



屏東縣教育網路中心

Fortigate-防火牆設定

聯易科技股份有限公司 林志豪

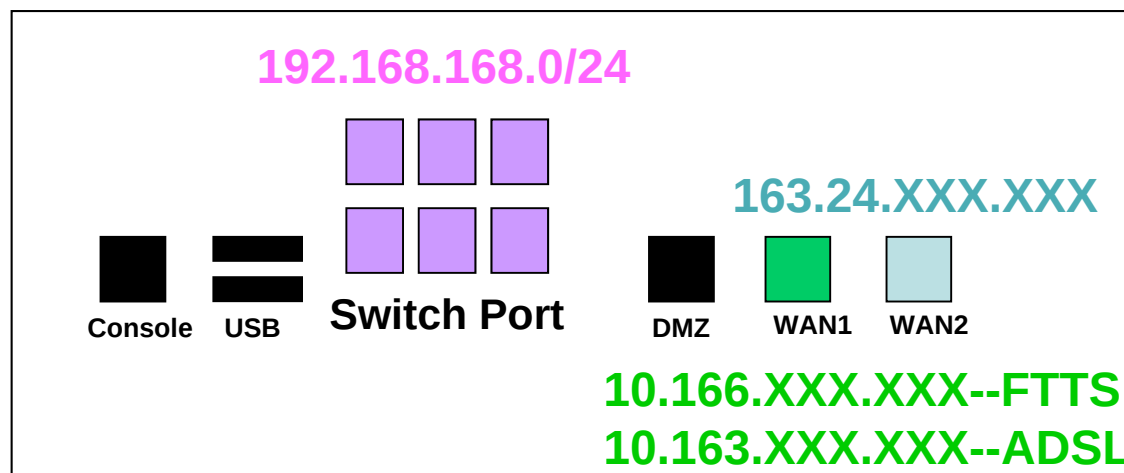
kirby@netease.com.tw

NETEASE
ease your networks

Agenda

1	設備基本功能簡介
2	架構簡介
3	IPv6簡介
4	防火牆設定注意事項
5	Log & Session的應用
6	Q&A

FTG-80C外觀

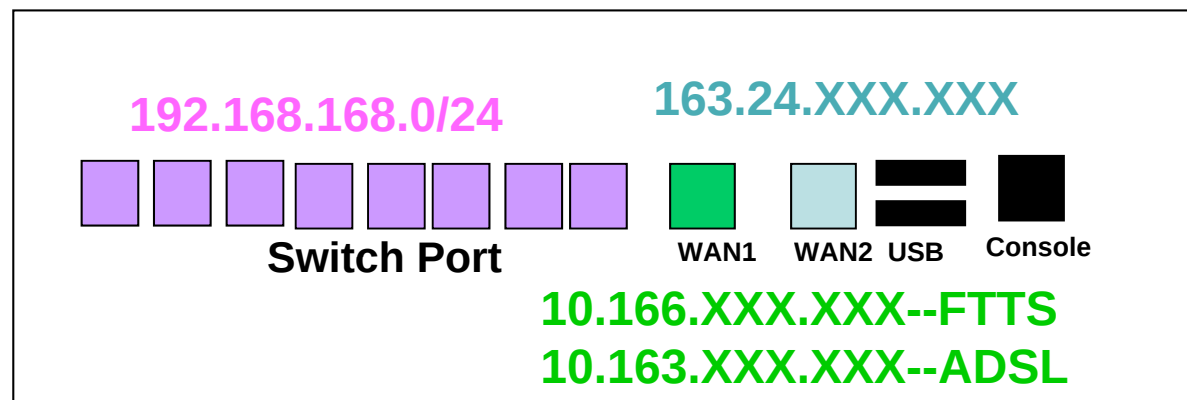


說明：

黑色：忽略不使用

其他三種顏色表示不同的網段

FTG-110C外觀



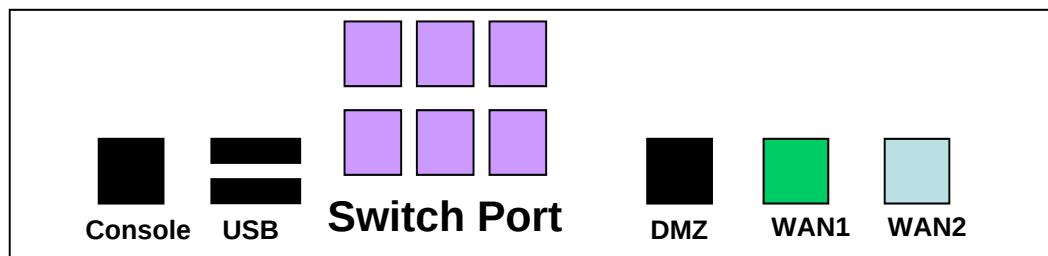
說明：

黑色：忽略不使用

其他三種顏色表示不同的網段

FORTINET

Port 名詞定義



Console Port：電腦透過特殊的Cable，直接連接該Port對設備做設定

USB Port：連接USB DISK，可備份防火牆設定檔或其它資料

Switch Port：區域網路的连接埠；泛指一般内部網路

DMZ Port：非軍事區，介於内部網路(軍事區)和外部網路之間，可受防火牆的監控與保護，或受其它安全機制的檢測

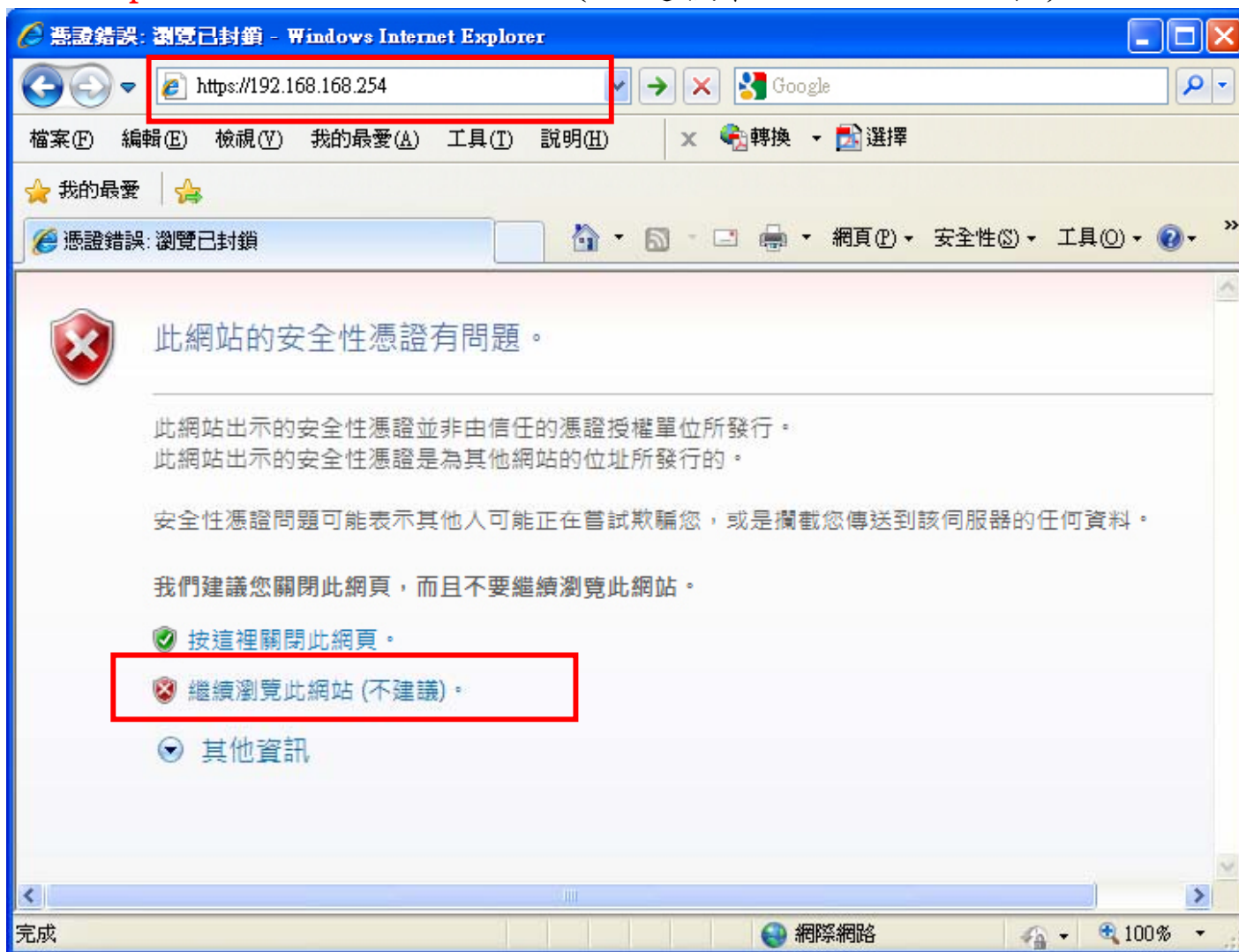
WAN1 Port：網際網路連結埠 1，一般接ADSL、對外網路線路、實體網段等……

WAN2 Port：網際網路連結埠 2，一般接ADSL、對外網路線路、實體網段等……

防火牆連線

1. 開啟瀏覽器，輸入防火牆的IP位址，點選【繼續瀏覽此網站（不建議）】

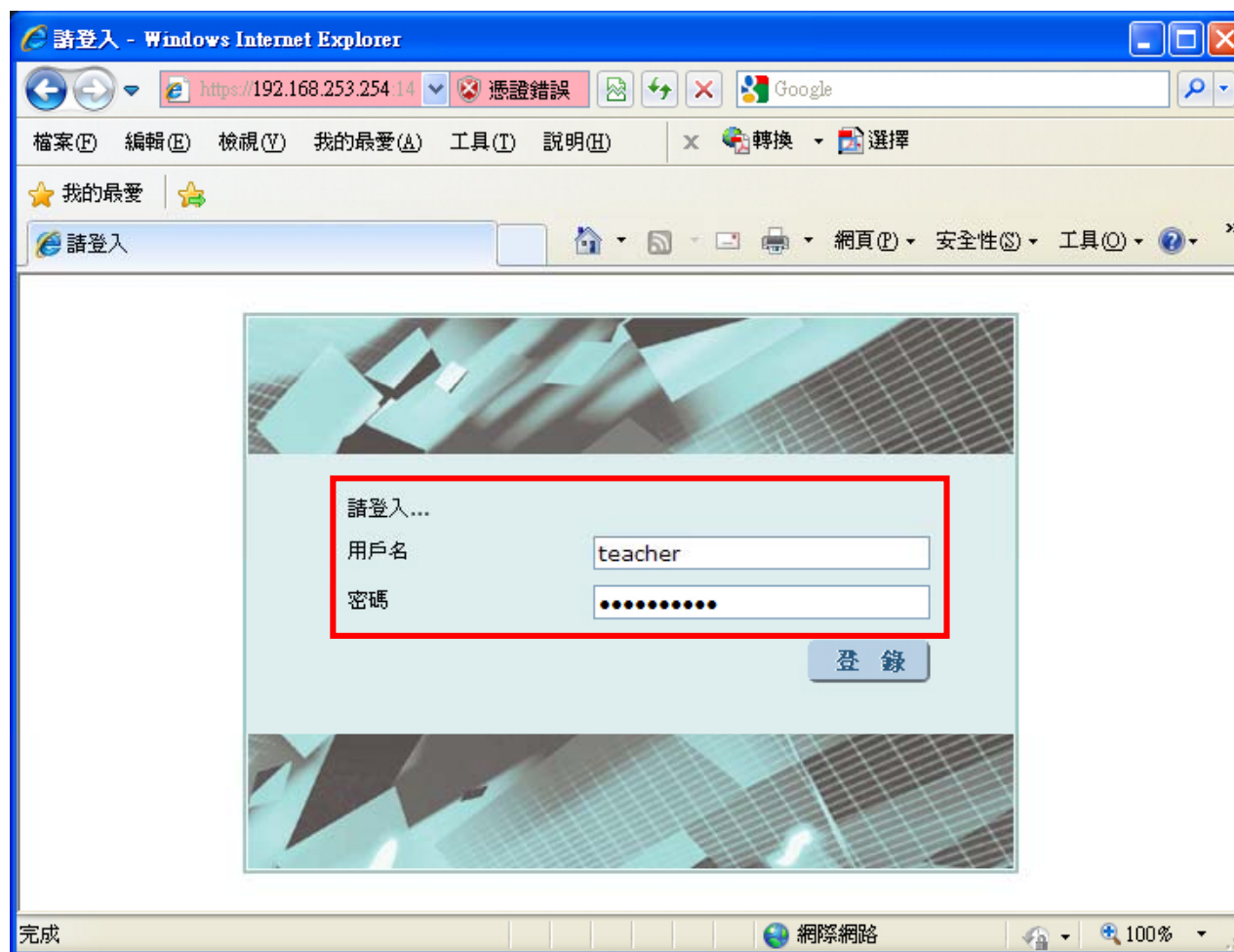
例： <https://192.168.168.254>（PC連接在Switch Port下）



2. 輸入用戶名 / 密碼

teacher / teacher123 → 僅瀏覽權限

teacher2 / teacher456 → 擁有可修改的權限



語系變更 \System\Admin\Settings

The screenshot shows the Fortinet web interface. On the left, the 'System' menu is highlighted, and the 'Admin' sub-menu is selected. On the right, the 'Settings' tab is active. The 'Language' dropdown menu is open, showing the following options: English, English, Simplified Chinese, Japanese, Korean, Spanish, Traditional Chinese, French, and Portuguese. The 'Apply' button is located at the bottom of the settings page.

System

Administrators Admin Profile Central Management Settings

Enable ☐

Minimum Length (8-32 characters)

Must Contain ☐ Upper Case Letters ☐ Lower Case Letters
☐ Numerical Digits ☐ Non-alphanumeric Letters

Apply Password Policy to ☒ Admin Password ☐ IPSEC Preshared Key

Admin Password Expires after (days)

Timeout Settings

Idle Timeout (1-480 mins)

Display Settings

Language (1,000)

Lines Per Page

IPv6 Support on GUI ☐

Enable SCP ☐

Enable Wireless Controller ☐

Apply

各界面的IP設定 \系統管理\網路\介面

系統管理 介面 區域 選項 DNS資料庫 網頁代理伺服器

可查看各個界面的狀態與IP位置

名稱	IP/遮罩	管理存取	管理狀態	連結狀態	
dmz	0.0.0.0 / 0.0.0.0		+	+	
internal (NAT_LAN)	192.168.168.254 / 255.255.255.0	HTTP,HTTPS,PING,SSH	+	+	
wan1 (WAN)	10.166.38.1 / 255.255.255.0	HTTP,HTTPS,PING,SSH,SNMP	+	+	
wan2 (LAN)	163.24.38.250 / 255.255.255.0	HTTP,HTTPS,PING,SSH,SNMP	+	+	

新增 Switch Mode [欄位設定]

網路介面

名稱 internal1 (00:09:0F:28:43:CE)
別名 Wireless
連結狀態 開啟

位址模式
☒ 用戶定義 ☐ DHCP ☐ PPPoE
IP網址/網路遮罩: 192.168.10.254/255.255.255.0
IPv6 地址: ::/0

☐ 啟動one-arm sniffer
☐ Enable Explicit Web Proxy
☐ Enable DDNS
☐ Override Default MTU Value 1500 (位元組)
☐ 啟用DNS查詢 [請選擇...]

系統管理存取
☒ HTTPS ☐ PING ☒ HTTP
☐ SSH ☐ SNMP ☐ TELNET

IPv6 Administrative Access
☐ HTTPS ☐ PING ☐ HTTP
☐ SSH ☐ SNMP ☐ TELNET

DHCP \系統管理\DHCP\服務

The screenshot displays the Fortinet system management interface for DHCP services. On the left, a sidebar menu shows '系統管理' (System Management) expanded, with 'DHCP' selected. The main panel shows a list of DHCP services under the '服務' (Services) tab. The 'internal(NAT_LAN)' service is highlighted, and its configuration is shown in the '編輯DHCP主機' (Edit DHCP Host) window.

編輯DHCP主機 (Edit DHCP Host) Configuration:

- 名稱 (Name): NAT_LAN_DHCP
- 啟動 (Enabled): ☒
- 類型 (Type): ☒ 正規 (Normal) ☐ IPSEC
- IP 範圍 (IP Range): 192.168.168.10 - 192.168.168.200
- 網路遮罩 (Network Mask): 255.255.255.0
- 預設閘道 (Default Gateway): 192.168.168.254
- 區域 (Area):
- 租期 (Lease Time): ☐ 無限 (Infinite) ☒ 0 (天) 4 (小時) 0 (分) (5分 - 100天)
- 進階... (Advanced...): (DNS, WINS, 客制選項, 例外範圍...)
- IP發派模式 (IP Assignment Mode): ☒ 主機IP範圍 (Host IP Range) ☐ 使用者群組定義方式 (User Group Definition Method)
- DNS 伺服器 1 (DNS Server 1): 163.24.239.1
- DNS 伺服器 2 (DNS Server 2): 168.95.1.1
- DNS 伺服器 3 (DNS Server 3): 8.8.8.8
- WINS 伺服器 1 (WINS Server 1):
- WINS 伺服器 2 (WINS Server 2):

Annotations:

- A red box highlights the '系統管理' (System Management) menu item in the sidebar.
- A red box highlights the 'DHCP' menu item in the sidebar.
- A red box highlights the 'internal(NAT_LAN)' service in the service list.
- A red box highlights the 'DNS 伺服器 1' field in the configuration window, with a callout pointing to it that says: 將DNS伺服器1指定到 163.24.239.1 (Specify DNS Server 1 to 163.24.239.1).
- Three icons with labels are shown on the right: a trash can icon labeled '刪除' (Delete), a pencil icon labeled '編輯' (Edit), and a plus sign icon labeled '新增DHCP主機' (Add DHCP Host).

FORTINET

路由 \路由設定\靜態路由\靜態路由

系統管理

路由設定

靜態路由

動態路由

路由狀態

防火牆

UTM

VPN

使用者認證

Endpoint NAC

無線網路控制器

紀錄與報表

靜態路由 政策路由

新增

ECMP Route Failover & Load Balance Method source based 採用

	IP地址/遮罩	網路閘道	設備	Distance	
▼ 路由	0.0.0.0/0.0.0.0	10.166.38.254	wan1	10	 
▼ IPv6 路由	::/0	2001:288:86ff:ffff:ffff:ffff:3002	wan1		 

編輯路由

目的 IP/網路遮罩 0.0.0.0/0.0.0.0

設備 wan1(WAN)

網路閘 10.166.38.254

Distance 10 (1-255)

允許 取消



刪除



編輯

FORTINET

虛擬IP \ 防火牆\ 虛擬IP\ 虛擬IP\ 新增

系統管理

路由設定

防火牆

防火牆策略

位址

服務

時間表

流量控制

虛擬IP

負載平衡

保護內容表

UTM

VPN

使用者認證

Endpoint NAC

無線網路控制器

紀錄與報表

虛擬IP

VIP群組

IP Pool

新增

新增虛擬網路對映

名稱

介面

類型

服務網路位址/範圍

要對映到的網路位址/範圍

☐ 埠號轉換

允許

取消

Web Server在內部網段，設定的方式

封包進入介面

進入介面的IP

對應內部的IP

特別指定TCP 80埠

名稱

介面

類型

服務網路位址/範圍

要對映到的網路位址/範圍

☒ 埠號轉換

網路協定

外部服務埠

要對映到的埠號

允許

取消

ET

流量查詢 \ 網路管理\狀態\面板\新增內容\最大的連線數

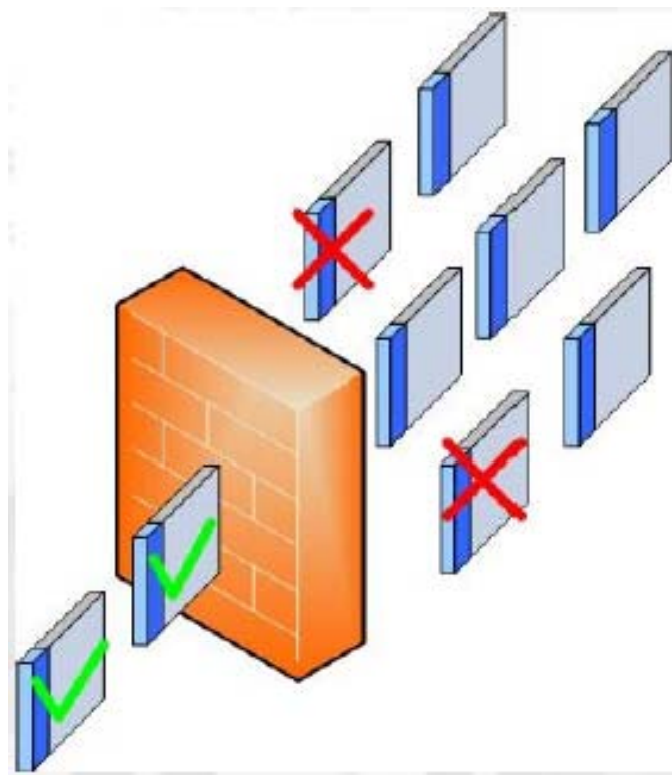


The table shows a list of connections with the following columns: #, 協定 (Protocol), 來源地址 (Source Address), 來源埠號 (Source Port), 目的地址 (Destination Address), 目的埠號 (Destination Port), 政策 ID (Policy ID), and 到期時間 (sec) (Expiration Time). The table is filtered to show 11 results out of a total of 96. The data is as follows:

#	協定	來源地址	來源埠號	目的地址	目的埠號	政策 ID	到期時間 (sec)
1	tcp	67.195.114.38	57598	163.24.38.10	80	3	62
2	tcp	209.85.210.168	57238	163.24.38.10	25	3	109
3	tcp	163.24.48.5	1487	163.24.38.38	445	3	77
4	tcp	71.182.73.5	8103	163.24.38.10	25	3	89
5	tcp	163.24.38.245	4982	65.197.197.27	80	2	3599
6	tcp	163.24.239.80	50757	163.24.38.10	80	3	67
7	tcp	163.24.38.245	1534	202.79.240.245	554	2	3585
8	tcp	163.24.177.136	7489	163.24.38.169	445	3	43
9	tcp	163.24.38.245	1532	69.147.84.103	5050	2	3560
10	udp	163.24.38.245	58840	168.95.192.1	53	2	71
11	tcp	116.59.11.98	59922	163.24.38.250	443		97

防火牆的運作原理

防火牆會對所有經過的封包Header進行檢查，按照一系列策略(Policy)，來決定封包的處理方式。防火牆策略會根據封包的來源和目的位址、協定、port、界面等因素進行判斷，決定是否讓封包通過。



功能-Firewall

- 依據封包表頭做過濾
 - IP (SA, DA, Protocol)
 - TCP/UDP (Port #)



SRC-IP	DST-IP	Protocol	SRC-Port	DST-Port
10.1.10.5	1.1.70.25 0	ftp	36033	80

防火牆策略 \防火牆\防火牆策略\防火牆策略



防火牆策略 DoS政策 Sniffer政策 IPv6政策

建立新防火牆策略

來源介面/域名: internal
來源位址名稱: all 多個
目的介面/域名: wan1
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
☐ 開啟用戶政策 啟動轉址服務

☒ 保護內容表: scan
☐ 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
☐ 啟動終端用戶NAC: [請選擇]
註解 (最多 63 字元):

允許 取消

設定介面輸入的來源與服務的項目

啟動保護功能 (防毒、入侵偵測..等)

完成後畫面

系統管理 路由設定 **防火牆** 防火牆策略 位址

防火牆策略 DoS政策 Sniffer政策

新增 [欄位設定?] ☒ 區域檢視 ☐ 全域檢視

狀態	ID	來源	目的	排程	服務	防護內容表	採取行動
▼ internal -> wan1 (1)							
☒	9	all	all	always	ANY	scan	ACCEPT

IP Pool \防火牆\虛擬IP\IP Pool

The screenshot displays the Fortinet web management interface. On the left is a vertical navigation menu with the following items: 系統管理, 路由設定, 防火牆 (highlighted with a red box), 防火牆策略, 位址, 服務, 時間表, 流量類型, 虛擬IP (highlighted with a red box), 負載平衡, 保護內容表, UTM, VPN, 使用者認證, Endpoint NAC, 無線網路控制器, and 紀錄與報表. The main content area has three tabs: 虛擬IP, VIP群組, and IP Pool (highlighted with a red box). Below the tabs is a '新增' (Add) button. The main configuration area is titled '新動態IP群組' and contains two input fields: '名稱' (Name) and 'IP 範圍/子網' (IP Range/Subnet) with the value '0.0.0.0-0.0.0.0'. At the bottom are '允許' (Allow) and '取消' (Cancel) buttons.

系統管理

路由設定

防火牆

防火牆策略

位址

服務

時間表

流量類型

虛擬IP

負載平衡

保護內容表

UTM

VPN

使用者認證

Endpoint NAC

無線網路控制器

紀錄與報表

虛擬IP VIP群組 IP Pool

新增

新動態IP群組

名稱

IP 範圍/子網 0.0.0.0-0.0.0.0

允許 取消

IP Pool 範例說明

在防火牆的策略中，Internal→Wan1使用IP Pool的選項

名稱	起始位址	終止位址	
PTC_NAT_IP	163.24.38.251	163.24.38.251	

編輯輸出策略

來源介面/域名: internal(NAT_LAN)
來源位址名稱: all 多個
目的介面/域名: wan1(WAN)
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 PTC_NAT_IP

如IP Pool的IP不正確，欲修改，請在IP範圍/子網的欄位填入IP即可

編輯動態IP群組

名稱: PTC_NAT_IP
IP 範圍/子網: 163.24.38.251-163.24.38.251
允許 取消

填入欲修改IP

紀錄啟用 \ 紀錄與報表 \ 記錄設定 \ 記錄設置

1. 至 紀錄與報表 > 記錄設定 > 事件記錄，將所要記錄行為的Log勾選

系統管理

路由設定

防火牆

UTM

VPN

使用者認證

Endpoint NAC

紀錄與報表

記錄設定

紀錄存取

隔離檔案

報表存取

紀錄設置

設定告警電子郵件

事件記錄

事件日誌

☒ 啟動

- ☒ 系統活動事件
- ☒ IPSec協商事件
- ☒ DHCP 服務事件
- ☒ L2TP/PPTP/PPPoE 服務事件
- ☒ 管理事件
- ☒ HA活動事件
- ☒ 防火牆認證事件
- ☒ Pattern更新事件
- ☒ SSL VPN 使用者認證事件
- ☒ SSL VPN 管理者事件
- ☒ SSL VPN 連線事件
- ☒ VIP 伺服器運作監控事件
- ☐ CPU與記憶體使用率(每5鐘)

採用

2. 至 紀錄與報表 > 記憶體 > 紀錄存取，可查看系統儲存之各種紀錄檔，可選擇不同的日誌類型，查閱相關的紀錄檔，找出可能造成問題的Log，再進一步的處理

The screenshot displays the FortiAnalyzer web interface. On the left sidebar, the navigation menu includes '系統管理', '路由設定', '防火牆', 'UTM', 'VPN', '使用者認證', 'Endpoint NAC', and '紀錄與報表'. Under '紀錄與報表', the sub-menu '紀錄存取' (Record Access) is highlighted with a red box. The main content area is titled 'FortiAnalyzer 記憶體' (FortiAnalyzer Memory). A dropdown menu for '日誌型態' (Log Type) is open, showing options: '系統事件' (System Events), '應用程式控制記錄' (Application Control Logs), 'DLP記錄' (DLP Logs), '郵件過濾記錄' (Mail Filtering Logs), '攻擊與異常' (Attacks and Anomalies), '網頁過濾' (Web Filtering), '病毒攔阻' (Virus Blocking), '系統事件' (System Events), and '網路流量' (Network Traffic). The '系統事件' option is selected and highlighted. Below the dropdown, there are links for '欄位設定' (Field Settings), '原始資料' (Raw Data), and '清除所有過濾設定' (Clear All Filter Settings). A table of log entries is displayed below, with columns for '#', '日期' (Date), '時間' (Time), '等級' (Severity), '子型式' (Sub-type), '識別碼' (ID), '使用者介面' (User Interface), '採取行動' (Action), and '訊息' (Message).

#	日期	時間	等級	子型式	識別碼	使用者介面	採取行動	訊息
1	2010-01-11	11:32:02	information	admin	41990	https(192.168.253.105)	login	Administrator admin logged in successfully from https(192.168.253.105)
2	2010-01-11	11:31:41	information	his-performance	40704		perf-stats	Performance statistics
3	2010-01-11	11:26:41	information	his-performance	40704		perf-stats	Performance statistics
4	2010-01-11	11:21:41	information	his-performance	40704		perf-stats	Performance statistics
5	2010-01-11	11:18:59	information	dhcp	37382			Assigns IP address/configuration parameters to the client
6	2010-01-11	11:18:59	information	dhcp	37382			Client requests IP address/configuration parameters

設定檔備份/還原

\系統管理\系統維護\備份與恢復

The screenshot shows the FortiNet system management interface. On the left, a sidebar menu has '系統管理' (System Management) and '系統維護' (System Maintenance) highlighted with red boxes. The main content area has tabs for '備份與恢復' (Backup & Restore), '修訂備份檔' (Edit Backup File), 'Scripts', and 'FortiGuard'. The '備份與恢復' tab is active, displaying the '系統設定 (上次備份: Fri Jan 15 07:48:53 2010)' (System Settings) page. Under the '備份' (Backup) section, the '備份設定至:' (Backup to:) field has three radio buttons: '本地磁碟機' (Local Disk), 'FortiManager', and 'USB 隨身碟' (USB Drive). The '本地磁碟機' option is selected and highlighted with a red box. Below this, there is a checkbox for '設定檔案加密' (Set file encryption), which is unchecked. There are also input fields for '密碼' (Password) and '確認' (Confirm). At the bottom of the form is a '備份' (Backup) button.

點選本機磁碟機，將備份檔儲存在目前操作的電腦內

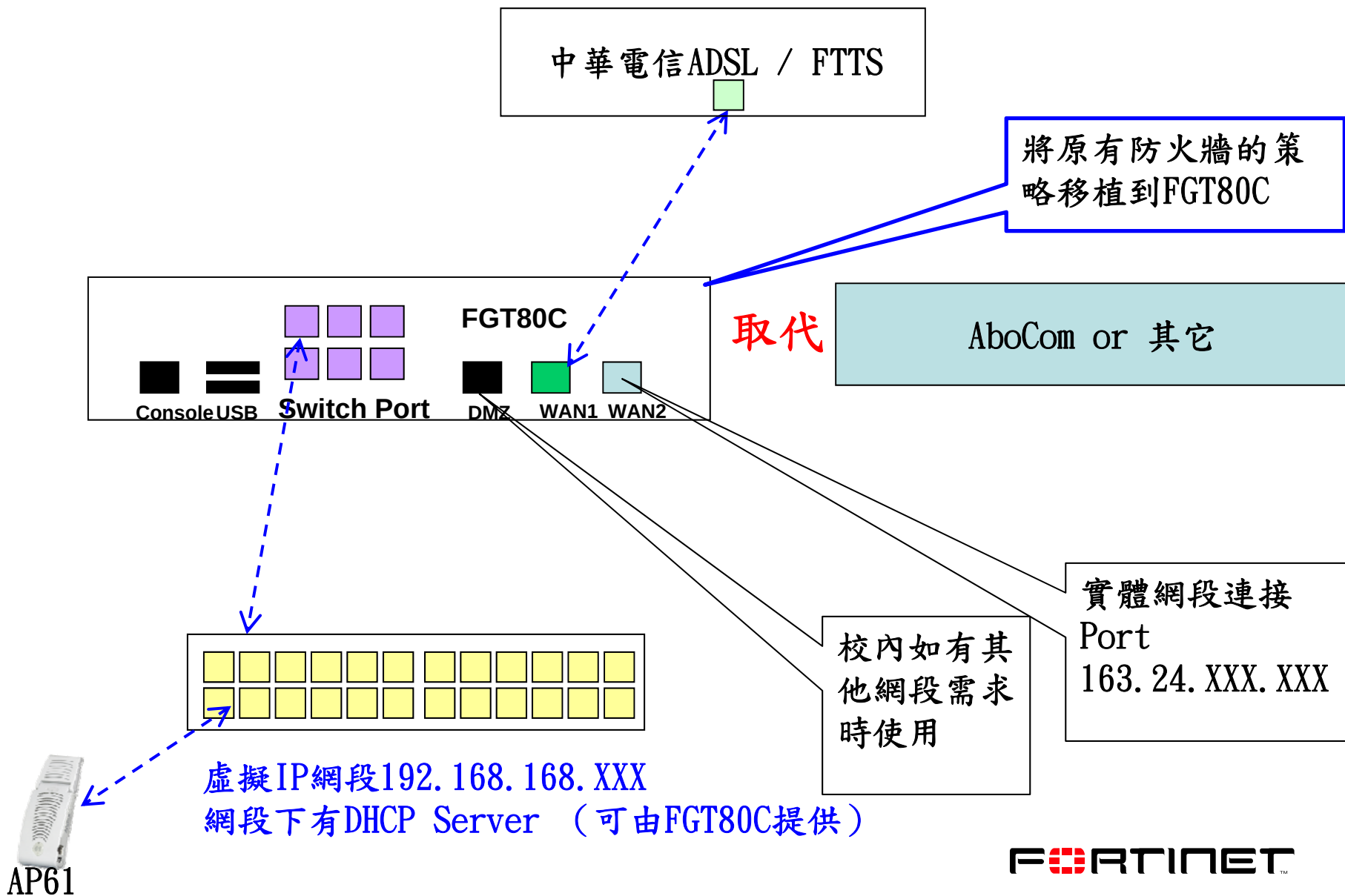
The screenshot shows the '還原' (Restore) page in the FortiNet system management interface. It has a title '還原' (Restore). Below the title, there is a section '復原設定從:' (Restore settings from:) with three radio buttons: '本地磁碟機' (Local Disk), 'FortiManager', and 'USB 隨身碟' (USB Drive). The '本地磁碟機' option is selected and highlighted with a red box. Below this, there is a text field for '檔案名稱:' (File name:) containing the path 'C:\Documents and Settings\Administrator\桌面\屏縣網'. This text field is also highlighted with a red box. There is a '瀏覽...' (Browse...) button next to the text field. Below the text field is a '密碼' (Password) input field. At the bottom of the form is a '還原' (Restore) button.

點選本機磁碟機，選擇瀏覽，從目前操作的電腦中選擇備份檔做還原

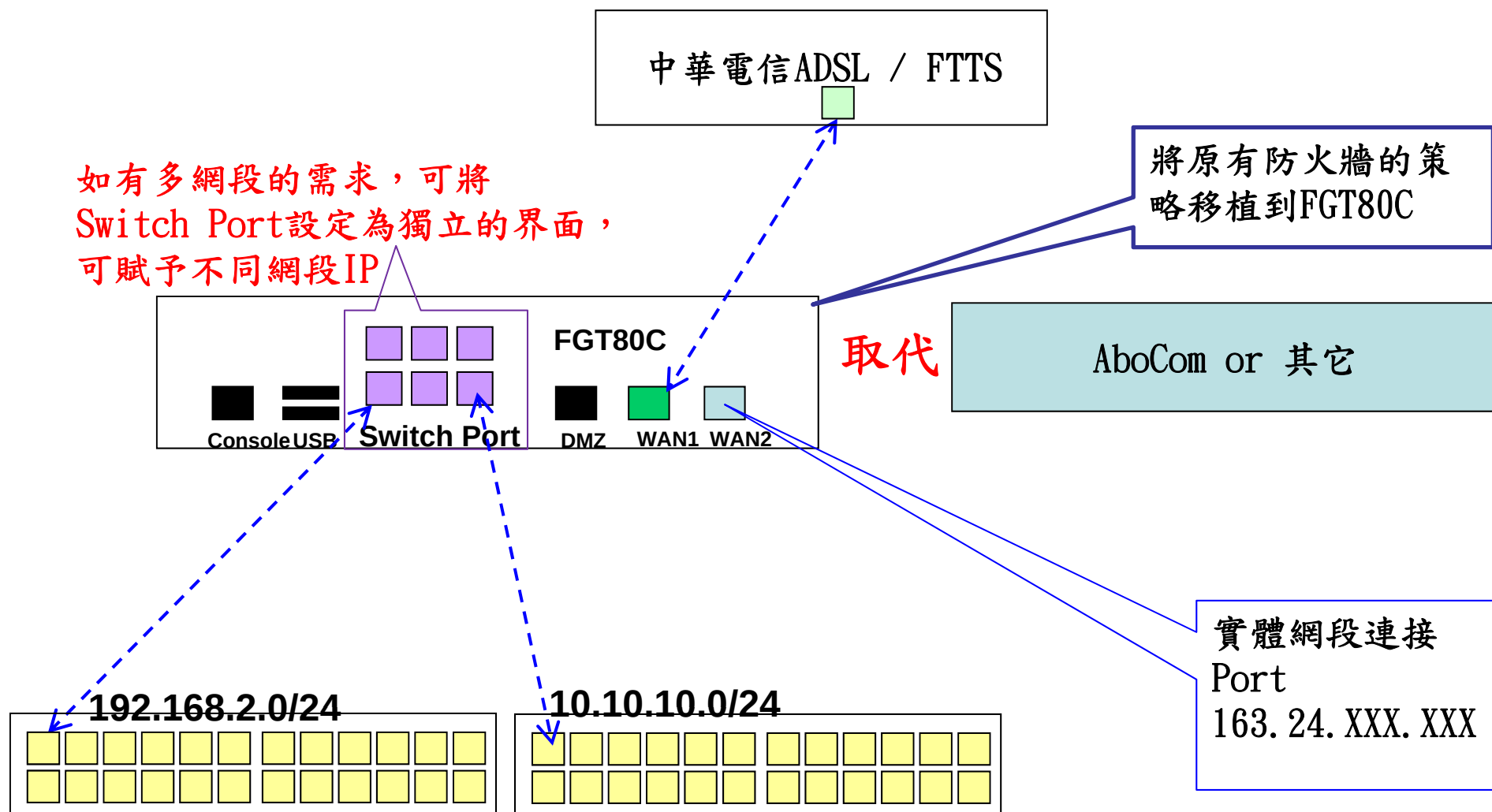
Agenda

1	設備基本功能簡介
2	架構簡介
3	IPv6簡介
4	防火牆設定注意事項
5	Log & Session的應用
6	Q&A

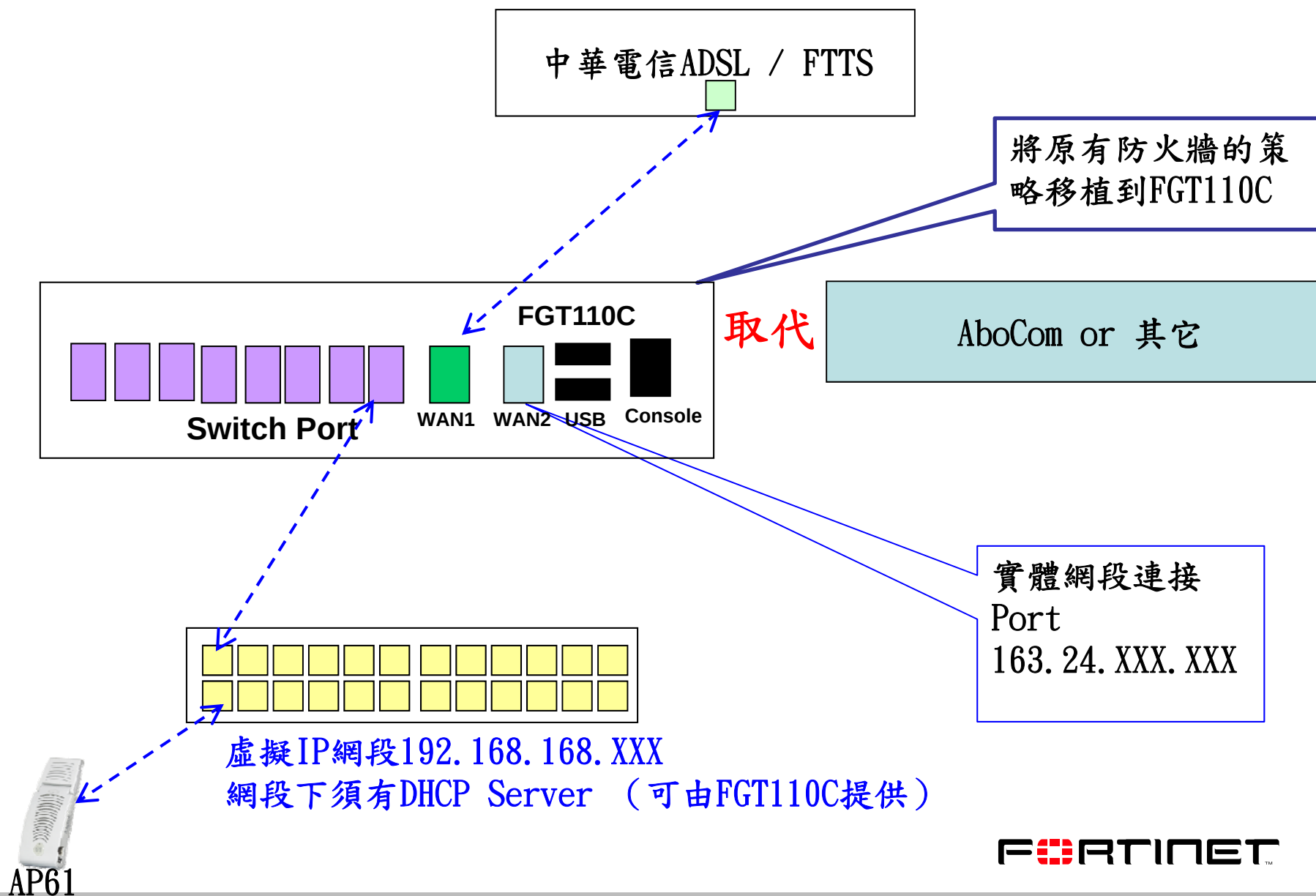
取代現有Router / 防火牆-80C



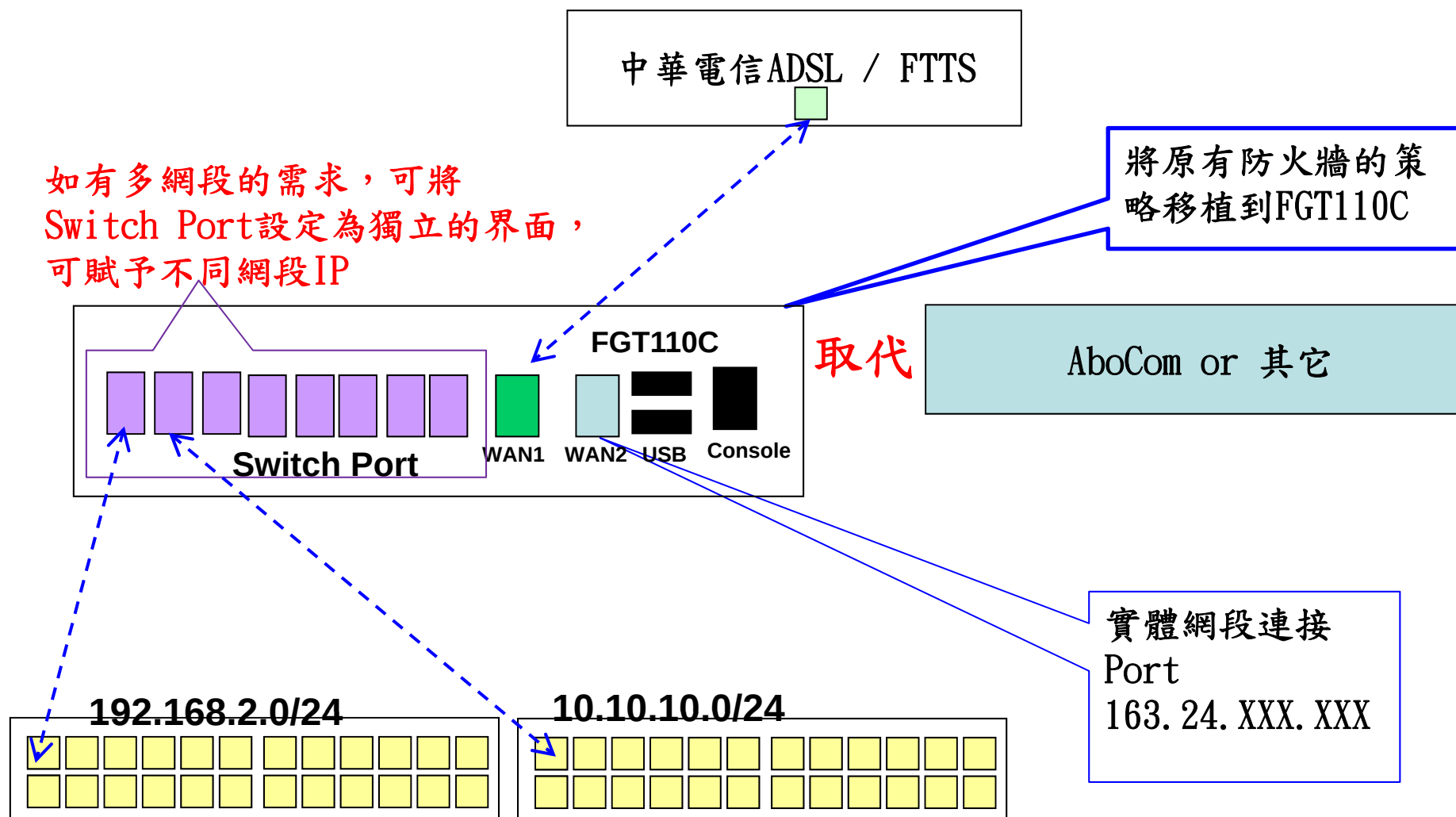
取代現有Router / 防火牆-80C



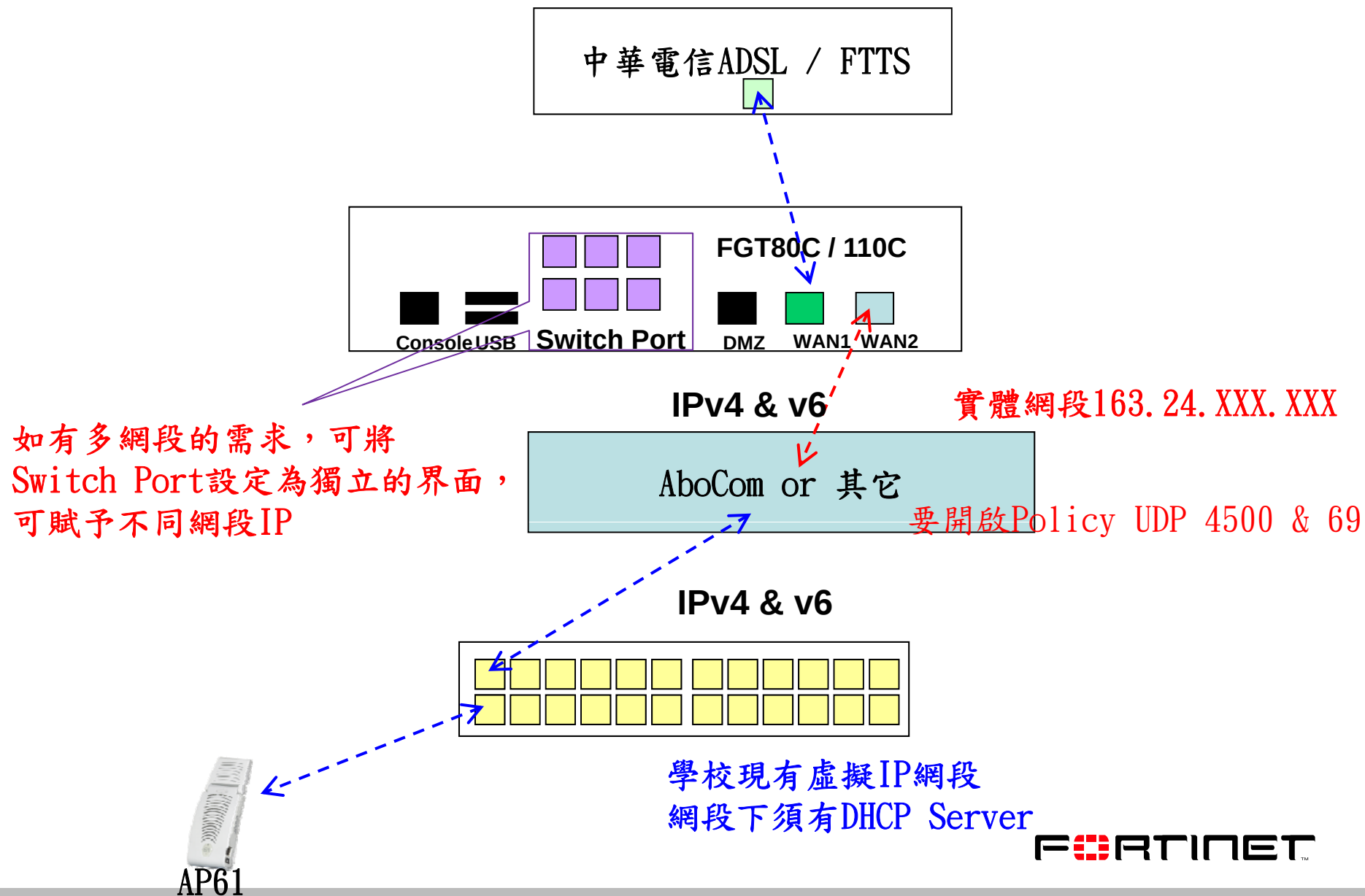
取代現有Router / 防火牆-110C



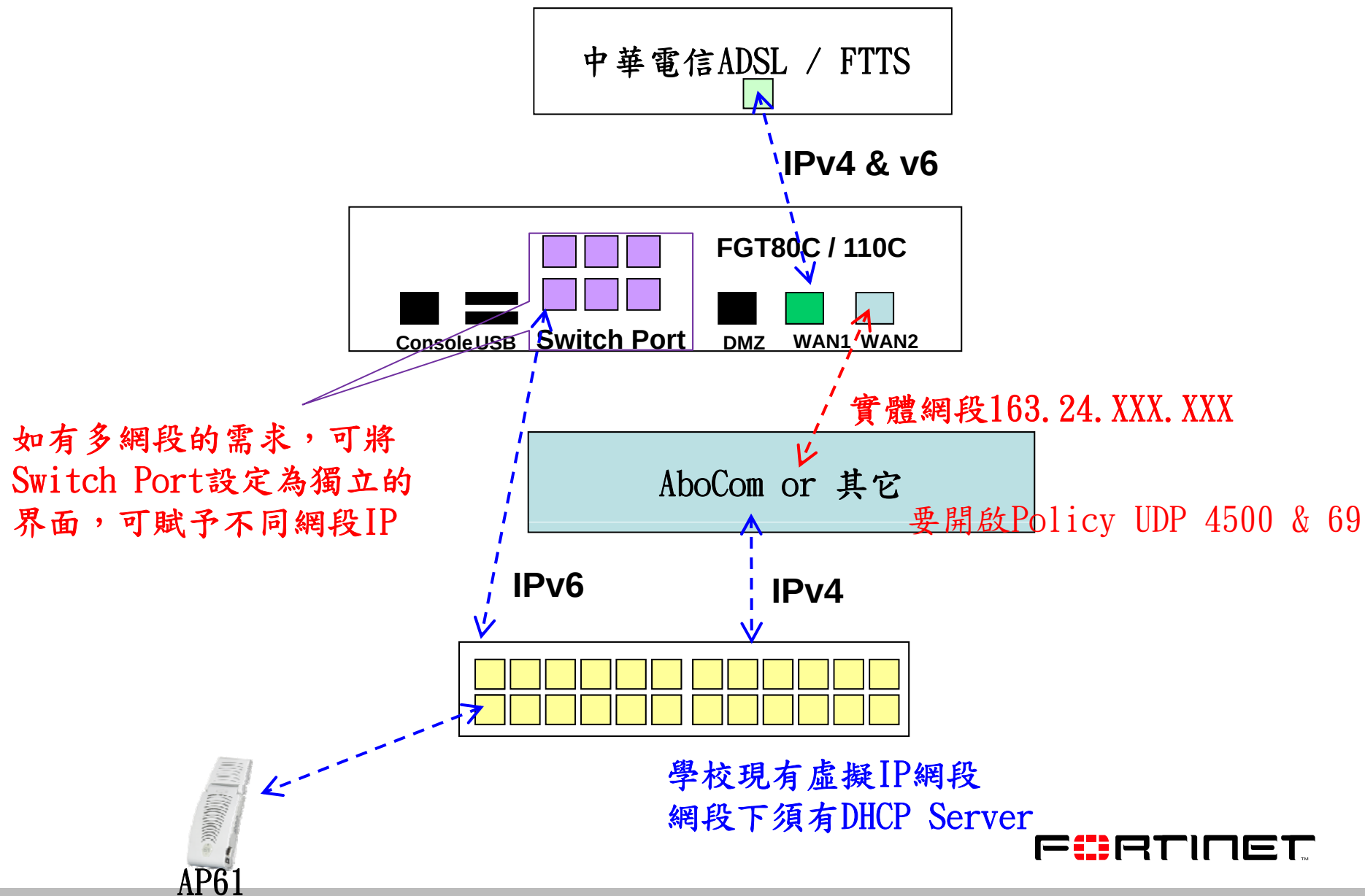
取代現有Router / 防火牆-110C



現有防火牆與Fortigate並存—原防火牆支援IPv6



現有防火牆與Fortigate並存—原防火牆不支援IPv6



注意事項

- 1 、Switch Port預設的網段192.168.168.0/24 ，可依實際需求變更
- 2 、Switch Port設定成獨立界面模式後，每一個Port都可以設定不同網段IP ，以及DHCP功能
- 3 、如將現有防火牆策略移植到FGT80C / 110C ，須確保UDP69 / 4500開啟
- 4 、FGT80C / 110C與現有防火牆並存，現有防火牆須開啟UDP69 / 4500
- 5 、WAN1的IP設定不可更改，如異動會造成對外網路不通

Agenda

1	設備基本功能簡介
2	架構簡介
3	IPv6簡介
4	防火牆設定注意事項
5	Log & Session的應用
6	Q&A

IPv6簡介

IPv6位址長度為**128**位元，

IPv6位址寫法為**八組四個位數的16進位數字**，中間用冒號分隔，且部分零可省略
例如：1234:5678:ffff:abcd:0000:0abf:12b0:0001

子網首碼長度：/16 /32 /48 /64 /80 /96 /112 /128

多個零可以被縮寫如下：

1、在每四個位數的區段，前面的零可以被消去，例如"0102"可以被縮寫成"102"而"0000"可以被縮寫成"0"

2、同一列中**四個零的集合可以被縮寫成兩個冒號(::)**。但，兩個冒號的縮寫**只能在每個位址中出現一次**

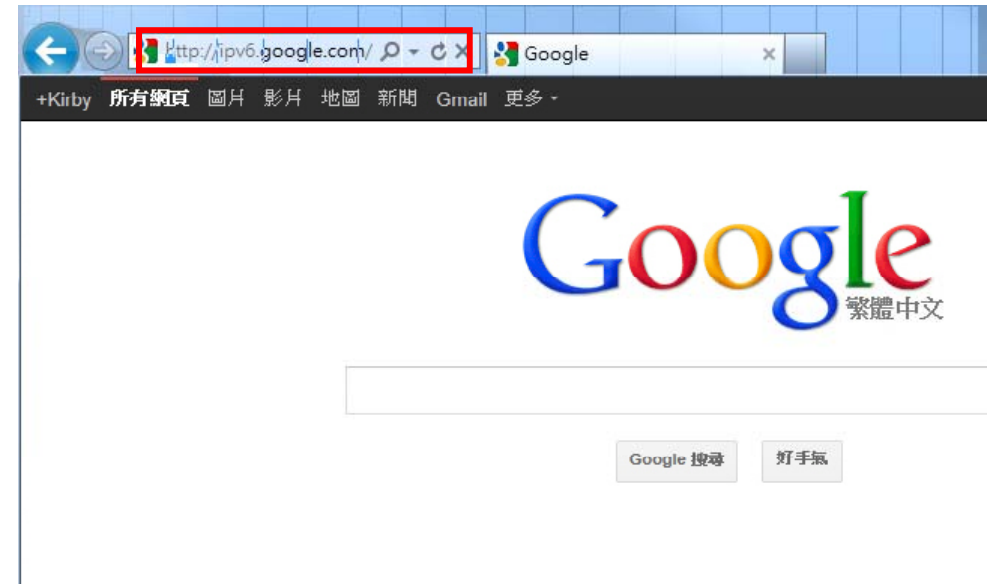
3、下面給的例子可以縮寫成如下：

3ffe:0102:0000:0000:0000:0000:0000:0000/32

消去每四個位數集合前面的零 3ffe:102:0:0:0:0:0:0/32

用雙冒號取代連續的零集合 3ffe:102::/32

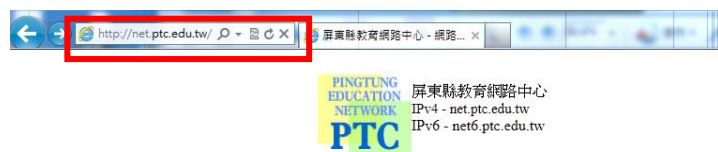
IPv6-網址輸入方式



輸入方式：

- 1、網址：<http://ipv6.google.com>
- 2、IPv6 IP：[http://\[2001:b000:180:3::5\]](http://[2001:b000:180:3::5])

IPv6-學校IPv6網段查詢



*公告
屏東縣教育網路中心無線網路/漫遊密碼單領用表 請至文件下載區下載

*屏東縣教育網路中心-網路使用說明聯結
NGN 新一代校園寬頻有線及無線網路
無線網路專區
屏東縣教育網路各校連網記錄

*NGN 無線基地台統計數量即時統計
目前無線基地台上線數AP: 257

NGN 防火牆統計數量 2011/05/31
總學校數 231 所學校
可連網學校數 222 所學校
無法連網學校數 9 所學校

1、http://net.ptc.edu.tw



2、點選『屏東縣IPv6網段分配表』

屏東縣(市)各級中小學IPv6網段									
學校資料			IPv6資料						
區域	學校名稱	網域	設備型號	學校 IPv6 網段	學校 UTM LAN (wan2)	學校 UTM (internal)	學校 UTM IPv6 Tunnel IP	中心 IPv6 Tunnel IP	
九如鄉	萬興國小	hnps	FGT80C	2001:288:874a::/48	2001:288:874a:1::1/64	2001:288:874a:2::1/64	2001:288:86ff:ffff:ffff:4a01/124	2001:288:86ff:ffff:ffff:4a02/124	
九如鄉	玉水分校	ysbh	FGT80C	2001:288:874b::/48	2001:288:874b:1::1/64	2001:288:874b:2::1/64	2001:288:86ff:ffff:ffff:4b01/124	2001:288:86ff:ffff:ffff:4b02/124	
九如鄉	三多國小	sdes	FGT80C	2001:288:874c::/48	2001:288:874c:1::1/64	2001:288:874c:2::1/64	2001:288:86ff:ffff:ffff:4c01/124	2001:288:86ff:ffff:ffff:4c02/124	
三地鄉	遠東分校	dibh	FGT80C	2001:288:87c5::/48	2001:288:87c5:1::1/64	2001:288:87c5:2::1/64	2001:288:86ff:ffff:ffff:c501/124	2001:288:86ff:ffff:ffff:c502/124	
三地鄉	大社分校	dsbh	FGT80C	2001:288:87c7::/48	2001:288:87c7:1::1/64	2001:288:87c7:2::1/64	2001:288:86ff:ffff:ffff:c701/124	2001:288:86ff:ffff:ffff:c702/124	
三地鄉	德文分校	dwubh	FGT80C	2001:288:87c6::/48	2001:288:87c6:1::1/64	2001:288:87c6:2::1/64	2001:288:86ff:ffff:ffff:c601/124	2001:288:86ff:ffff:ffff:c602/124	
三地鄉	口社國小	kse	FGT80C	2001:288:87ca::/48	2001:288:87ca:1::1/64	2001:288:87ca:2::1/64	2001:288:86ff:ffff:ffff:ca01/124	2001:288:86ff:ffff:ffff:ca02/124	
三地鄉	青葉國小	cyes	FGT80C	2001:288:87cb::/48	2001:288:87cb:1::1/64	2001:288:87cb:2::1/64	2001:288:86ff:ffff:ffff:cb01/124	2001:288:86ff:ffff:ffff:cb02/124	
三地鄉	萬興國小	scs	FGT80C	2001:288:87cb::/48	2001:288:87cb:1::1/64	2001:288:87cb:2::1/64	2001:288:86ff:ffff:ffff:cb01/124	2001:288:86ff:ffff:ffff:cb02/124	
三地鄉	三地國小	sdps	FGT80C	2001:288:87c4::/48	2001:288:87c4:1::1/64	2001:288:87c4:2::1/64	2001:288:86ff:ffff:ffff:c401/124	2001:288:86ff:ffff:ffff:c402/124	
內埔鄉	瑞華國小	aips	FGT80C	2001:288:877a::/48	2001:288:877a:1::1/64	2001:288:877a:2::1/64	2001:288:86ff:ffff:ffff:7a01/124	2001:288:86ff:ffff:ffff:7a02/124	
內埔鄉	廣智國小	chjs	FGT80C	2001:288:8775::/48	2001:288:8775:1::1/64	2001:288:8775:2::1/64	2001:288:86ff:ffff:ffff:7501/124	2001:288:86ff:ffff:ffff:7502/124	
內埔鄉	萬田國小	tps	FGT80C	2001:288:877e::/48	2001:288:877e:1::1/64	2001:288:877e:2::1/64	2001:288:86ff:ffff:ffff:7e01/124	2001:288:86ff:ffff:ffff:7e02/124	
內埔鄉	榮華國小	rhes	FGT80C	2001:288:8778::/48	2001:288:8778:1::1/64	2001:288:8778:2::1/64	2001:288:86ff:ffff:ffff:7801/124	2001:288:86ff:ffff:ffff:7802/124	
內埔鄉	新生國小	ssps	FGT80C	2001:288:8777::/48	2001:288:8777:1::1/64	2001:288:8777:2::1/64	2001:288:86ff:ffff:ffff:7701/124	2001:288:86ff:ffff:ffff:7702/124	
內埔鄉	泰安國小	taps	FGT80C	2001:288:877b::/48	2001:288:877b:1::1/64	2001:288:877b:2::1/64	2001:288:86ff:ffff:ffff:7b01/124	2001:288:86ff:ffff:ffff:7b02/124	
內埔鄉	育英國小	yips	FGT80C	2001:288:8774::/48	2001:288:8774:1::1/64	2001:288:8774:2::1/64	2001:288:86ff:ffff:ffff:7401/124	2001:288:86ff:ffff:ffff:7402/124	
竹田鄉	竹田國中	th	FGT80C	2001:288:870f::/48	2001:288:870f:1::1/64	2001:288:870f:2::1/64	2001:288:86ff:ffff:ffff:0f01/124	2001:288:86ff:ffff:ffff:0f02/124	

3、查看所屬『學校IPv6網段』

IPv6-賦予介面IPv6 IP \系統管理\網路\介面

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
- VPN

介面 區域 選項 DNS資料庫 網

新增 Switch Mode [欄位設定]

名稱	IP/遮罩	管理存取	管理狀態	連結狀態	
dmz	0.0.0.0 / 0.0.0.0		+	+	
internal1 (Wireless)	192.168.10.254 / 255.255.255.0	HTTP,HTTPS	+	+	
internal2 (Bonnie_LAN)	192.168.20.254 / 255.255.255.0	HTTP,HTTPS	+	+	
internal3	192.168.30.254 / 255.255.255.0		+	+	
internal4	0.0.0.0 / 0.0.0.0	HTTPS	+	+	
internal5	0.0.0.0 / 0.0.0.0		+	+	
internal6	0.0.0.0 / 0.0.0.0		+	+	
wan1 (Hinet)	122.117.250.48 / 255.255.255.255	HTTPS	+	+	
wan2	0.0.0.0 / 0.0.0.0		+	+	

網路介面

名稱 internal1 (00:09:0F:28:43:CE)
別名 Wireless
連結狀態 開啟

位址模式
☒ 用戶定義 ☐ DHCP ☐ PPPoE

IP網址/網路遮罩: 192.168.10.254/255.255.255.0
IPv6 地址: ::/0

☐ 啟動one-arm sniffer

參考各校IPv6網段

IPv6-靜態路由 \路由設定\靜態路由\靜態路由

系統管理

路由設定

靜態路由

動態路由

路由狀態

防火牆

UTM

VPN

使用者認證

靜態路由

政策路由

新增

路由

IPv6 路由

IP網址/遮罩

新增路由

目的 IP/網路遮罩

設備

網路閘

允許

取消

ATM：設備設Tunnel6

HTTS：設備設wan1

參考各校IPv6網段

HINET

IPv6-策略設定\防火牆\防火牆策略\IPv6政策

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

負載平衡

保護內容表

UTM

VPN

使用者認證

Endpoint NAC

無線網路控制器

紀錄與報表

防火牆策略 DoS政策 Sniffer政策 **IPv6政策**

建立輸出策略

來源介面/域名 dmz

來源位址名稱 ----- 網路位址 ----- 多個

目的介面/域名 internal(NAT_LAN)

目的位址名稱 ----- 網路位址 ----- 多個

排程 always

服務 ANY 多個

採取行動 ACCEPT

☐ 保護內容表 unfiltered

☐ 流量控制 [請選擇]

☐ 反向流量塑型 [請選擇]

☐ 紀錄合法流量

註解 (最多 63 字元)

允許 取消

設定 來源介面/位址

目的介面/位址

服務與採取行動

IPv6-DHCP設定步驟

config system interface

進入系統的介面

edit "DMZ"

針對" DMZ" Port設定

config ipv6

設定IPv6

set ip6-address 2001:288:87ff:1:1/64

賦予DMZ Port IPv6的IP

set ip6-allowaccess ping https ssh http telnet

設定允許哪些協定連線DMZ Port(管理用)

config ip6-prefix-list

設定IPv6要廣播的字首範圍

edit 2001:288:87ff:1::/64

廣播範圍

set autonomous-flag enable

啟動自治區旗標, 告知Client誰在發IP

Next

End

set ip6-send-adv enable

將IPv6的資訊廣播

end

IPv6-啟用



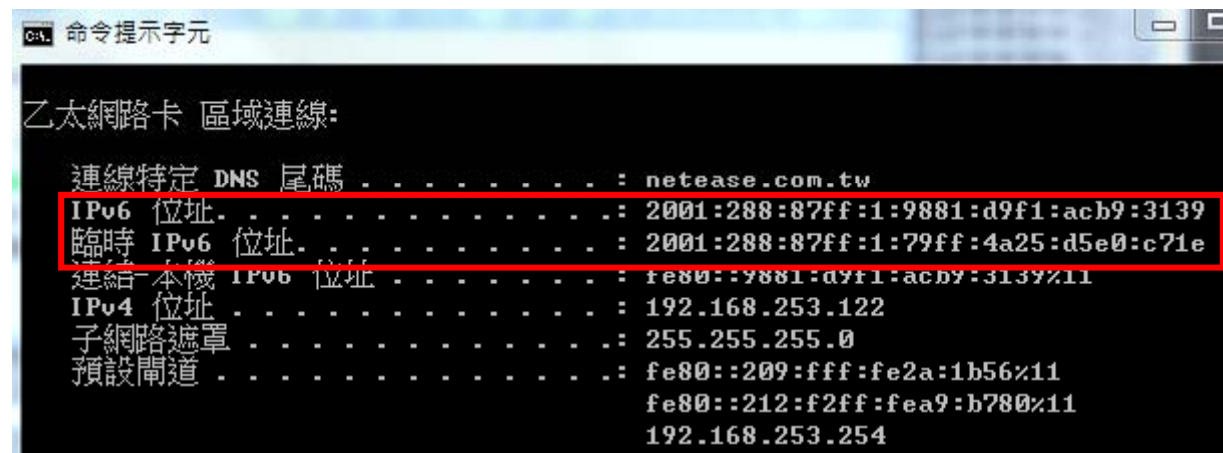
WinXP

1、進入命令提示字元，輸入 `ipv6 install`



2、安裝ipv6元件後，輸入 `ipconfig`

3、查看乙太網路卡 區域連線是否有取得所屬學校網段的IP。例如 `2001:288:87ff:XXXX:XXXX:XXXX:XXXX:XXXX`

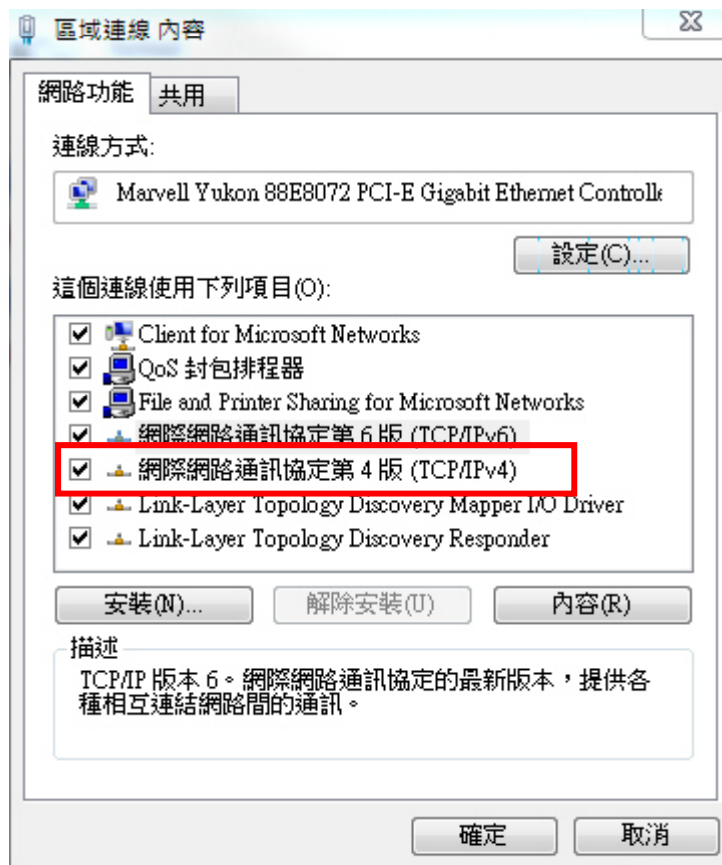


4、測試是否安裝完成→
`ping6 ::1`

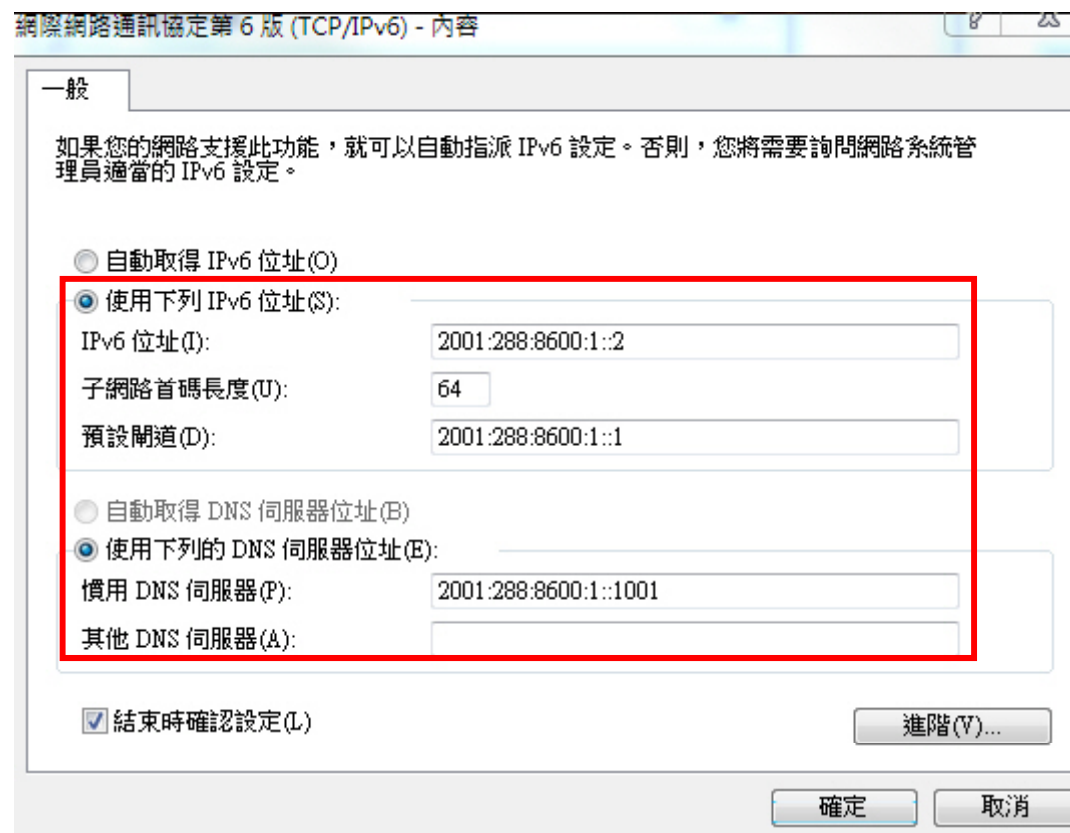
IPv6-Windows IP設定

範例：

IPv6 IP : 2001:288:8600:1::2 / 開道 : 2001:288:8600:1::1 / DNS : 2001:288:8600:1::1001



1、開啟區域網路連線，選擇網際網路通訊協定第6版(TCP/IP)



2、輸入IPv6位址、子網路首碼長度、預設開道、DNS伺服器IP，完成點選確定

FORTINET

IPv6-Linux(CentOS)IP設定

```
root@wireless:~ [80x24]
連線(C) 編輯(E) 檢視(V) 視窗(W) 選項(O) 說明(H)
[root@wireless ~]# vi /etc/sysconfig/network-scripts/ifcfg-eth0
[root@wireless ~]#
[root@wireless ~]#
```

```
root@wireless:~ [80x24]
連線(C) 編輯(E) 檢視(V) 視窗(W) 選項(O) 說明(H)
Advanced Micro Devices [AMD] 79c970 [PCnet32 LANCE]
DEVICE=eth0
BOOTPROTO=static
BROADCAST=163.24.239.255
HWADDR=00:50:56:87:57:87
IPADDR=163.24.239.115
IPV6ADDR=2001:288:8600:1::115/64
IPV6INIT=yes
IPV6_DEFAULTGW=2001:288:8600:1::1
NETMASK=255.255.255.0
NETWORK=163.24.239.0
ONBOOT=yes

"/etc/sysconfig/network-scripts/ifcfg-eth0" 12L, 289C
```

範例：

IPv6 IP：2001:288:8600:1::115/64

開道：2001:288:8600:1::1

1、輸入

vi /etc/sysconfig/network-scripts/ifcfg-eth0

2、新增

IPV6ADDR=IPv6 IP

IPV6INIT=yes

IPV6_DEFAULTGW=開道IP

3、存檔

IPv6-Web IP

校內的Web IPv6 IP統一為：

2001:288:XXXX:1::10 / 開道： 2001:288:XXXX:1::1 (Server在WAN2網段)

2001:288:XXXX:2::10 / 開道： 2001:288:XXXX:2::1 (Server在Internal網段)

網路介面	
名稱	wan2 (00:09:0F:C9:CC:DF)
別名	LAN
連結狀態	關閉
位址模式	
☒ 用戶定義 ☐ DHCP ☐ PPPoE	
IP網址/網路遮罩:	163.24.13.250/255.255.255.128
IPv6 地址:	2001:288:87c4:1::1/64

網路介面	
名稱	internal (00:09:0F:C9:CC:E1)
別名	NAT_LAN
連結狀態	開啟
位址模式	
☒ 用戶定義 ☐ DHCP ☐ PPPoE	
IP網址/網路遮罩:	192.168.1.250/255.255.255.0
IPv6 地址:	2001:288:87c4:2::1/64

Agenda

1	設備基本功能簡介
2	架構簡介
3	IPv6簡介
4	防火牆設定注意事項
5	Log & Session的應用
6	Q&A

虛擬IP 範例說明-Web Server在內部網段，設定的方式

新增虛擬網路對映

名稱: Web_Server

介面: wan1(WAN) **進入介面**

類型: 靜態 NAT

服務網路位址/範圍: 163.32.32.10 **Web Server對外實體IP**

要對映到的網路位址/範圍: 192.168.168.10 **Web Server虛擬的IP**

☒ 埠號轉換

網路協定: ☒ TCP ☐ UDP

外部服務埠: 80

要對映到的埠號: 80 **指定TCP 80埠**

允許 取消

2、防火牆必須新增 由Wan1→Internal

建立輸出策略

來源介面/域名: wan1(WAN)

來源位址名稱: all

目的介面/域名: internal(NAT LAN)

目的位址名稱: Web_Server

排程: always

服務: ANY

採取行動: ACCEPT

☐ NAT ☐ 動態 IP Pool

網頁過濾

範例說明-開心農場阻隔設定

系統管理
路由設定
防火牆
UTM
病毒檢查
入侵防禦
網頁過濾
Email Filter
資料外洩防護
應用軟體管控

Web 內容阻絕 網址過濾 跳過 本地網頁分類 本地網頁分級

新增

名稱 # 項目

新增

新列表

名稱 Web filter

註解 開心農場 (最多 63 字元)

允許 取消

※命名原則：有意義，易於解讀

網頁過濾 範例說明-開心農場阻隔設定(續)

Web 內容阻絕 | 網址過濾 | 跳過 | 本地網頁分類 | 本地網頁分級

名稱: Web filter

註解: 開心農場 (最多 63 字元) [允許]

[新增]

Pattern | 內容類型

新增

輸入欲阻隔的內容

新增禁止內容限制

採取行為: 封鎖

內容限制: 開心農場

內容限制類型: 正規式表示法

語言種類: 繁體中文

評分: 10

啟用: ☒

[允許] [取消]

正規式表示法：舉例→阻隔內容為開心農場，如內容有農場，並不會作阻隔

萬用字元：舉例→阻隔內容為農場，如內容有開心農場一樣作阻隔

評分：每找到一個阻隔元件的內容，得10分

網頁過濾

範例說明-開心農場阻隔設定(續)

將網址/頁阻隔設定加入內容表

The screenshot shows the Fortinet Web Filter configuration page. On the left sidebar, the '保護內容表' (Content Protection) menu item is highlighted with a red box. In the main area, the '新增' (Add) button is also highlighted with a red box. A blue callout box points to the '新增' button with the text: '將範例說明的Web filter 阻隔設定加入到保護內容表' (Add the Web filter blocking settings from the example to the content protection table).

The configuration form for '新增保護內容表' (Add Content Protection Table) is shown. The '保護內容表的名稱' (Content Protection Table Name) is 'Web filter'. The '註解' (Description) field is empty. The '協定識別' (Protocol Identification) section has '網頁過濾' (Web Filtering) checked. The '網頁內容阻絕' (Web Content Blocking) section has '網頁過濾' (Web Filtering) checked. The '選項' (Options) section has 'Web filter' selected, '門檻值: 20' (Threshold: 20) set, and 'PChome' selected. The '正常' (Normal) button is visible.

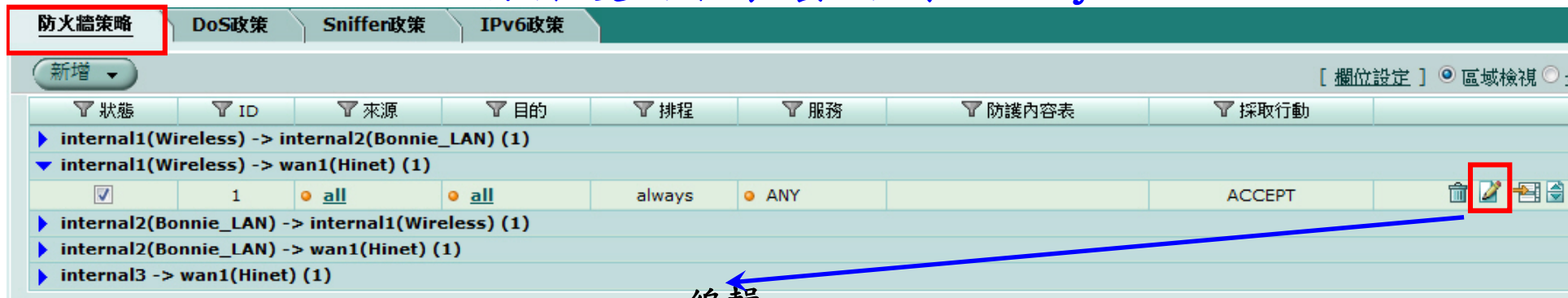
A red box highlights the '網頁內容阻絕' (Web Content Blocking) section. A blue callout box points to the '門檻值: 20' (Threshold: 20) setting with the text: '超過門檻值才阻隔' (Block only when the threshold is exceeded).

	HTTP	HTTPS	選項
網頁內容阻絕	☒		Web filter
網頁過濾	☒	☒	門檻值: 20
阻斷網頁續傳下載	☐		PChome
阻絕無效的URLs	☐	☐	
HTTP POST Action			正常
安全查詢			
Google			☐
Yahoo!			☐
Bing			☐

網頁過濾

範例說明-開心農場阻隔設定(續)

將保護內容表套用到Policy



編輯

編輯輸出策略

來源介面/域名: internal1(Wireless)

來源位址名稱: all 多個

目的介面/域名: wan1(Hinet)

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

☐ 開啟用戶政策

☒ 保護內容表: Web filter

☐ 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]

將範例說明的Web filter保護內容表套用在該筆Policy

RTINET

網頁過濾

範例說明-開心農場阻隔設定(續)

置換封鎖URL用戶端的顯示訊息

系統管理 高可靠性 SNMP v1/v2c 置換訊息 操作模式

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

名稱	描述	
郵件	無效電郵服務的提示訊息。	
HTTP	無效http服務的提示訊息。	
病毒訊息	遭受病毒感染網頁下載的提示訊息。	
感染快取訊息	替換緩存中下載的感染文件。	
file 阻絕訊息	被阻絕的網頁下載的提示訊息。	
檔案大小超過掃描設定訊息	遭受病毒感染網頁下載的提示訊息。	
DLP訊息	Replacement for data leak prevention downloads.	
DLP關鍵字訊息	Replacement for banned by data leak prevention.	
阻絕字彙訊息	網頁下載中包含阻絕字彙的提示訊息。	
內容類型封鎖訊息	Replacement for HTTP downloads of banned content-types.	
URL阻絕訊息	經由黑名單所阻絕網頁的提示訊息。	
http 用戶阻絕	被阻絕的網頁上傳的提示訊息。	
http 用戶防毒	遭受病毒感染網頁上傳的提示訊息。	
http 用戶檔案大小	遭受病毒感染網頁上傳的提示訊息。	
http 用戶不當字彙	網頁 上傳中包含阻絕字彙的提示訊息。	
POST 封鎖	Replacement for HTTP POST block.	

編輯

訊息設定: HTTP URL 阻絕訊息

允許格: HTML

大小: 8192 (字元)

Message Text:

<HTML><BODY>此網站已經被封鎖,如欲瀏覽此網站請洽資訊室</BODY></HTML>

允許

取消

FORTINET

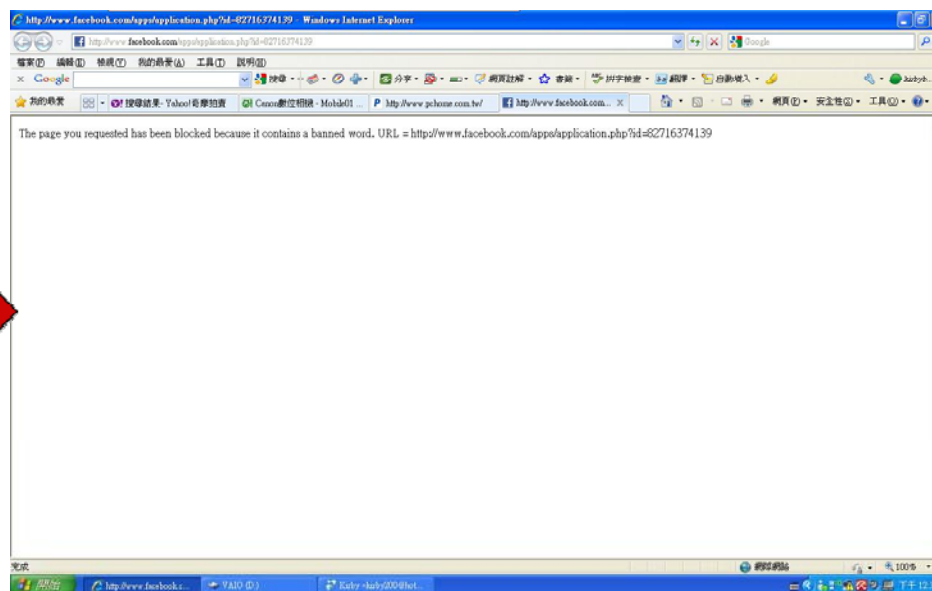
網頁過濾

範例說明-開心農場阻隔設定(續) 置換封鎖URL用戶端的顯示訊息

PChome網站



有開心農場內容的網站



IP Pool \防火牆\虛擬IP\IP Pool



名稱	起始位址	終止位址
OFFICE	163.24. .118	163.24. .123
STUDENT	163.24. .100	163.24. .115

可依不同的網段賦予不同的IP Pool

防火牆策略設定注意事項

1、防火牆策略有順序性，符合規則及採用的邏輯。

狀態	ID	來源	目的	排程	服務	防護內容表	採取行動
dmz -> wan1(WAN) (1)							
dmz -> wan2(LAN) (1)							
internal(NAT_LAN) -> wan1(WAN) (2)							
☒	1	all	all	always	ANY		ACCEPT
☒	6	all	all	always	跑跑		DENY
internal(NAT_LAN) -> wan2(LAN) (1)							
wan1(WAN) -> dmz (1)							
wan1(WAN) -> wan2(LAN) (1)							

wan1(Wan) -> switch(NAT_LAN) (4)							
☒	14	all	all	always	ANY		ACCEPT
☒	12	all	all	always	Service SIP SSH		ACCEPT
☒	10	all	Server 10 Server 100 Server 12 Server 120 Server 121 Server 15 Server 18 Server 19 Server 191 Server 20 Server 130 Server 11	always	DNS FTP HTTP POP3 SMTP SSH server 130		ACCEPT
☒	9	Service Lib	all	always	Allow service Lib		ACCEPT

2、策略中無定義的服務 / Port，代表Deny(拒絕存取)。

▼ port1(Subnet-0) -> wan1(Wan) (2)							
☒	5	<u>all</u>	<u>all</u>	always	○ DNS ○ FTP ○ HTTP ○ HTTPS ○ IMAP ○ IMAPS ○ PING ○ PING6 ○ POP3 ○ POP3S ○ RTSP ○ SQUID ○ SSH ○ TELNET ○ TFTP ○ IKE ○ <u>主計</u> ○ <u>win_auth</u>		ACCEPT
☒	9	<u>all</u>	<u>all</u>	always	○ ANY		DENY

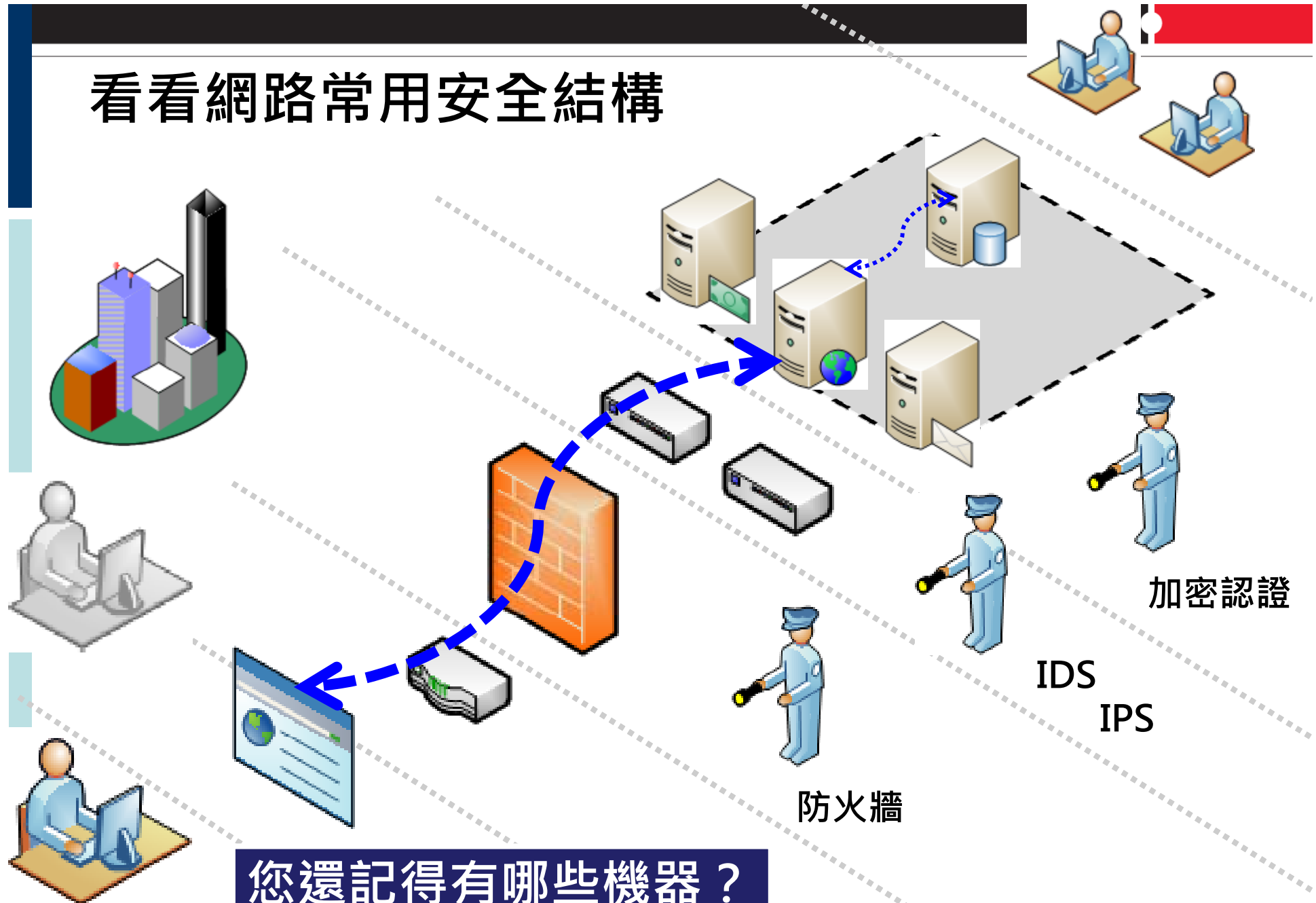
3、Deny(拒絕存取)的策略，建議放在最上層。

▼ wan1(Wan) -> wan2(LAN) (7)							
☒	15	- bad china - bad qay1	all	always	ANY		DENY
☐	13	all	dns	always	ANY		DENY
☒	10	block_mail	all	always	ANY		DENY
☒	8	all	all	always	- DNS - FTP - HTTP - HTTPS - IMAP - IMAPS - NNTP - PING - SMTP - SQUID - easyboard		ACCEPT
☒	7	jack_1	all	always	- SSH - LDAP - RDP		ACCEPT
☒	11	ptta	all	always	rsync		ACCEPT
☒	4	all	all	always	ANY		DENY

Agenda

1	設備基本功能簡介
2	架構簡介
3	IPv6簡介
4	防火牆設定注意事項
5	Log & Session的應用
6	Q&A

看看網路常用安全結構



您還記得有哪些機器？
已開啟哪些預設服務？

檢視防火牆的策略安全

狀態	ID	來源	目的	排程	服務	防護內容表	採取行動
▶	internal(NAT_LAN) -> wan1(WAN) (1)						
▶	internal(NAT_LAN) -> wan2(LAN) (1)						
▼	wan1(WAN) -> wan2(LAN) (1)						
☒	3	all	all	always	ANY		ACCEPT
▶	wan2(LAN) -> internal(NAT_LAN) (1)						
▶	wan2(LAN) -> wan1(WAN) (1)						

Wan1→Wan2 容許任何人利用任何服務長驅直入（**危險**）
建議限制來源IP / 目的IP / 服務

狀態	ID	來源	目的	排程	服務	防護內容表	採取行動
▶	internal(NAT_LAN) -> wan1(WAN) (1)						
▶	internal(NAT_LAN) -> wan2(LAN) (1)						
▼	wan1(WAN) -> internal(NAT_LAN) (2)						
☒	7	all	file	always	ANY		ACCEPT
☒	8	all	linmc	always	ANY		ACCEPT
▼	wan1(WAN) -> wan2(LAN) (1)						
☒	3	all	all	always	ANY		ACCEPT
▶	wan2(LAN) -> internal(NAT_LAN) (1)						
▶	wan2(LAN) -> wan1(WAN) (1)						

Wan1→Internal 容許任何人到File / linmc設備
Wan1→Wan2 容許任何人長驅直入（**危險**）
建議限制來源IP / 目的IP / 服務

紀錄啟用 \ 紀錄與報表 \ 記錄設定 \ 記錄設置

1. 至 紀錄與報表 > 記錄設定 > 事件記錄，將所要記錄行為的Log勾選

系統管理

路由設定

防火牆

UTM

VPN

使用者認證

Endpoint NAC

紀錄與報表

記錄設定

紀錄存取

隔離檔案

報表存取

紀錄設置

設定告警電子郵件

事件記錄

事件日誌

☒ 啓動

- ☒ 系統活動事件
- ☒ IPSec協商事件
- ☒ DHCP 服務事件
- ☒ L2TP/PPTP/PPPoE 服務事件
- ☒ 管理事件
- ☒ HA活動事件
- ☒ 防火牆認證事件
- ☒ Pattern更新事件
- ☒ SSL VPN 使用者認證事件
- ☒ SSL VPN 管理者事件
- ☒ SSL VPN 連線事件
- ☒ VIP 伺服器運作監控事件
- ☐ CPU與記憶體使用率(每5鐘)

採用

紀錄啟用 \防火牆\防火牆策略\防火牆策略



紀錄啟用 \ 防火牆 \ 保護內容表 \ 保護內容表

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

負載平衡

保護內容表

UTM

VPN

使用者認證

保護內容表

- 資訊洩漏保護感知器
- 應用程式控制
- 日誌

	日誌
防毒	
病毒記錄	☐
文件過濾記錄	☐
記錄超過掃描大小	☐
網頁過濾	
字彙封鎖記錄	☐
網址過濾記錄	☐
無效的網域名稱警告	☒
FortiGuard不當網頁過濾	
分類錯誤記錄(只有HTTP) (僅於 HTTP)	☒
郵件過濾	
垃圾郵件記錄	☐
入侵防禦	
入侵防護記錄	☐
應用程式控制	
紀錄應用程式控制	☐
資訊洩漏保護感知器	
記錄DLP	☐

允許 取消

檢視防火牆的紀錄啟用(續)

選擇網路流量

FortiAnalyzer 記憶體

日誌型態 網路流量

1 / 8456 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	來源	目的	服務	傳送	接收
1	2010-11-29	09:30:14	notice	allowed	2	192.168.253.156	168.95.1.1	53/udp	74	139
2	2010-11-29	09:30:13	notice	allowed	2	192.168.253.159	124.40.41.46	80/tcp	168	84
3	2010-11-29	09:30:13	notice	allowed	2	192.168.253.159	124.40.41.46	80/tcp	168	84
4	2010-11-29	09:30:13	notice	allowed	2	192.168.253.159	64.212.114.129	80/tcp	168	88
5	2010-11-29	09:30:13	notice	allowed	2	192.168.253.159	64.213.38.80	80/tcp	168	128
6	2010-11-29	09:30:13	notice	allowed	2	192.168.253.159	64.213.38.80	80/tcp	168	88
7	2010-11-29	09:30:13	notice	allowed	2	192.168.253.159	64.212.114.129	80/tcp	168	88
8	2010-11-29	09:30:13	notice	allowed	2	192.168.253.159	64.213.38.80	80/tcp	168	128
9	2010-11-29	09:30:13	notice	allowed	2	192.168.253.159	64.213.38.80	80/tcp	208	136
10	2010-11-29	09:30:13	notice	allowed	2	192.168.253.159	203.69.113.50	80/tcp	168	88
11	2010-11-29	09:30:12	notice	allowed	2	192.168.253.130	65.55.184.16	80/tcp	594	692
12	2010-11-29	09:30:11	notice	allowed	2	192.168.253.156	168.95.1.1	53/udp	74	139
13	2010-11-29	09:30:09	notice	allowed	2	192.168.253.155	210.242.196.104	80/tcp	1427	58329
14	2010-11-29	09:30:09	notice	allowed	2	192.168.253.156	168.95.1.1	53/udp	74	139
15	2010-11-29	09:30:09	notice	allowed	2	192.168.253.155	210.242.196.202	80/tcp	587	2249
16	2010-11-29	09:30:08	notice	allowed	2	192.168.253.155	118.165.44.182	13158/tcp	152	0
17	2010-11-29	09:30:08	notice	allowed	2	192.168.253.155	210.242.196.104	80/tcp	26694	1621983
18	2010-11-29	09:30:06	notice	allowed	2	192.168.253.155	168.95.1.1	53/udp	64	121
19	2010-11-29	09:30:06	notice	allowed	2	192.168.253.155	168.95.1.1	53/udp	64	381
20	2010-11-29	09:30:06	notice	allowed	2	192.168.253.156	168.95.1.1	53/udp	74	139

完整紀錄
來源IP到目的IP的訊息

FORTINET

即時紀錄查詢 \ 系統管理 \ 狀態 \ 最大的連線數

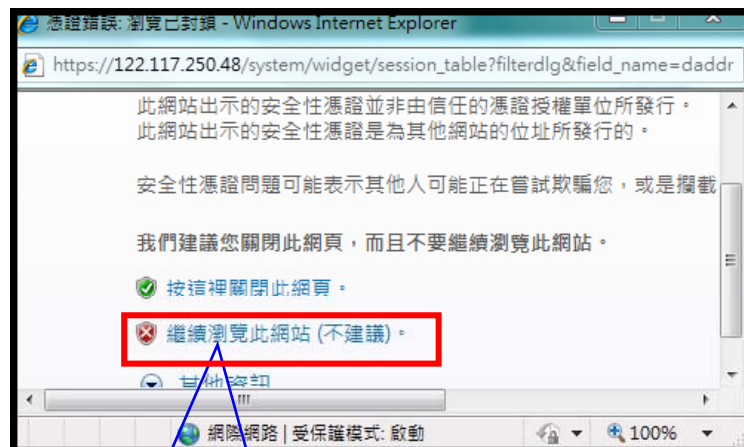


欲查詢目的地為
168.95.1.1的流量紀錄,點選目的地址

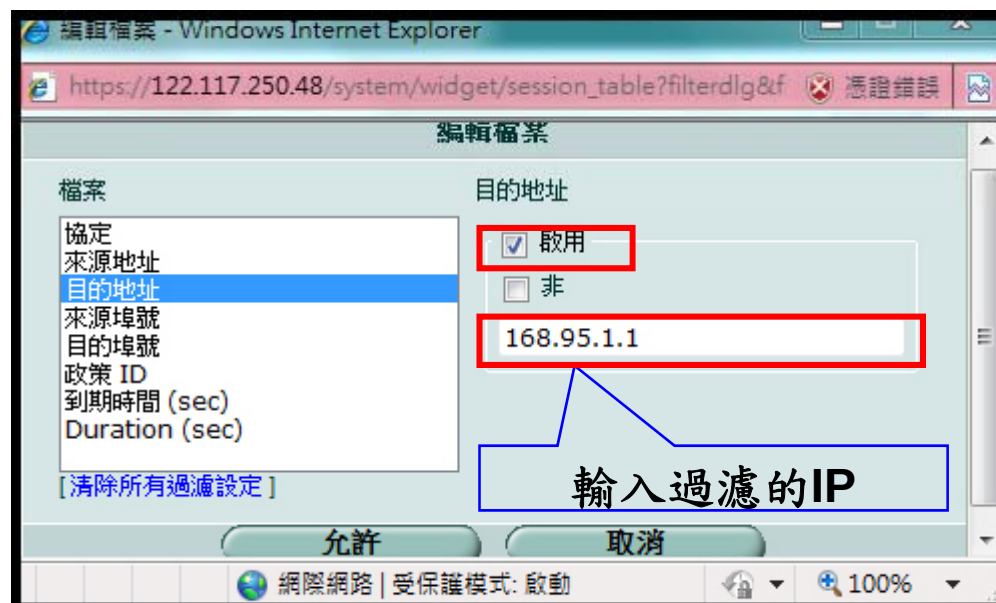
最大的連線數

總計: 55 清除所有過濾設定 返回

#	協定	來源地址	來源埠號	目的地址	目的埠號	政策 ID	到期
1	tcp	192.168.10.5	1190	111.248.9.85	13809	1	
2	tcp	192.168.10.5	1200	111.248.9.85	13809	1	
3	udp	192.168.10.5	3453	119.145.130.17	17788	1	1
4	udp	192.168.10.5	3453	119.145.130.20	17788	1	1
5	udp	192.168.10.5	3453	61.155.106.176	17788	1	1
6	udp	192.168.10.5	3453	61.155.106.169	17788	1	1
7	udp	192.168.10.5	3453	61.155.106.168	17788	1	1
8	udp	192.168.10.5	3453	61.155.106.166	17788	1	1
9	udp	192.168.10.5	3453	61.155.106.163	17788	1	1
10	udp	192.168.10.5	3453	218.85.135.94	8800	1	1
11	udp	192.168.10.5	3453	121.9.201.102	17788	1	1



跳出憑證錯誤畫面，
點選繼續瀏覽此網
站選項



最大的連線數

1 / 1 總計: 17 清除所有過濾設定 返回

#	協定	來源地址	來源埠號	目的地址	目的埠號	政策 ID	到期時間 (sec)
1	udp	192.168.10.5	58988	168.95.1.1	53	1	141
2	udp	192.168.10.5	59100	168.95.1.1	53	1	144
3	udp	192.168.10.5	60857	168.95.1.1	53	1	145
4	udp	192.168.10.5	60904	168.95.1.1	53	1	144
5	udp	192.168.10.5	60598	168.95.1.1	53	1	140
6	udp	192.168.10.5	62861	168.95.1.1	53	1	140
7	udp	192.168.10.5	64218	168.95.1.1	53	1	140
8	udp	192.168.10.5	50226	168.95.1.1	53	1	144
9	udp	192.168.10.5	50088	168.95.1.1	53	1	144
10	udp	192.168.10.5	50127	168.95.1.1	53	1	144
11	udp	192.168.10.5	50332	168.95.1.1	53	1	138

儲存紀錄查詢 \ 紀錄與報表 \ 紀錄存取 \ FortiAnalyzer



可選擇不同的日誌類型，
查閱相關的紀錄檔，找出
可能造成問
題的Log，再進一步的處
理

#	日期	時間	等級	子型式	識別碼	使用者介面	採取行動	訊息
1	2010-06-30	13:32:54	notice	admin	41989	GUI(112.104.125.110)	delete	User kirby deleted protection profile 'Web Filter' from GUI(112.104.125.110)
2	2010-06-30	13:32:48	notice	admin	41989	GUI(112.104.125.110)		User kirby changed IPv4 firewall policy 2 from GUI(112.104.125.110)
3	2010-06-30	13:32:41	notice	admin	41989	GUI(112.104.125.110)		User kirby changed IPv4 firewall policy 1 from GUI(112.104.125.110)
4	2010-06-30	13:13:10	information	admin	41990	https(112.104.125.110)	login	Administrator kirby logged in successfully from https(112.104.125.110)
5	2010-06-30	12:58:17	information	admin	41990	https(112.104.125.110)	logout	Administrator kirby timed out on https(112.104.125.110)
6	2010-06-30	12:19:42	notice	admin	41989	GUI(112.104.125.110)		User kirby changed IPv4 firewall policy 1 from GUI(112.104.125.110)
7	2010-06-30	12:19:17	notice	admin	41989	GUI(112.104.125.110)	modify	User kirby changed protection profile 'Web Filter' from GUI(112.104.125.110)



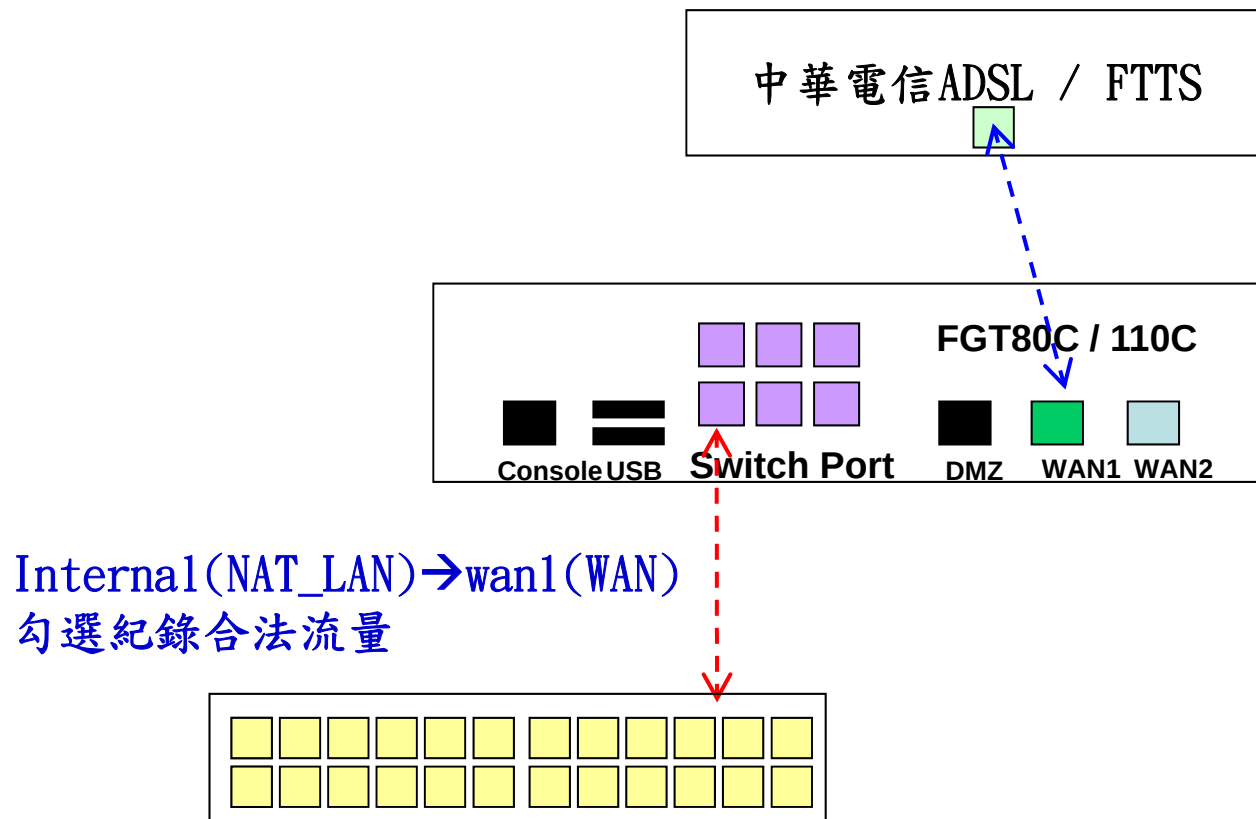
查詢系統事件,採取
行動,找出login行為
的Log

日誌型態 系統事件								
1 / 1 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	2010-06-30	13:13:10	information	admin	41990	https(112.104.125.110)	login	Administrator kirby logged in successfully from https(112.104.125.110)
2	2010-06-30	12:06:08	information	admin	41990	https(112.104.125.110)	login	Administrator kirby logged in successfully from https(112.104.125.110)
3	2010-06-30	11:29:28	information	admin	41990	https(122.117.142.235)	login	Administrator kirby logged in successfully from https(122.117.142.235)
4	2010-06-30	10:23:05	information	admin	41990	jsconsole	login	Administrator kirby logged in successfully from jsconsole
5	2010-06-30	10:11:20	information	admin	41990	jsconsole	login	Administrator kirby logged in successfully from jsconsole
6	2010-06-30	10:07:55	information	admin	41990	https(122.117.142.235)	login	Administrator kirby logged in successfully from https(122.117.142.235)

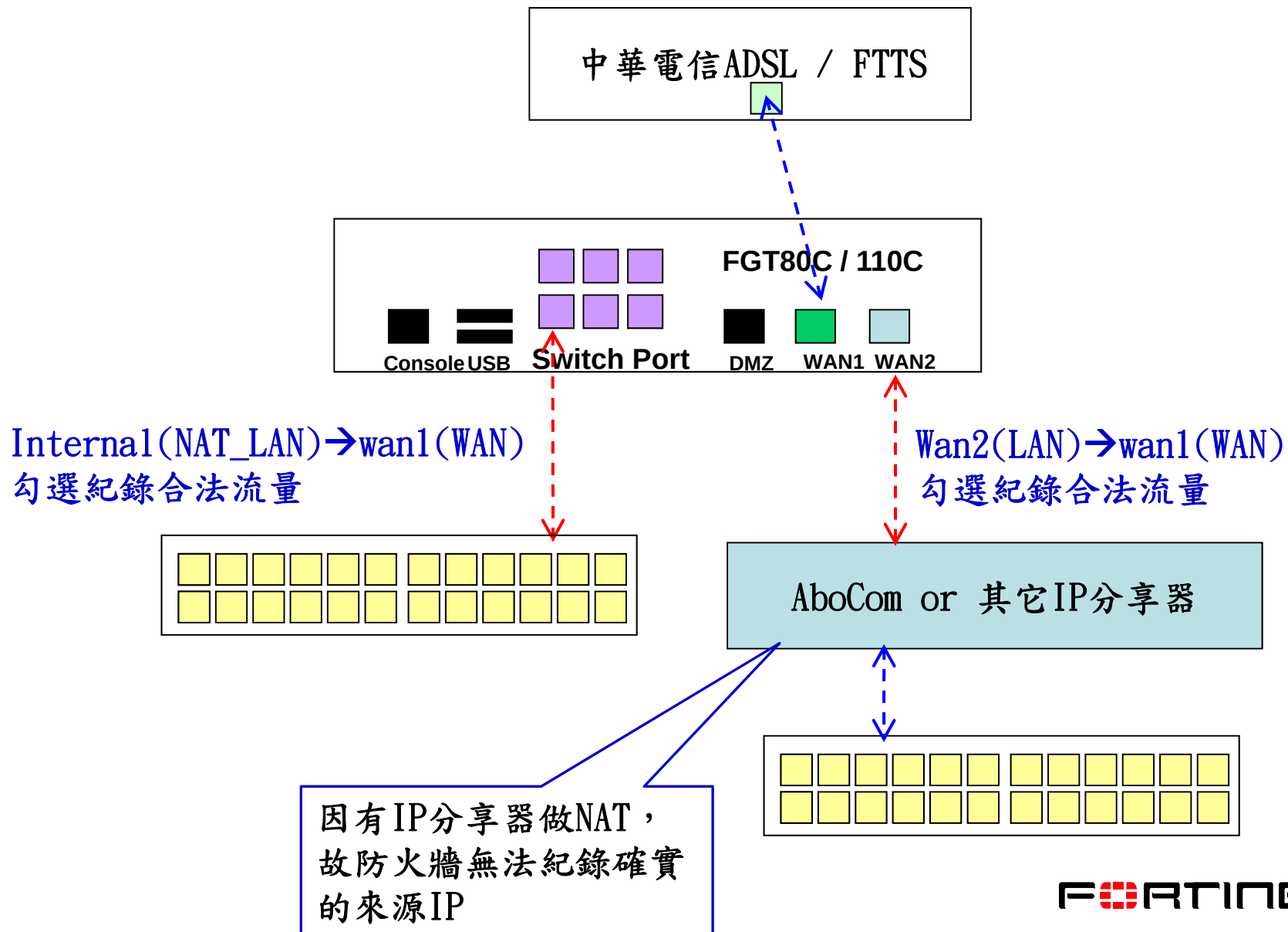
查詢該網站是因為
哪個關鍵字阻擋

FortiAnalyzer		記憶體							
日誌型態 網頁過濾									
   1 / 540  欄位設定 原始資料 清除所有過濾設定									
#	日期	時間	等級	來源	來源埠	目的	主機名稱	訊息	關鍵字
1	2011-07-01	11:52:52	warning	192.168.2.81	1181	119.160.246.241	tw.yahoo.com	URL was blocked because it contained banned word(s).	龍之刀
2	2011-07-01	11:52:00	warning	192.168.2.81	1125	119.160.246.241	tw.yahoo.com	URL was blocked because it contained banned word(s).	龍之刀
3	2011-07-01	11:51:54	warning	192.168.2.81	1123	119.160.246.241	tw.yahoo.com	URL was blocked because it contained banned word(s).	龍之刀
4	2011-07-01	11:51:21	warning	192.168.2.81	1122	74.125.71.190	www.youtube.com	URL was blocked because it contained banned word(s).	風之谷
5	2011-07-01	11:51:20	warning	192.168.2.81	1121	74.125.71.190	www.youtube.com	URL was blocked because it contained banned word(s).	風之谷
6	2011-07-01	11:50:11	warning	192.168.2.81	1079	74.125.71.190	www.youtube.com	URL was blocked because it contained banned word(s).	風之谷
7	2011-07-01	11:49:48	warning	192.168.2.81	1056	74.125.71.190	www.youtube.com	URL was blocked because it contained banned word(s).	風之谷
8	2011-07-01	09:09:19	warning	192.168.2.100	1476	74.125.71.132	azo-freeware.blogspot.com	URL was blocked because it contained banned word(s).	無界瀏覽
9	2011-07-01	09:09:10	warning	192.168.2.100	1473	74.125.71.132	azo-freeware.blogspot.com	URL was blocked because it contained banned word(s).	跑跑卡丁車
10	2011-07-01	09:08:59	warning	192.168.2.100	1470	74.125.71.132	azo-freeware.blogspot.com	URL was blocked because it contained banned word(s).	跑跑卡丁車
11	2011-06-29	11:52:14	warning	192.168.2.62	1098	203.84.192.95	tw.search.yahoo.com	URL was blocked because it contained banned word(s).	樂豆
12	2011-06-29	11:46:27	warning	192.168.2.73	1313	202.80.107.11	tw.beanfun.com	URL was blocked because it contained banned word(s).	樂豆
13	2011-06-29	11:45:07	warning	192.168.2.65	2168	66.220.147.57	apps.facebook.com	URL was blocked because it contained banned word(s).	開心農場
14	2011-06-29	11:40:08	warning	192.168.2.68	1452	204.152.214.178	sitetag.us	URL was blocked because it contained banned word(s).	女生遊戲網
15	2011-06-29	11:40:01	warning	192.168.2.68	1448	119.160.243.115	tw.wrs.yahoo.com	URL was blocked because it is in the URL filter list	
16	2011-06-29	11:40:00	warning	192.168.2.68	1446	203.84.192.95	tw.search.yahoo.com	URL was blocked because it is in the URL filter list	
17	2011-06-29	11:39:57	warning	192.168.2.68	1444	119.160.243.115	tw.wrs.yahoo.com	URL was blocked because it is in the URL filter list	
18	2011-06-29	11:39:56	warning	192.168.2.68	1441	203.84.192.95	tw.search.yahoo.com	URL was blocked because it is in the URL filter list	
19	2011-06-29	11:39:51	warning	192.168.2.68	1438	119.160.254.215	l.yimg.com	URL was blocked because it is in the URL filter list	
20	2011-06-29	11:39:25	warning	192.168.2.73	1260	203.84.192.95	tw.search.yahoo.com	URL was blocked because it contained banned word(s).	殭屍
21	2011-06-29	11:39:23	warning	192.168.2.68	1427	203.84.192.95	tw.search.yahoo.com	URL was blocked because it contained banned word(s).	火影忍者
22	2011-06-29	11:39:14	warning	192.168.2.73	1250	203.84.192.95	tw.search.yahoo.com	URL was blocked because it contained banned word(s).	火影忍者
23	2011-06-29	11:38:41	warning	192.168.2.73	1223	203.84.192.95	tw.search.yahoo.com	URL was blocked because it contained banned word(s).	火影忍者
24	2011-06-29	11:38:37	warning	192.168.2.73	1221	203.84.192.95	tw.search.yahoo.com	URL was blocked because it contained banned word(s).	火影忍者
25	2011-06-29	11:33:06	warning	192.168.2.53	1919	74.125.71.139	cbk0.google.com	URL was blocked because it contained banned word(s).	seer
26	2011-06-29	11:31:17	warning	192.168.2.65	1146	66.220.158.46	apps.facebook.com	URL was blocked because it contained banned word(s).	開心農場
27	2011-06-29	11:30:18	warning	192.168.2.68	1338	60.199.185.105	www.51mole.com.tw	URL was blocked because it contained banned word(s).	seer
28	2011-06-29	11:29:39	warning	192.168.2.61	1232	119.160.243.115	tw.wrs.yahoo.com	URL was blocked because it is in the URL filter list	
29	2011-06-29	11:29:39	warning	192.168.2.61	1230	203.84.192.95	tw.search.yahoo.com	URL was blocked because it is in the URL filter list	
30	2011-06-29	11:29:15	warning	192.168.2.61	1218	203.84.192.95	tw.search.yahoo.com	URL was blocked because it contained banned word(s).	cs online
31	2011-06-29	11:29:15	warning	192.168.2.73	1081	203.84.192.95	tw.search.yahoo.com	URL was blocked because it contained banned word(s).	開心農場
32	2011-06-29	11:29:11	warning	192.168.2.61	1216	119.160.243.115	tw.wrs.yahoo.com	URL was blocked because it is in the URL filter list	

檢視防火牆的紀錄啟用(續)

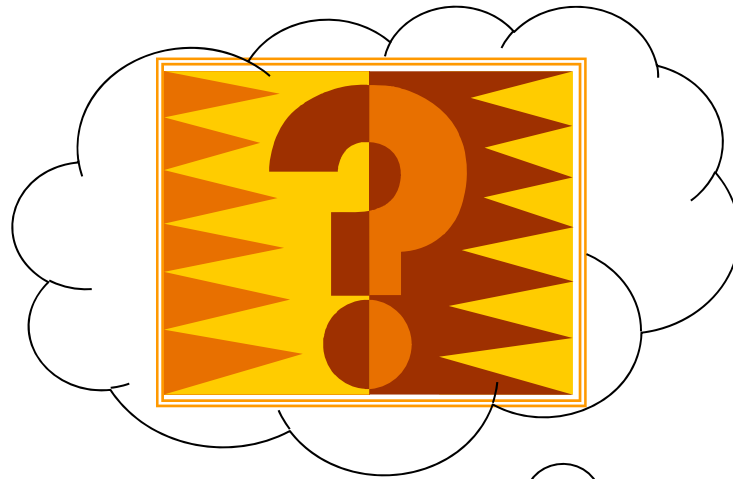


檢視防火牆的紀錄啟用(續)



Agenda

1	設備基本功能簡介
2	架構簡介
3	IPv6簡介
4	防火牆設定常見問題
5	Log & Session的應用
6	Q&A



FORTINET



Thank You!

NETEASE
ease your networks
用心服務 真誠對待
聯易科技股份有限公司