Fortinet®-Training
For 澎湖縣教網中心 NGN

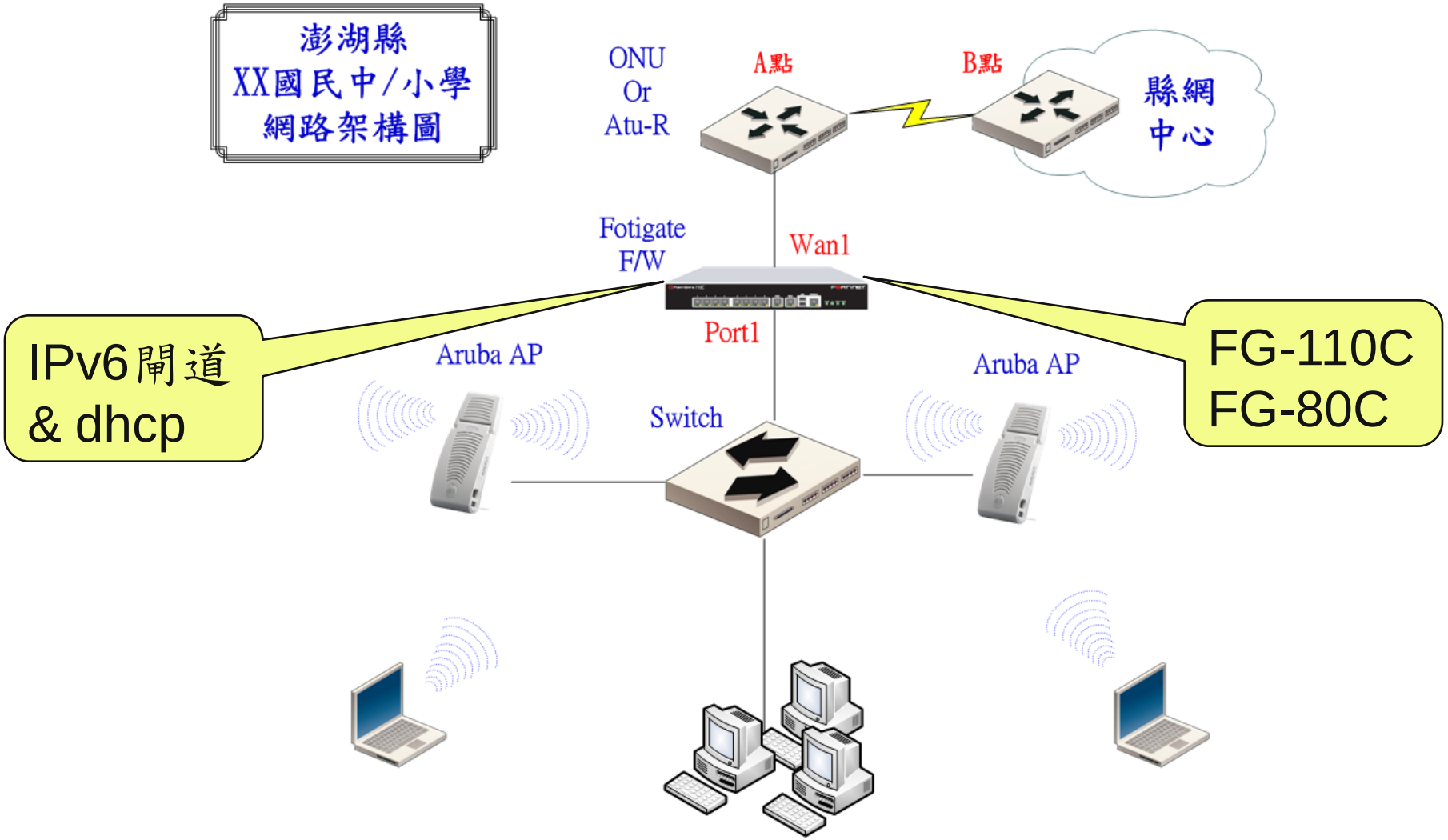
力麗科技 劉士豪
timliu@llt.com.tw

March 2010

Agenda

- 本案學校UTM網路架構
- 防火牆管理
- LAB

網路架構



防火牆管理

Web Login

https://fortigate ip

系統管理-狀態(1/4)

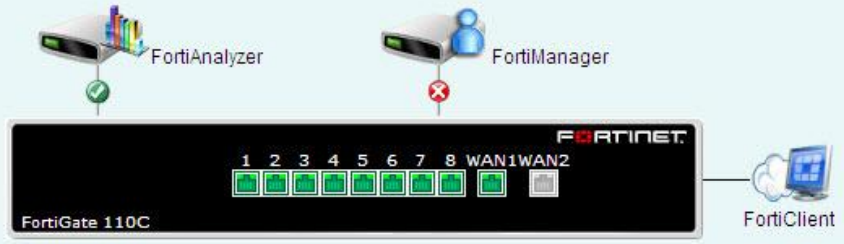
系統資訊

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 [更改]
HA 狀態	單機模式 [設定]
主機名稱	mkjh-UTM-FG110C [更改]
韌體版本	v4.0,build0185,091020 (MR1 Patch 1) [更新]
FortiClient 版本	未知
操作模式	NAT [更改]
虛擬區域	關閉 [啓用]
目前在線管理者	1 [詳情]
目前的使用者	admin [密碼變更]

授權資訊

支援合約		
Registration	連線失敗	
FortiGuard 訂閱		
防毒	連線失敗 [設定]	
AV 病毒碼	9.00795 (更新 2008-12-08) [更新]	
進階掃瞄資料設定	0.00000 (更新 2003-01-01)	
入侵防禦	連線失敗 [設定]	
IPS 特徵碼	2.00593 (更新 2009-02-05) [更新]	
網頁過濾	連線失敗 [設定]	
郵件過濾	連線失敗 [設定]	
管理及分析服務	連線失敗	
服務帳號 ID	[更改]	
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



重新啓動 關機

警示訊息控制台

- 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	[詳情]
HTTPS	0 網頁瀏覽	[詳情]
電子郵件	0 寄出郵件	[詳情]
	0 收取郵件	
FTP	0 網頁瀏覽	[詳情]
	0 檔案上傳	
	0 檔案下載	
IM	0 傳送檔案	[詳情]
	0 交談連線	
	0 交談訊息	

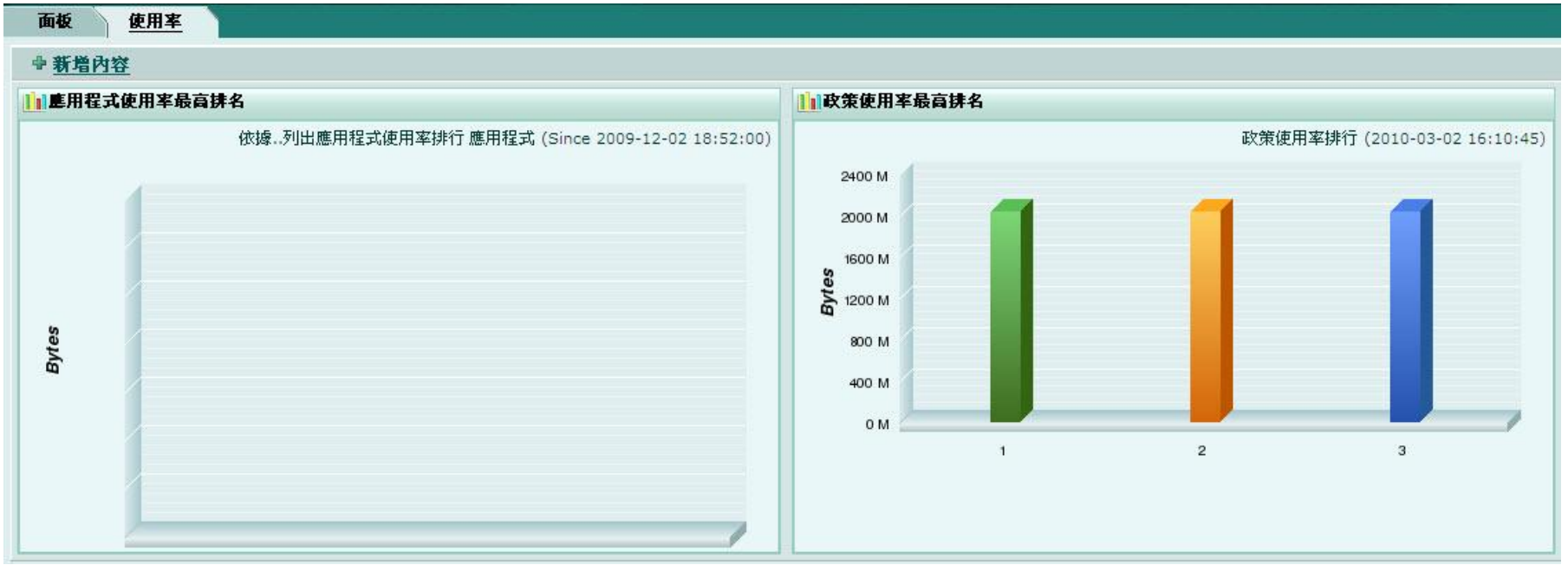
系統管理-狀態(2/4)


授權資訊
支援合約
Registration 連線失敗
FortiGuard 訂閱
防毒 連線失敗 [設定]
AV 病毒碼 9.00795 (更新 2008-12-08) [更新]
進階掃瞄資料設定 0.00000 (更新 2003-01-01)
入侵防禦 連線失敗 [設定]
IPS 特徵碼 2.00593 (更新 2009-02-05) [更新]
網頁過濾 連線失敗 [設定]
郵件過濾 連線失敗 [設定]
管理及分析服務 連線失敗
服務帳號 ID [更改]
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 . . .
2009-12-02 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 [詳情]
HTTPS 0 網頁瀏覽 [詳情]
電子郵件 0 寄出郵件 [詳情]
0 收取郵件
FTP 0 網頁瀏覽 [詳情]
0 檔案上傳
0 檔案下載
IM 0 傳送檔案 [詳情]
0 交談連線
0 交談訊息
VoIP 0 訊息 [詳情]
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 [詳情]
40653 被阻擋流量
病毒記錄 0 病毒攔截 [詳情]
IPS 0 攻擊阻斷 [詳情]
Email 0 垃圾郵件識別 [詳情]
Web 0 網頁封鎖 [詳情]
資料外洩防護 0 資料外洩 [詳情]
應用程式控制 0 應用程式控制訊息 [詳情]
事件 26207 發生的事件 [詳情]
全部 4 GB (26872192 messages) since last reset

系統管理-狀態(3/4)


系統資源
CPU使用率 12%
記憶體使用率 15%
FortiAnalyzer 使用率 54%
最大的連線數
最大連線數的來源IP (2010-03-02 16:05:34)
1800
1500
1200
900
600
300
0
140.127.235.22
140.127.235.21
140.127.235.72
140.127.235.232
118.171.45.185
10.163.128.85
140.127.235.219
140.127.235.4
140.127.235.38
140.127.235.10
線上總計連線數: 3210 [詳情]

系統管理-狀態(4/4)


面板
使用率
新增內容
應用程式使用率最高排名
依據..列出應用程式使用率排行 應用程式 (Since 2009-12-02 18:52:00)
Bytes
政策使用率最高排名
政策使用率排行 (2010-03-02 16:10:45)
Bytes
2400 M
2000 M
1600 M
1200 M
800 M
400 M
0 M
1
2
3

管理員設置

- 管理帳號/密碼

  新增/刪除/密碼修改/權限調整

系統維護-備份與恢復

- UTM 設定值備份/還原

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

防火牆策略~設定

介面/ip/動作

不要啟用NAT

F/W log(日誌)

防火牆位址

位址→
ip/ip範圍/
網段/網址

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

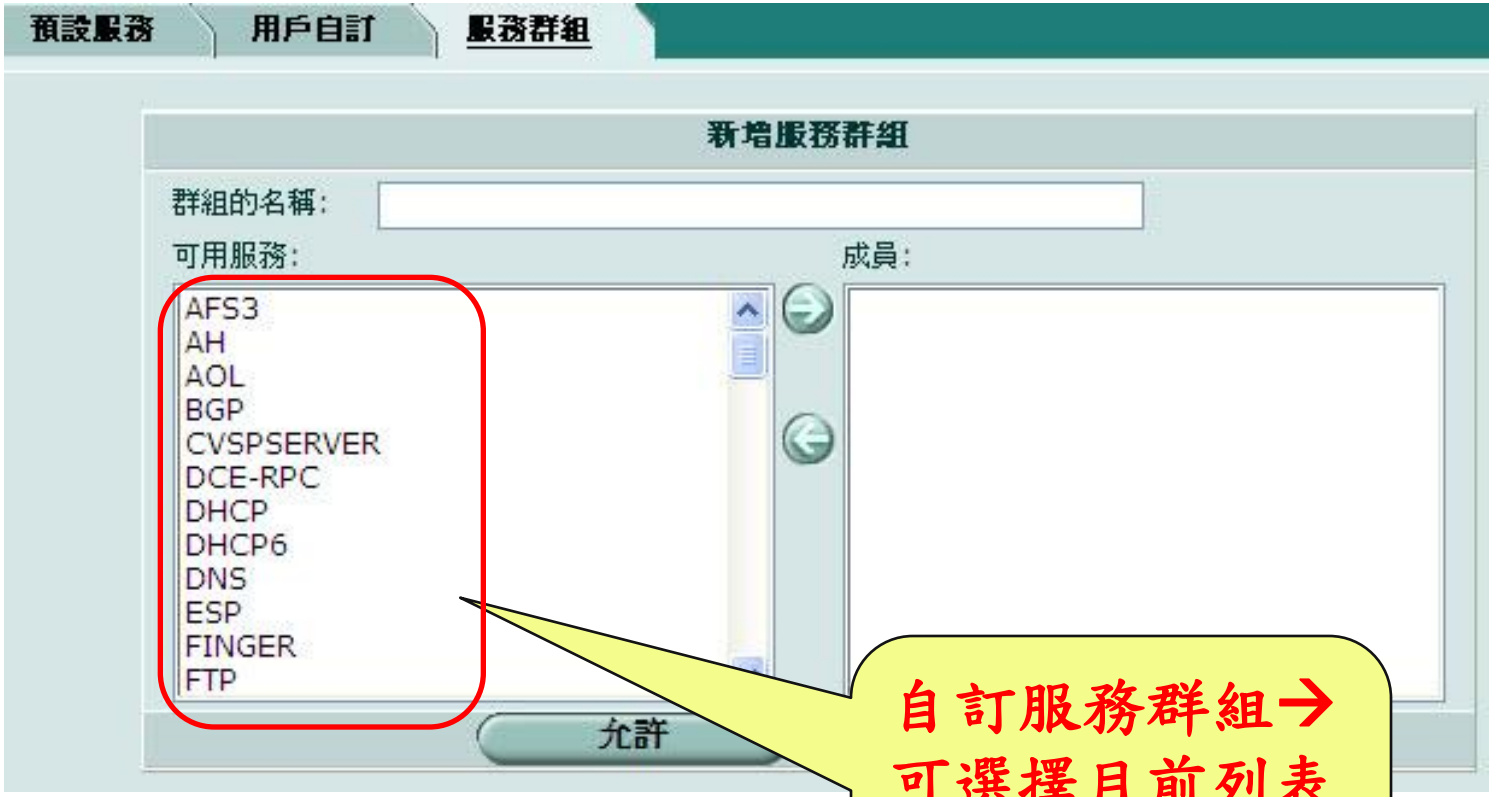
防火牆服務~預設服務

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
1
65535
0
0
增加
允許
取消
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


WEB CONFIG
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
記錄設定
紀錄存取
DLP檔案記錄
IPS Packet Archive
紀錄設置
設定告警電子郵件
事件記錄
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

#	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

防火牆日誌~尋找log


編輯檔案 - Windows Internet Explorer
https://140.127.235.254/log/display?log=tlog&frame=filter&field_name=src&content_type
編輯檔案
檔案
日期
等級
子型式
識別碼
來源
目的
服務
[清除所有過濾設定]
來源
啓用
欄位
等於
非
本文
來源IP位址或是FQDN.
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

設定步驟:

1. 在f/w的位址,新增pchome,對應FQDN→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.