新北教網
無線網路設定實作暨基礎無線行動箱設計研習會

中孚科技
Sanfran Technologies Inc.

李煒
106/06/27

課程大綱

1.校園設備簡介

2.防火牆使用介紹

3.無線AP運作介紹

4.故障排除

5.高可用性介紹

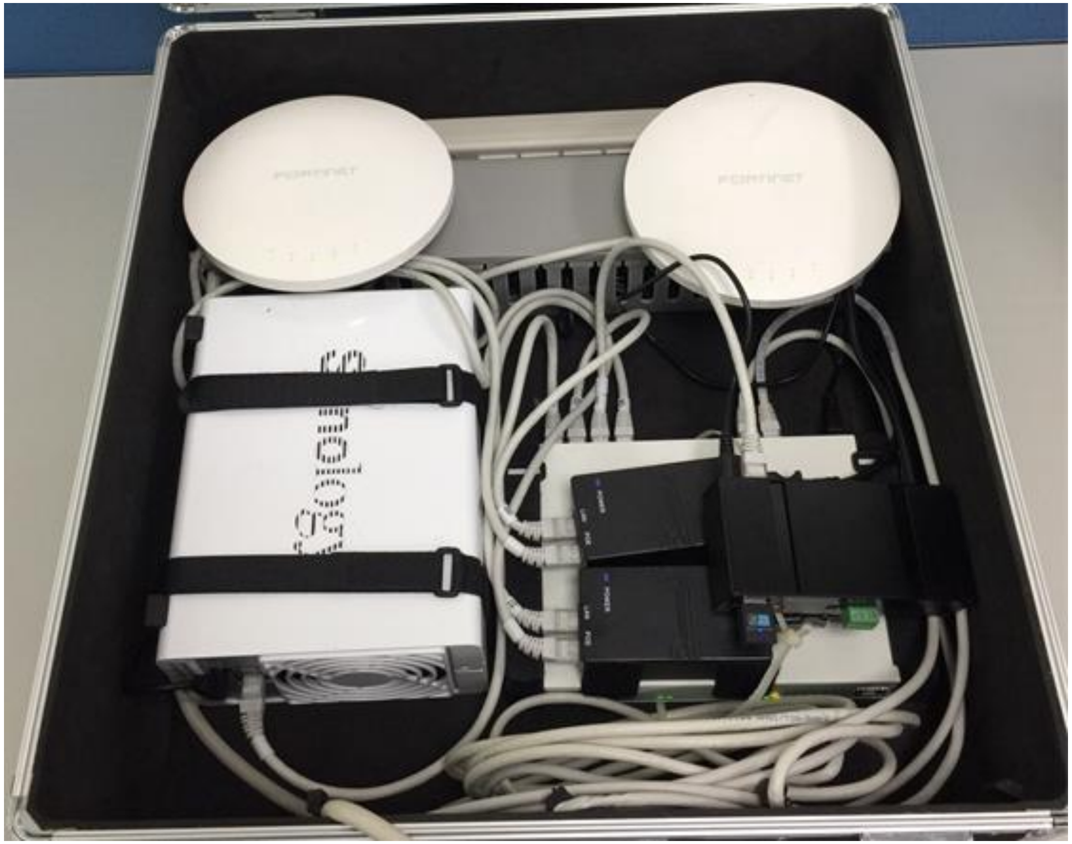
6.EZ-WP3000

7.Q&A

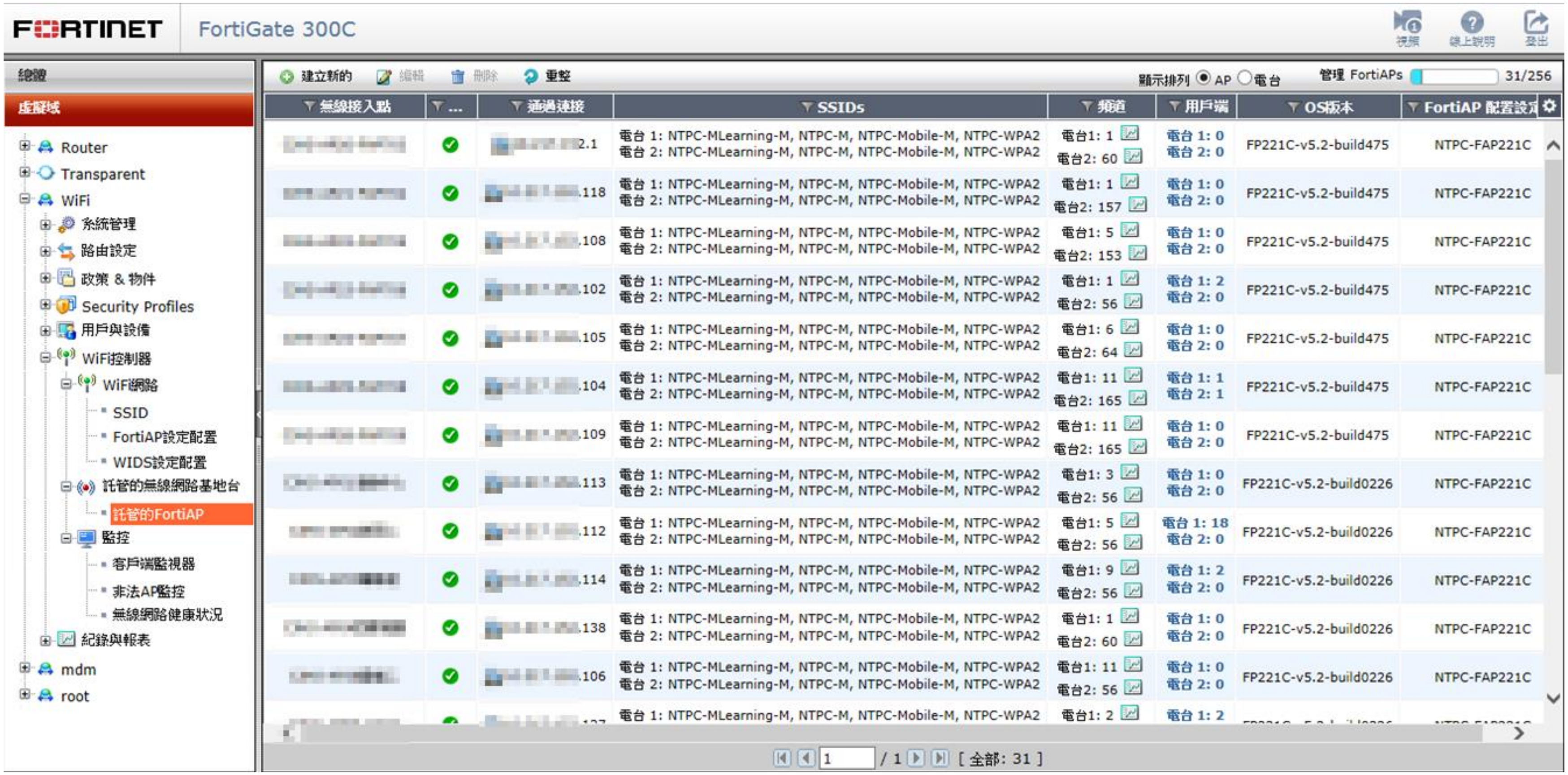
校園設備簡介

行動箱設備介紹

- Fortigate60D
- FortiAP221C
- AP adapter
- Synology NAS
- 投影裝置



教網中心端註冊畫面

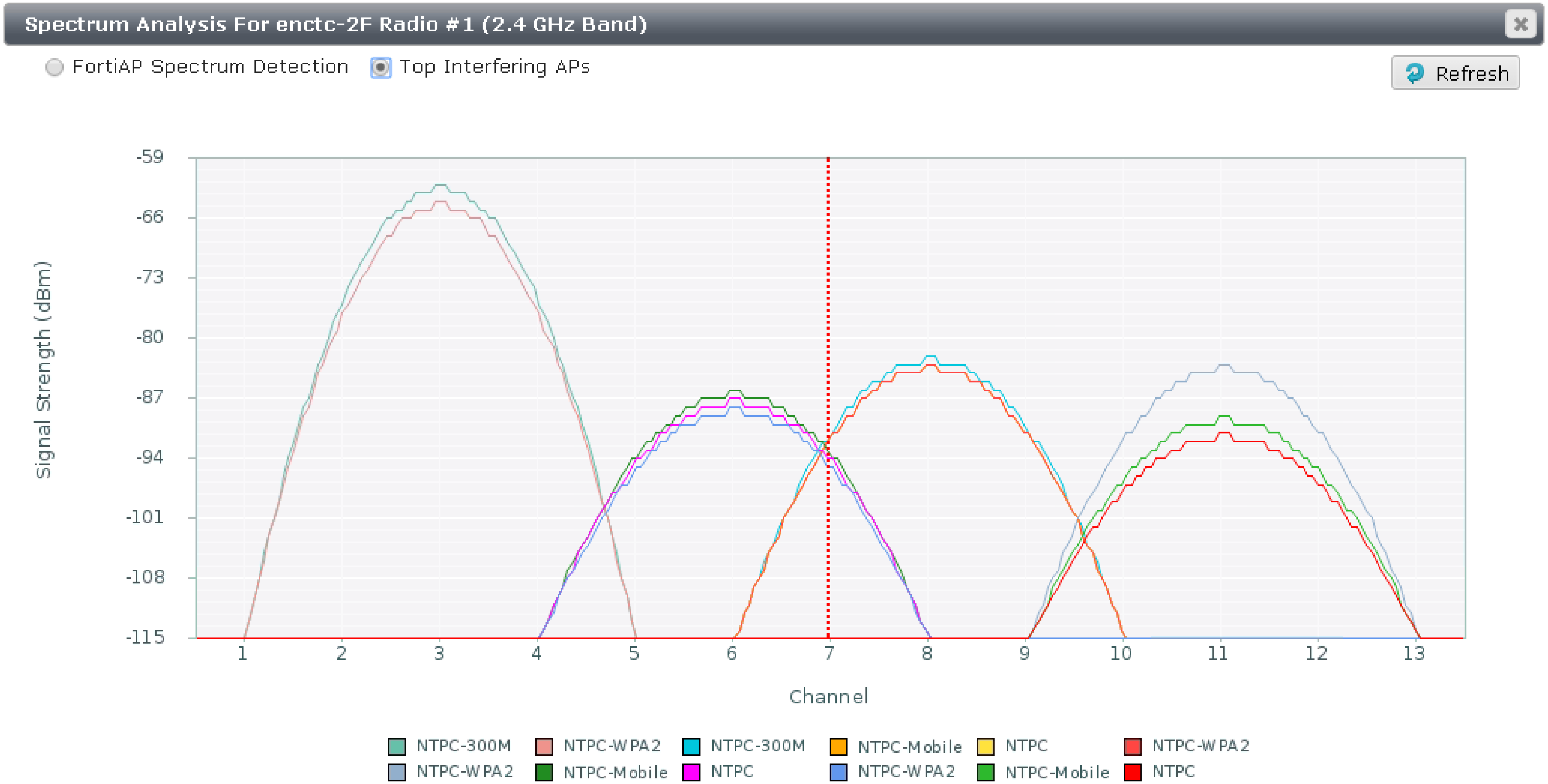


顯示排列 ● AP ○ 電台   管理 FortiAPs 31/256

無線接入點	...	通過連接	SSIDs	頻道	用戶端	OS版本	FortiAP 配置設定
[redacted]	✓	[redacted]2.1	電台 1: NTPC-MLearning-M, NTPC-M, NTPC-Mobile-M, NTPC-WPA2 電台 2: NTPC-MLearning-M, NTPC-M, NTPC-Mobile-M, NTPC-WPA2	電台1: 1 電台2: 60	電台 1: 0 電台 2: 0	FP221C-v5.2-build475	NTPC-FAP221C
[redacted]	✓	[redacted].118	電台 1: NTPC-MLearning-M, NTPC-M, NTPC-Mobile-M, NTPC-WPA2 電台 2: NTPC-MLearning-M, NTPC-M, NTPC-Mobile-M, NTPC-WPA2	電台1: 1 電台2: 157	電台 1: 0 電台 2: 0	FP221C-v5.2-build475	NTPC-FAP221C
[redacted]	✓	[redacted].108	電台 1: NTPC-MLearning-M, NTPC-M, NTPC-Mobile-M, NTPC-WPA2 電台 2: NTPC-MLearning-M, NTPC-M, NTPC-Mobile-M, NTPC-WPA2	電台1: 5 電台2: 153	電台 1: 0 電台 2: 0	FP221C-v5.2-build475	NTPC-FAP221C
[redacted]	✓	[redacted].102	電台 1: NTPC-MLearning-M, NTPC-M, NTPC-Mobile-M, NTPC-WPA2 電台 2: NTPC-MLearning-M, NTPC-M, NTPC-Mobile-M, NTPC-WPA2	電台1: 1 電台2: 56	電台 1: 2 電台 2: 0	FP221C-v5.2-build475	NTPC-FAP221C
[redacted]	✓	[redacted].105	電台 1: NTPC-MLearning-M, NTPC-M, NTPC-Mobile-M, NTPC-WPA2 電台 2: NTPC-MLearning-M, NTPC-M, NTPC-Mobile-M, NTPC-WPA2	電台1: 6 電台2: 64	電台 1: 0 電台 2: 0	FP221C-v5.2-build475	NTPC-FAP221C
[redacted]	✓	[redacted].104	電台 1: NTPC-MLearning-M, NTPC-M, NTPC-Mobile-M, NTPC-WPA2 電台 2: NTPC-MLearning-M, NTPC-M, NTPC-Mobile-M, NTPC-WPA2	電台1: 11 電台2: 165	電台 1: 1 電台 2: 1	FP221C-v5.2-build475	NTPC-FAP221C
[redacted]	✓	[redacted].109	電台 1: NTPC-MLearning-M, NTPC-M, NTPC-Mobile-M, NTPC-WPA2 電台 2: NTPC-MLearning-M, NTPC-M, NTPC-Mobile-M, NTPC-WPA2	電台1: 11 電台2: 165	電台 1: 0 電台 2: 0	FP221C-v5.2-build475	NTPC-FAP221C
[redacted]	✓	[redacted].113	電台 1: NTPC-MLearning-M, NTPC-M, NTPC-Mobile-M, NTPC-WPA2 電台 2: NTPC-MLearning-M, NTPC-M, NTPC-Mobile-M, NTPC-WPA2	電台1: 3 電台2: 56	電台 1: 0 電台 2: 0	FP221C-v5.2-build0226	NTPC-FAP221C
[redacted]	✓	[redacted].112	電台 1: NTPC-MLearning-M, NTPC-M, NTPC-Mobile-M, NTPC-WPA2 電台 2: NTPC-MLearning-M, NTPC-M, NTPC-Mobile-M, NTPC-WPA2	電台1: 5 電台2: 56	電台 1: 18 電台 2: 0	FP221C-v5.2-build0226	NTPC-FAP221C
[redacted]	✓	[redacted].114	電台 1: NTPC-MLearning-M, NTPC-M, NTPC-Mobile-M, NTPC-WPA2 電台 2: NTPC-MLearning-M, NTPC-M, NTPC-Mobile-M, NTPC-WPA2	電台1: 9 電台2: 56	電台 1: 2 電台 2: 0	FP221C-v5.2-build0226	NTPC-FAP221C
[redacted]	✓	[redacted].138	電台 1: NTPC-MLearning-M, NTPC-M, NTPC-Mobile-M, NTPC-WPA2 電台 2: NTPC-MLearning-M, NTPC-M, NTPC-Mobile-M, NTPC-WPA2	電台1: 1 電台2: 60	電台 1: 0 電台 2: 0	FP221C-v5.2-build0226	NTPC-FAP221C
[redacted]	✓	[redacted].106	電台 1: NTPC-MLearning-M, NTPC-M, NTPC-Mobile-M, NTPC-WPA2 電台 2: NTPC-MLearning-M, NTPC-M, NTPC-Mobile-M, NTPC-WPA2	電台1: 11 電台2: 56	電台 1: 0 電台 2: 0	FP221C-v5.2-build0226	NTPC-FAP221C
[redacted]	✓	[redacted]	電台 1: NTPC-MLearning-M, NTPC-M, NTPC-Mobile-M, NTPC-WPA2	電台1: 2	電台 1: 2		

1 / 1 [全部: 31]

校園展示畫面

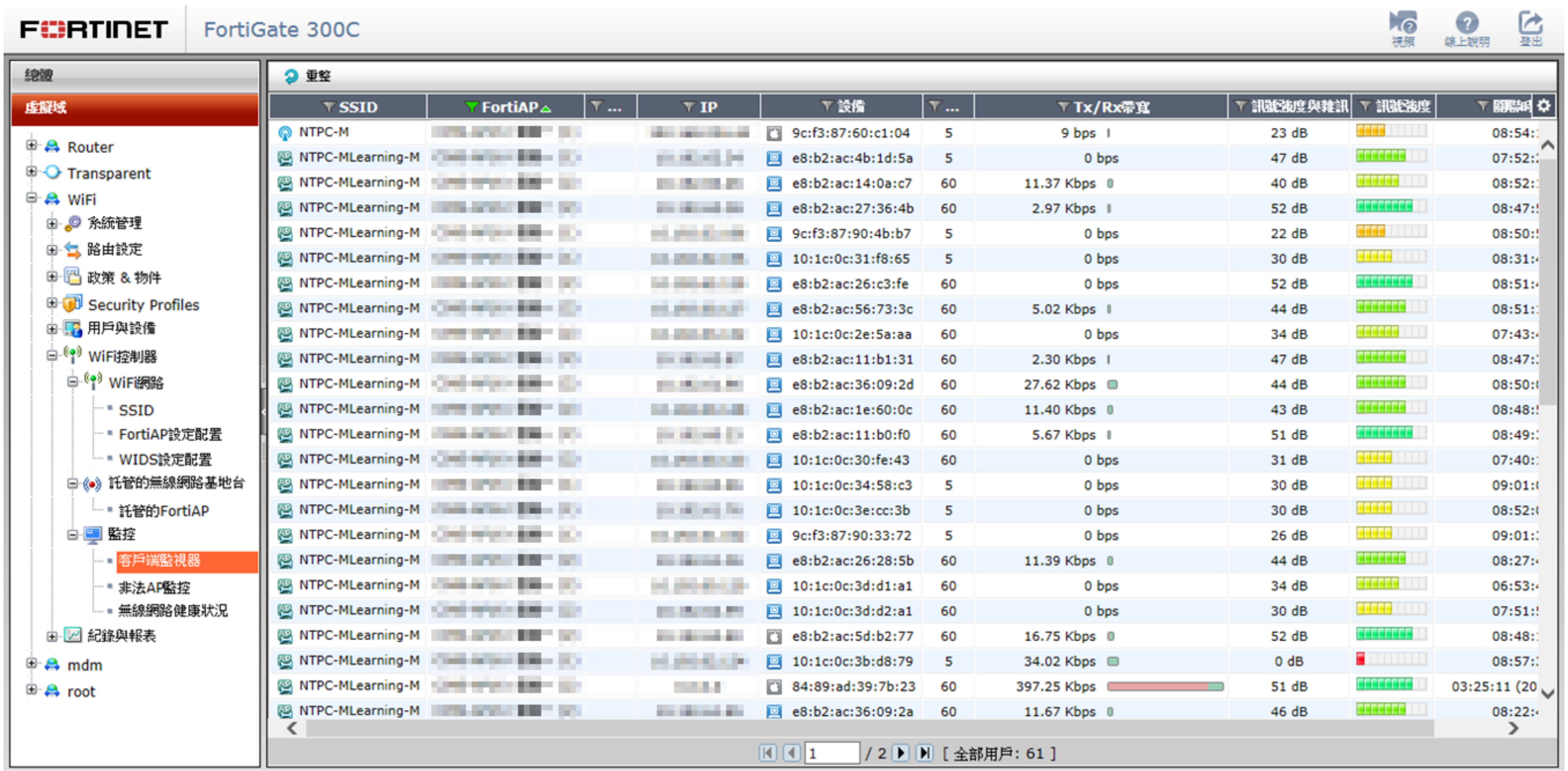


Spectrum Analysis For enctc-2F Radio #1 (2.4 GHz Band)

○ FortiAP Spectrum Detection ● Top Interfering APs

單一AP註冊數量

新北市政府 教育局
Education Department, New Taipei City Government



FORTINET FortiGate 300C

總覽

虛擬域

- Router
- Transparent
- WiFi
  - 系統管理
  - 路由設定
  - 政策 & 物件
  - Security Profiles
  - 用戶與設備
  - WiFi控制器
    - WiFi網路
      - SSID
      - FortiAP設定配置
      - WIDS設定配置
    - 託管的無線網路基地台
      - 託管的FortiAP
    - 監控
      - 客戶端監視器
      - 非法AP監控
      - 無線網路健康狀況
  - 紀錄與報表
- mdm
- root

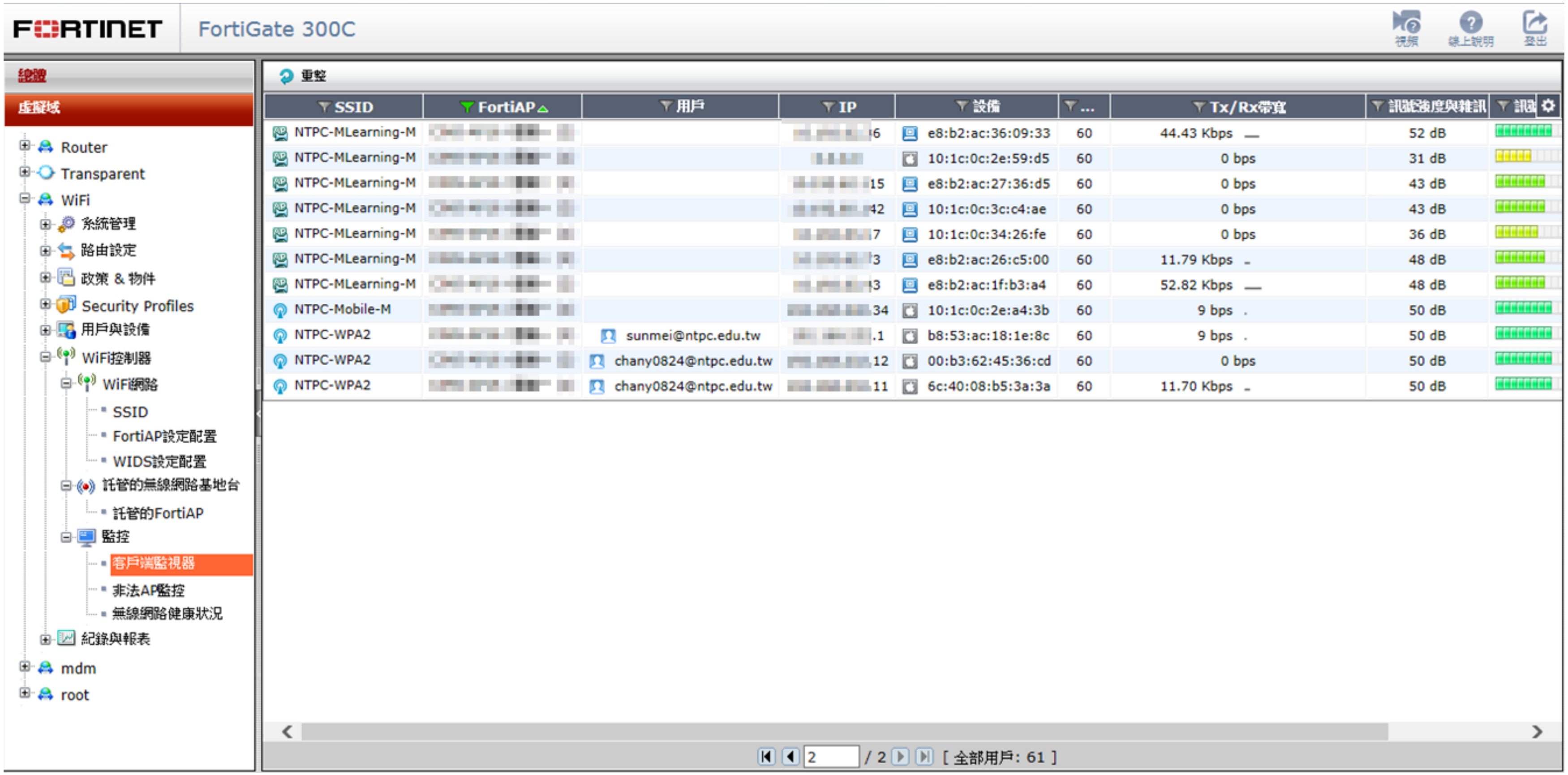
重整

SSID	FortiAP	...	IP	設備	...	Tx/Rx帶寬	訊號強度與雜訊	訊號強度	關聯時
NTPC-M	[redacted]		[redacted]	9c:f3:87:60:c1:04	5	9 bps	23 dB	🟧	08:54:
NTPC-MLearning-M	[redacted]		[redacted]	e8:b2:ac:4b:1d:5a	5	0 bps	47 dB	🟩	07:52:
NTPC-MLearning-M	[redacted]		[redacted]	e8:b2:ac:14:0a:c7	60	11.37 Kbps	40 dB	🟩	08:52:
NTPC-MLearning-M	[redacted]		[redacted]	e8:b2:ac:27:36:4b	60	2.97 Kbps	52 dB	🟩	08:47:
NTPC-MLearning-M	[redacted]		[redacted]	9c:f3:87:90:4b:b7	5	0 bps	22 dB	🟧	08:50:
NTPC-MLearning-M	[redacted]		[redacted]	10:1c:0c:31:f8:65	5	0 bps	30 dB	🟨	08:31:
NTPC-MLearning-M	[redacted]		[redacted]	e8:b2:ac:26:c3:fe	60	0 bps	52 dB	🟩	08:51:
NTPC-MLearning-M	[redacted]		[redacted]	e8:b2:ac:56:73:3c	60	5.02 Kbps	44 dB	🟩	08:51:
NTPC-MLearning-M	[redacted]		[redacted]	10:1c:0c:2e:5a:aa	60	0 bps	34 dB	🟨	07:43:
NTPC-MLearning-M	[redacted]		[redacted]	e8:b2:ac:11:b1:31	60	2.30 Kbps	47 dB	🟩	08:47:
NTPC-MLearning-M	[redacted]		[redacted]	e8:b2:ac:36:09:2d	60	27.62 Kbps	44 dB	🟩	08:50:
NTPC-MLearning-M	[redacted]		[redacted]	e8:b2:ac:1e:60:0c	60	11.40 Kbps	43 dB	🟩	08:48:
NTPC-MLearning-M	[redacted]		[redacted]	e8:b2:ac:11:b0:f0	60	5.67 Kbps	51 dB	🟩	08:49:
NTPC-MLearning-M	[redacted]		[redacted]	10:1c:0c:30:fe:43	60	0 bps	31 dB	🟨	07:40:
NTPC-MLearning-M	[redacted]		[redacted]	10:1c:0c:34:58:c3	5	0 bps	30 dB	🟨	09:01:
NTPC-MLearning-M	[redacted]		[redacted]	10:1c:0c:3e:cc:3b	5	0 bps	30 dB	🟨	08:52:
NTPC-MLearning-M	[redacted]		[redacted]	9c:f3:87:90:33:72	5	0 bps	26 dB	🟨	09:01:
NTPC-MLearning-M	[redacted]		[redacted]	e8:b2:ac:26:28:5b	60	11.39 Kbps	44 dB	🟩	08:27:
NTPC-MLearning-M	[redacted]		[redacted]	10:1c:0c:3d:d1:a1	60	0 bps	34 dB	🟨	06:53:
NTPC-MLearning-M	[redacted]		[redacted]	10:1c:0c:3d:d2:a1	60	0 bps	30 dB	🟨	07:51:
NTPC-MLearning-M	[redacted]		[redacted]	e8:b2:ac:5d:b2:77	60	16.75 Kbps	52 dB	🟩	08:48:
NTPC-MLearning-M	[redacted]		[redacted]	10:1c:0c:3b:d8:79	5	34.02 Kbps	0 dB	🟥	08:57:
NTPC-MLearning-M	[redacted]		[redacted]	84:89:ad:39:7b:23	60	397.25 Kbps	51 dB	🟩	03:25:11 (20
NTPC-MLearning-M	[redacted]		[redacted]	e8:b2:ac:36:09:2a	60	11.67 Kbps	46 dB	🟩	08:22:

1 / 2 [全部用戶: 61]

中孚科技
Sanfran Technologies Inc.

單一AP註冊數量



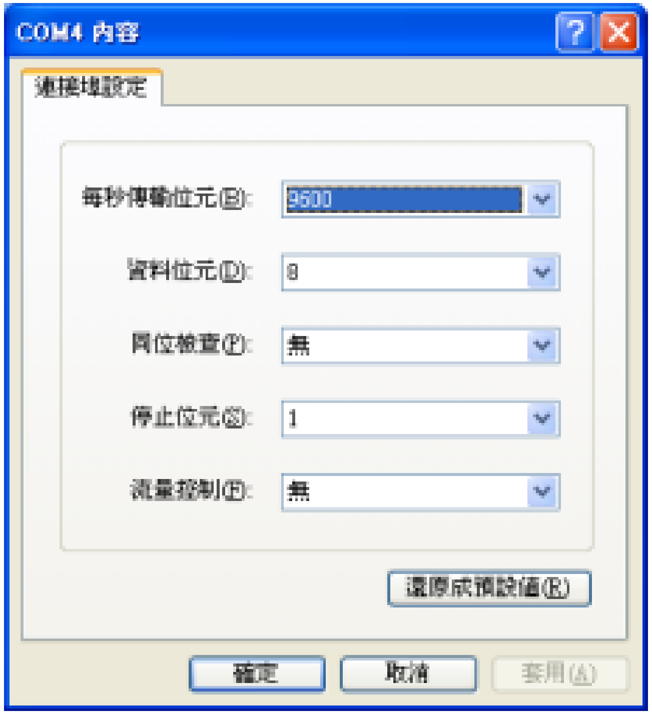
SSID	FortiAP	用戶	IP	設備	...	Tx/Rx帶寬	訊號強度與雜訊	訊號
NTPC-MLearning-M	[redacted]		[redacted]6	e8:b2:ac:36:09:33	60	44.43 Kbps	52 dB	🟩
NTPC-MLearning-M	[redacted]		[redacted]	10:1c:0c:2e:59:d5	60	0 bps	31 dB	🟨
NTPC-MLearning-M	[redacted]		[redacted]15	e8:b2:ac:27:36:d5	60	0 bps	43 dB	🟩
NTPC-MLearning-M	[redacted]		[redacted]42	10:1c:0c:3c:c4:ae	60	0 bps	43 dB	🟩
NTPC-MLearning-M	[redacted]		[redacted]7	10:1c:0c:34:26:fe	60	0 bps	36 dB	🟨
NTPC-MLearning-M	[redacted]		[redacted]3	e8:b2:ac:26:c5:00	60	11.79 Kbps	48 dB	🟩
NTPC-MLearning-M	[redacted]		[redacted]3	e8:b2:ac:1f:b3:a4	60	52.82 Kbps	48 dB	🟩
NTPC-Mobile-M	[redacted]		[redacted].34	10:1c:0c:2e:a4:3b	60	9 bps	50 dB	🟩
NTPC-WPA2	[redacted]	sunmei@ntpc.edu.tw	[redacted].1	b8:53:ac:18:1e:8c	60	9 bps	50 dB	🟩
NTPC-WPA2	[redacted]	chany0824@ntpc.edu.tw	[redacted].12	00:b3:62:45:36:cd	60	0 bps	50 dB	🟩
NTPC-WPA2	[redacted]	chany0824@ntpc.edu.tw	[redacted].11	6c:40:08:b5:3a:3a	60	11.70 Kbps	50 dB	🟩

2 / 2 [全部用戶: 61]

防火牆使用介紹

Console設定

- Serial Console (RJ45) for CLI
  - 每秒傳輸位元 ：9600
  - 資料位元：8
  - 同位檢查： 無
  - 停止位元：1
  - 流量控制： 無


COM4 內容

連接埠設定

每秒傳輸位元(B): 9600

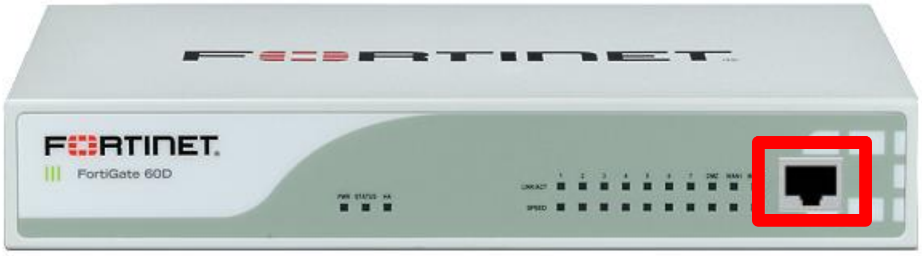
資料位元(D): 8

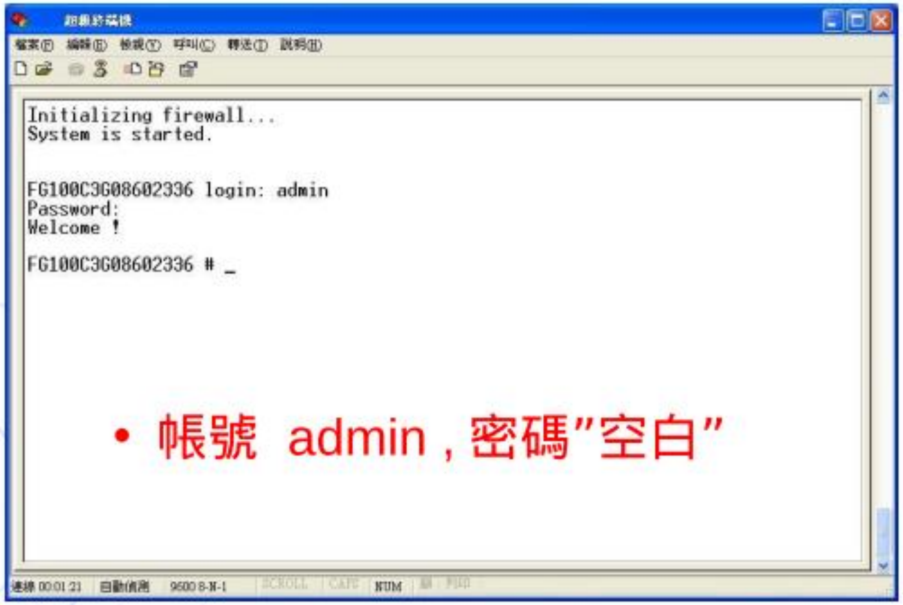
同位檢查(P): 無

停止位元(S): 1

流量控制(F): 無

Console Login



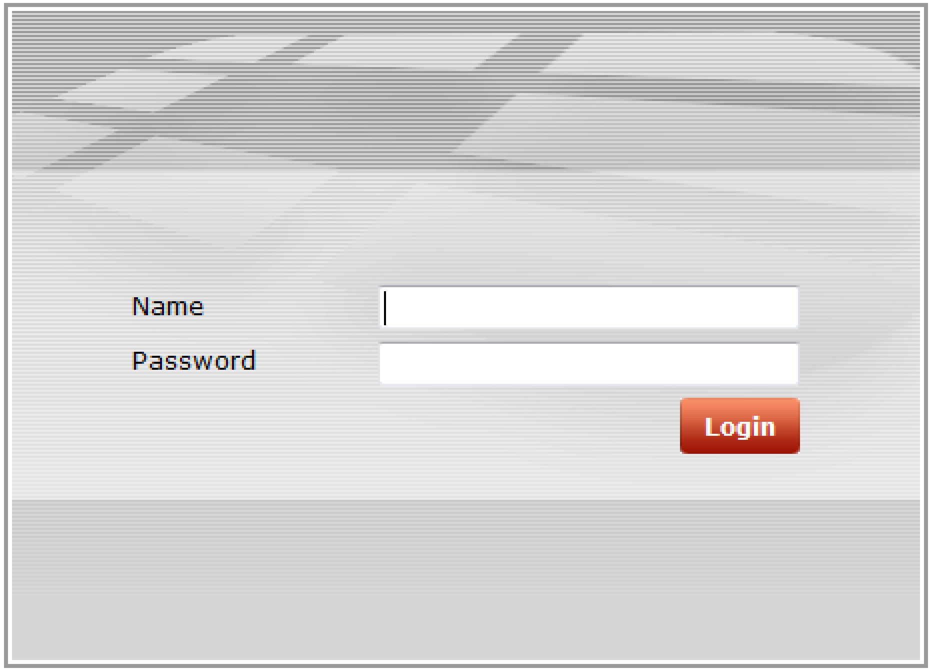

超級終端機
檔案(F) 編輯(E) 檢視(V) 呼叫(C) 轉送(T) 說明(H)
連線 00:01:21 自動偵測 9600 8-N-1 SCROLL CAPS NUM

```
Initializing firewall...
System is started.

FG100C3G08602336 login: admin
Password:
Welcome !

FG100C3G08602336 # _
```

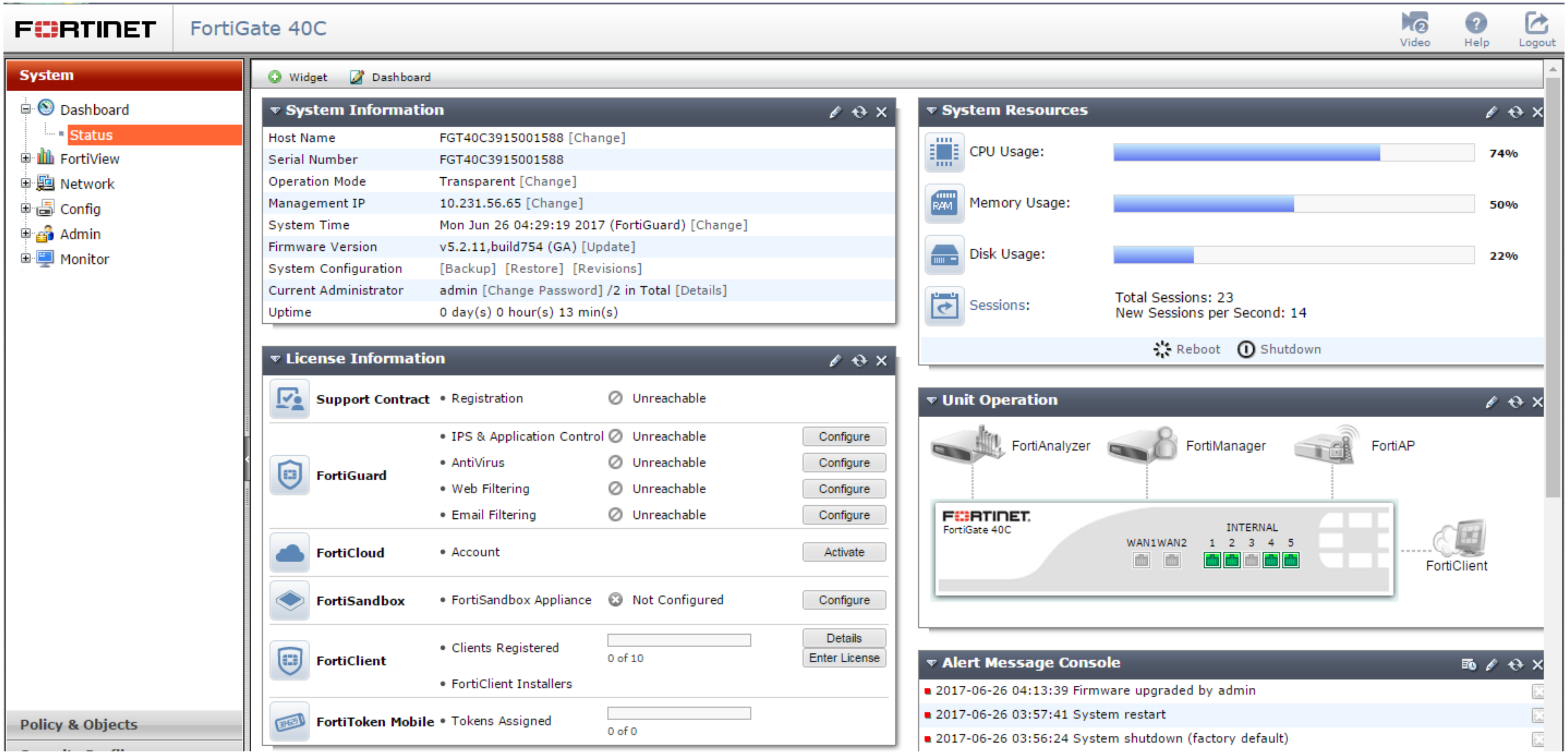
- 帳號 admin，密碼"空白"

管理頁面登入

- 連接第一埠與電腦並開啟瀏覽器
- 網址列輸入https://10.231.56.X
  - 預設登入帳號”admin”，密碼”空白”）
- 行動箱管理頁面為https://192.168.110.254
  - 登入帳號:admin 密碼 :!QAZ2wsx



儀表板概觀



System Information

Host Name	FGT40C3915001588 [Change]
Serial Number	FGT40C3915001588
Operation Mode	Transparent [Change]
Management IP	10.231.56.65 [Change]
System Time	Mon Jun 26 04:29:19 2017 (FortiGuard) [Change]
Firmware Version	v5.2.11,build754 (GA) [Update]
System Configuration	[Backup] [Restore] [Revisions]
Current Administrator	admin [Change Password] /2 in Total [Details]
Uptime	0 day(s) 0 hour(s) 13 min(s)

System Resources

CPU Usage:	74%
Memory Usage:	50%
Disk Usage:	22%
Sessions:	Total Sessions: 23 New Sessions per Second: 14

License Information

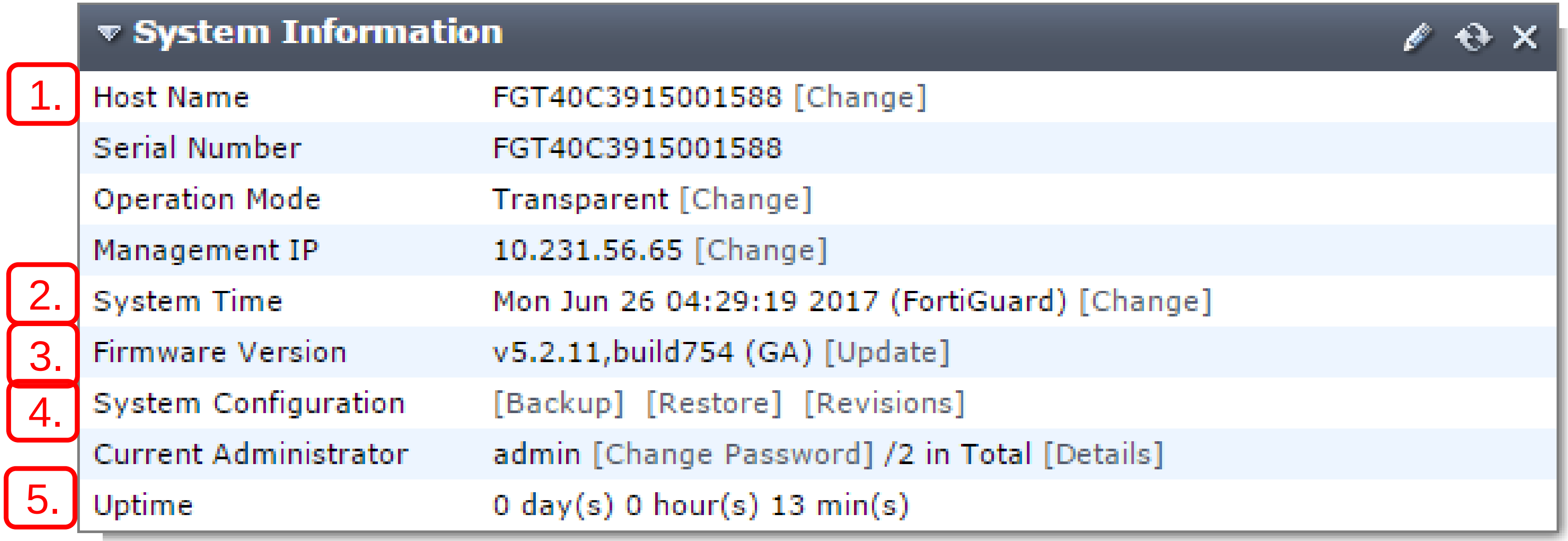
Support Contract	• Registration	⊘ Unreachable	
FortiGuard	• IPS & Application Control	⊘ Unreachable	Configure
	• AntiVirus	⊘ Unreachable	Configure
	• Web Filtering	⊘ Unreachable	Configure
	• Email Filtering	⊘ Unreachable	Configure
FortiCloud	• Account		Activate
FortiSandbox	• FortiSandbox Appliance	⊗ Not Configured	Configure
FortiClient	• Clients Registered	0 of 10	Details Enter License
	• FortiClient Installers		
FortiToken Mobile	• Tokens Assigned	0 of 0	

Unit Operation

Alert Message Console

- 2017-06-26 04:13:39 Firmware upgraded by admin
- 2017-06-26 03:57:41 System restart
- 2017-06-26 03:56:24 System shutdown (factory default)

系統資訊



▾ System Information

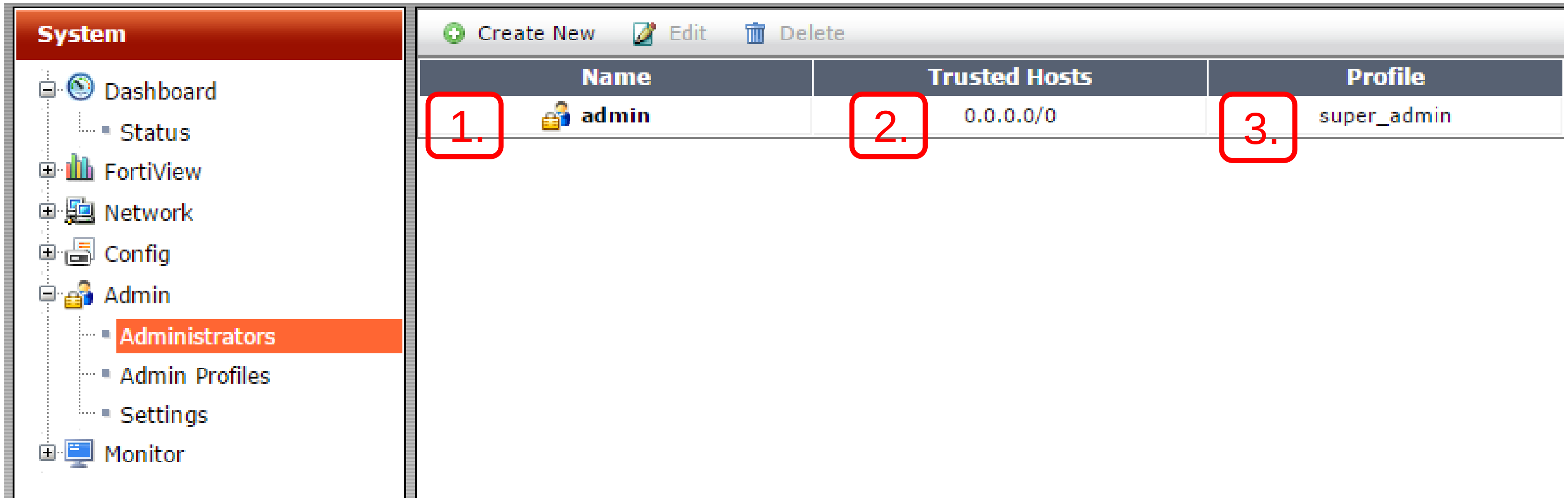
Host Name	FGT40C3915001588 [Change]
Serial Number	FGT40C3915001588
Operation Mode	Transparent [Change]
Management IP	10.231.56.65 [Change]
System Time	Mon Jun 26 04:29:19 2017 (FortiGuard) [Change]
Firmware Version	v5.2.11,build754 (GA) [Update]
System Configuration	[Backup] [Restore] [Revisions]
Current Administrator	admin [Change Password] /2 in Total [Details]
Uptime	0 day(s) 0 hour(s) 13 min(s)

1. 設定設備名稱
2. 設定系統時間
3. FortiOS版本
4. 設定備份及恢復
5. 檢視系統已開機時間

管理者新增

設備管理者

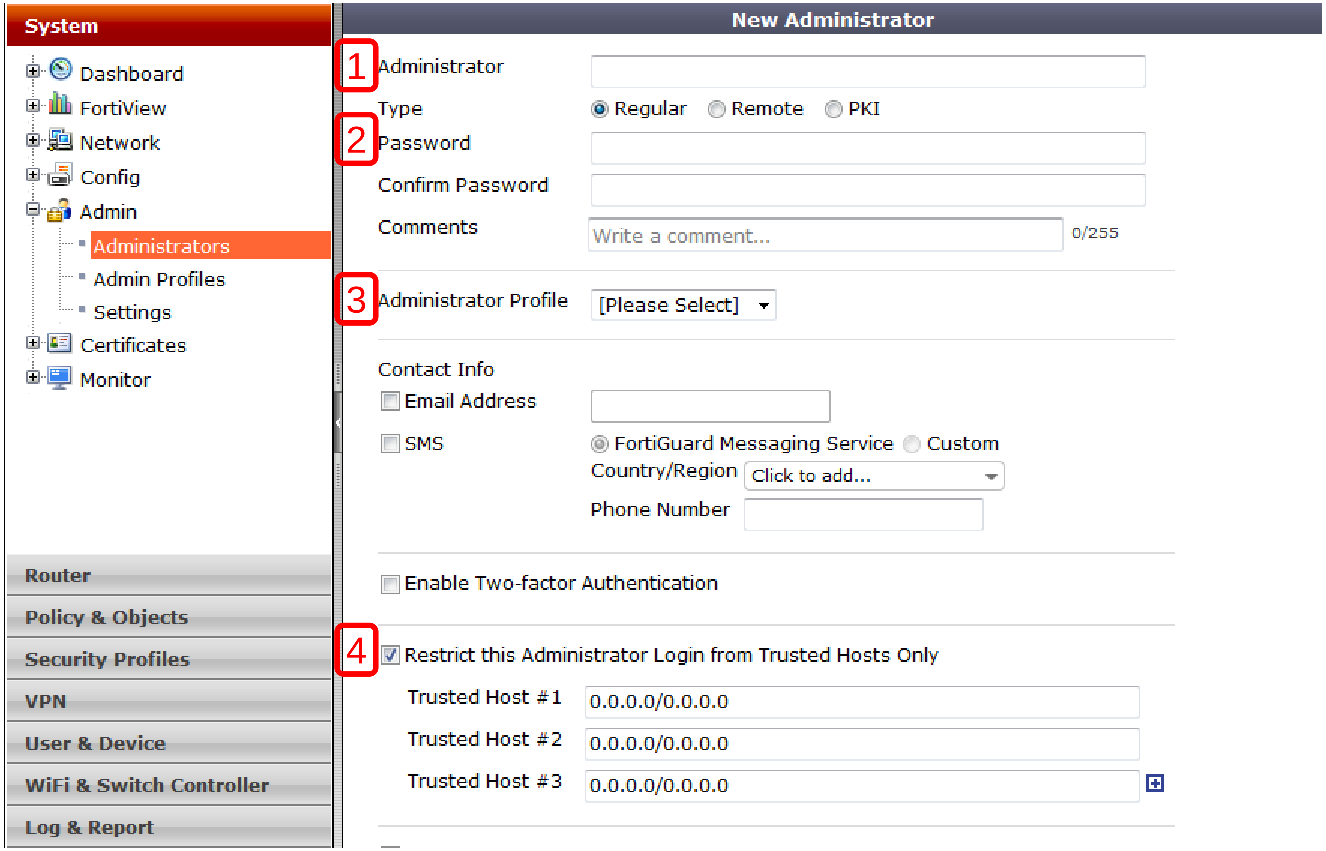
- 選單路徑System>Admin>Administrators



Name	Trusted Hosts	Profile
admin	0.0.0.0/0	super_admin

1. 管理者名稱
2. 限定管理IP
3. 管理者範本

新增管理者



New Administrator

Administrator
Type ● Regular ○ Remote ○ PKI
Password
Confirm Password
Comments Write a comment... 0/255

Administrator Profile [Please Select]

Contact Info
□ Email Address
□ SMS ● FortiGuard Messaging Service ○ Custom
Country/Region Click to add...
Phone Number

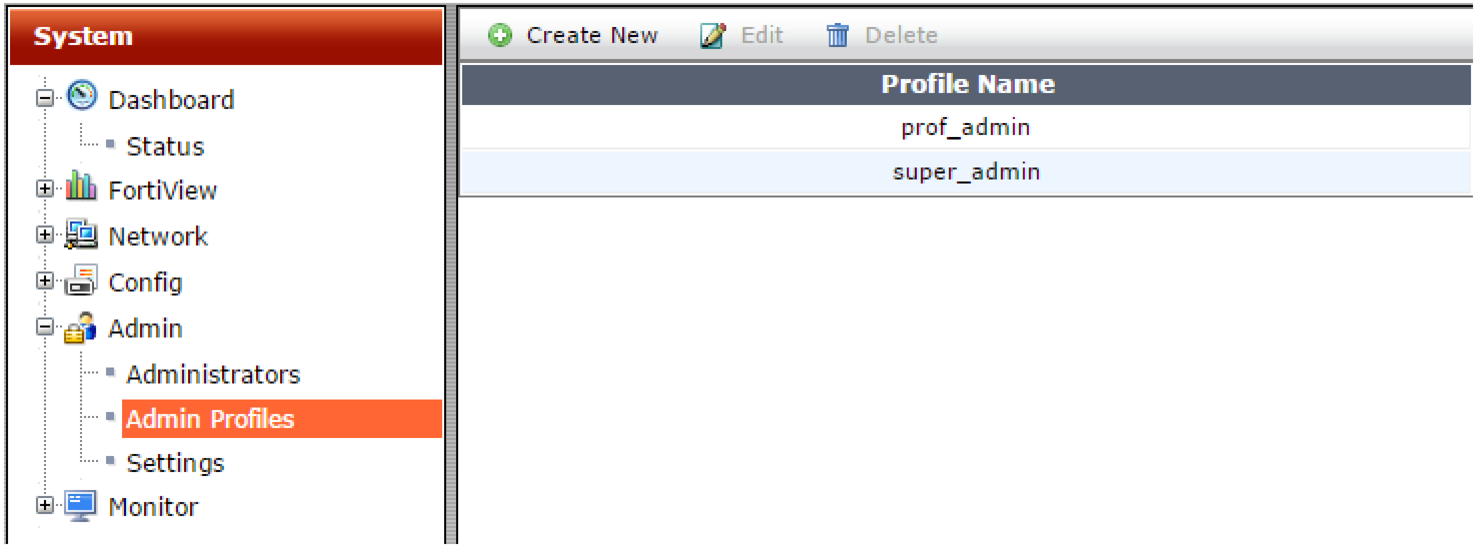
□ Enable Two-factor Authentication

☑ Restrict this Administrator Login from Trusted Hosts Only
Trusted Host #1 0.0.0.0/0.0.0.0
Trusted Host #2 0.0.0.0/0.0.0.0
Trusted Host #3 0.0.0.0/0.0.0.0

1. 管理者帳號名稱
2. 管理者密碼
3. 管理者權限範本
4. 管理者限定登入IP

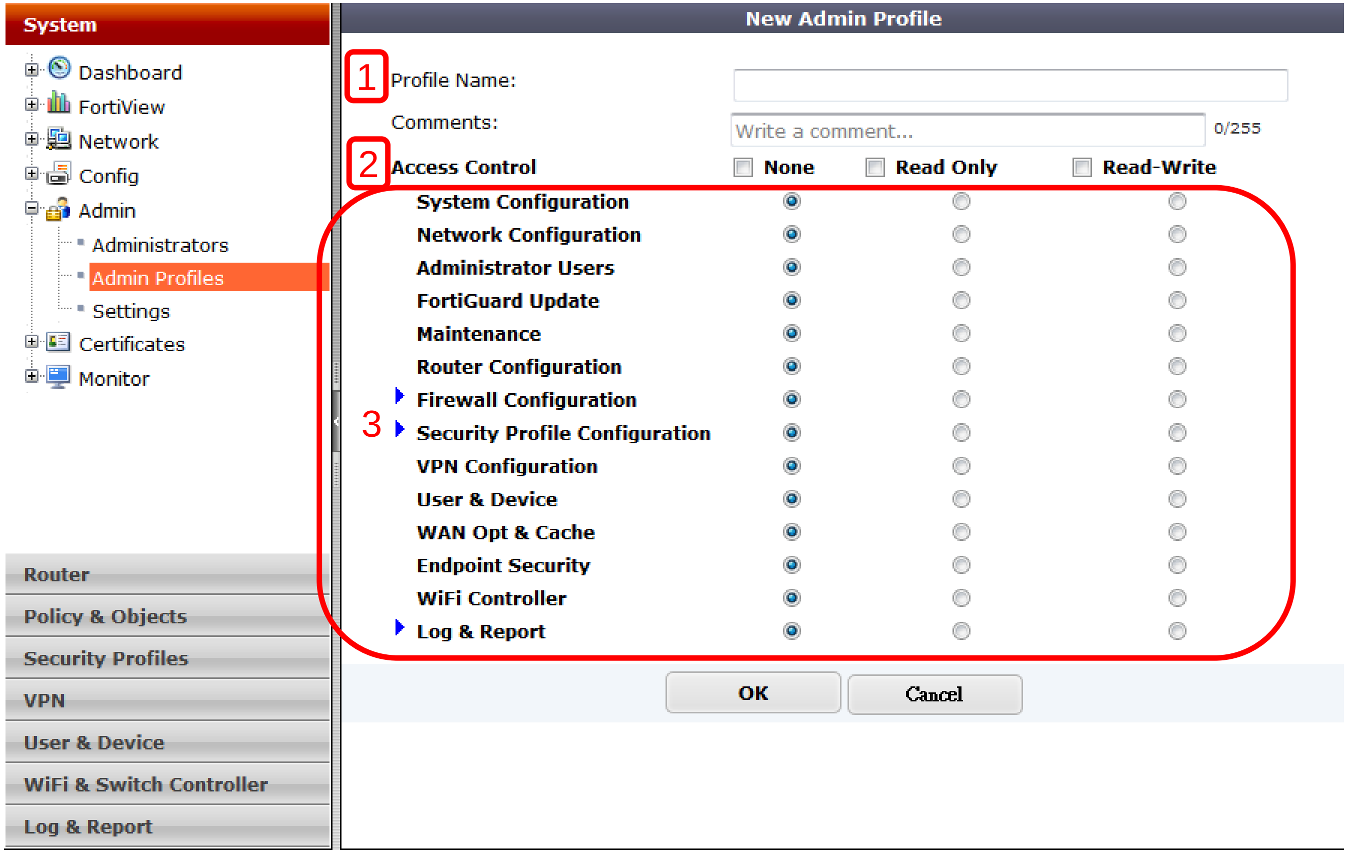
管理者權限範本

- 選單路徑System>Admin>Admin Profiles



Profile Name
prof_admin
super_admin

管理者範本



New Admin Profile

Profile Name:

Comments: Write a comment... 0/255

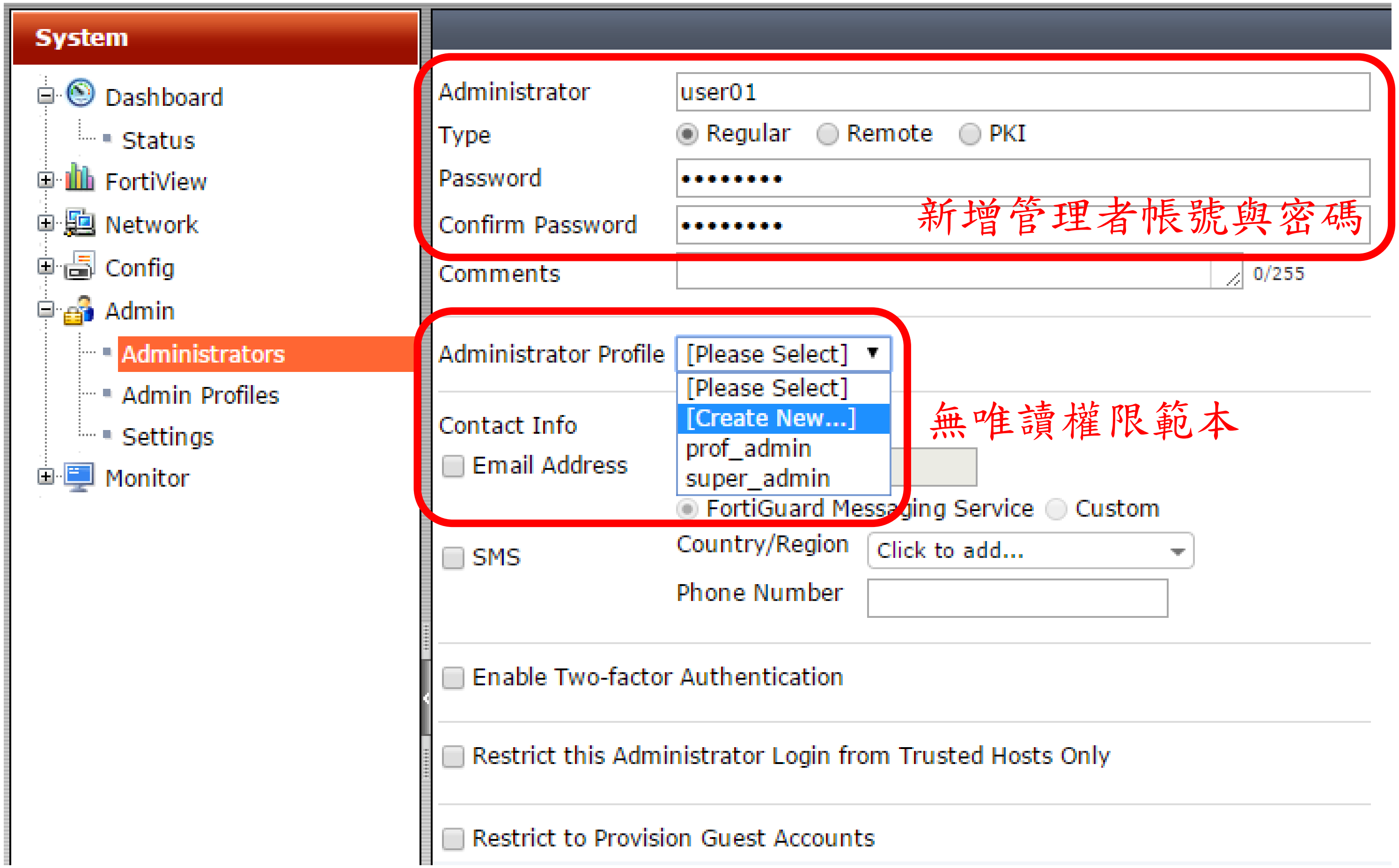
Access Control	□ None	□ Read Only	□ Read-Write
System Configuration	●	○	○
Network Configuration	●	○	○
Administrator Users	●	○	○
FortiGuard Update	●	○	○
Maintenance	●	○	○
Router Configuration	●	○	○
Firewall Configuration	●	○	○
Security Profile Configuration	●	○	○
VPN Configuration	●	○	○
User & Device	●	○	○
WAN Opt & Cache	●	○	○
Endpoint Security	●	○	○
WiFi Controller	●	○	○
Log & Report	●	○	○

1. 管理者範本名稱
2. 預設權限類型
3. 可管理項目

實機操作-唯讀管理者新增

- 1.建立管理者帳號
- 2.唯讀權限範本建立
- 3.權限範本套用與帳號IP綁定

實機操作-管理者新增



Administrator: user01

Type: ● Regular ○ Remote ○ PKI

Password: ••••••••

Confirm Password: ••••••••

新增管理者帳號與密碼

Comments: 0/255

Administrator Profile: [Please Select] ▼

- [Please Select]
- [Create New...]
- prof_admin
- super_admin

無唯讀權限範本

Contact Info

□ Email Address

● FortiGuard Messaging Service ○ Custom

□ SMS

Country/Region: Click to add...

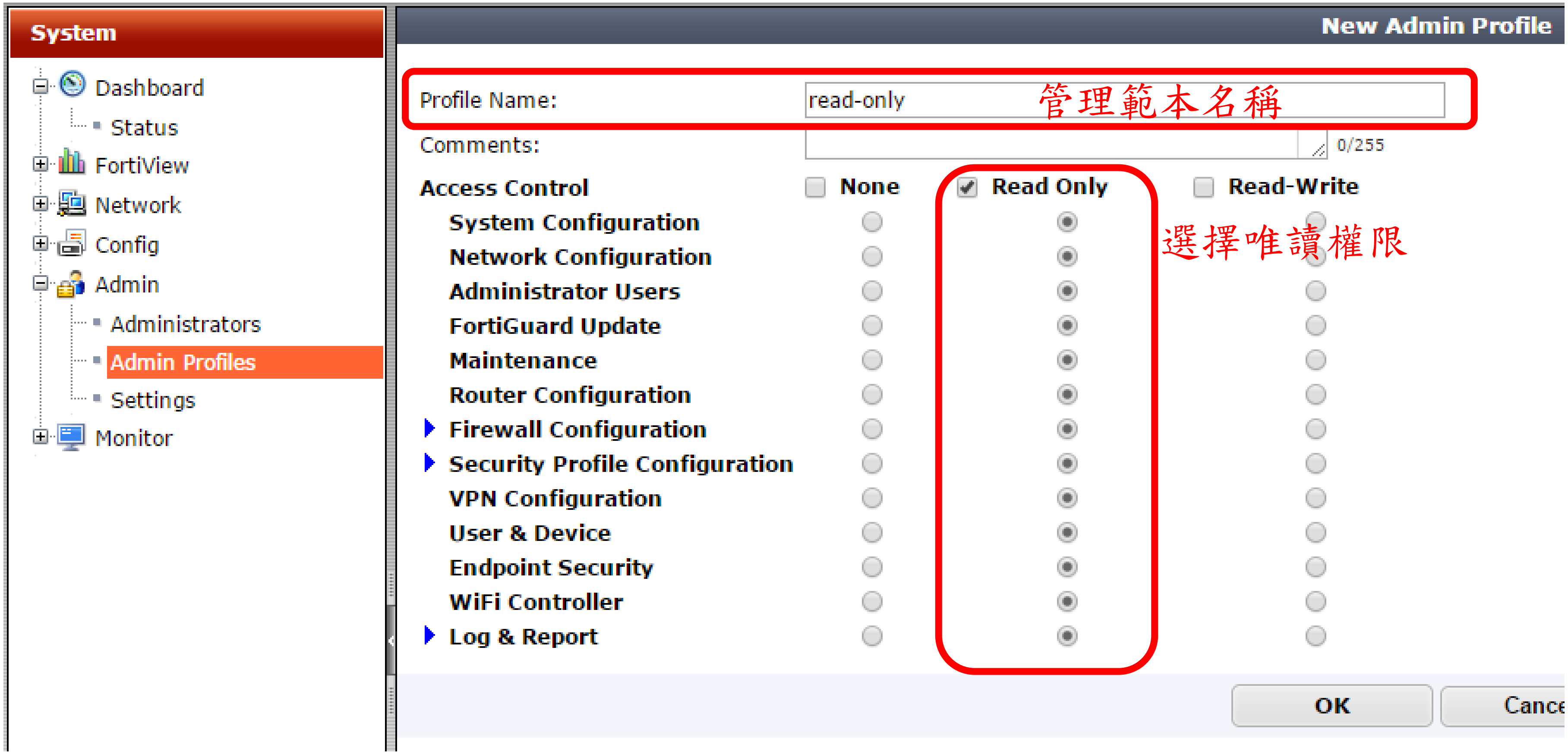
Phone Number:

□ Enable Two-factor Authentication

□ Restrict this Administrator Login from Trusted Hosts Only

□ Restrict to Provision Guest Accounts

實機操作-唯讀權限範本



Profile Name: read-only

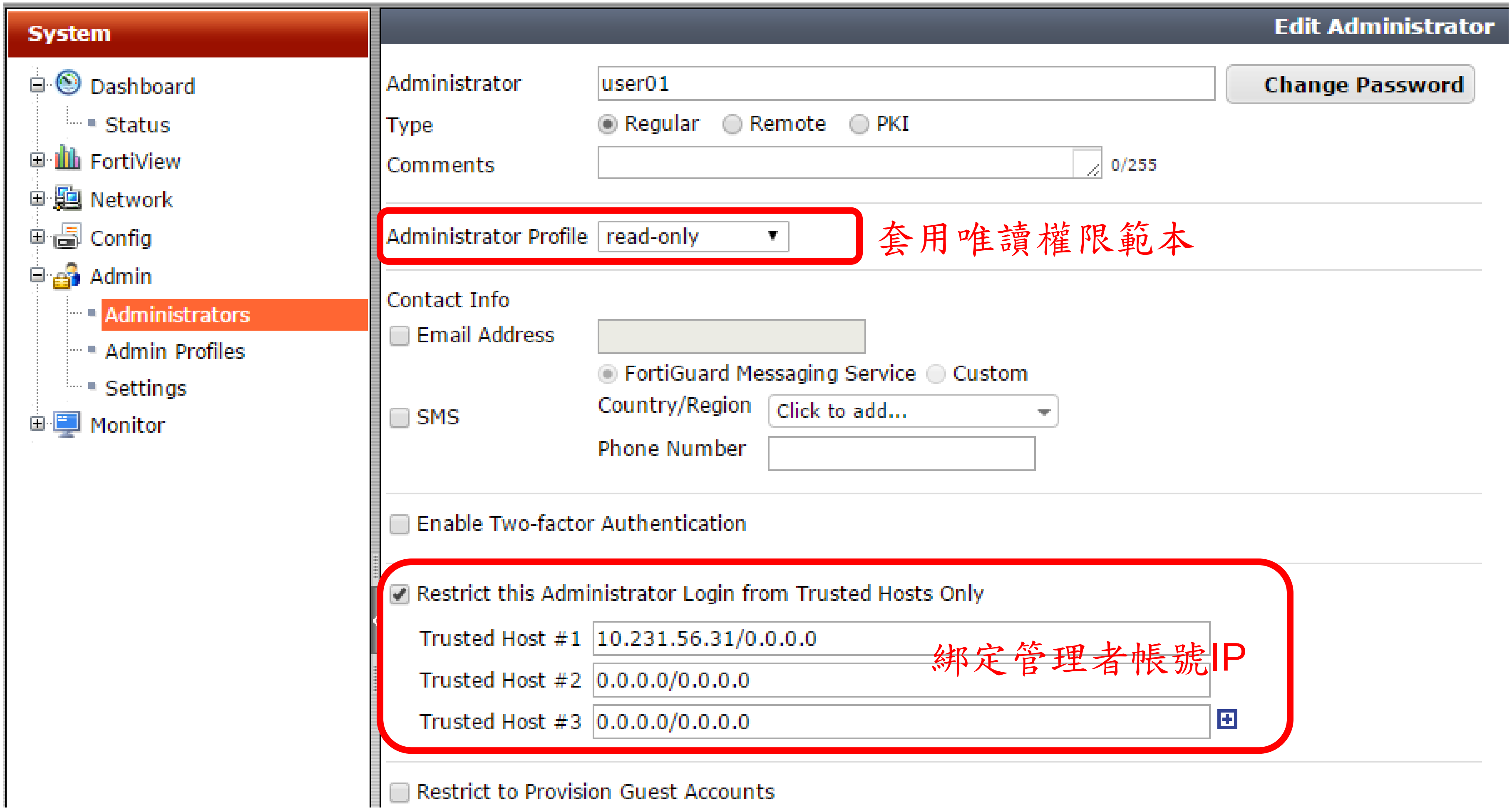
管理範本名稱

Comments: 0/255

Access Control	□ None	☑ Read Only	□ Read-Write
System Configuration	○	●	○
Network Configuration	○	●	○
Administrator Users	○	●	○
FortiGuard Update	○	●	○
Maintenance	○	●	○
Router Configuration	○	●	○
▶ Firewall Configuration	○	●	○
▶ Security Profile Configuration	○	●	○
VPN Configuration	○	●	○
User & Device	○	●	○
Endpoint Security	○	●	○
WiFi Controller	○	●	○
▶ Log & Report	○	●	○

選擇唯讀權限

實機操作-唯讀權限與IP綁定



Administrator: user01

Type: ● Regular ○ Remote ○ PKI

Comments: 0/255

Administrator Profile: read-only

套用唯讀權限範本

Contact Info

□ Email Address

● FortiGuard Messaging Service ○ Custom

□ SMS

Country/Region: Click to add...

Phone Number:

□ Enable Two-factor Authentication

☑ Restrict this Administrator Login from Trusted Hosts Only

Trusted Host #1: 10.231.56.31/0.0.0.0

Trusted Host #2: 0.0.0.0/0.0.0.0

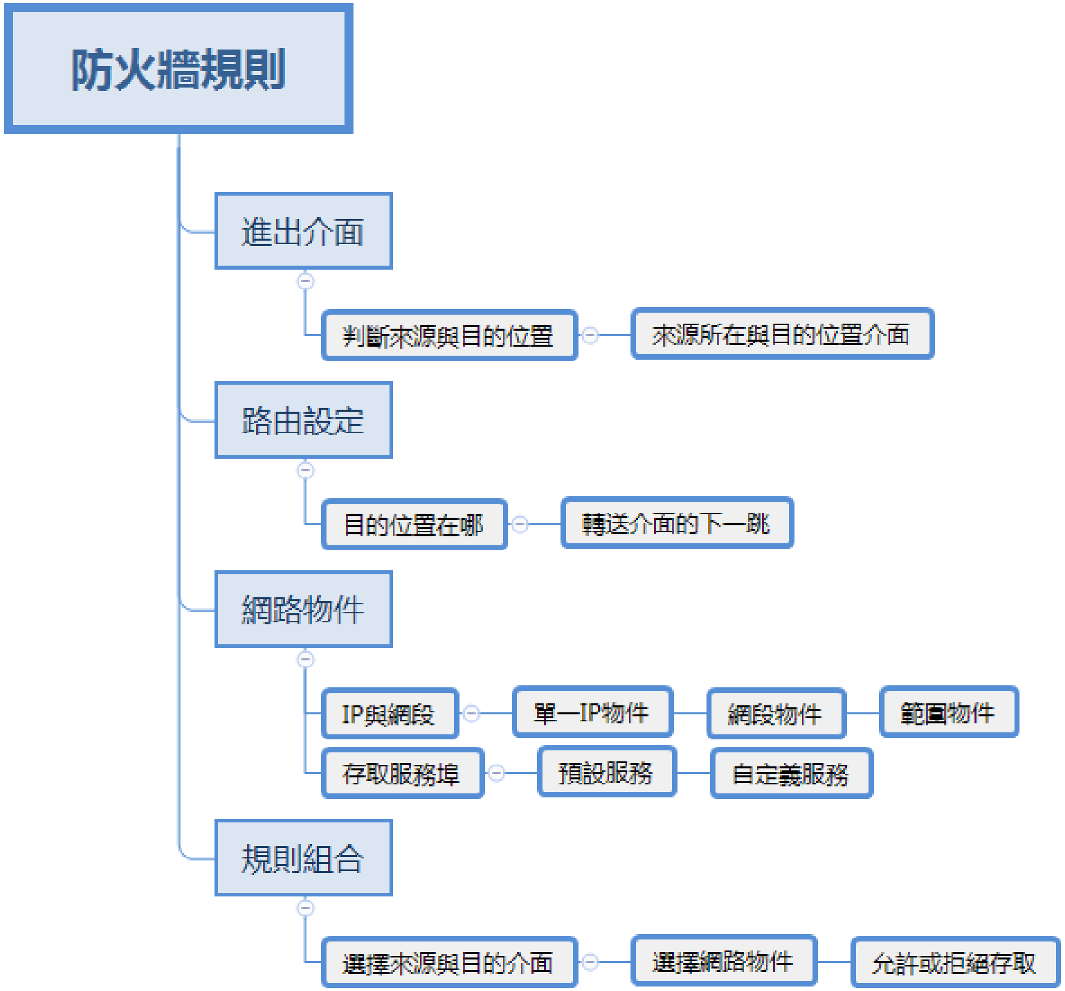
Trusted Host #3: 0.0.0.0/0.0.0.0

綁定管理者帳號IP

□ Restrict to Provision Guest Accounts

防火牆規則

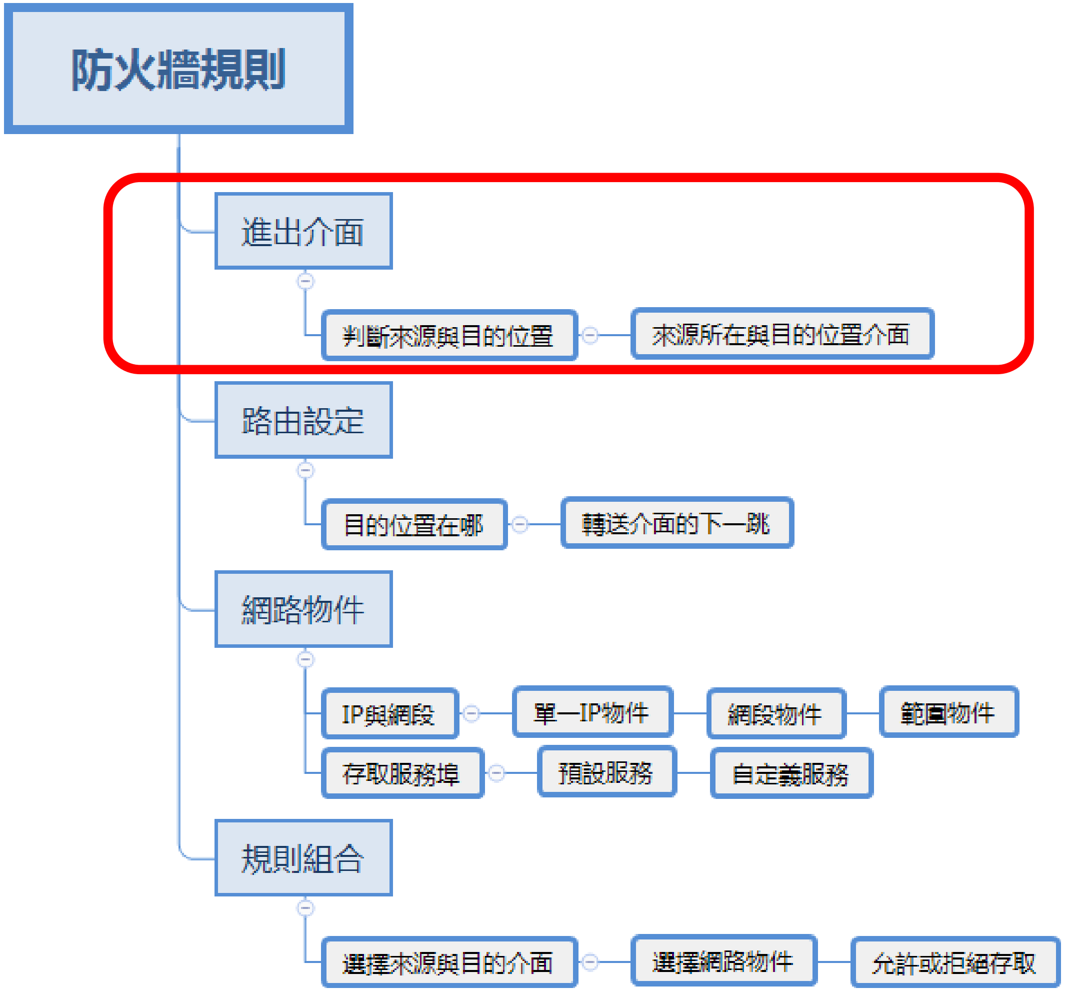
防火牆規則設定



防火牆規則

- 進出介面
  - 判斷來源與目的位置 — 來源所在與目的位置介面
- 路由設定
  - 目的位置在哪 — 轉送介面的下一跳
- 網路物件
  - IP與網段 — 單一IP物件 — 網段物件 — 範圍物件
  - 存取服務埠 — 預設服務 — 自定義服務
- 規則組合
  - 選擇來源與目的介面 — 選擇網路物件 — 允許或拒絕存取

進出介面


防火牆規則

進出介面

判斷來源與目的位置

來源所在與目的位置介面

路由設定

目的位置在哪

轉送介面的下一跳

網路物件

IP與網段

單一IP物件

網段物件

範圍物件

存取服務埠

預設服務

自定義服務

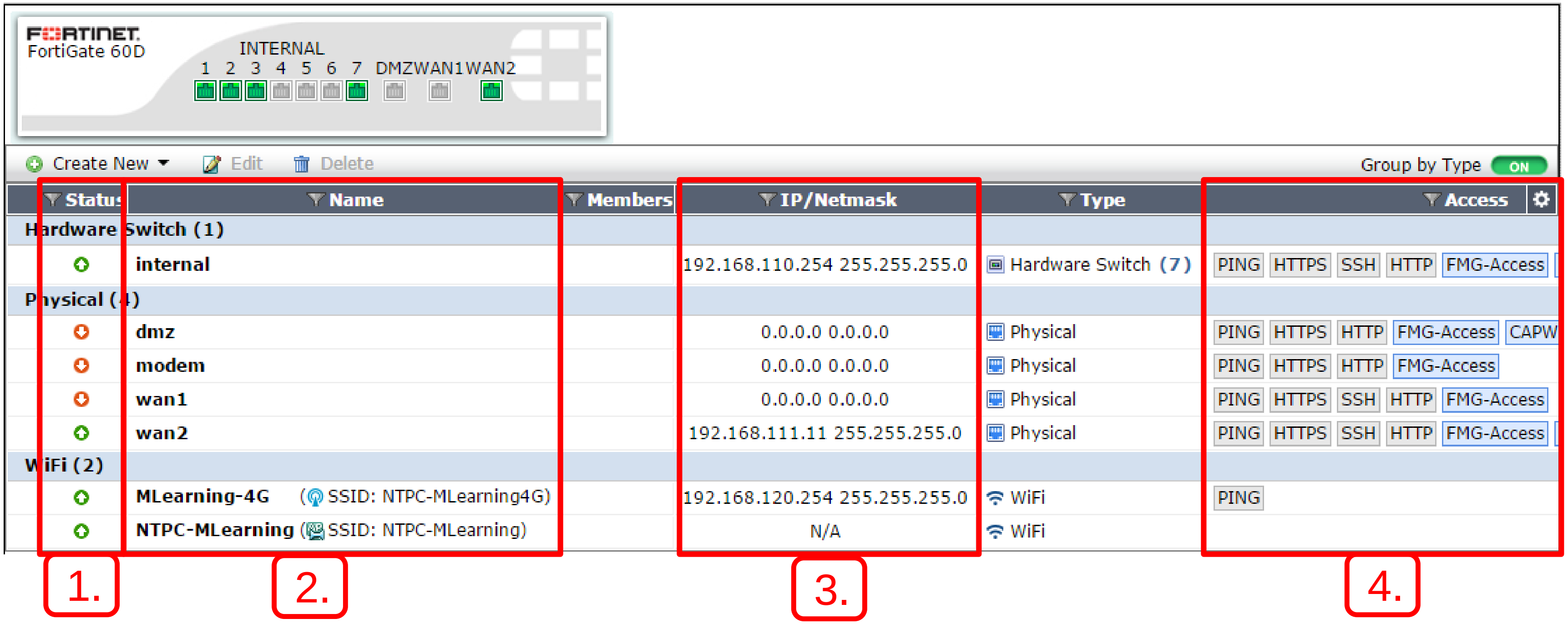
規則組合

選擇來源與目的介面

選擇網路物件

允許或拒絕存取

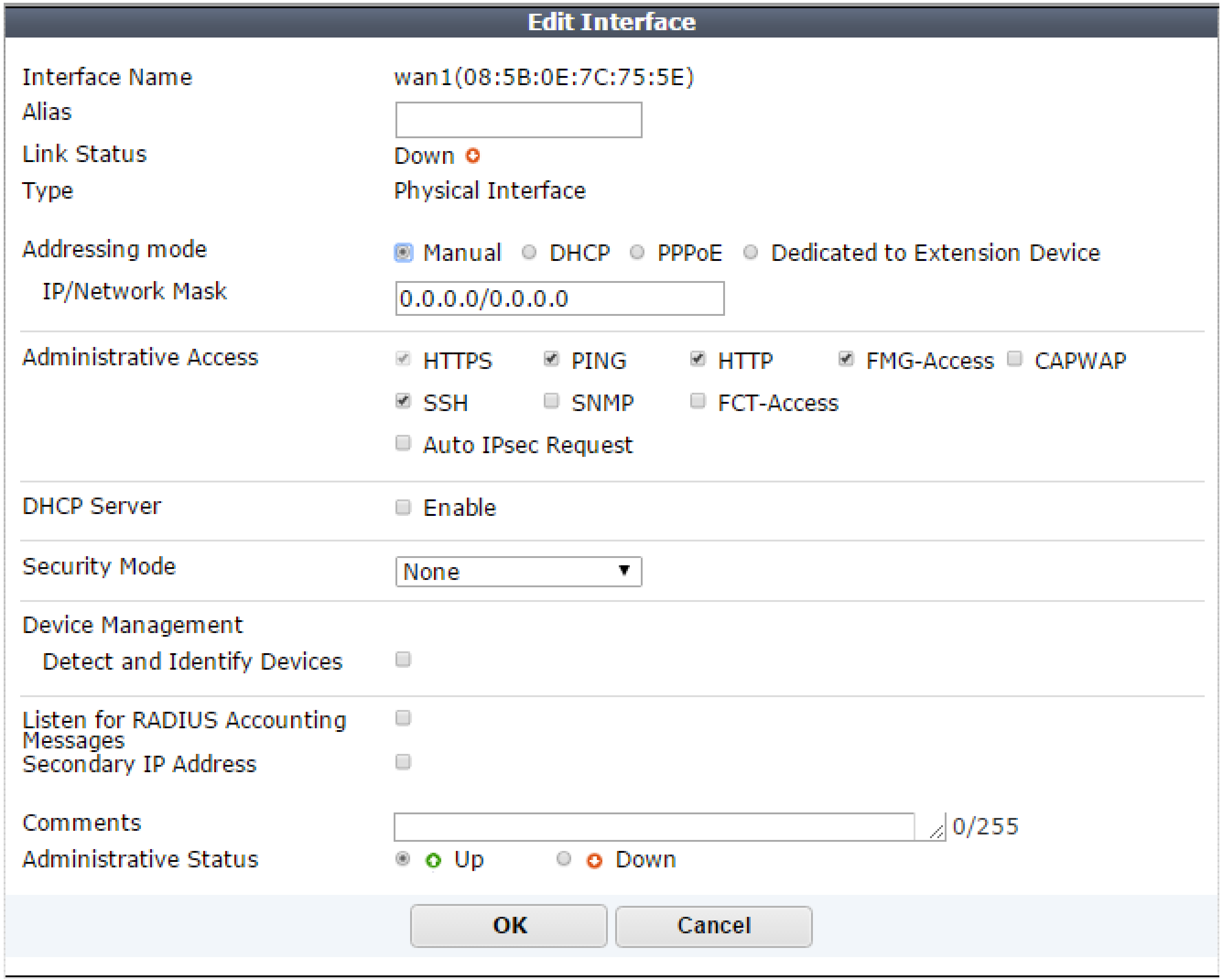
介面說明



Status	Name	Members	IP/Netmask	Type	Access
Hardware Switch (1)					
▲	internal		192.168.110.254 255.255.255.0	Hardware Switch (7)	PING HTTPS SSH HTTP FMG-Access
Physical (4)					
▼	dmz		0.0.0.0 0.0.0.0	Physical	PING HTTPS HTTP FMG-Access CAPW
▼	modem		0.0.0.0 0.0.0.0	Physical	PING HTTPS HTTP FMG-Access
▼	wan1		0.0.0.0 0.0.0.0	Physical	PING HTTPS SSH HTTP FMG-Access
▲	wan2		192.168.111.11 255.255.255.0	Physical	PING HTTPS SSH HTTP FMG-Access
WiFi (2)					
▲	MLearning-4G (SSID: NTPC-MLearning4G)		192.168.120.254 255.255.255.0	WiFi	PING
▲	NTPC-MLearning (SSID: NTPC-MLearning)		N/A	WiFi	

1. 介面狀態
2. 介面名稱
3. IP位址
4. 開放存取

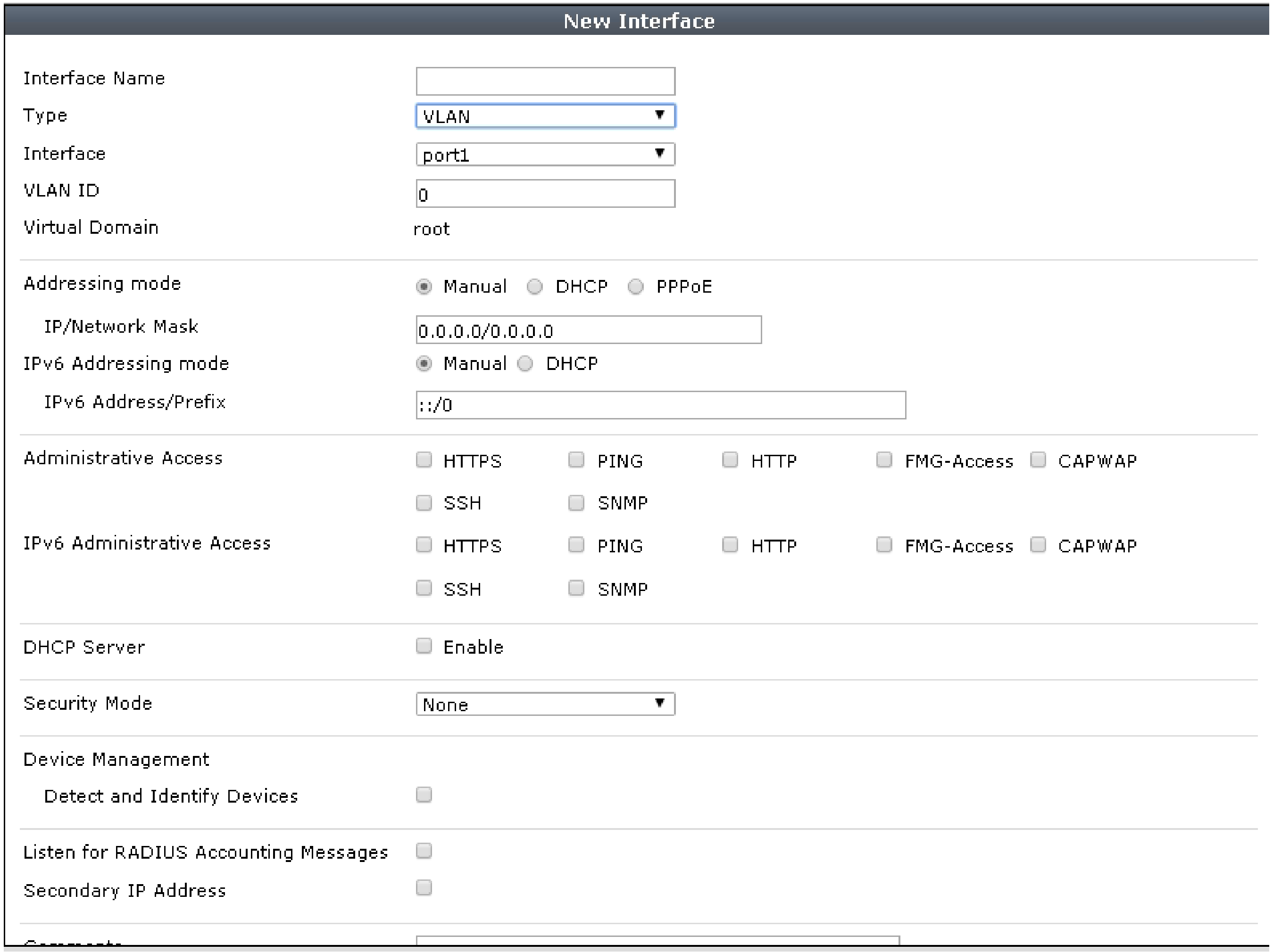
編輯介面



Edit Interface

Interface Name	wan1(08:5B:0E:7C:75:5E)
Alias	
Link Status	Down
Type	Physical Interface
Addressing mode	● Manual ○ DHCP ○ PPPoE ○ Dedicated to Extension Device
IP/Network Mask	0.0.0.0/0.0.0.0
Administrative Access	☑ HTTPS ☑ PING ☑ HTTP ☑ FMG-Access □ CAPWAP ☑ SSH □ SNMP □ FCT-Access □ Auto IPsec Request
DHCP Server	□ Enable
Security Mode	None
Device Management	
Detect and Identify Devices	□
Listen for RADIUS Accounting Messages	□
Secondary IP Address	□
Comments	0/255
Administrative Status	● Up ○ Down

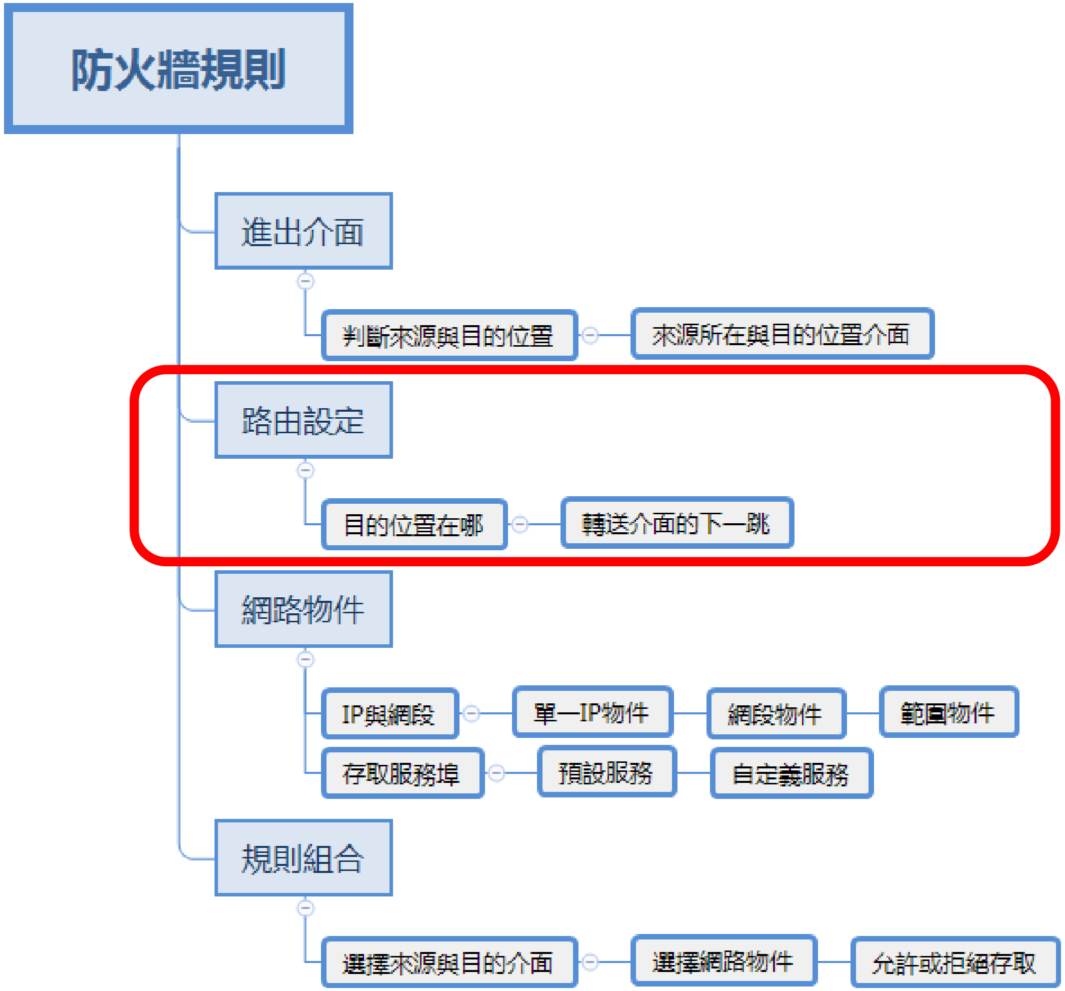
Vlan介面



New Interface

Interface Name	
Type	VLAN ▼
Interface	port1 ▼
VLAN ID	0
Virtual Domain	root
Addressing mode	● Manual ○ DHCP ○ PPPoE
IP/Network Mask	0.0.0.0/0.0.0.0
IPv6 Addressing mode	● Manual ○ DHCP
IPv6 Address/Prefix	::/0
Administrative Access	□ HTTPS □ PING □ HTTP □ FMG-Access □ CAPWAP □ SSH □ SNMP
IPv6 Administrative Access	□ HTTPS □ PING □ HTTP □ FMG-Access □ CAPWAP □ SSH □ SNMP
DHCP Server	□ Enable
Security Mode	None ▼
Device Management	
Detect and Identify Devices	□
Listen for RADIUS Accounting Messages	□
Secondary IP Address	□
Comments	

路由設定

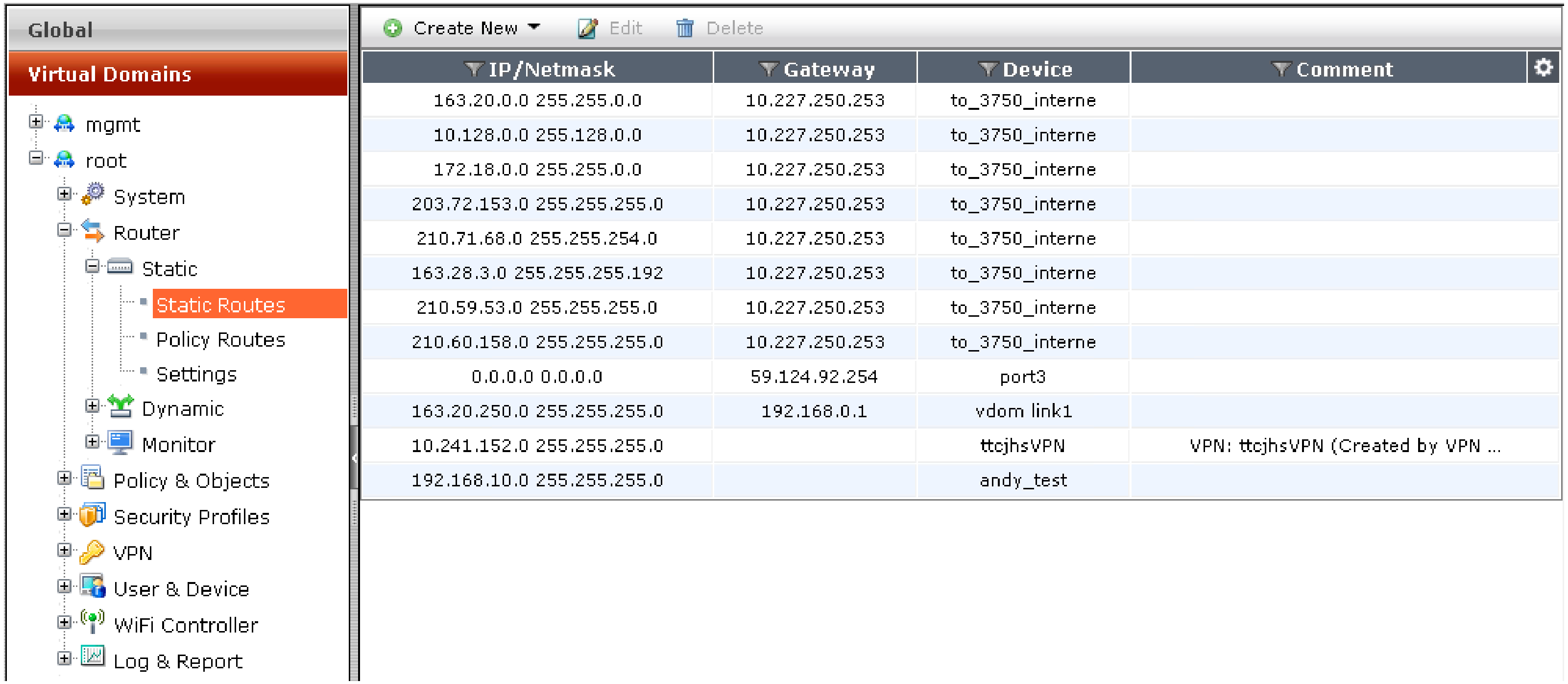


防火牆規則

- 進出介面
  - 判斷來源與目的位置
    - 來源所在與目的位置介面
- 路由設定
  - 目的位置在哪
    - 轉送介面的下一跳
- 網路物件
  - IP與網段
    - 單一IP物件
    - 網段物件
    - 範圍物件
  - 存取服務埠
    - 預設服務
    - 自定義服務
- 規則組合
  - 選擇來源與目的介面
    - 選擇網路物件
    - 允許或拒絕存取

路由設定

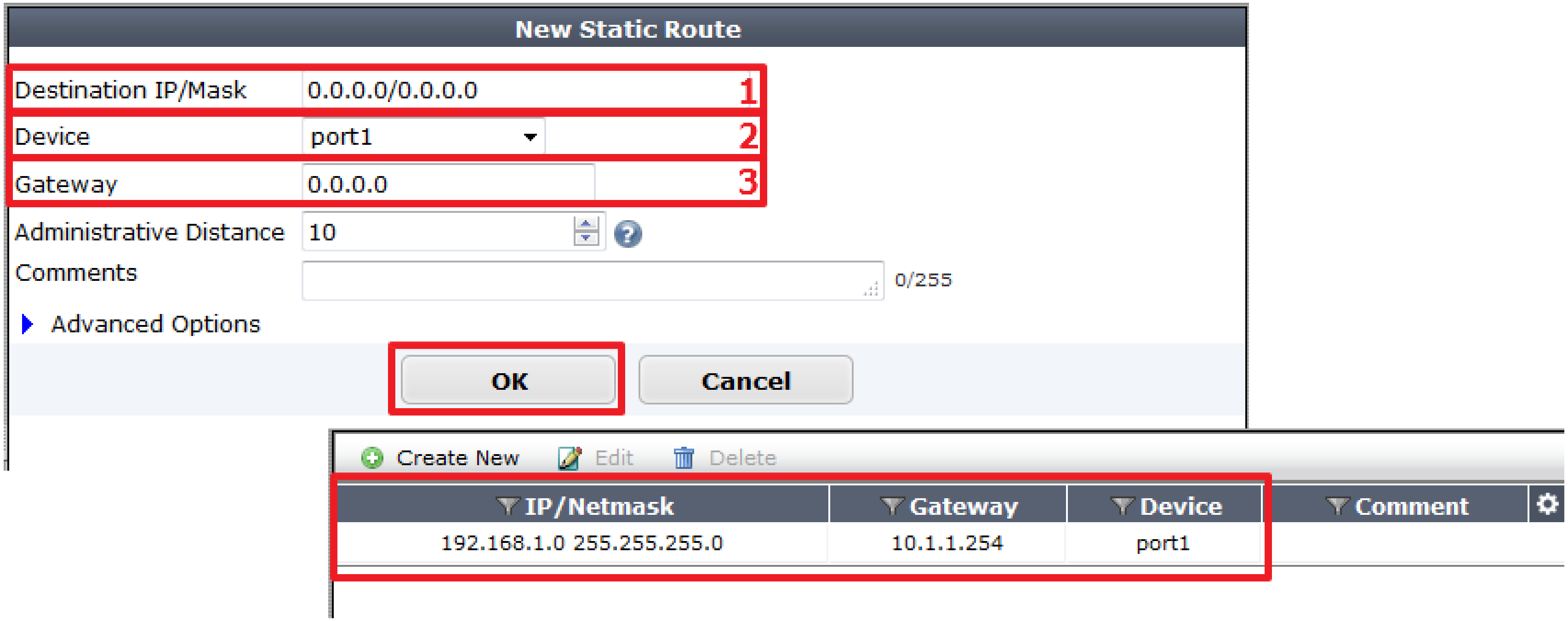
- 選單路徑Router>Static>StaticRoutes
- 點選Create New，進入新增畫面



IP/Netmask	Gateway	Device	Comment
163.20.0.0 255.255.0.0	10.227.250.253	to_3750_interne	
10.128.0.0 255.128.0.0	10.227.250.253	to_3750_interne	
172.18.0.0 255.255.0.0	10.227.250.253	to_3750_interne	
203.72.153.0 255.255.255.0	10.227.250.253	to_3750_interne	
210.71.68.0 255.255.254.0	10.227.250.253	to_3750_interne	
163.28.3.0 255.255.255.192	10.227.250.253	to_3750_interne	
210.59.53.0 255.255.255.0	10.227.250.253	to_3750_interne	
210.60.158.0 255.255.255.0	10.227.250.253	to_3750_interne	
0.0.0.0 0.0.0.0	59.124.92.254	port3	
163.20.250.0 255.255.255.0	192.168.0.1	vdom link1	
10.241.152.0 255.255.255.0		ttcjhsVPN	VPN: ttcjhsVPN (Created by VPN ...
192.168.10.0 255.255.255.0		andy_test	

新增路由

- 1.目的位置網段，往Next Hop轉送的IP資訊
- 2.出口介面，Next Hop所在的設備介面
- 3.出口匝道，Next Hop的IP位址

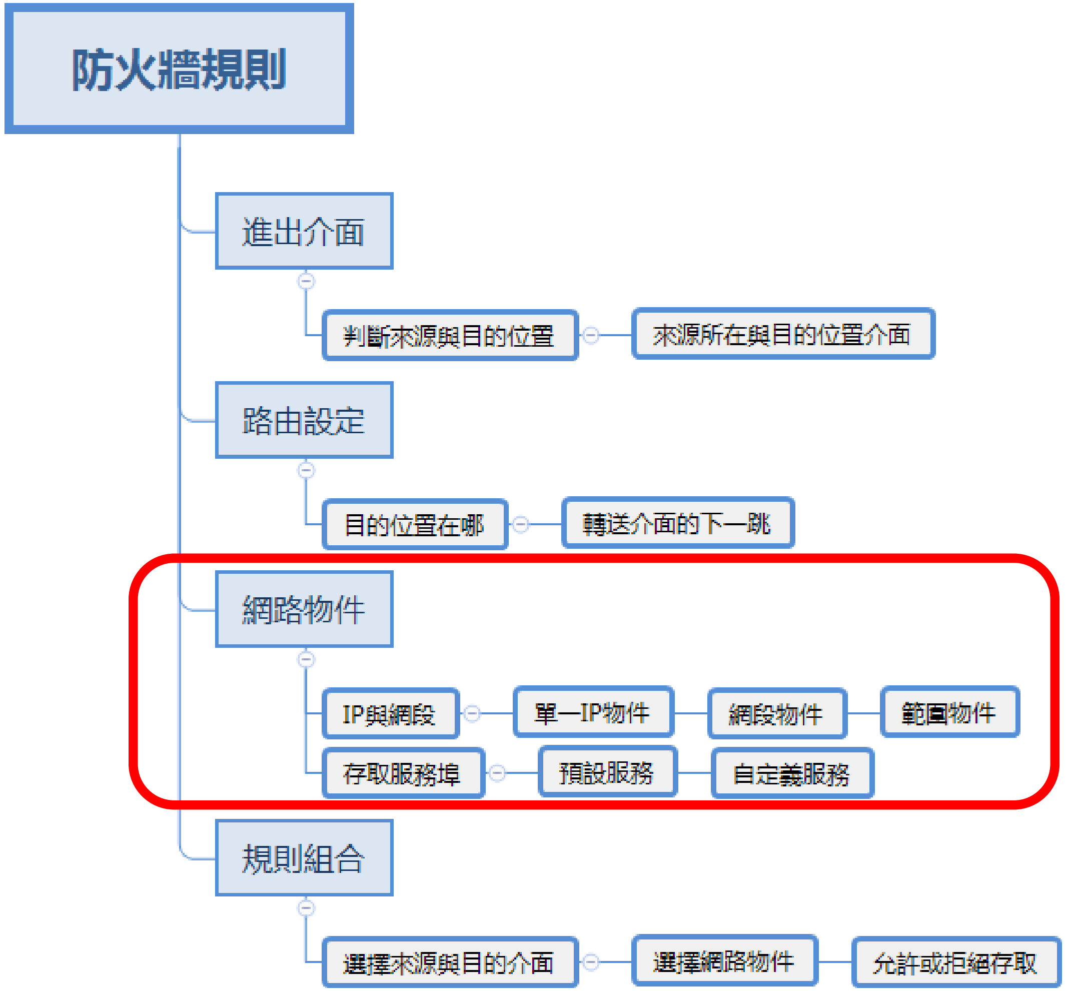


New Static Route

Destination IP/Mask	0.0.0.0/0.0.0.0	1
Device	port1	2
Gateway	0.0.0.0	3
Administrative Distance	10	
Comments		0/255

IP/Netmask	Gateway	Device	Comment
192.168.1.0 255.255.255.0	10.1.1.254	port1	

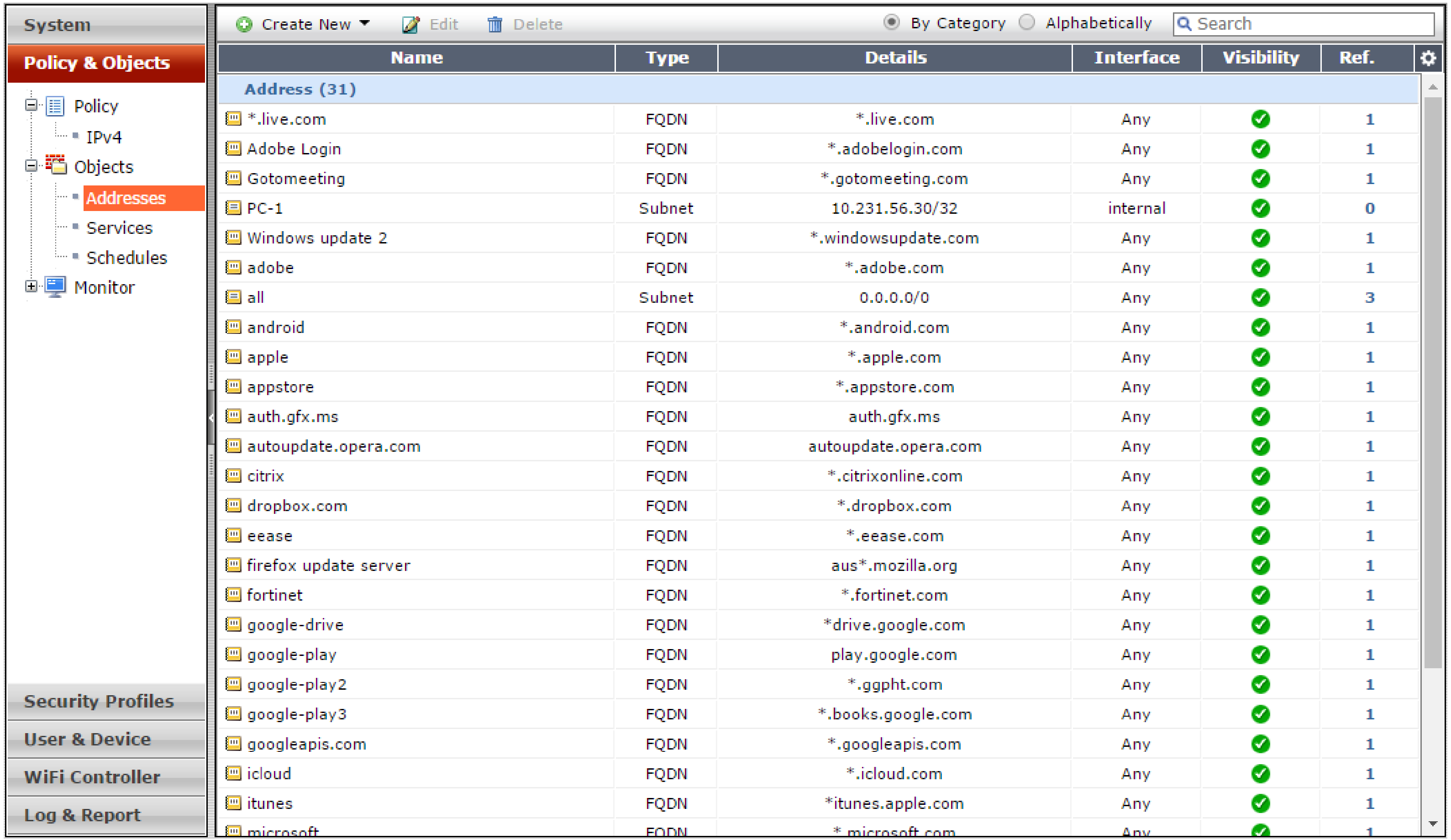
網路物件



- 防火牆規則
  - 進出介面
    - 判斷來源與目的位置 — 來源所在與目的位置介面
  - 路由設定
    - 目的位置在哪 — 轉送介面的下一跳
  - 網路物件
    - IP與網段 — 單一IP物件 — 網段物件 — 範圍物件
    - 存取服務埠 — 預設服務 — 自定義服務
  - 規則組合
    - 選擇來源與目的介面 — 選擇網路物件 — 允許或拒絕存取

IP與網段物件

- 選單路徑Policy&Objects>Objects>Address

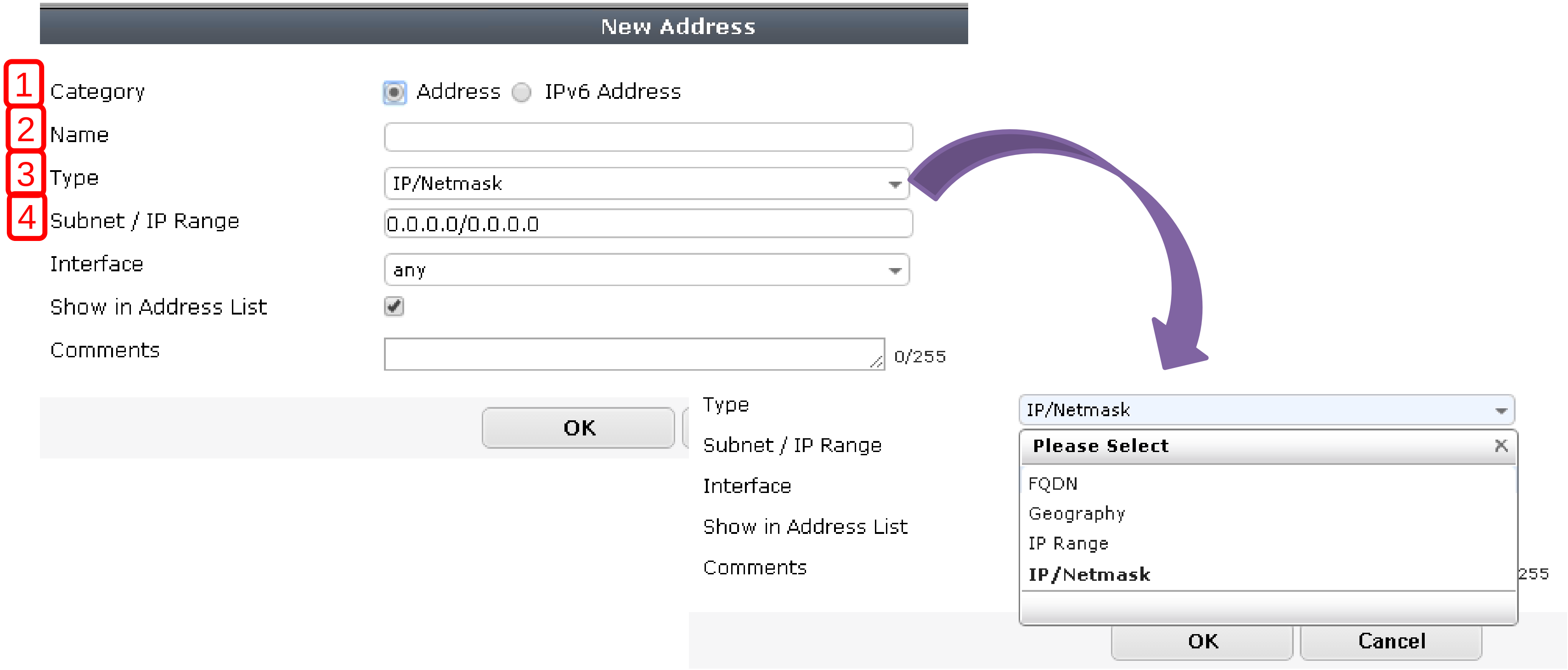


Address (31)

Name	Type	Details	Interface	Visibility	Ref.
*.live.com	FQDN	*.live.com	Any	✓	1
Adobe Login	FQDN	*.adobelogin.com	Any	✓	1
Gotomeeting	FQDN	*.gotomeeting.com	Any	✓	1
PC-1	Subnet	10.231.56.30/32	internal	✓	0
Windows update 2	FQDN	*.windowsupdate.com	Any	✓	1
adobe	FQDN	*.adobe.com	Any	✓	1
all	Subnet	0.0.0.0/0	Any	✓	3
android	FQDN	*.android.com	Any	✓	1
apple	FQDN	*.apple.com	Any	✓	1
appstore	FQDN	*.appstore.com	Any	✓	1
auth.gfx.ms	FQDN	auth.gfx.ms	Any	✓	1
autoupdate.opera.com	FQDN	autoupdate.opera.com	Any	✓	1
citrix	FQDN	*.citrixonline.com	Any	✓	1
dropbox.com	FQDN	*.dropbox.com	Any	✓	1
eease	FQDN	*.eease.com	Any	✓	1
firefox update server	FQDN	aus*.mozilla.org	Any	✓	1
fortinet	FQDN	*.fortinet.com	Any	✓	1
google-drive	FQDN	*drive.google.com	Any	✓	1
google-play	FQDN	play.google.com	Any	✓	1
google-play2	FQDN	*.ggpht.com	Any	✓	1
google-play3	FQDN	*.books.google.com	Any	✓	1
googleapis.com	FQDN	*.googleapis.com	Any	✓	1
icloud	FQDN	*.icloud.com	Any	✓	1
itunes	FQDN	*itunes.apple.com	Any	✓	1
microsoft	FQDN	*.microsoft.com	Any	✓	1

新增網路物件

- 1. IP分類
- 2. 物件名稱
- 3. 物件類型
- 4. IP網段



New Address

1 Category: ● Address ○ IPv6 Address

2 Name:

3 Type: IP/Netmask

4 Subnet / IP Range: 0.0.0.0/0.0.0.0

Interface: any

Show in Address List: ☑

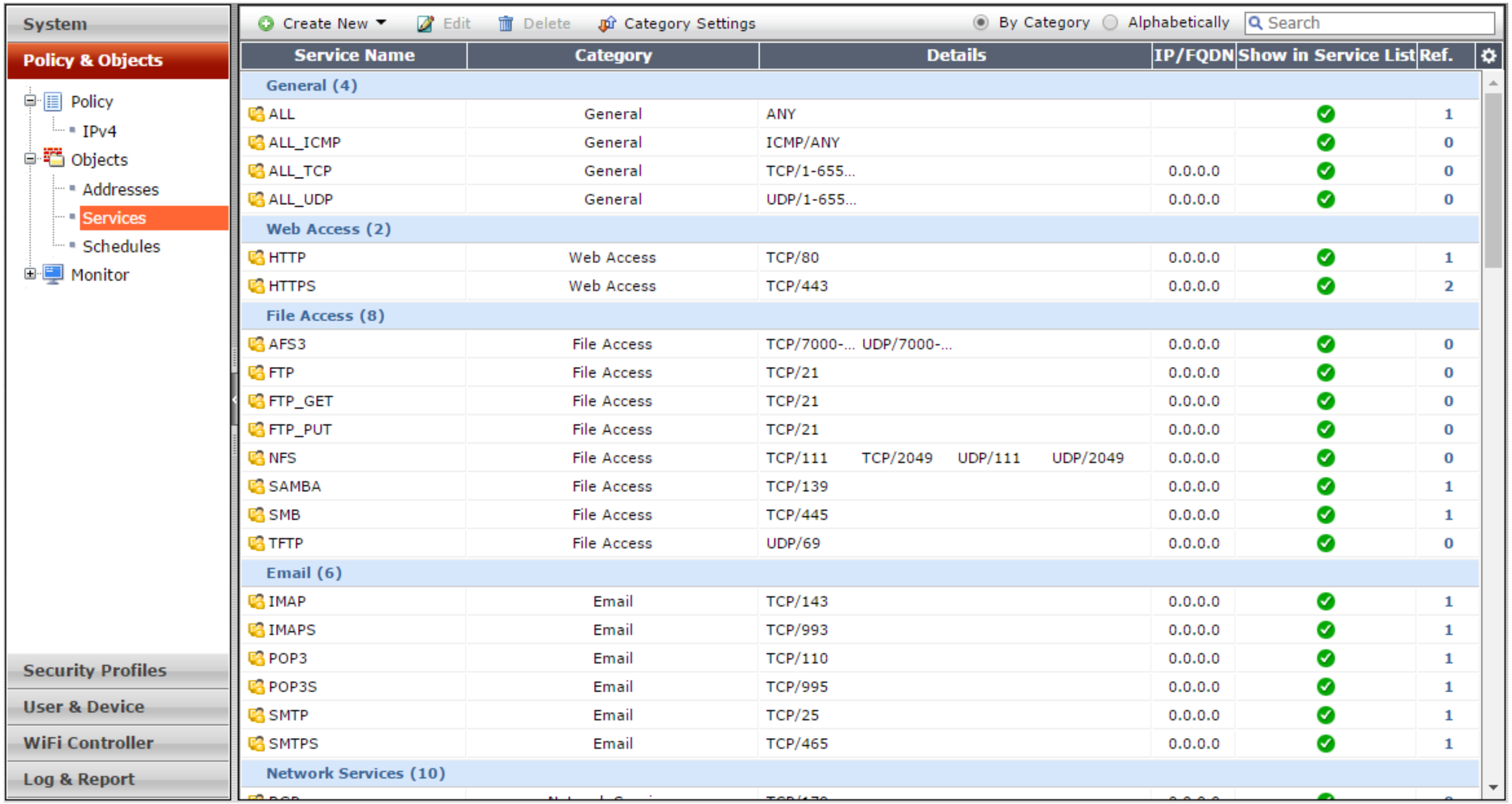
Comments: 0/255

Type: IP/Netmask

Please Select ✕
- FQDN
- Geography
- IP Range
- **IP/Netmask**

服務埠物件

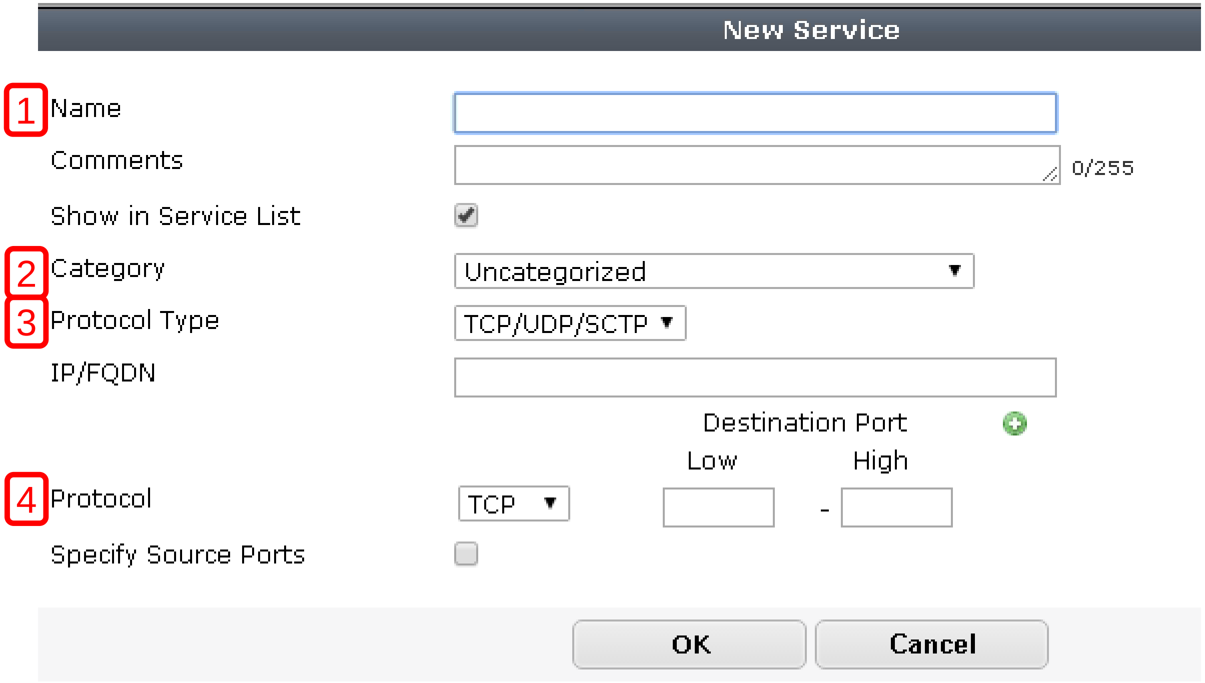
- 選單路徑Policy&Objects>Objects>Services



Service Name	Category	Details	IP/FQDN	Show in Service List	Ref.
General (4)					
ALL	General	ANY		✓	1
ALL_ICMP	General	ICMP/ANY		✓	0
ALL_TCP	General	TCP/1-655...	0.0.0.0	✓	0
ALL_UDP	General	UDP/1-655...	0.0.0.0	✓	0
Web Access (2)					
HTTP	Web Access	TCP/80	0.0.0.0	✓	1
HTTPS	Web Access	TCP/443	0.0.0.0	✓	2
File Access (8)					
AFS3	File Access	TCP/7000-... UDP/7000-...	0.0.0.0	✓	0
FTP	File Access	TCP/21	0.0.0.0	✓	0
FTP_GET	File Access	TCP/21	0.0.0.0	✓	0
FTP_PUT	File Access	TCP/21	0.0.0.0	✓	0
NFS	File Access	TCP/111 TCP/2049 UDP/111 UDP/2049	0.0.0.0	✓	0
SAMBA	File Access	TCP/139	0.0.0.0	✓	1
SMB	File Access	TCP/445	0.0.0.0	✓	1
TFTP	File Access	UDP/69	0.0.0.0	✓	0
Email (6)					
IMAP	Email	TCP/143	0.0.0.0	✓	1
IMAPS	Email	TCP/993	0.0.0.0	✓	1
POP3	Email	TCP/110	0.0.0.0	✓	1
POP3S	Email	TCP/995	0.0.0.0	✓	1
SMTP	Email	TCP/25	0.0.0.0	✓	1
SMTPS	Email	TCP/465	0.0.0.0	✓	1
Network Services (10)					

新增服務埠

- 1.服務物件名稱
- 2.服務物件分類
- 3.服務協定類型
- 4.服務埠



New Service

1 Name

Comments 0/255

Show in Service List ☑

2 Category Uncategorized ▼

3 Protocol Type TCP/UDP/SCTP ▼

IP/FQDN

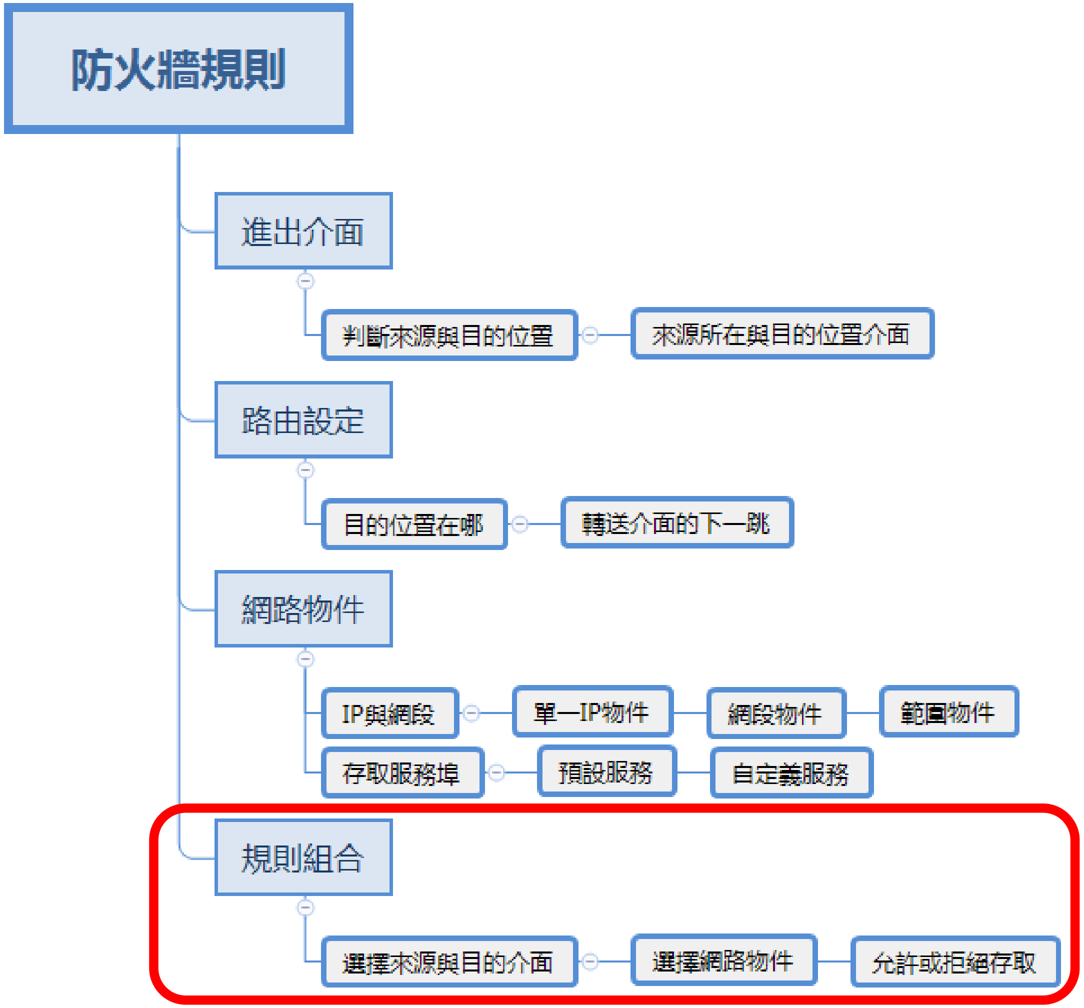
Destination Port

Low High

4 Protocol TCP ▼ -

Specify Source Ports ☐

規則組合


防火牆規則

進出介面

判斷來源與目的位置

來源所在與目的位置介面

路由設定

目的位置在哪

轉送介面的下一跳

網路物件

IP與網段

單一IP物件

網段物件

範圍物件

存取服務埠

預設服務

自定義服務

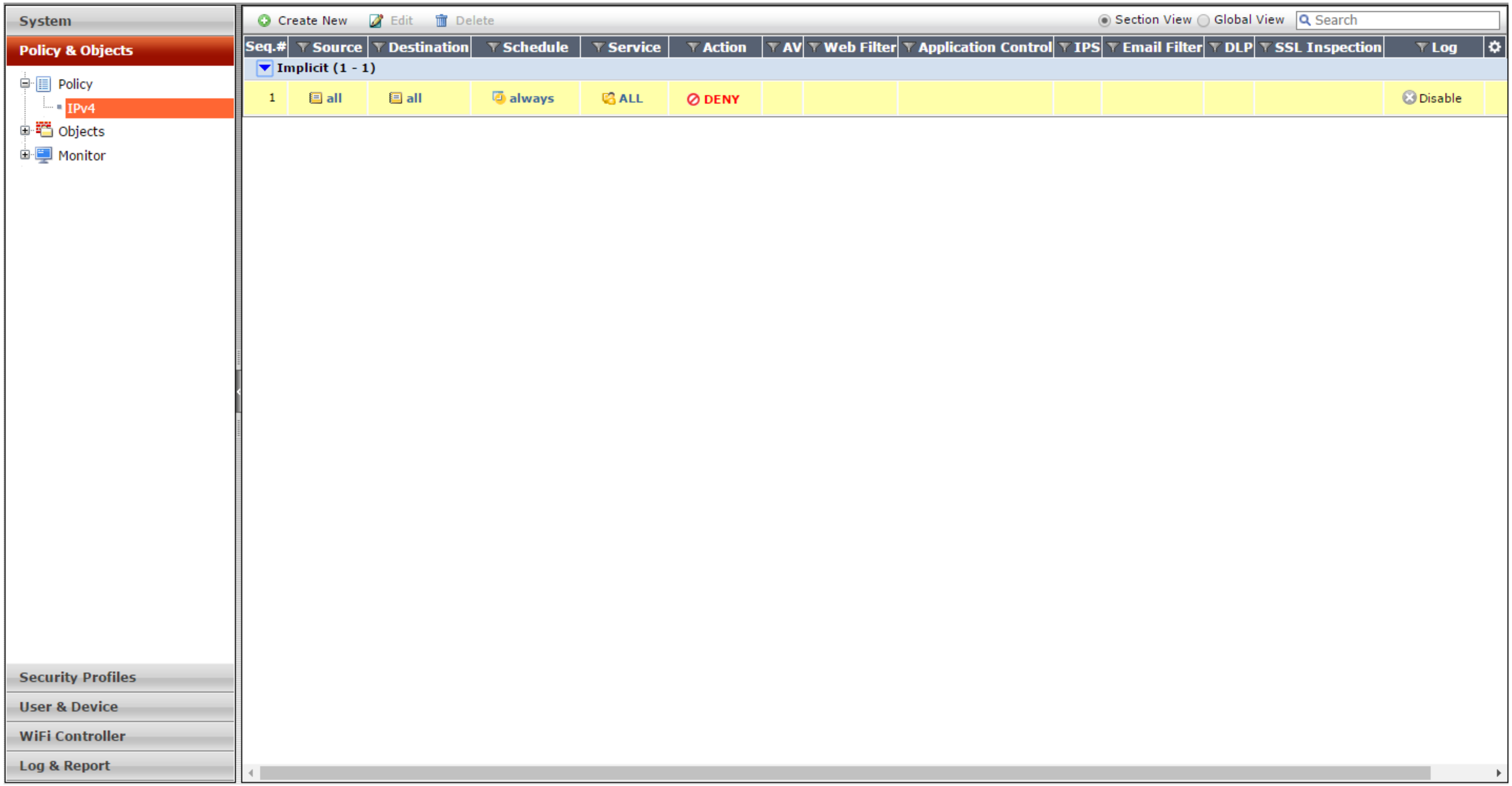
規則組合

選擇來源與目的介面

選擇網路物件

允許或拒絕存取

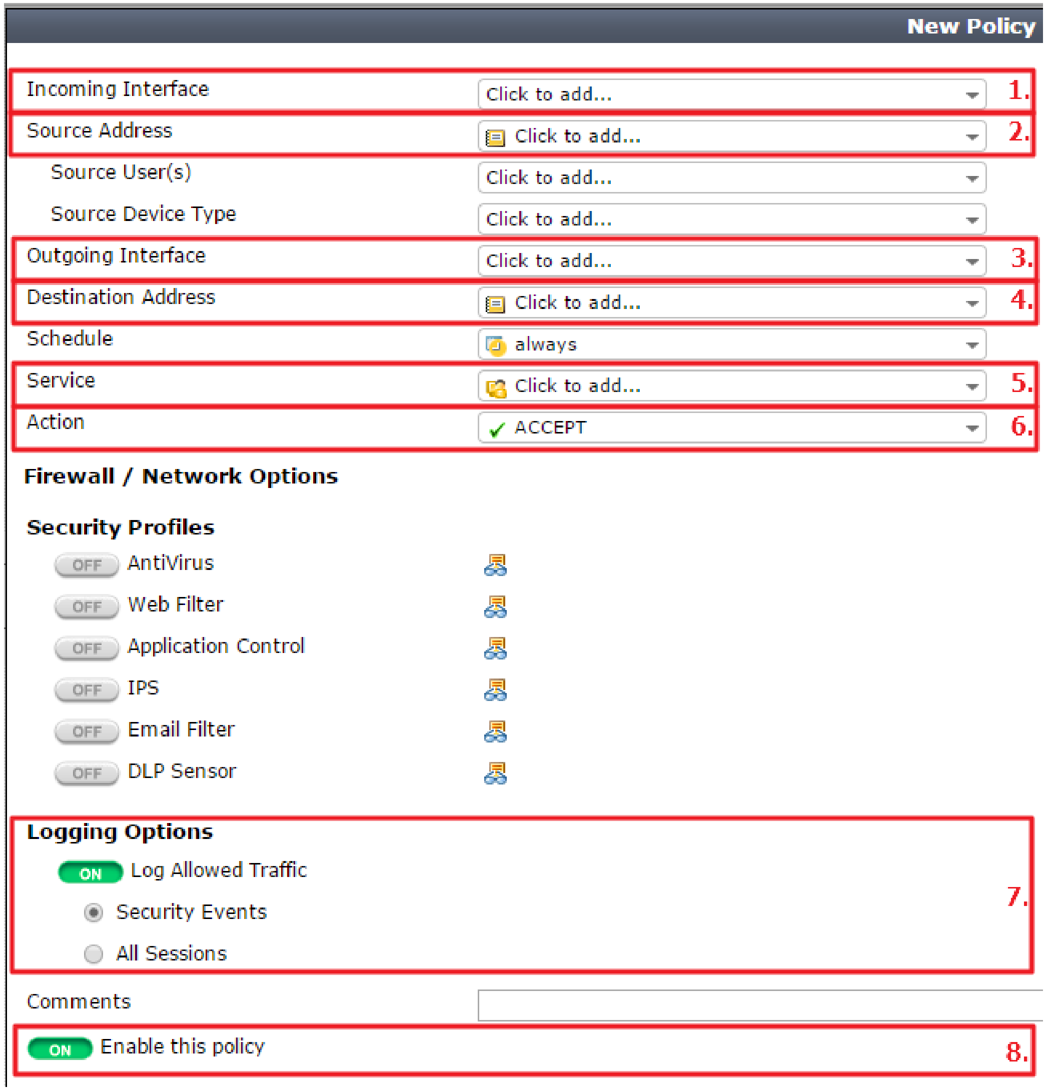
防火牆規則概觀



Seq.#	Source	Destination	Schedule	Service	Action	AV	Web Filter	Application Control	IPS	Email Filter	DLP	SSL Inspection	Log
Implicit (1 - 1)													
1	all	all	always	ALL	DENY								Disable

防火牆規則建立

- 1. 來源介面
  - 起始連線的主機所在介面。
- 2. 來源IP位址
  - 可限定來源IP位址發起連線。
- 3. 目的介面
  - 目的主機的所在介面。
- 4. 目的IP位址
  - 連線至目的IP位址。
- 5. 連線的服務類型
  - 連線至特定服務。
- 6. 採取的行動
  - 允許或是阻擋連線行為。
- 7. Syslog紀錄
  - 紀錄連線資訊或紀錄事件。
- 8. 規則開啟或關閉。



New Policy

Incoming Interface	Click to add...	1.
Source Address	Click to add...	2.
Source User(s)	Click to add...	
Source Device Type	Click to add...	
Outgoing Interface	Click to add...	3.
Destination Address	Click to add...	4.
Schedule	always	
Service	Click to add...	5.
Action	✓ ACCEPT	6.

Firewall / Network Options

Security Profiles

- OFF AntiVirus
- OFF Web Filter
- OFF Application Control
- OFF IPS
- OFF Email Filter
- OFF DLP Sensor

Logging Options 7.

- ON Log Allowed Traffic
  - ● Security Events
  - ○ All Sessions

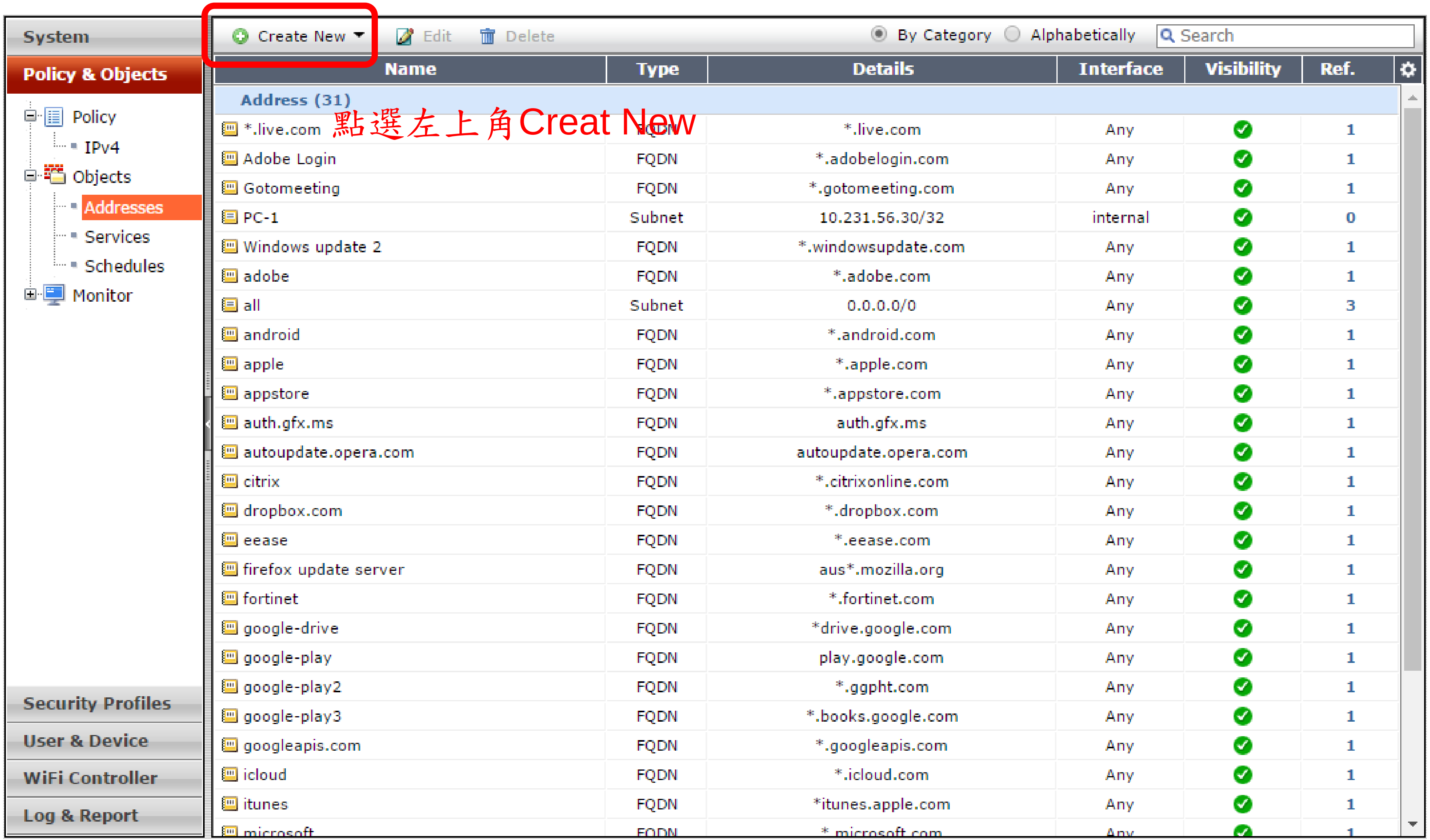
Comments

ON Enable this policy 8.

實機操作-防火牆規則建立

- 1.新增IP物件
- 2.新增防火牆規則
  - 允許對外存取
  - 阻擋網頁存取
- 3.調整防火牆規則順序
- 4.開啟與關閉防火牆規則

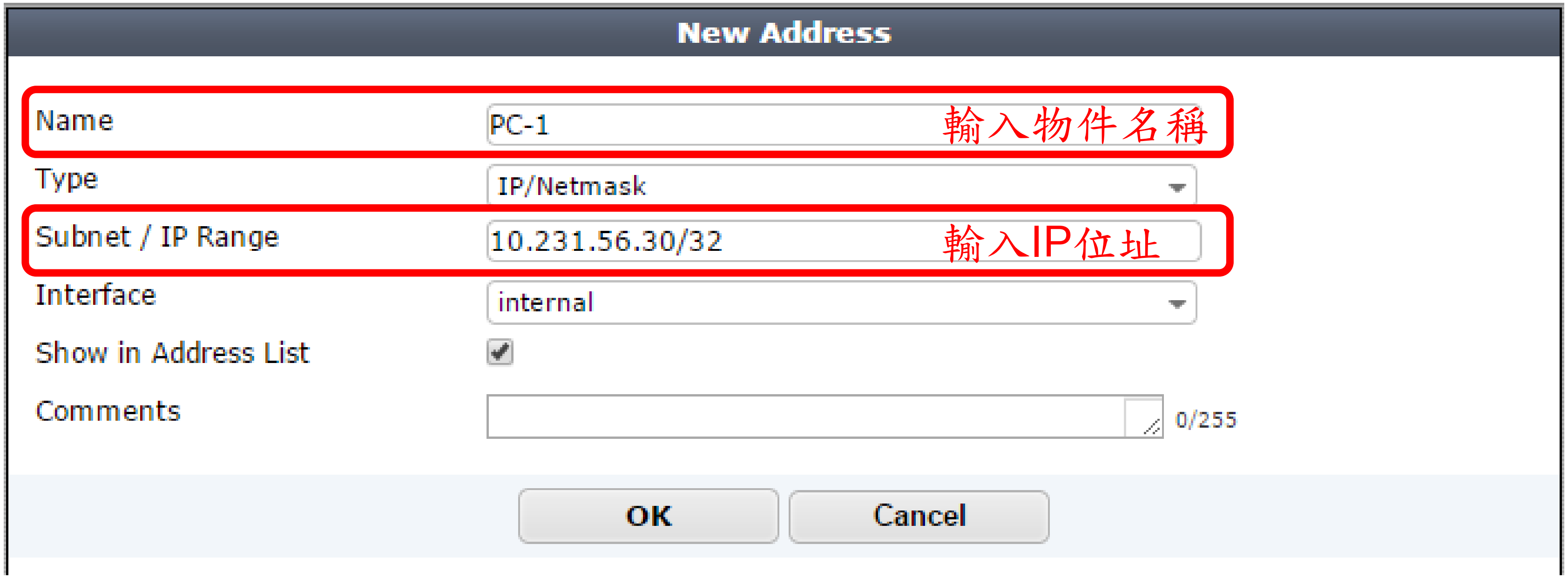
實機操作-新增IP物件



點選左上角Creat New

Name	Type	Details	Interface	Visibility	Ref.
Address (31)					
*.live.com	FQDN	*.live.com	Any	✓	1
Adobe Login	FQDN	*.adobelogin.com	Any	✓	1
Gotomeeting	FQDN	*.gotomeeting.com	Any	✓	1
PC-1	Subnet	10.231.56.30/32	internal	✓	0
Windows update 2	FQDN	*.windowsupdate.com	Any	✓	1
adobe	FQDN	*.adobe.com	Any	✓	1
all	Subnet	0.0.0.0/0	Any	✓	3
android	FQDN	*.android.com	Any	✓	1
apple	FQDN	*.apple.com	Any	✓	1
appstore	FQDN	*.appstore.com	Any	✓	1
auth.gfx.ms	FQDN	auth.gfx.ms	Any	✓	1
autoupdate.opera.com	FQDN	autoupdate.opera.com	Any	✓	1
citrix	FQDN	*.citrixonline.com	Any	✓	1
dropbox.com	FQDN	*.dropbox.com	Any	✓	1
eease	FQDN	*.eease.com	Any	✓	1
firefox update server	FQDN	aus*.mozilla.org	Any	✓	1
fortinet	FQDN	*.fortinet.com	Any	✓	1
google-drive	FQDN	*drive.google.com	Any	✓	1
google-play	FQDN	play.google.com	Any	✓	1
google-play2	FQDN	*.ggpht.com	Any	✓	1
google-play3	FQDN	*.books.google.com	Any	✓	1
googleapis.com	FQDN	*.googleapis.com	Any	✓	1
icloud	FQDN	*.icloud.com	Any	✓	1
itunes	FQDN	*itunes.apple.com	Any	✓	1
microsoft	FQDN	*.microsoft.com	Any	✓	1

實機操作-新增IP物件



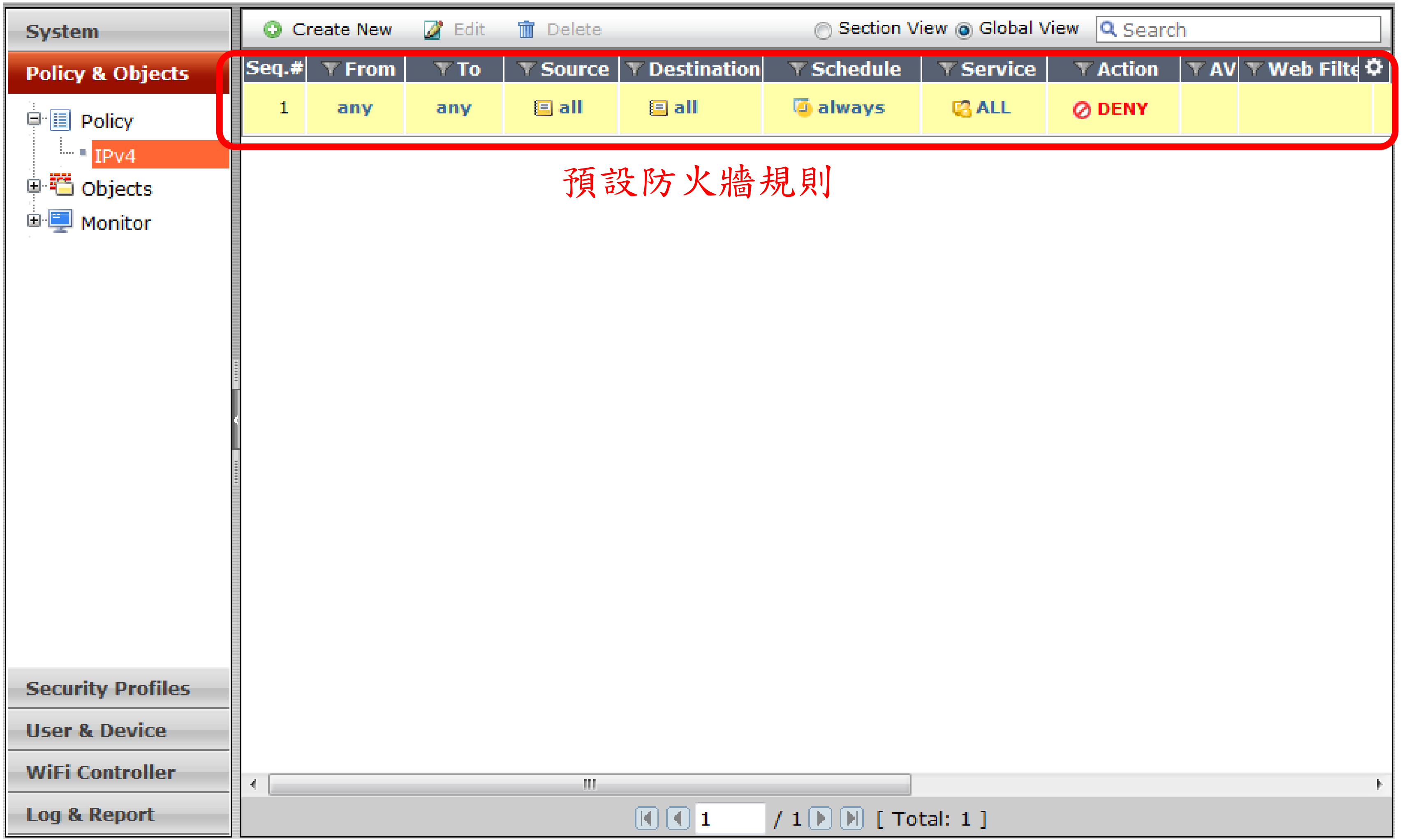
New Address

Name	PC-1
Type	IP/Netmask
Subnet / IP Range	10.231.56.30/32
Interface	internal
Show in Address List	☑
Comments	0/255

輸入物件名稱

輸入IP位址

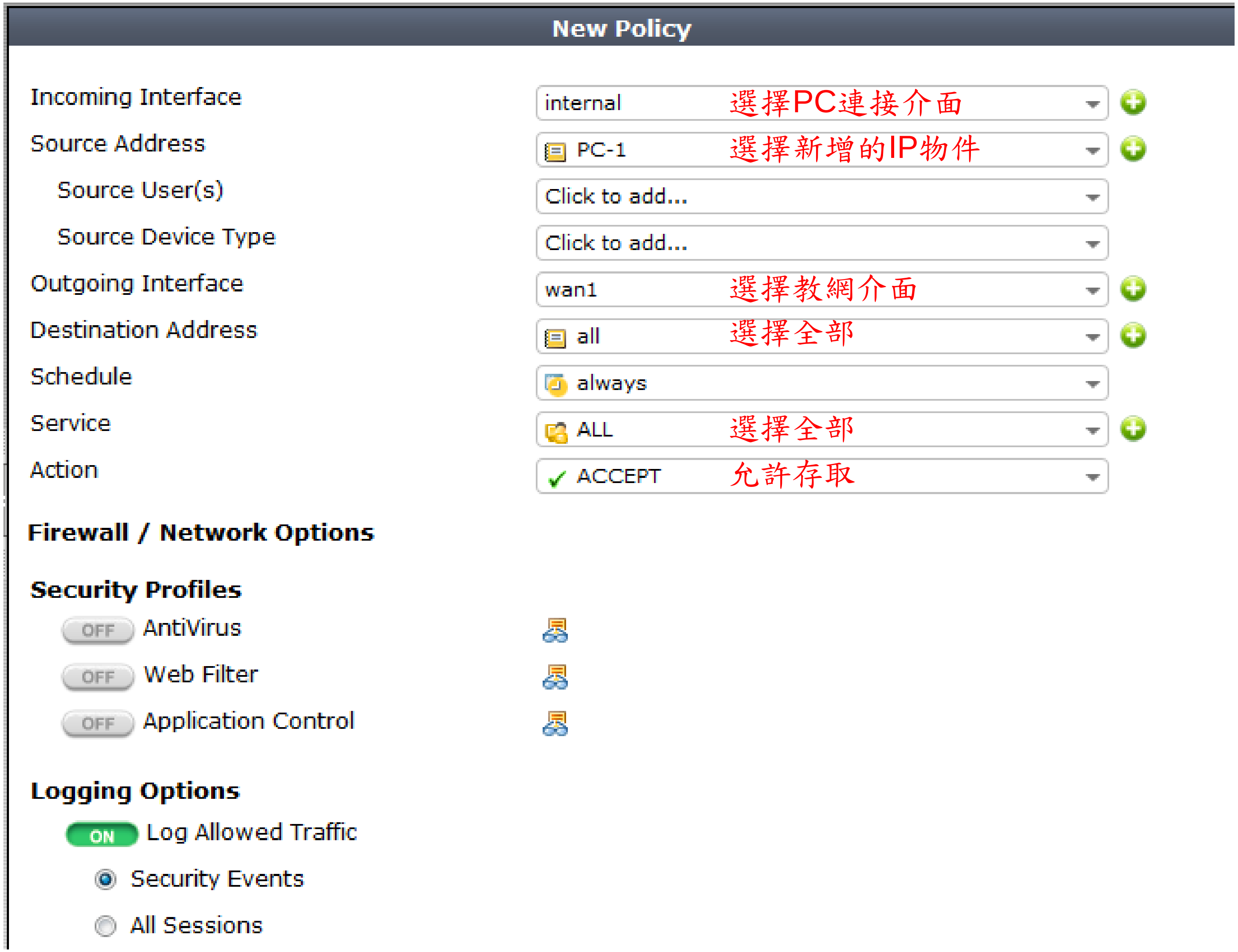
實機操作-規則新增



Seq.#	From	To	Source	Destination	Schedule	Service	Action	AV	Web Filte
1	any	any	all	all	always	ALL	⊘ DENY		

預設防火牆規則

實機操作-規則新增



New Policy

Incoming Interface: internal 選擇PC連接介面

Source Address: PC-1 選擇新增的IP物件

Source User(s): Click to add...

Source Device Type: Click to add...

Outgoing Interface: wan1 選擇教網介面

Destination Address: all 選擇全部

Schedule: always

Service: ALL 選擇全部

Action: ✓ ACCEPT 允許存取

Firewall / Network Options

Security Profiles

OFF AntiVirus

OFF Web Filter

OFF Application Control

Logging Options

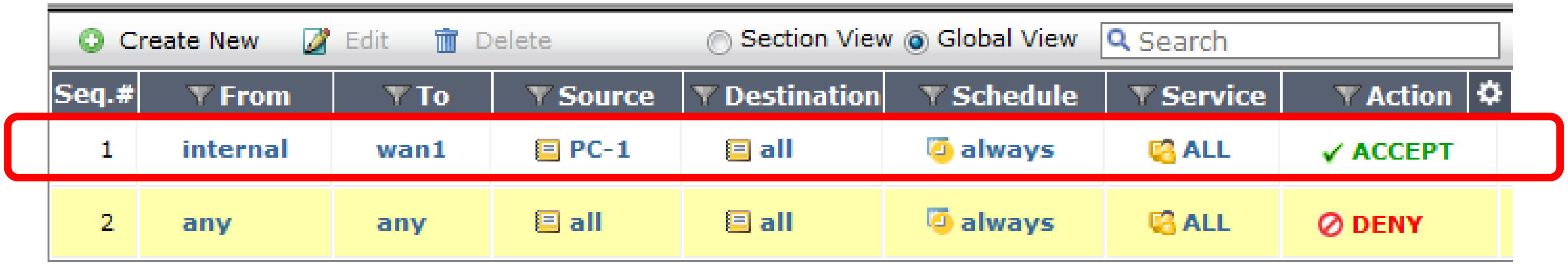
ON Log Allowed Traffic

● Security Events

○ All Sessions

實機操作-規則新增

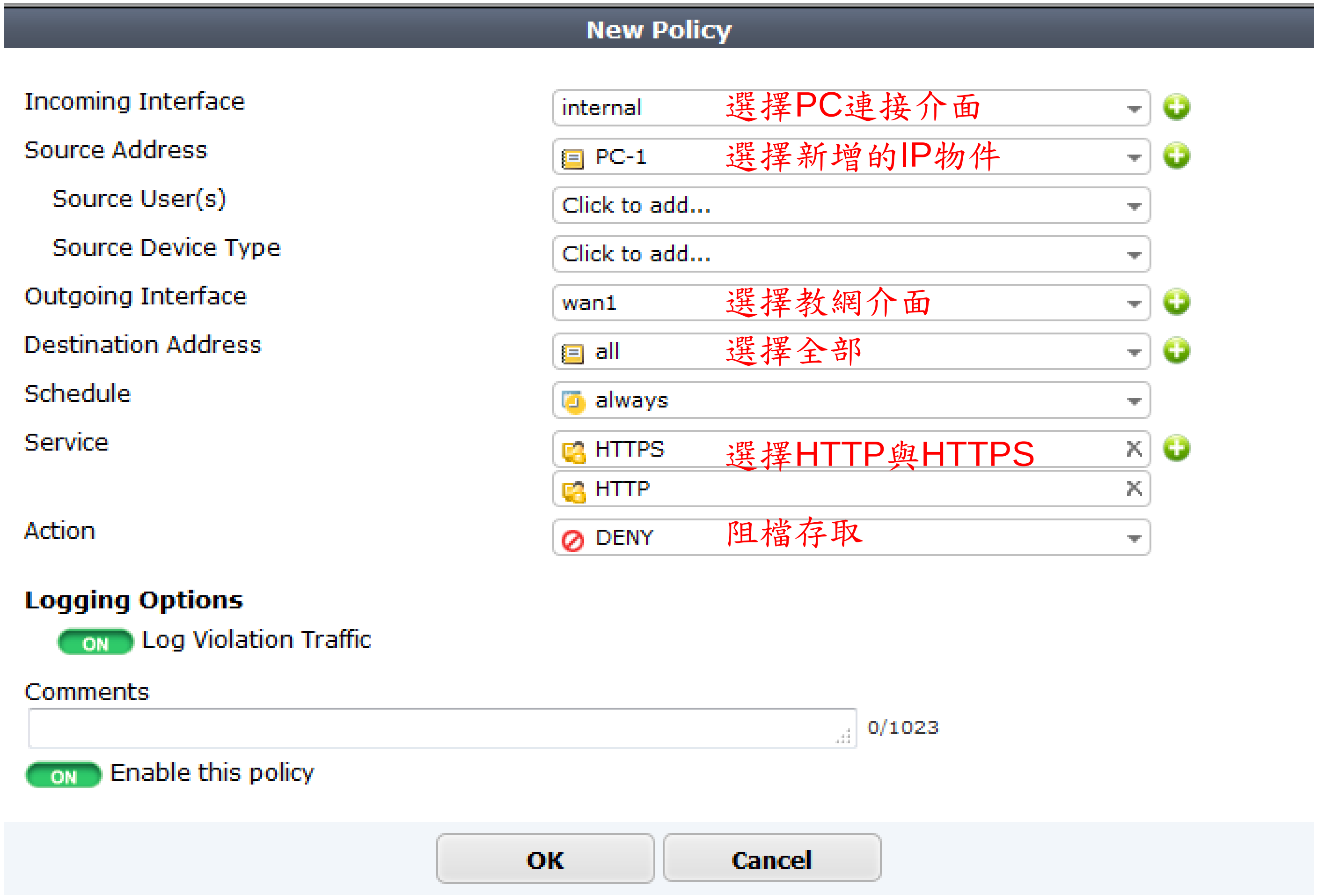
完成第一筆規則新增



Seq.#	From	To	Source	Destination	Schedule	Service	Action
1	internal	wan1	PC-1	all	always	ALL	✓ ACCEPT
2	any	any	all	all	always	ALL	⊘ DENY

請測試PC是否可以上網

實機操作-規則新增



New Policy

Incoming Interface: internal 選擇PC連接介面

Source Address: PC-1 選擇新增的IP物件

Source User(s): Click to add...

Source Device Type: Click to add...

Outgoing Interface: wan1 選擇教網介面

Destination Address: all 選擇全部

Schedule: always

Service: HTTPS 選擇HTTP與HTTPS
HTTP

Action: DENY 阻檔存取

Logging Options

ON Log Violation Traffic

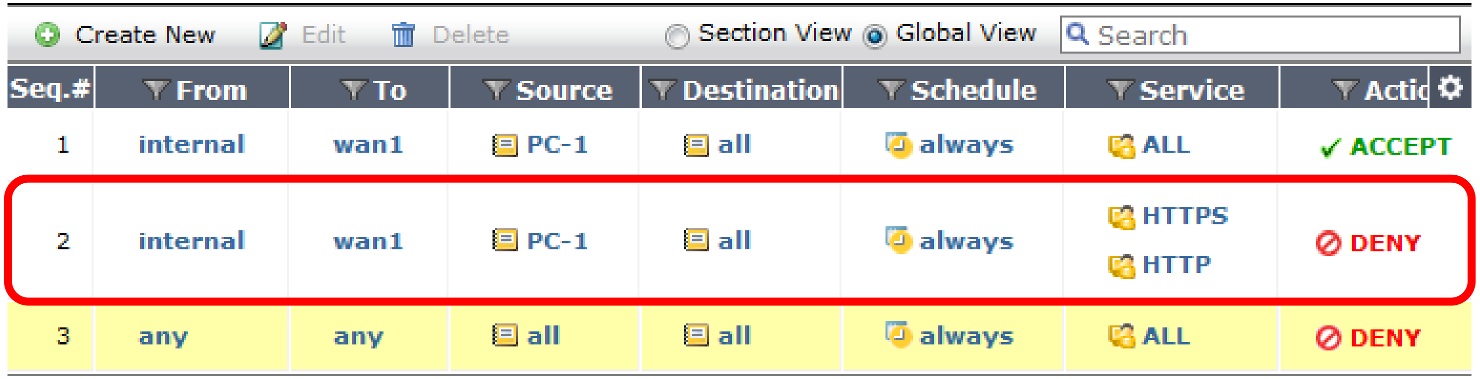
Comments

0/1023

ON Enable this policy

實機操作-規則新增

完成第二筆規則新增

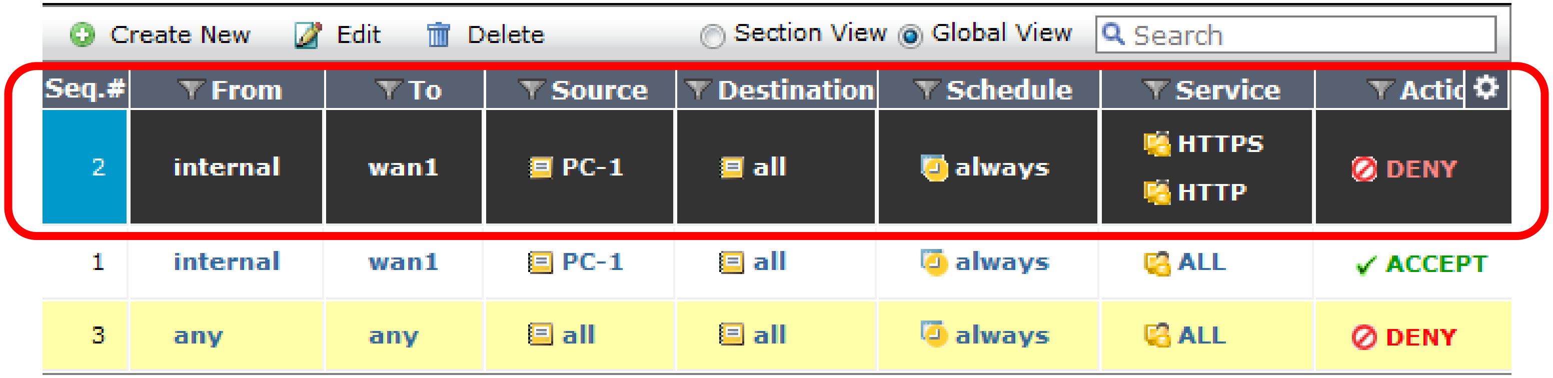


Seq.#	From	To	Source	Destination	Schedule	Service	Actic
1	internal	wan1	PC-1	all	always	ALL	✓ ACCEPT
2	internal	wan1	PC-1	all	always	HTTPS HTTP	⊘ DENY
3	any	any	all	all	always	ALL	⊘ DENY

請測試PC是否可以上網

實機操作-規則順序調整

將第二筆規則拖拉至第一筆上方

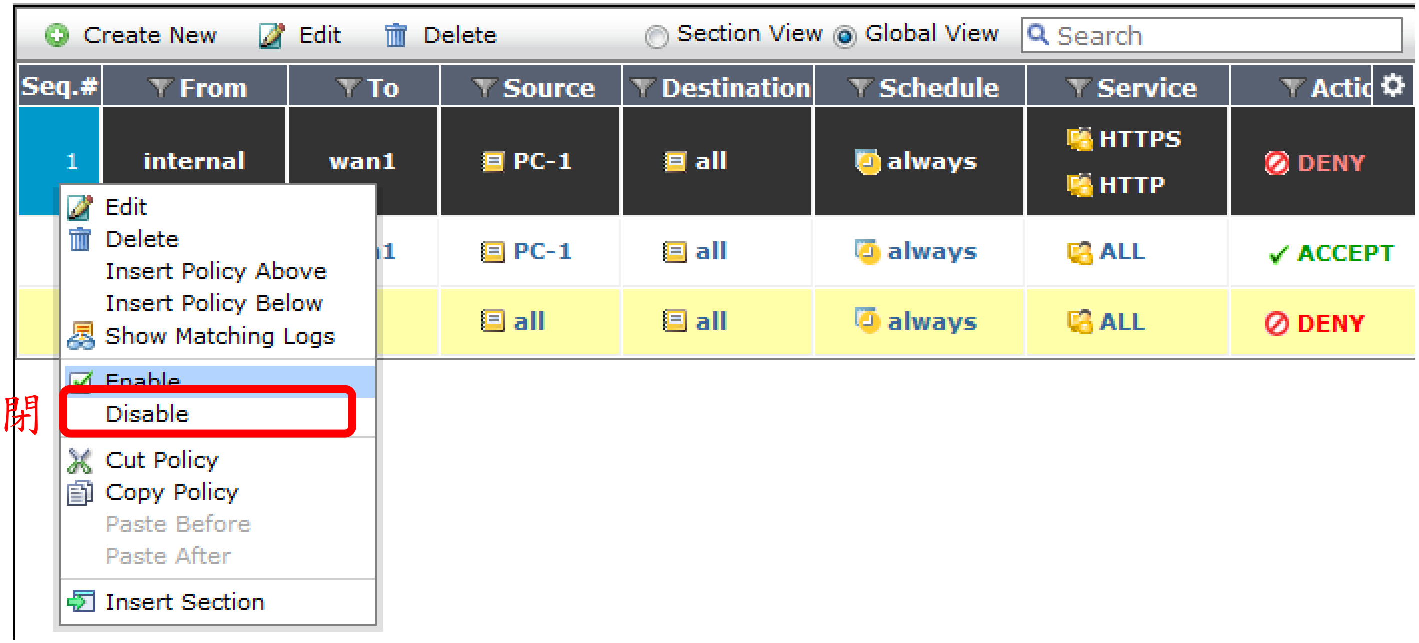


Seq.#	From	To	Source	Destination	Schedule	Service	Actic
2	internal	wan1	PC-1	all	always	HTTPS HTTP	DENY
1	internal	wan1	PC-1	all	always	ALL	✓ ACCEPT
3	any	any	all	all	always	ALL	DENY

請測試PC是否可以上網

實機操作-啟用或關閉規則

右鍵點選規則

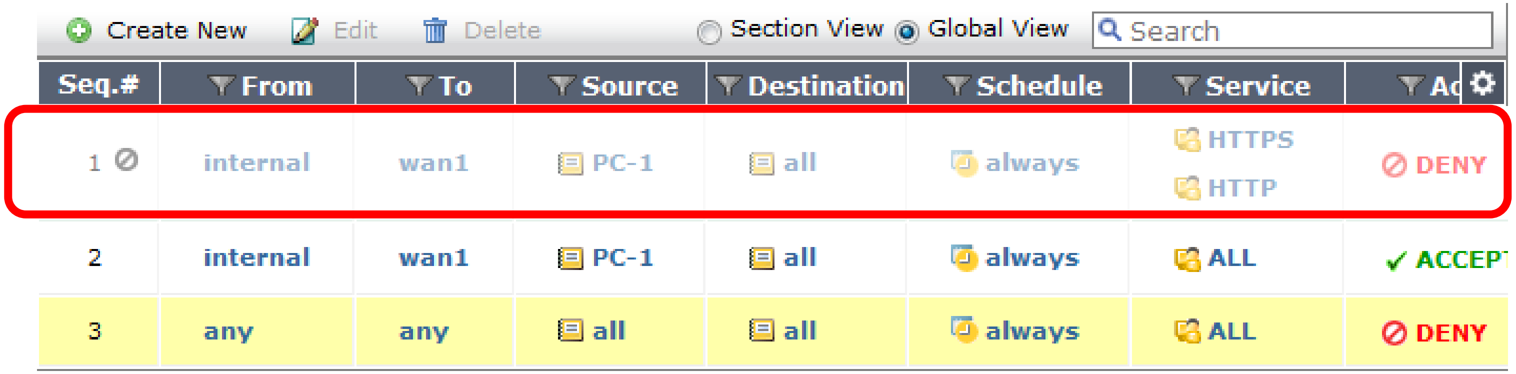


Seq.#	From	To	Source	Destination	Schedule	Service	Actic
1	internal	wan1	PC-1	all	always	HTTPS HTTP	DENY
		1	PC-1	all	always	ALL	✓ ACCEPT
			all	all	always	ALL	DENY

選擇關閉

實機操作-啟用或關閉規則

防火牆規則關閉



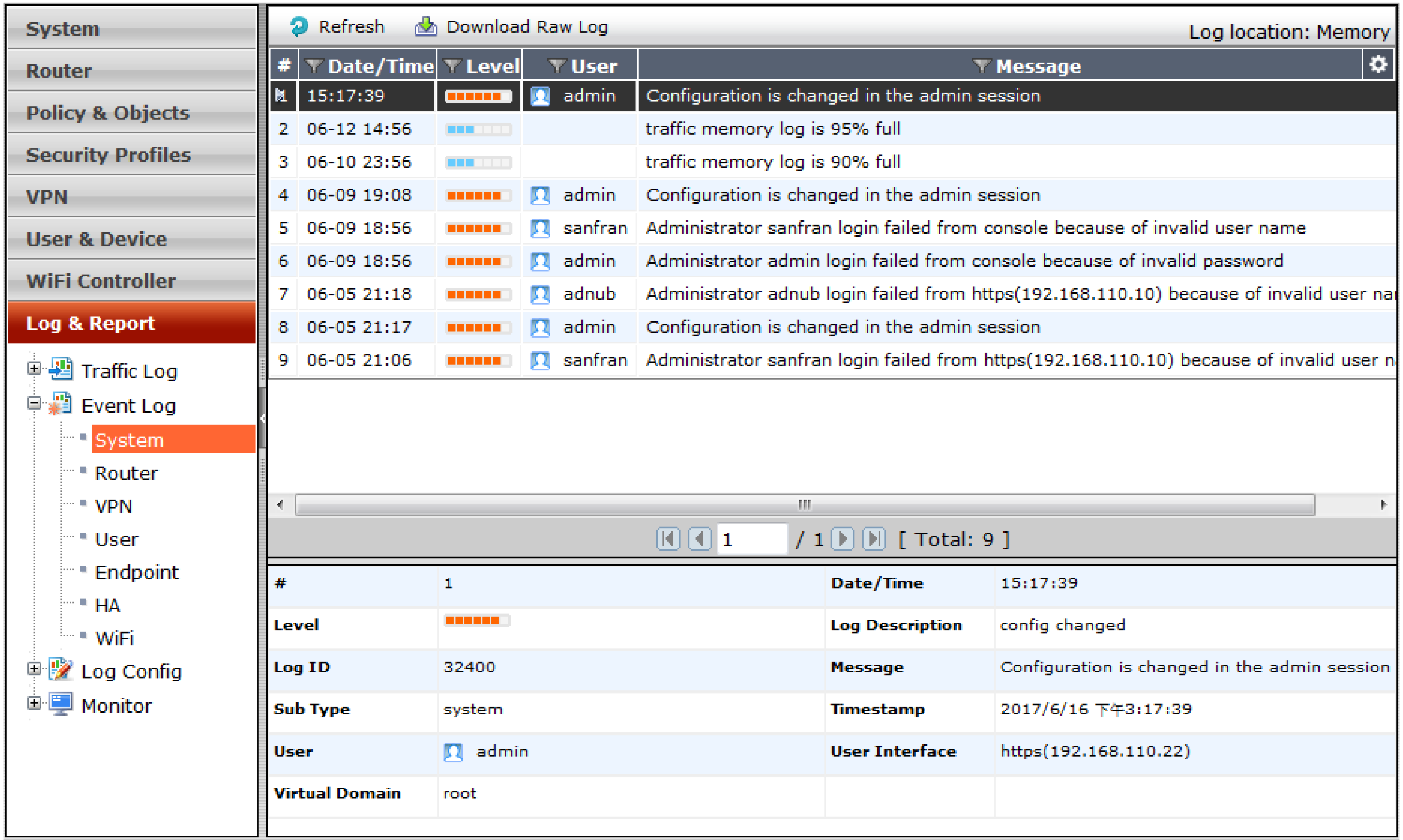
Create New Edit Delete ○ Section View ● Global View Search

Seq.#	From	To	Source	Destination	Schedule	Service	Ac
1 ⊘	internal	wan1	PC-1	all	always	HTTPS HTTP	⊘ DENY
2	internal	wan1	PC-1	all	always	ALL	✓ ACCEPT
3	any	any	all	all	always	ALL	⊘ DENY

系統訊息查閱

事件紀錄

- 選單路徑Log&Report>EventLog>System



System
Router
Policy & Objects
Security Profiles
VPN
User & Device
WiFi Controller
Log & Report
- Traffic Log
- Event Log
  - System
  - Router
  - VPN
  - User
  - Endpoint
  - HA
  - WiFi
- Log Config
- Monitor

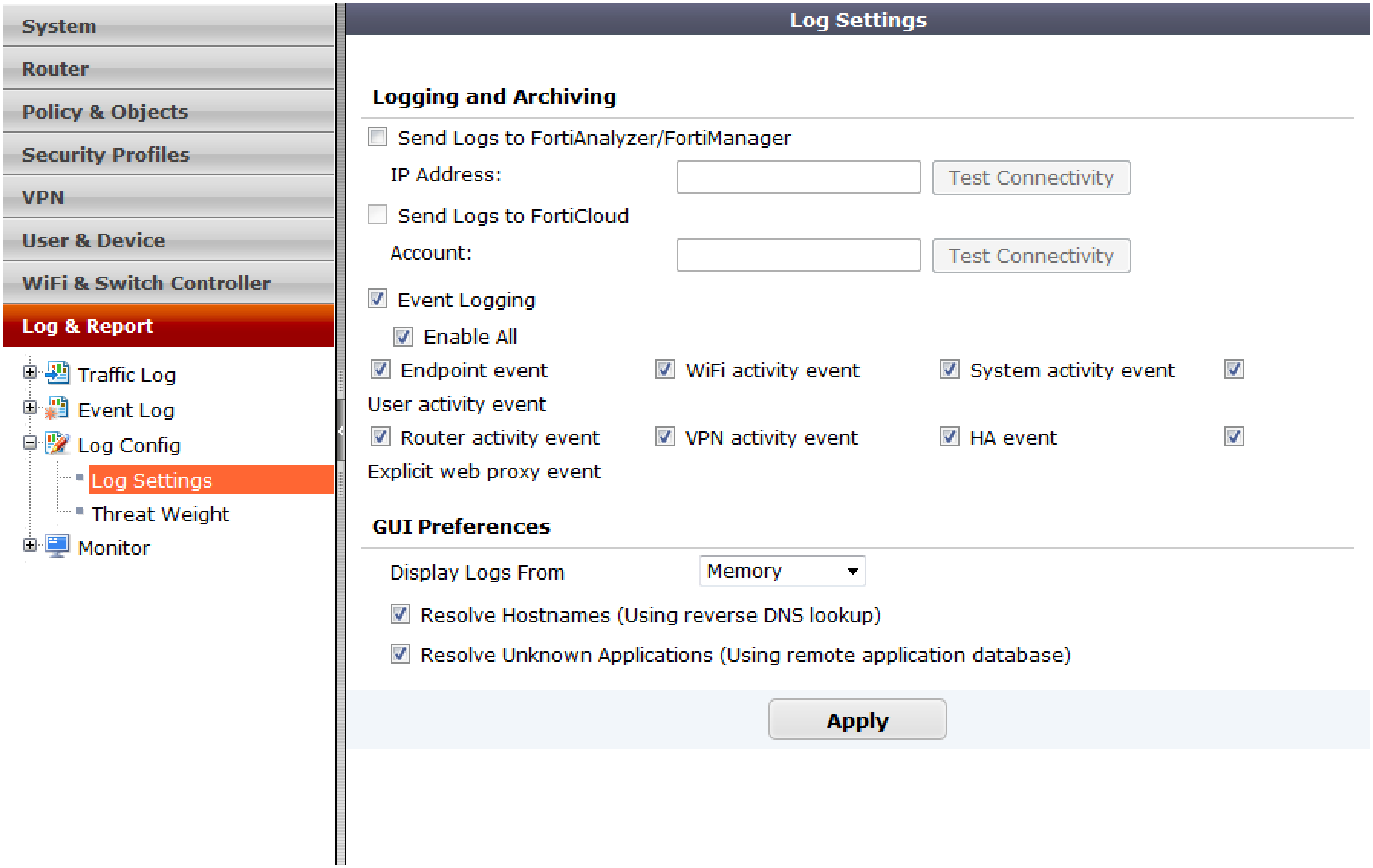
Refresh Download Raw Log Log location: Memory

#	Date/Time	Level	User	Message
1	15:17:39	🟧	admin	Configuration is changed in the admin session
2	06-12 14:56	🟦		traffic memory log is 95% full
3	06-10 23:56	🟦		traffic memory log is 90% full
4	06-09 19:08	🟧	admin	Configuration is changed in the admin session
5	06-09 18:56	🟧	sanfran	Administrator sanfran login failed from console because of invalid user name
6	06-09 18:56	🟧	admin	Administrator admin login failed from console because of invalid password
7	06-05 21:18	🟧	adnub	Administrator adnub login failed from https(192.168.110.10) because of invalid user na
8	06-05 21:17	🟧	admin	Configuration is changed in the admin session
9	06-05 21:06	🟧	sanfran	Administrator sanfran login failed from https(192.168.110.10) because of invalid user n

1 / 1 [Total: 9]

#	1	Date/Time	15:17:39
Level	🟧	Log Description	config changed
Log ID	32400	Message	Configuration is changed in the admin session
Sub Type	system	Timestamp	2017/6/16 下午3:17:39
User	admin	User Interface	https(192.168.110.22)
Virtual Domain	root		

訊息設定



Log Settings

Logging and Archiving

□ Send Logs to FortiAnalyzer/FortiManager

IP Address: [ ] Test Connectivity

□ Send Logs to FortiCloud

Account: [ ] Test Connectivity

☑ Event Logging

☑ Enable All

☑ Endpoint event ☑ WiFi activity event ☑ System activity event ☑
User activity event
☑ Router activity event ☑ VPN activity event ☑ HA event ☑
Explicit web proxy event

GUI Preferences

Display Logs From: Memory

☑ Resolve Hostnames (Using reverse DNS lookup)

☑ Resolve Unknown Applications (Using remote application database)

Apply

無線AP運作介紹

無線網路種類

- 常見的無線數據網路有：
  - 無線區域網路（Wi-Fi）
  - 無線個人網路（紅外線、藍芽）
  - 無線都會網路（全球互通微波存取WiMAX）
  - 無線射頻通訊（RFID、NFC）
  - 衛星網路

WiFi

- Wi-Fi 的標準：
  - IEEE 802.11
  - IEEE 802.11b
  - IEEE 802.11a
  - IEEE 802.11g
  - IEEE 802.11n

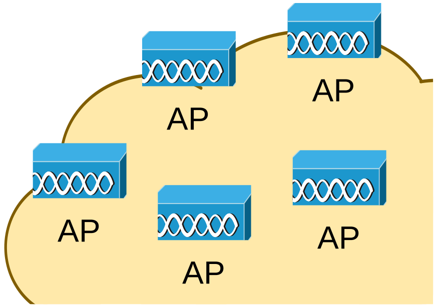
無線佈署方式

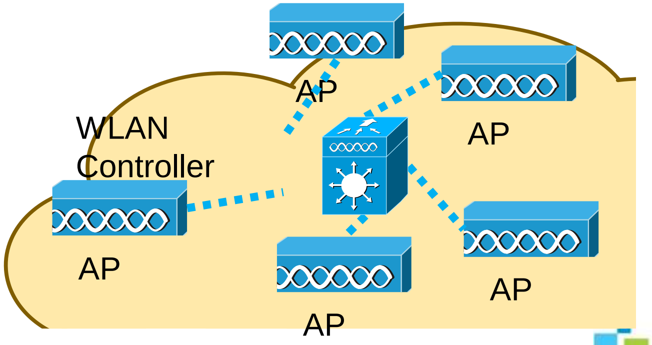
分散式架構(FAT AP)

- 符合業界標準
  - *802.11 a/b/g/n for connectivity*
  - *WPA2 for stronger security*
- 業界最佳效能
- 投資保障

集中式架構(Thin AP)

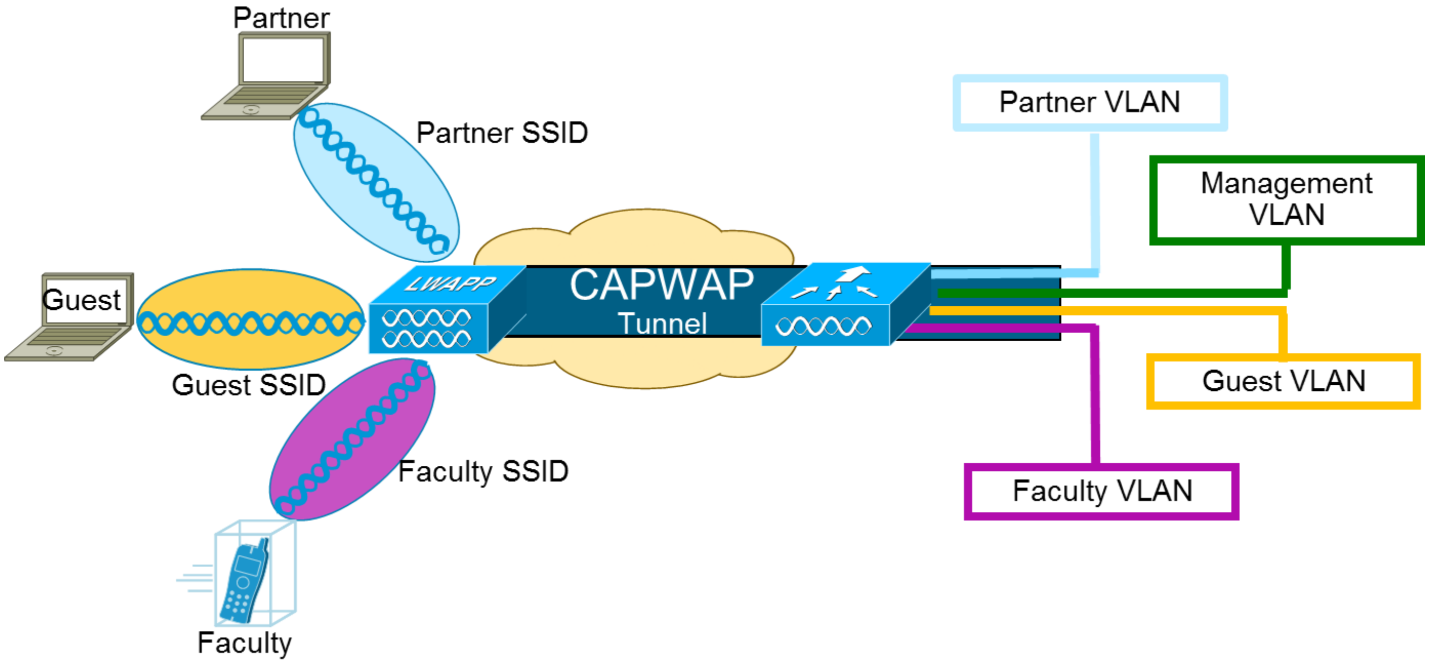
- 集中管理
- 動態無線資源管理
- 進階的網路安全
  - *安全的訪客網路*
  - *無線入侵防禦偵測*
- Mobility移動服務
  - *Wi-Fi無線語音服務*
  - *定位服務*



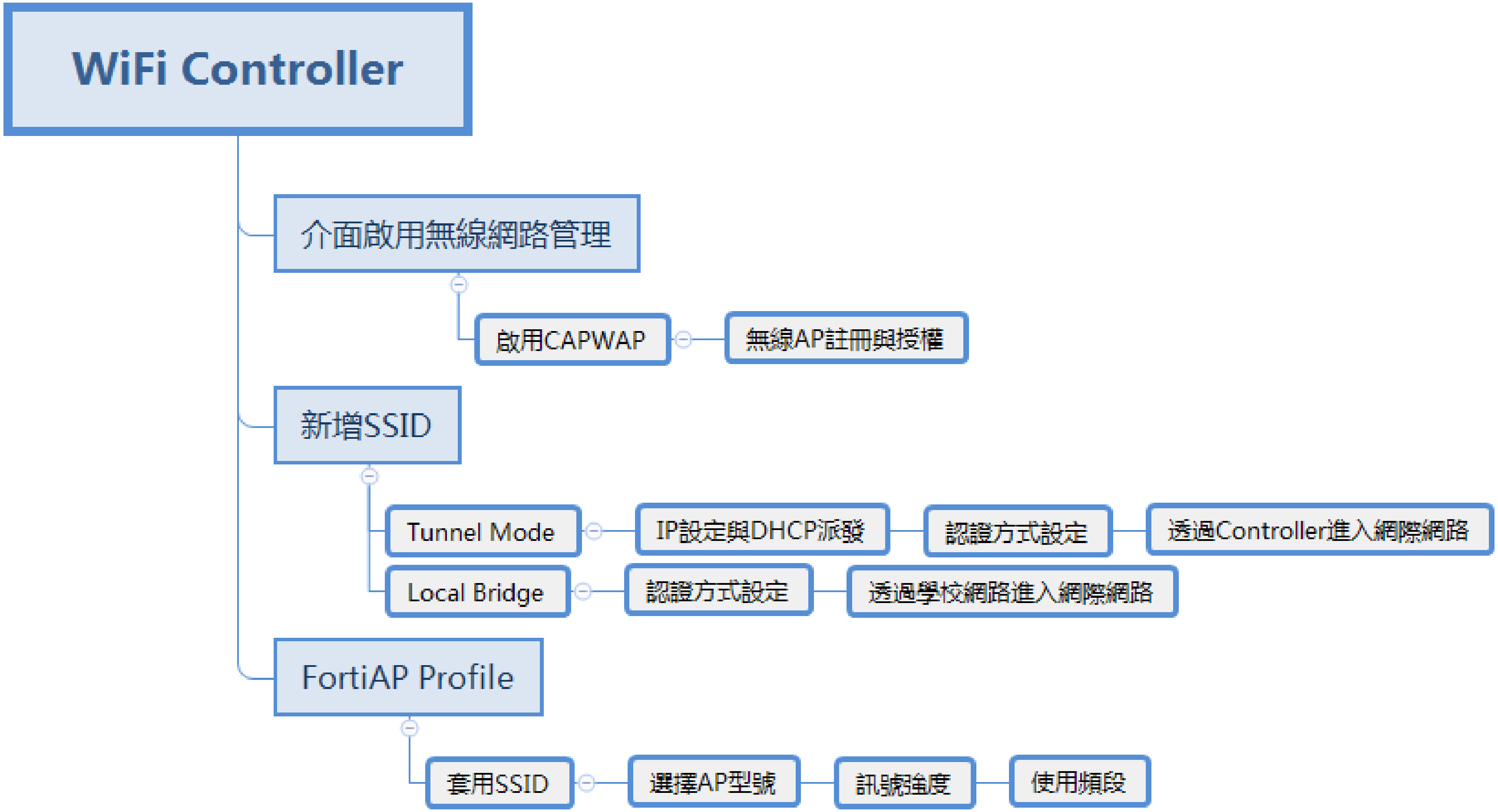


集中式無線網路架構圖

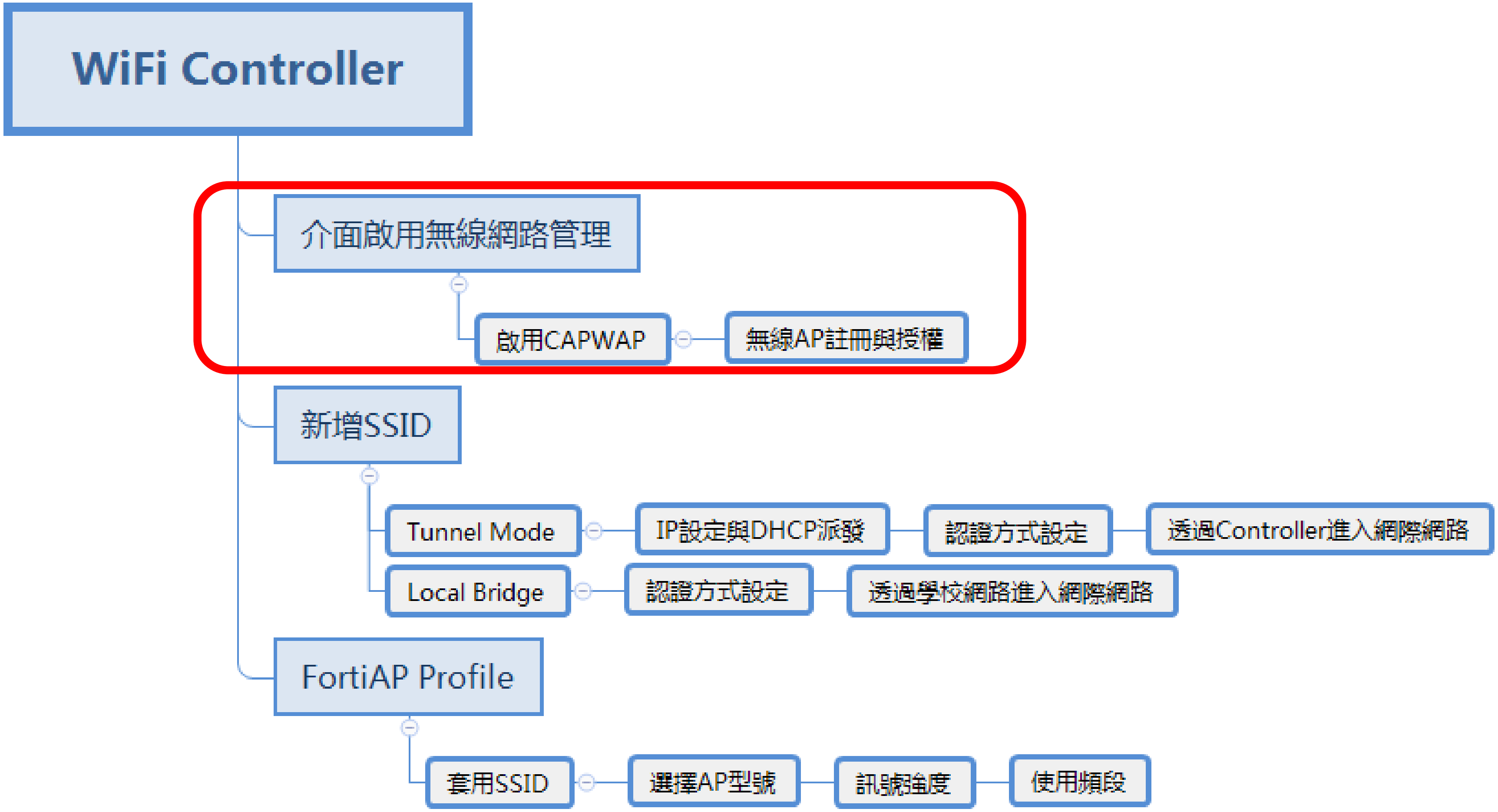
- **CAPWAP**
  - **Control And Provisioning of Wireless Access Points Protocol Specification**



無線網路設定


WiFi Controller
介面啟用無線網路管理
啟用CAPWAP
無線AP註冊與授權
新增SSID
Tunnel Mode
IP設定與DHCP派發
認證方式設定
透過Controller進入網際網路
Local Bridge
認證方式設定
透過學校網路進入網際網路
FortiAP Profile
套用SSID
選擇AP型號
訊號強度
使用頻段

啟動AP管理



WiFi Controller

介面啟用無線網路管理

啟用CAPWAP

無線AP註冊與授權

新增SSID

Tunnel Mode

IP設定與DHCP派發

認證方式設定

透過Controller進入網際網路

Local Bridge

認證方式設定

透過學校網路進入網際網路

FortiAP Profile

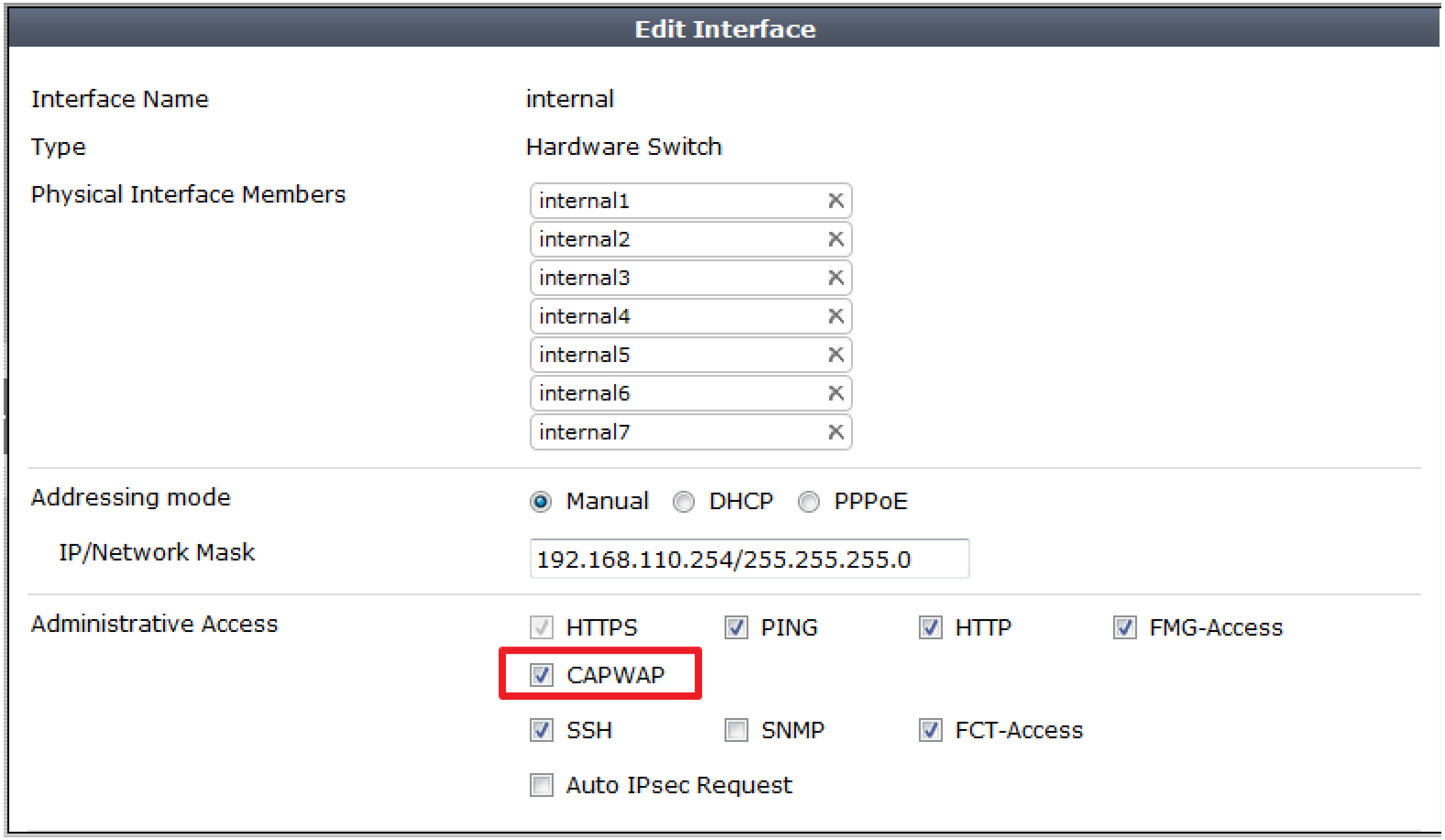
套用SSID

選擇AP型號

訊號強度

使用頻段

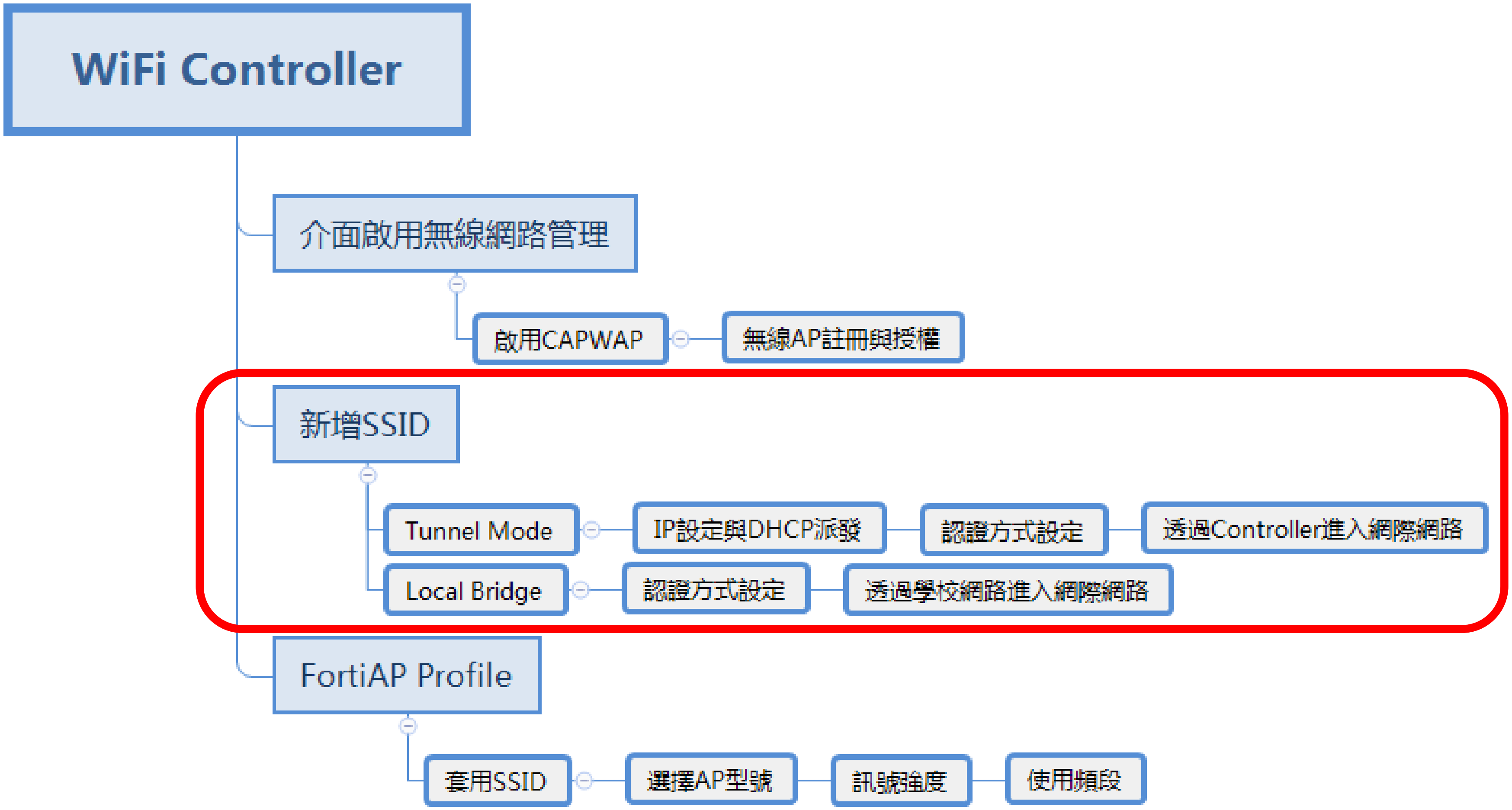
啟動介面管理AP



Edit Interface

Interface Name	internal
Type	Hardware Switch
Physical Interface Members	internal1 ✕ internal2 ✕ internal3 ✕ internal4 ✕ internal5 ✕ internal6 ✕ internal7 ✕
Addressing mode	● Manual ○ DHCP ○ PPPoE
IP/Network Mask	192.168.110.254/255.255.255.0
Administrative Access	☑ HTTPS ☑ PING ☑ HTTP ☑ FMG-Access ☑ CAPWAP ☑ SSH □ SNMP ☑ FCT-Access □ Auto IPsec Request

新增SSID



WiFi Controller

介面啟用無線網路管理

啟用CAPWAP

無線AP註冊與授權

新增SSID

Tunnel Mode

IP設定與DHCP派發

認證方式設定

透過Controller進入網際網路

Local Bridge

認證方式設定

透過學校網路進入網際網路

FortiAP Profile

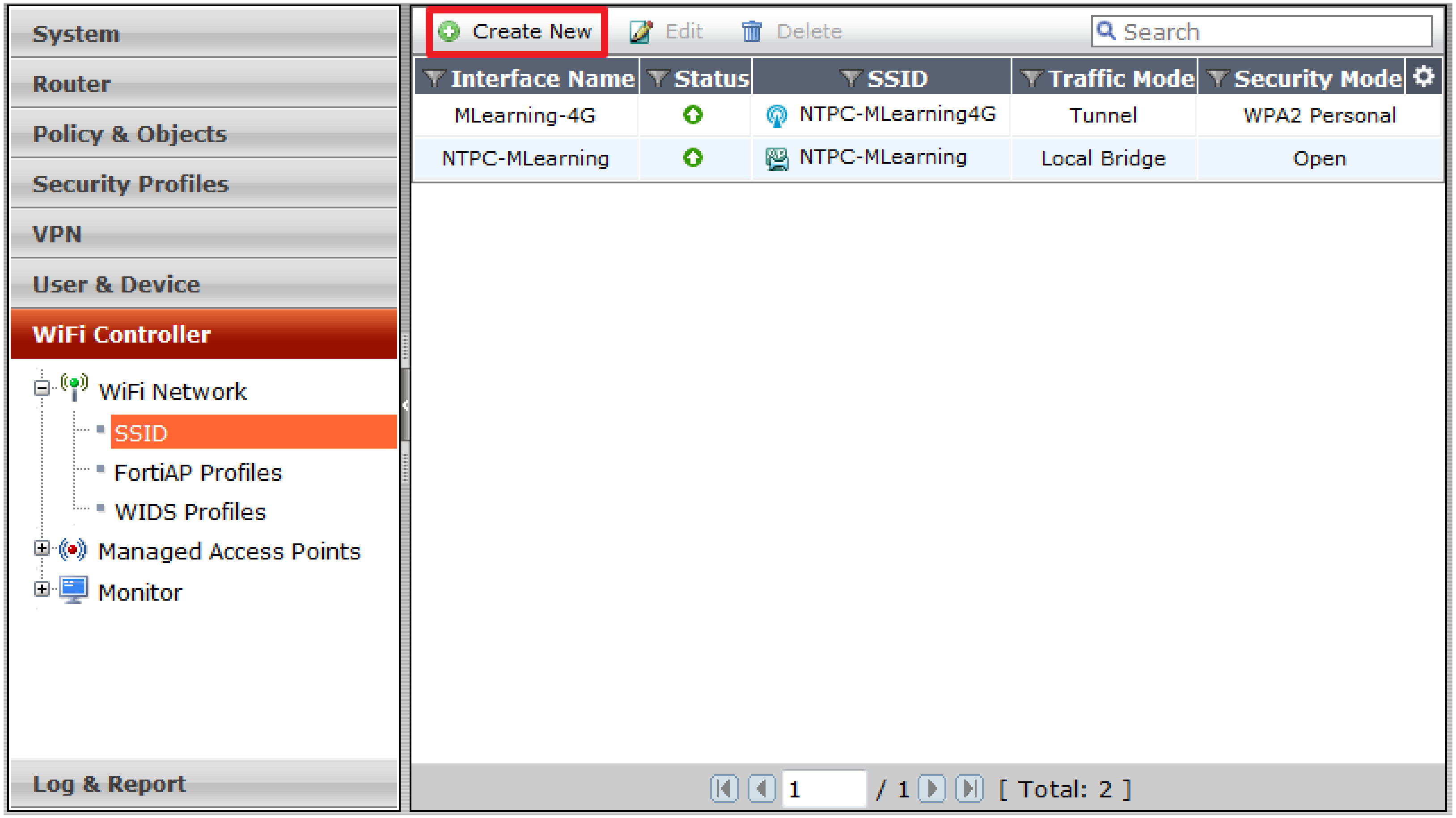
套用SSID

選擇AP型號

訊號強度

使用頻段

新增SSID

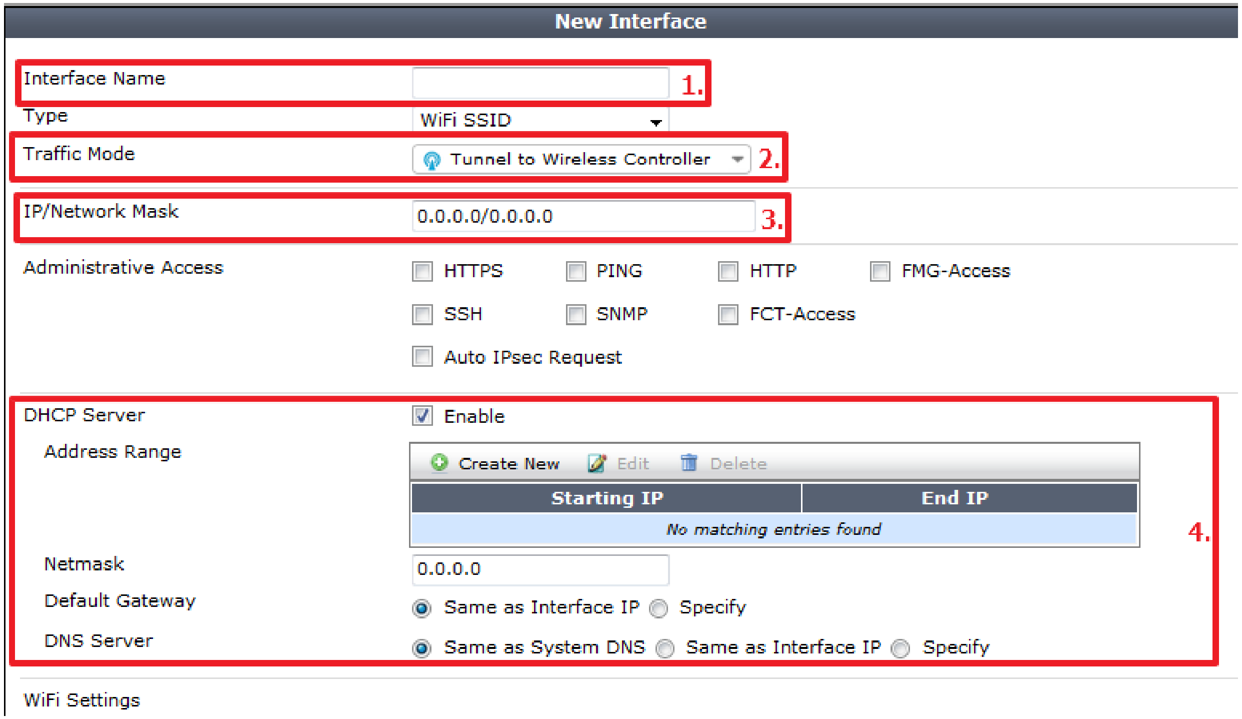


Interface Name	Status	SSID	Traffic Mode	Security Mode
MLearning-4G	●	NTPC-MLearning4G	Tunnel	WPA2 Personal
NTPC-MLearning	●	NTPC-MLearning	Local Bridge	Open

1 / 1 [Total: 2]

新增SSID

- 1.SSID名稱
- 2.流通模式
- 3.無線網路介面IP
- 4.DHCP派發設定



New Interface

1. Interface Name:

Type: WiFi SSID

2. Traffic Mode: Tunnel to Wireless Controller

3. IP/Network Mask: 0.0.0.0/0.0.0.0

Administrative Access: □ HTTPS □ PING □ HTTP □ FMG-Access □ SSH □ SNMP □ FCT-Access □ Auto IPsec Request

4. DHCP Server: ☑ Enable

Address Range: Create New | Edit | Delete

Starting IP	End IP
No matching entries found	

Netmask: 0.0.0.0

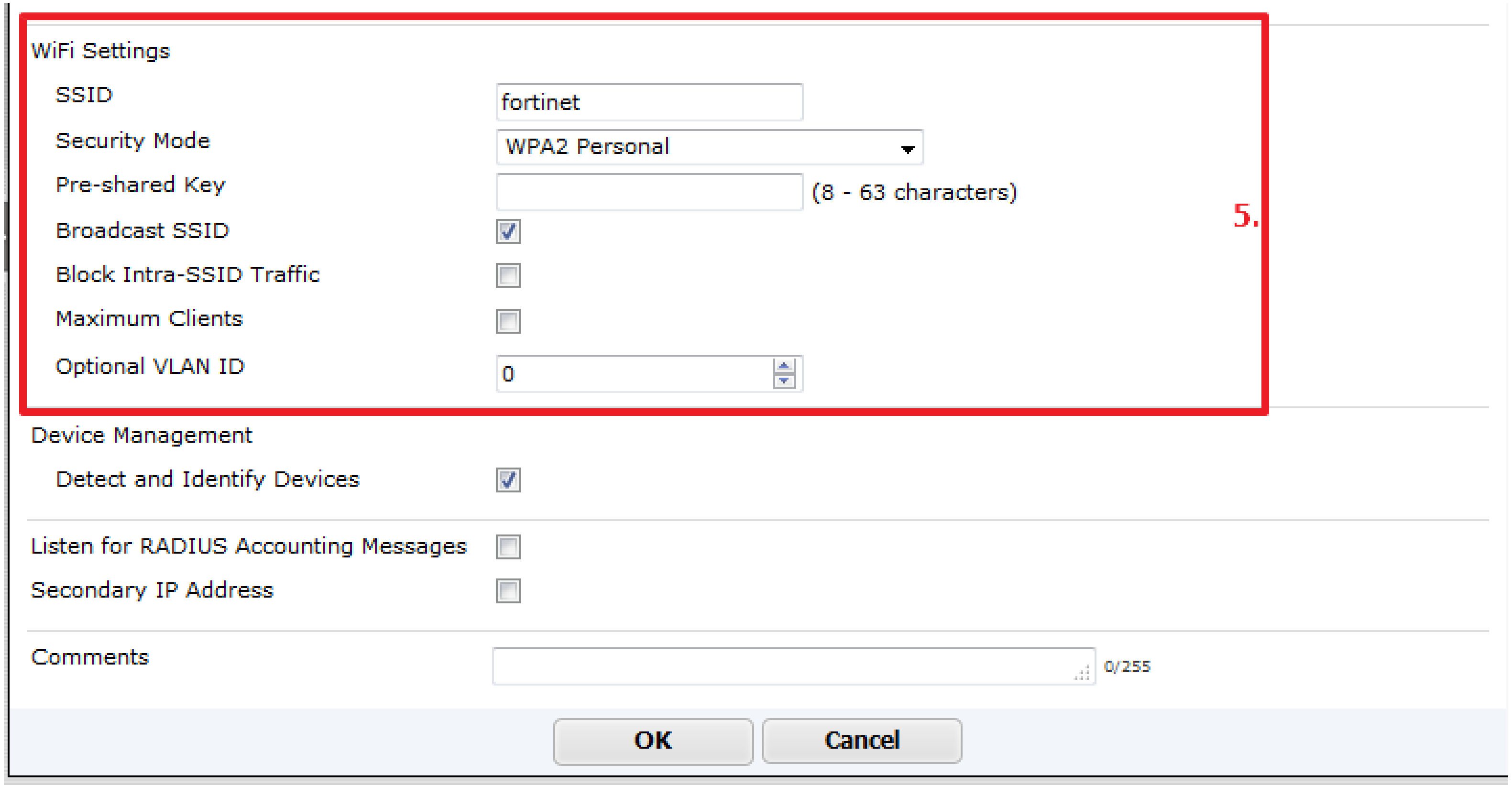
Default Gateway: ● Same as Interface IP ○ Specify

DNS Server: ● Same as System DNS ○ Same as Interface IP ○ Specify

WiFi Settings

新增SSID

- **5.SSID認證設定**



WiFi Settings

SSID	fortinet
Security Mode	WPA2 Personal
Pre-shared Key	(8 - 63 characters)
Broadcast SSID	☑
Block Intra-SSID Traffic	□
Maximum Clients	□
Optional VLAN ID	0

5.

Device Management

Detect and Identify Devices	☑
Listen for RADIUS Accounting Messages	□
Secondary IP Address	□
Comments	0/255

SSID額外項目

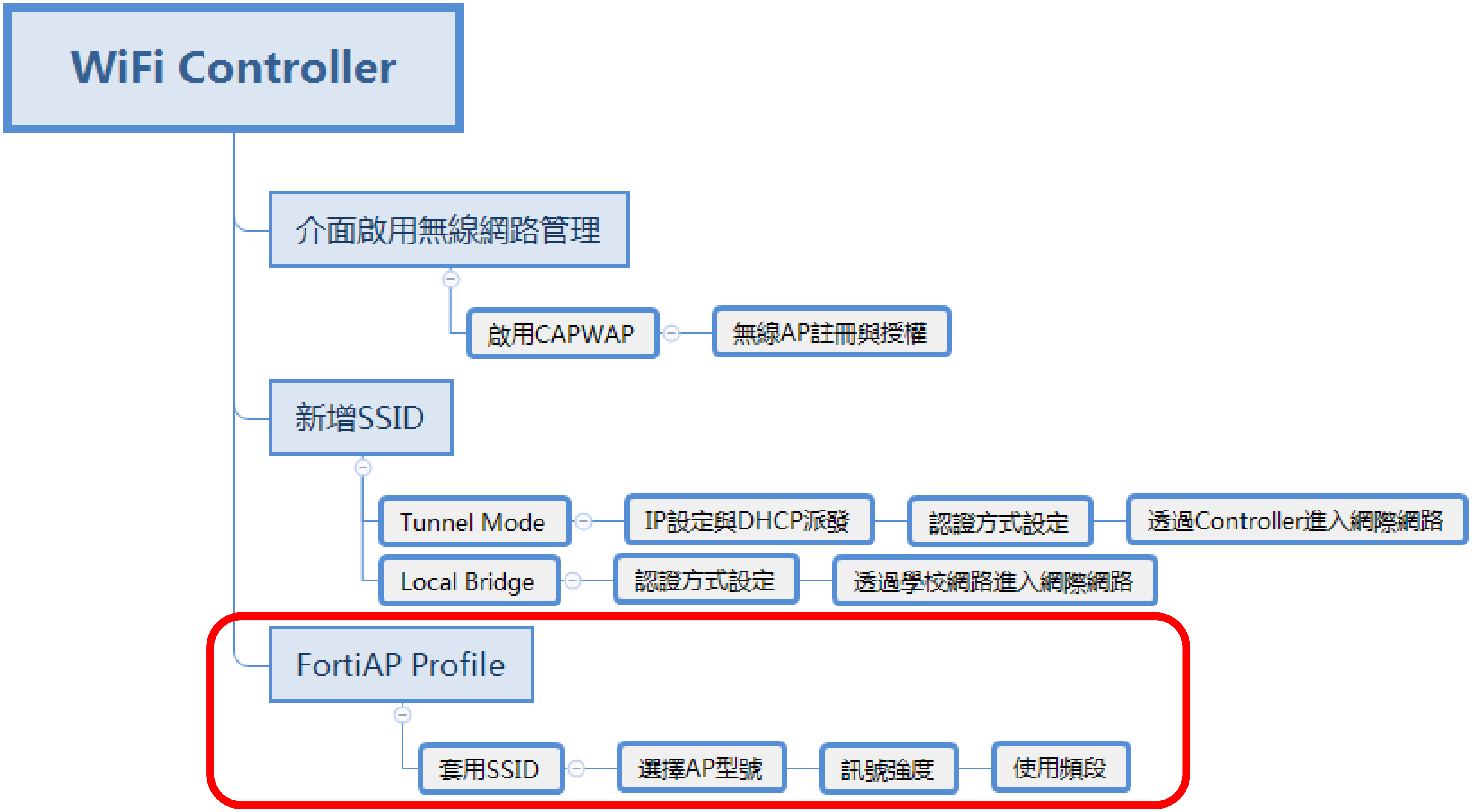
- 開放式SSID

```
config wireless-controller vap
edit [SSID]
set security open
end
```

- 國別設定

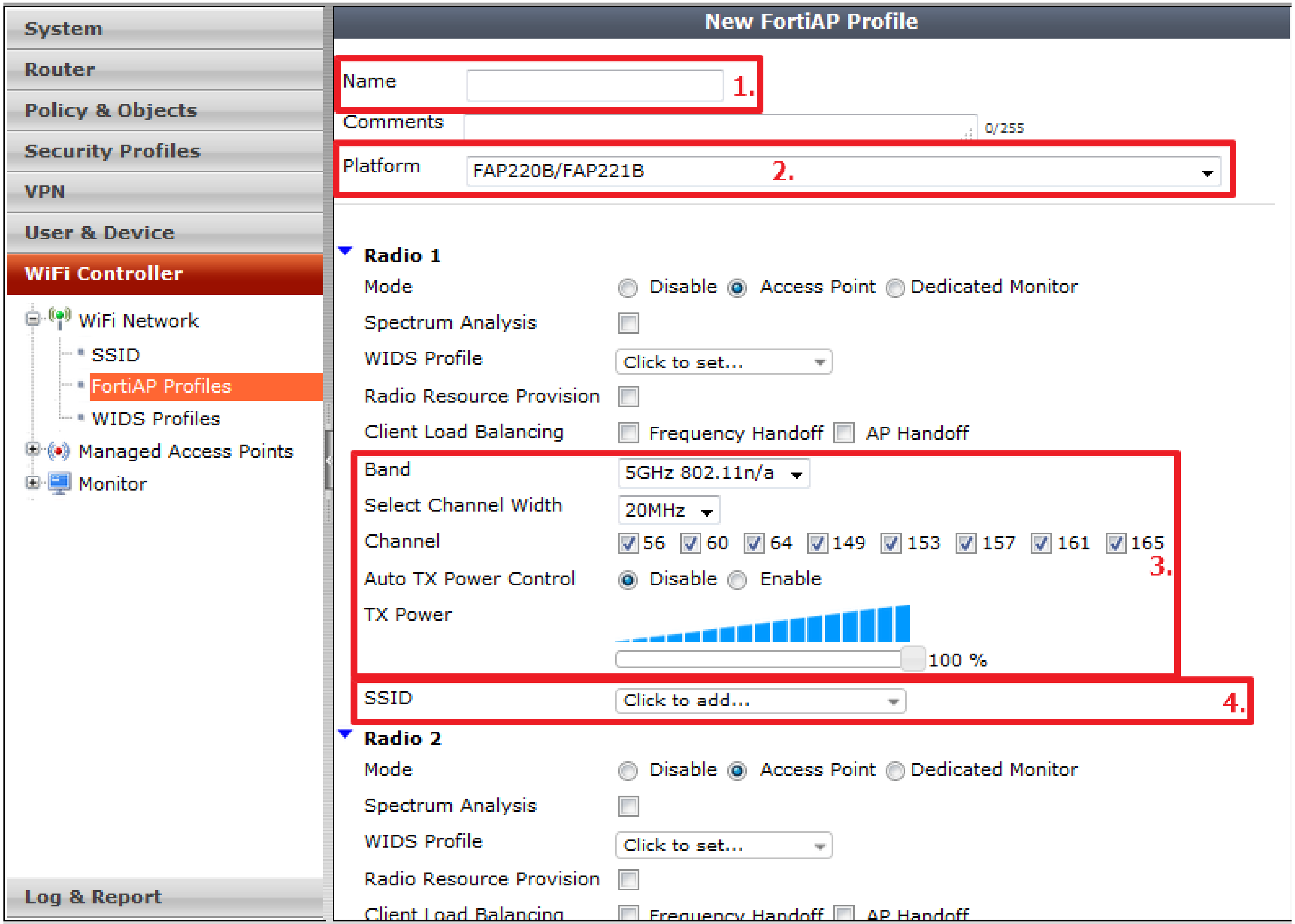
```
config wireless-controller setting
set country TW
end

FGT(setting) # end
This operation will also clear channel settings of all the existing wtp profiles.
Do you want to continue? (y/n) y
```

AP管理範本



- WiFi Controller
  - 介面啟用無線網路管理
    - 啟用CAPWAP — 無線AP註冊與授權
  - 新增SSID
    - Tunnel Mode — IP設定與DHCP派發 — 認證方式設定 — 透過Controller進入網際網路
    - Local Bridge — 認證方式設定 — 透過學校網路進入網際網路
  - FortiAP Profile
    - 套用SSID — 選擇AP型號 — 訊號強度 — 使用頻段

無線AP管理範本



System
Router
Policy & Objects
Security Profiles
VPN
User & Device
WiFi Controller
- WiFi Network
  - SSID
  - FortiAP Profiles
  - WIDS Profiles
- Managed Access Points
- Monitor

Log & Report

New FortiAP Profile

1. Name:
Comments: 0/255

2. Platform: FAP220B/FAP221B

Radio 1

Mode: ○ Disable ● Access Point ○ Dedicated Monitor
Spectrum Analysis: □
WIDS Profile: Click to set...
Radio Resource Provision: □
Client Load Balancing: □ Frequency Handoff □ AP Handoff

3.
Band: 5GHz 802.11n/a
Select Channel Width: 20MHz
Channel: ☑ 56 ☑ 60 ☑ 64 ☑ 149 ☑ 153 ☑ 157 ☑ 161 ☑ 165
Auto TX Power Control: ● Disable ○ Enable
TX Power: 100 %

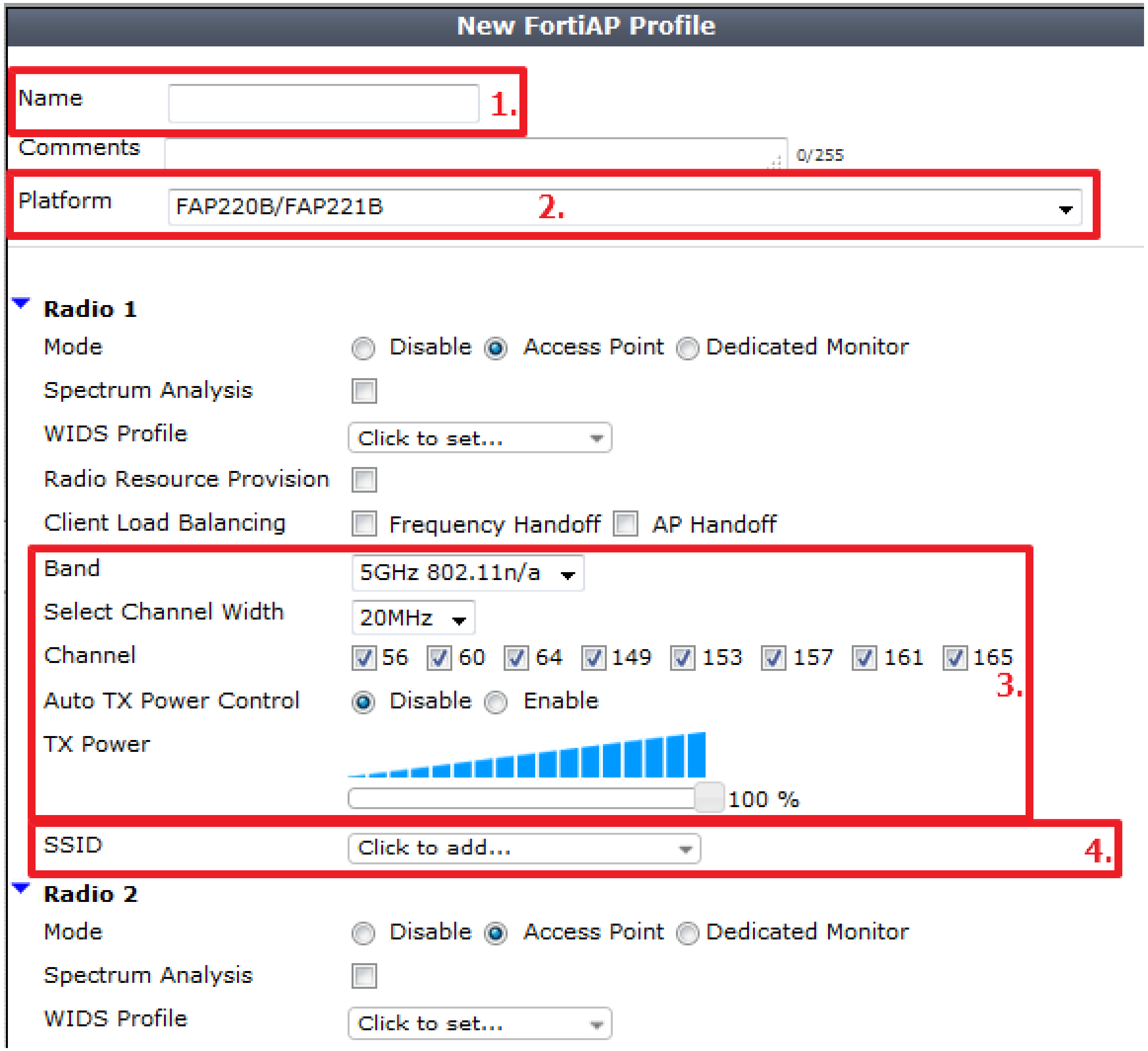
4. SSID: Click to add...

Radio 2

Mode: ○ Disable ● Access Point ○ Dedicated Monitor
Spectrum Analysis: □
WIDS Profile: Click to set...
Radio Resource Provision: □
Client Load Balancing: □ Frequency Handoff □ AP Handoff

無線AP管理範本

- 1.範本名稱
- 2.AP型號
- 3.使用頻段
- 4.SSID



New FortiAP Profile

Name 1.

Comments 0/255

Platform FAP220B/FAP221B 2.

Radio 1

Mode ○ Disable ● Access Point ○ Dedicated Monitor

Spectrum Analysis □

WIDS Profile Click to set...

Radio Resource Provision □

Client Load Balancing □ Frequency Handoff □ AP Handoff

Band 5GHz 802.11n/a

Select Channel Width 20MHz

Channel ☑ 56 ☑ 60 ☑ 64 ☑ 149 ☑ 153 ☑ 157 ☑ 161 ☑ 165 3.

Auto TX Power Control ● Disable ○ Enable

TX Power 100 %

SSID Click to add... 4.

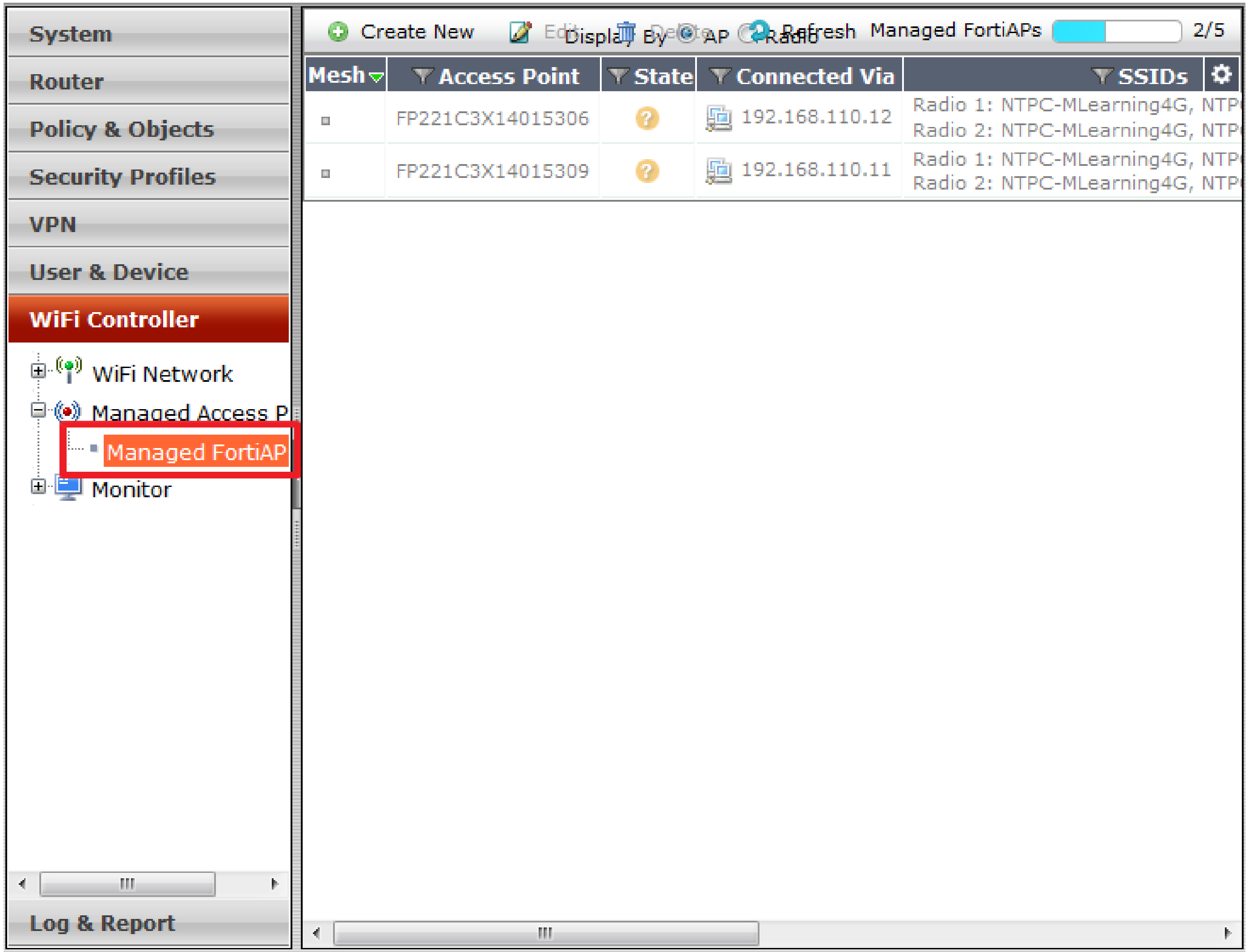
Radio 2

Mode ○ Disable ● Access Point ○ Dedicated Monitor

Spectrum Analysis □

WIDS Profile Click to set...

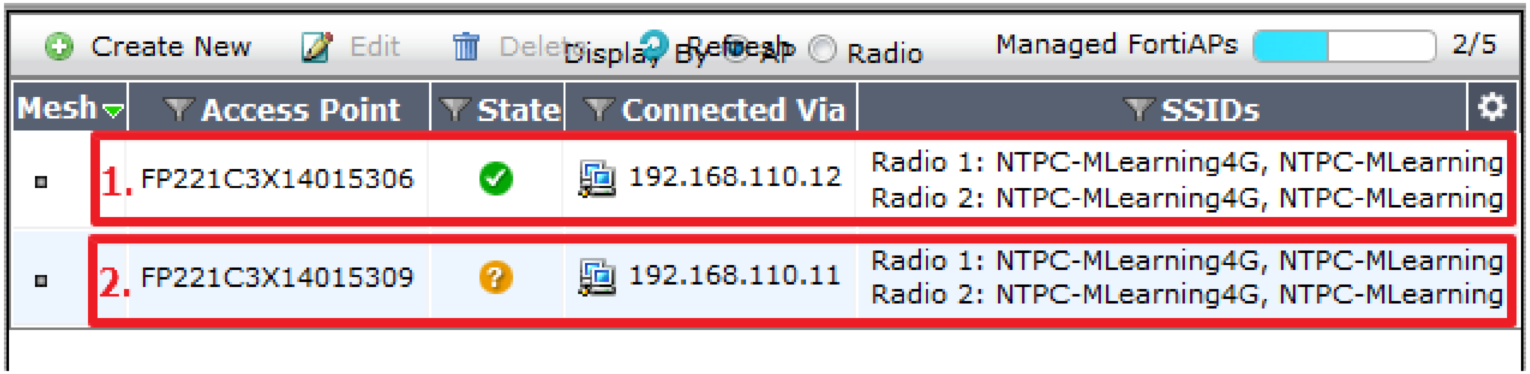
授權無線AP



Mesh	Access Point	State	Connected Via	SSIDs
□	FP221C3X14015306	?	192.168.110.12	Radio 1: NTPC-MLearning4G, NTP Radio 2: NTPC-MLearning4G, NTP
□	FP221C3X14015309	?	192.168.110.11	Radio 1: NTPC-MLearning4G, NTP Radio 2: NTPC-MLearning4G, NTP

授權無線AP

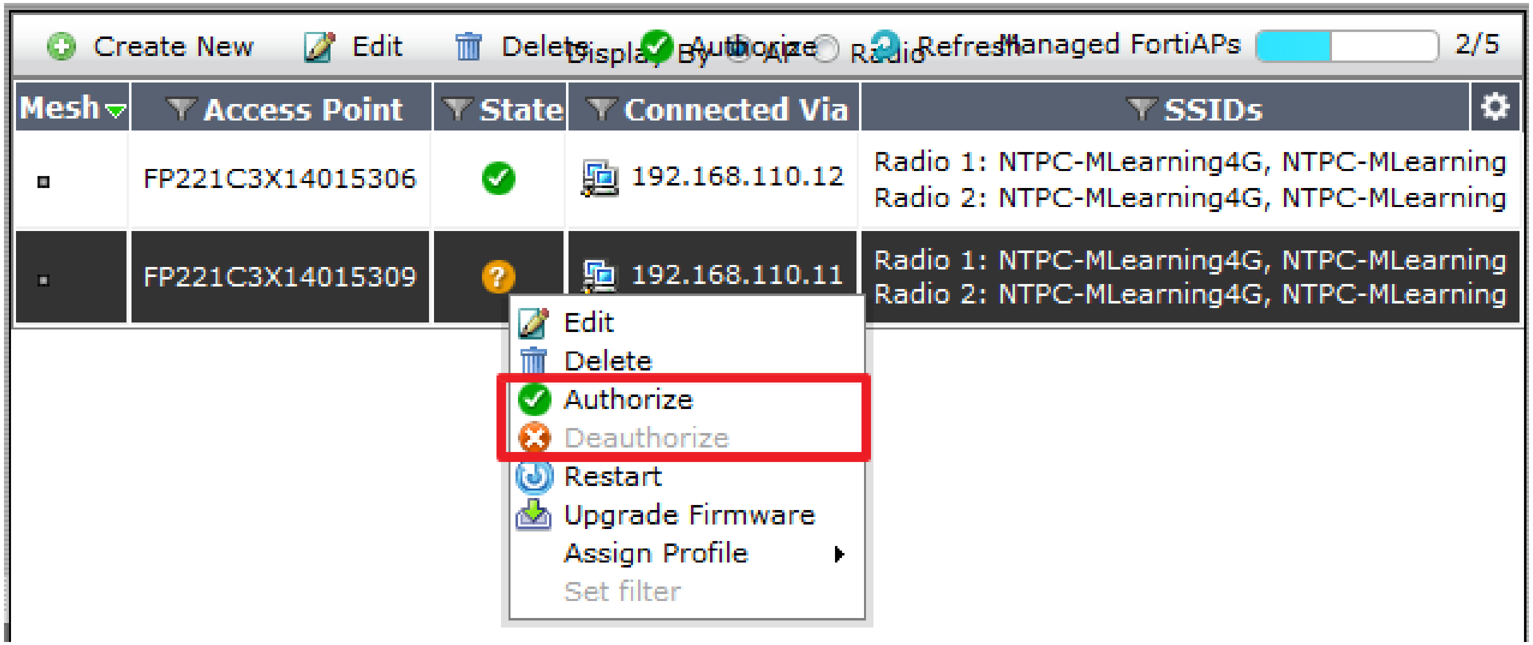
- 1.正常授權狀態
- 2.未授權狀態



Mesh	Access Point	State	Connected Via	SSIDs
□	1. FP221C3X14015306	✓	192.168.110.12	Radio 1: NTPC-MLearning4G, NTPC-MLearning Radio 2: NTPC-MLearning4G, NTPC-MLearning
□	2. FP221C3X14015309	?	192.168.110.11	Radio 1: NTPC-MLearning4G, NTPC-MLearning Radio 2: NTPC-MLearning4G, NTPC-MLearning

授權無線AP

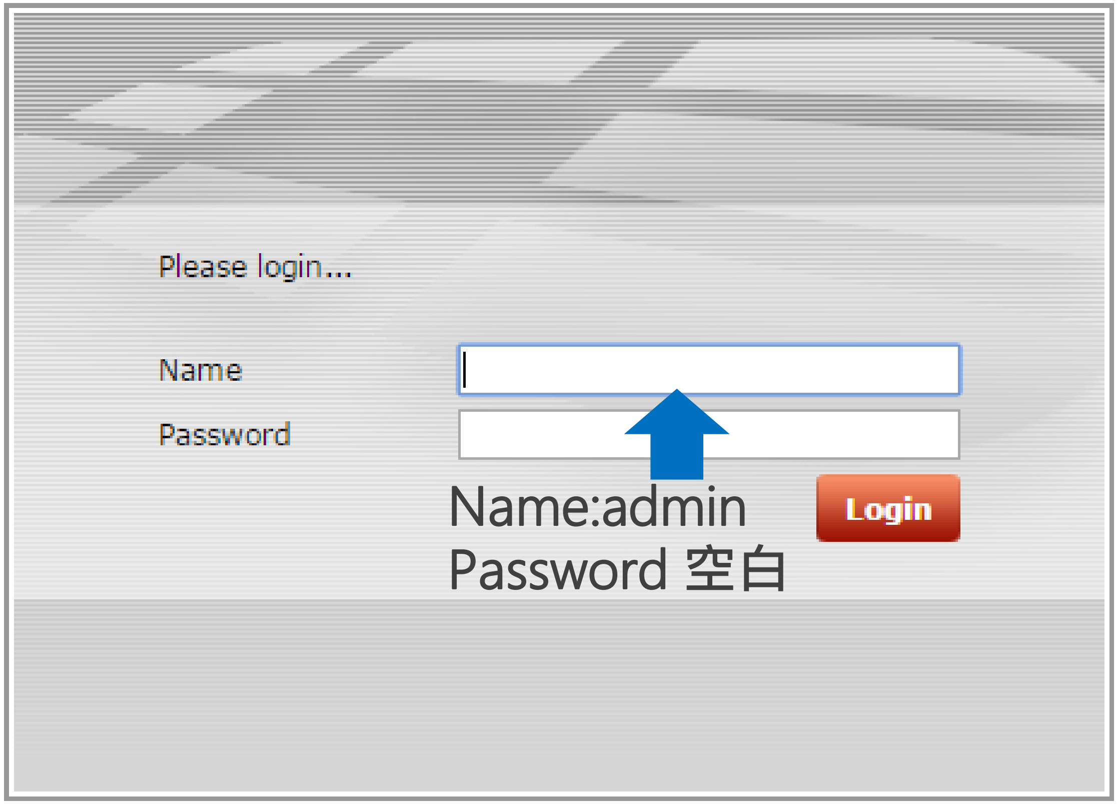
- 右鍵點選Authorize進行授權



Mesh	Access Point	State	Connected Via	SSIDs
▪	FP221C3X14015306	✓	192.168.110.12	Radio 1: NTPC-MLearning4G, NTPC-MLearning Radio 2: NTPC-MLearning4G, NTPC-MLearning
▪	FP221C3X14015309	?	192.168.110.11	Radio 1: NTPC-MLearning4G, NTPC-MLearning Radio 2: NTPC-MLearning4G, NTPC-MLearning

FortiAP設定

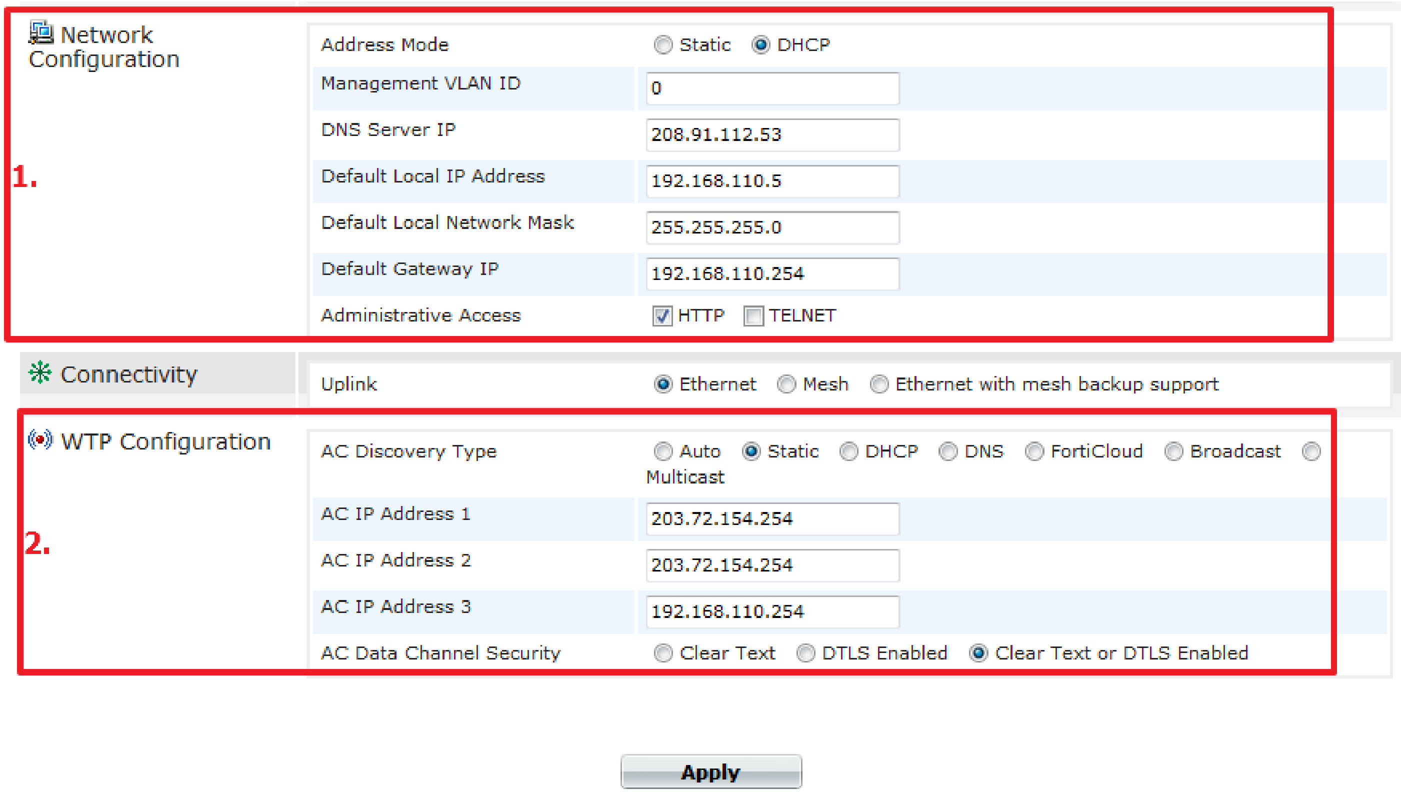
- 使用瀏覽器連結 AP輸入IP:192.168.1.2



Name:admin
Password 空白

FortiAP設定

- 1.AP介面設定
- 2.Controller IP設定



1.

Network Configuration

Address Mode	○ Static ● DHCP
Management VLAN ID	0
DNS Server IP	208.91.112.53
Default Local IP Address	192.168.110.5
Default Local Network Mask	255.255.255.0
Default Gateway IP	192.168.110.254
Administrative Access	☑ HTTP □ TELNET

Connectivity

Uplink	● Ethernet ○ Mesh ○ Ethernet with mesh backup support

2.

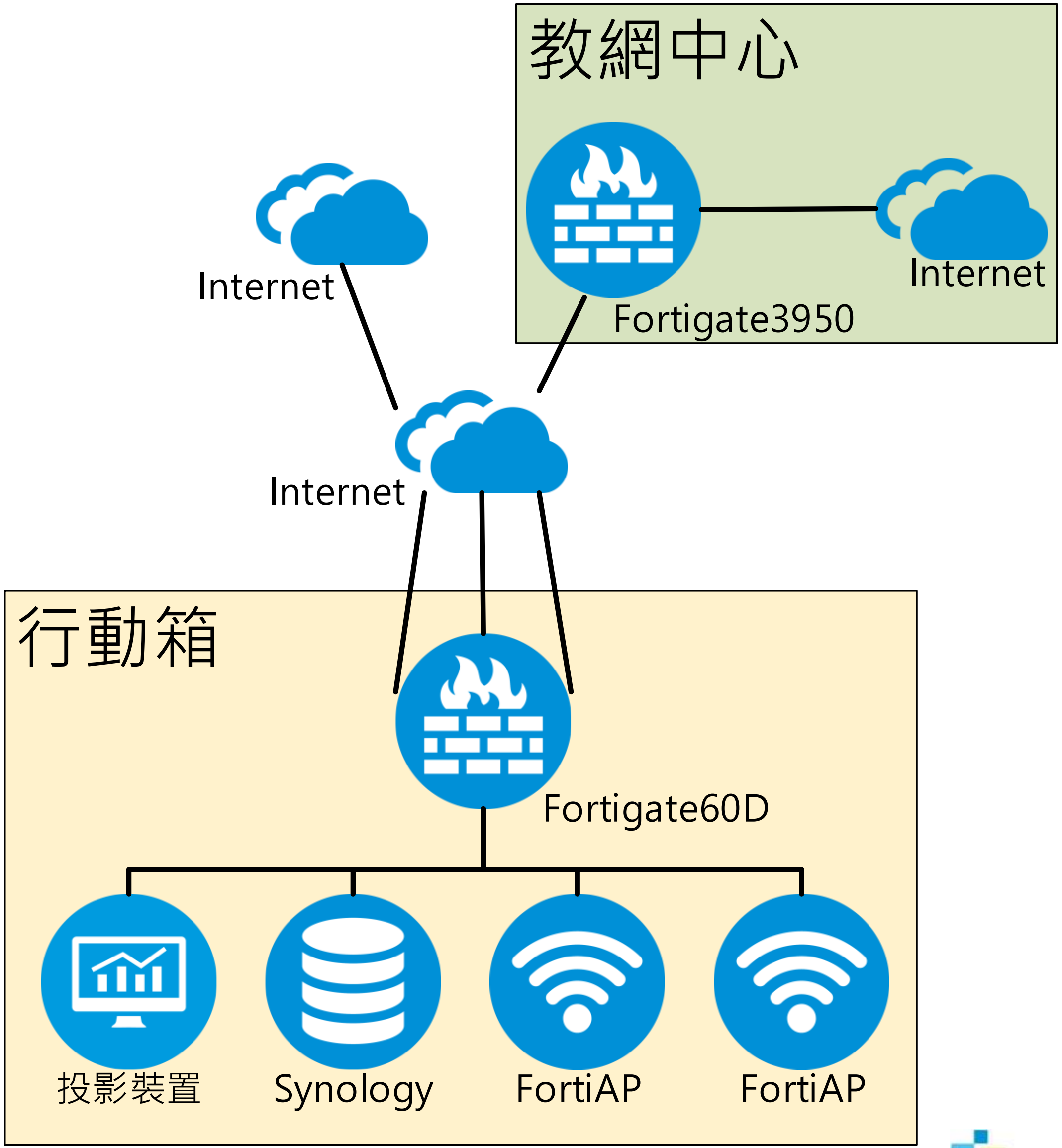
WTP Configuration

AC Discovery Type	○ Auto ● Static ○ DHCP ○ DNS ○ FortiCloud ○ Broadcast ○ Multicast
AC IP Address 1	203.72.154.254
AC IP Address 2	203.72.154.254
AC IP Address 3	192.168.110.254
AC Data Channel Security	○ Clear Text ○ DTLS Enabled ● Clear Text or DTLS Enabled

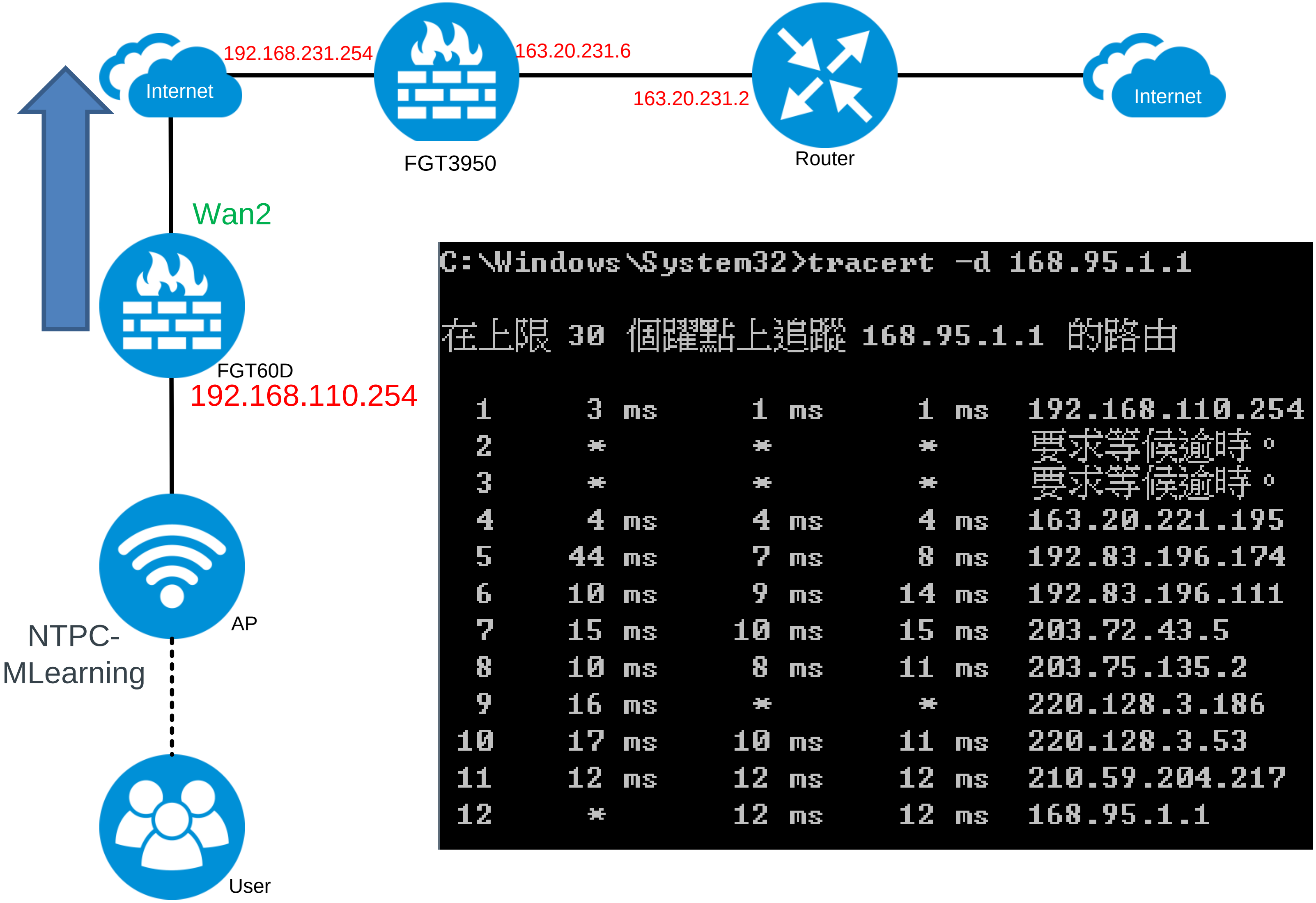
行動箱網路架構圖

SSID(上網用)
1.NTPC_MLearing
2.NTPC-Mlearing4G

SSID(存取教網資源)
1.NTPC-M
2.NTPC-MLearing
3.NTPC-Mobile
4.NTPC-WPA2-M

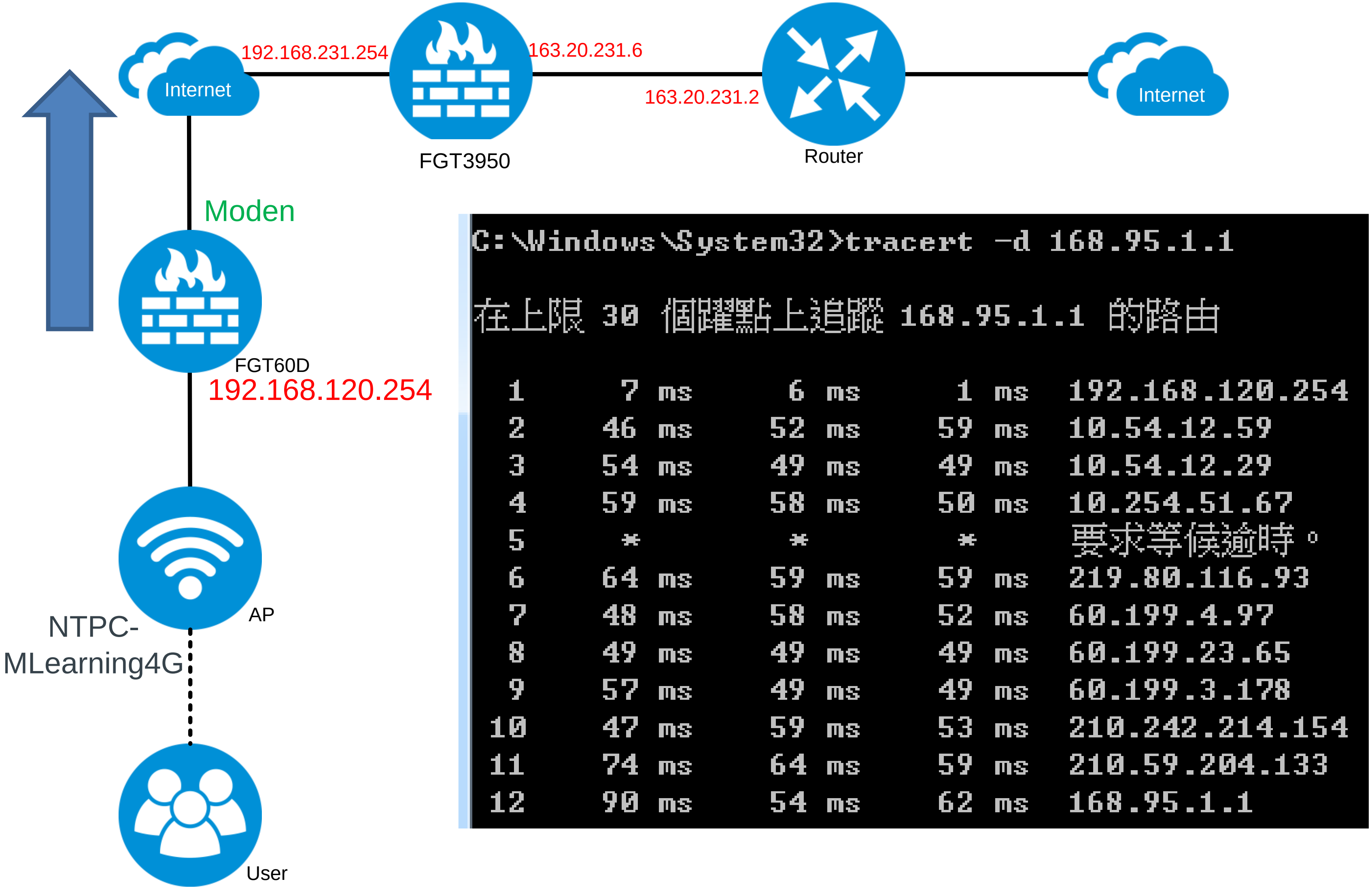


NTPC-MLearning



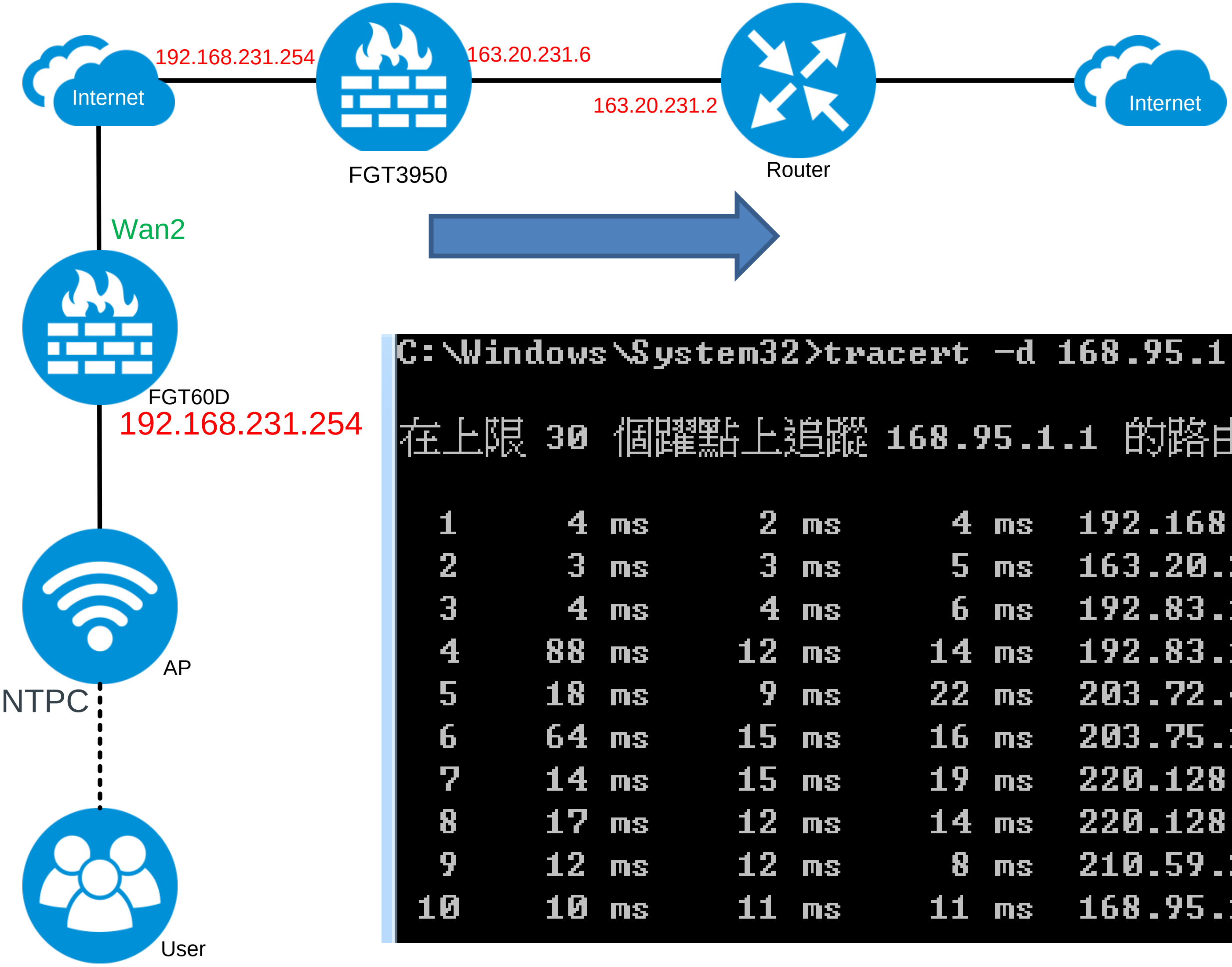
```
C:\Windows\System32>tracert -d 168.95.1.1

在上限 30 個躍點上追蹤 168.95.1.1 的路由

  1     3 ms     1 ms     1 ms  192.168.110.254
  2     *        *        *     要求等候逾時。
  3     *        *        *     要求等候逾時。
  4     4 ms     4 ms     4 ms  163.20.221.195
  5    44 ms     7 ms     8 ms  192.83.196.174
  6    10 ms     9 ms    14 ms  192.83.196.111
  7    15 ms    10 ms    15 ms  203.72.43.5
  8    10 ms     8 ms    11 ms  203.75.135.2
  9    16 ms     *        *     220.128.3.186
 10    17 ms    10 ms    11 ms  220.128.3.53
 11    12 ms    12 ms    12 ms  210.59.204.217
 12     *       12 ms    12 ms  168.95.1.1
```

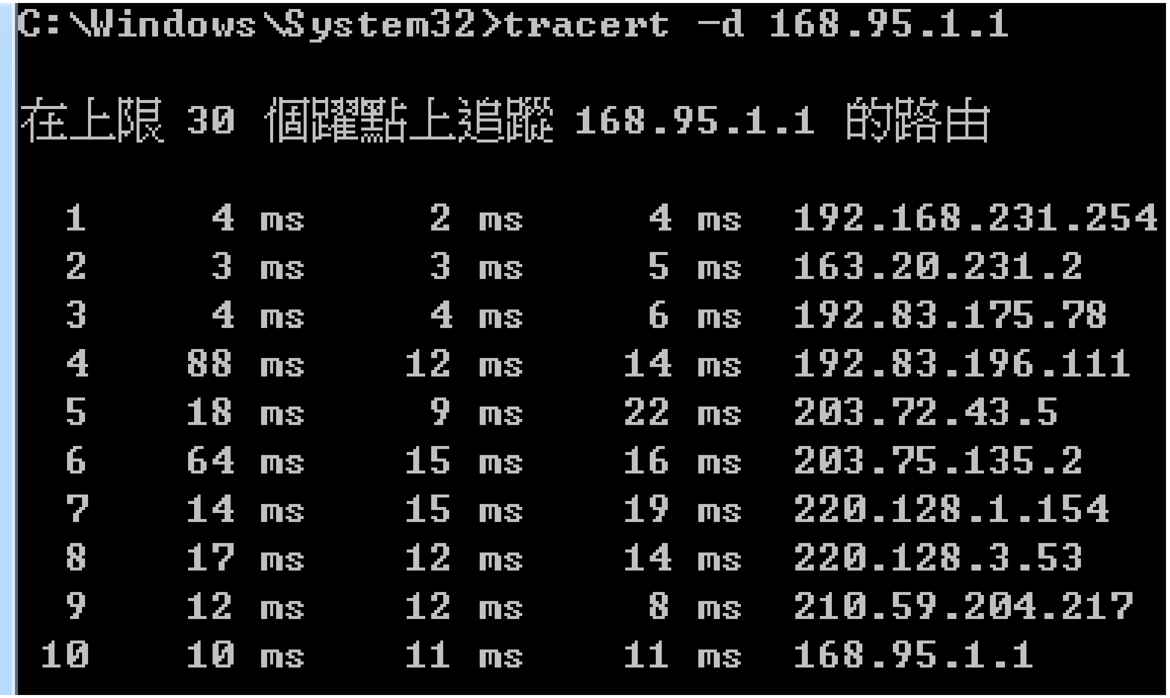
NTPC-MLearning4G



```
C:\Windows\System32>tracert -d 168.95.1.1

在上限 30 個躍點上追蹤 168.95.1.1 的路由

  1     7 ms     6 ms     1 ms  192.168.120.254
  2    46 ms    52 ms    59 ms  10.54.12.59
  3    54 ms    49 ms    49 ms  10.54.12.29
  4    59 ms    58 ms    50 ms  10.254.51.67
  5     *        *        *     要求等候逾時。
  6    64 ms    59 ms    59 ms  219.80.116.93
  7    48 ms    58 ms    52 ms  60.199.4.97
  8    49 ms    49 ms    49 ms  60.199.23.65
  9    57 ms    49 ms    49 ms  60.199.3.178
 10    47 ms    59 ms    53 ms  210.242.214.154
 11    74 ms    64 ms    59 ms  210.59.204.133
 12    90 ms    54 ms    62 ms  168.95.1.1
```

NTPC

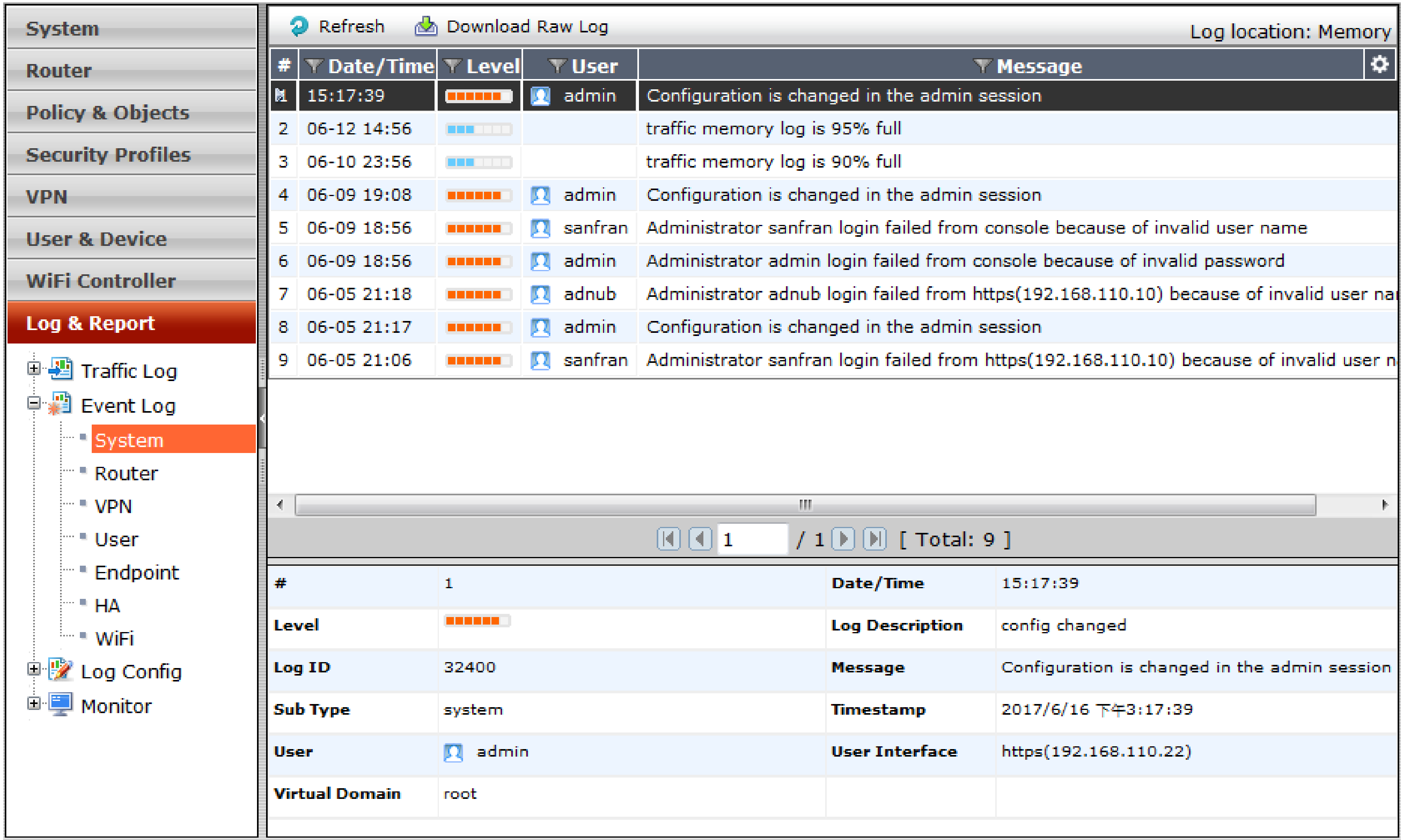




```
C:\Windows\System32>tracert -d 168.95.1.1

在上限 30 個躍點上追蹤 168.95.1.1 的路由

  1     4 ms     2 ms     4 ms  192.168.231.254
  2     3 ms     3 ms     5 ms  163.20.231.2
  3     4 ms     4 ms     6 ms  192.83.175.78
  4    88 ms    12 ms    14 ms  192.83.196.111
  5    18 ms     9 ms    22 ms  203.72.43.5
  6    64 ms    15 ms    16 ms  203.75.135.2
  7    14 ms    15 ms    19 ms  220.128.1.154
  8    17 ms    12 ms    14 ms  220.128.3.53
  9    12 ms    12 ms     8 ms  210.59.204.217
 10    10 ms    11 ms    11 ms  168.95.1.1
```

故障排除

Event log

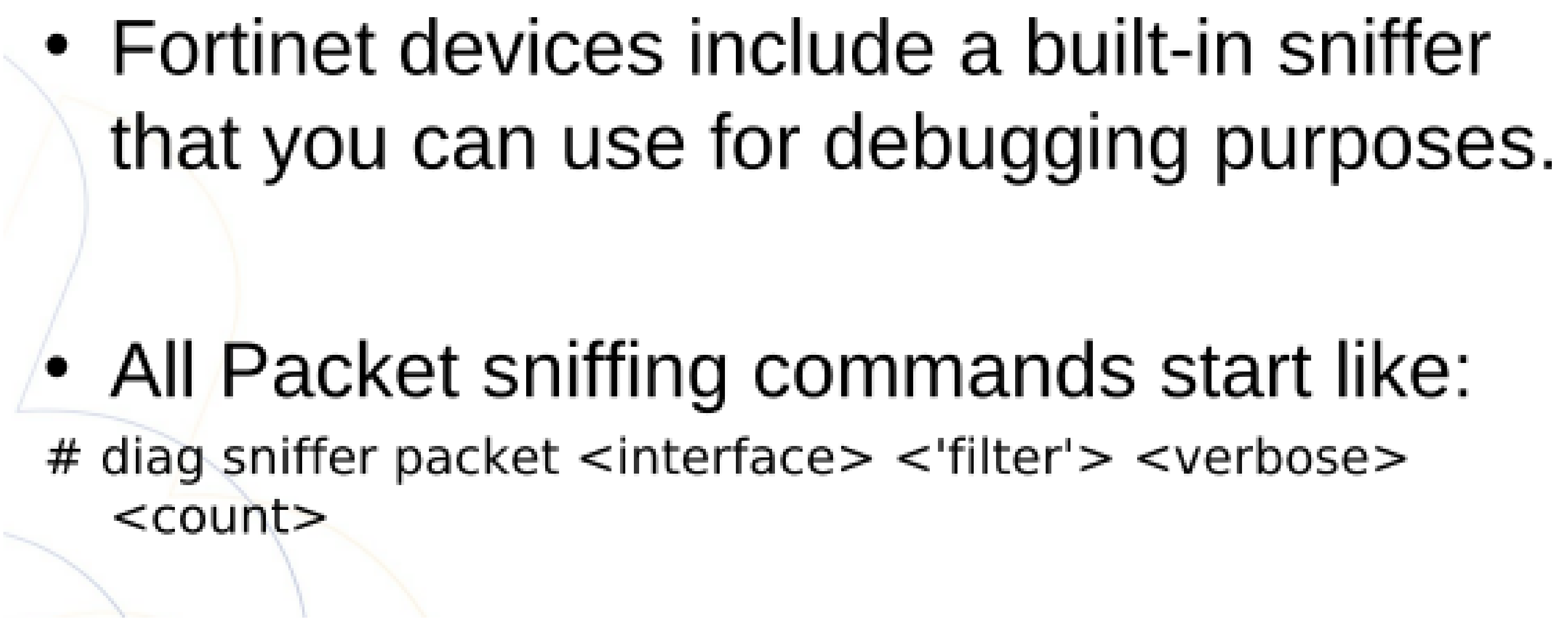


#	Date/Time	Level	User	Message
1	15:17:39	■■■■■■	admin	Configuration is changed in the admin session
2	06-12 14:56	■■■		traffic memory log is 95% full
3	06-10 23:56	■■■		traffic memory log is 90% full
4	06-09 19:08	■■■■■■	admin	Configuration is changed in the admin session
5	06-09 18:56	■■■■■■	sanfran	Administrator sanfran login failed from console because of invalid user name
6	06-09 18:56	■■■■■■	admin	Administrator admin login failed from console because of invalid password
7	06-05 21:18	■■■■■■	adnub	Administrator adnub login failed from https(192.168.110.10) because of invalid user na
8	06-05 21:17	■■■■■■	admin	Configuration is changed in the admin session
9	06-05 21:06	■■■■■■	sanfran	Administrator sanfran login failed from https(192.168.110.10) because of invalid user n

1 / 1 [Total: 9]

#	1	Date/Time	15:17:39
Level	■■■■■■	Log Description	config changed
Log ID	32400	Message	Configuration is changed in the admin session
Sub Type	system	Timestamp	2017/6/16 下午3:17:39
User	admin	User Interface	https(192.168.110.22)
Virtual Domain	root		

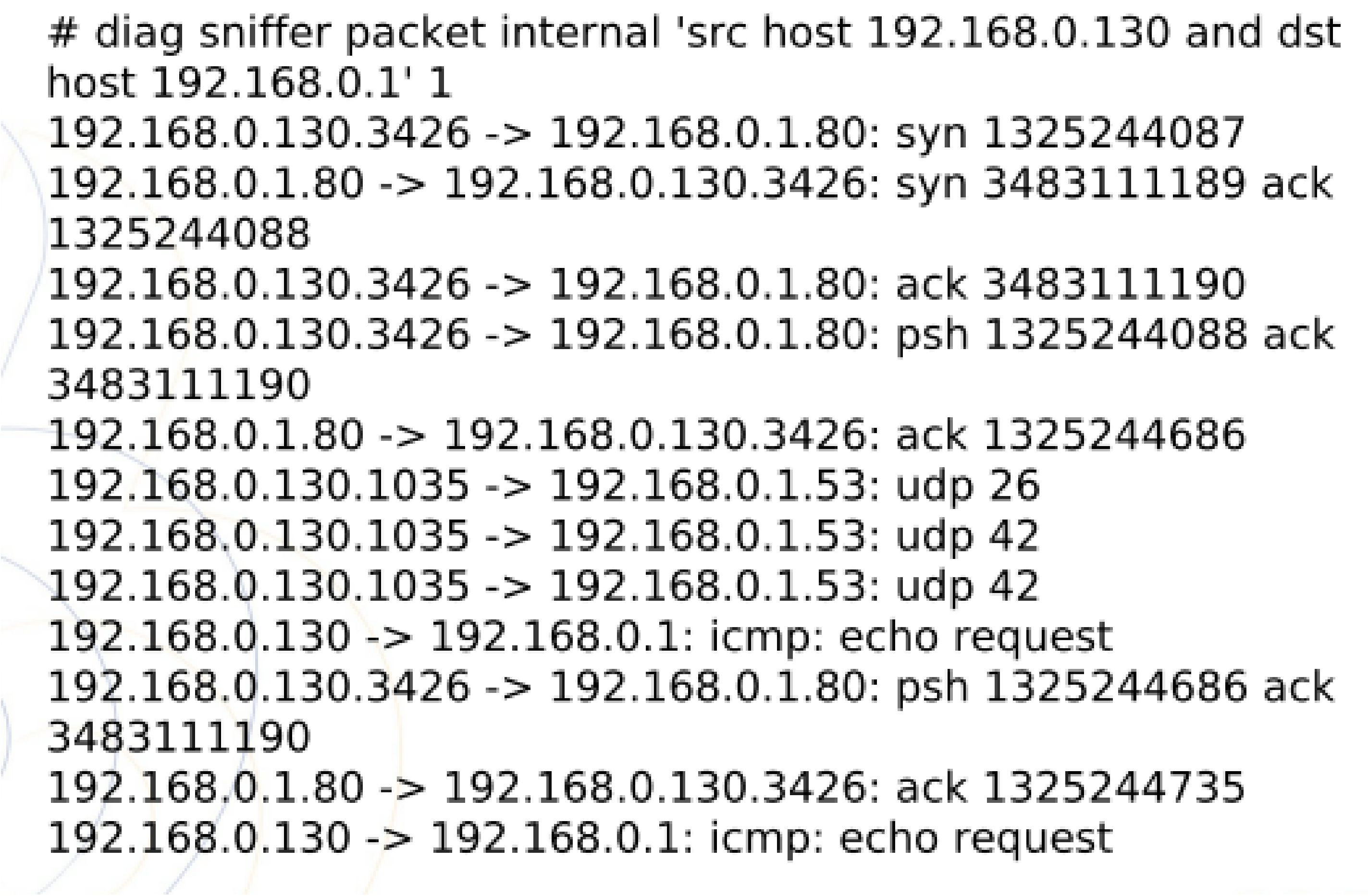
Debug Command



- Fortinet devices include a built-in sniffer that you can use for debugging purposes.
- All Packet sniffing commands start like:

```
# diag sniffer packet <interface> <'filter'> <verbose>
    <count>
```

Debug Command Example



```
# diag sniffer packet internal 'src host 192.168.0.130 and dst
host 192.168.0.1' 1
192.168.0.130.3426 -> 192.168.0.1.80: syn 1325244087
192.168.0.1.80 -> 192.168.0.130.3426: syn 3483111189 ack
1325244088
192.168.0.130.3426 -> 192.168.0.1.80: ack 3483111190
192.168.0.130.3426 -> 192.168.0.1.80: psh 1325244088 ack
3483111190
192.168.0.1.80 -> 192.168.0.130.3426: ack 1325244686
192.168.0.130.1035 -> 192.168.0.1.53: udp 26
192.168.0.130.1035 -> 192.168.0.1.53: udp 42
192.168.0.130.1035 -> 192.168.0.1.53: udp 42
192.168.0.130 -> 192.168.0.1: icmp: echo request
192.168.0.130.3426 -> 192.168.0.1.80: psh 1325244686 ack
3483111190
192.168.0.1.80 -> 192.168.0.130.3426: ack 1325244735
192.168.0.130 -> 192.168.0.1: icmp: echo request
```

參考網站

FortiGate Knowledge Base Libary
http://kb.fortinet.com/kb/microsites/microsite.do

FortiGate Technical Document
http://docs.fortinet.com/fgt.html

FortiGate Treat Center
http://www.fortiguard.com/

FortiGate Support(Tools Firmware)
https://support.fortinet.com/login/UserLogin.aspx

高可用性介紹

高可用性介紹

- Active-Passive－

平時只有一台FG（Master）處理網路流量，另一台（Slave）僅作同步參數用（如設定等）；只有在Master 的界面狀態有異動，亦或其離線時，Slave才會上線接手。

- Active-Active－

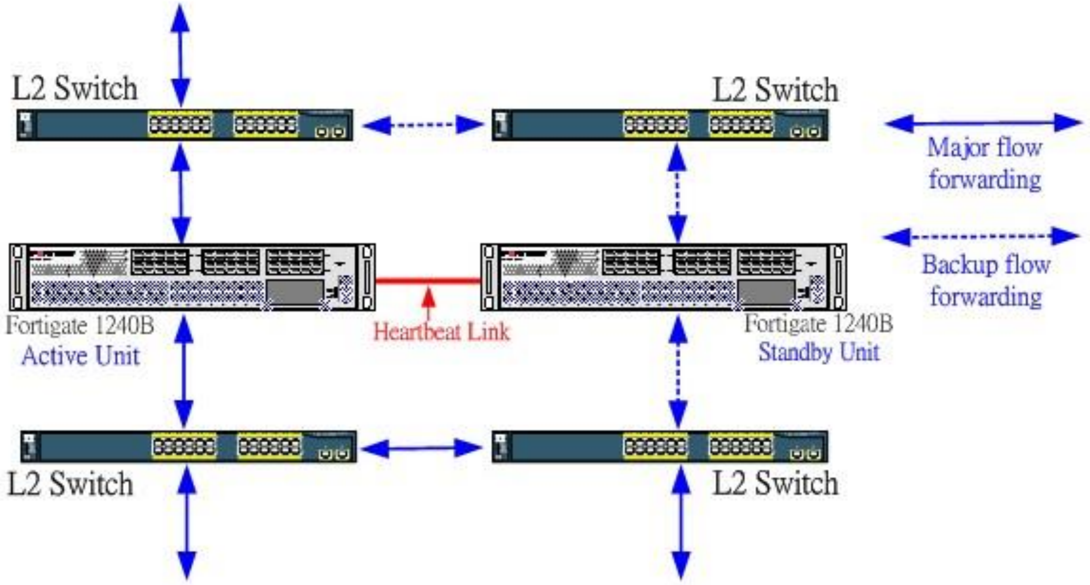
不同於A-P模式下，會有一台FG是閒置的；HA Cluster下的兩台設備，同時間皆會處理網路流量。

高可用性介紹

- 流量經由Active Unit uplink交換器轉發，透過FGCP協定產生虛擬Mac Address (00-09-0f-xx-cluster group number-port number)來作二層回應需求，而standby unit作為待命設備不主動作回應。
- FGCP判定條件： (default ha override is disable)
  - 1. Port Monitor (取決於Active Monitor interface為Cluster Master)
  - 2. HA Age Time (開機存活時間，若差異小於5min，則忽略此項)
  - 3. Priority (較大者Cluster Master)
  - 4. S/N (較大者為Cluster Master)

Active-Passive

正常工作下…

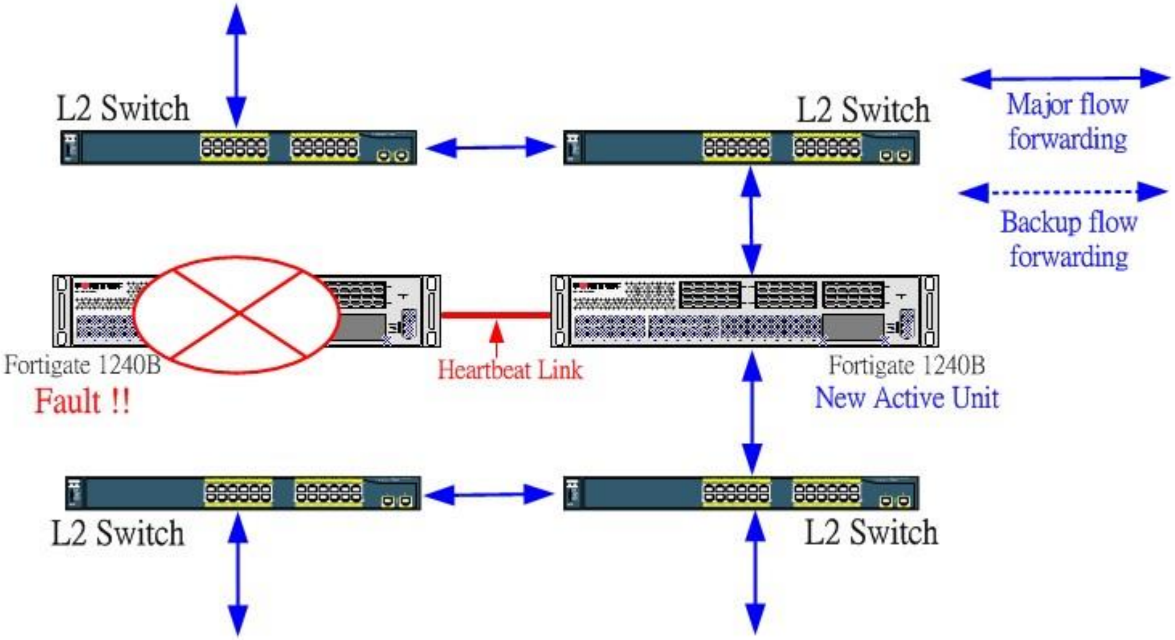


高可用性介紹

- 若發生Active Unit故障，透過FGCP協定於一秒內完成Active-Passive切換動作，
  - 此時Active role會由standby unit接手(Lost Heartbeat Packet in interval time,default is 200ms)，防火牆服務不會中斷
- 為避免重新連線的情形，需Enable Session Pick-up，同步設備間的連線資訊
  - 支援A-A與A-P模式中所有非UTM的流量類型
- 此時由Standby Unit繼續提供服務，不會造成中斷情形。

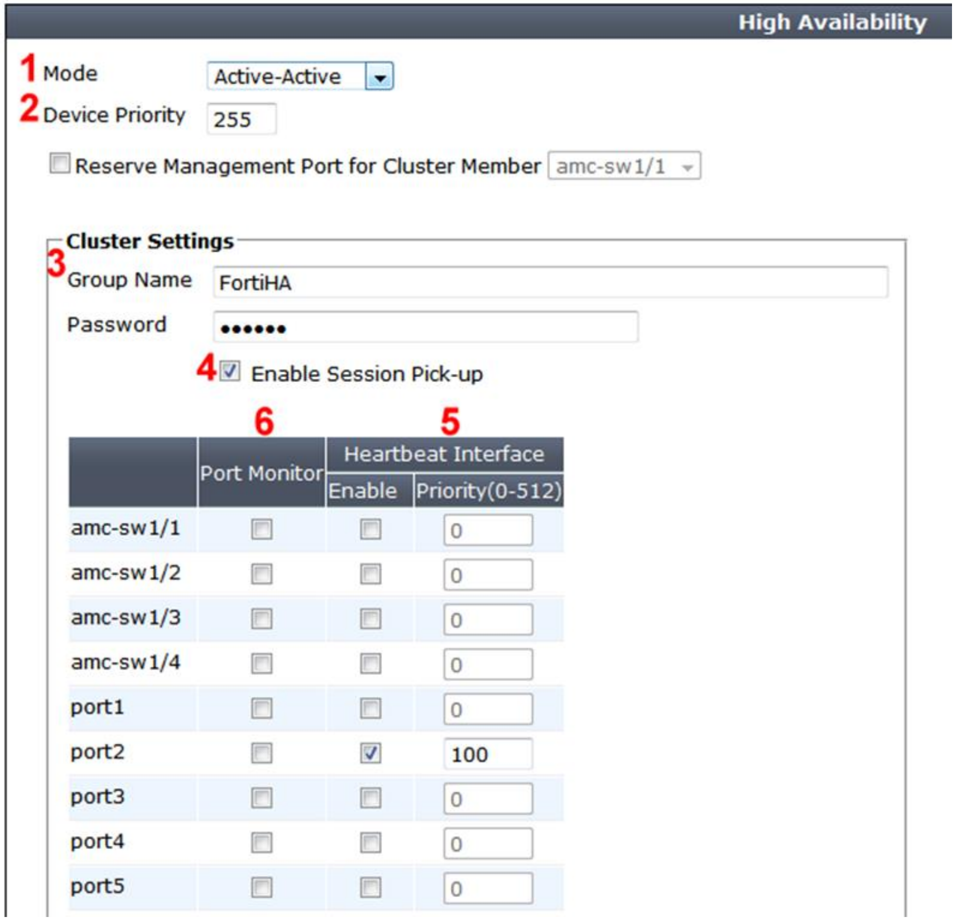
Active-Passive

電源斷電或設備故障



設定防火牆HA功能

- 1.HA模式選擇
  - Active/Active或Active/Passive
- 2.設備權重值
  - 數值大者為Active
- 3.HA群組名稱
- 4.Session Pick-UP
- 5.HeartBeat介面指定
- 6.監控介面選擇



High Availability

1 Mode: Active-Active

2 Device Priority: 255

☐ Reserve Management Port for Cluster Member: amc-sw1/1

Cluster Settings

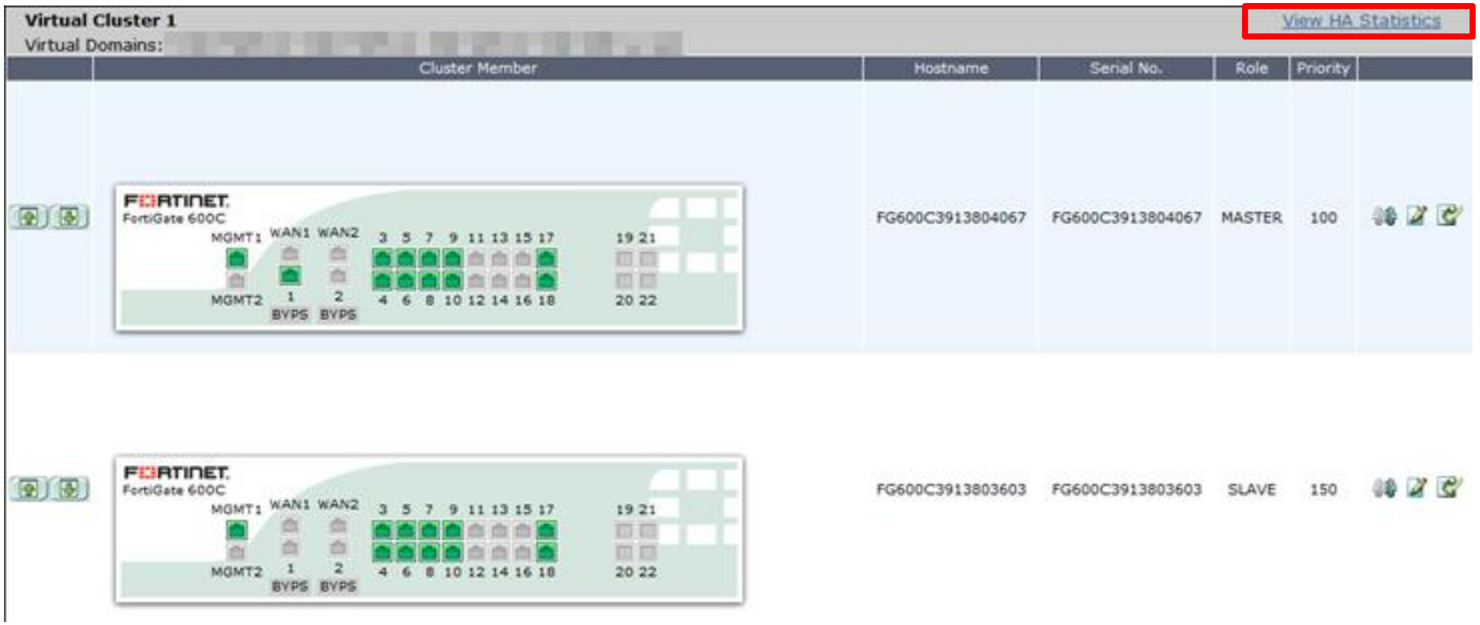
3 Group Name: FortiHA

Password: ●●●●●●

4 ☑ Enable Session Pick-up

	6 Port Monitor	5 Heartbeat Interface	
		Enable	Priority(0-512)
amc-sw1/1	☐	☐	0
amc-sw1/2	☐	☐	0
amc-sw1/3	☐	☐	0
amc-sw1/4	☐	☐	0
port1	☐	☐	0
port2	☐	☑	100
port3	☐	☐	0
port4	☐	☐	0
port5	☐	☐	0

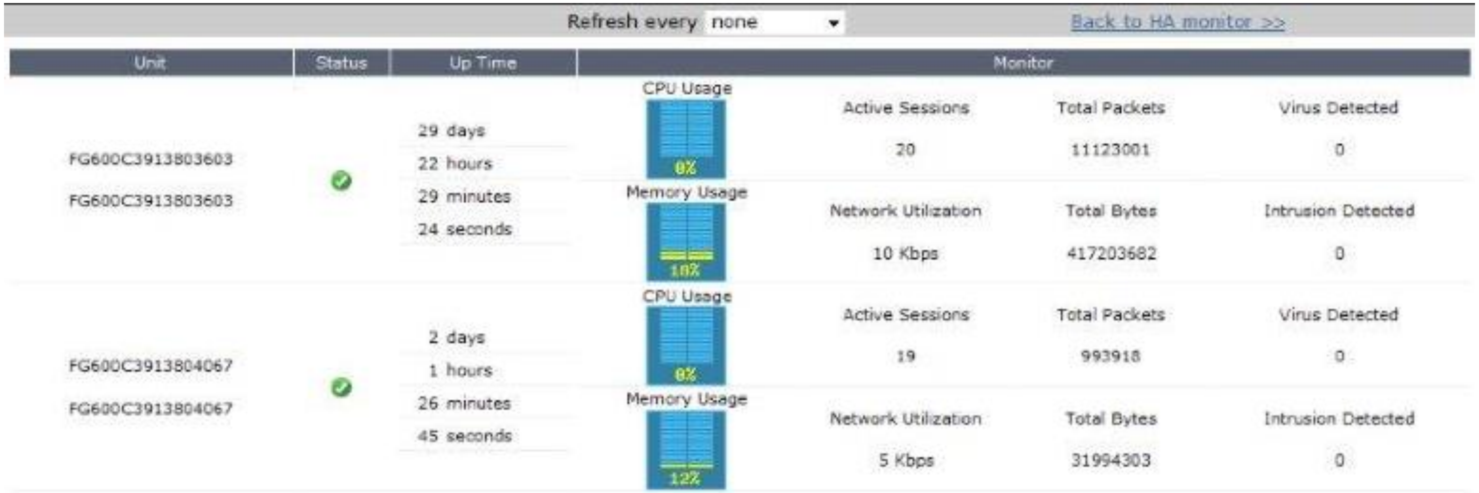
設定防火牆HA功能



Virtual Cluster 1
Virtual Domains: [redacted]

View HA Statistics

	Cluster Member	Hostname	Serial No.	Role	Priority	
	FORTINET FortiGate 600C	FG600C3913804067	FG600C3913804067	MASTER	100	
	FORTINET FortiGate 600C	FG600C3913803603	FG600C3913803603	SLAVE	150	



Refresh every none

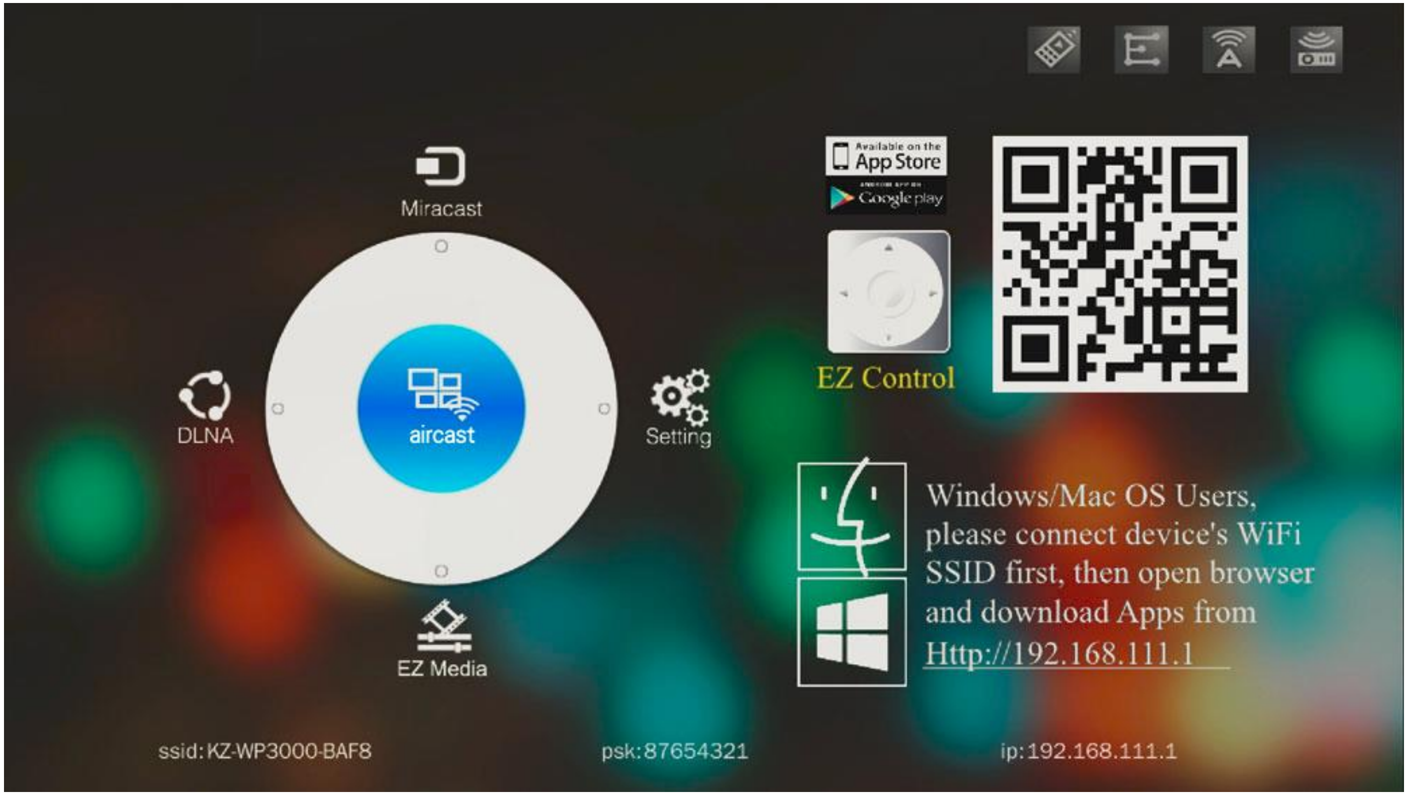
Back to HA monitor >>

Unit	Status	Up Time	Monitor			
FG600C3913803603 FG600C3913803603	✓	29 days 22 hours 29 minutes 24 seconds	CPU Usage 0%	Active Sessions 20	Total Packets 11123001	Virus Detected 0
			Memory Usage 18%	Network Utilization 10 Kbps	Total Bytes 417203682	Intrusion Detected 0
FG600C3913804067 FG600C3913804067	✓	2 days 1 hours 26 minutes 45 seconds	CPU Usage 0%	Active Sessions 19	Total Packets 993918	Virus Detected 0
			Memory Usage 12%	Network Utilization 5 Kbps	Total Bytes 31994303	Intrusion Detected 0

EZ-WP3000

EZ-WP3000

- 設定畫面如圖，使用EZcontrol程式或遙控器操作。
- 點選右邊Setting修改網路設定



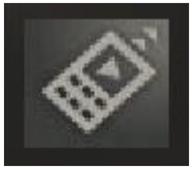
Windows/Mac OS Users, please connect device's WiFi SSID first, then open browser and download Apps from Http://192.168.111.1

ssid: KZ-WP3000-BAF8

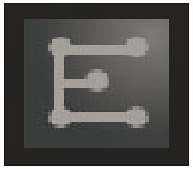
psk:87654321

ip:192.168.111.1

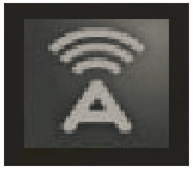
右上角四個狀態圖示



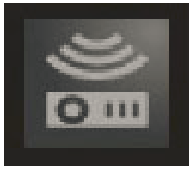
遙控器啟用圖示：預設為開啟，可至Setting→Lan→EZ Remote 關閉



區域網路啟用圖示：連接RJ-45有線網路時會顯示圖示

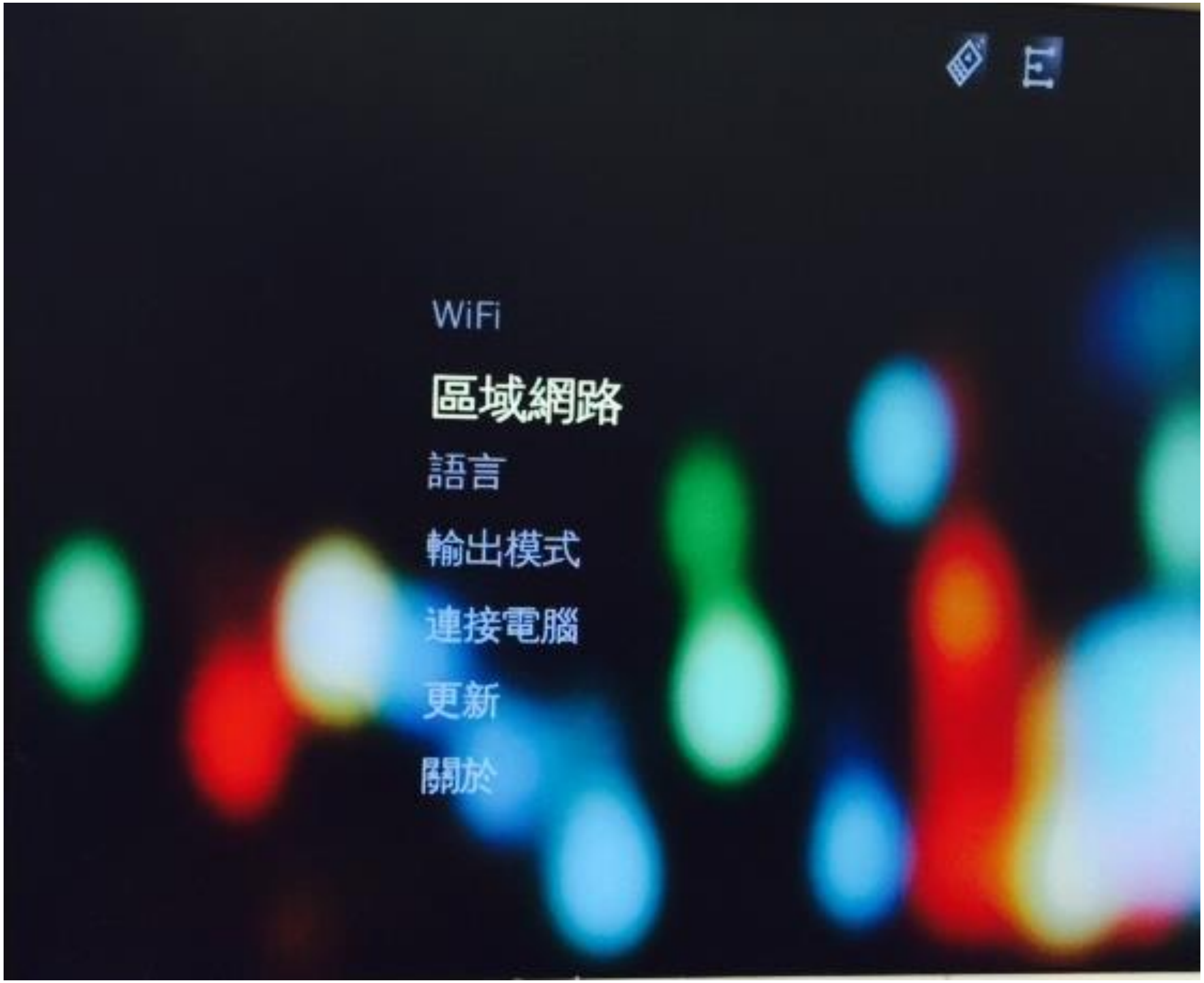


無線Dongle啟用圖示：USB連接無線Dongle時會顯示圖示

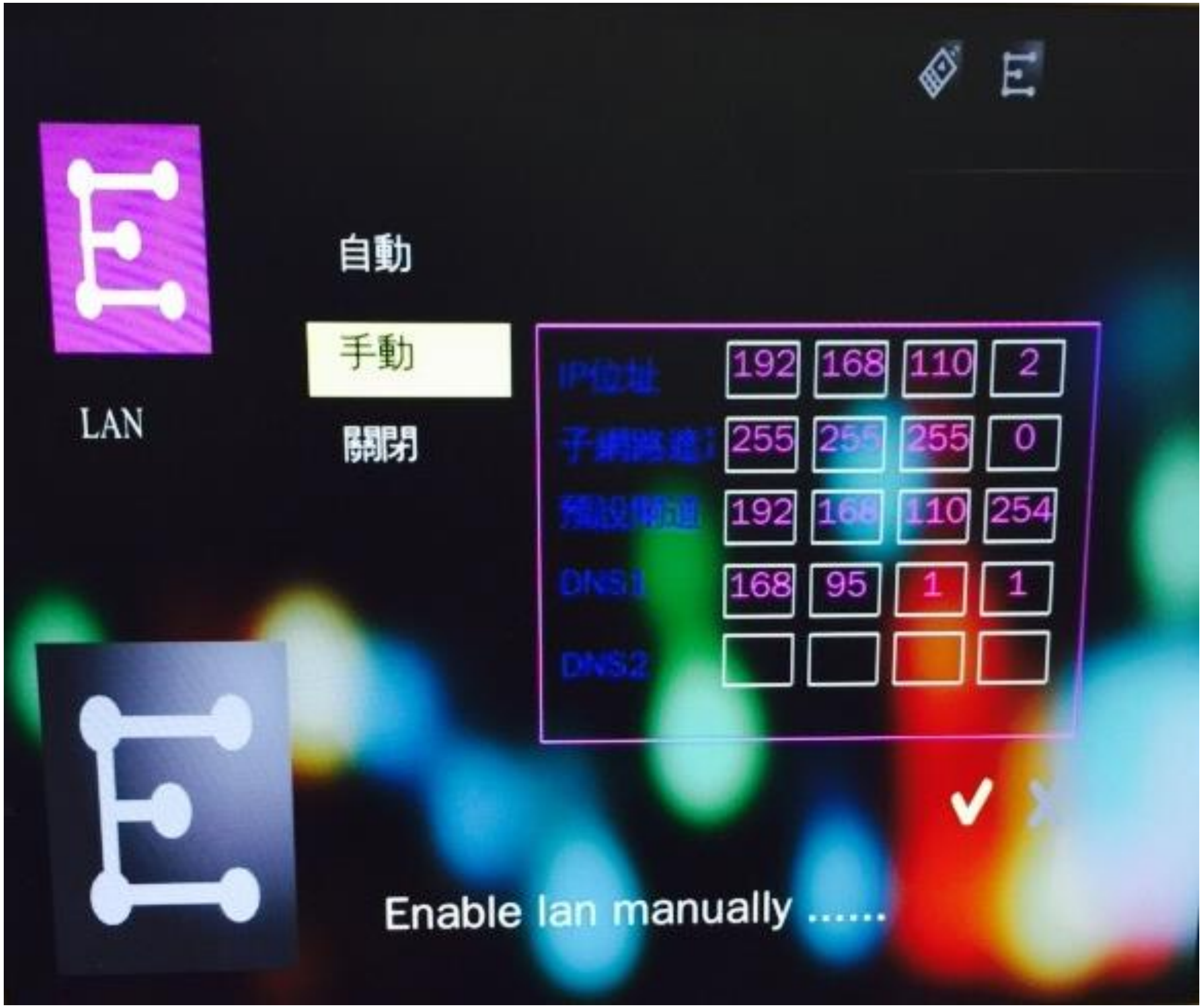


連接無線網路啟用圖示：預設為關閉，於Setting→WiFi 開啟功能

進入區域網路



選擇”手動”設定

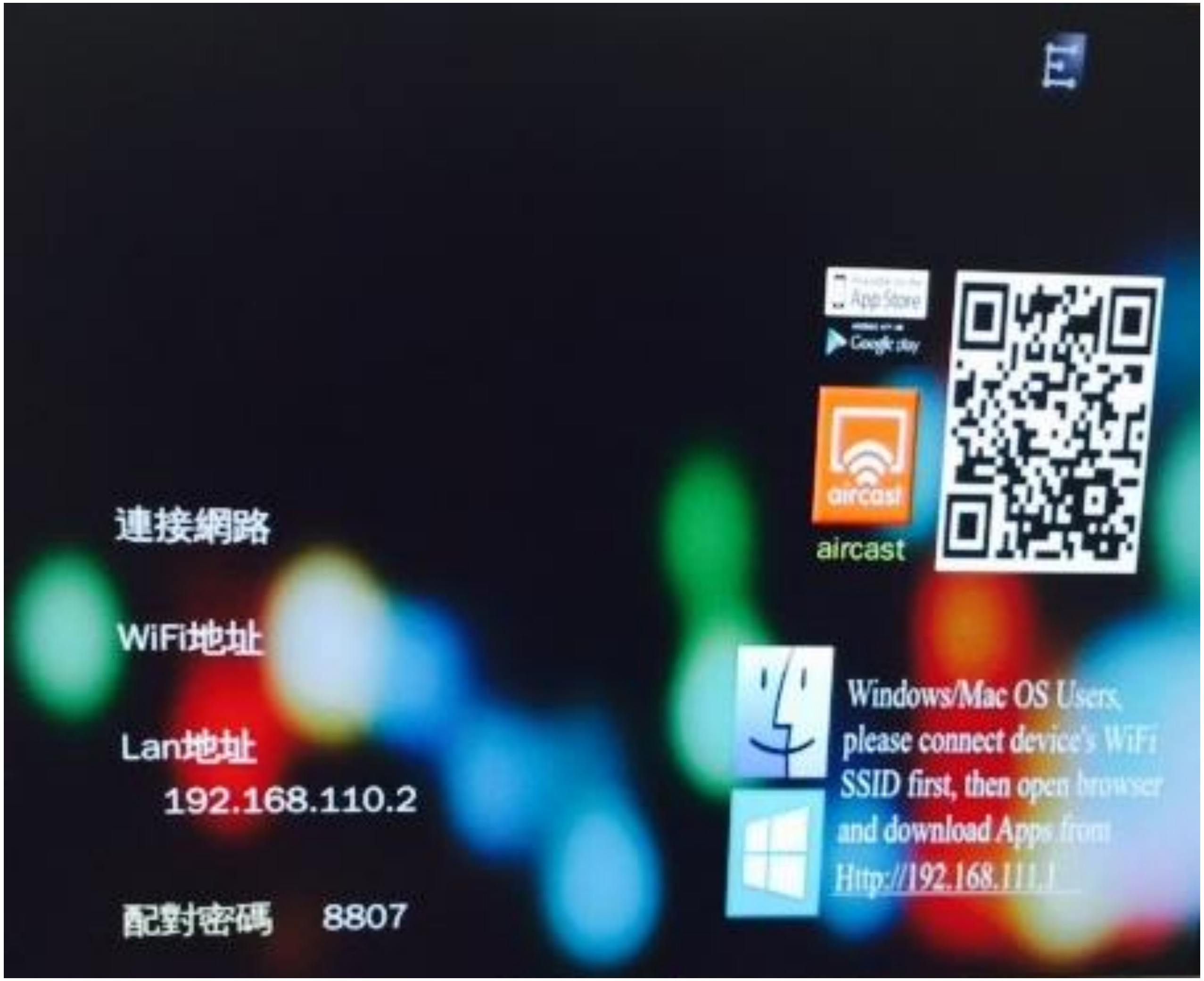


IP位址	192	168	110	2
子網路遮罩	255	255	255	0
預設閘道	192	168	110	254
DNS1	168	95	1	1
DNS2				

✓ ✕

Enable lan manually ......

主畫面確認IP是否正確



連接網路

WiFi地址

Lan地址
192.168.110.2

配對密碼 8807

Windows/Mac OS Users,
please connect device's WiFi
SSID first, then open browser
and download Apps from
Http://192.168.111.1

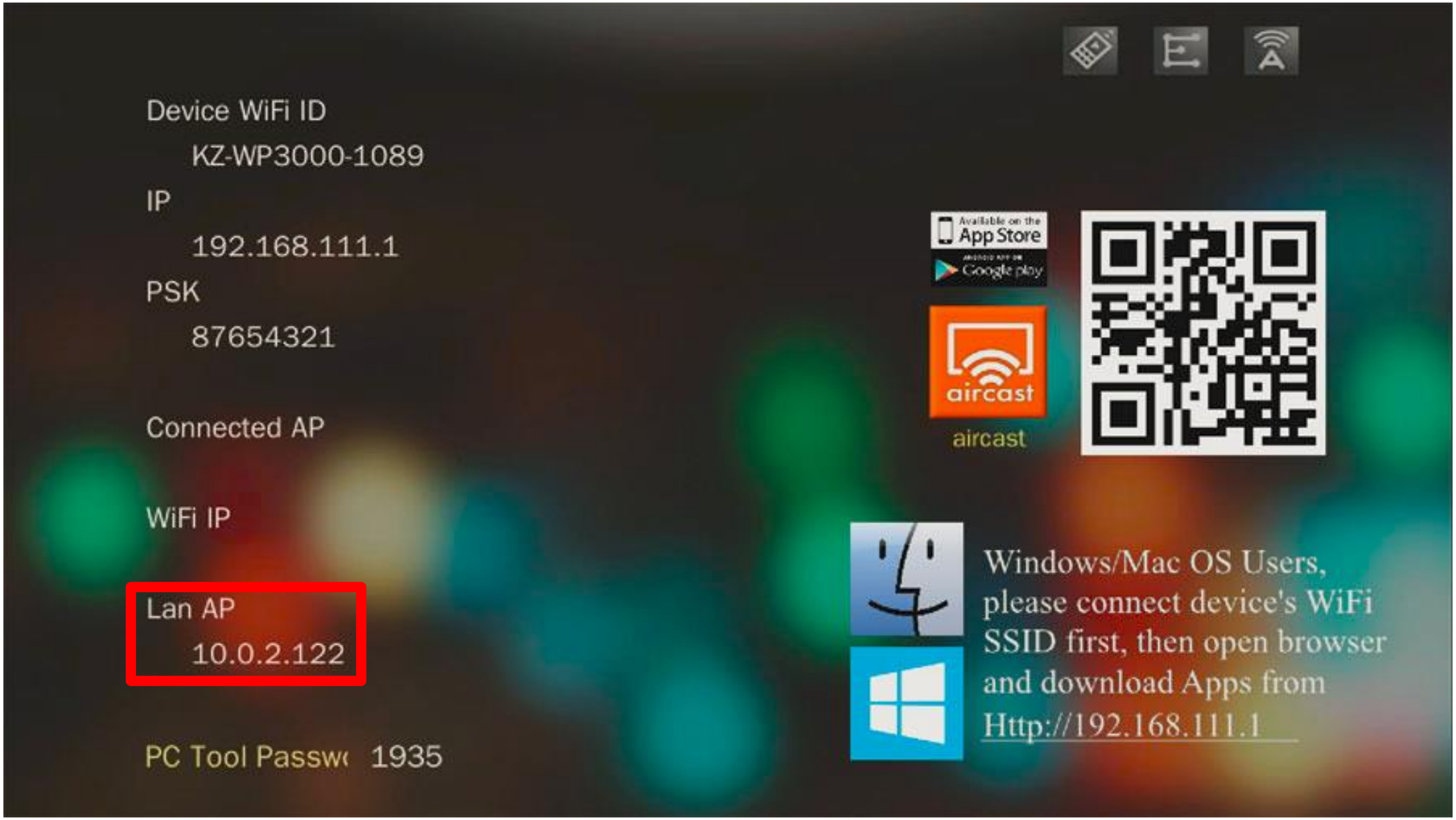
Windows電腦連線操作

- 於aircast等待連線的畫面，開啟任一網頁瀏覽器

- 有線網路：輸入至圖中紅框所顯示的Lan IP位置(需位於同一網段)。

- 無線網路：使用WiFi連線至EZ BOX後（預設密碼為87654321），輸入預設IP位置（192.168.111.1）。

示意圖



Device WiFi ID

KZ-WP3000-1089

IP

192.168.111.1

PSK

87654321

Connected AP

WiFi IP

Lan AP

10.0.2.122

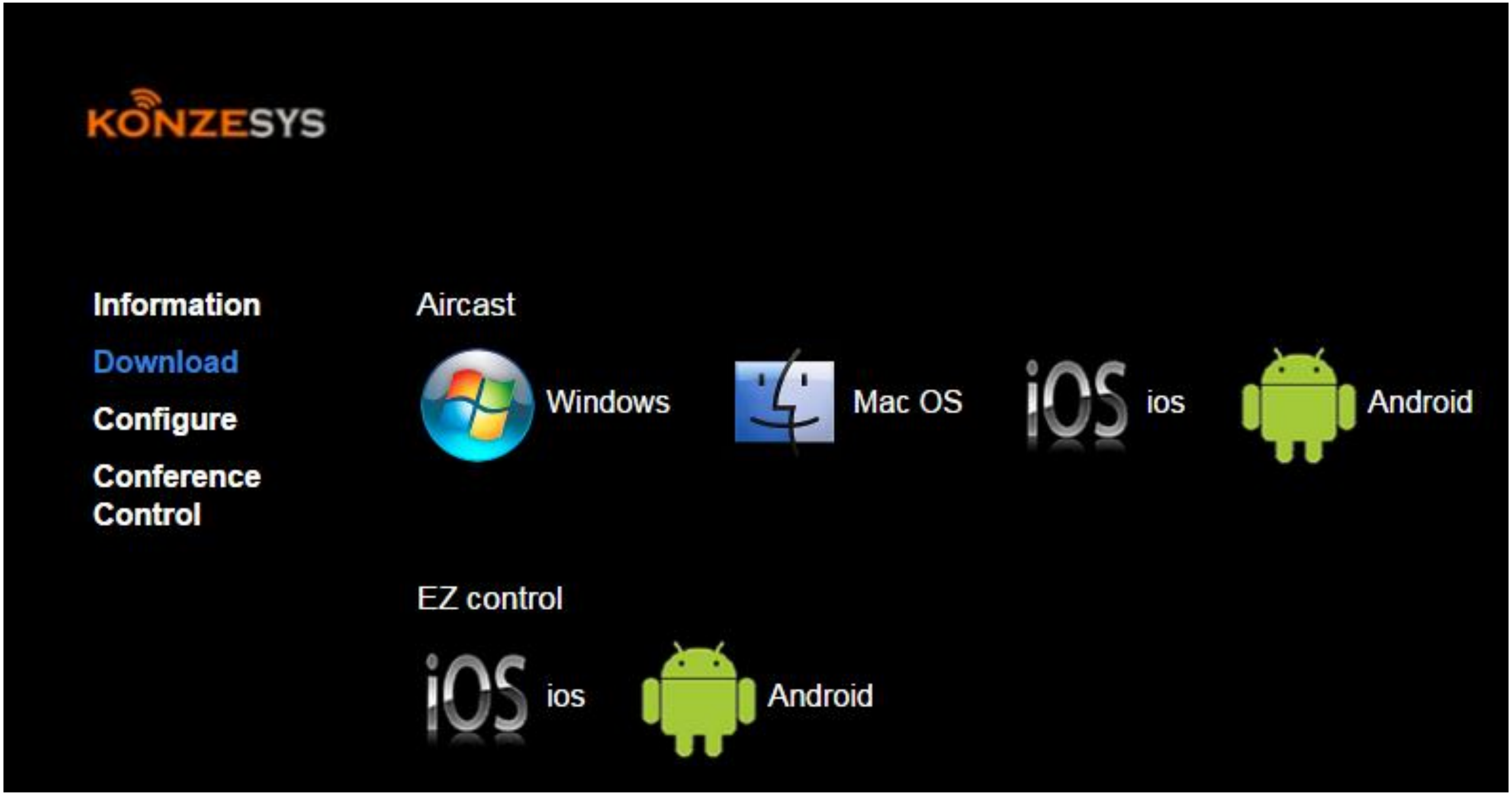
PC Tool Passw(1935

Windows/Mac OS Users, please connect device's WiFi SSID first, then open browser and download Apps from Http://192.168.111.1

下載方式

- 進入EZ Box內置網站程式下載頁面(Lan地址)，下載Windows版aircast程式，亦可至網站(http://www.konzesys.com/aircast_download.html)下載。

內置網站



Information

Download

Configure

Conference Control

Aircast

Windows

Mac OS

ios

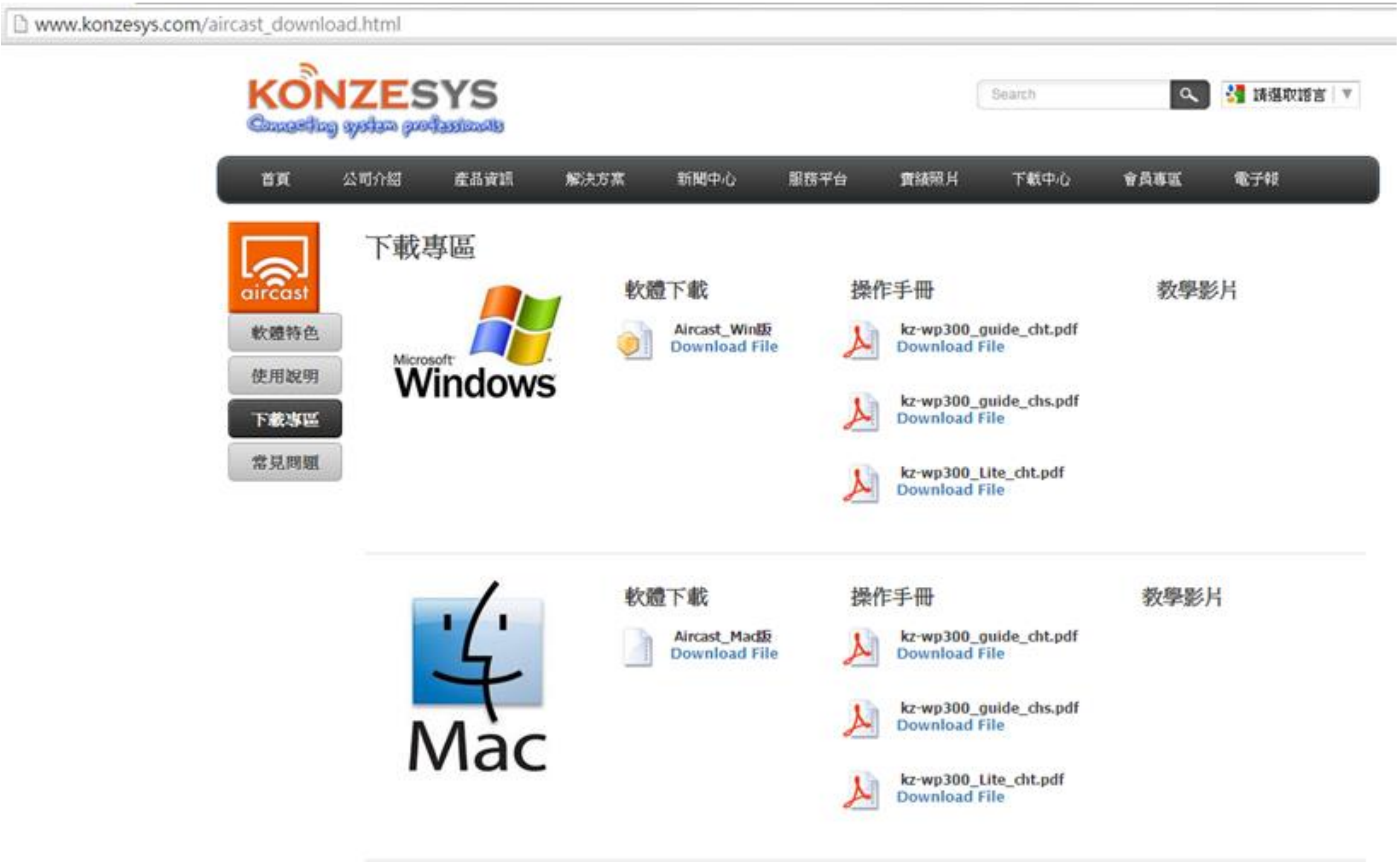
Android

EZ control

ios

Android

官方網站



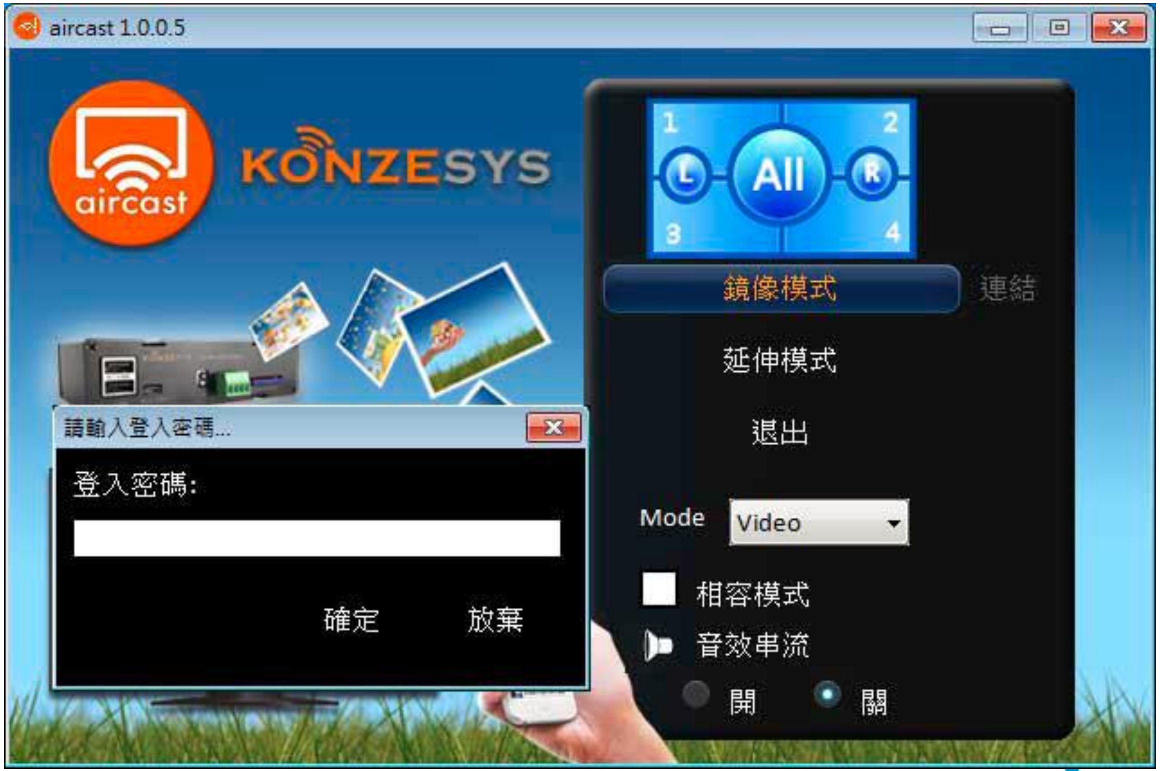
下載專區

軟體下載	操作手冊	教學影片
Aircast_Win版 Download File	kz-wp300_guide_cht.pdf Download File kz-wp300_guide_chs.pdf Download File kz-wp300_Lite_cht.pdf Download File	

軟體下載	操作手冊	教學影片
Aircast_Mac版 Download File	kz-wp300_guide_cht.pdf Download File kz-wp300_guide_chs.pdf Download File kz-wp300_Lite_cht.pdf Download File	

自動搜尋

- 安裝完後執行aircast程式(自動搜尋)，出現輸入登入密碼視窗，請輸入aircast等待連線的畫面中〝PassCode〞四位數字。



請輸入登入密碼...

登入密碼:

確定　放棄

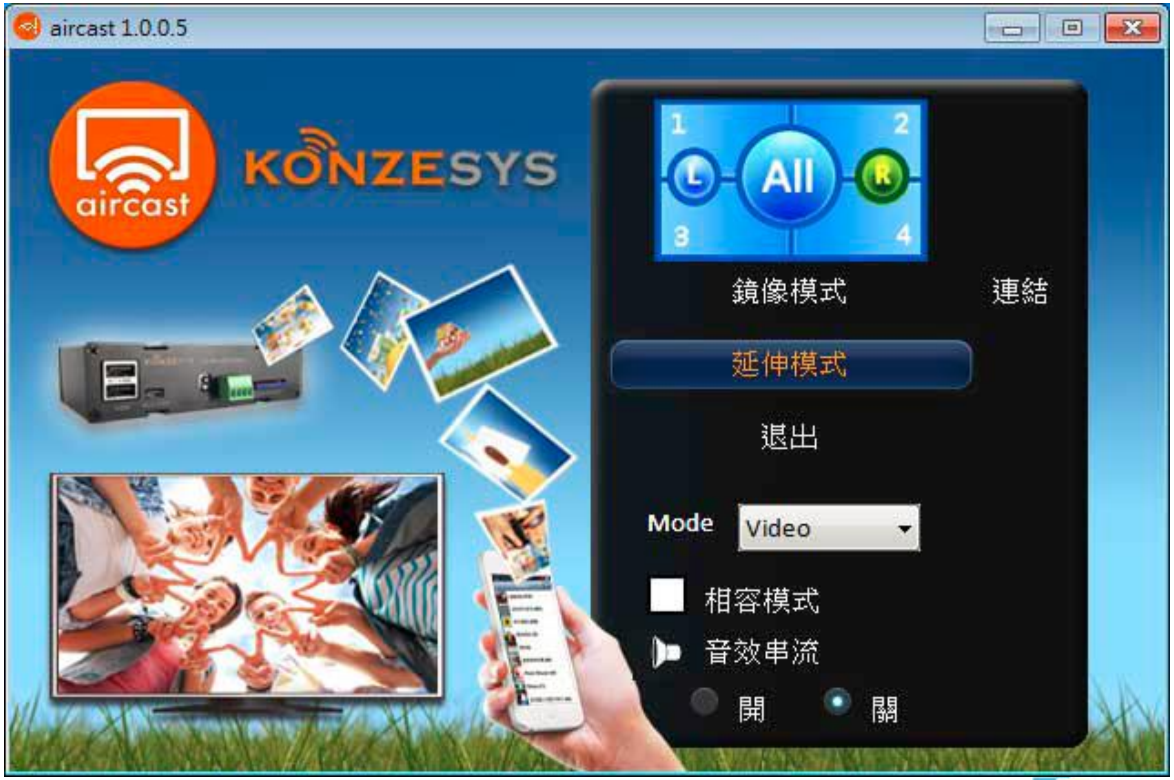
Mode　Video

□ 相容模式

音效串流　○ 開　● 關

畫面分割

- 登入後會將目前電腦畫面同步輸出至輸出裝置，可於右邊分割螢幕中選擇分割，有單畫面(ALL)、雙畫面(L R)以及四分割(1 2 3 4)。



Mode Video

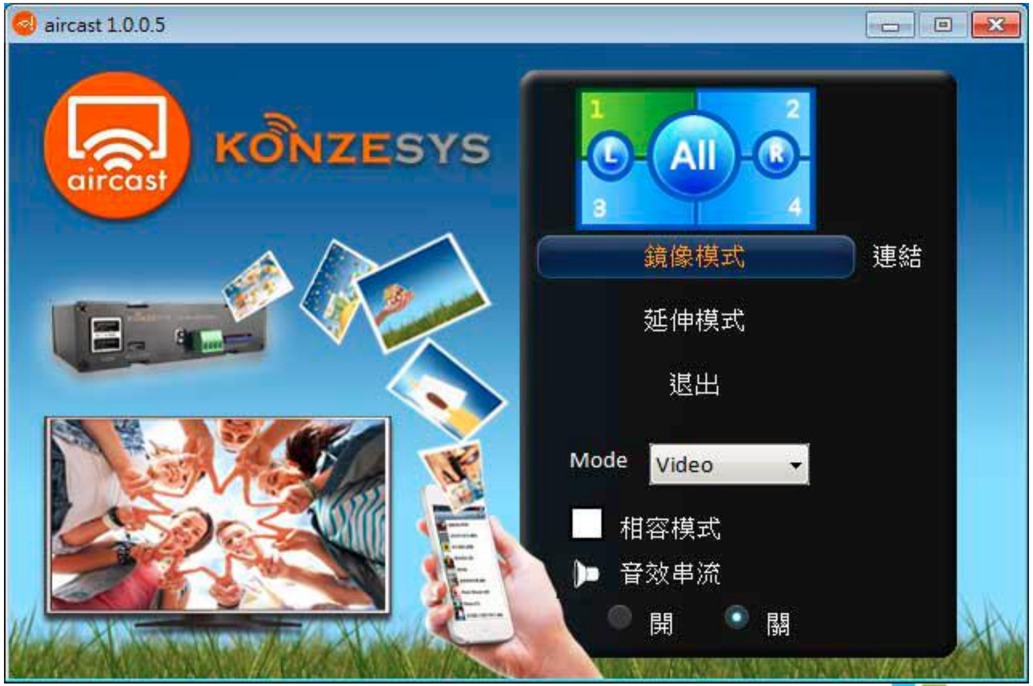
□ 相容模式

音效串流

○ 開 ● 關

畫面模式

- 鏡像模式：將電腦畫面同步輸出至螢幕上。
- 延伸模式：將電腦畫面做延伸至螢幕上。
- 退出：離開程式。



Mode Video

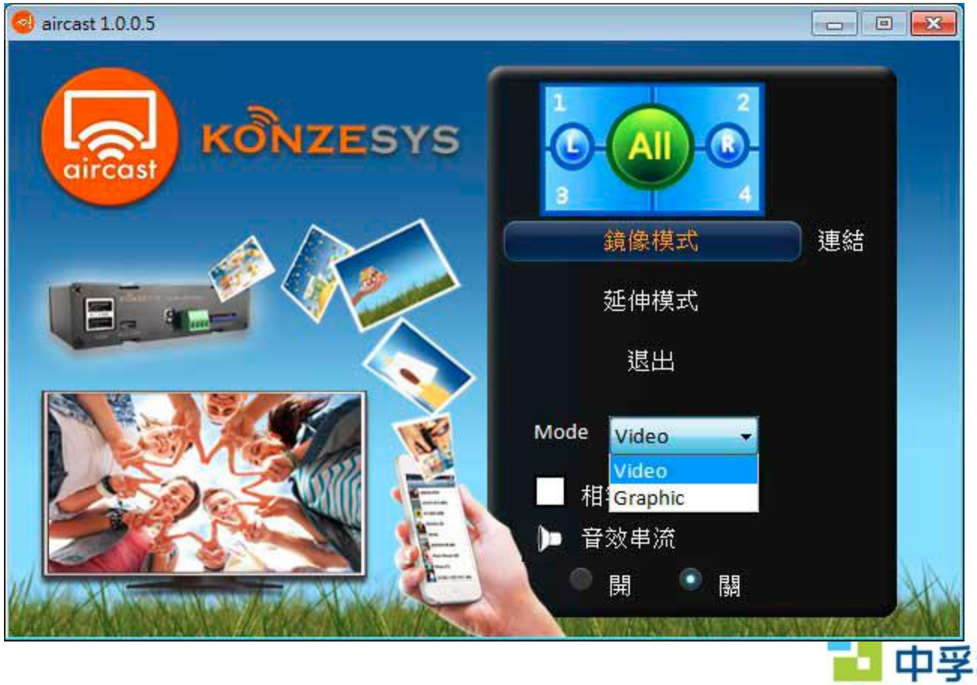
□ 相容模式

音效串流

○ 開 ● 關

畫面類型

- Video：為影片直接傳輸，頻寬流量較大。
- Graphic：為擷取畫面為圖片傳輸，頻寬流量較小。
- 相容模式：Windows Aero 色彩配置相容性。
- 音效串流：控制聲音是否傳輸。



Mode Video

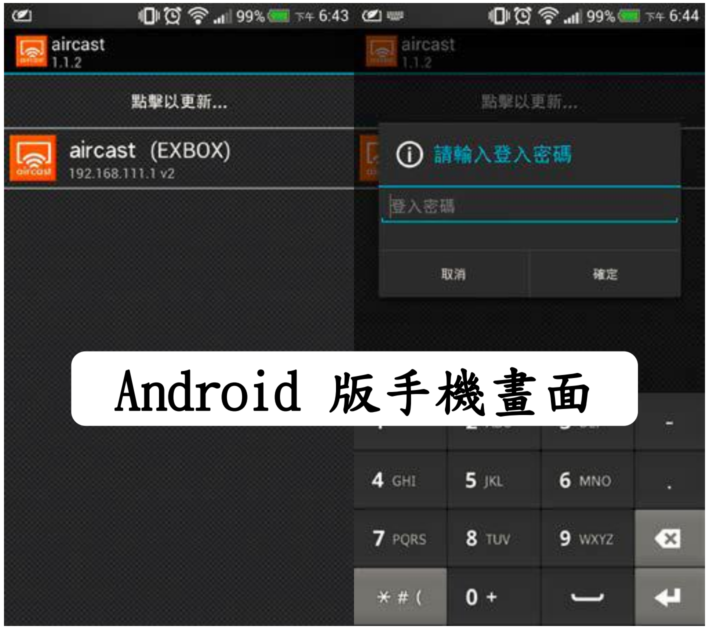
□ 相

音效串流

○ 開 ● 關

手持裝置連線操作

- Android 系統請至Play Store ，Apple 系統請至App Store 免費下載aircast
- 開啟aircast，選擇要連線的EZ Box後，出現輸入登入密碼視窗 ，請輸入
- aircast等待連線的畫面中〝PassCode〞四位數字。


aircast 1.1.2

點擊以更新...

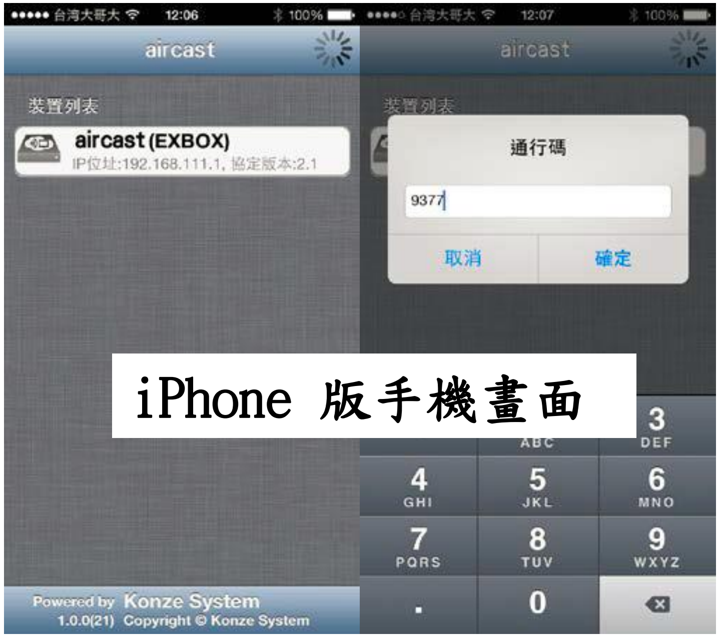
aircast (EXBOX)
192.168.111.1 v2

請輸入登入密碼

登入密碼

取消 確定

Android 版手機畫面


aircast

裝置列表

aircast (EXBOX)
IP位址:192.168.111.1, 協定版本:2.1

通行碼

9377

取消 確定

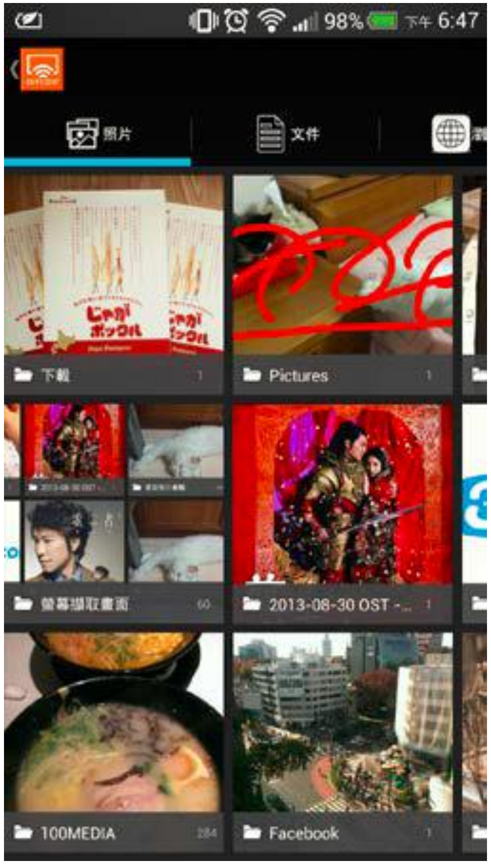
Powered by Konze System
1.0.0(21) Copyright © Konze System

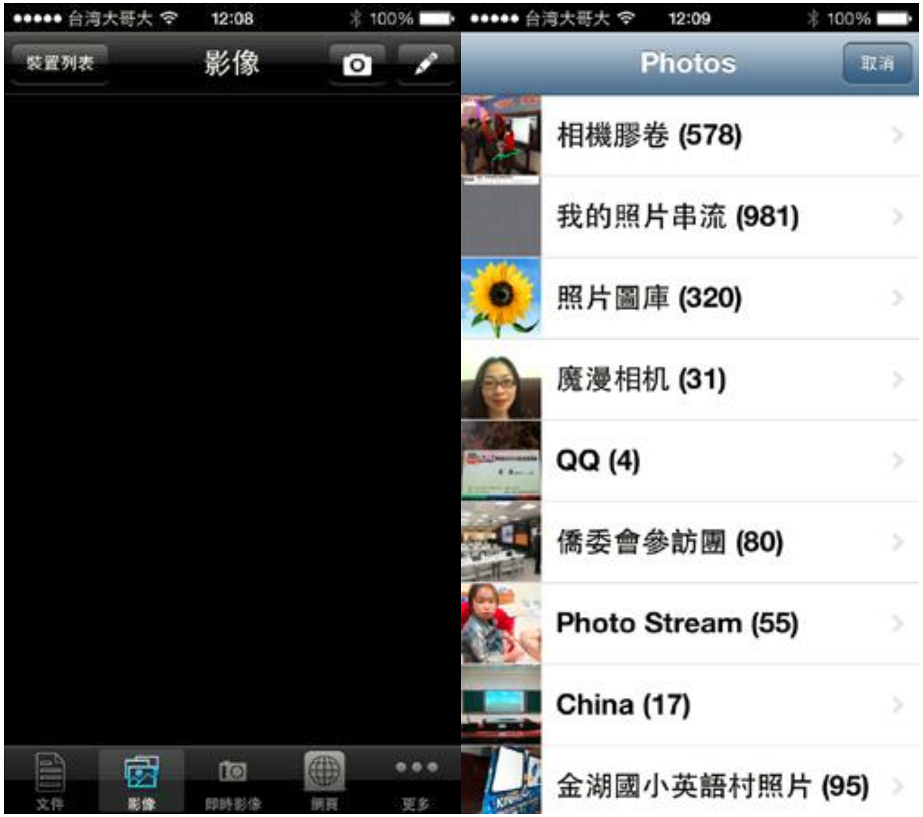
iPhone 版手機畫面

登入後有七個功能選項：

- 照片(影像)：開啟圖片後畫面會投影至輸出裝置

Android 版直接開啟相簿選擇圖片　Apple 版點選按鍵後開啟相簿選擇圖片

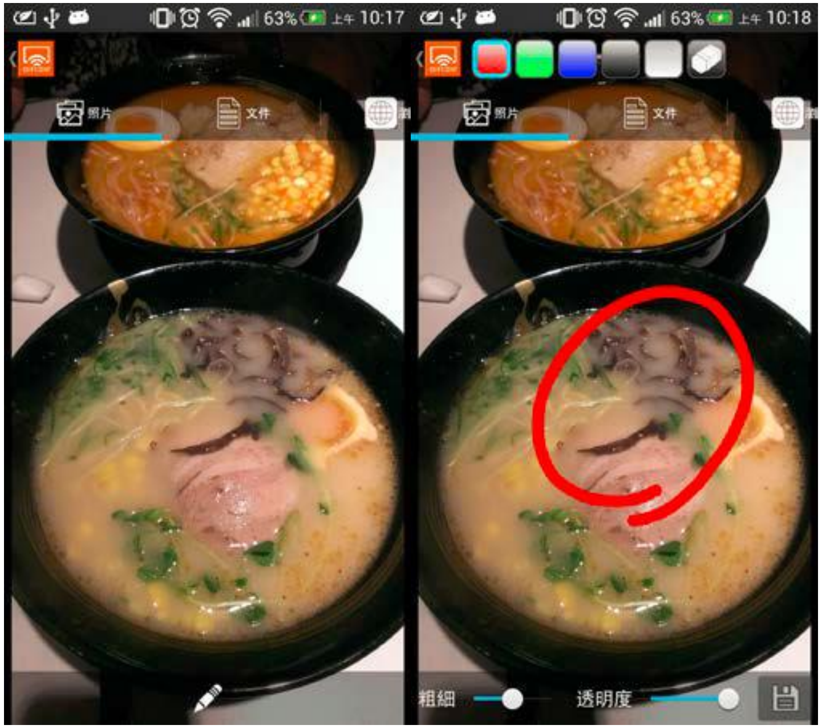




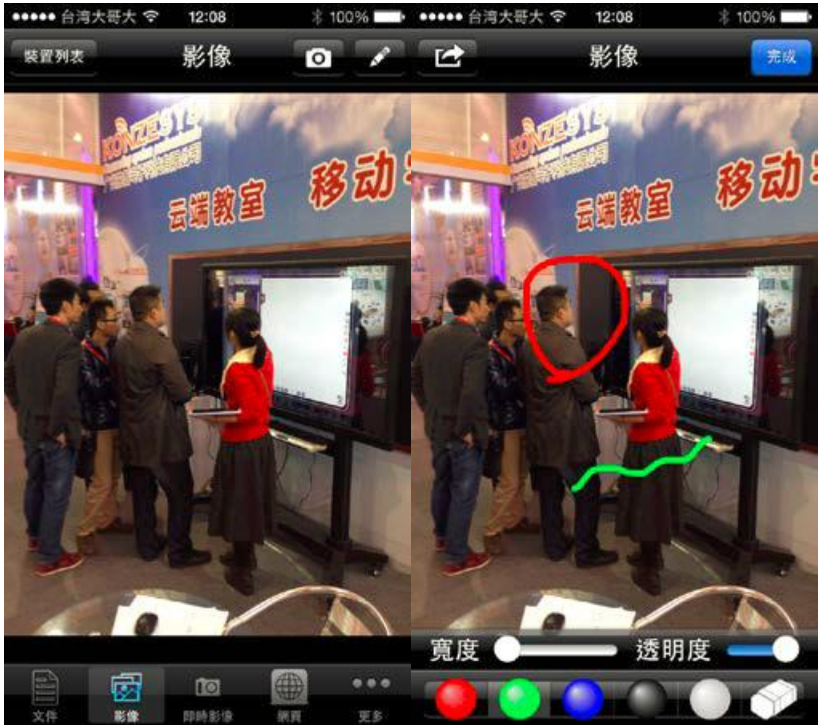
圖片工具

- 點選圖片中筆型工具可進入白板模式，可在圖片中書寫，亦可選擇筆畫粗細、顏色、透明度、橡皮擦功能及存檔成圖片。

Android 版手機畫面

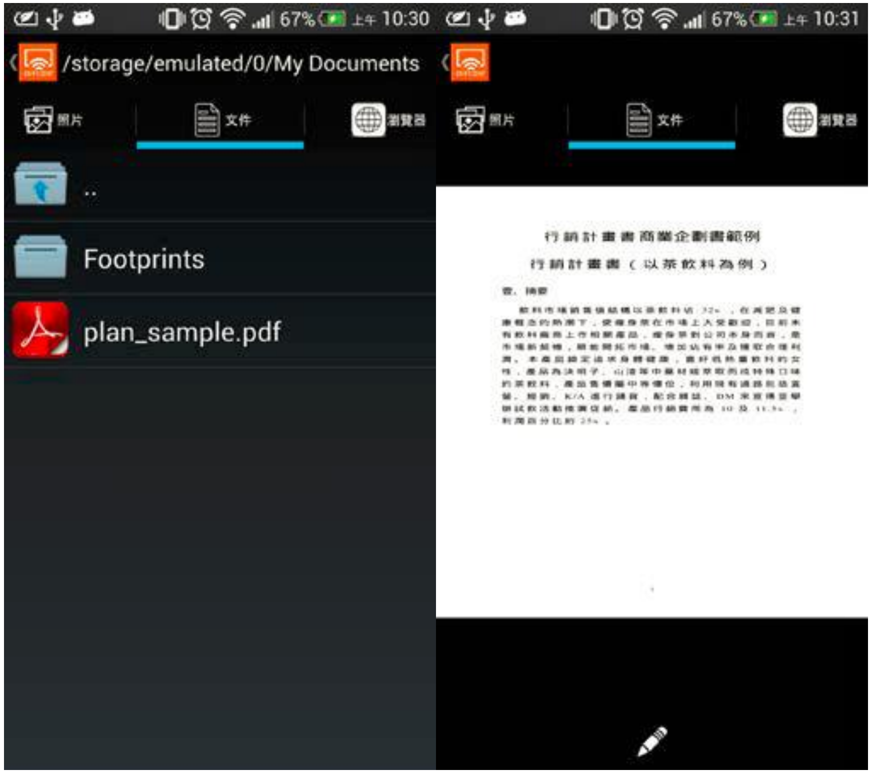


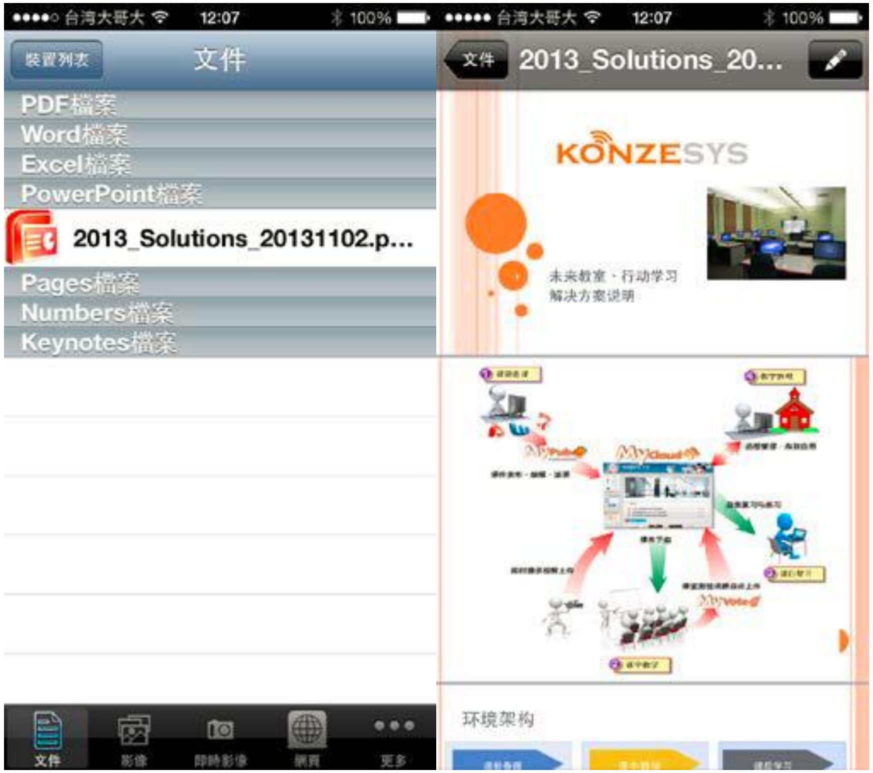
iPhone 版手機畫面



開啟文件投影至輸出裝置

Android 版開啟檔案總管選擇文件　Apple 版直接顯示裝置中可支援文件

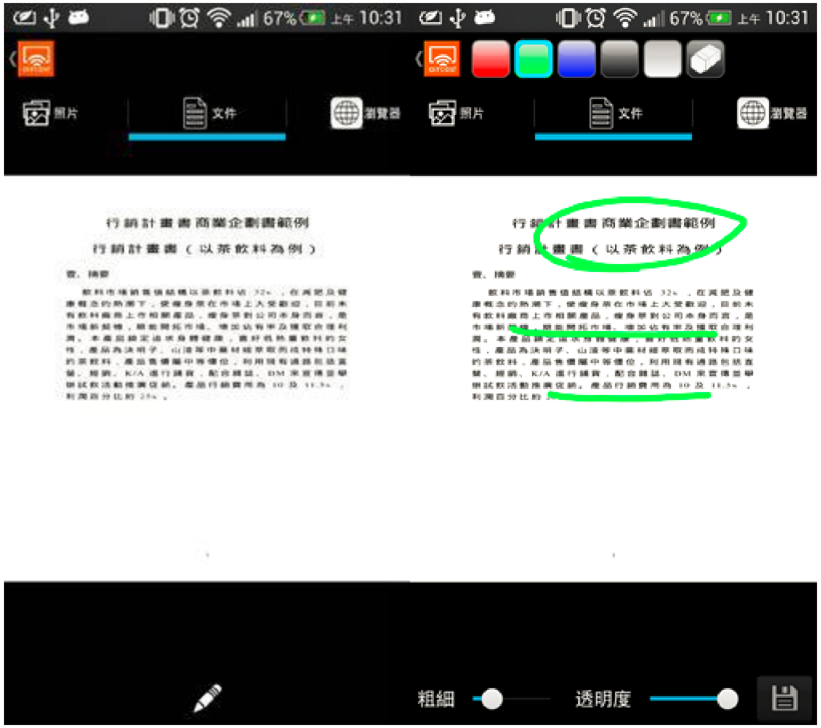




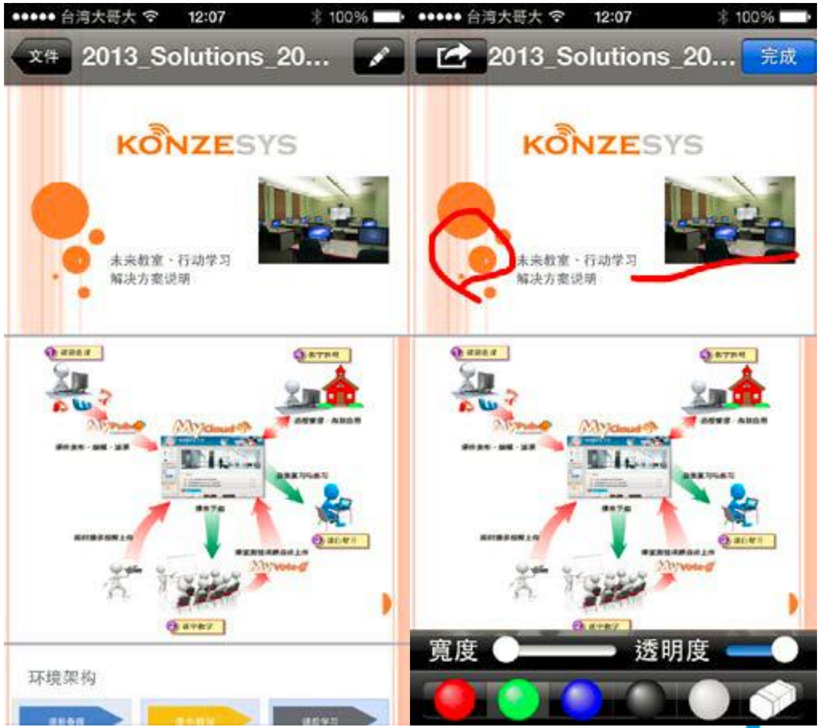
文件工具

- 點選文件中筆型工具可進入白板模式，可在文件中書寫，亦可選擇筆畫粗細、顏色、透明度、橡皮擦功能及存檔成圖片。

Android 版手機畫面



iPhone 版手機畫面



Q&A