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

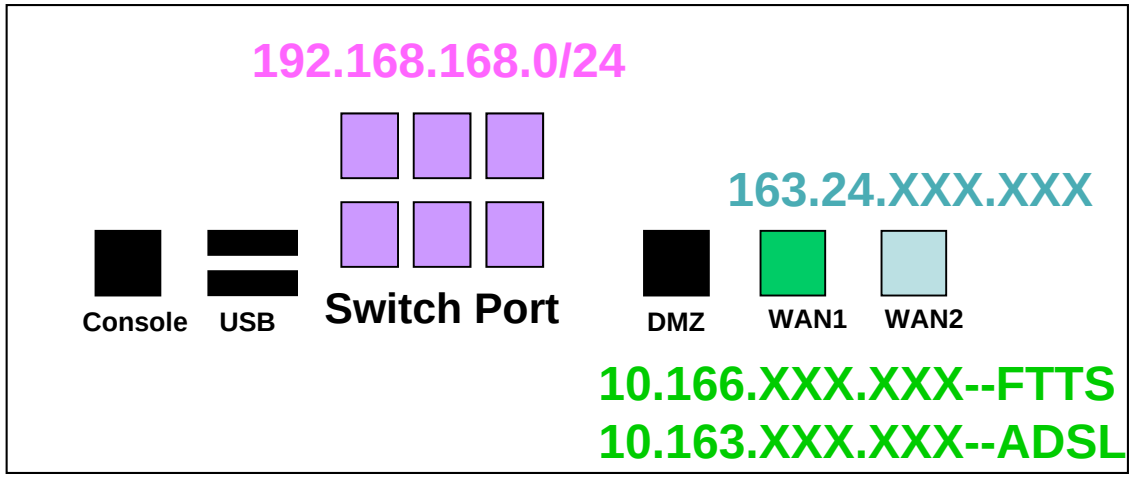
NETEASE
ease your networks

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

FORTINET

FTG-80C外觀

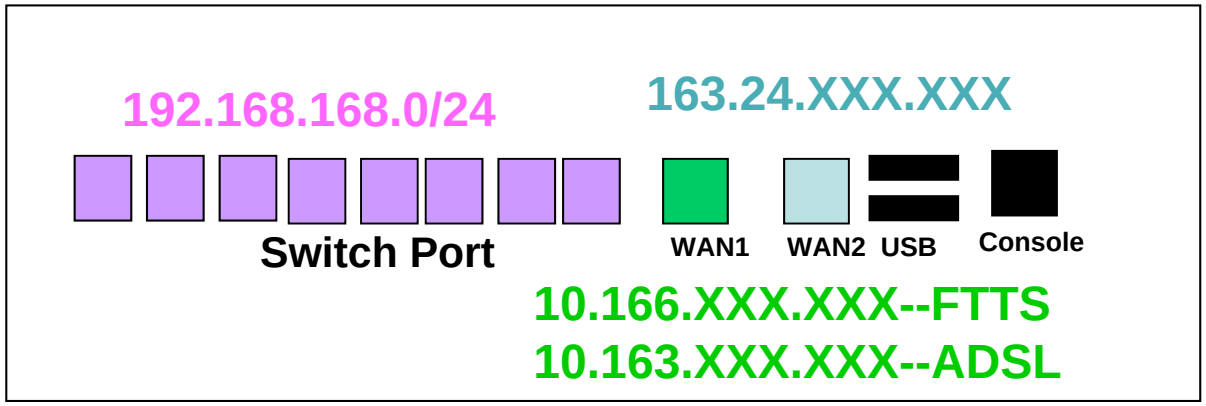


說明：

黑色：忽略不使用

其他三種顏色表示不同的網段

FTG-110C外觀

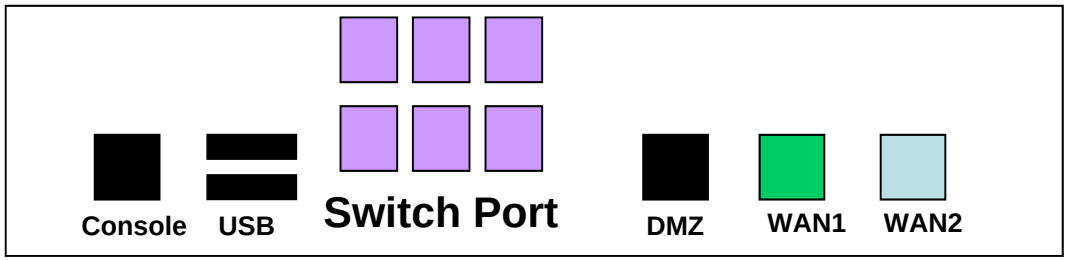


說明：

黑色：忽略不使用

其他三種顏色表示不同的網段

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：區域網路的連接埠；泛指一般內部網路

DMZ Port：非軍事區，介於內部網路(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

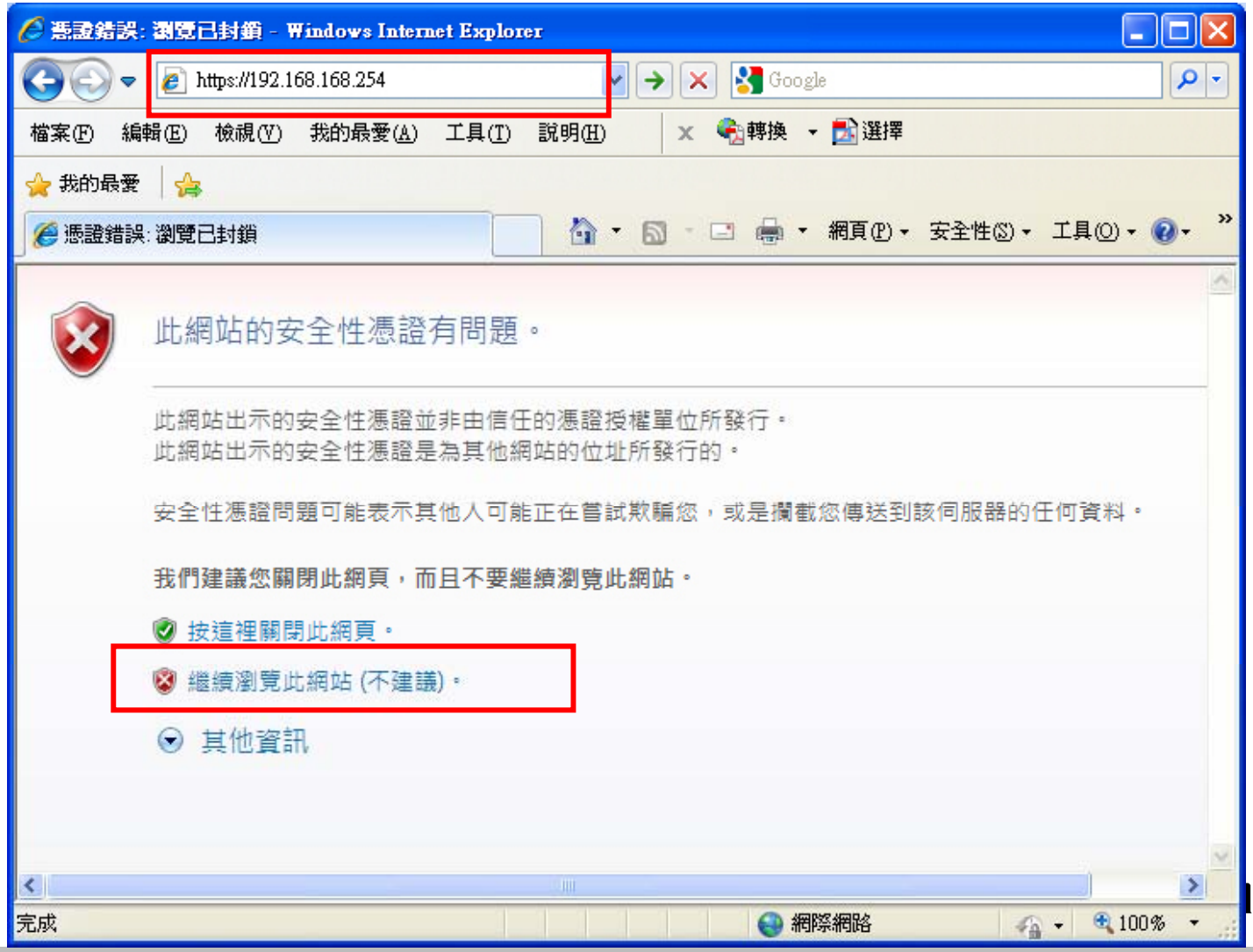
WAN1 Port：網際網路連結埠 1，一般接ADSL、對外網路線路、實體網段等……

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……

FORTINET

防火牆連線

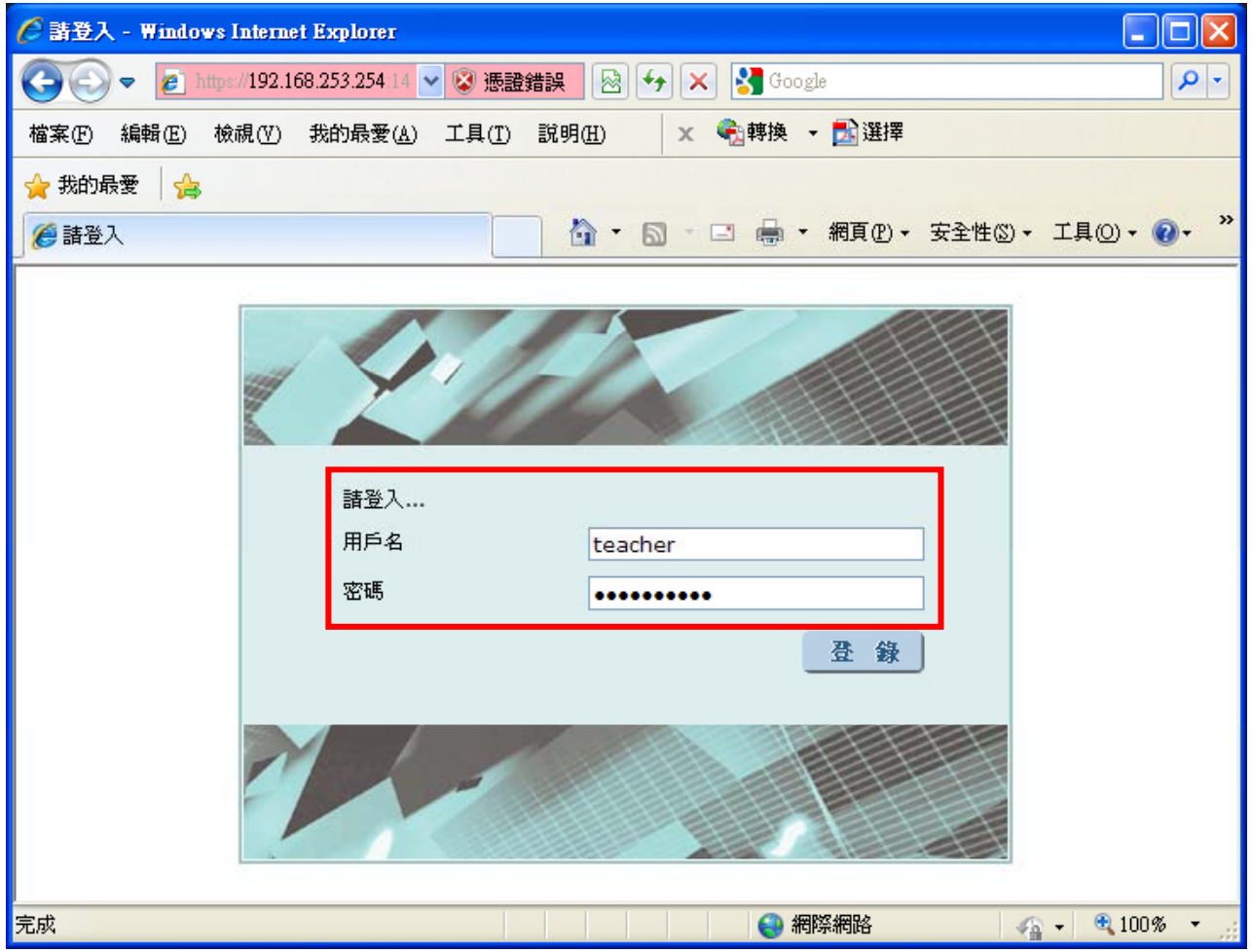
1.開啟瀏覽器，輸入防火牆的IP位址，點選【繼續瀏覽此網站（不建議）】
例： https://192.168.168.254（PC連接在Switch Port下）



2.輸入用戶名 / 密碼

teacher / teacher123→僅瀏覽權限

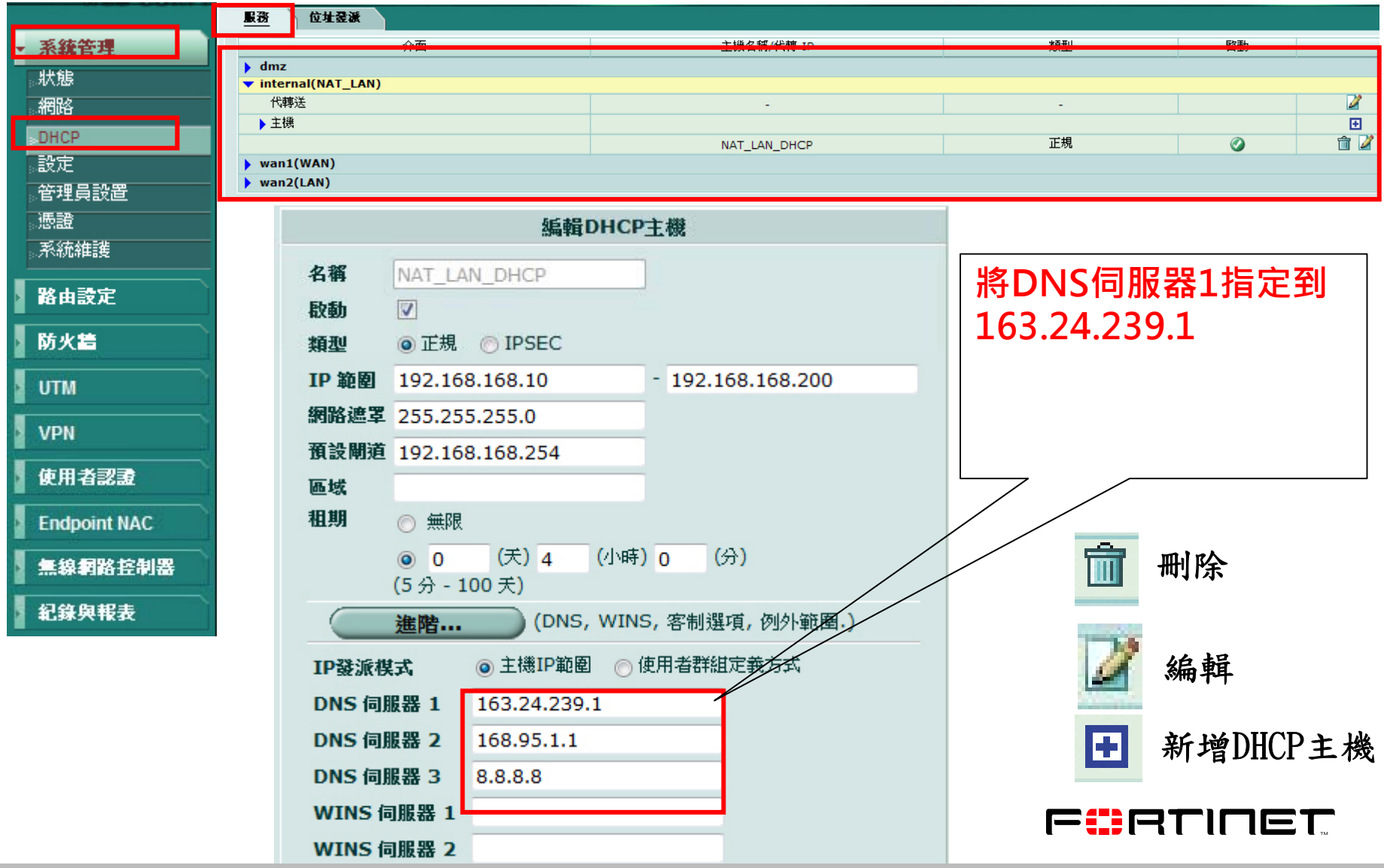
teacher2 / teacher456→擁有可修改的權限



語系變更 \System\Admin\Settings

各界面的IP設定 \系統管理\網路\介面

DHCP \系統管理\DHCP\服務



路由 \路由設定\靜態路由\靜態路由

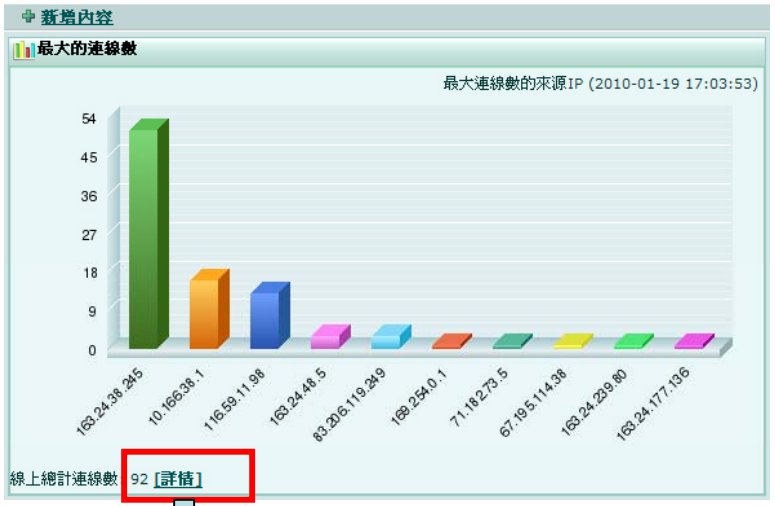
刪除

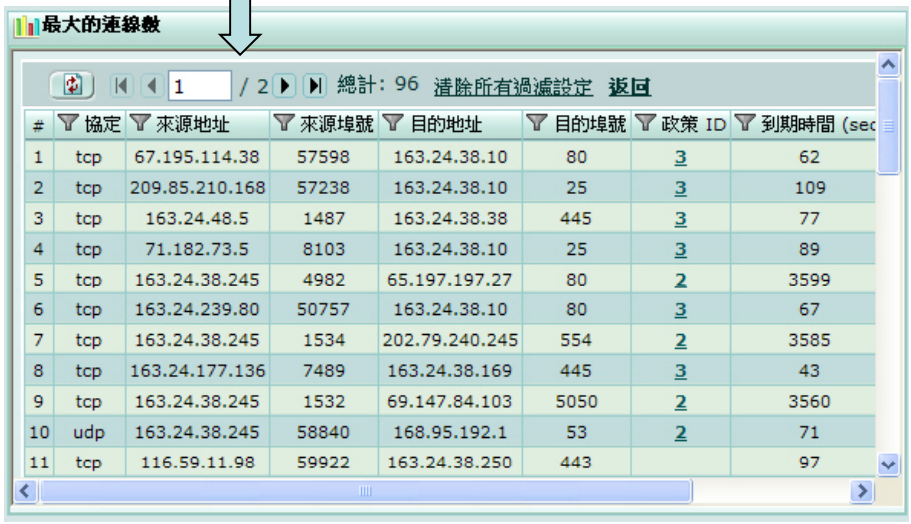
編輯

FORTINET

虛擬IP \防火牆\虛擬IP\虛擬IP\新增

流量查詢 \網路管理\狀態\面板\新增內容\最大的連線數

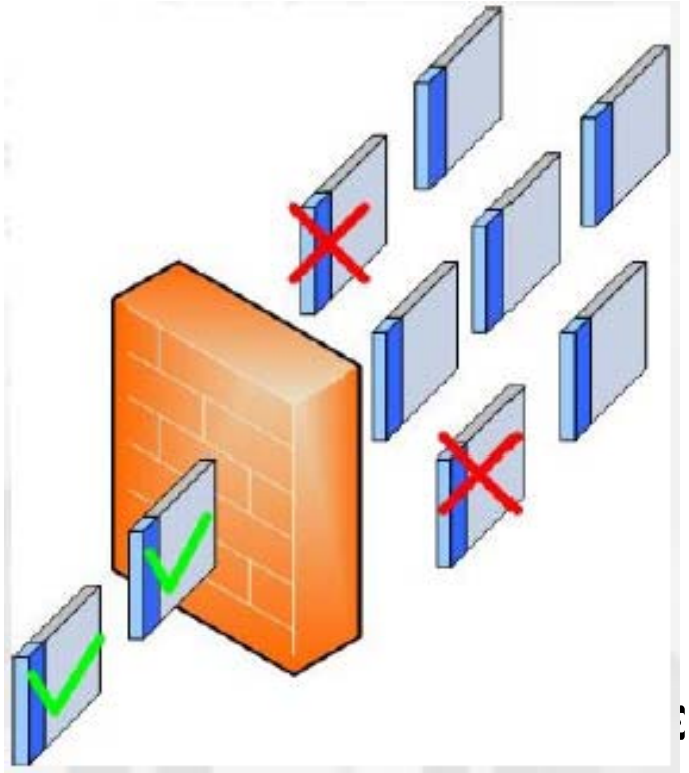




#	協定	來源地址	來源埠號	目的地址	目的埠號	政策 ID	到期時間 (sec
1	tcp	67.195.114.38	57598	163.24.38.10	80	3	62
2	tcp	209.85.210.168	57238	163.24.38.10	25	3	109
3	tcp	163.24.48.5	1487	163.24.38.38	445	3	77
4	tcp	71.182.73.5	8103	163.24.38.10	25	3	89
5	tcp	163.24.38.245	4982	65.197.197.27	80	2	3599
6	tcp	163.24.239.80	50757	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	1.1.70.250	ftp	36033	80

防火牆策略 \防火牆\防火牆策略\防火牆策略

完成後畫面

FORTINET

IP Pool \防火牆\虛擬IP\IP Pool

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	

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

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

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

#	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

點選本機磁碟機，將備份檔儲存在目前操作的電腦內

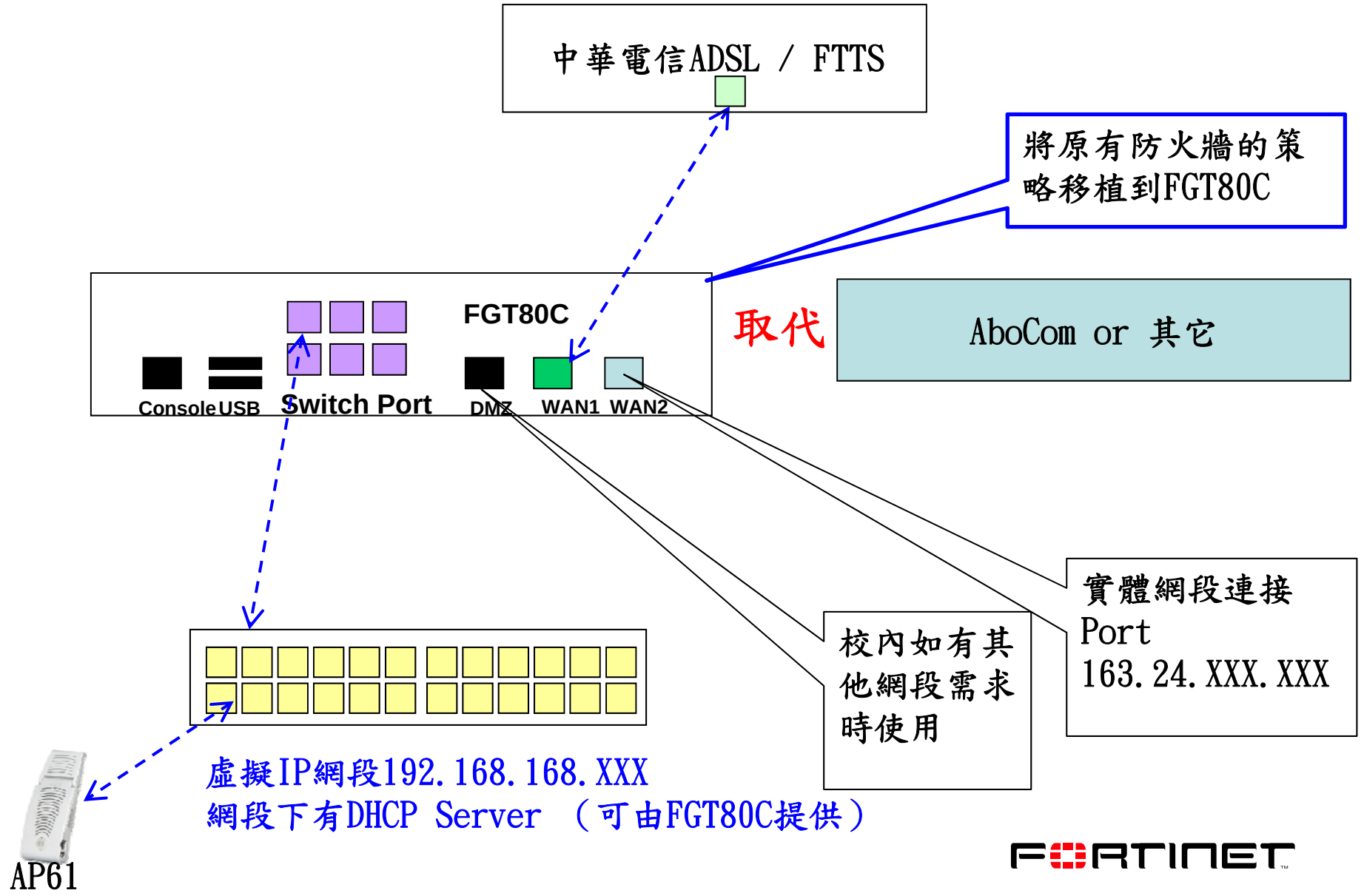
點選本機磁碟機，選擇瀏覽，從目前操作的電腦中選擇備份檔做還原

FORTINET

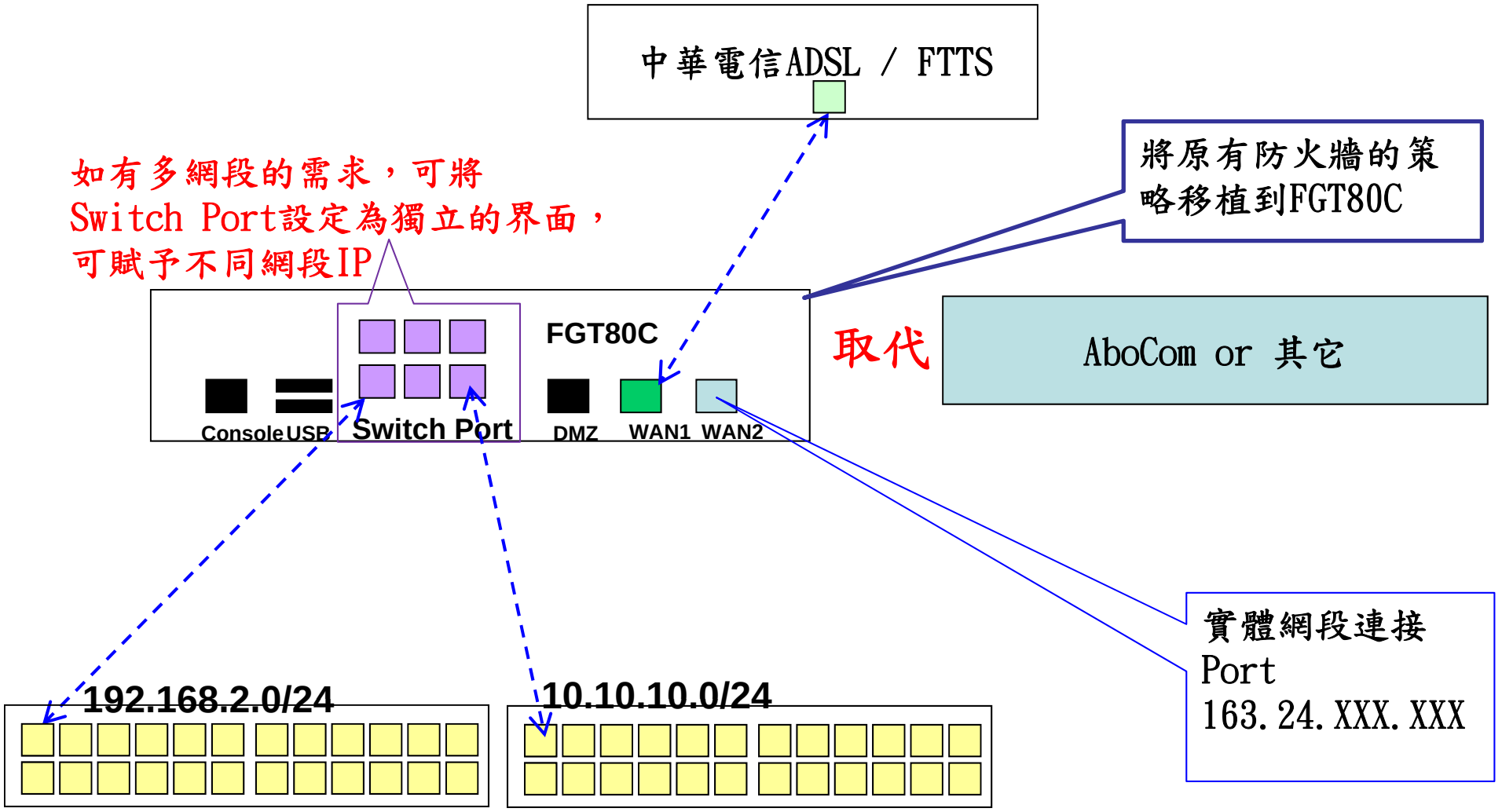
Agenda

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

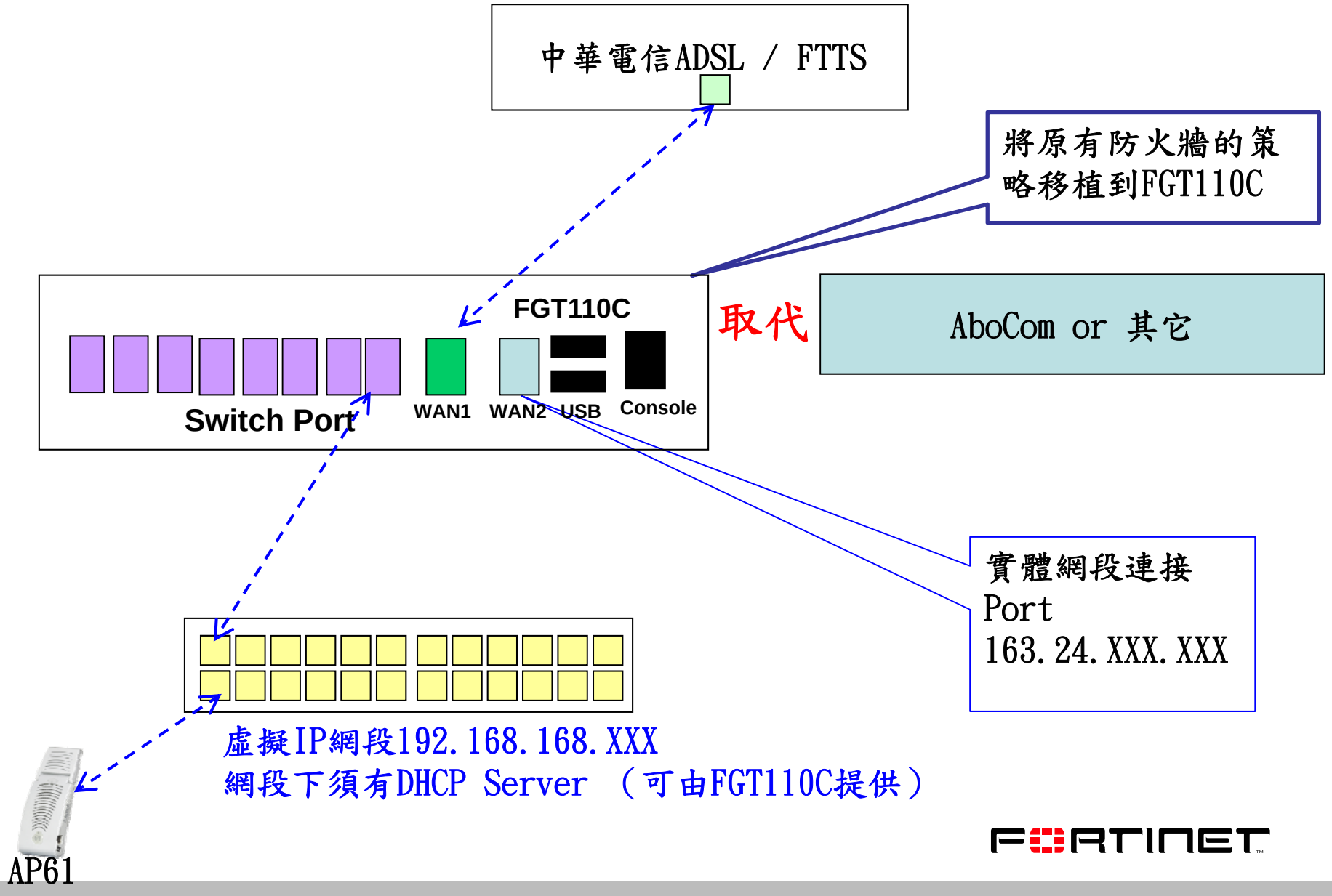
取代現有Router / 防火牆-80C



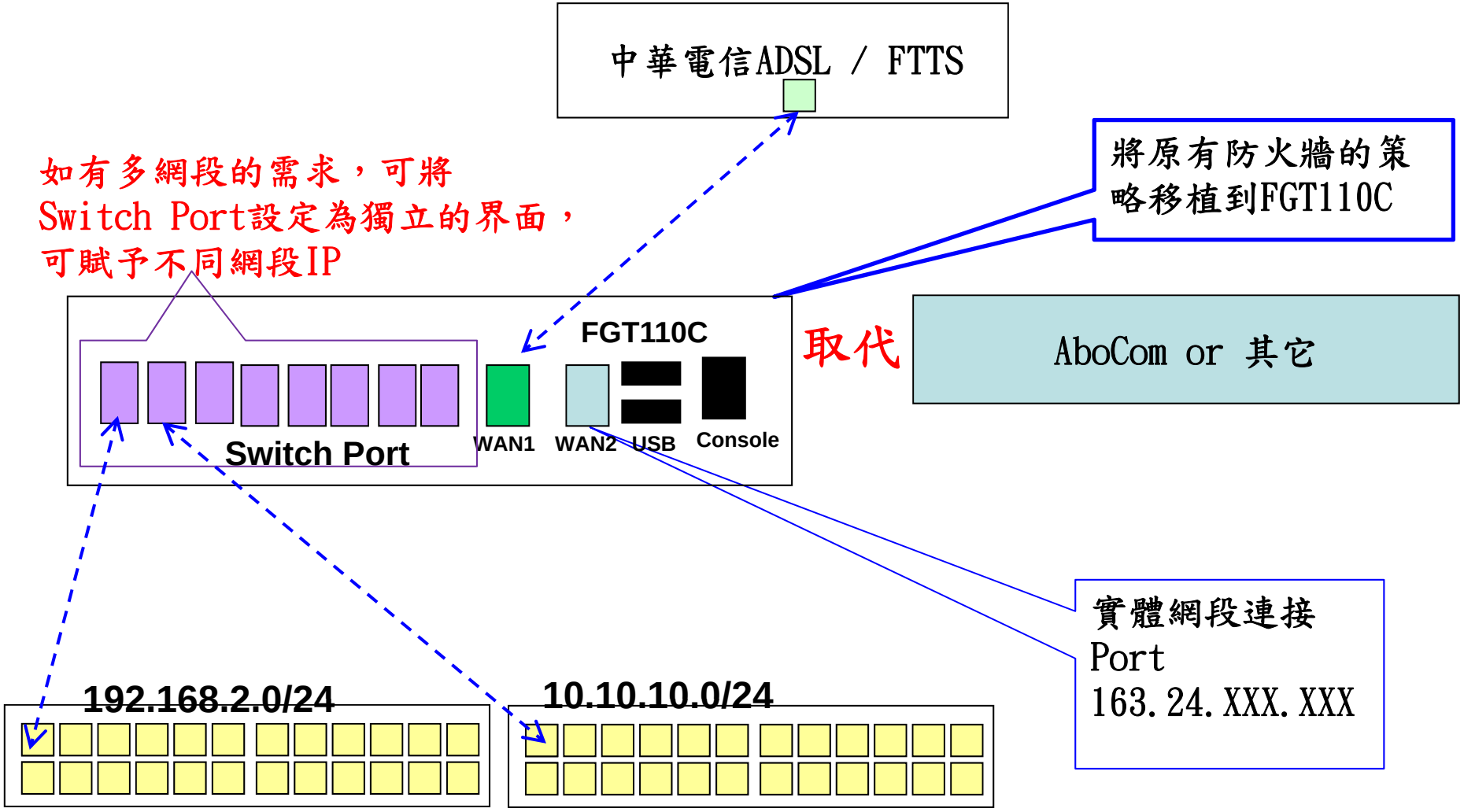
取代現有Router / 防火牆-80C



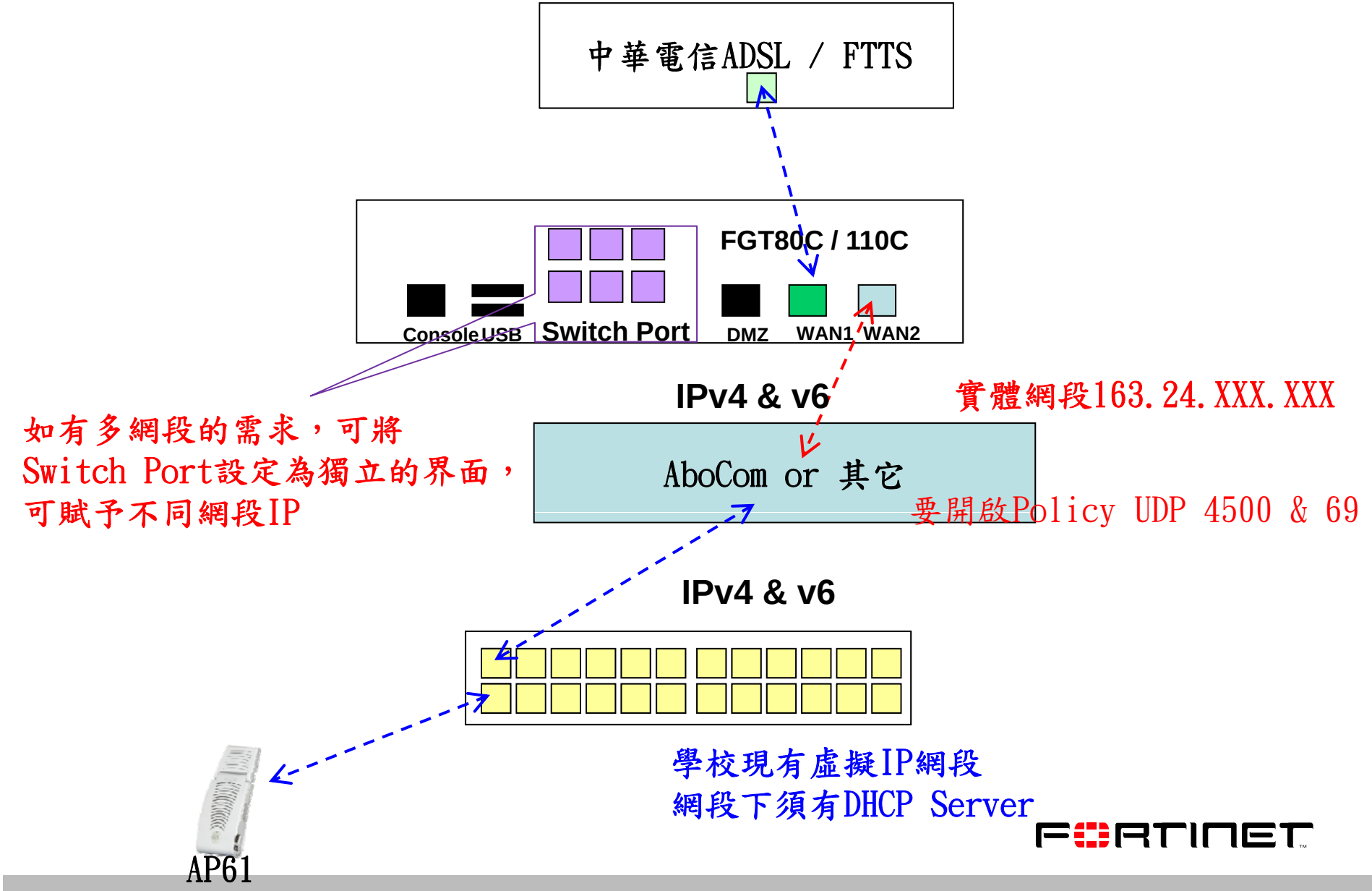
取代現有Router / 防火牆-110C



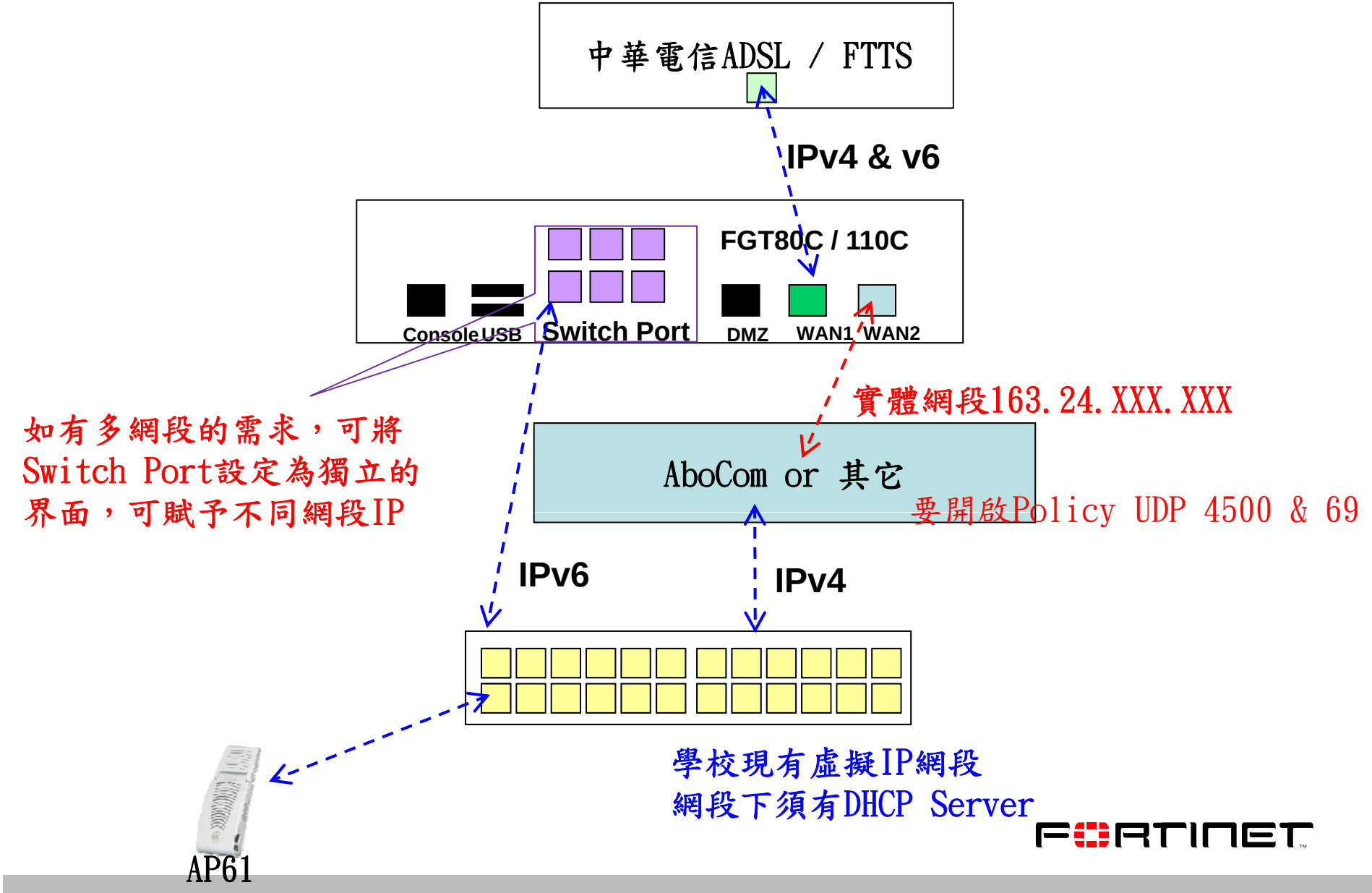
取代現有Router / 防火牆-110C



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

FORTINET

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

FORTINET

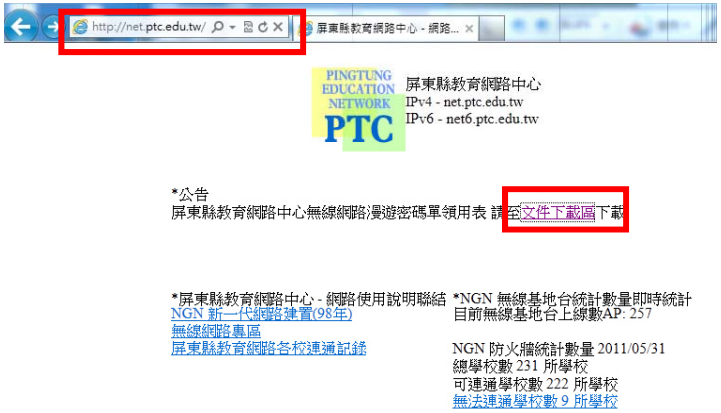
IPv6-網址輸入方式

輸入方式：

1 、網址：http://ipv6.google.com

2 、IPv6 IP：http://[2001:b000:180:3::5]

IPv6-學校IPv6網段查詢



1、http://net.ptc.edu.tw

2、點選『屏東縣IPv6網段分配表』

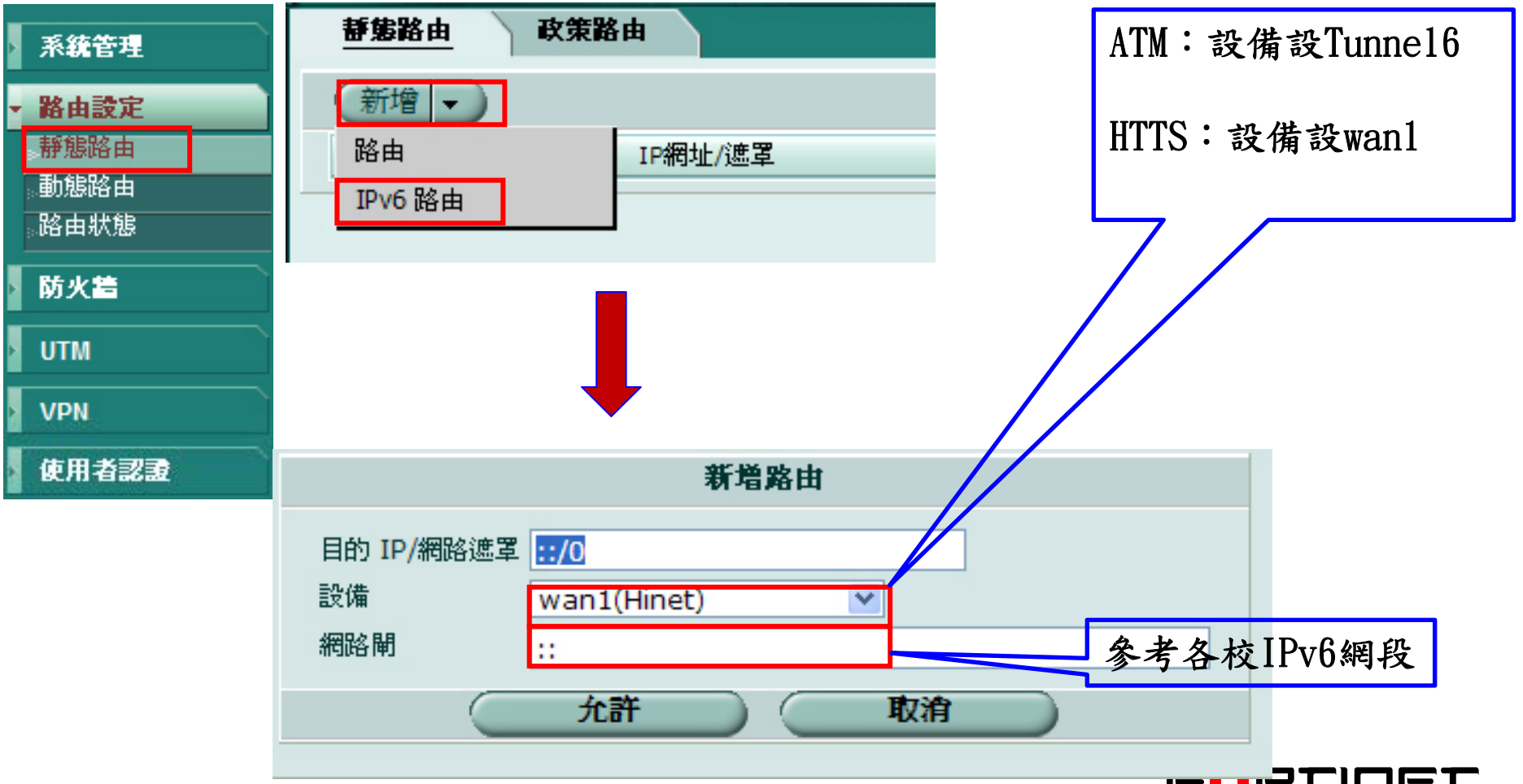
屏東縣(市)各級中小學IPv6網段

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 Tunnal IP	中心 IPv6 Tunnal IP
九如鄉	惠農國小	hnps	FGT80C	2001:288:874a::/48	2001:288:874a:1::1/64	2001:288:874a:2::1/64	2001:288:86ff:ffff:ffff:ffff:ffff:4a01/124	2001:288:86ff:ffff:ffff:ffff:ffff:4a02/124
九如鄉	玉水分班	ysbh	FGT80C	2001:288:874b::/48	2001:288:874b:1::1/64	2001:288:874b:2::1/64	2001:288:86ff:ffff:ffff:ffff:ffff:4b01/124	2001:288:86ff:ffff:ffff:ffff:ffff:4b02/124
九如鄉	三多國小	sdes	FGT80C	2001:288:8748::/48	2001:288:8748:1::1/64	2001:288:8748:2::1/64	2001:288:86ff:ffff:ffff:ffff:ffff:4801/124	2001:288:86ff:ffff:ffff:ffff:ffff:4802/124
三地鄉	達來分班	dlbh	FGT80C	2001:288:87c5::/48	2001:288:87c6:1::1/64	2001:288:87c6:2::1/64	2001:288:86ff:ffff:ffff:ffff:ffff:c601/124	2001:288:86ff:ffff:ffff:ffff:ffff:c602/124
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:ffff:ffff:c701/124	2001:288:86ff:ffff:ffff:ffff:ffff:c702/124
三地鄉	德文分校	dwubh	FGT80C	2001:288:87c6::/48	2001:288:87c5:1::1/64	2001:288:87c5:2::1/64	2001:288:86ff:ffff:ffff:ffff:ffff:c501/124	2001:288:86ff:ffff:ffff:ffff:ffff:c502/124
三地鄉	口社國小	kses	FGT80C	2001:288:87ca::/48	2001:288:87ca:1::1/64	2001:288:87ca:2::1/64	2001:288:86ff:ffff:ffff:ffff:ffff:ca01/124	2001:288:86ff:ffff:ffff:ffff:ffff:ca02/124
三地鄉	青葉國小	cyes	FGT80C	2001:288:87c9::/48	2001:288:87c9:1::1/64	2001:288:87c9:2::1/64	2001:288:86ff:ffff:ffff:ffff:ffff:c901/124	2001:288:86ff:ffff:ffff:ffff:ffff:c902/124
三地鄉	賽嘉國小	sces	FGT80C	2001:288:87cb::/48	2001:288:87cb:1::1/64	2001:288:87cb:2::1/64	2001:288:86ff:ffff:ffff:ffff:ffff:cb01/124	2001:288:86ff:ffff:ffff: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:ffff:ffff:c401/124	2001:288:86ff:ffff:ffff:ffff:ffff:c402/124
內埔鄉	隘寮國小	alps	FGT80C	2001:288:877a::/48	2001:288:877a:1::1/64	2001:288:877a:2::1/64	2001:288:86ff:ffff:ffff:ffff:ffff:7a01/124	2001:288:86ff:ffff:ffff:ffff:ffff:7a02/124
內埔鄉	僑智國小	chjps	FGT80C	2001:288:8775::/48	2001:288:8775:1::1/64	2001:288:8775:2::1/64	2001:288:86ff:ffff:ffff:ffff:ffff:7501/124	2001:288:86ff:ffff:ffff:ffff:ffff:7502/124
內埔鄉	富田國小	ftps	FGT80C	2001:288:877e::/48	2001:288:877e:1::1/64	2001:288:877e:2::1/64	2001:288:86ff:ffff:ffff:ffff:ffff:7e01/124	2001:288:86ff:ffff:ffff: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:ffff:ffff:7801/124	2001:288:86ff:ffff:ffff: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:ffff:ffff:7701/124	2001:288:86ff:ffff:ffff: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:ffff:ffff:7b01/124	2001:288:86ff:ffff:ffff: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:ffff:ffff:7401/124	2001:288:86ff:ffff:ffff:ffff:ffff:7402/124
竹田鄉	竹田國中	tjh	FGT80C	2001:288:870f::/48	2001:288:870f:1::1/64	2001:288:870f:2::1/64	2001:288:86ff:ffff:ffff:ffff:ffff:0f01/124	2001:288:86ff:ffff:ffff: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

IPv6-靜態路由\路由設定\靜態路由\靜態路由



IPv6-策略設定\防火牆\防火牆策略\IPv6政策

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	

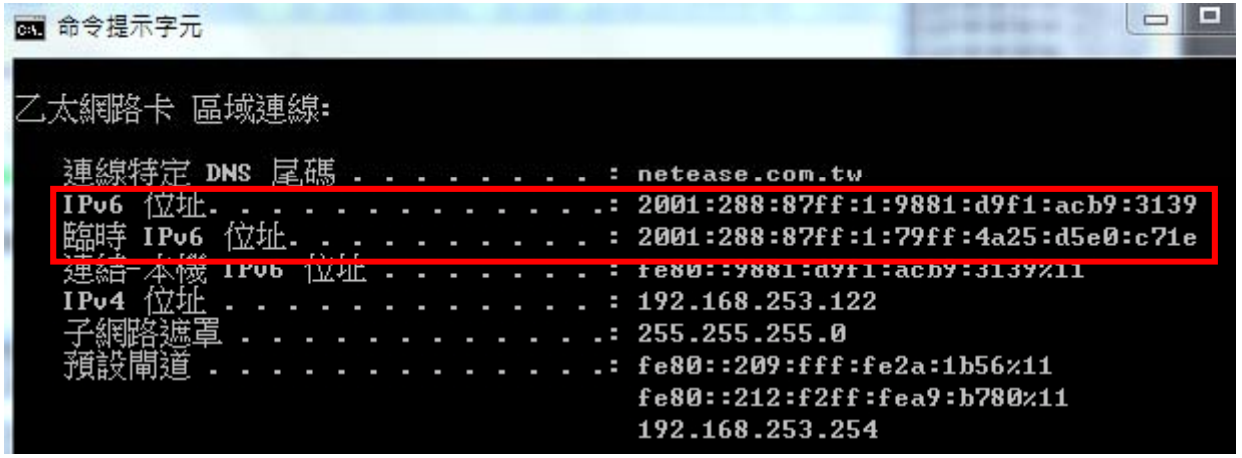
FORTINET

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



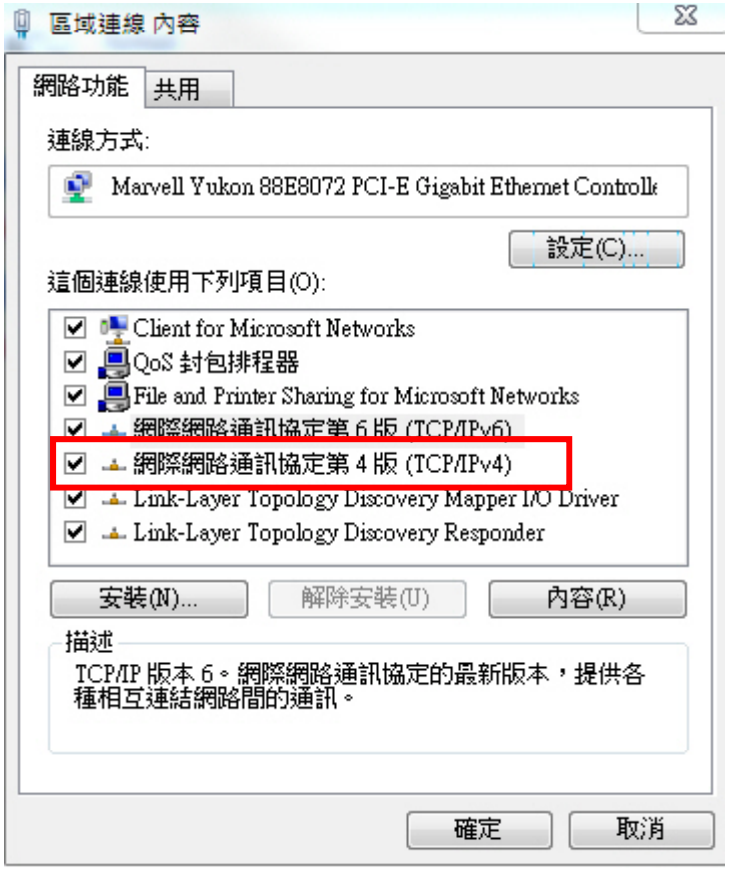
4、測試是否安裝完成→
ping6 ::1

FORTINET

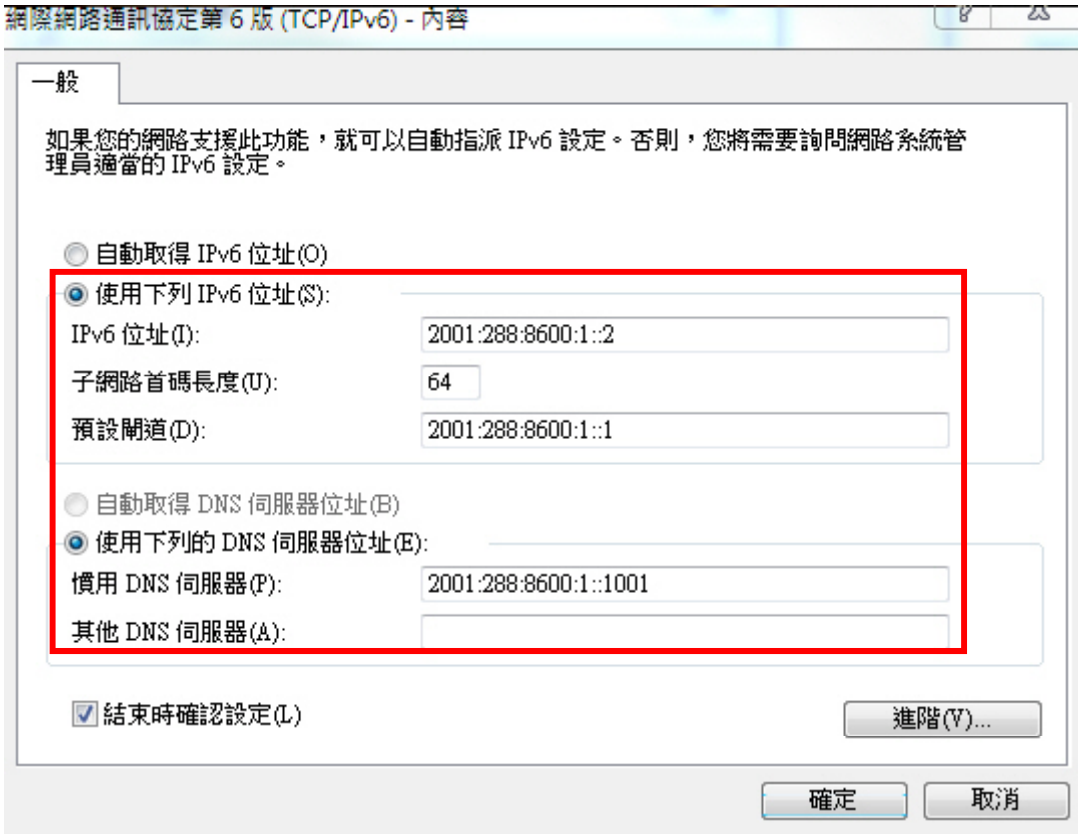
IPv6-Windows IP設定

範例：

IPv6 IP：2001:288:8600:1::2 / 閘道： 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)

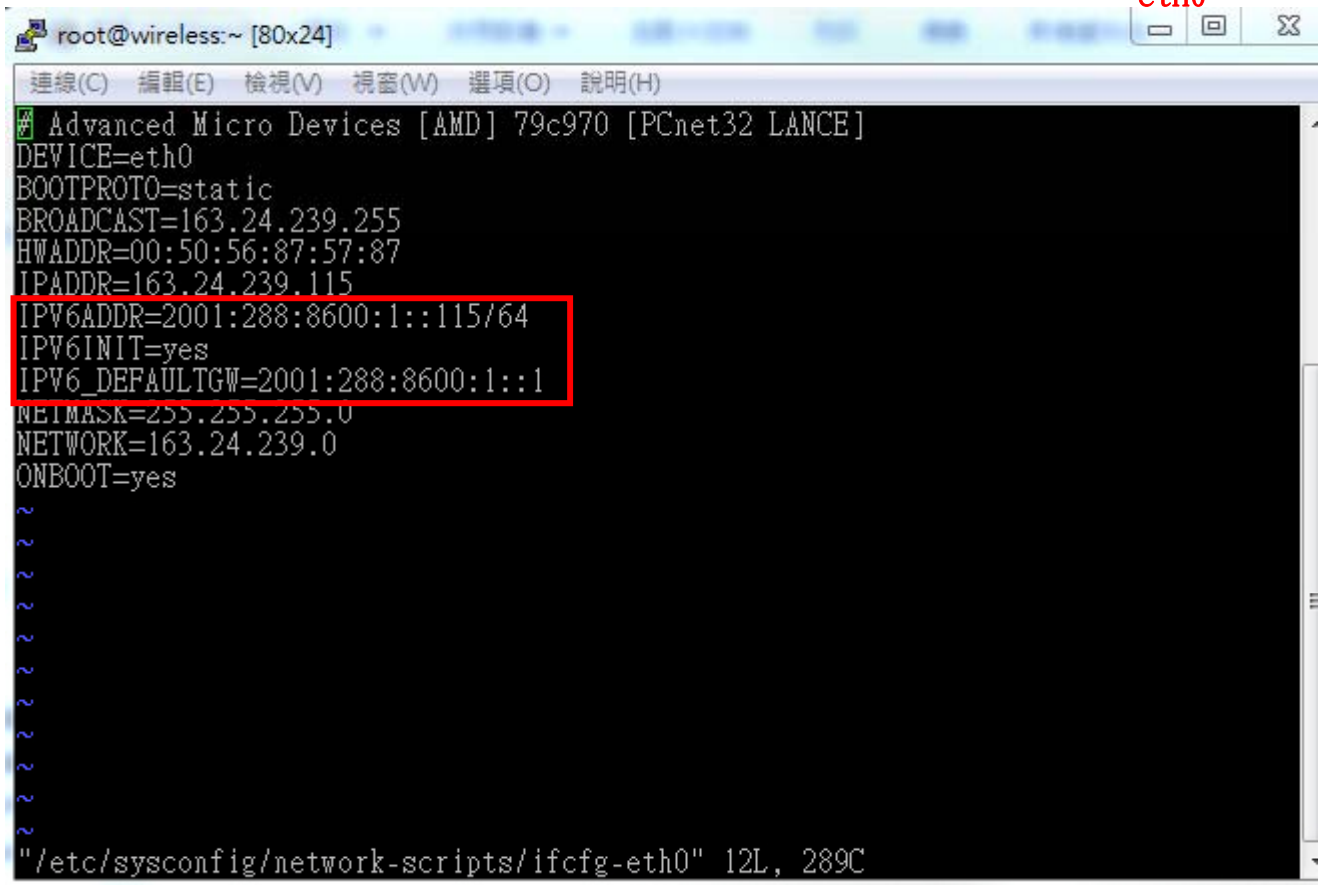


2、輸入IPv6位址、子網路首碼長度、預設閘道、DNS伺服器IP，完成點選確定

IPv6-Linux(CentOS)IP設定

範例：
IPv6 IP：2001:288:8600:1::115/64
閘道：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=閘道IP

3、存檔

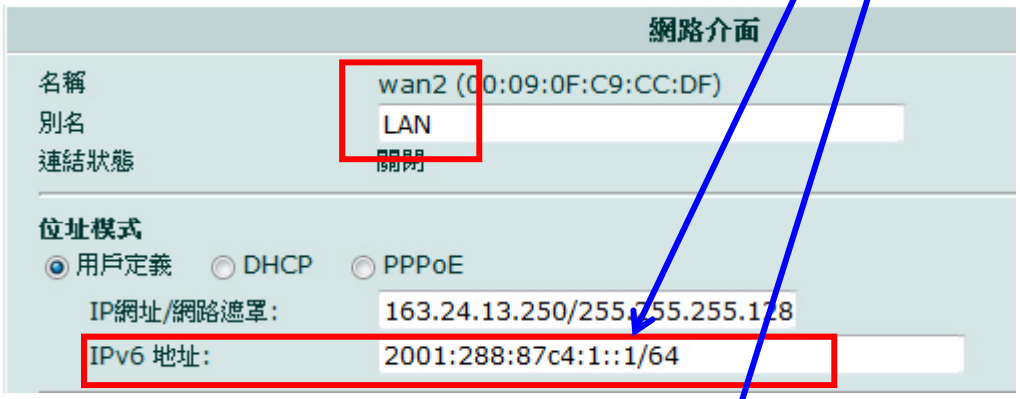
FORTINET

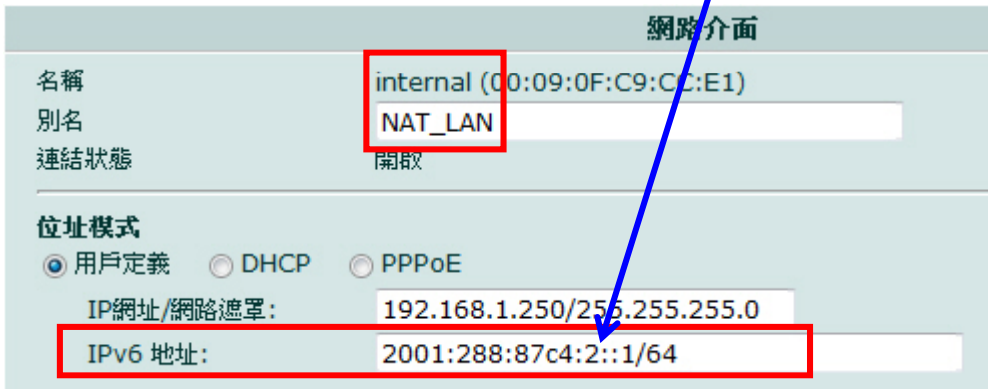
IPv6-Web IP

校內的Web IPv6 IP統一為：

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

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



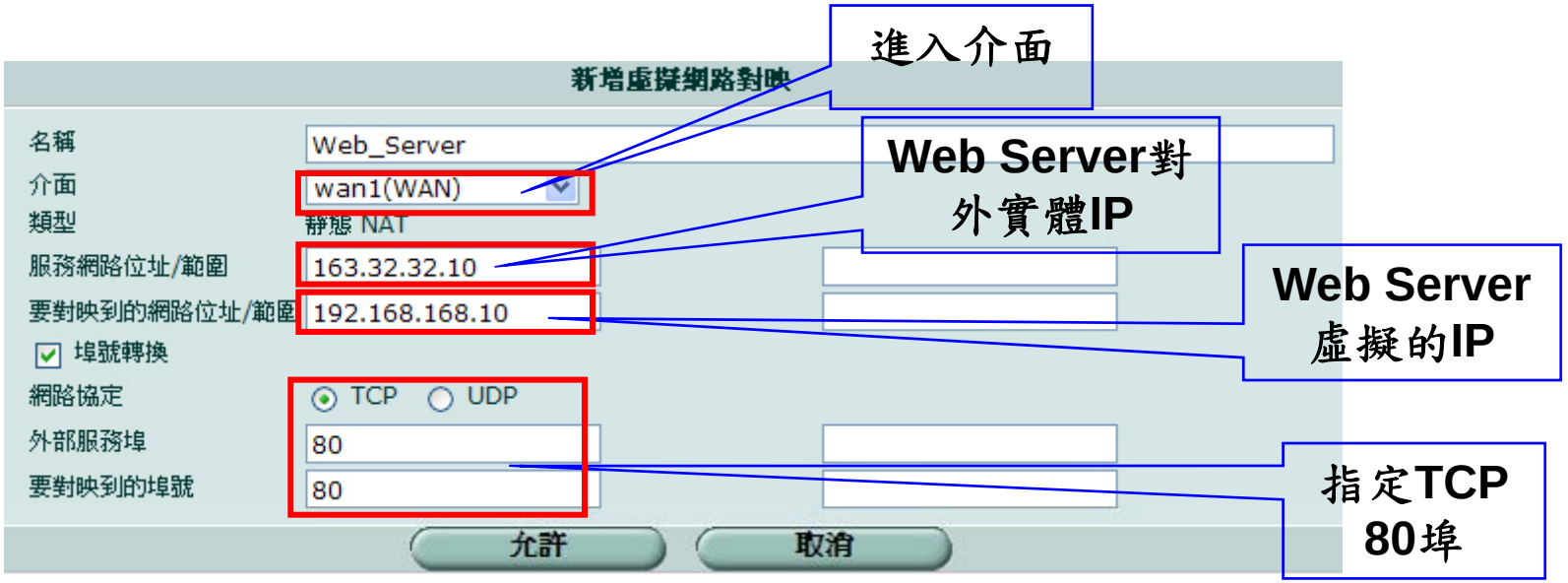


FORTINET

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



2、防火牆必須新增 由Wan1→Internal

網頁過濾 範例說明-開心農場阻隔設定

※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)

輸入欲阻隔的內容

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

FORTINET

網頁過濾

範例說明-開心農場阻隔設定(續)

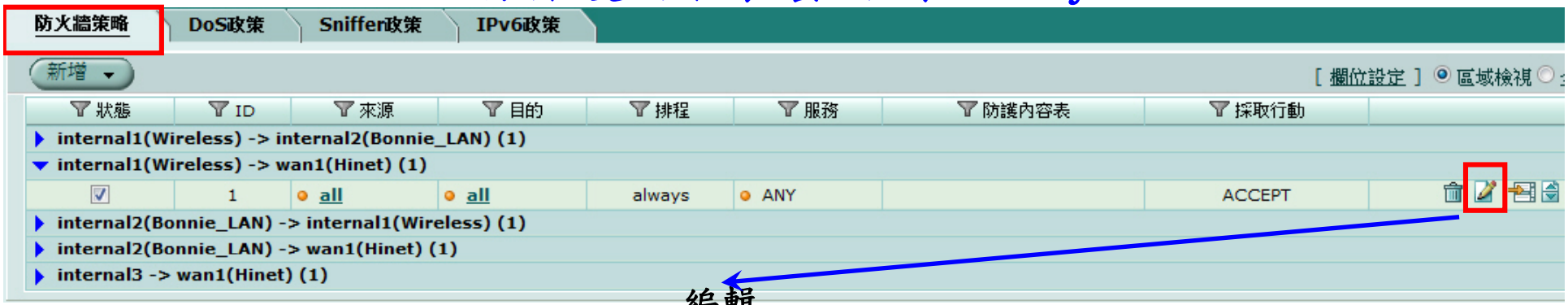
將網址/頁阻隔設定加入內容表

將範例說明的**Web filter**阻隔設定加入到保護內容表

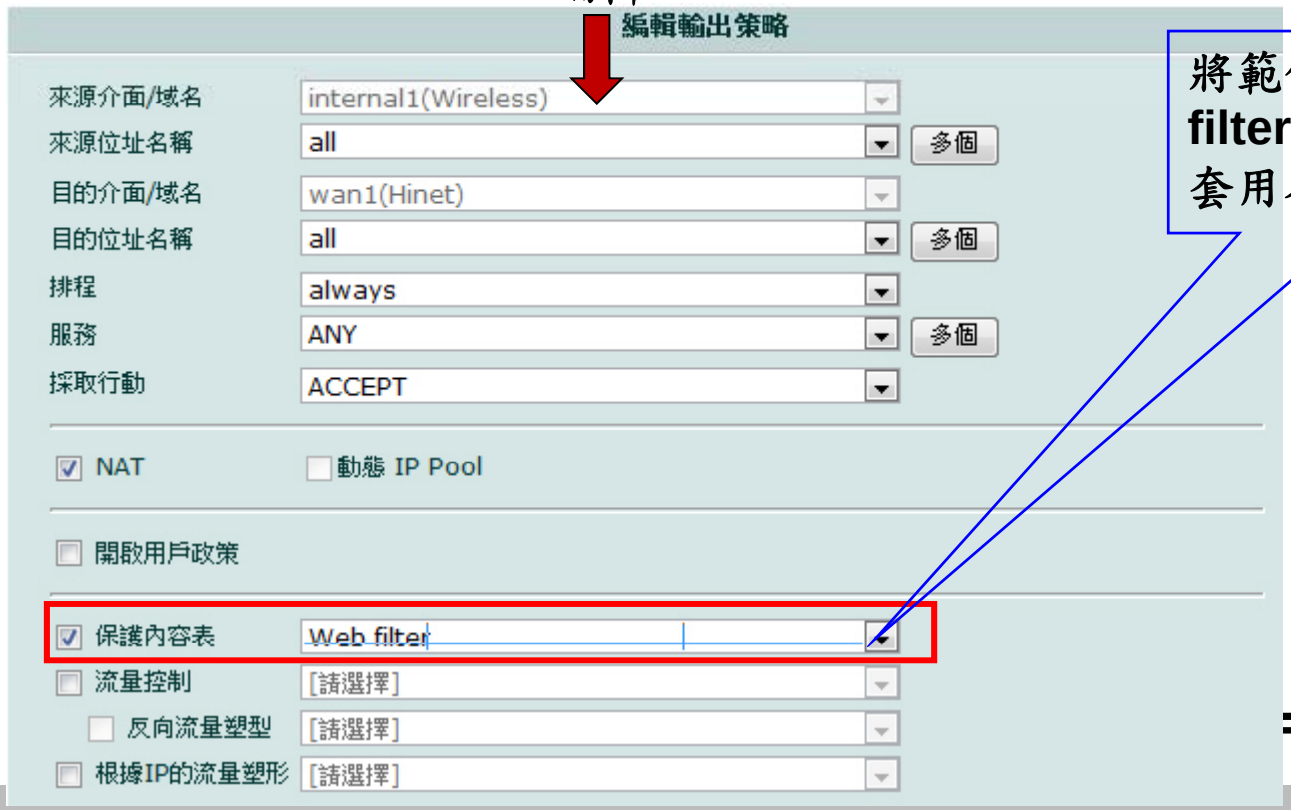
超過門檻值才阻隔

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



將範例說明的Web filter保護內容表套用在該筆Policy

網頁過濾 範例說明-開心農場阻隔設定(續)

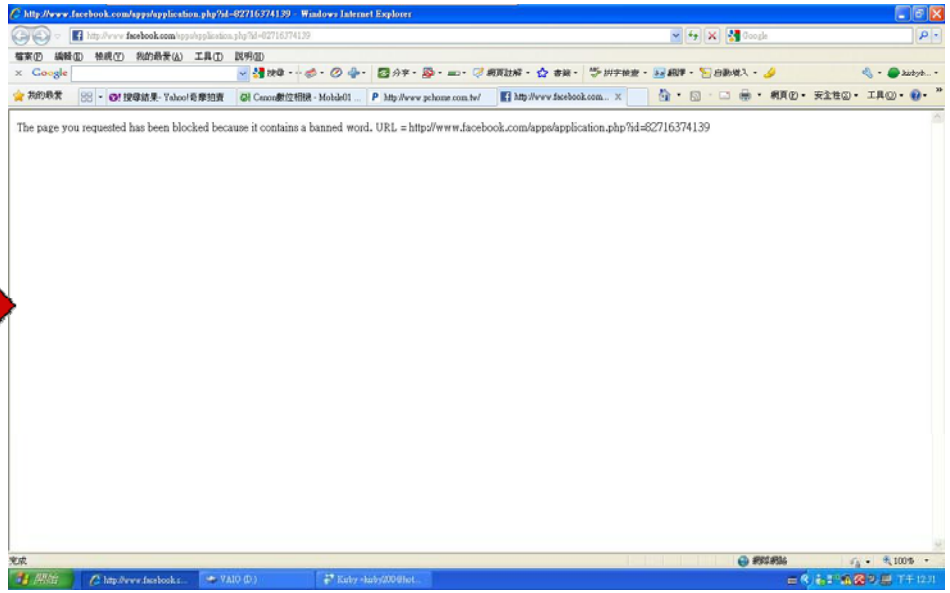
置換封鎖URL用戶端的顯示訊息

網頁過濾 範例說明-開心農場阻隔設定(續)

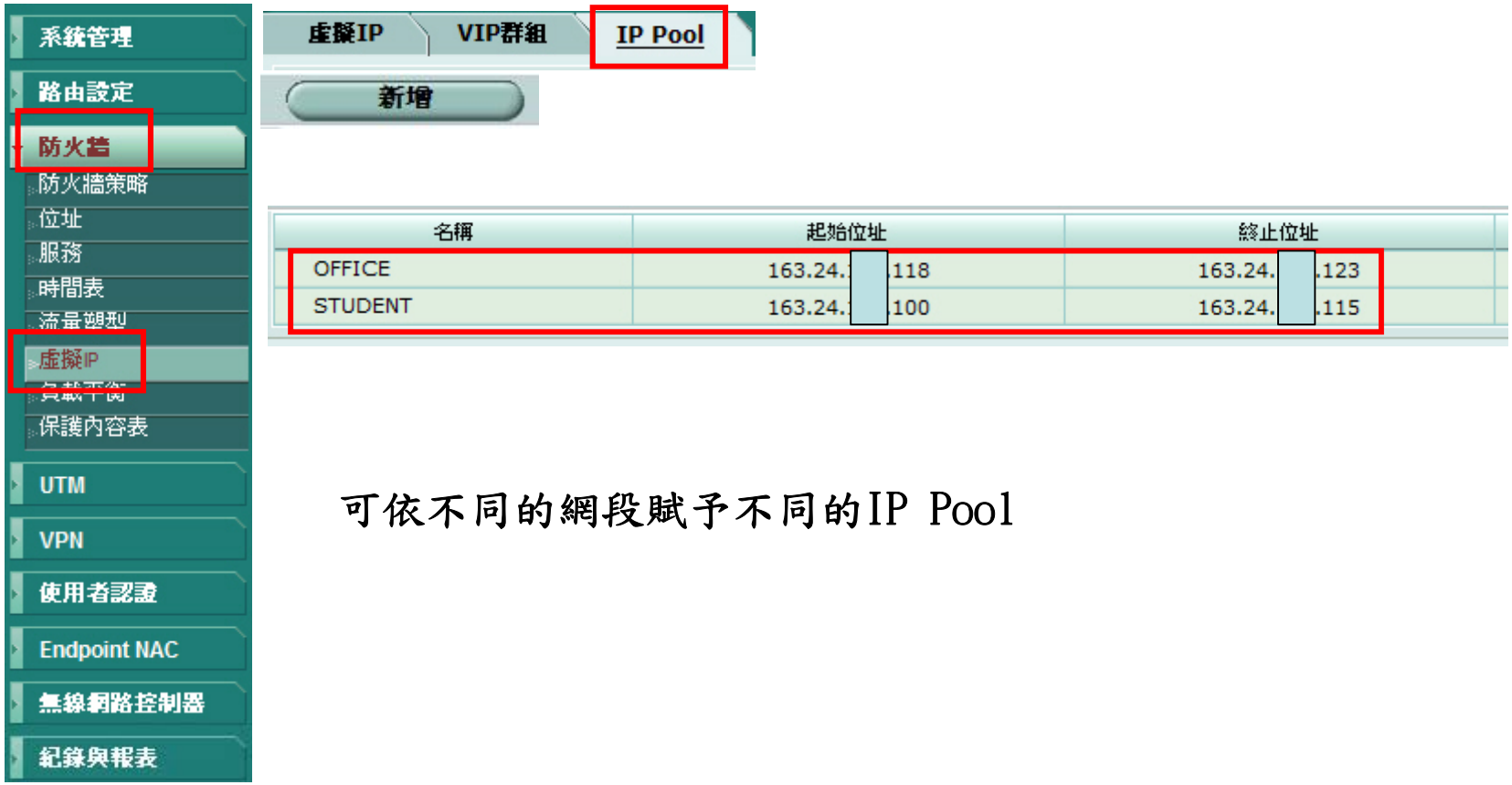
置換封鎖URL用戶端的顯示訊息

PChome網站

有開心農場內容的網站



IP Pool \防火牆\虛擬IP\IP Pool



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	all	all	always	DNS FTP HTTP HTTPS IMAP IMAPS PING PING6 POP3 POP3S RTSP SQUID SSH TELNET TFTP IKE 主計 win_auth		ACCEPT
☑	9	all	all	always	ANY		DENY

3、Deny(拒絕存取)的策略，建議放在最上層。

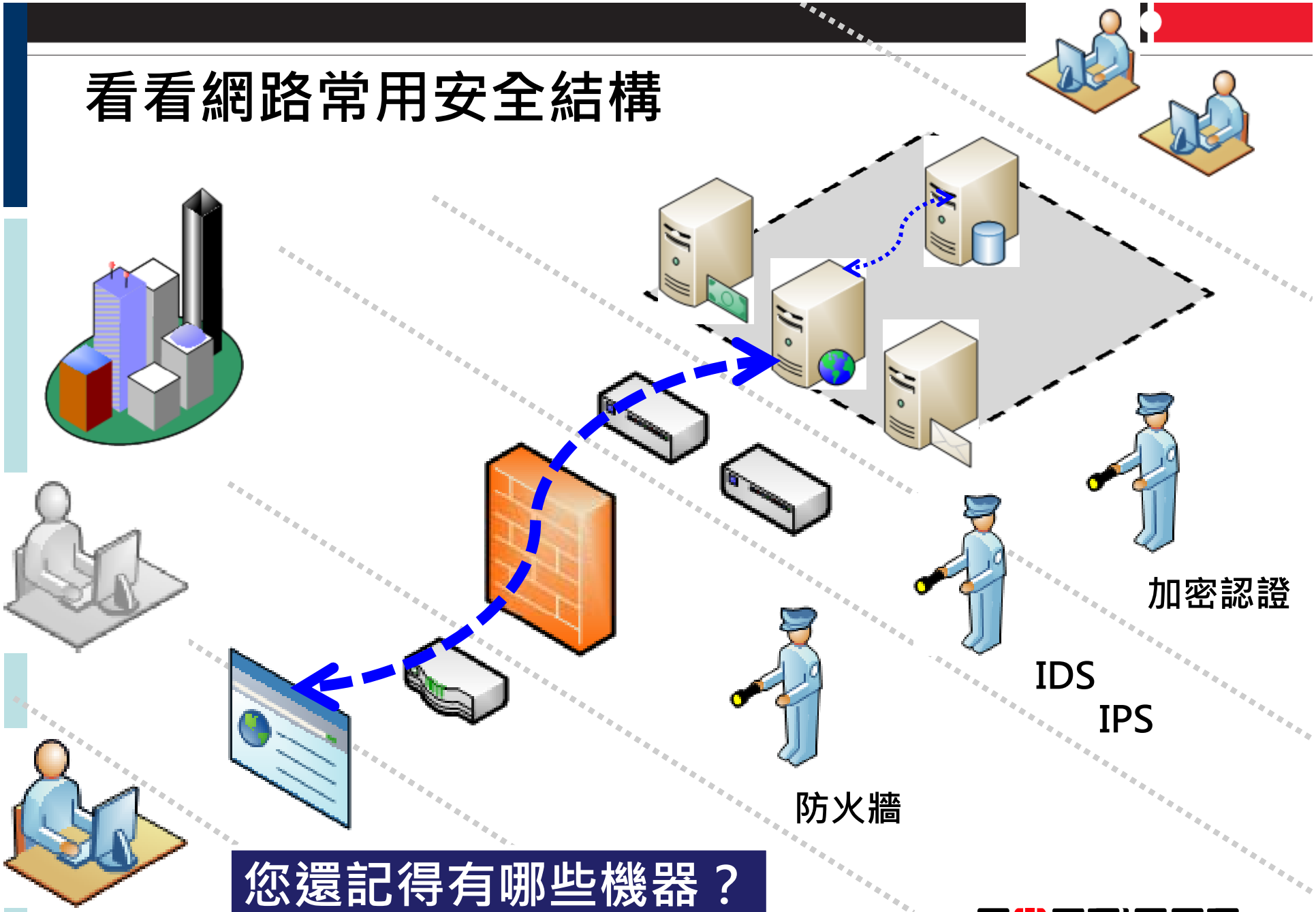
wan1(Wan) -> wan2(LAN) (7)							
☑	15	bad china bad gay1	all	always	ANY		DENY
☐	13	all	dns	always	ANY		DENY
☑	10	block_mail	all	always	ANY		DENY
☑	8	all	all	always	DNS FTP HTTP HTTPS IMAP IMAPS NNTP PING SMTP SQUID easyboard		ACCEPT
☑	7	jack_1	all	always	SSH LDAP RDP		ACCEPT
☑	11	ptta	all	always	rsync		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

FORTINET

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?

FORTINET

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 / limmc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

FORTINET

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

紀錄啟用 \防火牆\防火牆策略\防火牆策略

編輯

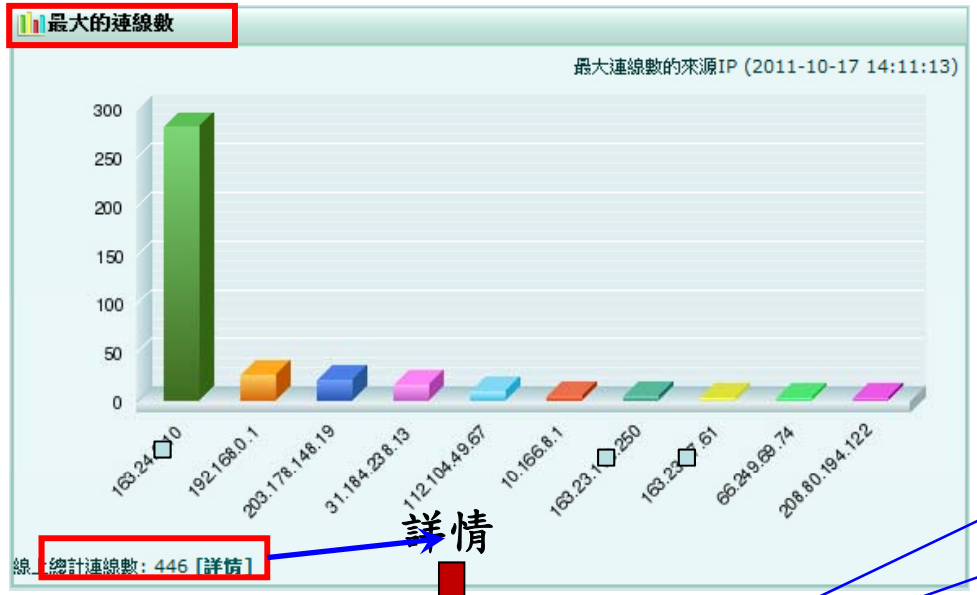
紀錄啟用\防火牆\保護內容表\保護內容表

檢視防火牆的紀錄啟用(續)

#	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

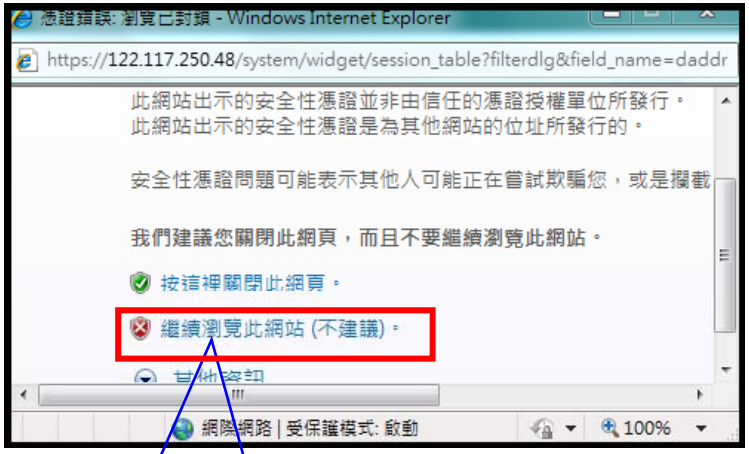
即時紀錄查詢\系統管理\狀態\最大的連線數



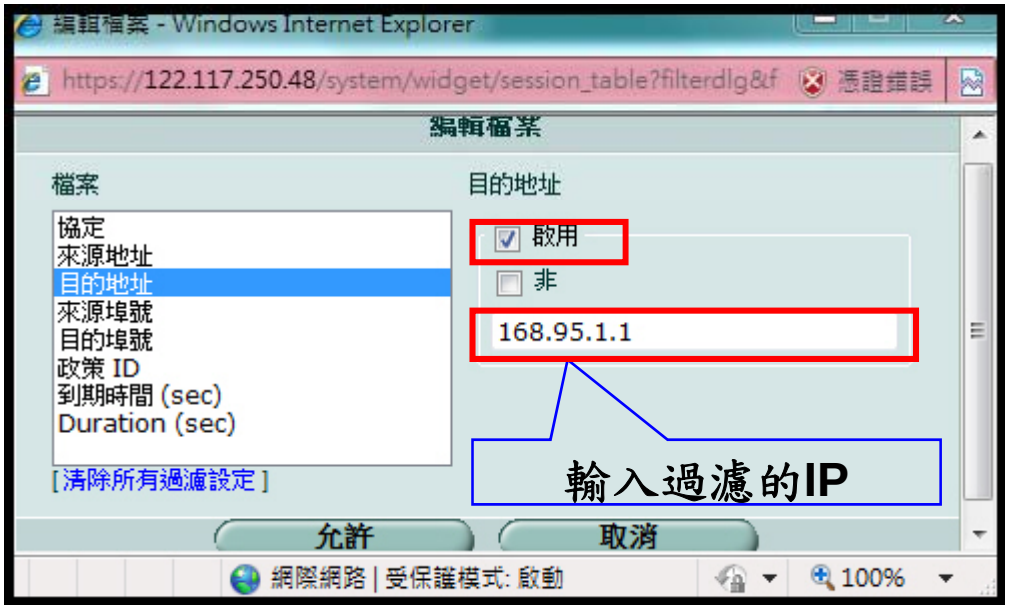
詳情

#	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	
4	udp	192.168.10.5	3453	119.145.130.20	17788	1	
5	udp	192.168.10.5	3453	61.155.106.176	17788	1	
6	udp	192.168.10.5	3453	61.155.106.169	17788	1	
7	udp	192.168.10.5	3453	61.155.106.168	17788	1	
8	udp	192.168.10.5	3453	61.155.106.166	17788	1	
9	udp	192.168.10.5	3453	61.155.106.163	17788	1	
10	udp	192.168.10.5	3453	218.85.135.94	8800	1	
11	udp	192.168.10.5	3453	121.9.201.102	17788	1	

欲查詢目的地為**168.95.1.1**的流量紀錄,點選目的地址



跳出憑證錯誤畫面，點選繼續瀏覽此網站選項



#	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)

FORTINET

查詢該網站是因為
哪個關鍵字阻擋

FortiAnalyzer | 記憶體

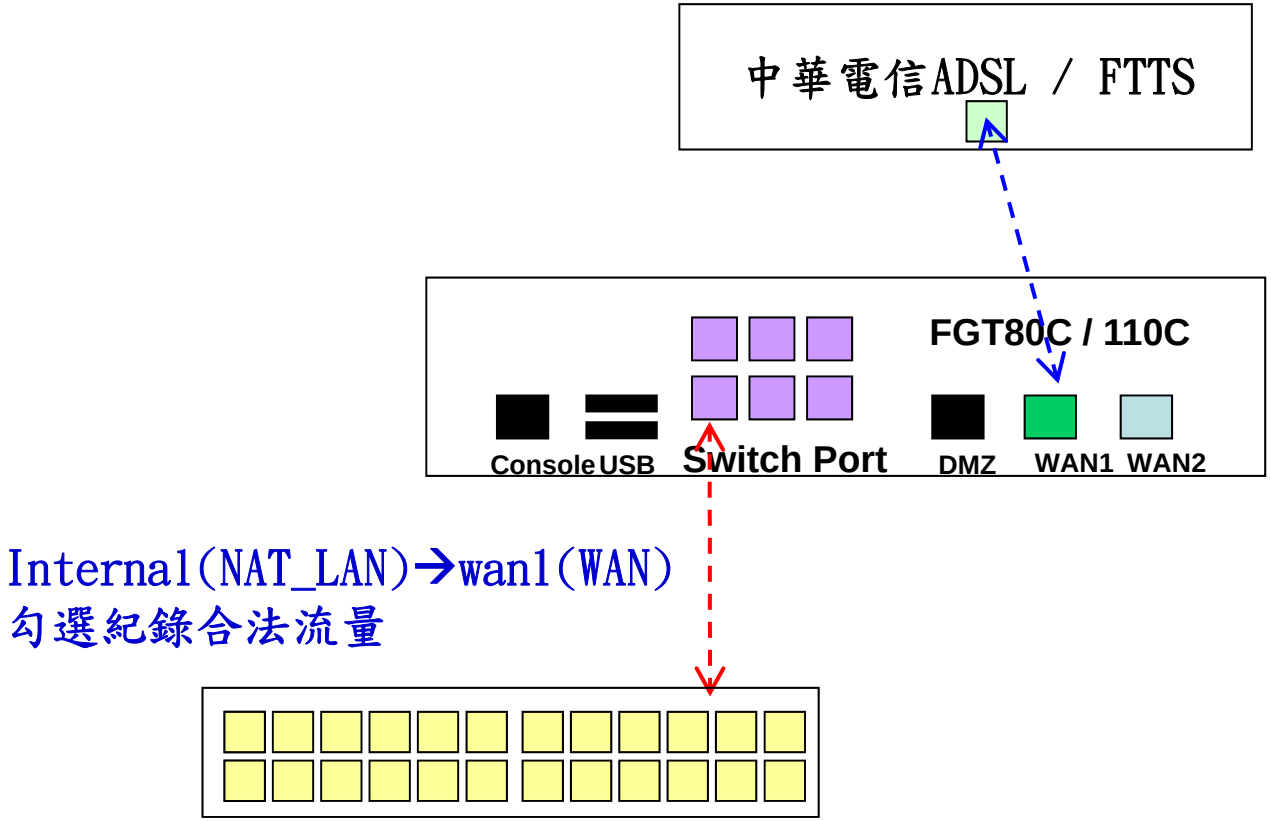
日誌型態 網頁過濾

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).	龍之刃
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).	龍之刃
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).	龍之刃
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).	女生遊戲鍋
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	

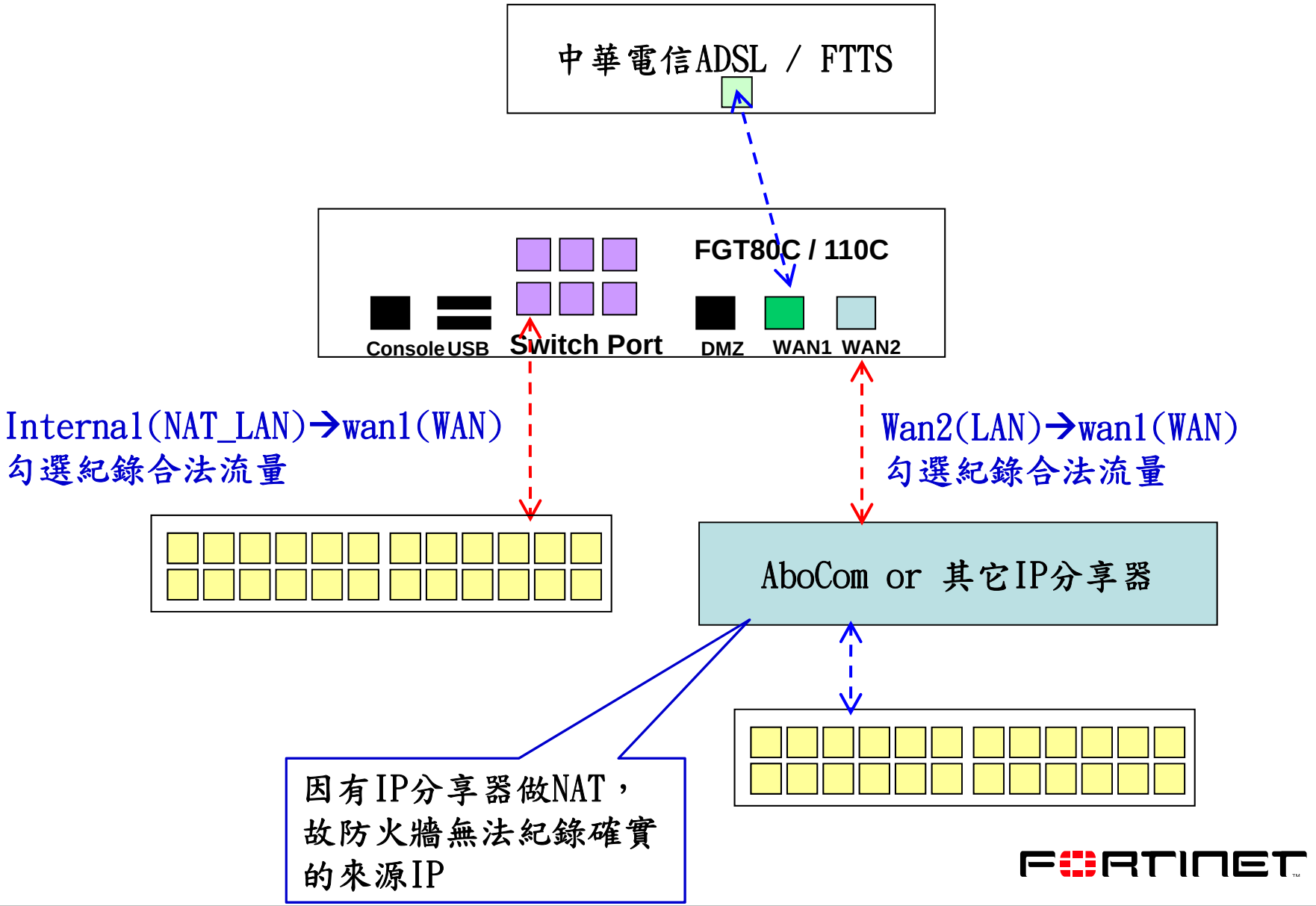
FORTINET

檢視防火牆的紀錄啟用(續)



Internal(NAT_LAN)→wan1(WAN)
勾選紀錄合法流量

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

Thank You!

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