2P

警報正確率：80%

類型正確率：30%

三、**警報觀察平面圖**，一旦發生警報在異常電腦顯示警報閃燈，可即時查對異常電腦位置及相關資訊。

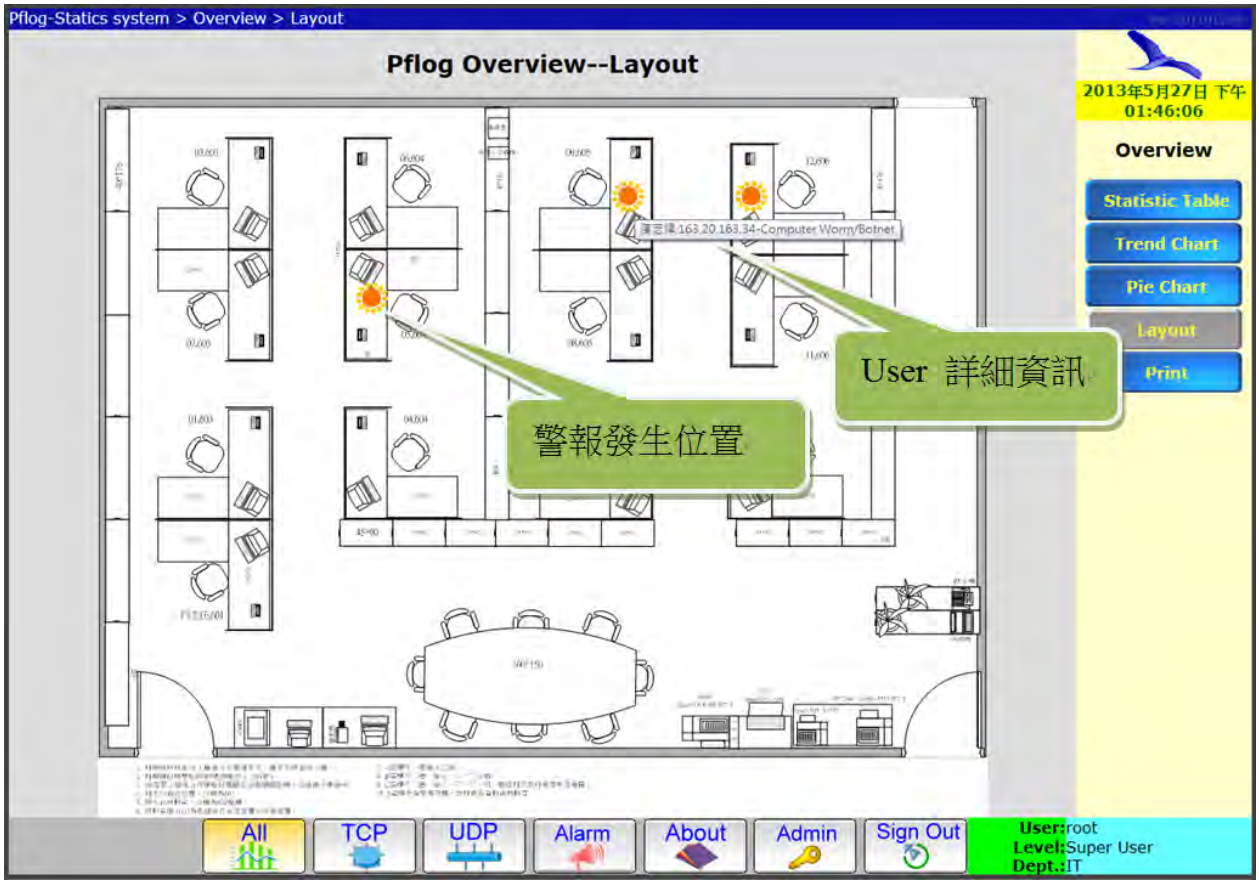


圖 34-警報觀察平面圖(點警報發生位置有**詳細資訊**)

四、網路管理成效分析

一旦網路發生**異常警報**可立即在**警報觀察平面圖**找出異常電腦位置，再由詳細列表中了解實際警報狀況，處理上可電話通知，或派維修人員協助。這樣的處理方式仍然有一缺點，如果沒有在電腦前監控警報網頁，則無法立即發現異常。下表統計所發生警報之反應時間，可由偵測到第一筆異常，與發生警報之時間來計算：

編號	來源 IP	警報類型	異常時間	警報時間	反應時間(分)
1	163.20.163.111	Worm/botnet	13/3/19 12:01	13/3/19 12:09	8
2	163.20.163.108	Worm/botnet	13/3/16 9:32	13/3/16 9:36	4
3	163.20.163.108	Worm/botnet	13/3/15 12:09	13/3/15 12:18	9
4	163.20.163.67	P2P	13/3/15 12:09	13/3/15 12:18	9
5	163.20.163.128	P2P	13/3/15 12:09	13/3/15 12:18	9
6	163.20.163.106	P2P	13/3/15 12:09	13/3/15 12:18	9
7	163.20.163.170	P2P	13/3/15 3:33	13/3/15 3:36	3
8	163.20.163.57	P2P	13/3/14 17:24	13/3/14 17:27	3
9	163.20.163.125	P2P	13/3/14 17:24	13/3/14 17:27	3
10	163.20.163.17	Worm/botnet	13/3/14 17:24	13/3/14 17:27	3
				平均	6

表 10-警報反應時間表

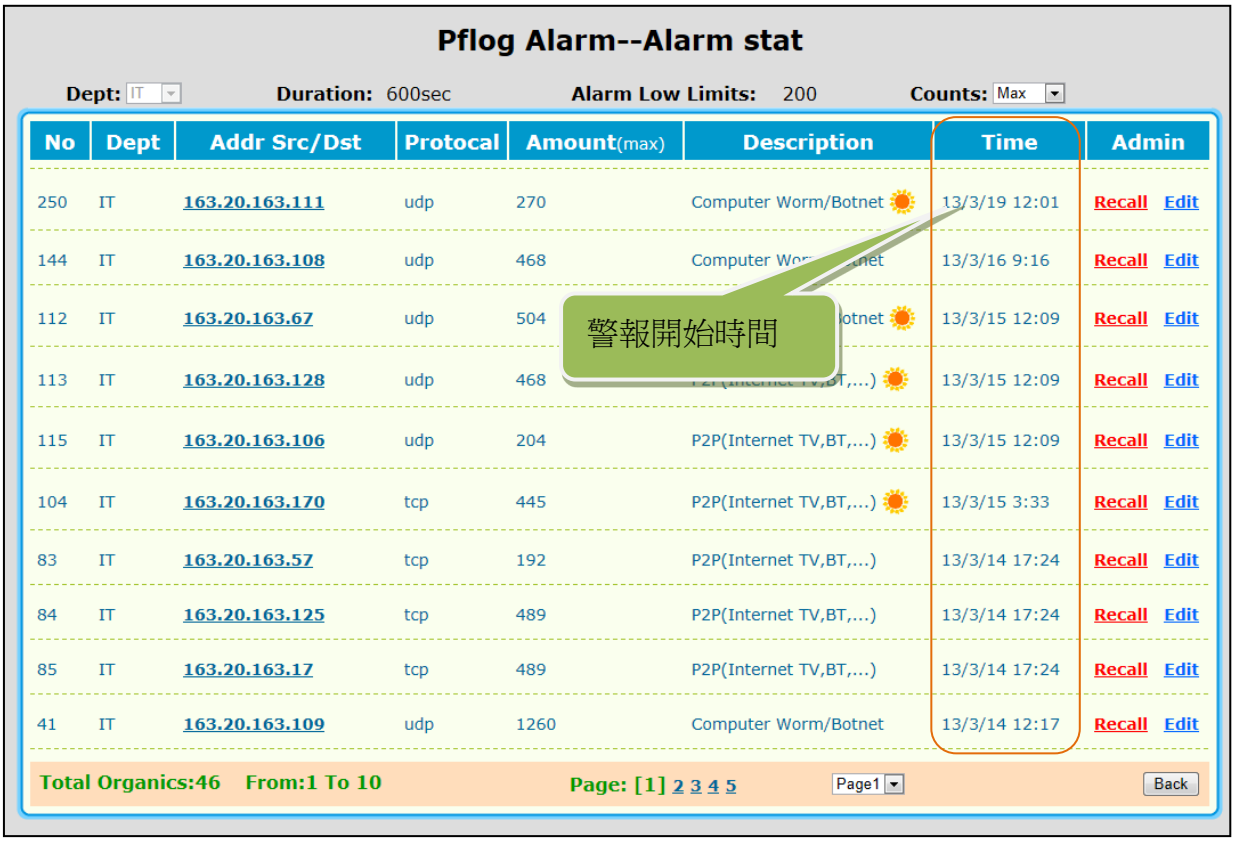


圖 35-警報紀錄對照時間

陸、討論

初期計劃分析單純的超量連線紀錄，在考慮 TCP/IP 服務的複雜度，決定先分析埠口 1024 至埠口 65535 這類未定義服務埠口，後續的處理又碰到區域網路(LAN)中，大量的多點傳送(Multicast)紀錄、網路印表機(net printer)、網路芳鄰(NetBios over TCP/IP)及網際網路群組管理協定(IGMP)，加上 TCP 維持連線確認的 ACK，一度讓人摸不著頭緒。後來一一到網路查詢資料，加上老師的解說，終於將大部份此類狀況排除或**列入錯誤警報**。

這次研究有一部分是加入異常警報程式，除了釐清各種異常的狀況，還要推出程式的演算法，尤其是在統計的時間範圍及可能是異常的最大上限值，這必須配合實驗出正確率的成果，讓人體會深夜爬電腦格子程式除錯的痛苦，現在有那麼多軟體可以使用，不知道是多少人的血汗結晶的成果，真的要好好珍惜。

雖然這次的成果中可以在分析網頁中查到警報，然而還是要到異常使用的電腦前面將異常排除，在人工排除之前，如果可以增加讓防火牆自動加入**限制頻寬**的機制，如此一來可以等異常排除後，再行回復限制頻寬，可以提升整體網路連線服務品質，在未來也許可以考慮增加此一機制，以 pf 防火牆設定頻寬限制方式如下：

```
# Queueing
altq on $ext_if bandwidth 100Mb cbq queue {cc_hosts,others}
#設定對外頻寬 100Mbps，有 cc_host 及 others 二個設定，可加入防火牆規則之中，來指定頻寬
queue cc_hosts bandwidth 40Mb cbq(default)
#設定 cc_host 的最大頻寬為 40Mbps
queue others bandwidth 60Mb cbq(ecn) {users,custody_users,bad_users}
#設定 cc_host 的最大頻寬為 60Mpbs，以下為在 others 的子設定，有 users,custody_users,bad_users，3
個設定
        queue users bandwidth 50Mb cbq(red)
        #設定 users 的最大頻寬為 50Mbps，頻寬管理為 red(隨機早偵測)方式
        queue custody_users bandwidth 2Mb cbq(red)
        #設定 custody_users 的最大頻寬為 2Mbps，頻寬管理為 red 方式
        queue bad_users bandwidth 100Kb cbq(red)
        #設定 bad_users 的最大頻寬為 100kbps，頻寬管理為 red 方式
pass    out on $ext_if proto { tcp udp } from port domain to $local_net    queue users
#引入 users 頻寬設定
```

表 11- pf 防火牆的頻寬管理功能設定(學校的舊防火牆設定值)

另外有一個提升即時性構想，若是可以使用 USB 加上 I/O 電路，將警示 LED 連接到各電腦上面，可以**使用 LED 的燈號當做警報**，這樣可以即時提醒 User 可能的異常，這也許是一個不錯的未來方案。或者自動發即時訊息到 Facebook，透過網路即時通知 User。

柒、結論

經過這次**超量網路連線分析**的實驗，過程雖然辛苦，但是可以將網路 80%的大量連線異常找出來，這樣對於第一線的網路管理應該有很大的幫助，在經費日益拮据之下可以使用這個簡單有效的方法維持網路的正常運作。

因為**超量網路連線分析**主要針對影響網路運作之異常大量連線進行分析。所以可以避免大量資料處理；不易使系統超出負荷且可避免複雜性資料的解讀不易。再來可完全的針對校園需求，以客製化的設定 User 位置，在警報平面圖的功能上，可迅速找出問題電腦的故障位置，不用人工比對異常電腦位置，以下列出本次超量連線實驗的特點：

超量網路連線分析研究特色表

編號	特色項目	特色說明
1	分析異常大量連線	僅針對影響網路頻寬及負荷的超量連線進行分析
2	可分散處理負載	可將 web 站、資料庫、防火牆安裝在不同電腦，分工處理
3	介面擴充容易	可自行擴充一般網路介面卡或光纖卡
4	軟體更新快	採自由軟體更新速度快，約一季更新一個版本

5	軟體安裝設定容易	相關自由軟體有完整的說明文件，並且有大量網友的討論
6	可建立客製化資訊	可自行定義 User IP 及所在平面圖位置，追踪容易
7	可搭配防火牆設定	使用安全性極高的 pf 防火牆，規則可立即加入
8	可自動頻寬限制	對於發生警報的使用端電腦，可自動頻寬限制，減少影響
9	硬體要求低	一般個人電腦即可勝任，硬體門檻低，未來升級容易
10	程式軟體彈性高	程式軟體自行開發，可依需要調整功能，具有彈性

表 11-超量網路連線分析研究特色表

另外這次實驗中需要不斷的找出問題並且解決問題，除了在研究經驗上增長不少，也讓我們對於網路運作的細節也有更深一層的認識，下面把所面臨的四項議題分別討論：

一、 分析量大、系統無法負荷

如果有一部超級電腦，再加上無限大的資料庫空間，也許就可以全面對網路封包進行分析。這一次僅僅對資訊科 20 台左右的電腦進行紀錄分析，紀錄的範圍也僅限於未定義服務埠(Unknown ports)超量的部份，就發現隨著分析網路資料量不斷增加，使得伺服器處理上產生瓶頸；首先是寫入資料庫時間變長，當防火牆紀錄檔 pflog 超過 10MB，匯入及計算時間將超過 10 分鐘，因而會重疊到下一次的匯入時間。當統計範圍加大 PHP 顯示也開始要等待，有的甚至超過 30 秒，從伺服器觀察在系統資源的使用也急遽上升。

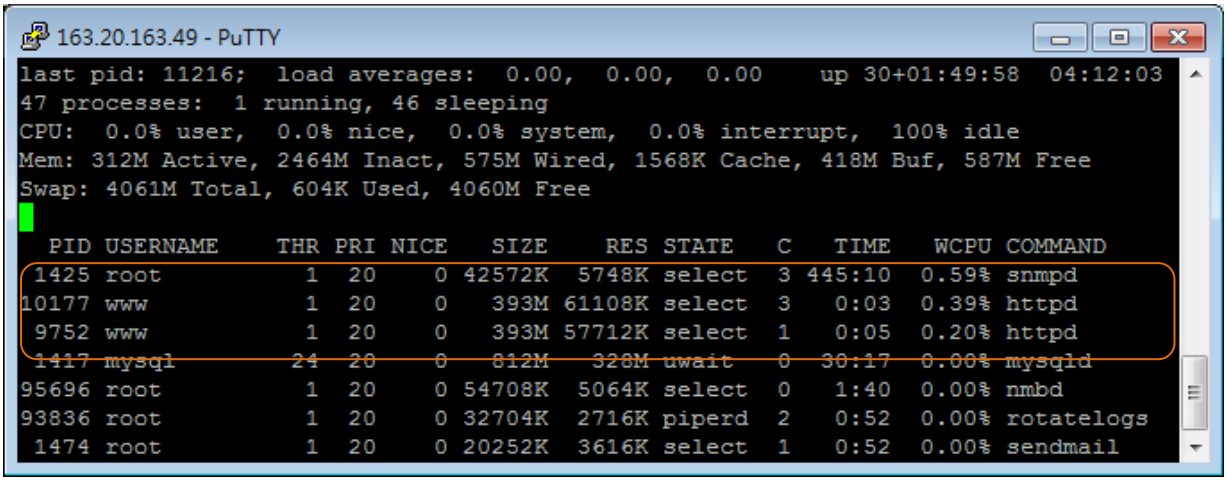


圖 36-伺服器使用資源前 7 筆程式

後來採取的方案是將 MySQL 資料庫與 PHP 網站分開，另外架設在不同的伺服器上，透過分散處理來分擔工作，在網頁運作上才比較流暢。

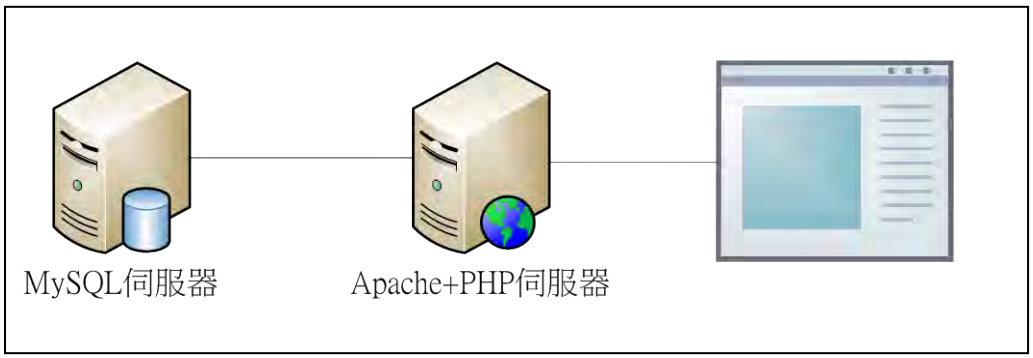


圖 37-MySQL 伺服器與 Web 伺服器分開運作

二、 TCP/IP 服務繁多、分析難度高

從原來已知服務埠(Well-Known Ports)，至今已有很多網路服務埠不斷加入，就連 1024-65535 未知服務埠(UKnown ports)也有 450 以上埠口被定義為特定服務，很肯定的未來新的服務一定會被加入，分析也要重新定義。再來 IPV6 也讓網路從定址的基礎上煥然一新，以及 IPV6 在區域網路採用的多點傳送(Multicast)，運作，在初期超量連線實驗的紀錄時也曾偵測到，因此對於新的服務在更新後必需隨之調整，才能正確分辨。

三、 加密連線無法分辨

常見的加密連線 SSL、SSH，這一類的連線就算是把封包打開來看，也難以找出規則，不禁令人擔憂，萬一未來殭屍網路或木馬病毒也採用加密式連線，這會讓網路分析的工作更加困難，對照目前的超量連線檢測僅解決網路順暢，這個議題需更加深入。

四、 非 DDOS 特洛伊木馬程式，難以從流量偵測

同樣使用網路運作的特洛伊木馬程式很少以大量網路連線出現，如果想要在網路上偵測，必須以完整封包內容來解析，才有可能分析辨別。不過這一類型的危害程式，對頻寬的影響不太，在維持網路順暢的管理上優先性較低。

捌、參考資料及其他

一、中文部分

【一本書】

施威銘工作室(2011)。**網路概論 2012**。台北市：施標出版社。

張亞飛(2012)。**PHP+MySQL 全能權威指南**。台北市：上奇資訊股份有限公司。

尹國正(2013)。**第 2 版 PHP+MySQL 程式設計**。新北市：新文京開發出版股份有限公司。

楊水清(2008)。**深入淺出 JavaScript 與 Ajax 網頁設程式設計**。台北縣:博碩文化股份公司。

文淵閣工作室（2008）。**挑戰 PHP5/MySQL 程式設計樂活學**。台北市：基峰資訊股份有限公司。

【一本書】

W.Richard Stens(2009)。**TCP/IP Illuxtrated，Volumel 中譯本**。台北市：和碩科技文化有限公司。

Michael w.Lucas(2004)。**OpenBSD 完全探索**。台北市：上奇科技股份有限公司。

二、網路資源

(一) 中文部分

【安裝及設定說明文件】

PHP 教學資源站。http://163.20.163.49/

(二) 英文部分

【安裝及設定說明文件】

The FreeBSD Foundation。http://www.freebsd.org/

【HTTP SERVER 安裝及設定說明文件】

The Apache Software Foundation。http://www.apache.org/

【安裝及設定說明文件】

MySQL Server Database。http://www.mysql.com/

【PHP Language 安裝及設定說明文件】

The PHP Group。http://www.php.net/

【PF 安裝及設定說明文件】

The OpenBSD project 。http://www.openbsd.org/

【評語】091001

1. 作品題目明確且實作完整度高，且三位合作同學分工合作合宜，值得嘉許。

2. 網路預警偵測是一重要的資訊安全課題，其技術涵蓋範圍相當廣，同學們對於 DDOS 攻擊已有完整的認識，未來可多加入其他攻擊的分析，增進系統實用性。

3. 本作品提供了視覺化的偵測結果顯示方式，方便管理者快速確認問題電腦並加以排除。

4. 建議針對網路預警成效做更為完整的實驗，必要時，可與其他類似預警軟體做一比較。除了正確率外，宜將錯誤結果進一步分類，以深入了解系統限制及改進之處。

5. 建議海報與口頭報告要多注重科學探究與實驗層面的討論，避免僅為實作作品的呈現。