



# Fortinet®-Training For 澎湖縣教網中心 NGN

力麗科技 劉士豪

[timliu@llt.com.tw](mailto:timliu@llt.com.tw)

March 2010

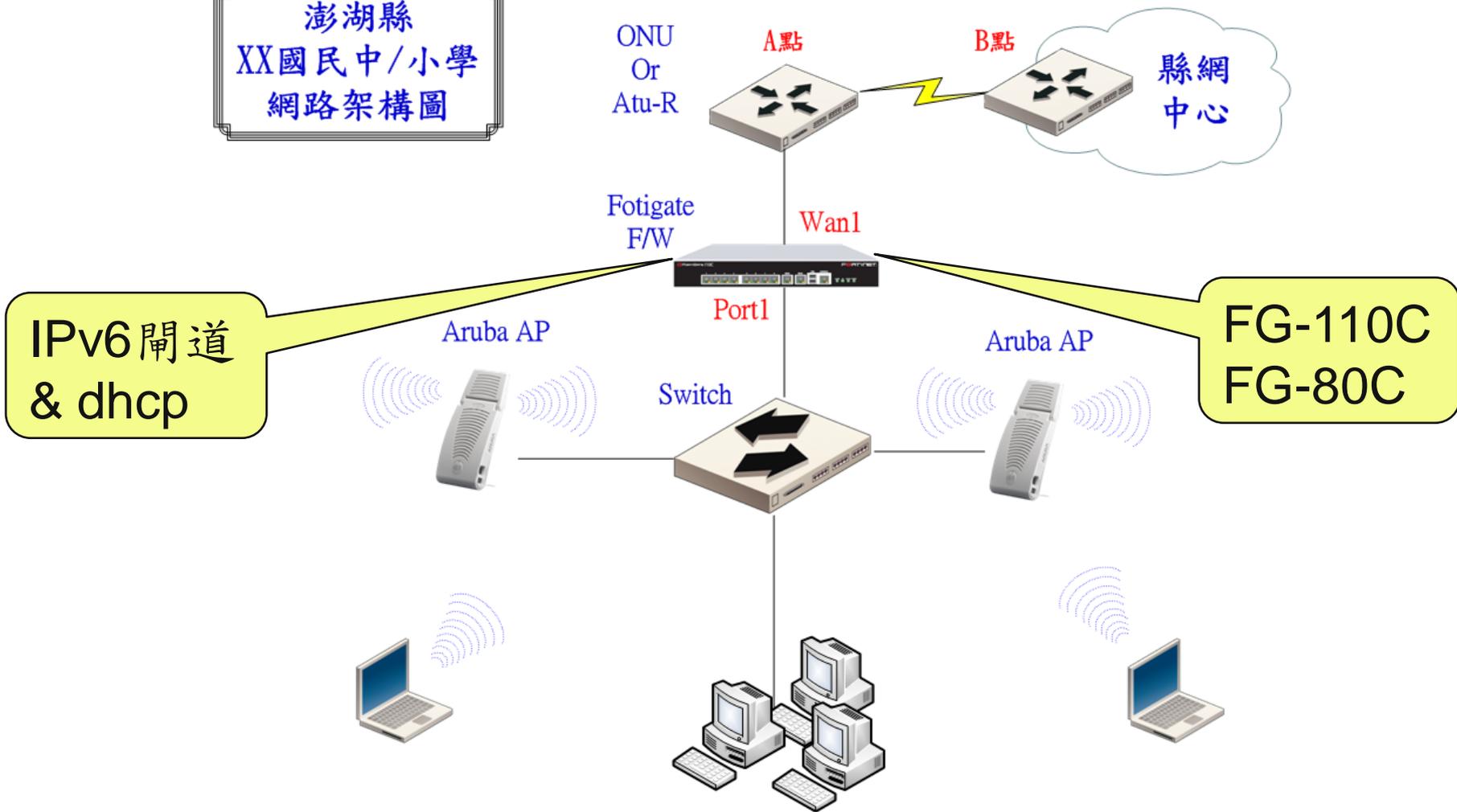


# Agenda

- 本案學校UTM網路架構
- 防火牆管理
- LAB

# 網路架構

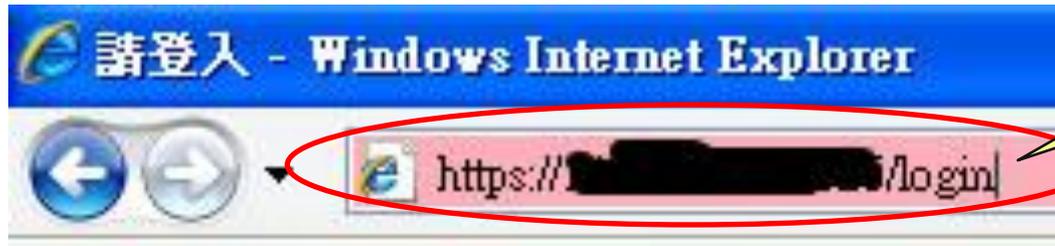
澎湖縣  
XX國民中/小學  
網路架構圖





# 防火牆管理

# Web Login



[https://fortigate\\_ip](https://fortigate_ip)

 此網站的安全性憑證有問題。

此網站出示的安全性憑證並非由信任的憑證授權單位所發行。  
此網站出示的安全性憑證是為其他網站的位址所發行的。

安全性憑證問題可能表示其他人可能正在嘗試欺騙您，或是攔截您的資料。

我們建議您關閉此網頁，而且不要繼續瀏覽此網站。

- 按這裡關閉此網頁。
- 繼續瀏覽此網站 (不建議)。
- 其他資訊

A screenshot of a web login page. The page has a light blue background with a grid pattern. The text "請登入..." is at the top. Below it are the labels "用戶名" and "密碼". There are two input fields for the username and password, both of which are circled in red. A blue button labeled "登錄" is positioned to the right of the password field.

# 系統管理-狀態(1/4)

### 系統資訊

序號	FG100C3G09610049
已開機時間	90 天(數) 5 小時(數) 18 分(數)
系統時間	Tue Mar 2 16:05:33 2010 <a href="#">[更改]</a>
HA 狀態	單機模式 <a href="#">[設定]</a>
主機名稱	mkjh-UTM-FG110C <a href="#">[更改]</a>
韌體版本	v4.0,build0185,091020 (MR1 Patch 1) <a href="#">[更新]</a>
FortiClient 版本	未知
操作模式	NAT <a href="#">[更改]</a>
虛擬區域	關閉 <a href="#">[啓用]</a>
目前在線管理者	1 <a href="#">[詳情]</a>
目前的使用者	admin <a href="#">[密碼變更]</a>

### 授權資訊

#### 支援合約

Registration	連線失敗	<input type="checkbox"/>
--------------	------	--------------------------

#### FortiGuard 訂閱

防毒	連線失敗 <a href="#">[設定]</a>	<input type="checkbox"/>
AV 病毒碼	9.00795 (更新 2008-12-08) <a href="#">[更新]</a>	
進階掃描資料設定	0.00000 (更新 2003-01-01)	
入侵防禦	連線失敗 <a href="#">[設定]</a>	<input type="checkbox"/>
IPS 特徵碼	2.00593 (更新 2009-02-05) <a href="#">[更新]</a>	
網頁過濾	連線失敗 <a href="#">[設定]</a>	<input type="checkbox"/>
郵件過濾	連線失敗 <a href="#">[設定]</a>	<input type="checkbox"/>
管理及分析服務	連線失敗	<input type="checkbox"/>
服務帳號 ID	<a href="#">[更改]</a>	

#### 虛擬區域

虛擬領域允許使用	10
----------	----

#### 終端用戶安全

FortiClient軟體	連線失敗
應用程式特徵碼檔案	1.131 (更新 2009-10-21)

### 設備作業

FortiGate 110C status: 1 2 3 4 5 6 7 8 WAN1 WAN2

[重新啓動](#) [關機](#)

### 警告訊息控制台

- 2009-12-09 23:24:53 Failed admin authentication attempt for admin
- 2009-12-02 18:54:01 Failed admin authentication attempt for admin
- 2009-12-02 18:53:47 Failed admin authentication attempt for admin
- 2009-12-02 18:53:39 Failed admin authentication attempt for admin
- 2009-12-02 18:51:37 系統重新啓動

### 記錄與檔案統計 (從 2009-12-02 18:51:59)

#### DLP檔案記錄 -- 平均 0 B 每天 since last reset

HTTP	0 網頁瀏覽	<a href="#">[詳情]</a>
HTTPS	0 網頁瀏覽	<a href="#">[詳情]</a>
電子郵件	0 寄出郵件	<a href="#">[詳情]</a>
	0 收取郵件	
FTP	0 網頁瀏覽	<a href="#">[詳情]</a>
	0 檔案上傳	
	0 檔案下載	
IM	0 傳送檔案	<a href="#">[詳情]</a>
	0 交談連線	
	0 交談訊息	

# 系統管理-狀態(2/4)

**授權資訊**

**支援合約**

Registration	連線失敗
--------------	------

**FortiGuard 訂閱**

防毒	連線失敗 <a href="#">[設定]</a>
AV 病毒碼	9.00795 (更新 2008-12-08) <a href="#">[更新]</a>
進階掃描資料設定	0.00000 (更新 2003-01-01)
入侵防禦	連線失敗 <a href="#">[設定]</a>
IPS 特徵碼	2.00593 (更新 2009-02-05) <a href="#">[更新]</a>
網頁過濾	連線失敗 <a href="#">[設定]</a>
郵件過濾	連線失敗 <a href="#">[設定]</a>
管理及分析服務	連線失敗
服務帳號 ID	<a href="#">[更改]</a>

**虛擬區域**

虛擬領域允許使用	10
----------	----

**終端用戶安全**

FortiClient軟體	連線失敗
應用程式特徵碼檔案	1.131 (更新 2009-10-21)

**命令列控制台 (中斷)**

```
啟動連線...
```

**2009-12-09 23:24:53 Failed admin authentication attempt for admin**

**2009-12-02 18:54:01 Failed admin authentication attempt for admin**

**2009-12-02 18:53:47 Failed admin authentication attempt for admin**

**2009-12-02 18:53:39 Failed admin authentication attempt for admin**

**2009-12-02 18:51:37 系統重新啟動**

**記錄與檔案統計 (從 2009-12-02 18:51:59)**

**DLP檔案記錄 -- 平均 0 B 每天 since last reset**

HTTP	0 網頁瀏覽	<a href="#">[詳情]</a>
HTTPS	0 網頁瀏覽	<a href="#">[詳情]</a>
電子郵件	0 寄出郵件	<a href="#">[詳情]</a>
	0 收取郵件	
FTP	0 網頁瀏覽	<a href="#">[詳情]</a>
	0 檔案上傳	
	0 檔案下載	
IM	0 傳送檔案	<a href="#">[詳情]</a>
	0 交談連線	
	0 交談訊息	
VoIP	0 訊息	<a href="#">[詳情]</a>
全部	0 B since last reset	

**記錄 -- 平均 47 MB (298963 messages) 每天 since last reset**

流量	26805332 允許通過流量	<a href="#">[詳情]</a>
	40653 被阻擋流量	
病毒記錄	0 病毒攔截	<a href="#">[詳情]</a>
IPS	0 攻擊阻斷	<a href="#">[詳情]</a>
Email	0 垃圾郵件識別	<a href="#">[詳情]</a>
Web	0 網頁封鎖	<a href="#">[詳情]</a>
資料外洩防護	0 資料外洩	<a href="#">[詳情]</a>
應用程式控制	0 應用程式控制訊息	<a href="#">[詳情]</a>
事件	26207 發生的事件	<a href="#">[詳情]</a>
全部	4 GB (26872192 messages) since last reset	

# 系統管理-狀態(3/4)



# 系統管理-狀態(4/4)



# 管理員設置

- 管理帳號/密碼  
新增/刪除/密碼修改/權限調整

管理員	信任主機	許可權	類型	
admin	0.0.0.0/0, ::/0	super_admin	本地	 
cht	0.0.0.0/0, ::/0	super_admin	本地	  
llt	0.0.0.0/0, ::/0	super_admin	本地	  
phc	0.0.0.0/0, ::/0	super_admin	本地	  

# 系統維護-備份與恢復

- UTM 設定值備份/還原

WEB CONFIG

系統管理

- 狀態
- 網路
- DHCP
- 設定
- 管理員設置
- 憑證
- 系統維護
- 路由設定
- 防火牆
- UTM

備份與恢復 修訂備份檔 Scripts FortiGuard

系統設定 (上次備份: Wed Dec 9 15:30:12 2009)

備份

備份設定至:

本地磁碟機  FortiManager  USB 隨身碟

設定檔案加密

密碼

確認

還原

還原設定從:

本地磁碟機  FortiManager  USB 隨身碟

檔案名稱:  瀏覽...

密碼

備份 還原

備份時  
不要設密碼

# 防火牆策略

- 防火牆策略

來源介面/來源ip/目的介面/目的ip/[防護內容]/動作

修改 調整順序

刪除 插入

狀態	ID	來源	目的	排程	服務	防護內容表	採取行動
▼ internal -> wan1 (1)							
<input checked="" type="checkbox"/>	1	all	all	always	ANY		ACCEPT    
▼ wan1 -> internal (1)							
<input checked="" type="checkbox"/>	2	all	all	always	ANY		ACCEPT    

# 防火牆策略~設定

介面/ip/動作

不要啟用  
NAT

F/W log(日誌)

建立輸出策略

來源介面/域名	dmz	
來源位址名稱	all	多個
目的介面/域名	internal	
目的位址名稱	all	多個
排程	always	
服務	ANY	多個
採取行動	ACCEPT	

NAT       動態 IP Pool

開啓用戶政策

保護內容表      unfiltered

流量控制      [請選擇]

反向流量塑型      [請選擇]

根據IP的流量塑型      [請選擇]

紀錄合法流量

啓動終端用戶NAC      [請選擇]

註解 (最多 63 字元)

允許      取消

# 防火牆位址



WEB CONFIG

系統管理  
路由設定  
防火牆  
防火牆策略  
位址  
服務  
時間表  
流量塑型  
虛擬IP

位址 位址群組

新增

名稱	位址 / 完全網域名稱	介面	
網路位址/遮罩			
all	0.0.0.0/0.0.0.0	任意	
網路位址範圍			
SSLVPN_TUNNEL_ADDR1	10.0.0.[1-10]	任意	
IPv6			
all	::/0		

位址 →  
ip/ip範圍/  
網段/網址



系統管理  
路由設定  
防火牆  
防火牆策略  
位址  
服務  
時間表  
流量塑型

位址 位址群組

新設位址

位址名稱: pc1

類型: 子網段/網路位址範圍

子網段/網路位址範圍: 0.0.0.0/0.0.0.0

介面: 任何

允許 取消

# 防火牆位址~群組

位址 位址群組

新增位址群組

群組名稱

可用位址:

SSLVPN\_TUNNEL\_ADDR1  
all

↓ ↑

成員:

允許 取消

自訂群組→  
可選擇目前列表  
的位址組成位址  
群組

# 防火牆服務~預設服務



The screenshot displays the 'WEB CONFIG' interface for a Fortinet firewall. The left sidebar contains a navigation menu with the following items: 系統管理, 路由設定, 防火牆 (highlighted), 防火牆策略, 位址, 服務 (highlighted), 時間表, 流量塑型, 虛擬IP, 負載平衡, 保護內容表, UTM, VPN, 使用者認證, and Endpoint NAC. The main content area is titled '預設服務' and is divided into three columns: '預設服務', '用戶自訂', and '服務群組'. The '預設服務' column lists various protocols, and the '服務群組' column lists their corresponding ports and protocols.

預設服務	用戶自訂	服務群組
ESP		IP/50
FINGER		TCP/79
FTP		TCP/21
FTP_GET		TCP/21
FTP_PUT		TCP/21
GOPHER		TCP/70
GRE		IP/47
H323		TCP/1720,1503 UDP/1719
HTTP		TCP/80
HTTPS		TCP/443
ICMP_ANY		ICMP/ANY
IKE		UDP/500,4500
IMAP		TCP/143
IMAPS		TCP/993
INFO_ADDRESS		ICMP/17
INFO_REQUEST		ICMP/15
IRC		TCP/6660-6669
Internet-Locator-Service		TCP/389
L2TP		TCP/1701 UDP/1701

# 防火牆服務~自訂服務

預設服務 用戶自訂 服務群組

### 新增客制服務

名稱

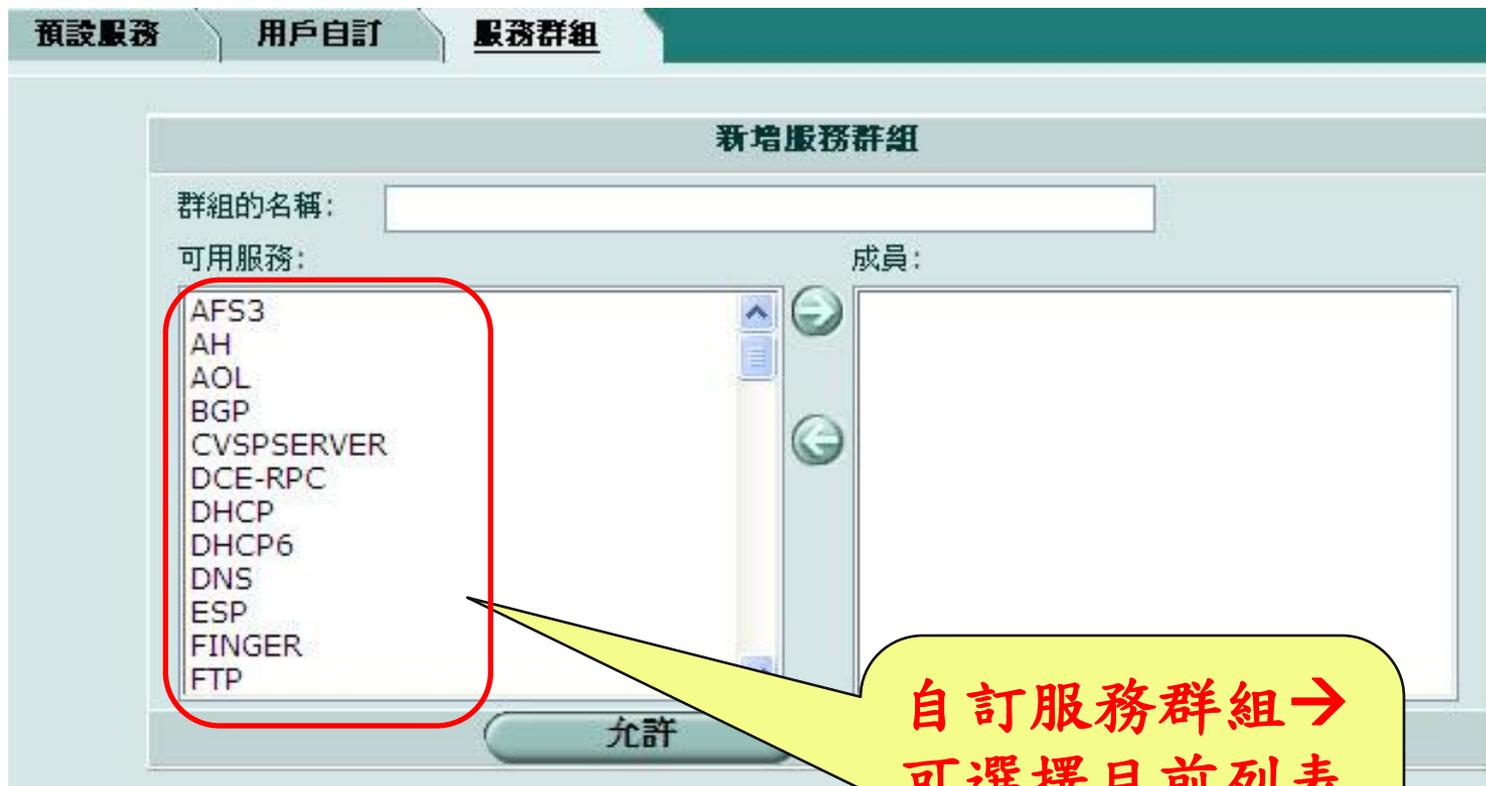
協定型態 TCP/UDP

網路協定	來源埠		目的埠	
	低	高	低	高
TCP <input type="button" value="v"/>	<input type="text" value="1"/>	<input type="text" value="65535"/>	<input type="text" value="0"/>	<input type="text" value="0"/>

**TCP/UDP**

**指定port範圍**

# 防火牆服務~服務群組



自訂服務群組→  
可選擇目前列表  
的服務組成服務  
群組

# 防火牆日誌



The screenshot displays the 'WEB CONFIG' interface for firewall logging settings. The left sidebar shows a navigation menu with '紀錄與報表' (Logging and Reporting) selected. The main content area is titled '日誌設定' (Logging Settings) and contains two sections: '遠端檔案記錄' (Remote File Logging) and 'Local Logging'. Both sections have their respective checkboxes checked. The '遠端檔案記錄' section includes a text input for 'IP地址' (IP Address) with the value '203.68.253.245' and a '連接測試' (Test Connection) button. The 'Local Logging' section includes a '選擇分級日誌' (Select Log Level) dropdown menu with '信息' (Info) selected. A '採用' (Apply) button is located at the bottom right of the settings area.

WEB CONFIG

紀錄設置    設定告警電子郵件    事件記錄

系統管理  
路由設定  
防火牆  
UTM  
VPN  
使用者認證  
Endpoint NAC  
無線網路控制器  
紀錄與報表  
紀錄設定  
紀錄存取  
DLP檔案記錄  
IPS Packet Archive  
隔離檔案

日誌設定

遠端檔案記錄  
 FortiAnalyzer  
IP地址: 203.68.253.245    連接測試  
選擇分級日誌: 信息

FortiGuard 遠端分析服務  
 日誌伺服器

Local Logging  
 記憶體  
選擇分級日誌: 信息

採用

# 防火牆日誌

Log 分類

漏斗 →  
過濾所須 log

WEB CONFIG

FortiAnalyzer 記憶體

日誌型態: 系統事件

1 / 410 欄位設定 原始資料 清除所有過濾設定

#	日期	時間	等級	子型式	識別碼	使用者介面	採取行動	訊息
1	2010-03-02	17:45:01	information	his-performance	40704		perf-stats	Performance statistics
2	2010-03-02	17:40:01	information	his-performance	40704		perf-stats	Performance statistics
3	2010-03-02	17:36:10	information	admin	41990	https(118.171.45.185)	login	Administrator admin logge
4	2010-03-02	17:36:04	information	admin	41990	https(118.171.45.185)	logout	Administrator admin time
5	2010-03-02	17:35:01	information	his-performance	40704		perf-stats	Performance statistics
6	2010-03-02	17:30:16	information	admin	41990	https(118.171.45.185)	login	Administrator admin logge
7	2010-03-02	17:30:03	information	admin	41990	https(118.171.45.185)	logout	Administrator admin time
8	2010-03-02	17:30:01	information	his-performance	40704		perf-stats	Performance statistics
9	2010-03-02	17:25:01	information	his-performance	40704		perf-stats	Performance statistics
10	2010-03-02	17:22:44	information	admin	41990	https(118.171.45.185)	login	Administrator admin logge
11	2010-03-02	17:22:38	information	admin	41990	https(118.171.45.185)	logout	Administrator admin time
12	2010-03-02	17:20:01	information	his-performance	40704		perf-stats	Performance statistics
13	2010-03-02	17:15:56	information	admin	41990	https(118.171.45.185)	login	Administrator admin logge
14	2010-03-02	17:15:47	information	admin	41990	https(118.171.45.185)	logout	Administrator admin time
15	2010-03-02	17:15:01	information	his-performance	40704		perf-stats	Performance statistics
16	2010-03-02	17:10:01	information	his-performance	40704		perf-stats	Performance statistics
17	2010-03-02	17:05:01	information	his-performance	40704		perf-stats	Performance statistics
18	2010-03-02	17:00:01	information	his-performance	40704		perf-stats	Performance statistics
19	2010-03-02	16:57:40	information	admin	41990	https(118.171.45.185)	login	Administrator admin logge

# 防火牆日誌~尋找log

編輯檔案 - Windows Internet Explorer

https://140.127.235.254/log/display?log=log&frame=filter&field\_name=src&content\_type

### 編輯檔案

檔案	來源
日期	<input checked="" type="checkbox"/> 啟用
等級	欄位 等於 <input type="checkbox"/> 非
子型式	本文
識別碼	
來源	
目的	
服務	

來源IP位址或是FQDN.

[清除所有過濾設定]

Log 欄位

啟用 →  
過濾條件

# LAB

# LAB#1

- Q; 阻擋學校某一個ip連上internet

設定步驟:

1. 在f/w的位址, 新增該ip位址
2. 新增一條策略, 來源為該ip, 目的→all(any), 服務→all(any), 採取行動→deny
3. 注意策略順序, 若需要則調整策略位置

# LAB#2

- Q: 限定某一學校的WEB Server只能用http連線, 其餘deny  
設定步驟:
  1. 在f/w的位址, 新增WEB Server ip位址
  2. 新增一條策略, 來源→all(any), 目的→ WEB Server, 服務→http, 採取行動→accept
  3. 注意策略順序, 若需要則調整策略位置

# LAB#3

- Q: 阻擋某一學校, 連上 [www.pchome.com.tw](http://www.pchome.com.tw)

設定步驟:

1. 在 f/w 的位址, 新增 pchome, 對應 FQDN → [www.pchome.com.tw](http://www.pchome.com.tw) 網址
2. 新增一條策略, 來源 → all(any), 目的 → \_pchome, 服務 → all(any), 採取行動 → deny
3. 注意策略順序, 若需要則調整策略位置



**THANK YOU.**