



管理課程



Enterprise Grade Security

企業級防護



1996



Performance

效能



Simplicity

簡單



Visibility

可視性



Future Proof

未來發展



WatchGuard 管理工具

1. Web UI 管理 https://firewall_ip:8080
2. WatchGuard System Manager (WSM) 專屬管理軟體
 - WatchGuard Policy
 - Traffic Monitor
 - Host Watch
3. WatchGuard Dimension Reporting System

WatchGuard System Manager 安裝



Step 1 :

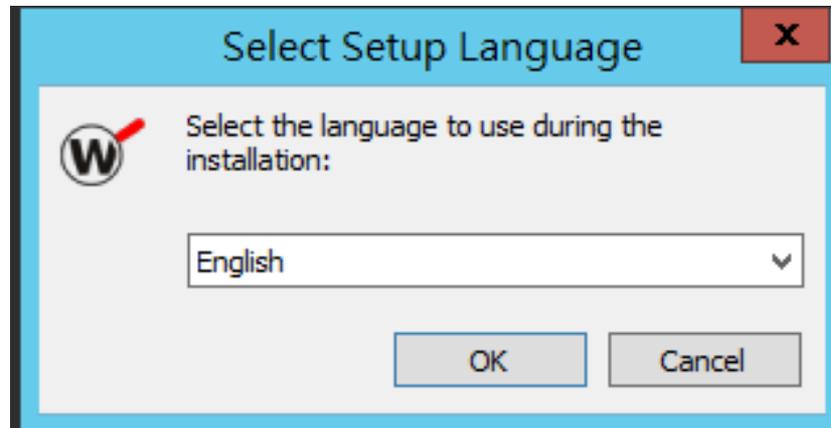
執行WSM安裝軟體

WSM軟體僅可安裝於Windows OS

WatchGuard System Manager 安裝

Step 2 :

軟體安裝語言請選“英文”



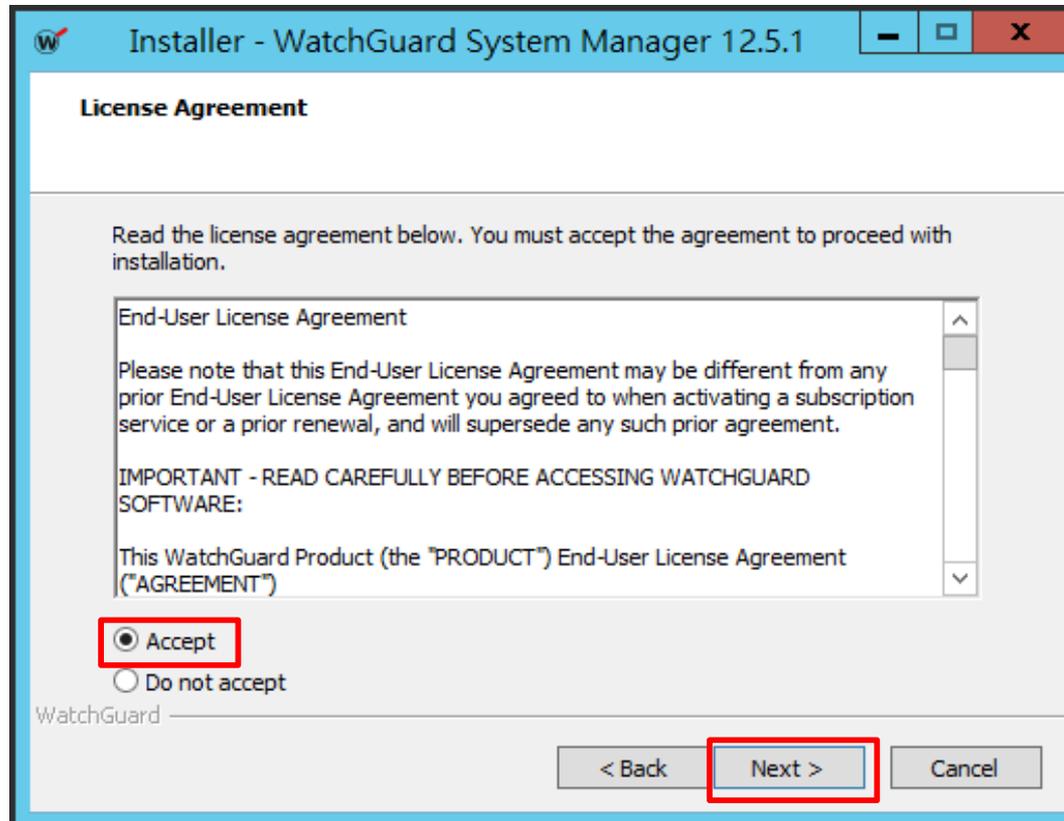
WatchGuard System Manager 安裝



Step 3 :

點選“Next”開始進行安裝精靈

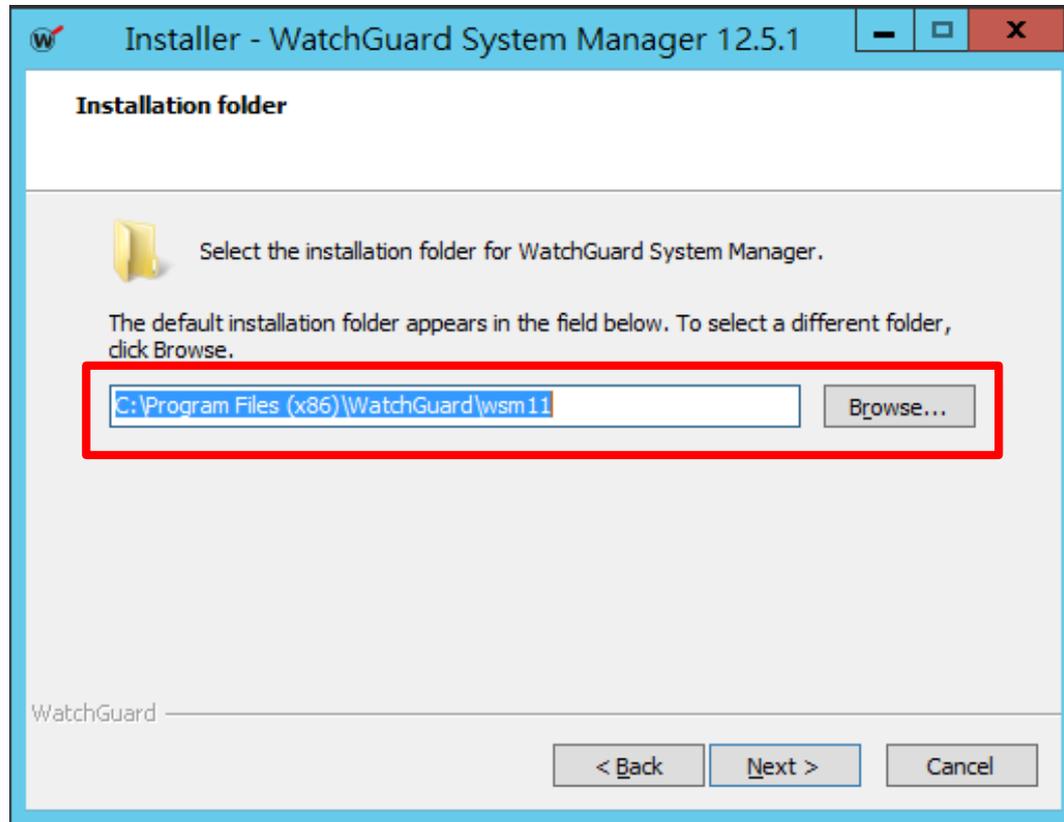
WatchGuard System Manager 安裝



Step 4 :

點選“Accept”接受合約內容，並點選“Next”下一步

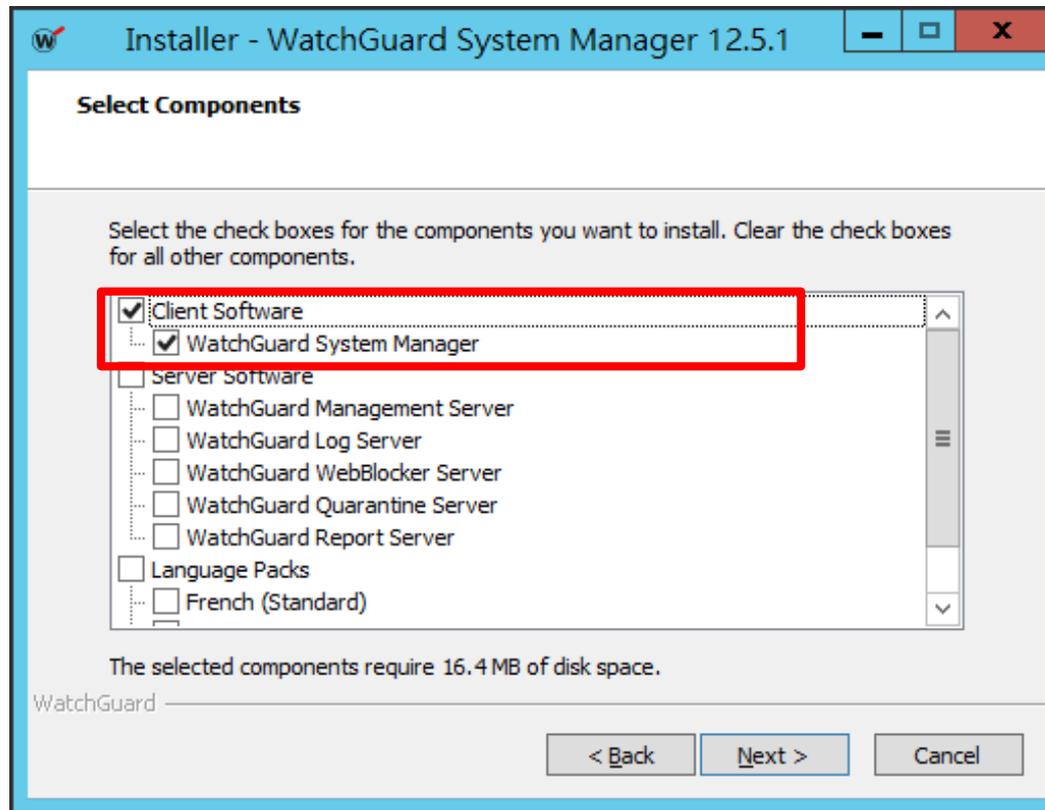
WatchGuard System Manager 安裝



Step 5 :

選擇安裝路徑，可以使用預設路徑也可以自訂路徑安裝

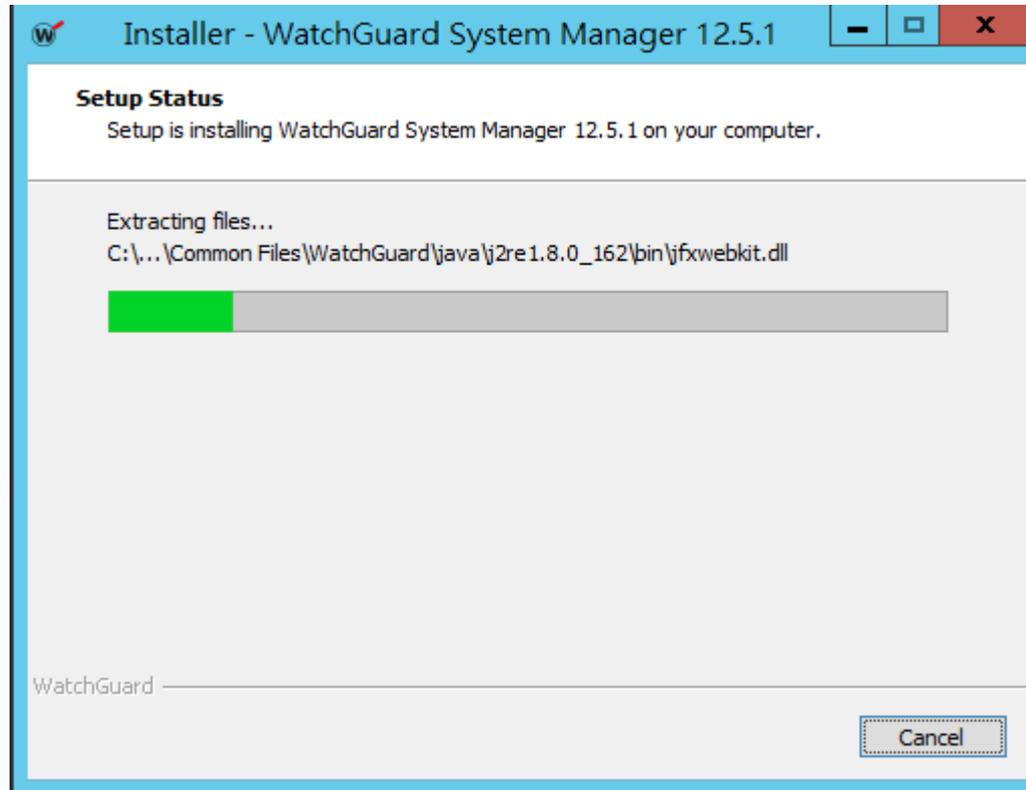
WatchGuard System Manager 安裝



Step 6 :

只需要選擇安裝第一個選項”WatchGuard System Manager”

WatchGuard System Manager 安裝



Wait For Installation

執行WSM

WatchGuard System Manager 12.5.1



Documentation 12.5.1



Quick Setup Wizard 12.5.1 新增



WatchGuard System Man... 新增

安裝完成後在程式集中將出現
WatchGuard System Manager
點選此Icon開啟WSM

WSM Icon說明

Connect to Device

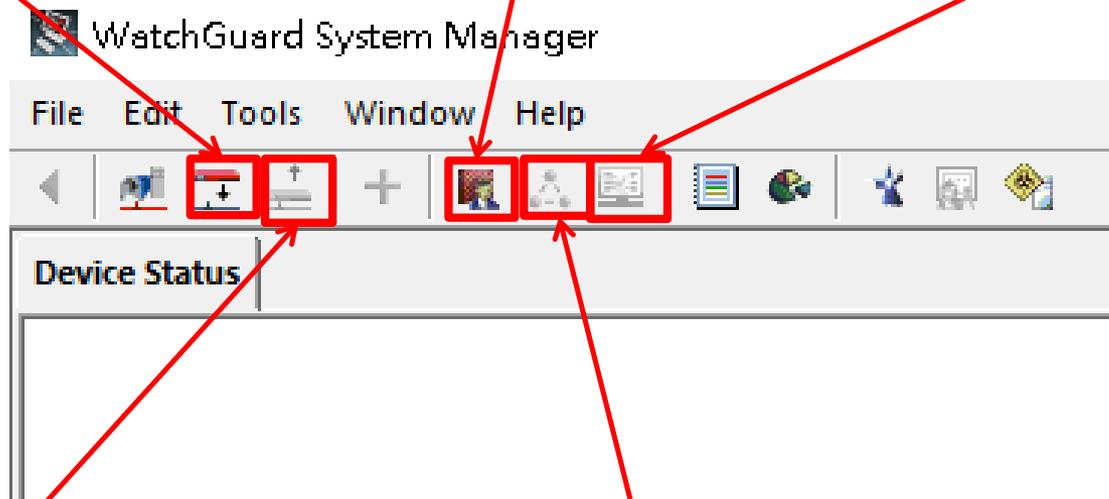
連線至防火牆，如需要設定或是監控防火牆請點選此Icon

Policy Manager

設定防火牆政策點選此Icon

Host Watch

繪製出通過防火牆流量的連線圖表



Disconnect

中斷WSM和防火牆中間的連線

Firebox System Manager

透過此功能可察看防火牆狀態以及網路流量狀態等等連線資訊。

Firebox Interface 預設 IP



Eth0 External
IP : 10.0.0.1

Eth1 Trusted
IP : 10.0.1.1
預設啟動DHCP

Eth2 Optional
IP : 10.0.2.1

External Eth0 是無法管理WatchGuard，其餘介面皆可連線管理設定防火牆。

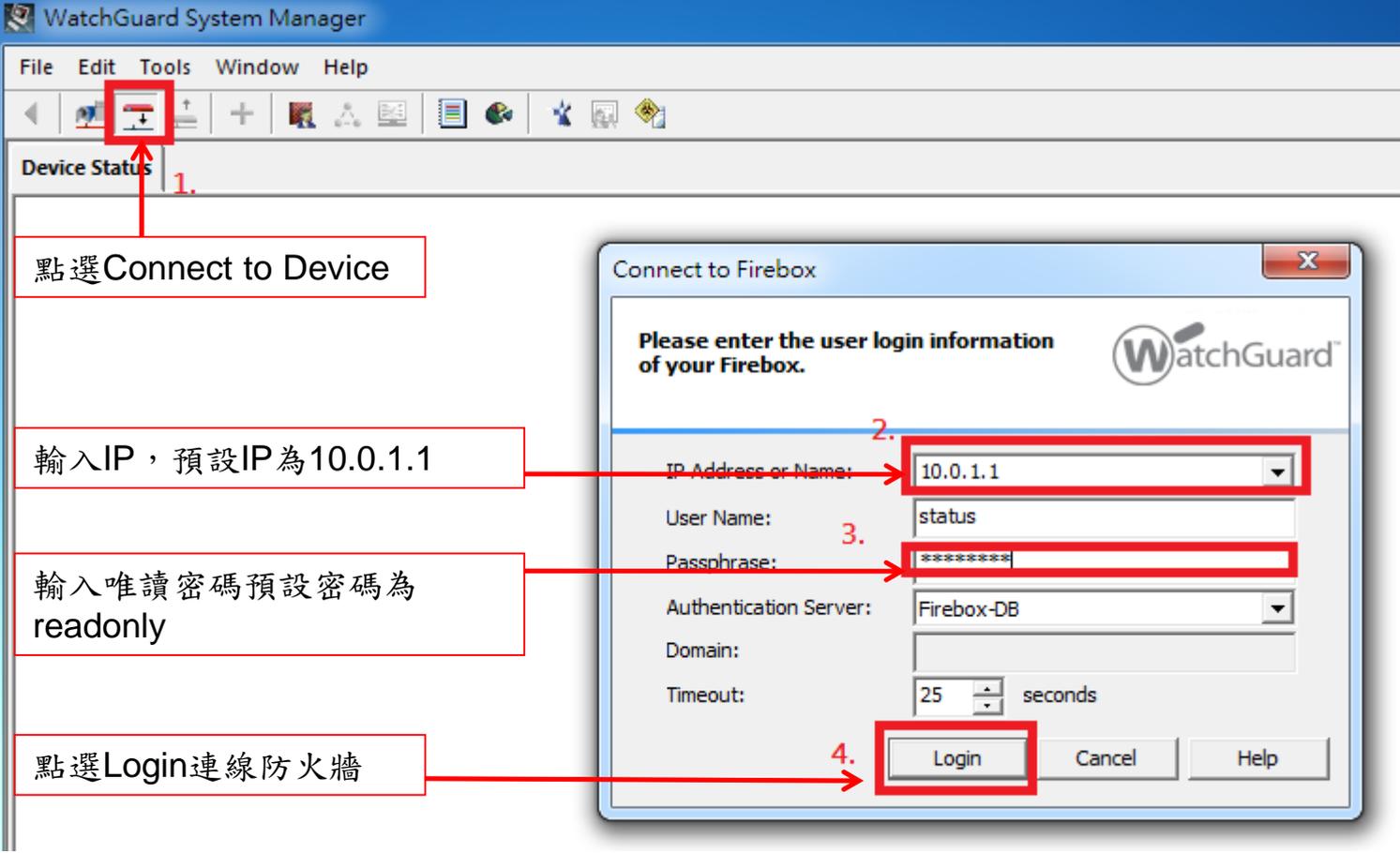
連線管理Firebox Firewall



Notebook設定網路卡IP為
10.0.1.2/24 連接至防火牆Eth1進行
設定



使用WSM連線管理Firewall



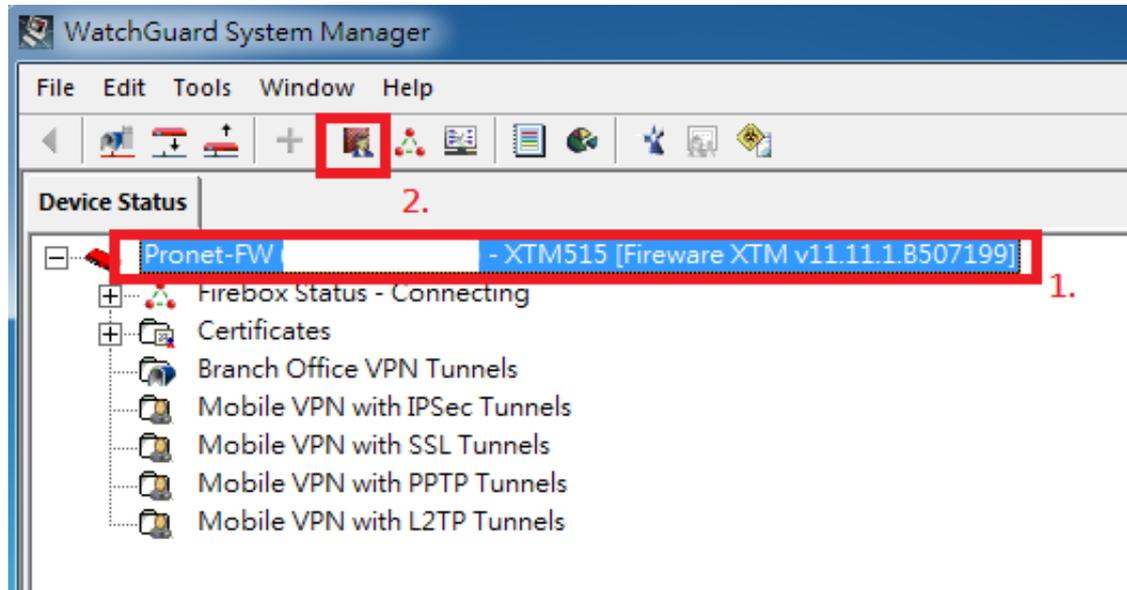
1. 點選Connect to Device

2. 輸入IP，預設IP為10.0.1.1

3. 輸入唯讀密碼預設密碼為readonly

4. 點選Login連線防火牆

開啟Firewall Policy Manager



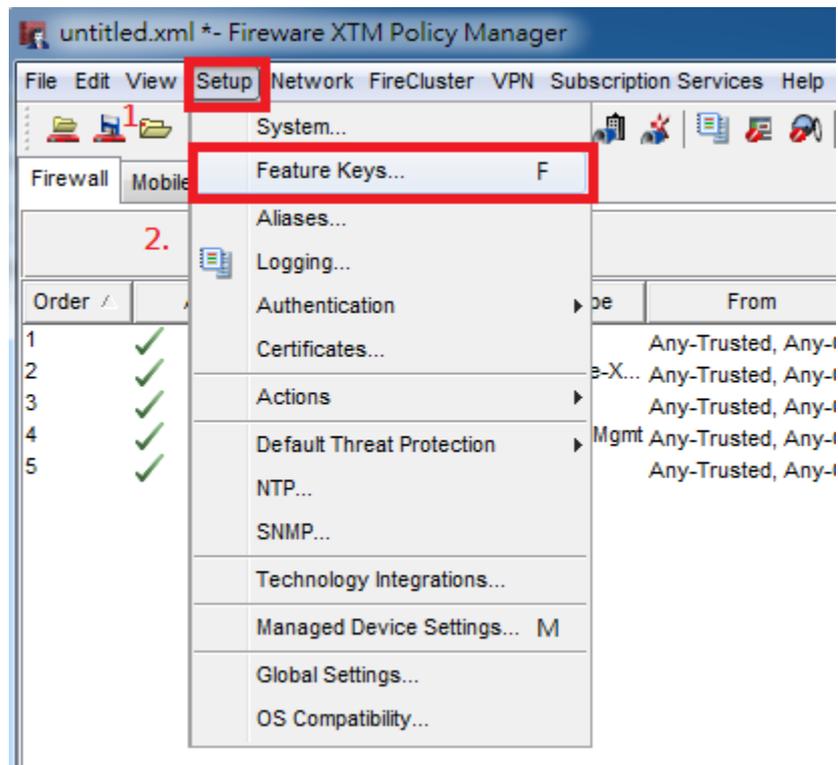
連線防火牆後

1.點選防火牆

2.點選Policy Manager進行防火牆政策設定

Note：必須先點選一下要設定的防火牆再點選Policy Manager否則不會進到您要設定的防火牆中

匯入 Feature Key

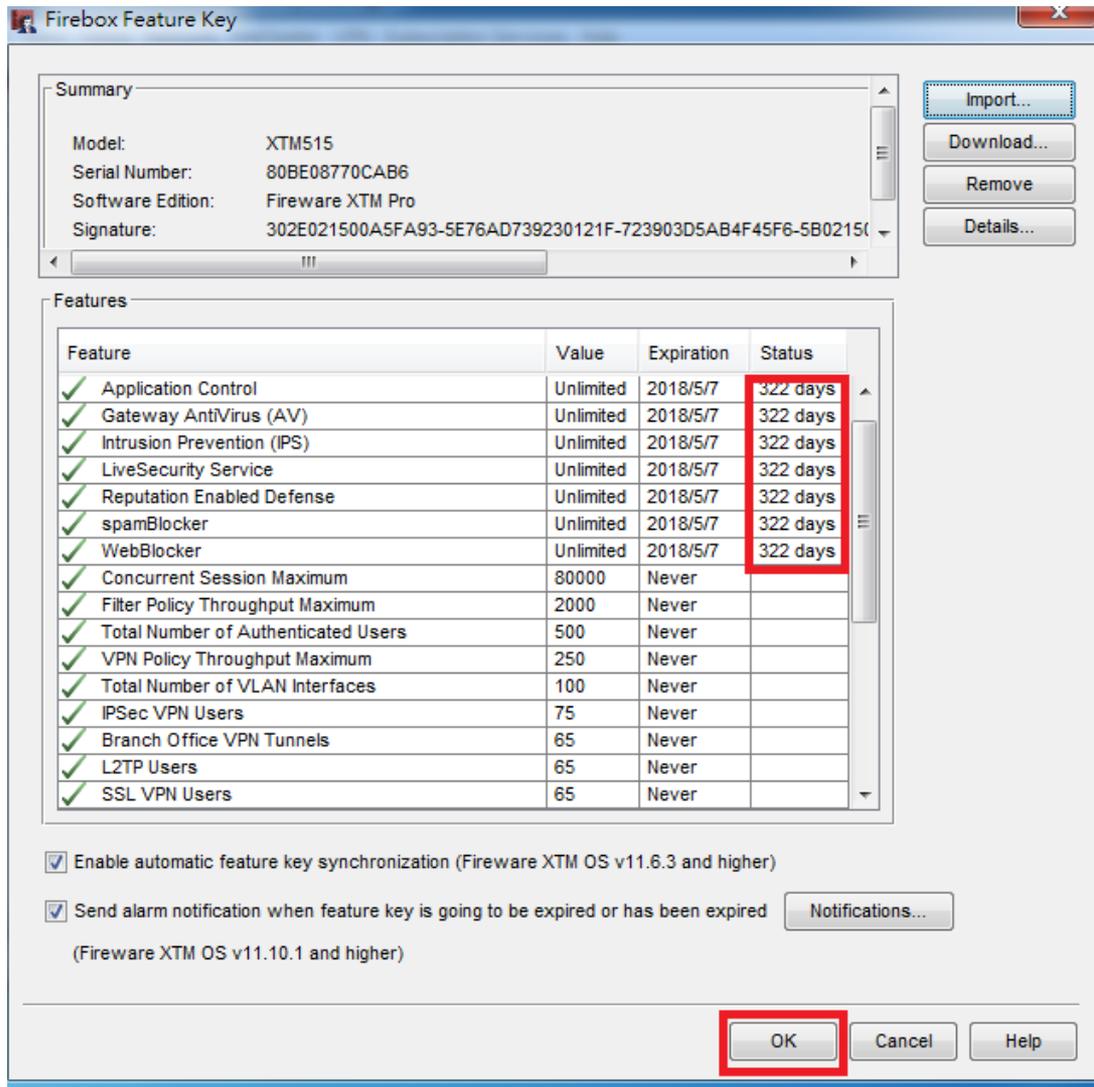


Step 1 :

點選 Setup → Feature Keys

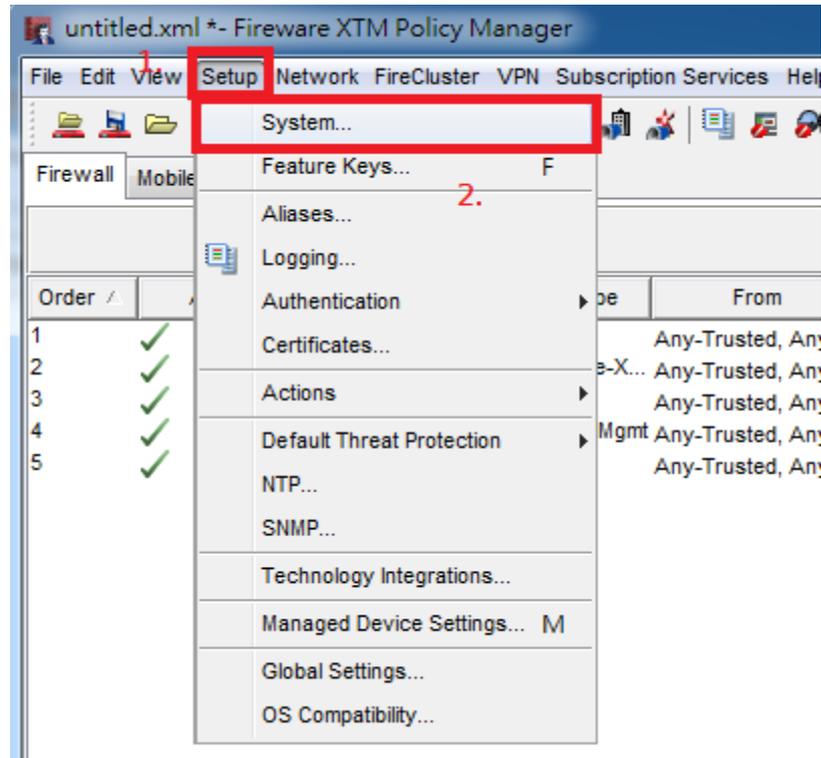
Note : WatchGuard 必須要貼上 Feature Key 才能正常運作

確認 Feature Key



1. Feature Key貼上後確認 License到期的時間是否正確
2. 點選OK

設定時區及防火牆名稱

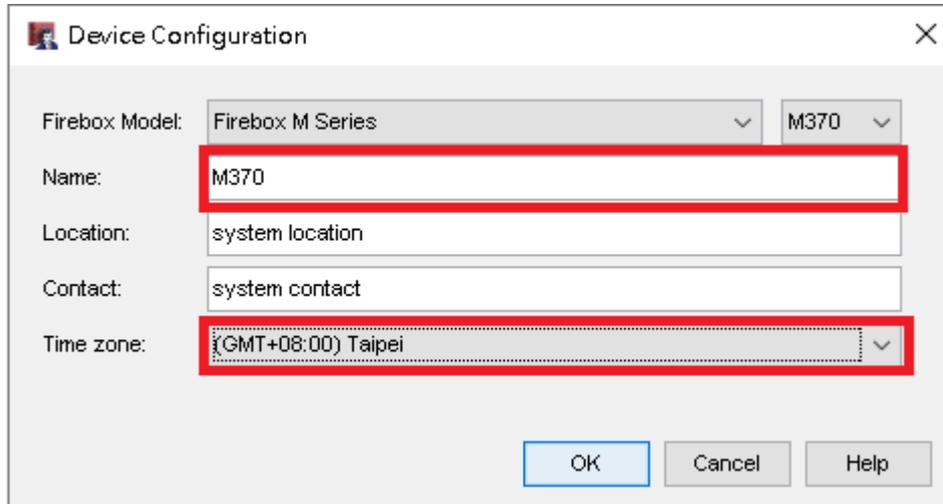


Step 1 :

點選 Setup → System

Note : 時區必須設定正確，否則LOG時間會錯誤

設定時區及防火牆名稱2



The image shows a 'Device Configuration' dialog box with the following fields:

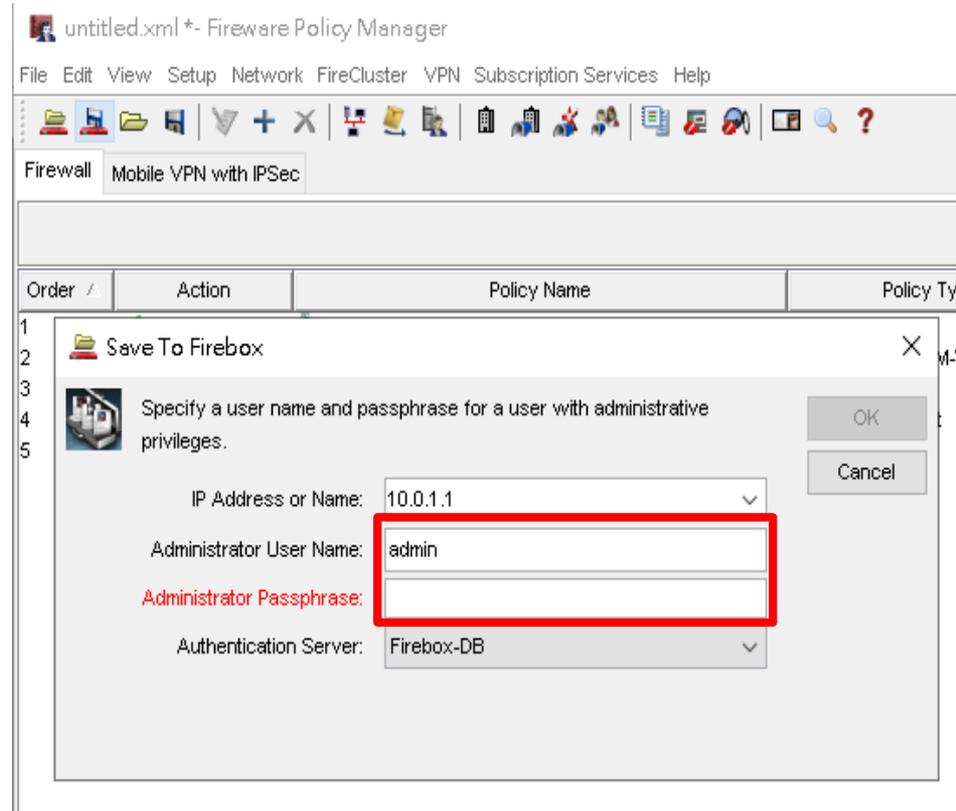
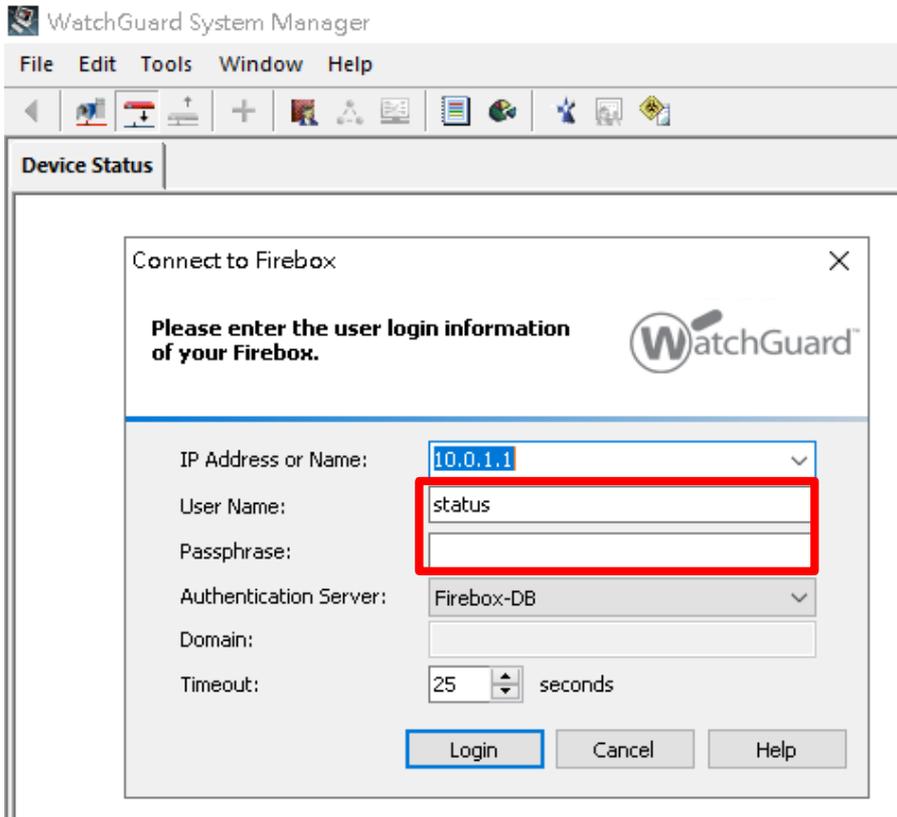
- Firebox Model: Firebox M Series (dropdown) and M370 (dropdown)
- Name: M370 (text input, highlighted with a red box)
- Location: system location (text input)
- Contact: system contact (text input)
- Time zone: (GMT+08:00) Taipei (dropdown, highlighted with a red box)

Buttons: OK, Cancel, Help

Step 2 :

- 1.輸入防火牆名稱以方便後續辨識
2. 時區選擇Taipei

創建帳號與密碼



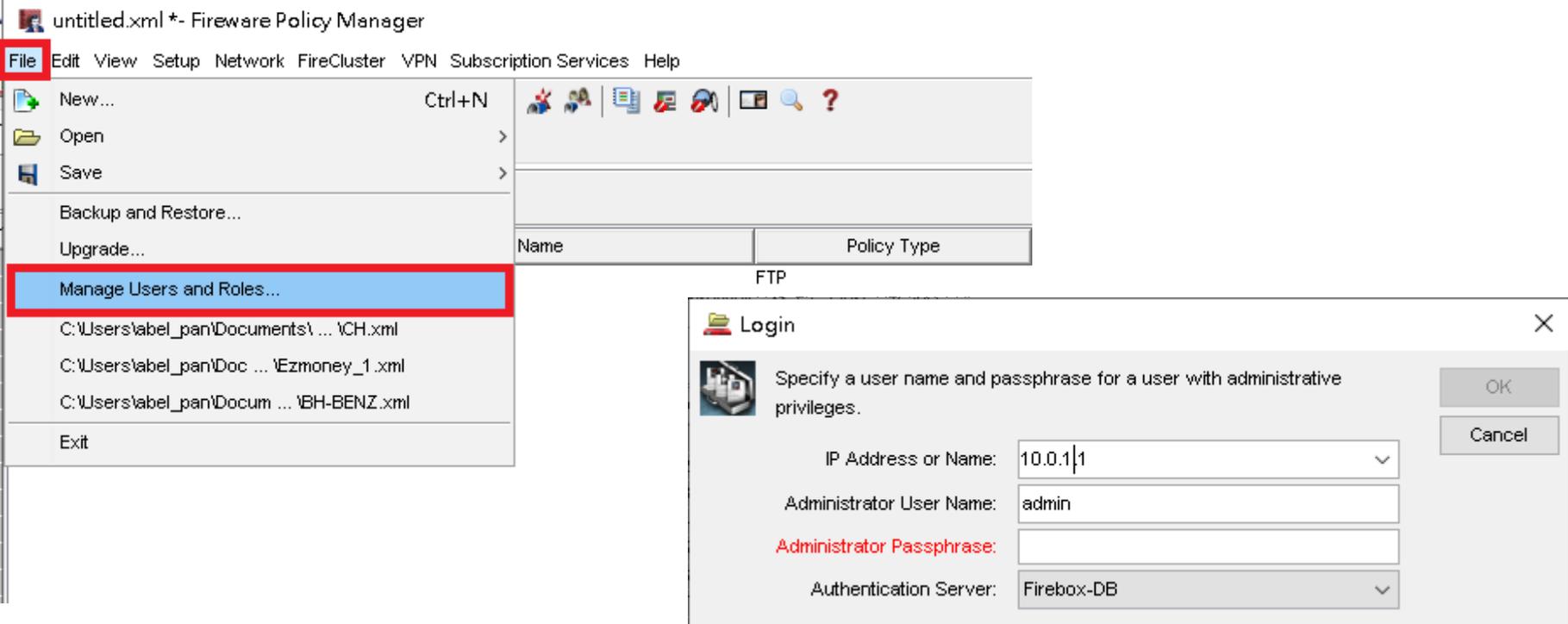
WatchGuard 預設有兩組帳號

1. Device Monitor : status
2. Device Administrator : admin

預設密碼
readonly
readwrite

*建議初始化設定完成後
要修改預設密碼

創建帳號與密碼



The screenshot displays the Fireware Policy Manager application window. The 'File' menu is open, and 'Manage Users and Roles...' is highlighted. A 'Login' dialog box is overlaid on the main window, prompting for user credentials. The dialog box contains the following fields:

- IP Address or Name: 10.0.1|1
- Administrator User Name: admin
- Administrator Passphrase: (empty)
- Authentication Server: Firebox-DB

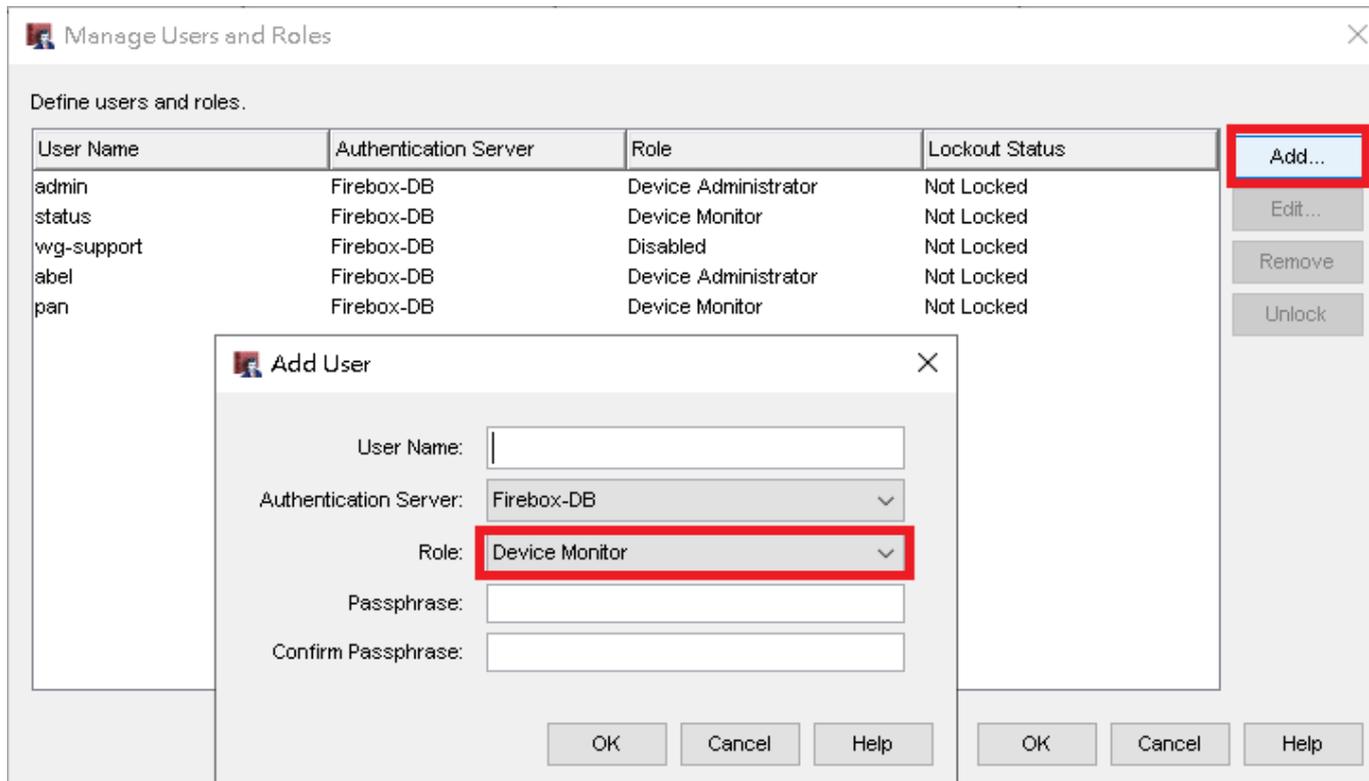
Buttons for 'OK' and 'Cancel' are visible on the right side of the dialog box.

Step 1 :

1.點選File → Manage Users and Roles

2.點選後會出現登入畫面需要輸入admin 帳號

創建帳號與密碼



Manage Users and Roles

Define users and roles.

User Name	Authentication Server	Role	Lockout Status
admin	Firebox-DB	Device Administrator	Not Locked
status	Firebox-DB	Device Monitor	Not Locked
wg-support	Firebox-DB	Disabled	Not Locked
abel	Firebox-DB	Device Administrator	Not Locked
pan	Firebox-DB	Device Monitor	Not Locked

Buttons: Add..., Edit..., Remove, Unlock

Add User

User Name:

Authentication Server: Firebox-DB

Role: Device Monitor

Passphrase:

Confirm Passphrase:

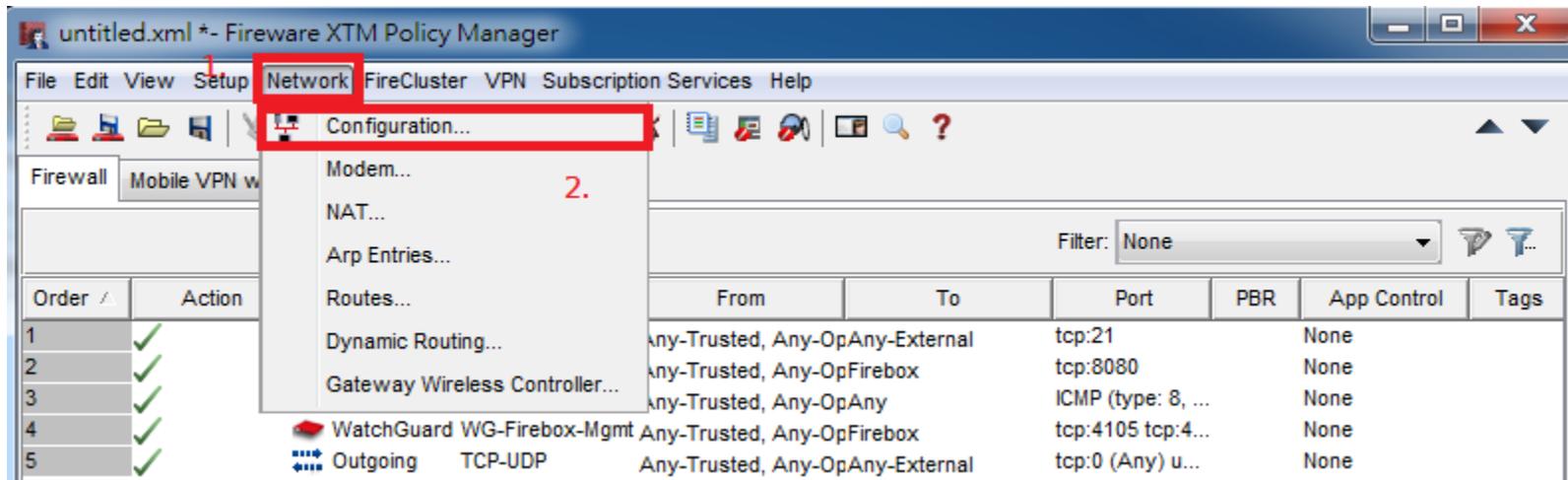
Buttons: OK, Cancel, Help

Step 2 : 1. 點選Add 新增帳號

2. Add User 畫面填寫好認別的名稱並選擇帳戶的角色
*若是選擇修改現有的帳號要重新登入才會生效

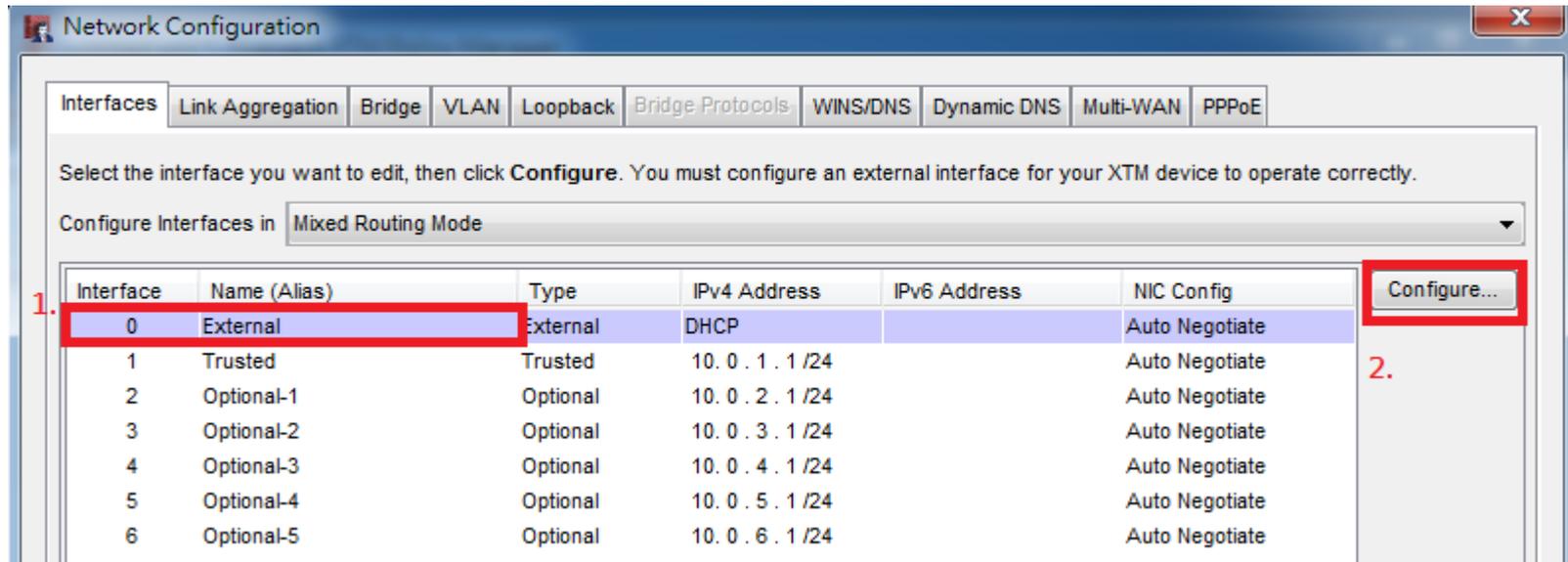
Network 參數設定

網路介面設定



點選 Network → Configuration

網路介面設定



Network Configuration

Interfaces | Link Aggregation | Bridge | VLAN | Loopback | Bridge Protocols | WINS/DNS | Dynamic DNS | Multi-WAN | PPPoE

Select the interface you want to edit, then click **Configure**. You must configure an external interface for your XTM device to operate correctly.

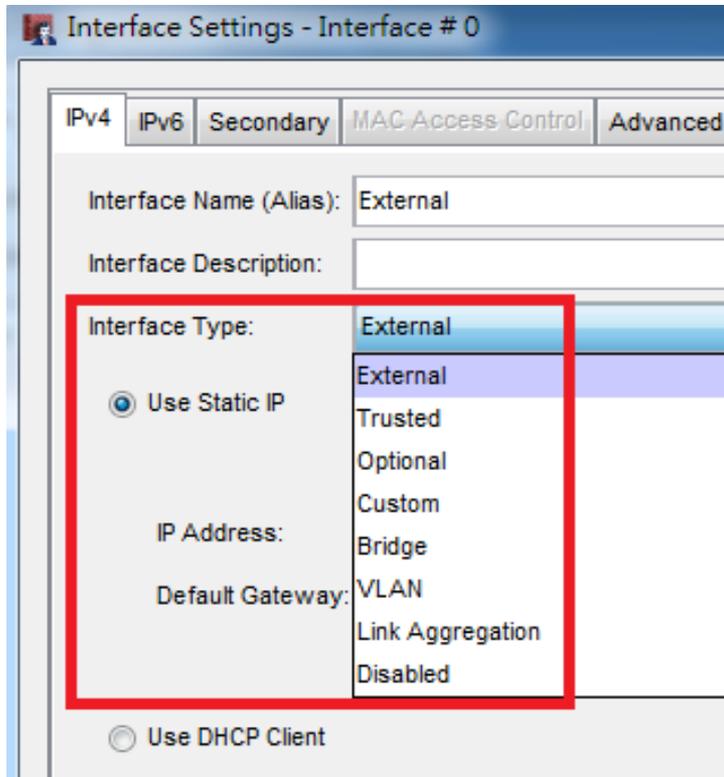
Configure Interfaces in: Mixed Routing Mode

Interface	Name (Alias)	Type	IPv4 Address	IPv6 Address	NIC Config
0	External	External	DHCP		Auto Negotiate
1	Trusted	Trusted	10.0.1.1/24		Auto Negotiate
2	Optional-1	Optional	10.0.2.1/24		Auto Negotiate
3	Optional-2	Optional	10.0.3.1/24		Auto Negotiate
4	Optional-3	Optional	10.0.4.1/24		Auto Negotiate
5	Optional-4	Optional	10.0.5.1/24		Auto Negotiate
6	Optional-5	Optional	10.0.6.1/24		Auto Negotiate

Configure...

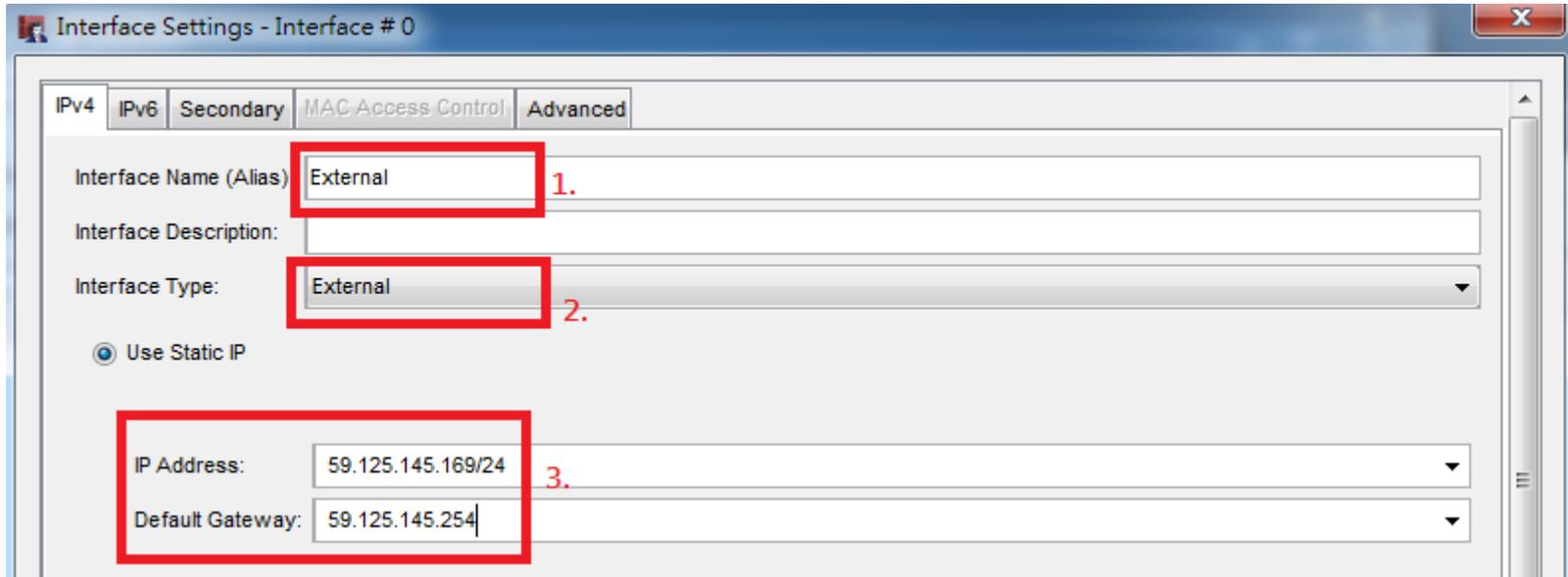
點選要設定的介面→ Configure

Interface Type



- **External** – 外部介面，連接對外線路
- **Trusted** – 內部介面
- **Optional** – DMZ或是Branch Office網段
- **Custom** – 自訂選項介面，如訪客區
- **Bridge** – 將多個介面綁在一起，如同Switch
- **VLAN** – 透過Firewall進行VLAN間的路由
- **Link Aggregation** – 設定介面Port Channel
- **Disable** – 關閉介面

網路介面參數



Interface Settings - Interface # 0

IPv4 | IPv6 | Secondary | MAC Access Control | Advanced

Interface Name (Alias): External 1.

Interface Description:

Interface Type: External 2.

Use Static IP

IP Address: 59.125.145.169/24 3.

Default Gateway: 59.125.145.254

1.輸入名稱，以方便後續識別介面

2.選擇Interface Type

3.輸入IP，如果此介面為External請輸入Default Gateway

Note：WatchGuard Firewall所有型號皆可介接4條對外線路

設定DHCP Server

Interface Settings - Interface # 1

IPv4 IPv6 Secondary MAC Access Control Advanced

Interface Name (Alias): Trusted

Interface Description:

Interface Type: Trusted

IP Address: 10.0.1.1/24

Disable DHCP

Use DHCP Server 1.

You can configure a maximum of six address ranges.

Address Pool: 2.

Starting IP	Ending IP	Add
10.0.1.2	10.0.1.254	Add Edit Delete

Reserved Addresses: 3.

Reserved Name	Reservation IP	MAC Address	Add
			Add Edit Delete

Leasing Time: 8 hours 4.

Configure DNS/WINS servers DHCP Options...

OK Cancel Help

1. 點選 Use DHCP Server
2. 點選新增DHCP Pool
3. Reserved Addresses 設定指定配發IP
4. Leasing Time 設定IP釋放時間
5. Configure DNS/WINS Server 設定DHCP Client所取得的DNS或是WINS Server IP

設定DHCP Pool

Use DHCP Server

You can configure a maximum of six address ranges.

Address Pool:

Starting IP	Ending IP	
10.0.1.2		1. Add
		Edit
		Delete

Reserved Addresses:

Reserved Name	
	Add
	Edit
	Delete

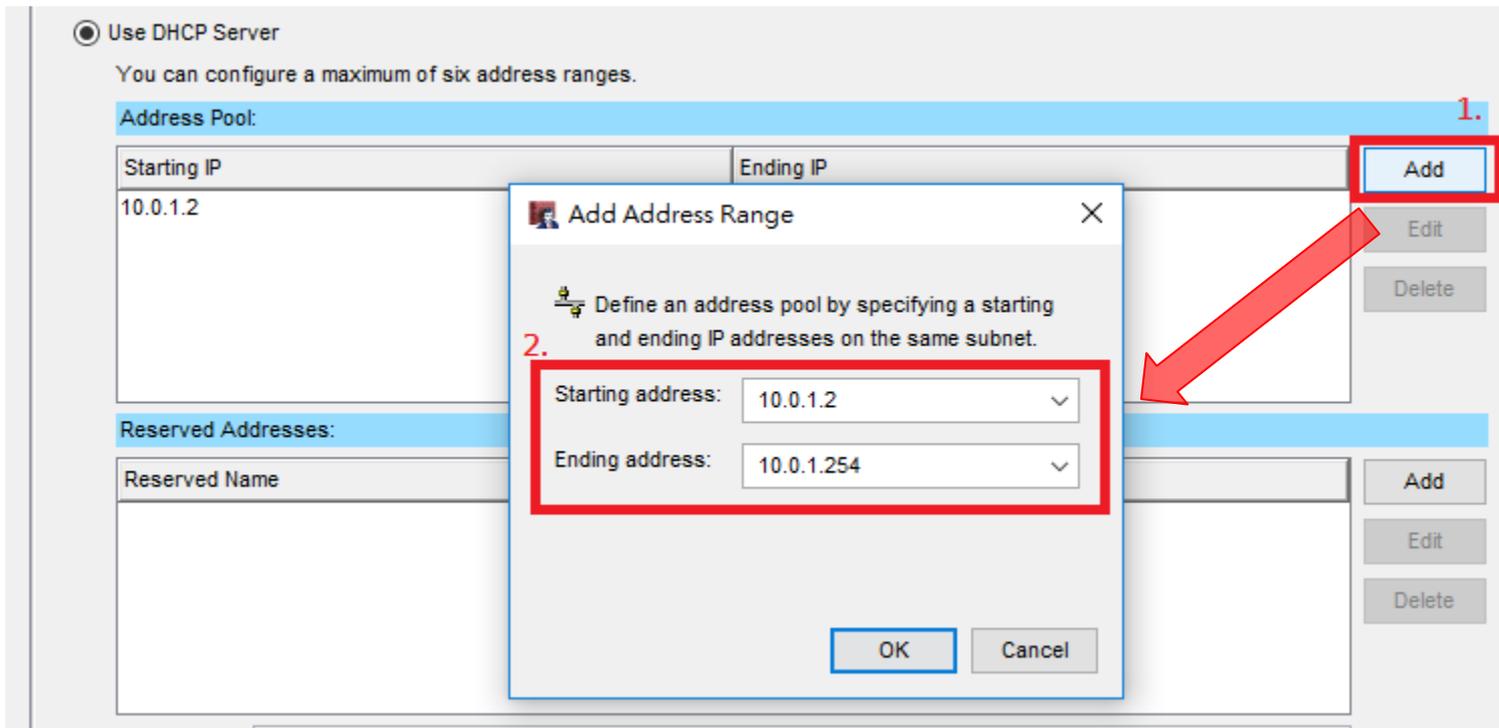
2. Add Address Range

Define an address pool by specifying a starting and ending IP addresses on the same subnet.

Starting address: 10.0.1.2

Ending address: 10.0.1.254

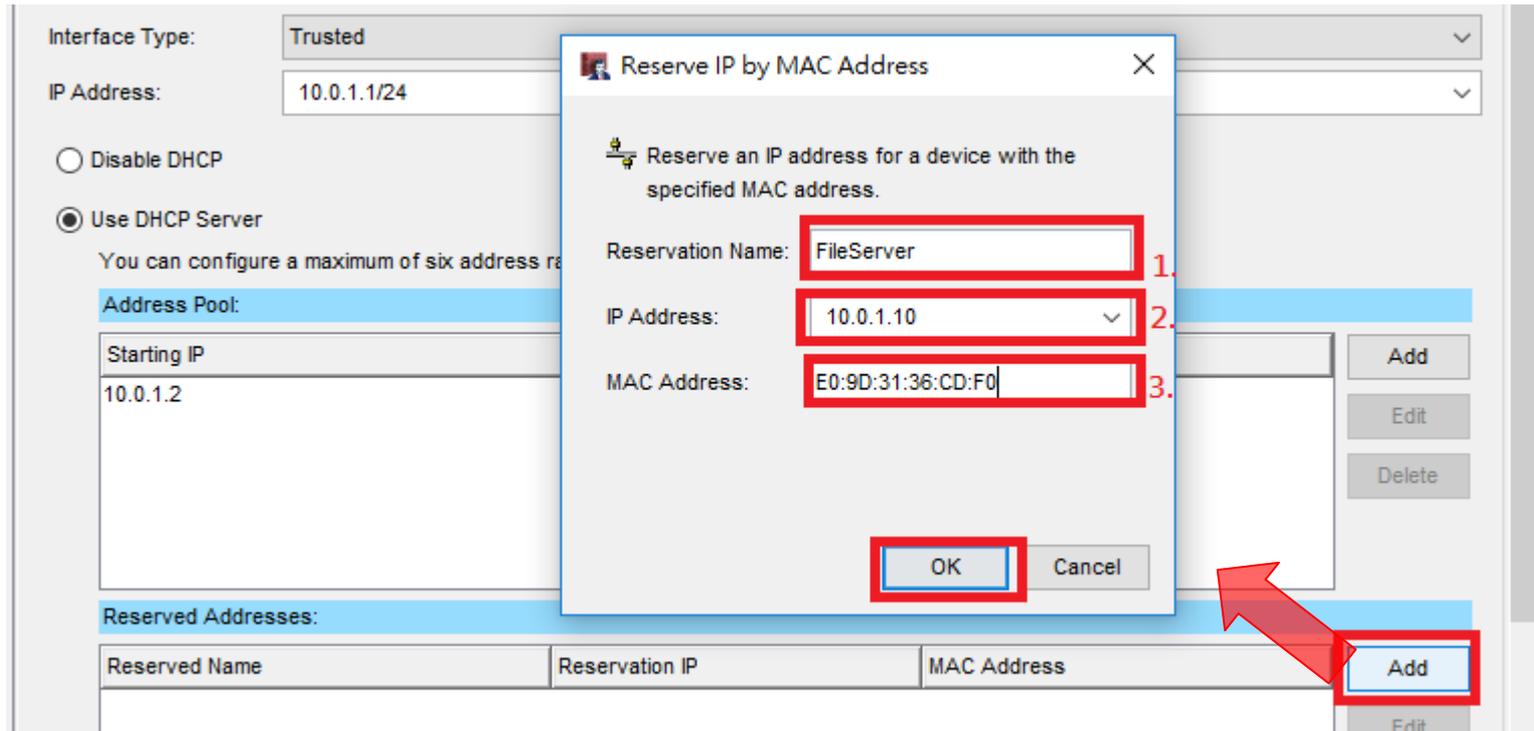
OK Cancel



點選Add新增DHCP Pool

Note : DHCP Pool必須和介面同一個網段

設定Reserved Addressed



Interface Type: Trusted

IP Address: 10.0.1.1/24

Disable DHCP

Use DHCP Server

You can configure a maximum of six address reservations.

Address Pool:

Starting IP
10.0.1.2

Reserved Addresses:

Reserved Name	Reservation IP	MAC Address
---------------	----------------	-------------

Reserve IP by MAC Address

Reserve an IP address for a device with the specified MAC address.

Reservation Name: FileServer

IP Address: 10.0.1.10

MAC Address: E0:9D:31:36:CD:F0

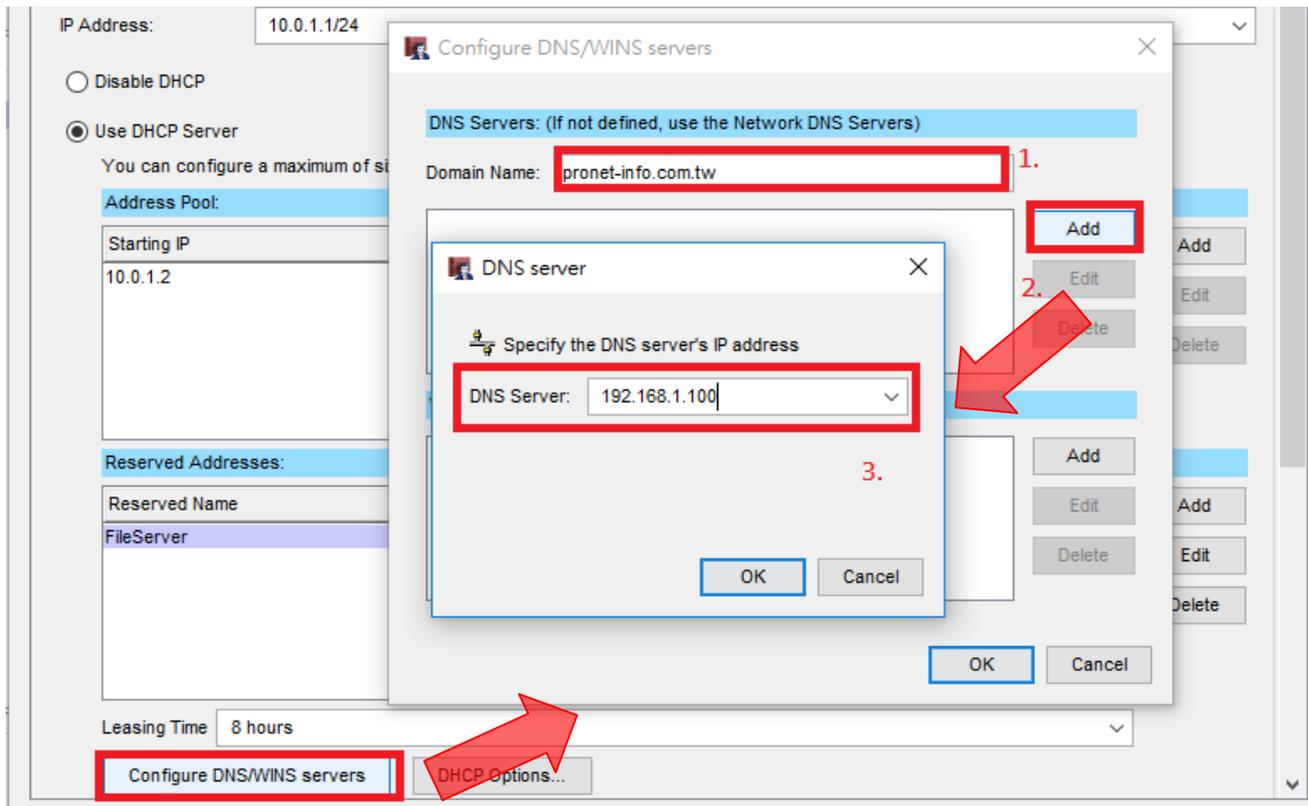
OK Cancel

Add Edit Delete

點選Add新增排除的IP位置

1. 輸入主機名稱
2. 輸入主機的IP Address
3. 輸入主機的MAC Address

設定DHCP發放的DNS IP



點選Configure DNS/WINS Server

1. 輸入Domain Name (Option)
2. 點選Add
3. 輸入DNS IP Address

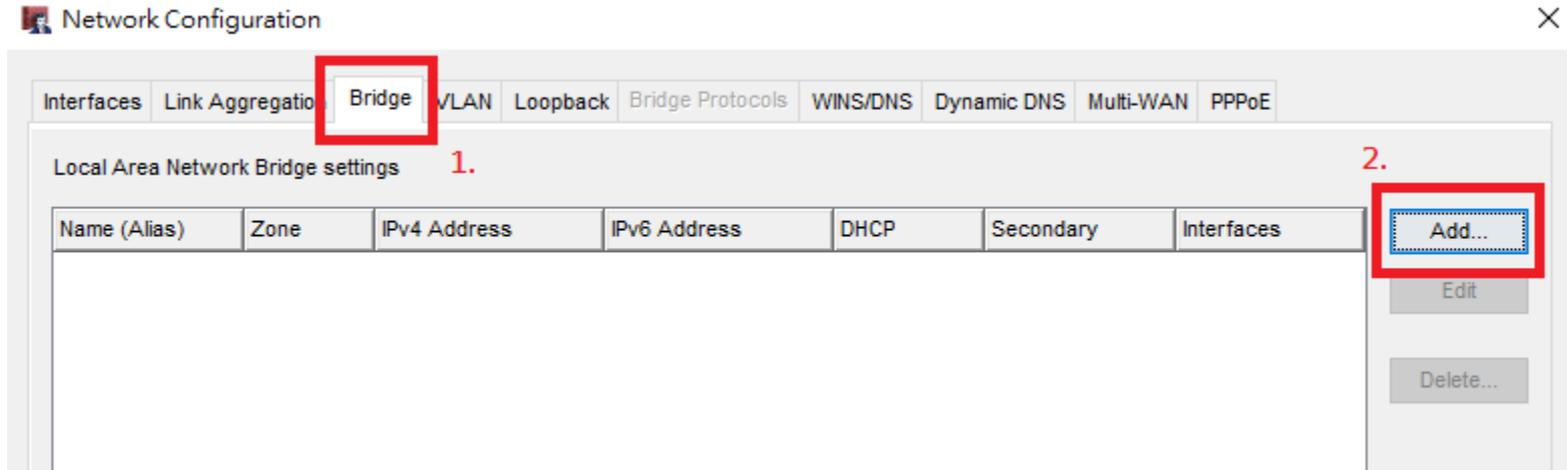
Interface Bridge



Interface Bridge 說明

當網路管理人員需要把多個Port綁在一起，設定成同個網段時，可利用 Interface Bridge將多個Port綁一起。

Interface Bridge 設定



Step 1 :

Network → Configuration

1. 選擇上方頁簽 Bridge
2. 點選Add

Interface Bridge 設定

New Bridge Configuration

IPv4 IPv6 Secondary Bridge Protocols

Name (Alias) : Inside 1.

Description :

Security Zone : Trusted 2.

IP Address : 192.168.1.1/24 3.

Disable DHCP

Use DHCP Server

You can configure a maximum of six address ranges.

Address Pool:

Starting IP	Ending IP	Add

Reserved Addresses:

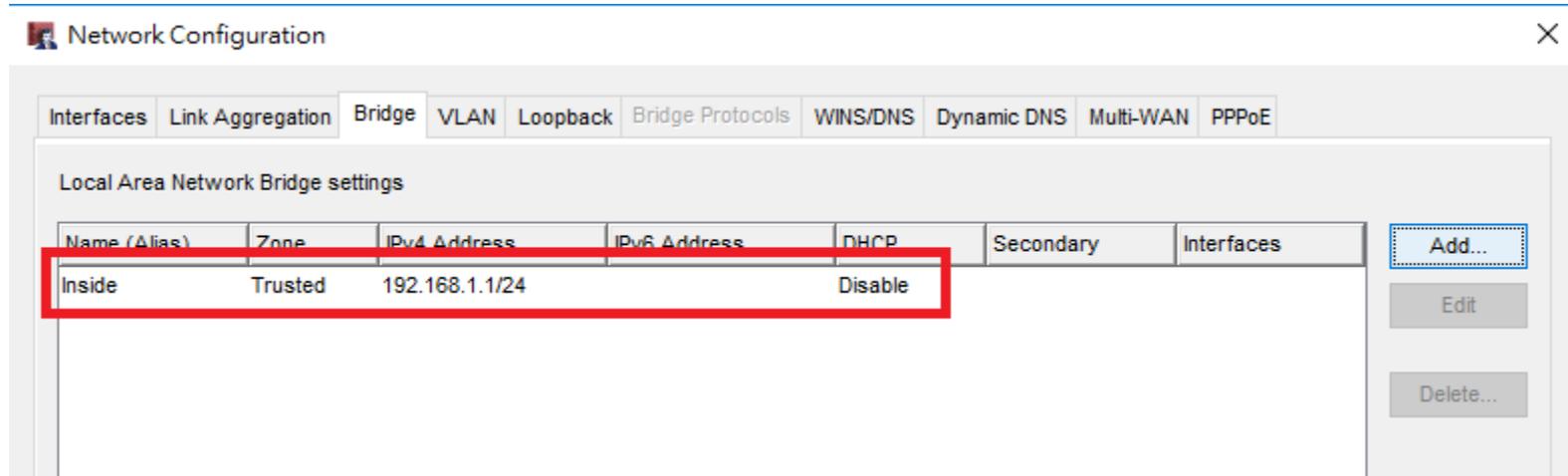
Reserved Name	Reservation IP	MAC Address	Add

OK Cancel Help

Step 2 :

1. 設定介面名稱
2. 選擇 Security Zone , External
介面不可設定 Bridge
3. 輸入 IP Address
4. 點選 OK

確認Interface Bridge 設定



Network Configuration

Interfaces Link Aggregation Bridge VLAN Loopback Bridge Protocols WINS/DNS Dynamic DNS Multi-WAN PPPoE

Local Area Network Bridge settings

Name (Alias)	Zone	IPv4 Address	IPv6 Address	DHCP	Secondary	Interfaces
Inside	Trusted	192.168.1.1/24		Disable		

Add...
Edit
Delete...

Bridge介面資訊設定完成後顯示於Bridge頁面

將實體介面加入Interface Bridge

Interface Settings - Interface # 5

IPv4 IPv6 Secondary MAC Access Control Advanced

Interface Name: Optional-4

Interface Description:

Interface Type: Bridge 1.

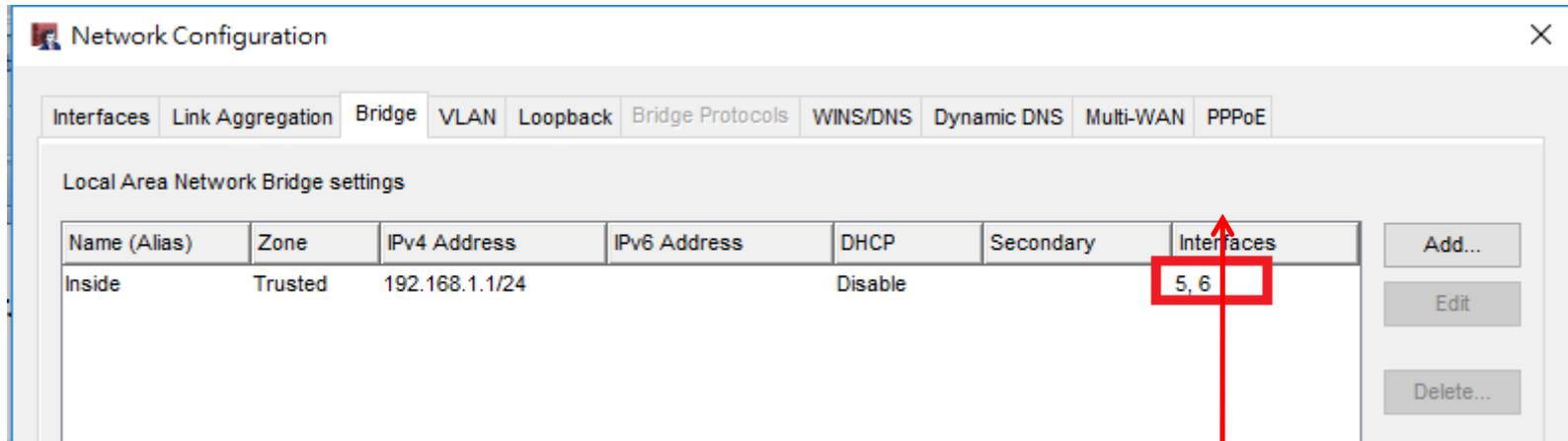
Send and receive traffic for selected Bridge interface

Member	Zone	Name	IPv4 Address	IPv6 Address	DHCP	Secondary
<input checked="" type="radio"/> 2.	Trusted	Inside	192.168.1.1/24		Disable	

進入實體Interface設定

1. Interface Type選擇“Bridge”
2. 點選下方Bridge Member
3. 要加入同個Bridge的Interface重覆進行上兩步設定

確認Interface Bridge 設定完成



The screenshot shows the 'Network Configuration' window with the 'Bridge' tab selected. Under 'Local Area Network Bridge settings', there is a table with the following data:

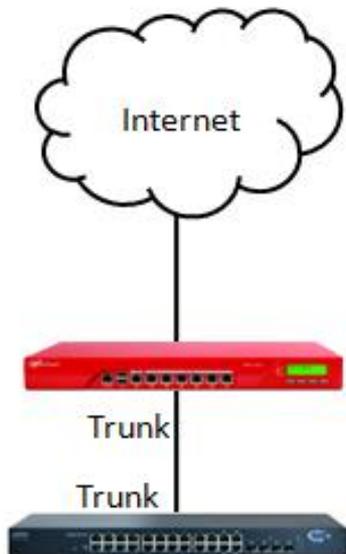
Name (Alias)	Zone	IPv4 Address	IPv6 Address	DHCP	Secondary	Interfaces
Inside	Trusted	192.168.1.1/24		Disable		5, 6

The 'Interfaces' column value '5, 6' is highlighted with a red box, and a red arrow points from this box to a text box below.

Eth5以及Eth6設定完成加入
到同一個Bridge

VLAN設定

範例情境

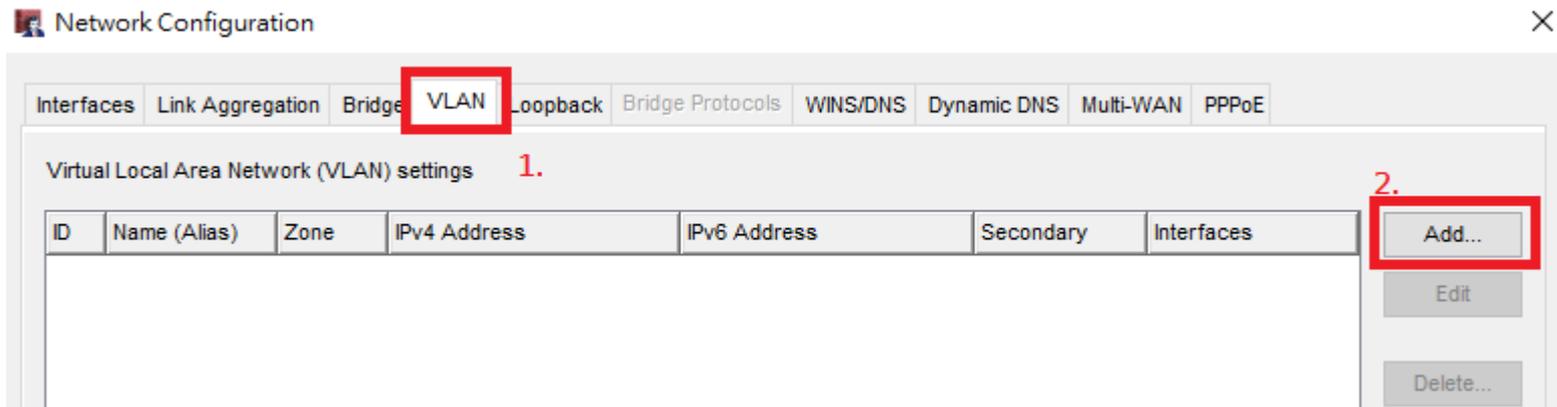


VLAN 10
192.168.10.0/24
VLAN 20
192.168.10.0/24

架構說明

1. WatchGuard 下方介接的Switch為L2 Switch沒有Routing的功能。
2. Switch中畫分兩個VLAN，分別為VLAN10,20
3. 兩個VLAN需要靠WatchGuard交換路由
4. Firewall和Switch介接的介面需要設定Trunk

VLAN設定



Network → Configuration

1. 選擇上方頁簽 VLAN
2. 點選Add

VLAN介面設定

New VLAN Configuration

IPv4 IPv6 Secondary Bridge Protocols

Name (Alias) : 1.

Description :

VLAN ID : 2.

Security Zone : 3.

IP Address : 4.

VLAN設定說明

1. Name : 輸入VLAN名稱
2. VLAN ID : 此為VLAN Tag設定，如果此VLAN為VLAN 10，此欄位要輸入10
3. Security Zone : 選擇該VLAN所屬的型態
4. IP Address : 輸入此Interface VLAN IP位置

實體介面VLAN設定

Interface Settings - Interface # 2

IPv4 IPv6 Secondary MAC Access Control Advanced

Interface Name: Optional-1

Interface Description:

Interface Type: **VLAN** 1.

Send and receive tagged traffic for selected VLANs

You can add one or more VLANs to this interface. New VLAN

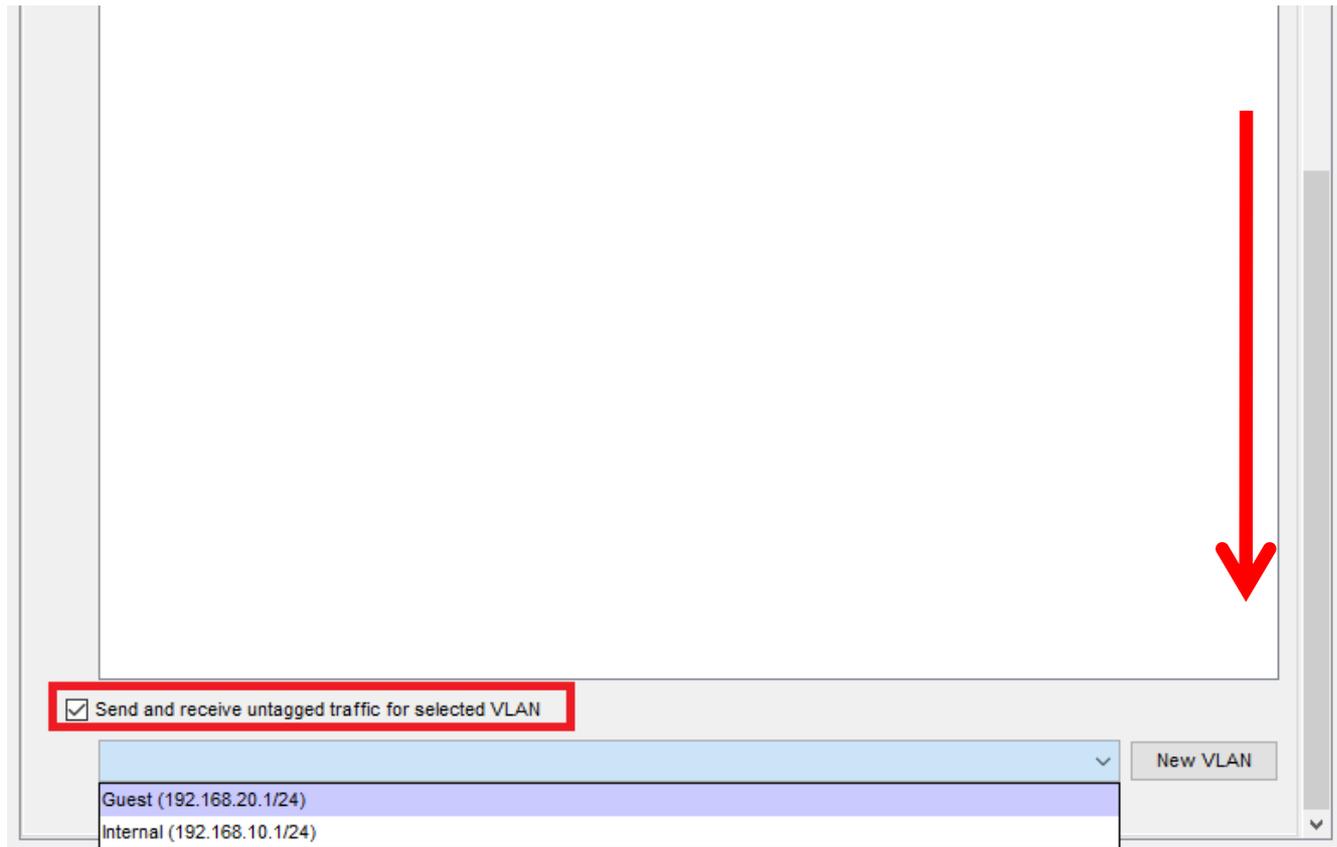
Member	ID	Zone	Name	IPv4 Address	IPv6 Address	Secondary
<input checked="" type="checkbox"/>	10	Trusted	Internal	192.168.10.1/24 (DHCP disabled)		
<input checked="" type="checkbox"/>	20	Trusted	Guest	192.168.20.1/24 (DHCP disabled)		

2.

1. Interface Type選擇VLAN

2. 將下方Member VLAN勾選起來

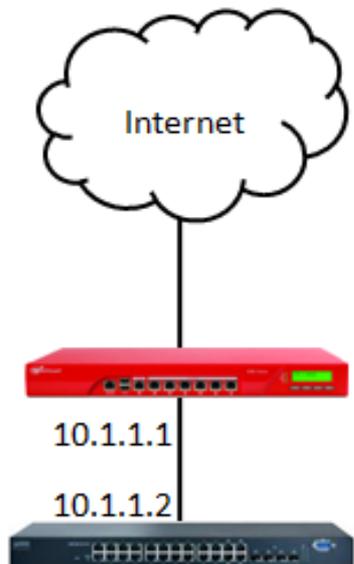
Native VLAN設定



1. 將右方下拉霸往下拉到最下面
2. 勾選Send and receive untagged traffic for selected VLAN
3. 選擇要設定為Native VLAN的VLAN

Static Route設定

範例情境二

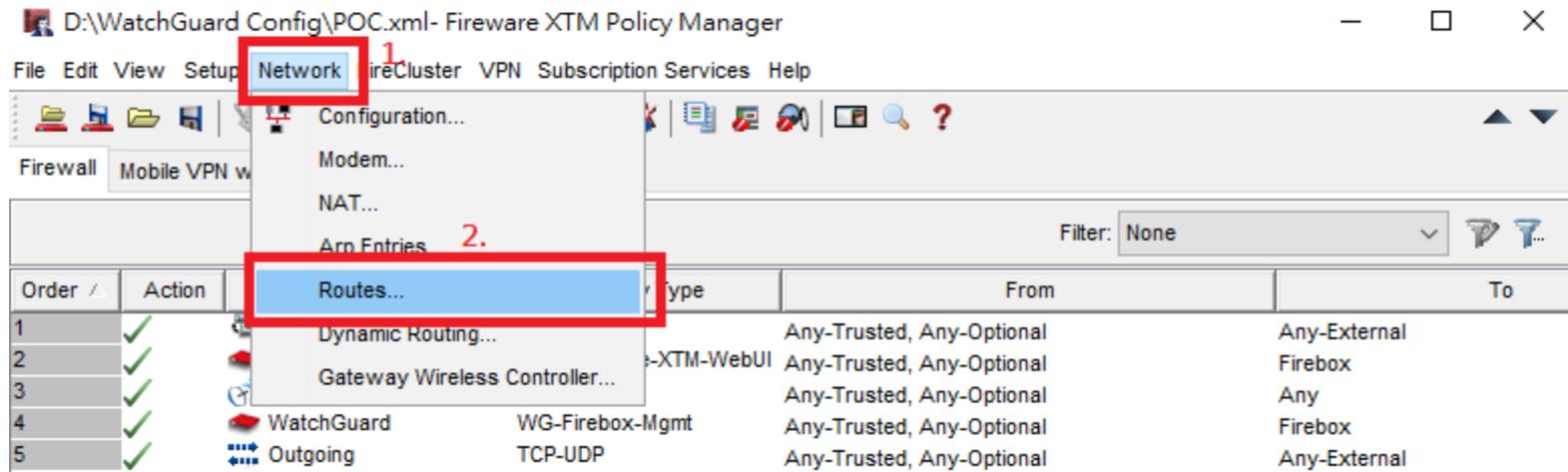


VLAN 10
192.168.10.0/24
VLAN 20
192.168.20.0/24
VLAN 30
192.168.30.0/24

架構說明

1. WatchGuard 下方介接的Switch為L3 Switch
2. 內部網段路由在Core Switch完成
3. WatchGuard必須設定靜態路由江內部網段指回Core Switch

Static Route設定

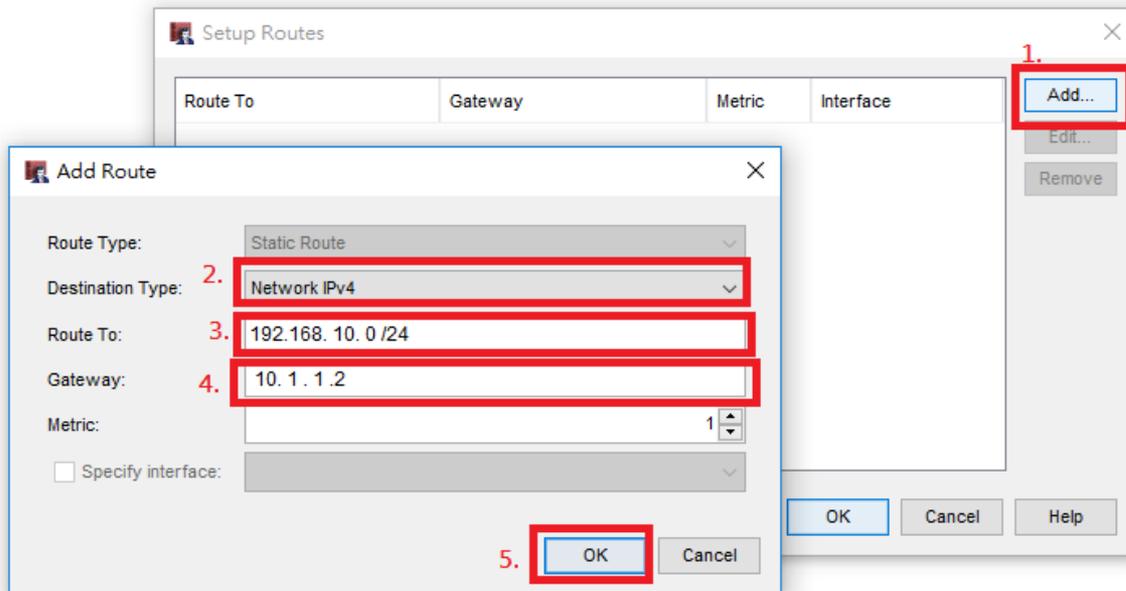


The screenshot shows the WatchGuard XTM Policy Manager interface. The 'Network' menu is open, and the 'Routes...' option is highlighted. A red box highlights the 'Network' menu item, and another red box highlights the 'Routes...' option. A red '1' is next to the 'Network' menu, and a red '2' is next to the 'Routes...' option. The main table below the menu shows the following data:

Order	Action	Type	From	To
1	✓	Dynamic Routing...	Any-Trusted, Any-Optional	Any-External
2	✓	Gateway Wireless Controller...	Any-Trusted, Any-Optional	Firebox
3	✓	WatchGuard	Any-Trusted, Any-Optional	Any
4	✓	WG-Firebox-Mgmt	Any-Trusted, Any-Optional	Firebox
5	✓	Outgoing	Any-Trusted, Any-Optional	Any-External

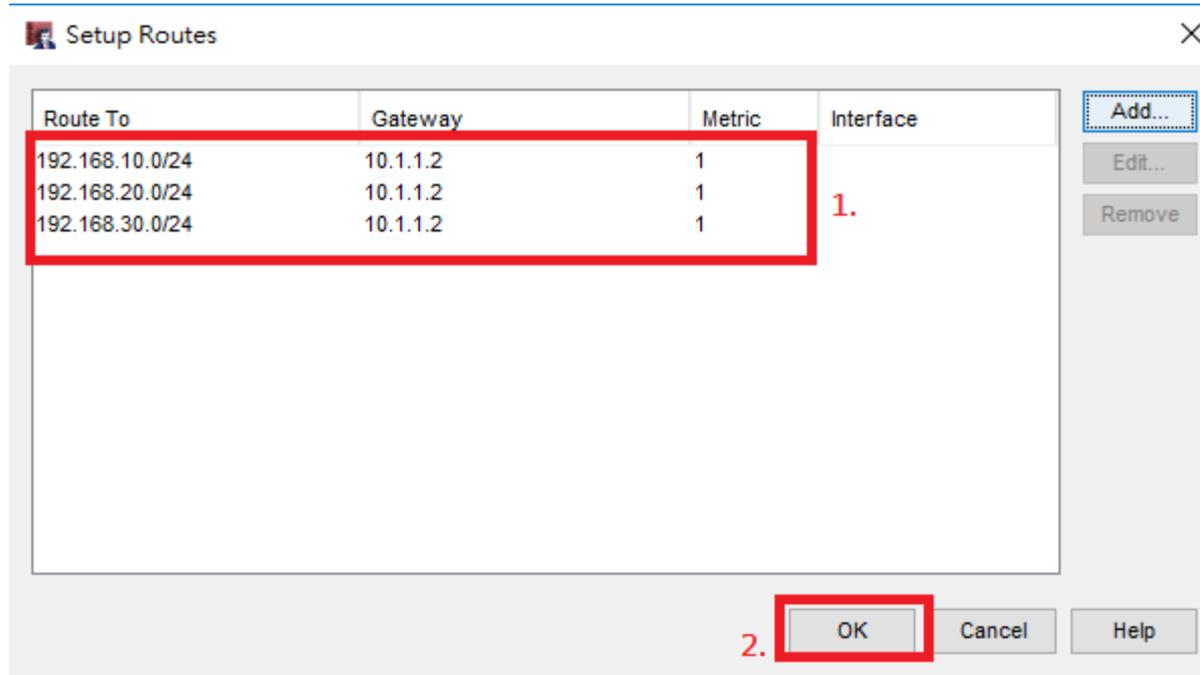
點選Network → Routes

Static Route設定



1. 點選Add
2. Destination Type 選擇 Network IPv4
3. Route to 輸入內部VLAN網段
4. Gateway輸入Core Switch對點 IP Address
5. 點選OK

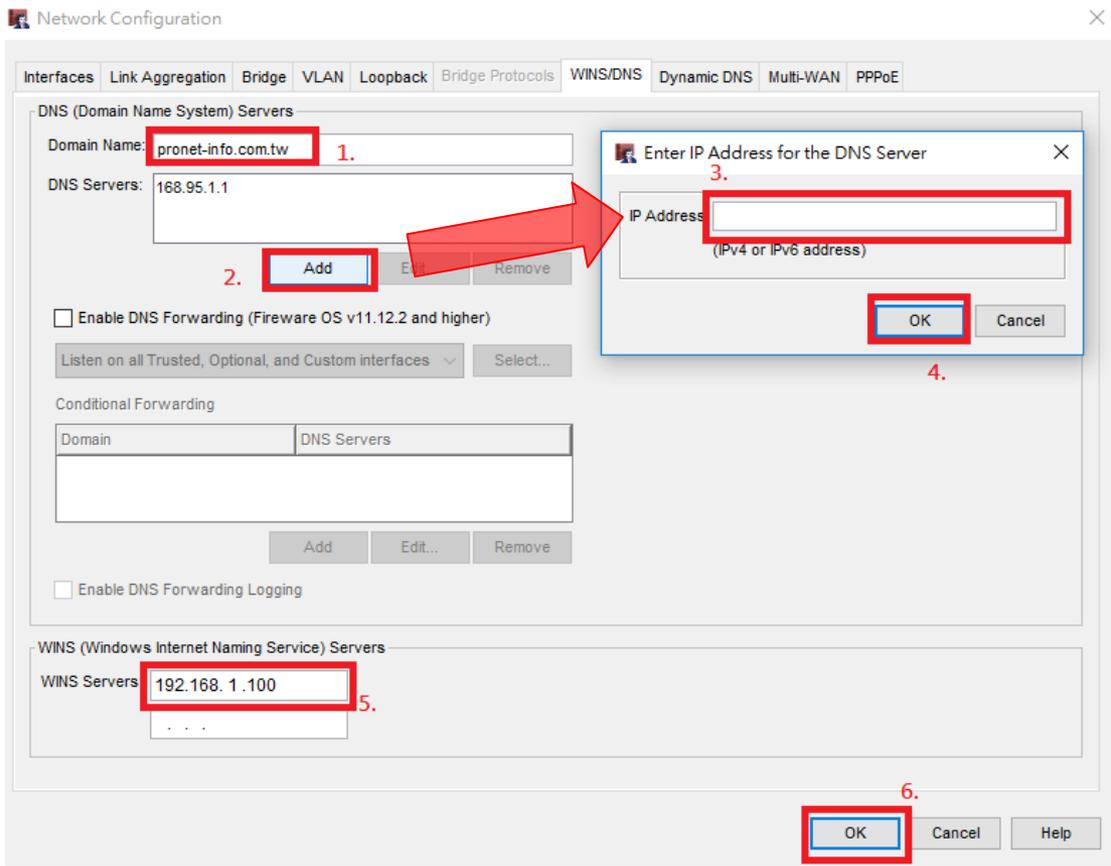
Static Route設定確認



1. 確認Static Route設定
2. 點選OK

DNS Server 設定

Firewall DNS、WINS設定

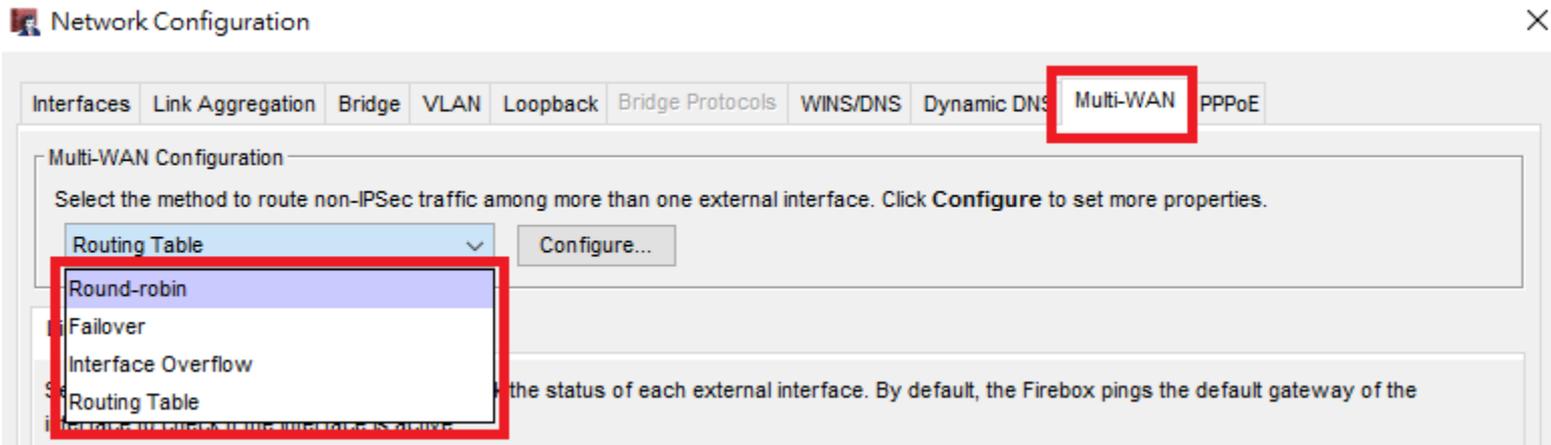


防火牆必需設定DNS特徵碼才可進行更新

1. 輸入Domain Name
2. 點選下方Add
3. 輸入DNS IP Address
4. 點選OK
5. 輸入WINS Server IP
6. 點選OK完成設定

Muti-WAN 參數設定

Muti-WAN設定



Muti-WAN切換模式

1. **Round-robin** – 對外線路隨機選擇
2. **Failover** – 當主要線路中斷才會切換至另一條
3. **Interface Overflow** – Loading較輕的線路優先
4. **Routing Table** – 依據Policy判斷要走哪一條對外線路

Muti-WAN設定

對外線路可透過Ping或是偵測服務
是否有回應來判斷該線路是否中斷，
而非單單只判斷第一層訊號

1. 輸入要偵測的IP位置
2. 設定偵測間隔以及切換的時間

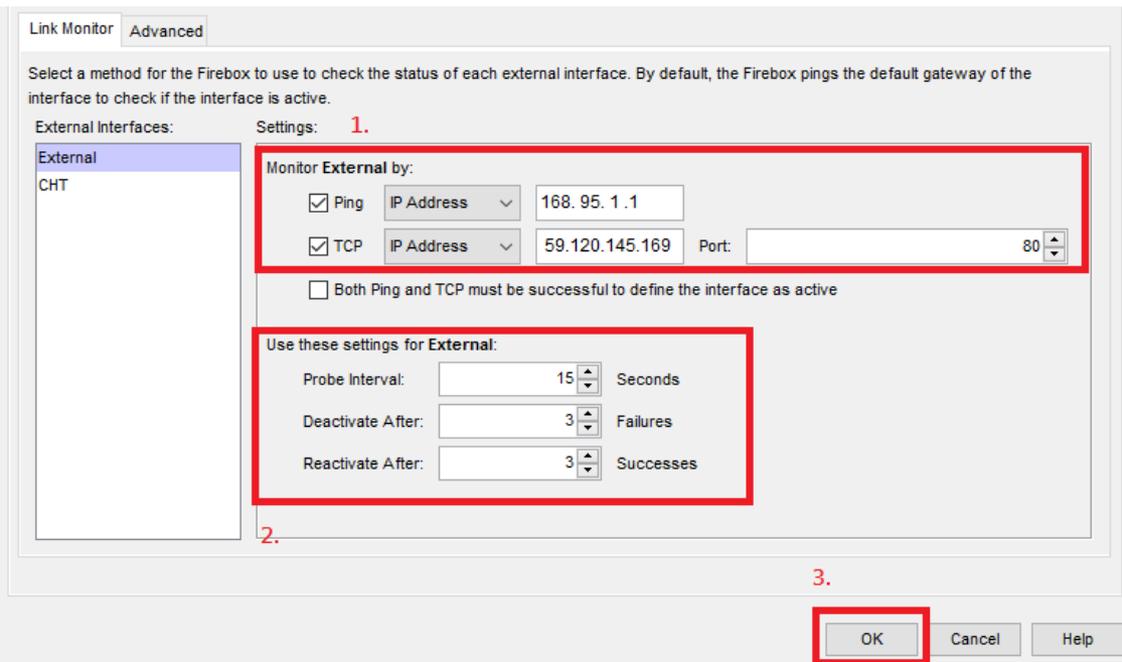
預設值

每15秒測試一次

測試3次失敗後切換線路

測試成功3次切回主線路

3. 點選OK



Link Monitor Advanced

Select a method for the Firebox to use to check the status of each external interface. By default, the Firebox pings the default gateway of the interface to check if the interface is active.

External Interfaces: External
CHT

Settings: 1.

Monitor External by:

Ping IP Address 168.95.1.1

TCP IP Address 59.120.145.169 Port: 80

Both Ping and TCP must be successful to define the interface as active

Use these settings for External:

Probe Interval: 15 Seconds

Deactivate After: 3 Failures

Reactivate After: 3 Successes

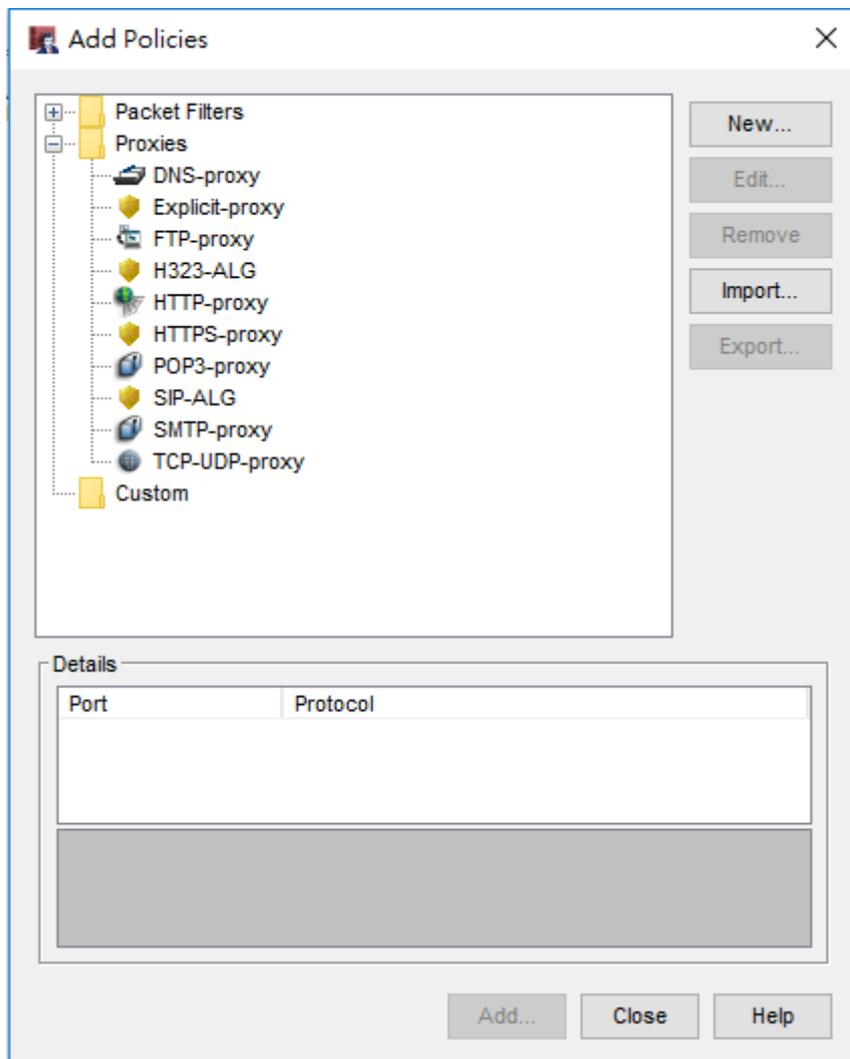
2.

3.

OK Cancel Help

Policy 設定

WatchGuard Policy種類



WatchGuard Policy分為下列三種

- 1. Packet Filters** – WatchGuard已建立好多種常用的Service，使用者可依據需求找到要設定的服務。
- 2. Proxies** – Proxy Policy可設定內容過濾，包含閘道防毒以及網頁過濾需要使用Proxy Policy進行設定。
- 3. Custom** – 可自行建立要設定的Port或是服務群組。

WatchGuard Policy 特性

File Edit View Setup Network FireCluster VPN Subscription Services Help

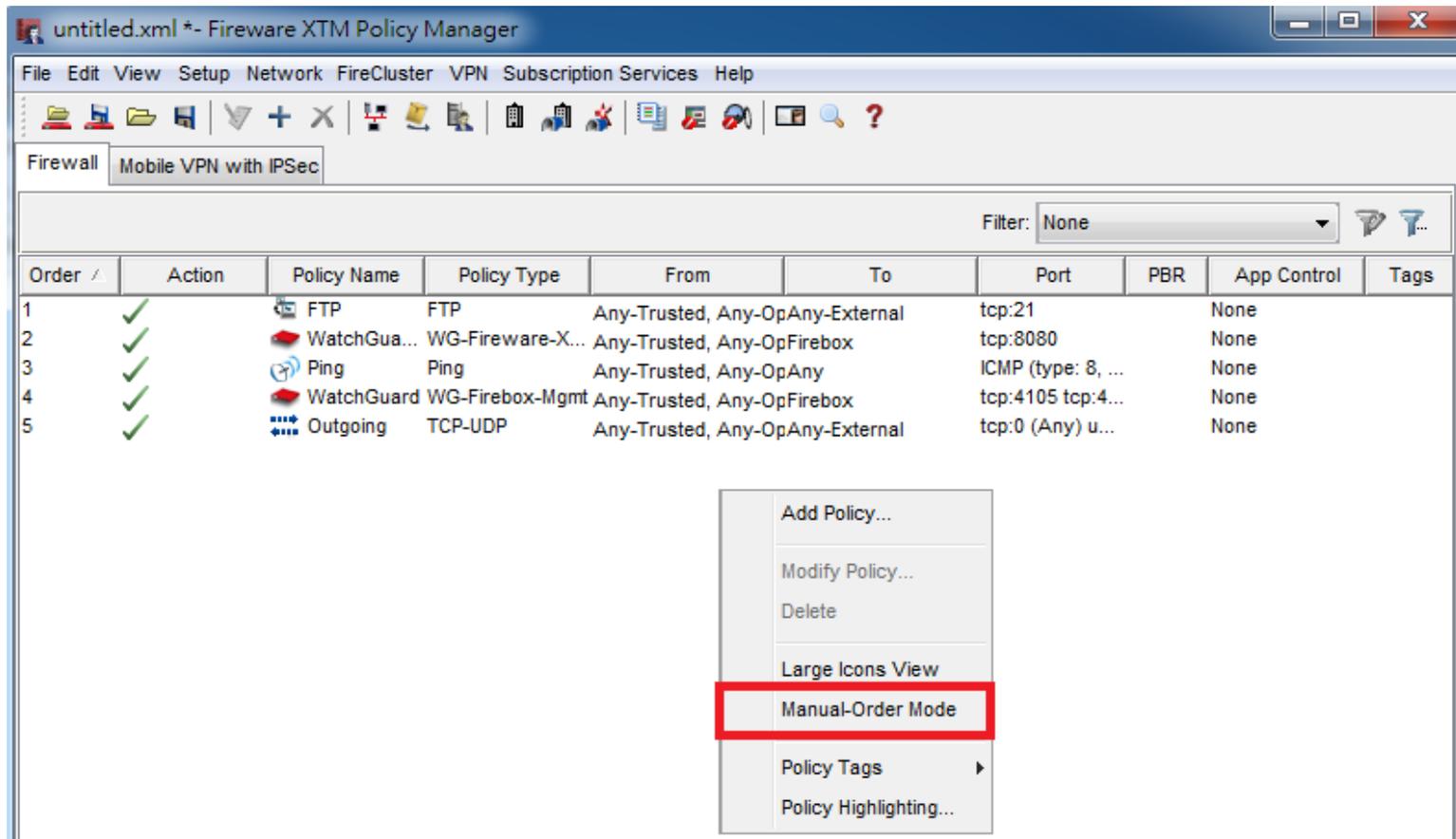
Firewall Mobile VPN with IPSec

Filter: None

Order /	Action	Policy Name	Policy Type	From	To	Port
1	✓	FTP	FTP	Any-Trusted, Any-Optional	Any-External	tcp:21
2	✗	HTTP	HTTP	Any-Trusted	Any-External	tcp:80
3	✓	WatchGuard Web UI	WG-Fireware-XTM-WebUI	Any-Trusted, Any-Optional	Firebox	tcp:8080
4	✓	Ping	Ping	Any-Trusted, Any-Optional	Any	icmp (type: 8, code: 255)
5	✓	WatchGuard	WG-Firebox-Mgmt	Any-Trusted, Any-Optional	Firebox	tcp:4105 tcp:4117 tcp:4118
6	✓	Outgoing	TCP-UDP	Any-Trusted, Any-Optional	Any-External	tcp:0 (Any) udp:0 (Any)

*WatchGuard Firewall 會依據order 數字順序進行作用

Policy Manual Order Mode



The screenshot shows the Fireware XTM Policy Manager interface. The window title is "untitled.xml *- Fireware XTM Policy Manager". The menu bar includes File, Edit, View, Setup, Network, FireCluster, VPN, Subscription Services, and Help. The toolbar contains various icons for file operations and network management. The main area is titled "Firewall" and "Mobile VPN with IPSec". A filter dropdown is set to "None". Below the filter is a table of policies:

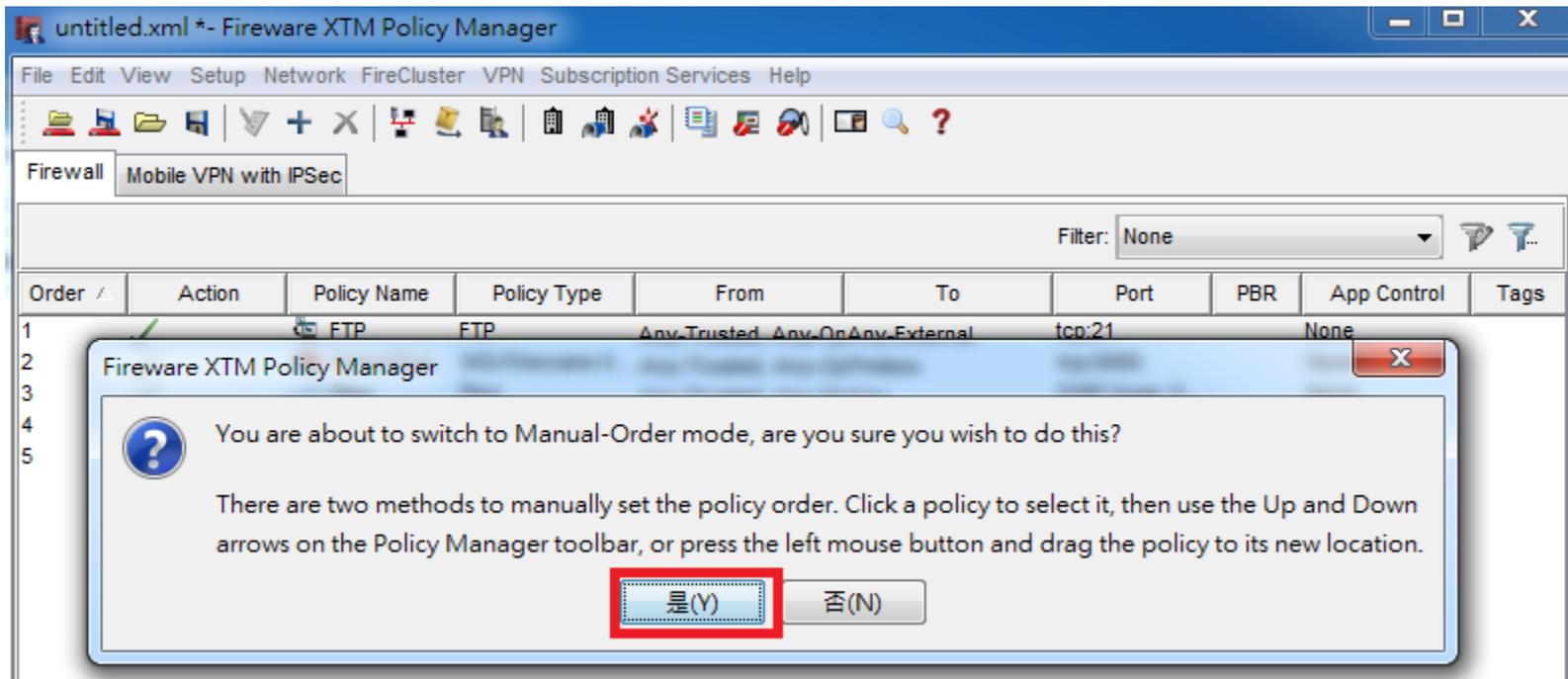
Order /	Action	Policy Name	Policy Type	From	To	Port	PBR	App Control	Tags
1	✓	FTP	FTP	Any-Trusted, Any-Op	Any-External	tcp:21		None	
2	✓	WatchGua...	WG-Fireware-X...	Any-Trusted, Any-Op	Firebox	tcp:8080		None	
3	✓	Ping	Ping	Any-Trusted, Any-Op	Any	ICMP (type: 8, ...		None	
4	✓	WatchGuard	WG-Firebox-Mgmt	Any-Trusted, Any-Op	Firebox	tcp:4105 tcp:4...		None	
5	✓	Outgoing	TCP-UDP	Any-Trusted, Any-Op	Any-External	tcp:0 (Any) u...		None	

A context menu is open over the table, with the following options:

- Add Policy...
- Modify Policy...
- Delete
- Large Icons View
- Manual-Order Mode** (highlighted with a red box)
- Policy Tags ▶
- Policy Highlighting...

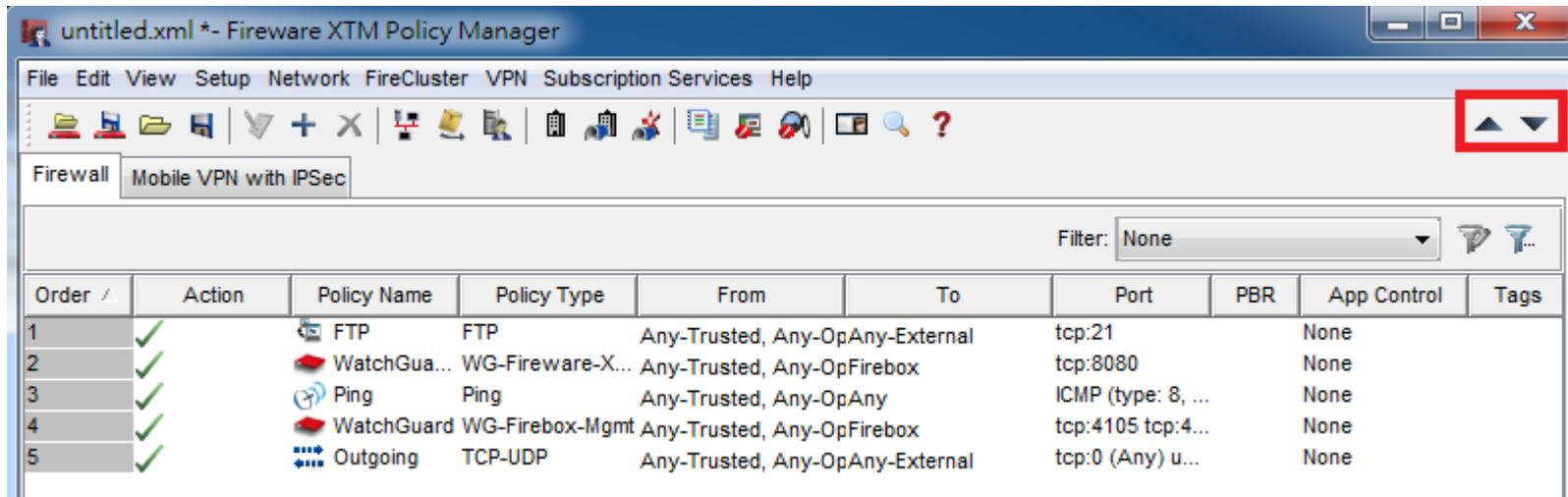
Step 1 : WatchGuard Policy預設會自動設定Policy順序，必須先調整成手動排序，在空白處按右鍵點選“Manual-Order Mode”

Policy Manual Order Mode



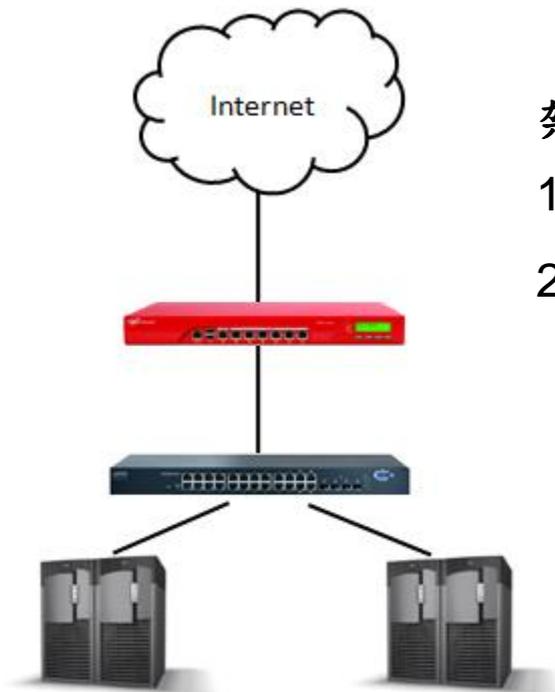
Step 2 : 按下Manual-Order Mode後將出現警告訊息，表示後續Policy可上下調整位置不在做自動排序，點選“是”。

Policy Manual Order Mode 設定完成



設定完成後Policy Manager右上角出現上下的按鍵
可以調整Policy的順序

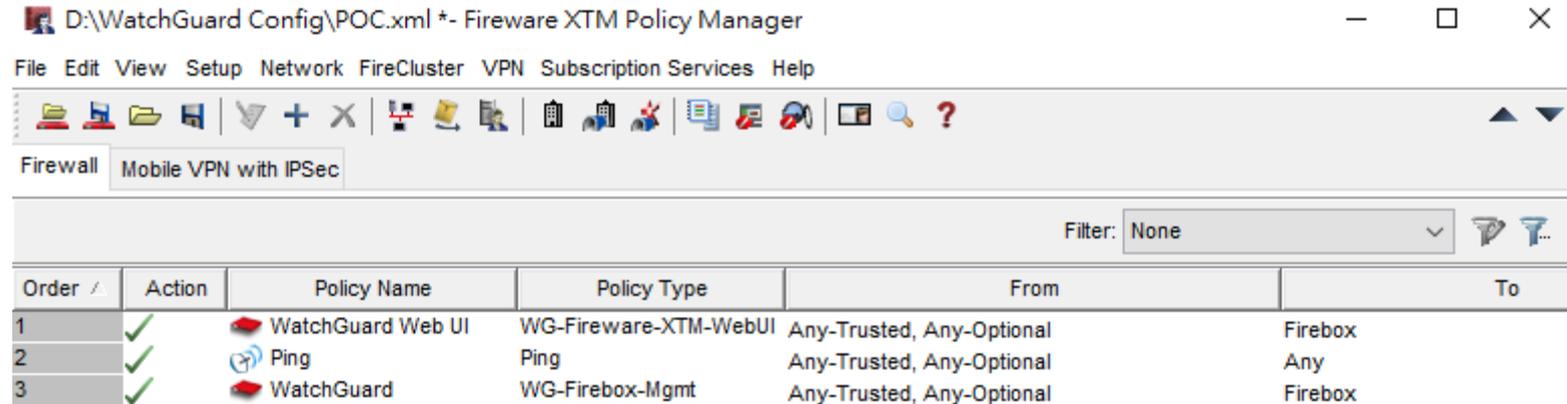
原則範例情境一



架構說明

1. 內部電腦要可以上Internet
2. 對外僅開啟TCP 21,80以及443三個Port

設定Service Group



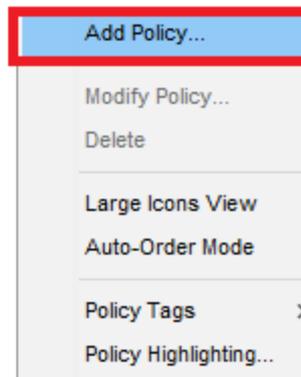
D:\WatchGuard Config\POC.xml *- Fireware XTM Policy Manager

File Edit View Setup Network FireCluster VPN Subscription Services Help

Firewall Mobile VPN with IPsec

Filter: None

Order /	Action	Policy Name	Policy Type	From	To
1	✓	WatchGuard Web UI	WG-Fireware-XTM-WebUI	Any-Trusted, Any-Optional	Firebox
2	✓	Ping	Ping	Any-Trusted, Any-Optional	Any
3	✓	WatchGuard	WG-Firebox-Mgmt	Any-Trusted, Any-Optional	Firebox

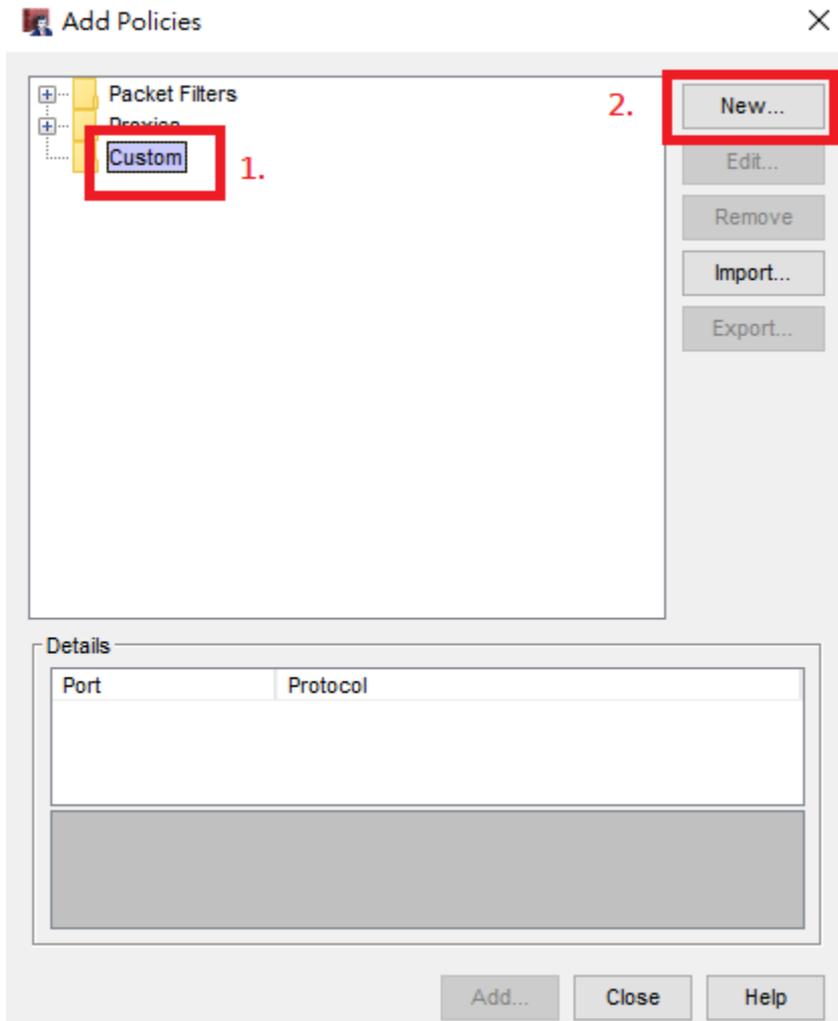


- Add Policy...
- Modify Policy...
- Delete
- Large Icons View
- Auto-Order Mode
- Policy Tags >
- Policy Highlighting...

Step 1 :

Policy Manager空白處按右鍵點選Add Policy

設定Service Group

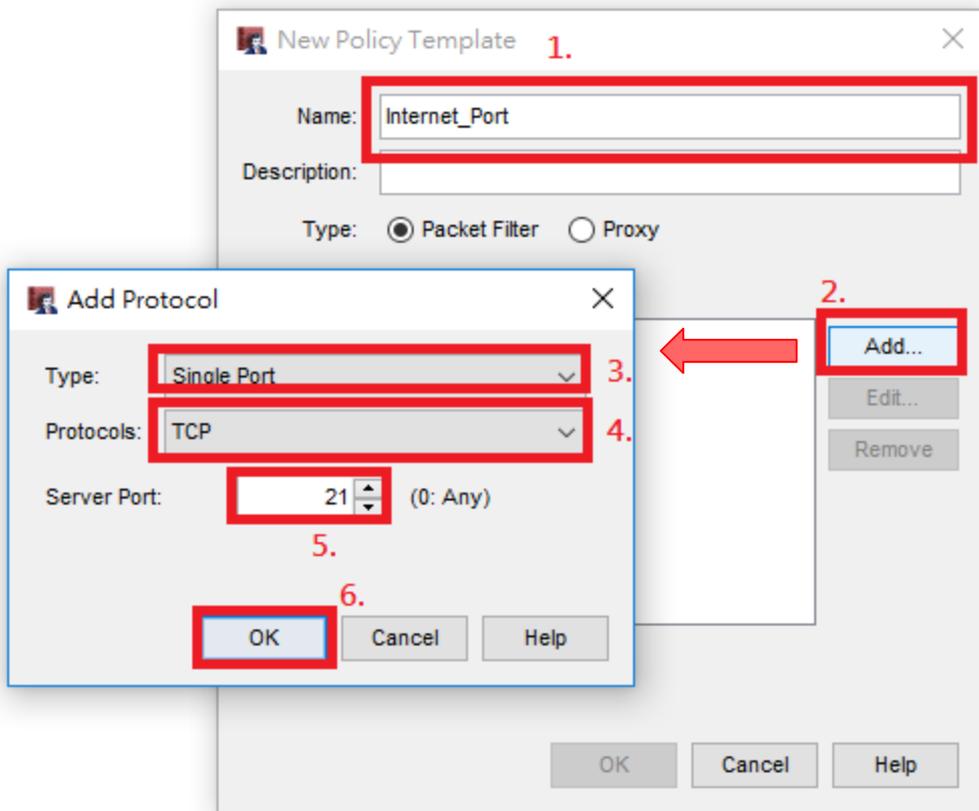


Step 2 :

1. 點選Custom
2. 點選New

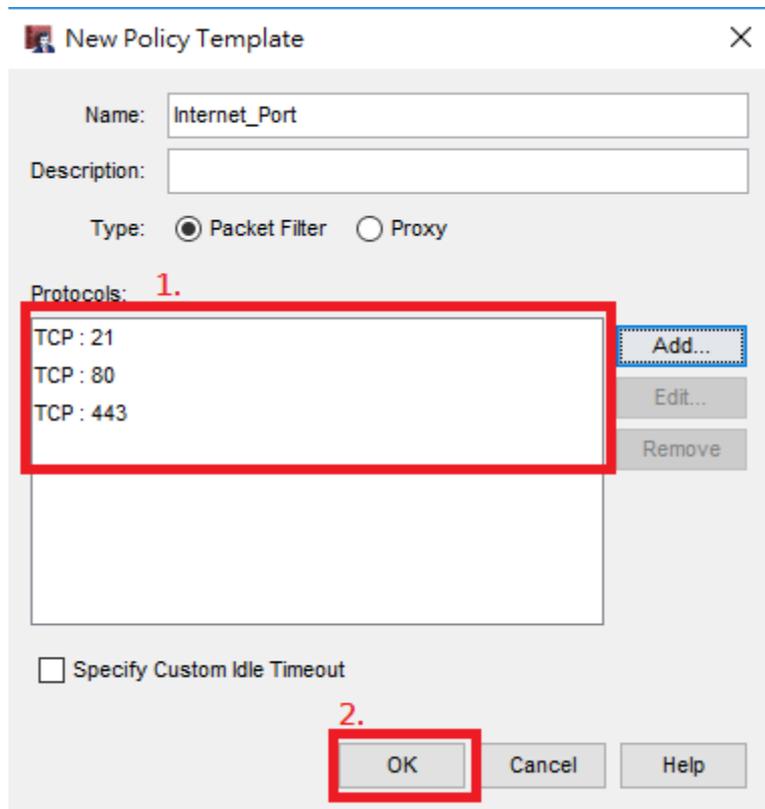
設定Service Group

Step 3 :



1. Name : 輸入Port Group名稱
2. 點選Add
3. Type : 選擇Single Port或是Port Range
4. Protocols : 選擇所要使用的類型
5. Server Port : 輸入要使用的Port
6. 點選OK

設定Service Group



New Policy Template

Name: Internet_Port

Description:

Type: Packet Filter Proxy

Protocols: 1.

- TCP : 21
- TCP : 80
- TCP : 443

Buttons: Add... Edit... Remove

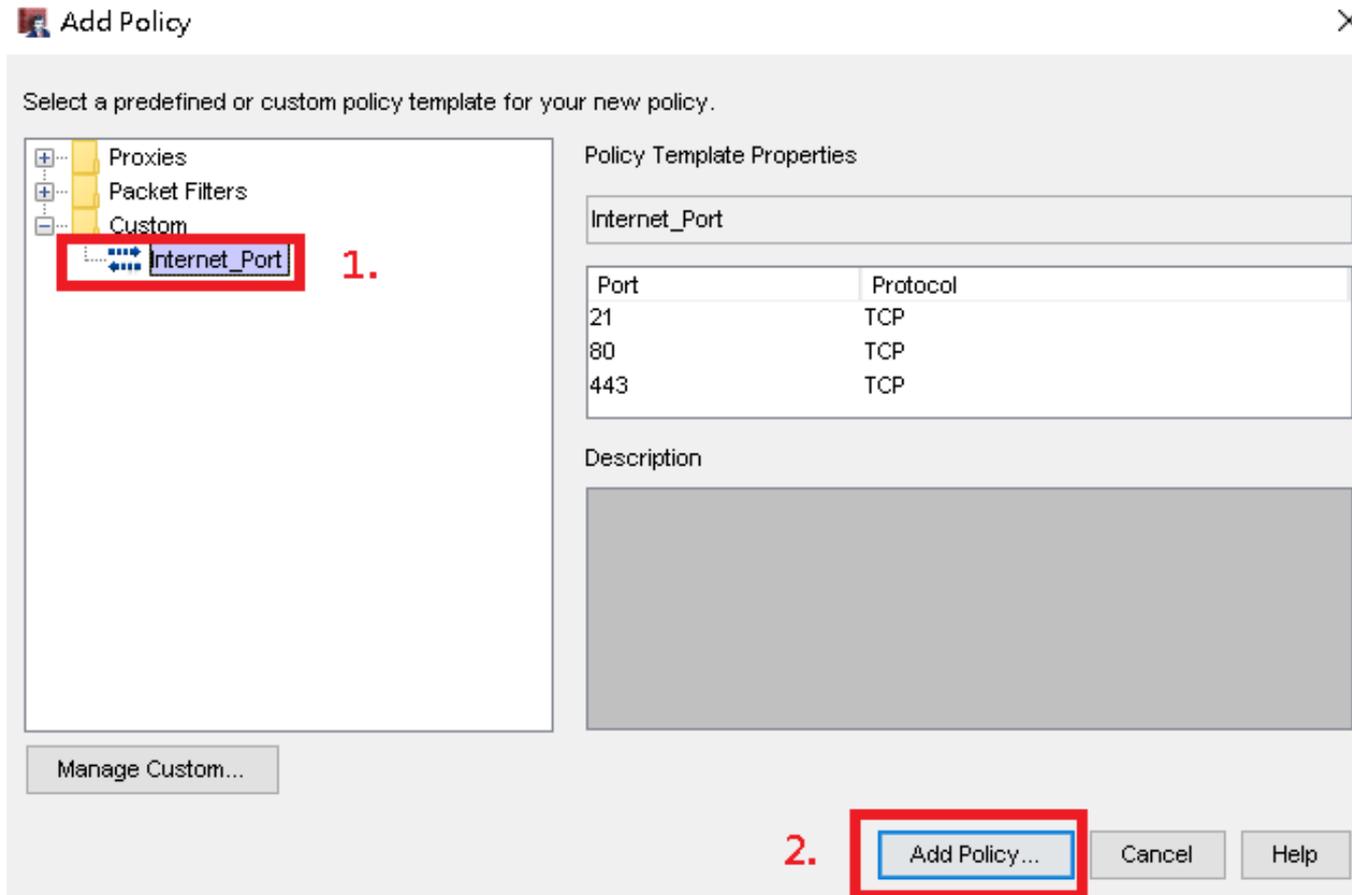
Specify Custom Idle Timeout

Buttons: 2. OK Cancel Help

Step 4 :

1. 確認要控制的Port輸入完成
2. 點選OK

新增Policy



- Step 1 :
1. 點選先前所新增的Custom Port
 2. 點選下方Add

新增Policy

New Policy Properties

Name: Enable

Policy Properties Advanced **1.**

Internet_Port connections are...

Allowed

From

2.

4.

To

3.

Route outbound traffic using (Fireware OS v12.3 or higher)

SD-WAN Action

Enable Application Control:

Enable Geolocation:

Enable IPS for this policy

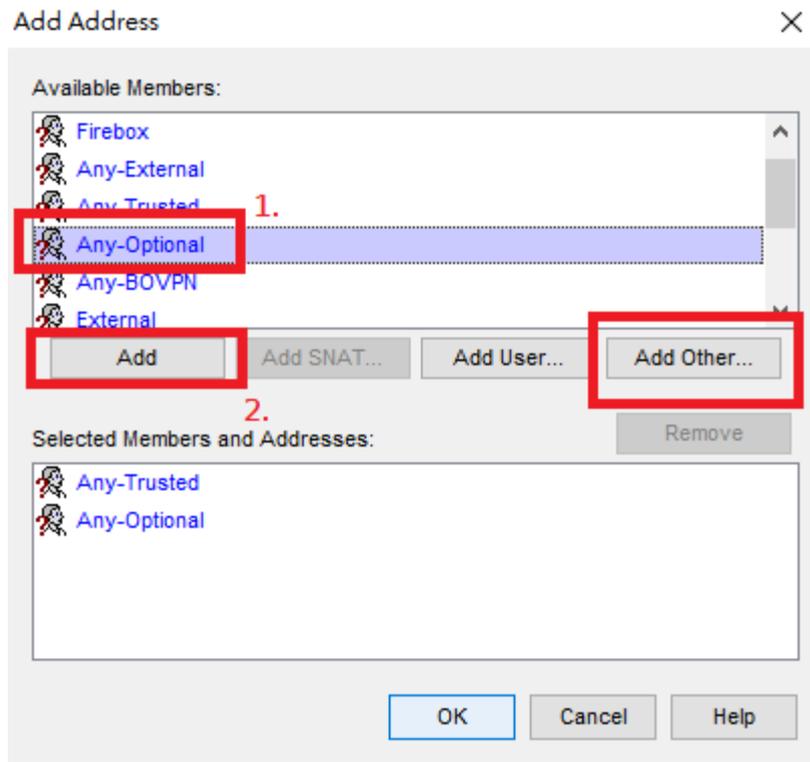
Enable bandwidth and time quotas (Fireware OS v11.10 and higher)

Proxy action:

Step 2 :

1. Name : 輸入Policy名稱
2. From – 來源
3. To – 目的地
4. 點選Add修改來源位置，如目的地位置需要修改，點選To下方Add進行修改

新增Policy



Step 3 :

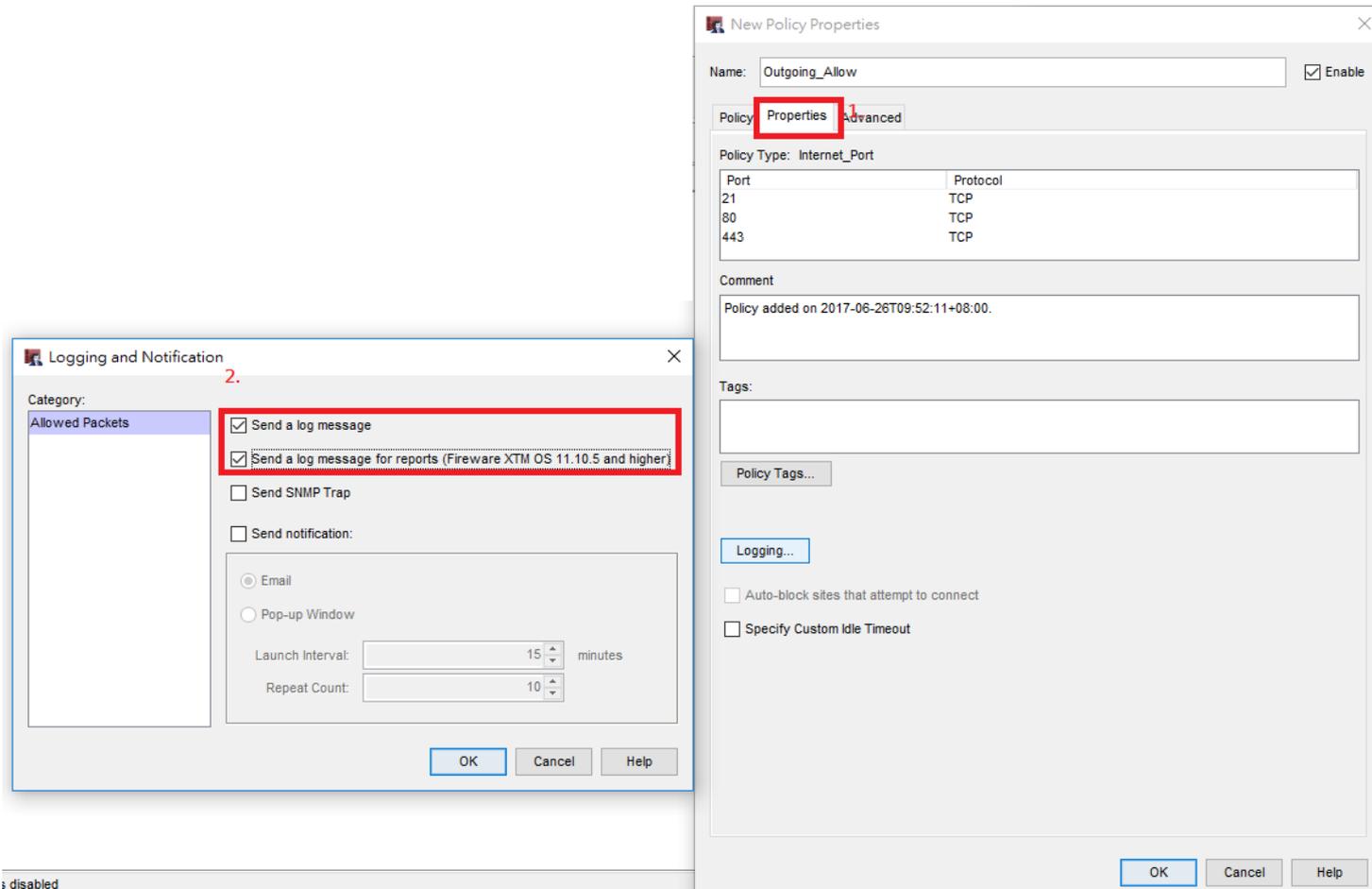
本範例為內部網段可以出Internet

1. 點選Any-Optional，預設來源已經有Any-Trusted，將Any-Optional加入後即允許內部所有網段。

2. 點選Add

如需要加入其他型態的來源時，點選Add Other來選擇。

設定Policy Log



1. 點選Properties

2. 將Send a log message以及Send log message for report

確認Policy設定

untitled.xml *- Firewall Policy Manager

File Edit View Setup Network FireCluster VPN Subscription Services Help

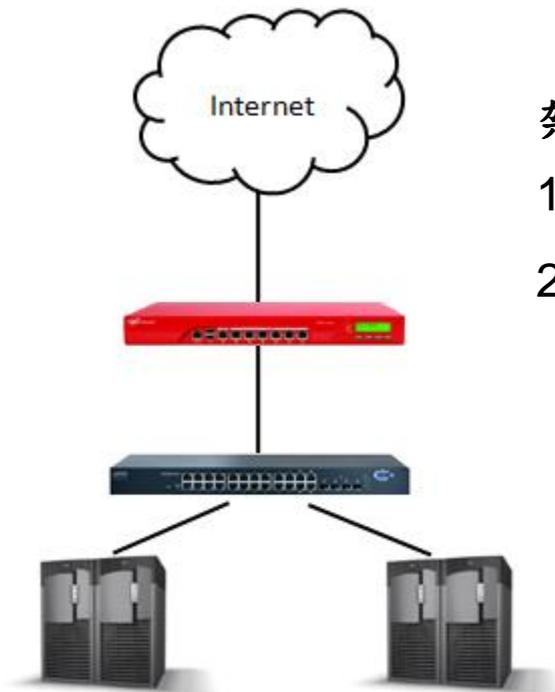
Firewall Mobile VPN with IPSec

Filter: None

Order /	Action	Policy Name	Policy Type	From	
1	✓	WatchGuard Web UI	WG-Fireware-XTM-WebUI	Any-Trusted, Any-Optional	Firebox
2	✓	Ping	Ping	Any-Trusted, Any-Optional	Any
3	✓	Outgoing-Allow	Internet_Port	Any-Trusted, Any-Optional	Any-External
4	✓	WatchGuard	WG-Firebox-mgmt	Any-Trusted, Any-Optional	Firebox
5	✓	Outgoing	TCP-UDP	Any-Trusted, Any-Optional	Any-External

Policy設定完成後顯示於Policy Manager

原則範例情境二



架構說明

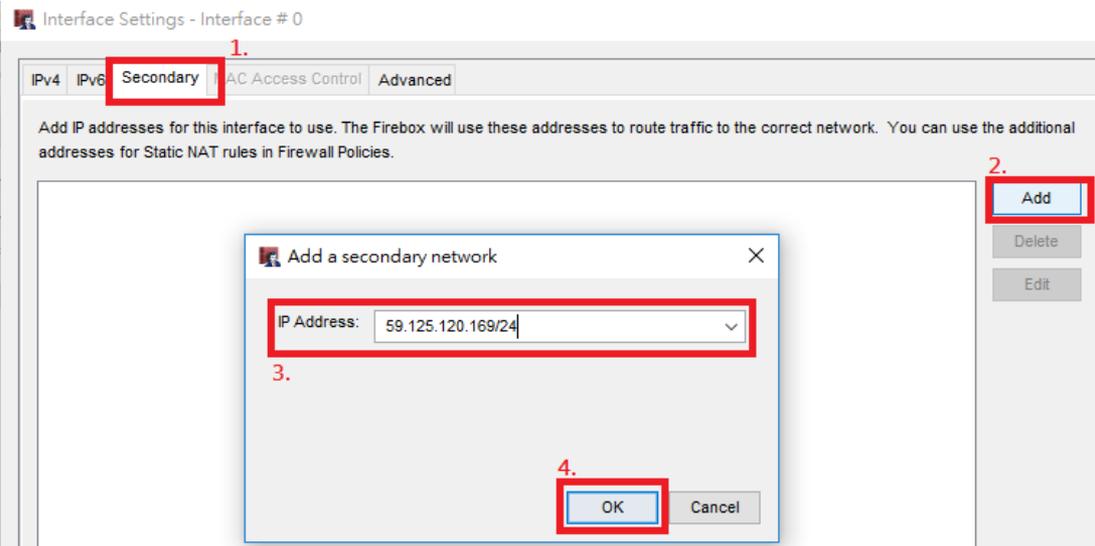
1. Mail Server要提供對外服務
2. 對外開啟TCP 25,110以及443三個Port

Mail Server

外部IP 59.125.120.170

內部IP 192.168.1.100

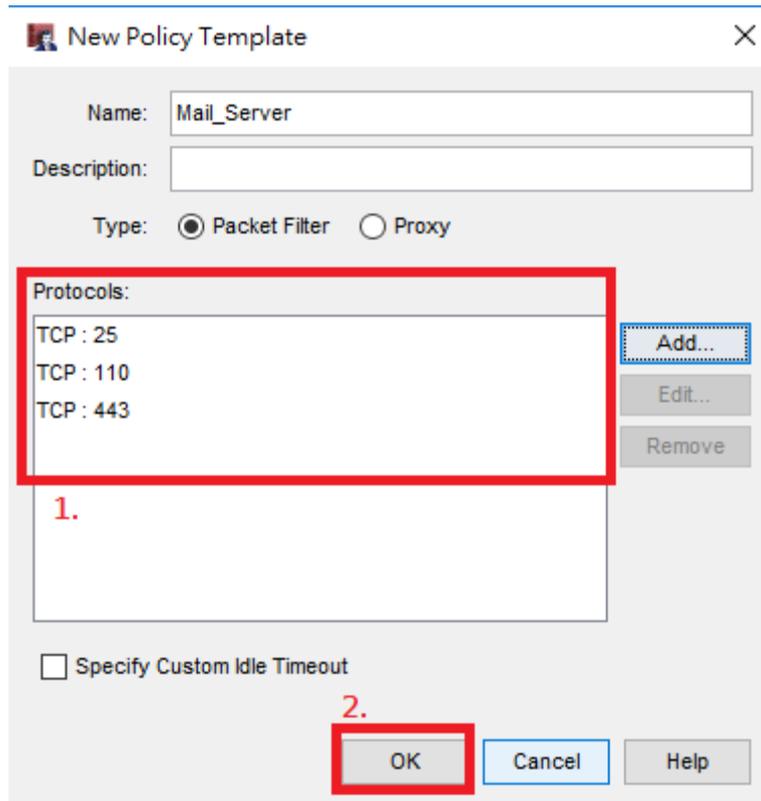
設定 Secondary IP Address



1. 於External Interface點選上方 Secondary
2. 點選Add
3. 輸入IP Address和子網路遮罩
4. 點選OK

Note : 要開放對外服務的IP必須事先設定好External Secondary IP Address

新增Service Group



New Policy Template

Name: Mail_Server

Description:

Type: Packet Filter Proxy

Protocols:

- TCP : 25
- TCP : 110
- TCP : 443

1.

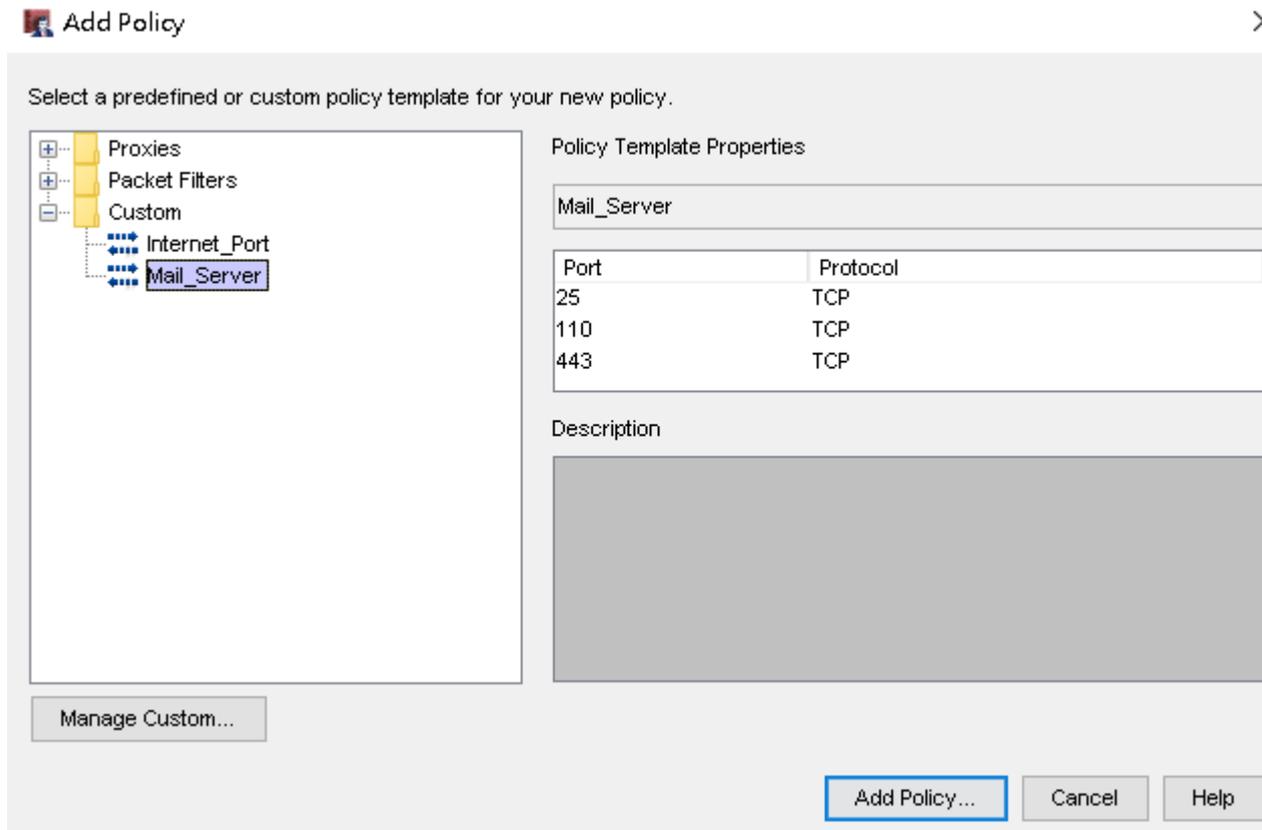
Specify Custom Idle Timeout

2.

OK Cancel Help

1. 新增TCP 25,110以及443 Service Group
2. 點選OK

新增對外服務Policy



- Step 1 :
1. 點選新增的Service Group
 2. 點選Add



新增對外服務Policy

New Policy Properties

Name: Enable

Policy Properties Advanced

Mail_Server connections are...

Allowed Send TCP RST

From

Any-Trusted 1.

Add... Edit... Remove

To

Any-External 2.

Add... Edit... Remove 3.

Route outbound traffic using (Fireware OS v12.3 or higher)

SD-WAN Action

Enable Application Control:

Enable Geolocation:

Enable IPS for this policy

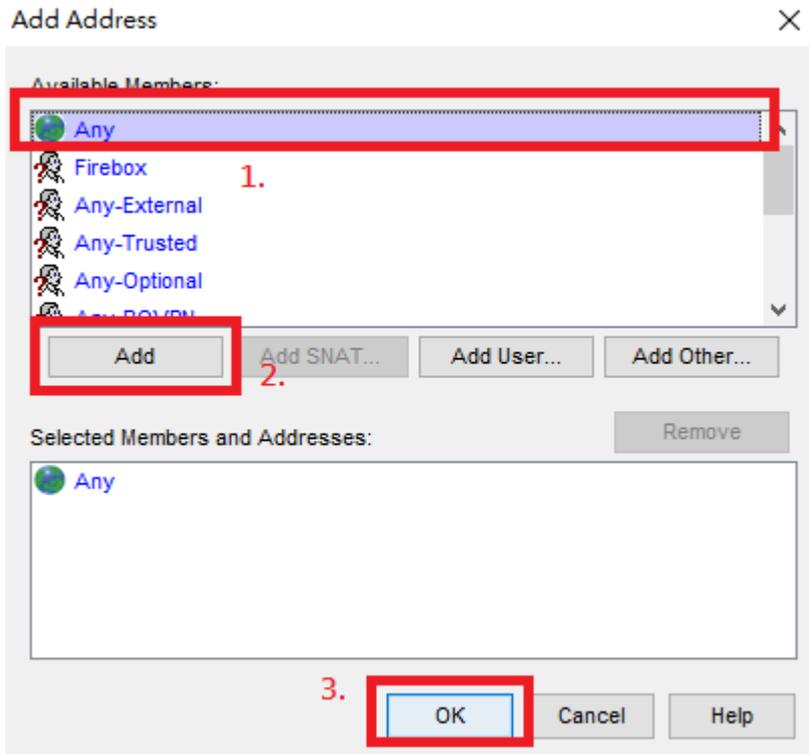
Enable bandwidth and time quotas (Fireware OS v11.10 and higher)

Proxy action:

Step 2 :

1. Name : 輸入Policy名稱
2. 點選Any-External
3. 點選Remove
4. 點選From欄位下方Add

選擇來源位置



1. 此要開起對外服務的Policy，來源位置選擇Any
2. 點選Add
3. 點選OK

設定SNAT

New Policy Properties ×

Name: Enable

Policy Properties Advanced

Mail_Server connections are...

Allowed

From

 Any

To

 None

Route outbound traffic using (Fireware OS v12.3 or higher)

SD-WAN Action

Enable Application Control:

Enable Geolocation:

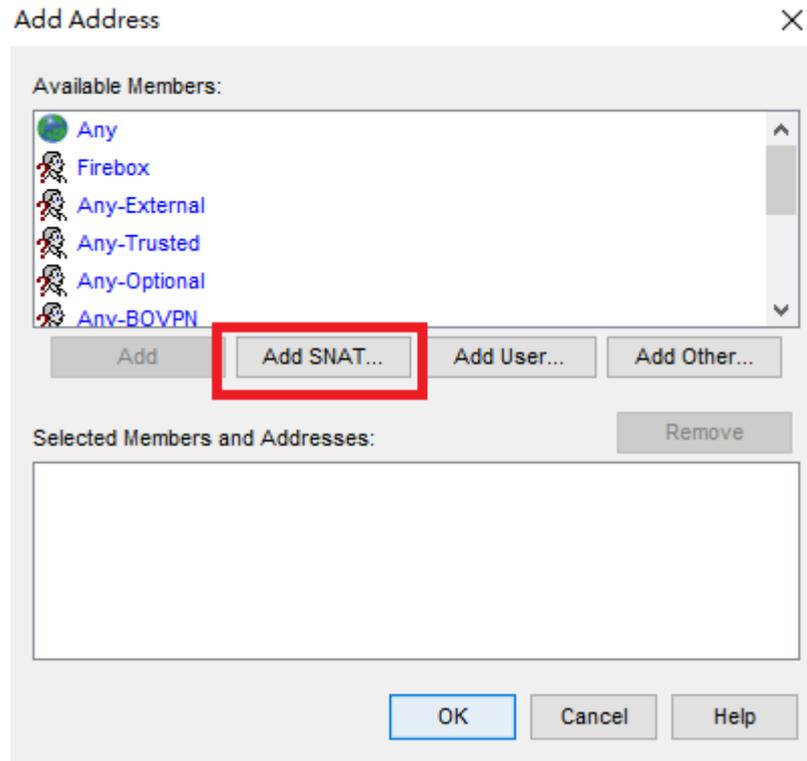
Enable IPS for this policy

Enable bandwidth and time quotas (Fireware OS v11.10 and higher)

Proxy action:

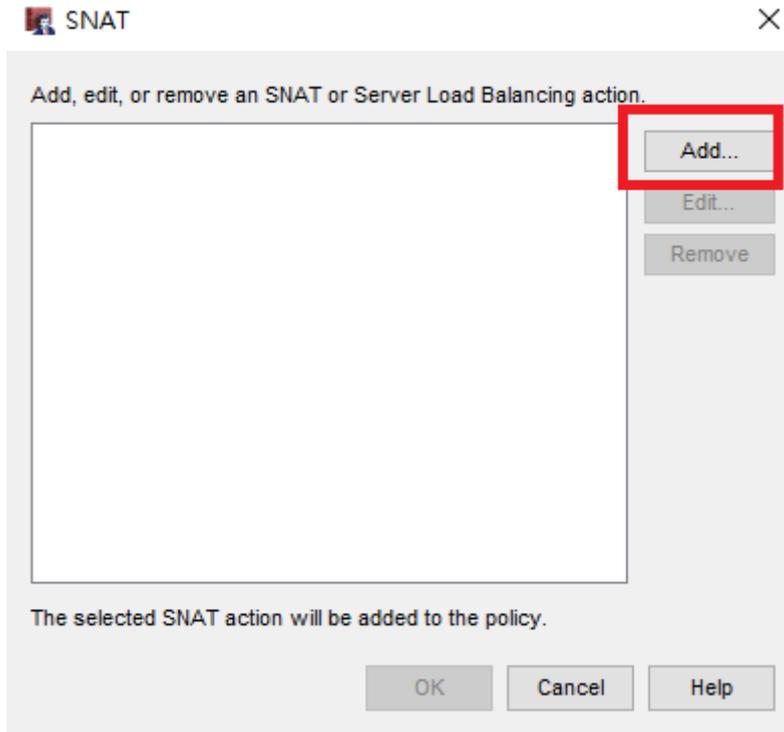
點選To欄位下方Add

設定SNAT



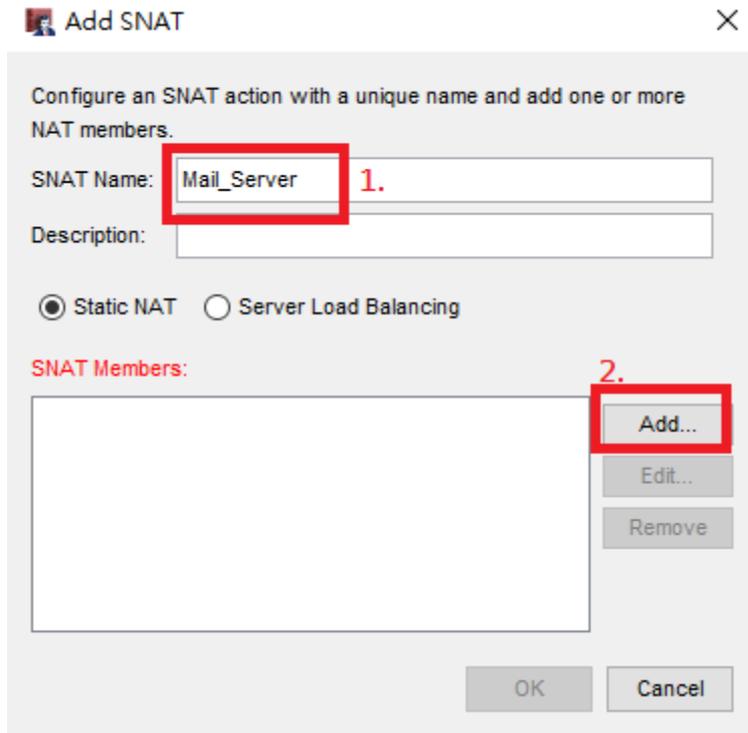
點選Add SNAT

設定SNAT



SNAT視窗點選Add

設定SNAT

 Add SNAT

Configure an SNAT action with a unique name and add one or more NAT members.

SNAT Name: 1.

Description:

Static NAT Server Load Balancing

SNAT Members:

2.

1. 設定SNAT名稱

2. 點選Add

設定SNAT

Add Static NAT

External/Optional IP Address: 1.

Set source IP

Internal IP Address: 2.

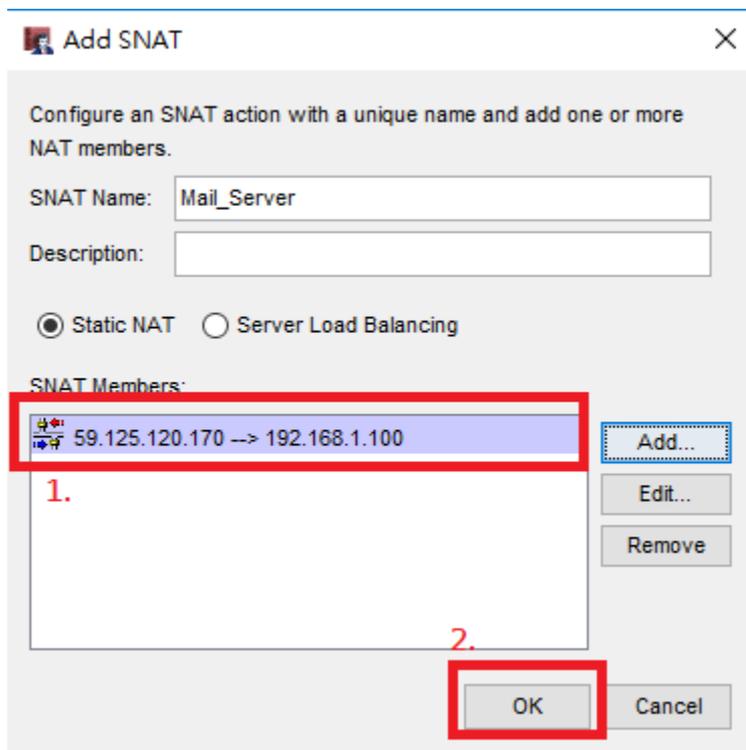
Set internal port to a different port

(Static NAT for an Optional IP address requires Fireware XTM OS v11.8.1 or higher)

3.

1. 於下拉式選單選擇外部IP Address
2. 輸入Server Private IP Address
3. 點選OK

確認內外部IP對應設定



Add SNAT

Configure an SNAT action with a unique name and add one or more NAT members.

SNAT Name: Mail_Server

Description:

Static NAT Server Load Balancing

SNAT Members:

59.125.120.170 --> 192.168.1.100

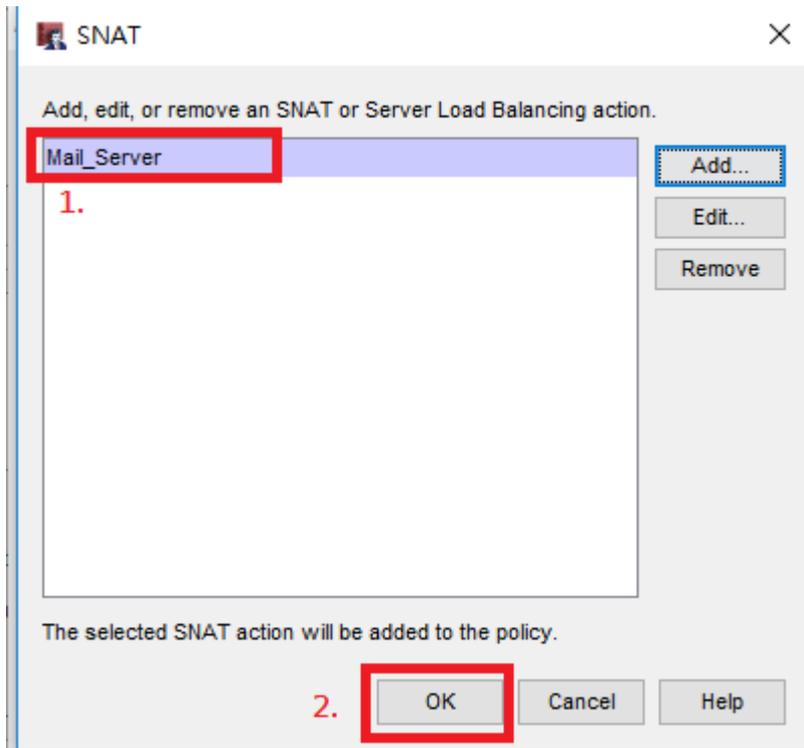
1.

2.

OK Cancel

1. 確認內外部IP對應設定
2. 點選OK

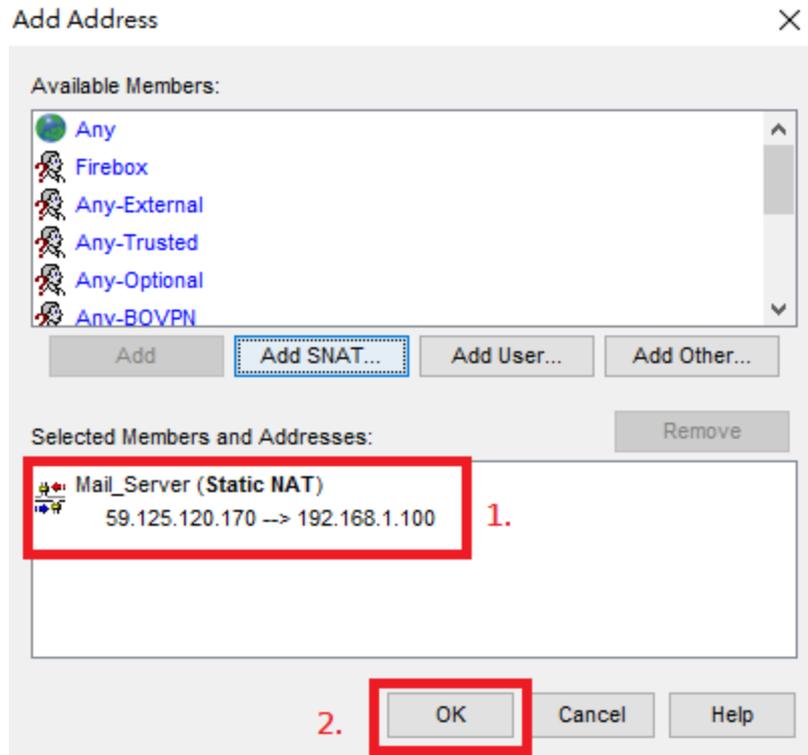
完成SNAT設定



1. 確認SNAT名稱

2. 點選OK

確認目的地SNAT設定



1. 確認目的地SNAT設定
2. 點選OK

完成對外服務Policy設定

Name: Enable

Policy Properties Advanced

Mail_Server connections are...

Allowed

From

 Any

Add... Edit... Remove

To

 newSnat.1 (Static NAT)
 59.125.120.170 --> 192.168.1.100

Add... Edit... Remove

Route outbound traffic using (Fireware OS v12.3 or higher)

SD-WAN Action

Enable Application Control:

Enable Geolocation:

Enable IPS for this policy

Enable bandwidth and time quotas (Fireware OS v11.10 and higher)

Proxy action:

1. 確認Policy設定

2. 點選OK

完成SNAT POLICY 畫面

untitled.xml *- Fireware Policy Manager

File Edit View Setup Network FireCluster VPN Subscription Services Help

Firewall Mobile VPN with IPSec

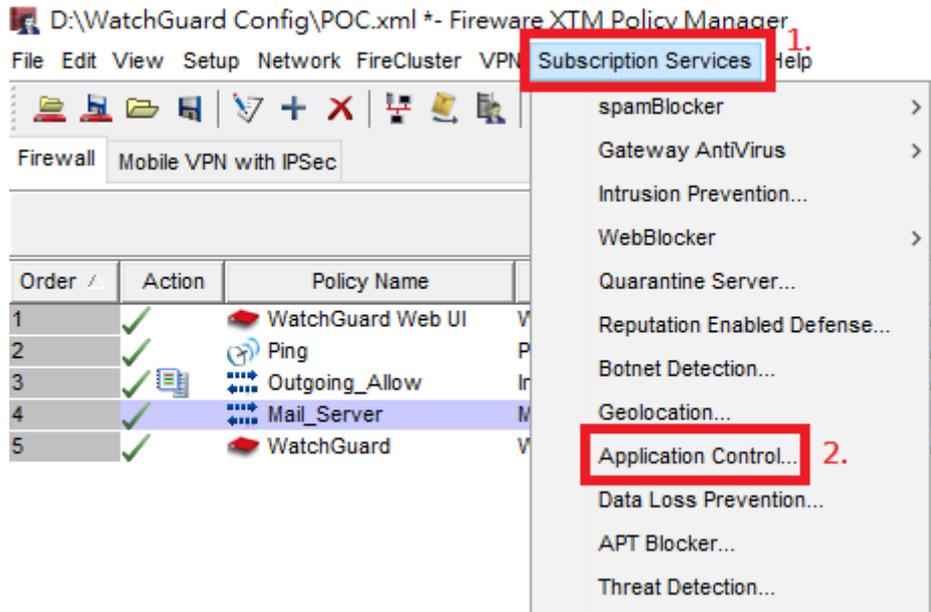
Filter: None

Action	Policy Name	Policy Type	From	To
✓	WatchGuard Web UI	WG-Fireware-XTM-WebUI	Any-Trusted, Any-Optional	Firebox
✓	Ping	Ping	Any-Trusted, Any-Optional	Any
✓	Outgoing_Allow	Internet_Port	Any-Trusted, Any-Optional	Any-External
✓	Mail_Server	Mail_Server	Any	59.125.120.170 --> 192.168.1.100
✓	WatchGuard	WG-Firebox-mgmt	Any-Trusted, Any-Optional	Firebox
✓	Outgoing	TCP-UDP	Any-Trusted, Any-Optional	Any-External

UTM 設定

Application Control設定

設定Application Control



1. Subscription Service

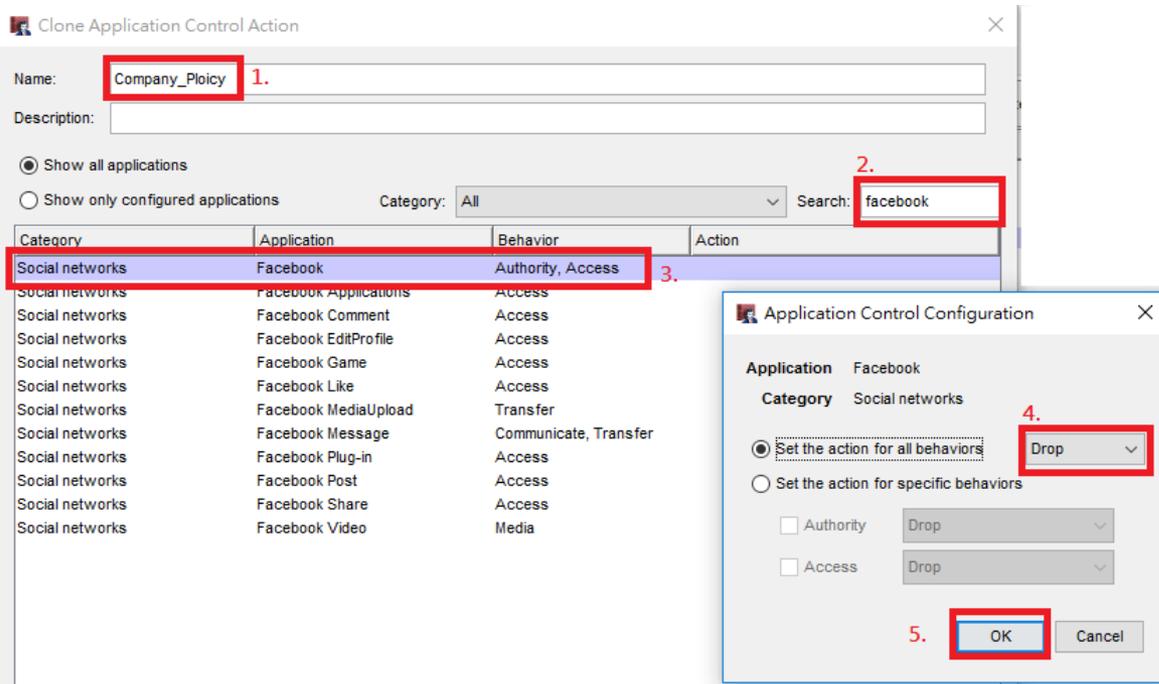
2. 點選Application Control

複製 Global Policy



1. 點選Global
2. 點選Clone

設定要封鎖的Application Control

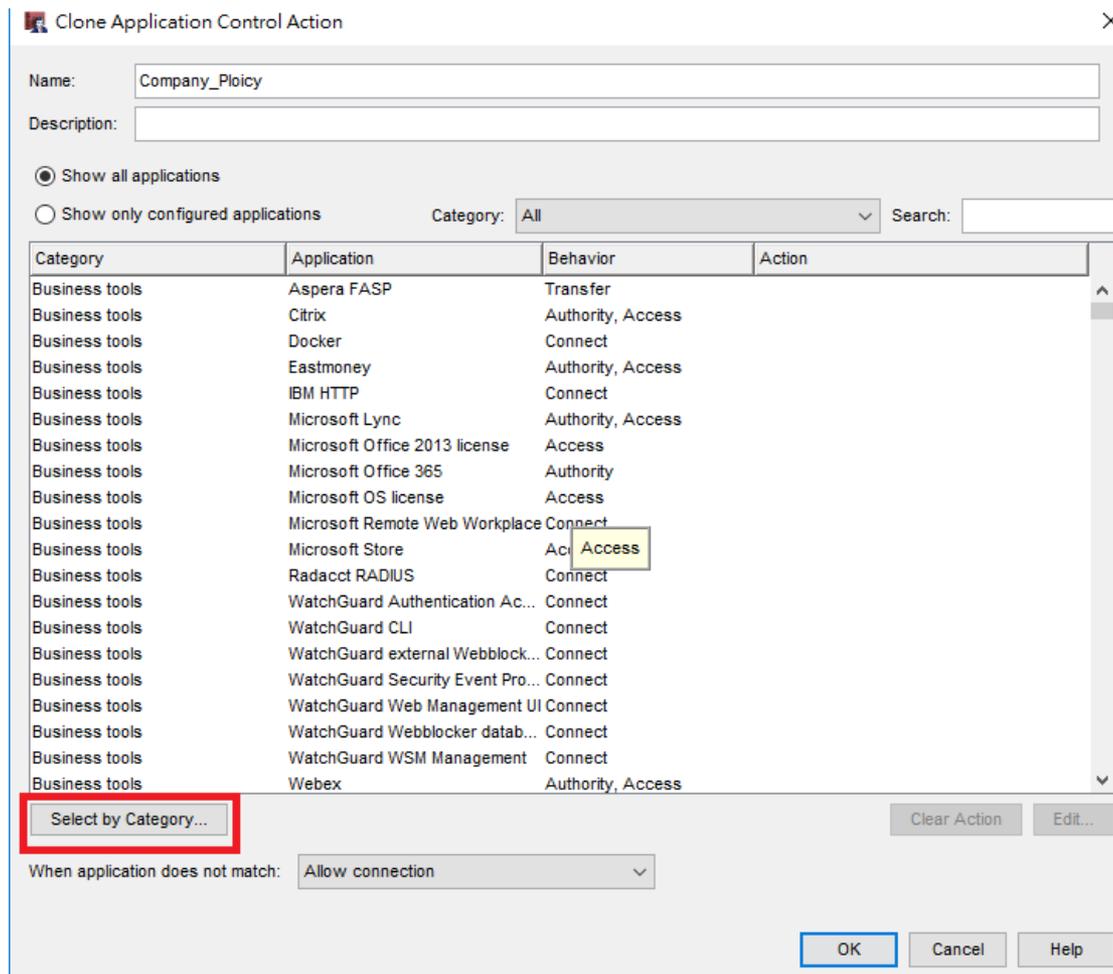


The screenshot shows the 'Clone Application Control Action' dialog box. The 'Name' field is set to 'Company_Ploicy' (1). The 'Search' field is set to 'facebook' (2). A table lists various applications under the 'Social networks' category, with 'Facebook' selected (3). The 'Application Control Configuration' dialog box is open, showing the 'Application' as 'Facebook' and the 'Category' as 'Social networks'. The 'Set the action for all behaviors' radio button is selected, and the 'Drop' dropdown menu is open (4). The 'OK' button is highlighted (5).

Category	Application	Behavior	Action
Social networks	Facebook	Authority, Access	3.
Social networks	Facebook Applications	Access	
Social networks	Facebook Comment	Access	
Social networks	Facebook EditProfile	Access	
Social networks	Facebook Game	Access	
Social networks	Facebook Like	Access	
Social networks	Facebook MediaUpload	Transfer	
Social networks	Facebook Message	Communicate, Transfer	
Social networks	Facebook Plug-in	Access	
Social networks	Facebook Post	Access	
Social networks	Facebook Share	Access	
Social networks	Facebook Video	Media	

1. 設定Application Control政策名稱
2. 搜尋要管控的應用程式
3. 連續點選兩下要控管的應用程式
4. 於下拉式選單選擇要控管的方式
5. 點選OK

依據分類設定封鎖



點選下方Select by category

勾選要封鎖的應用程式分類

Select by Category

Application-specific actions take precedence over category actions

<input type="checkbox"/> Business tools	Drop	<input type="checkbox"/> Database tools	Drop
<input type="checkbox"/> Email messaging services	Drop	<input type="checkbox"/> File sharing services and tools	Drop
<input type="checkbox"/> Instant messengers	Drop	<input type="checkbox"/> Investment platforms	Drop
<input type="checkbox"/> Media streaming services	Drop	<input type="checkbox"/> Network protocols	Drop
<input type="checkbox"/> Network Protocols(1)	Drop	<input type="checkbox"/> Network Protocols(2)	Drop
<input type="checkbox"/> Network Protocols(3)	Drop	<input type="checkbox"/> Online games	Drop
<input checked="" type="checkbox"/> Peer-to-peer networks	Drop	<input type="checkbox"/> Private protocols	Drop
<input type="checkbox"/> Remote access terminals	Drop	<input checked="" type="checkbox"/> Tunnelling and proxy services	Drop
<input type="checkbox"/> Social networks	Drop	<input type="checkbox"/> Security update tools	Drop
<input type="checkbox"/> VoIP services	Drop	<input type="checkbox"/> Web instant messengers	Drop
<input type="checkbox"/> Web services	Drop		

OK Cancel Help

勾選要封鎖的應用程式分類

Application Control Profile設定完成

Clone Application Control Action

Name:

Description:

Show all applications
 Show only configured applications

Category: Search:

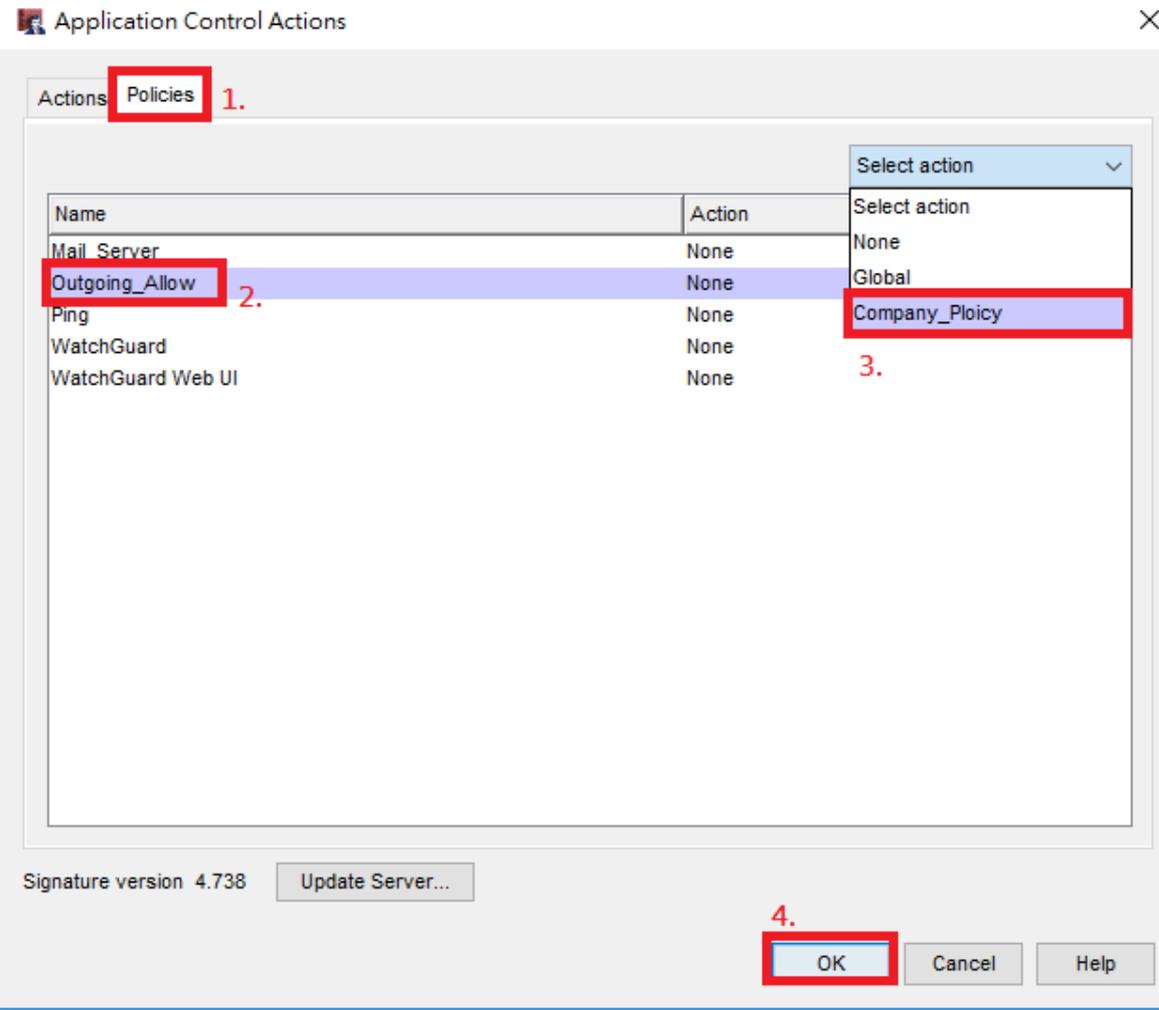
Category	Application	Behavior	Action
Business tools	Aspera FASP	Transfer	
Business tools	Citrix	Authority, Access	
Business tools	Docker	Connect	
Business tools	Eastmoney	Authority, Access	
Business tools	IBM HTTP	Connect	
Business tools	Microsoft Lync	Authority, Access	
Business tools	Microsoft Office 2013 license	Access	
Business tools	Microsoft Office 365	Authority	
Business tools	Microsoft OS license	Access	
Business tools	Microsoft Remote Web Workplace	Connect	
Business tools	Microsoft Store	Access	
Business tools	Radacct RADIUS	Connect	
Business tools	WatchGuard Authentication Ac...	Connect	
Business tools	WatchGuard CLI	Connect	
Business tools	WatchGuard external Webblock...	Connect	
Business tools	WatchGuard Security Event Pro...	Connect	
Business tools	WatchGuard Web Management UI	Connect	
Business tools	WatchGuard Webblocker datab...	Connect	
Business tools	WatchGuard WSM Management	Connect	
Business tools	Webex	Authority, Access	

Select by Category...

When application does not match:

要控管的應用程式設定好之後點選OK完成Application Profile設定

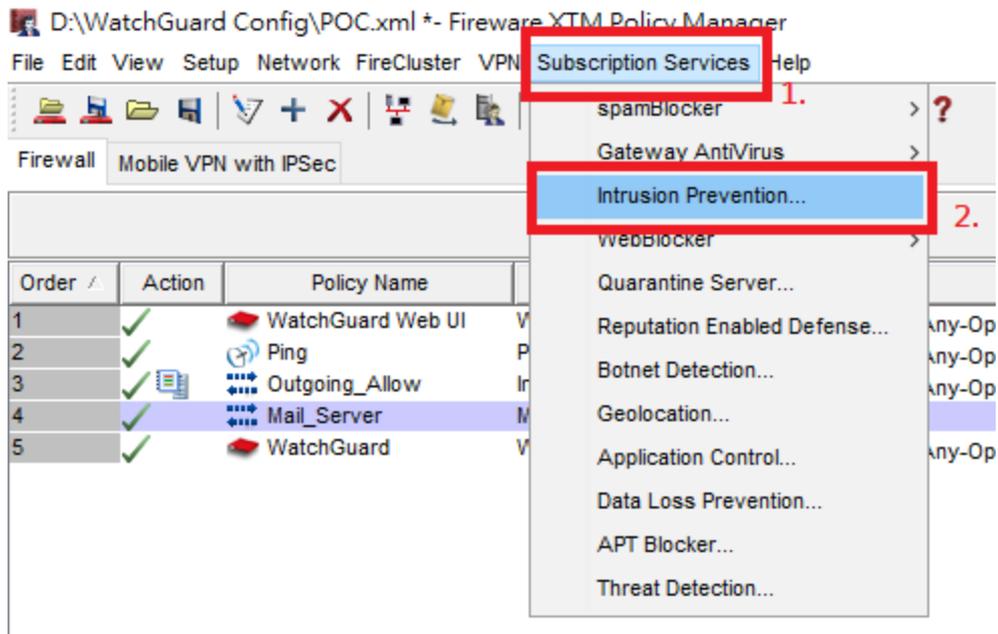
設定Application Control要套用的Policy



1. 點選上方Policies
2. 點選要套用的Policy
3. 於下拉式選單選擇要套用的Application Control Profile
4. 點選OK

IPS設定

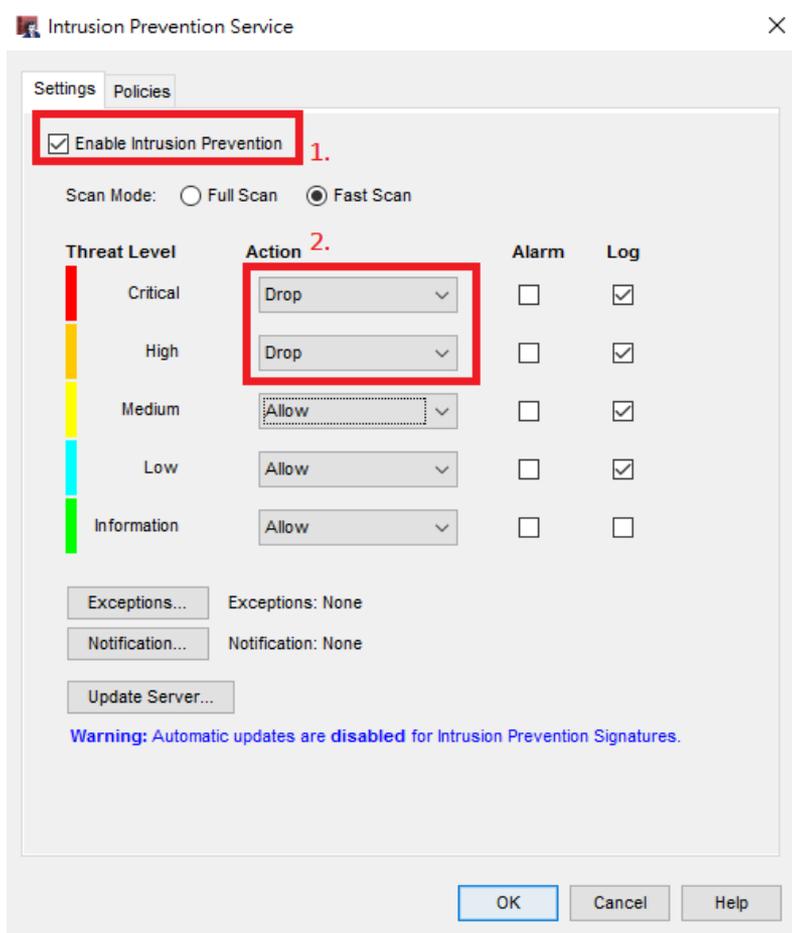
設定IPS



1. Subscription Service

2. 點選Intrusion Prevention

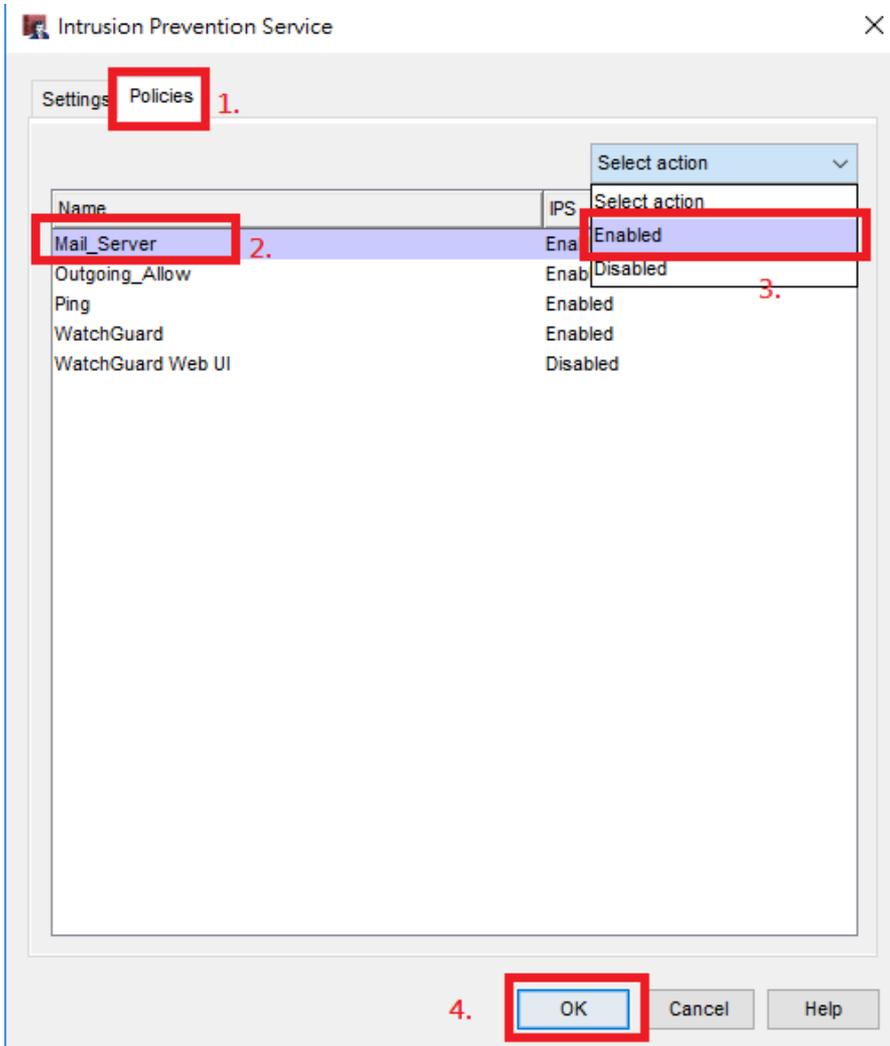
封鎖風險等級設定



1. 勾選Enable Intrusion Prevention

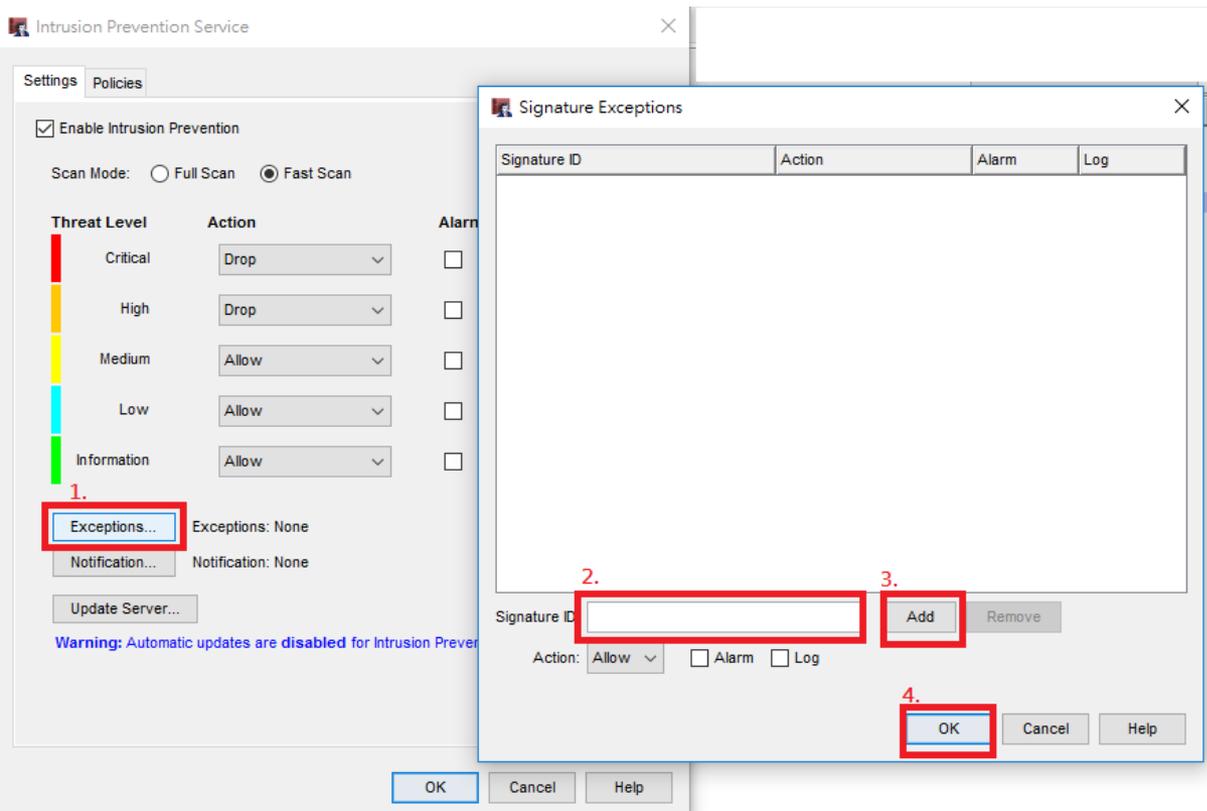
2. 將要風選的風險等級選擇Drop

選擇要套用的Policy



1. 點選上方Policies
2. 點選要套用的Policy
3. 於下拉式選單選擇要開啟或關閉Policy
4. 點選OK

IPS例外清單設定



1. 點選Exception

2. 輸入要排除的Signature ID

3. 點選Add

4. 點選OK

Note : Signature ID可於System Manager或是在報表中查詢

Traffic Manager設定

Traffic Manager說明

WatchGuard Traffic 可依據下列幾種方式進行設定

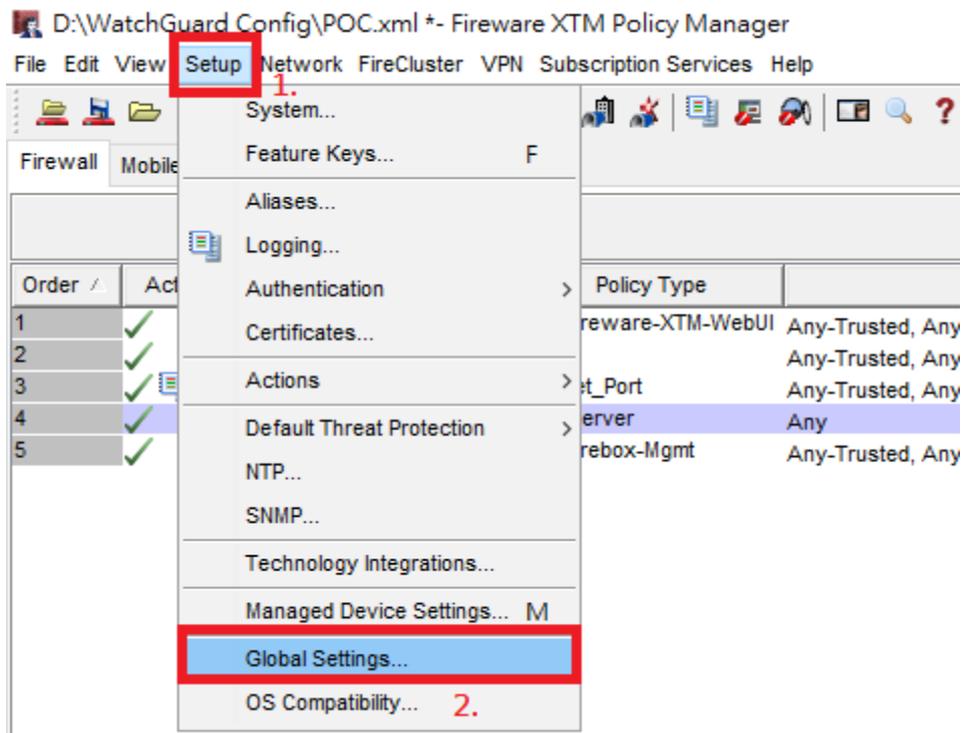
1. 限制內部每個IP可使用的對外頻寬
2. 保障內部某個IP或是服務的對外頻寬
3. 限制某個應用程式的對外頻寬

啟用 Traffic Manager

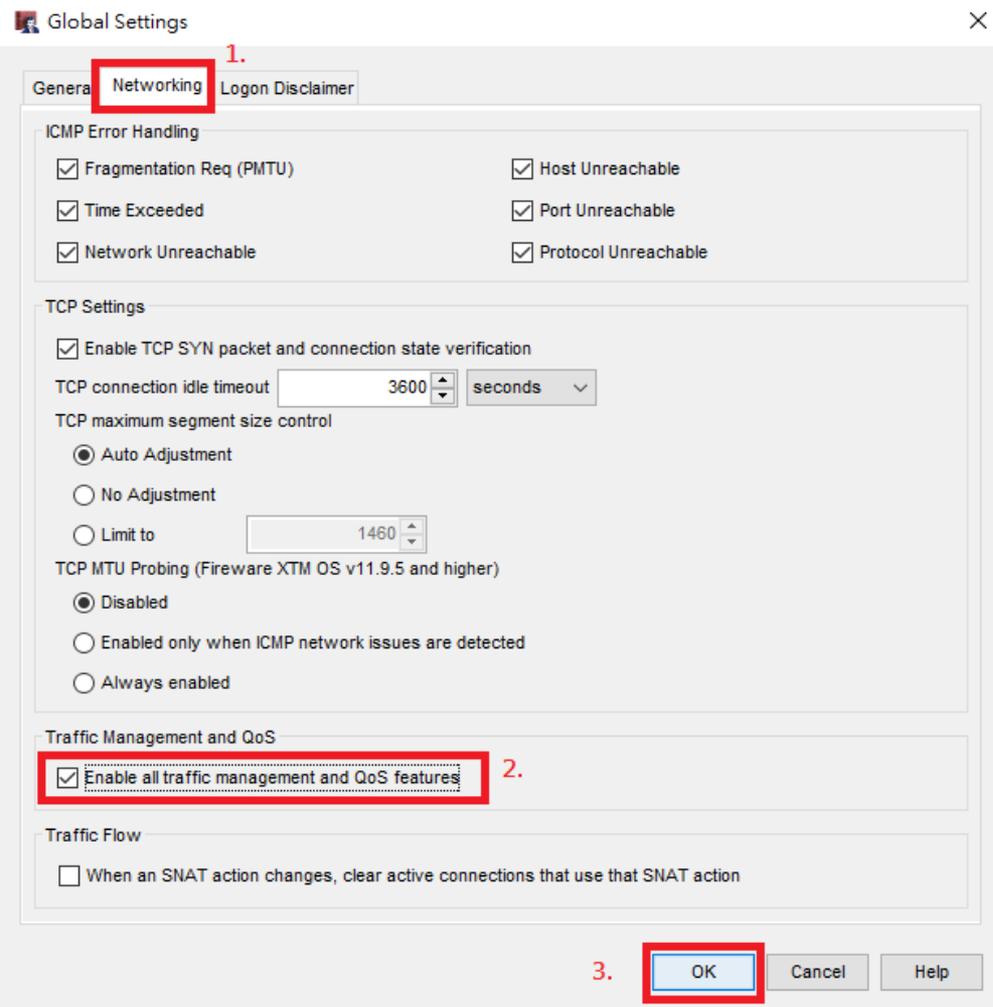
Step 1 :

1. 點選 Setup

2. 點選 Global Settings



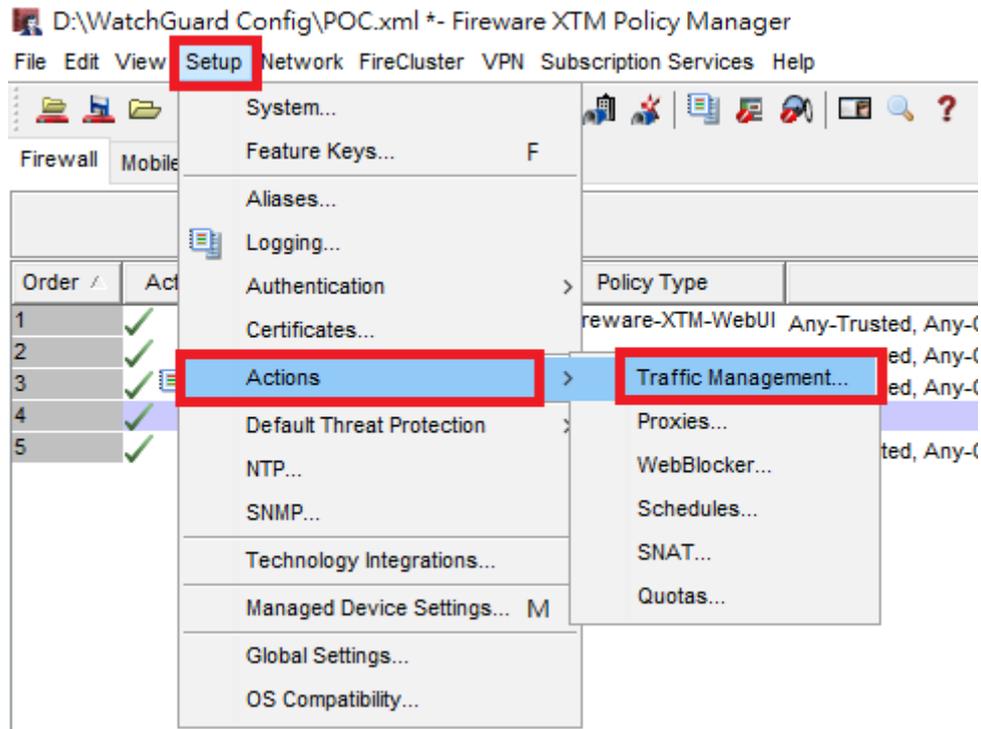
啟用 Traffic Manager



Step 2 :

1. 點選 Networking
2. 點選 Enable all traffic management and QoS feature
3. 點選 OK

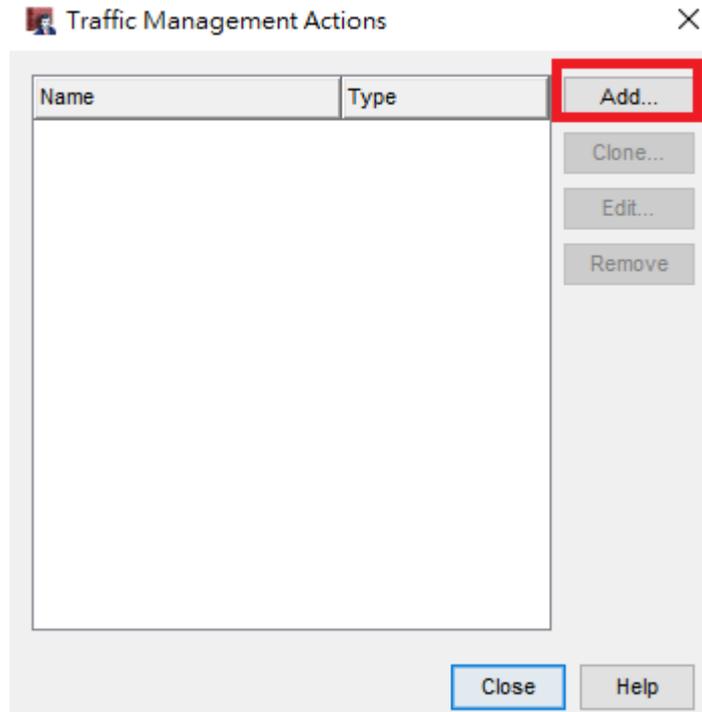
設定Traffic Manager Profile



Step 1 :

Setup → Actions → Traffic Management

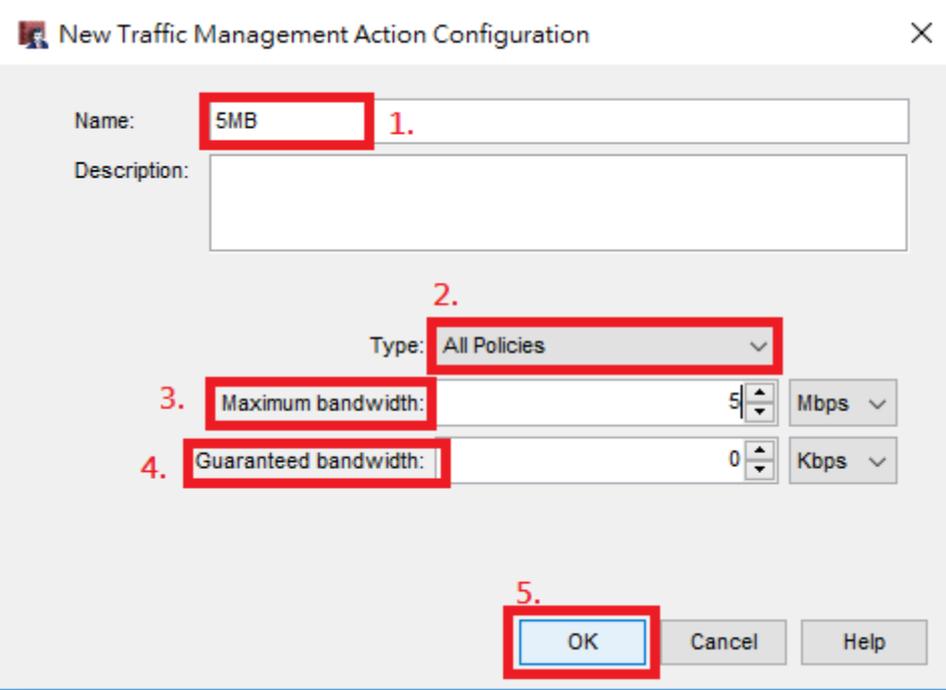
設定Traffic Manager Profile 2



Step 2 :

點選Add

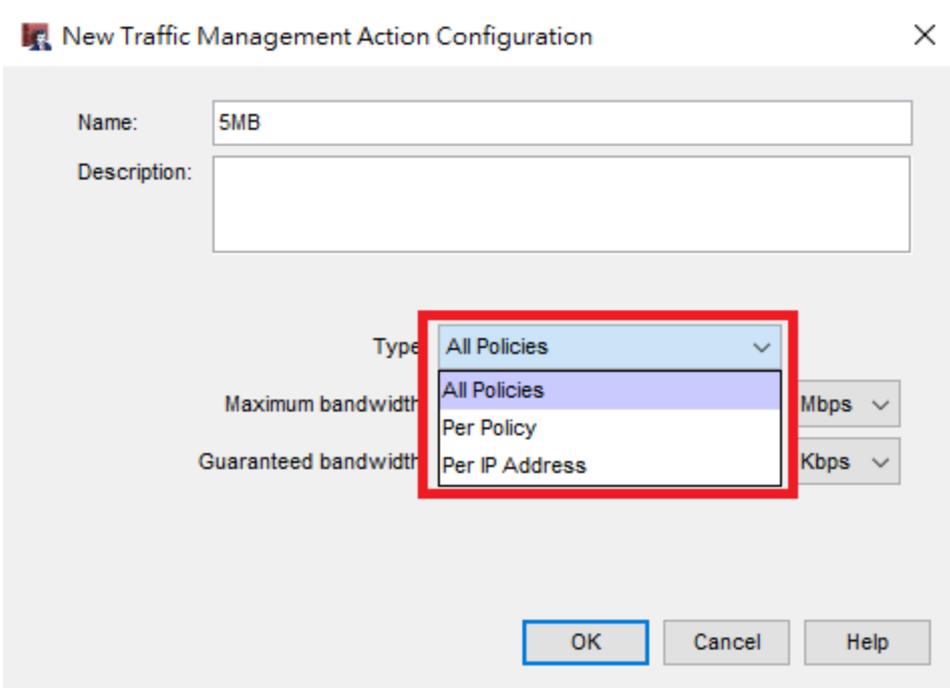
設定Traffic Manager Profile



Step 3 :

1. 設定Traffic management Profile 名稱
2. 選擇Profile Type
3. Maximum Bandwidth : 最大頻寬，套用此Profile Policy可使用的頻寬上限
4. Guaranteed Bandwidth : 保證頻寬，套用到此Profile的Policy至少可使用的頻寬下限。
5. 點選OK

Traffic Manager Profile Type說明



New Traffic Management Action Configuration

Name: SMB

Description:

Type: All Policies

Maximum bandwidth: Mbps

Guaranteed bandwidth: Kbps

OK Cancel Help

1. **All Policies** – 整台防火牆只要套用到這個Profile的Policy共同Share所設定的頻寬
2. **Per Policy** – 防火牆中個別Policy套用到這個Profile皆獨立可使用所設定的頻寬
3. **Per IP Address** – Policy中每一個IP都可以獨立使用所設定的頻寬。

Per IP Address設定

New Traffic Management Action Configuration

Name: 5MB

Description:

Type: Per IP Address

Maximum bandwidth: 5 Mbps

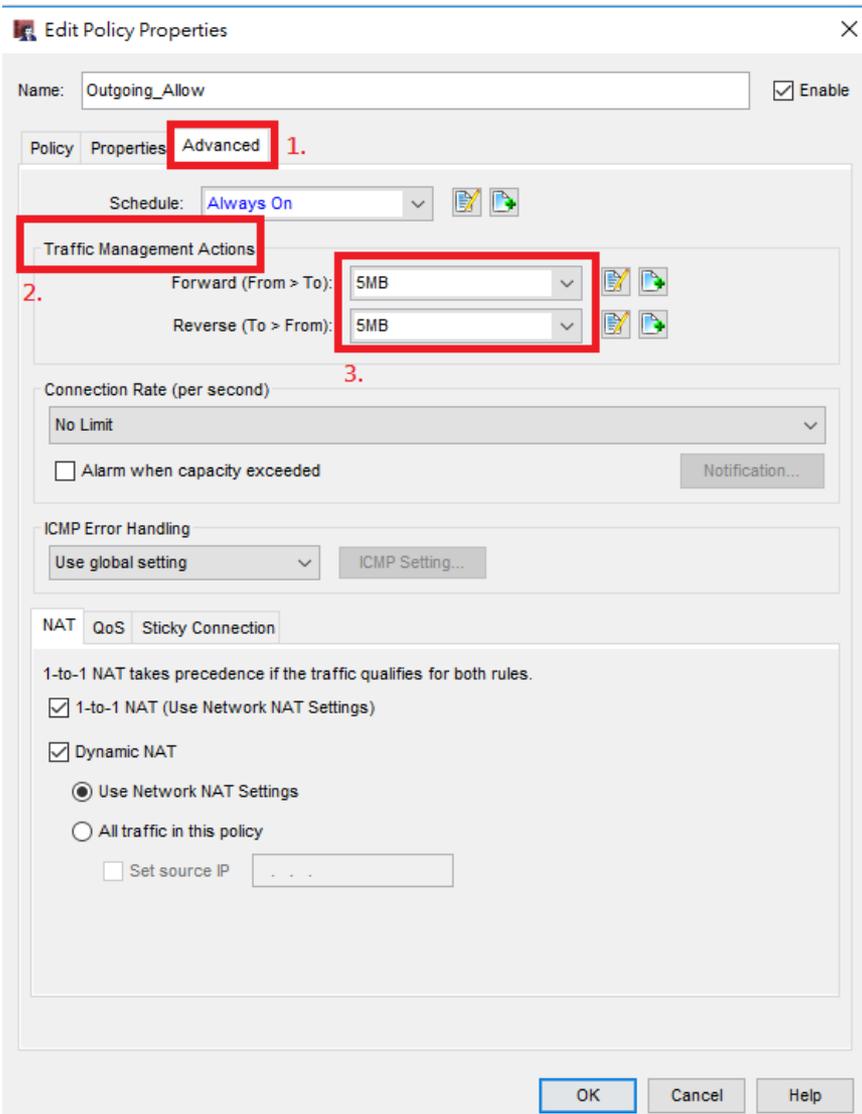
Guaranteed bandwidth: 0 Kbps

Maximum instance: 256

OK Cancel Help

Type 設定Per IP Address時，Maximum instance設定256

Traffic Manager Profile 套用至Policy



1. 編輯Policy點選Advance

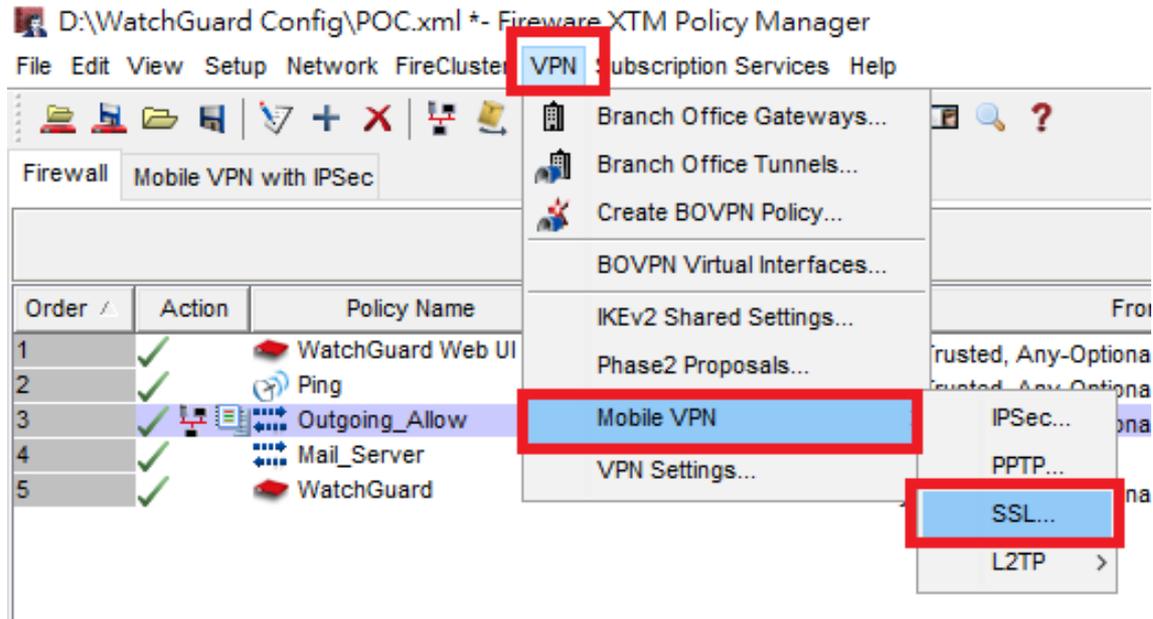
2. Traffic Management Action 中選擇設定好的Profile

Forward – 上傳頻寬

Reverse – 下載頻寬

VPN 設定

啟用SSL VPN設定



Step 1 :

VPN → Mobile VPN → SSL



啟用SSL VPN設定

Mobile VPN with SSL Configuration

When you activate Mobile VPN with SSL, the "SSLVPN-Users" group and the "WatchGuard SSLVPN" policy are created to allow Mobile VPN with SSL connections from the Internet to the external interface.

Activate Mobile VPN with SSL 1.

General Authentication Advanced

Firebox IP Addresses

Type or select a Firebox IP address or domain name for SSL VPN users to connect to.

Primary: Backup: 2.

Networking and IP Address Pool

Choose the method the Firebox uses to send traffic through the VPN tunnel. Select **Bridge VPN traffic** if you want to bridge the user to a network you specify. Select **Route VPN traffic** if you want the Firebox to route VPN traffic to specified networks and resources.

Force all client traffic through tunnel 3.

Allow access to all Trusted, Optional, and Custom networks

Specify allowed resources

Virtual IP Address Pool

Enter a subnet that is not used by computers locally connected to the Firebox. Your Firebox allows 65 Mobile VPN with SSL user(s).

4.

Step 2 :

1. 勾選Active Mobile VPN with SSL
2. 選擇要提供給SSL VPN連線的IP
3. Force all client traffic through tunnel – 勾選此選項，連線SSL VPN的電腦所有流量都會經過VPN Tunnel。
4. 輸入SSL VPN所可以取得的IP Pool

SSL VPN DNS參數設定

Mobile VPN with SSL Configuration

When you activate Mobile VPN with SSL, the "SSLVPN-Users" group and the "WatchGuard SSLVPN" policy are created to allow Mobile VPN with SSL connections from the Internet to the external interface.

Activate Mobile VPN with SSL

General Authentication **Advanced** 1.

Authentication: SHA-1

Encryption: AES (256-bit)

Data channel: TCP : 443

Configuration channel: TCP : 443

Keep-alive: Interval: 10 seconds
Timeout: 60 seconds

Renegotiate data channel: Interval: 61 minutes

DNS and WINS Servers

Domain name: 2.

DNS servers: 192.168.1.100

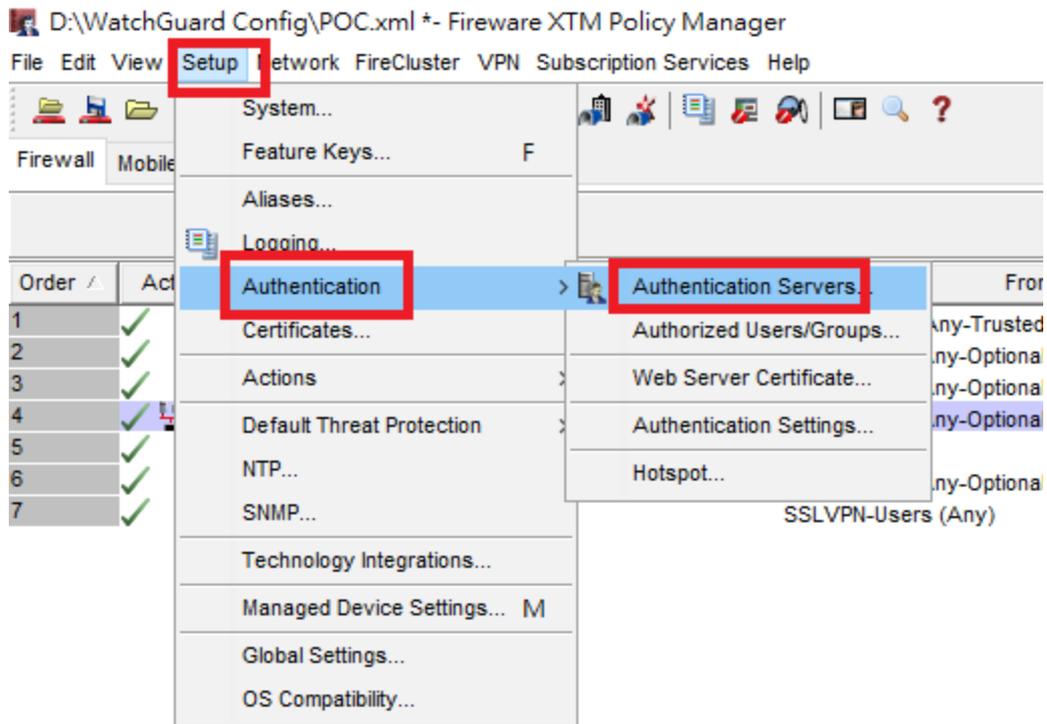
WINS servers: . . .

Restore Defaults

3. OK Cancel Help

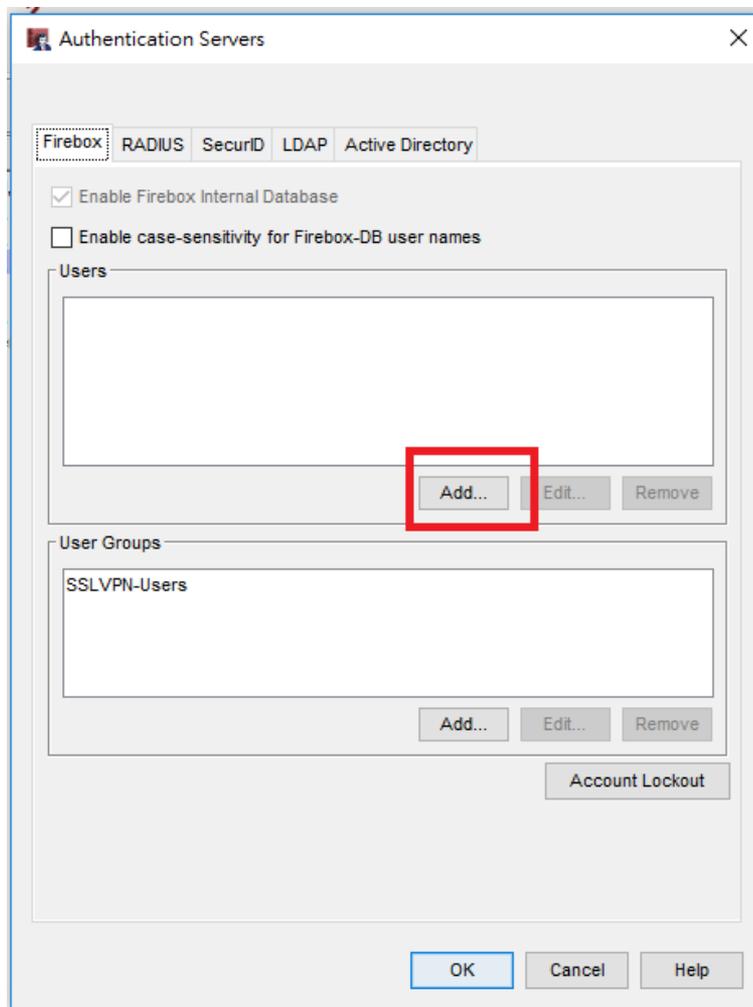
1. 點選Advance
2. 輸入DNS Server IP，Client連線SSL VPN後所會取得的DNS IP

設定SSL VPN連線帳號



Setup → Authentication → Authentication Server

新增SSL VPN連線帳號



Step 1 :

點選Add

新增SSL VPN連線帳號

Setup Firebox User

User Information

Name: 1.

Description:

Passphrase: 2.

Confirm:

Session Timeout: hours

Idle Timeout: minutes

Enable login limits for each user or group

Allow unlimited concurrent firewall authentication logins from the same account

Limit concurrent user sessions to

When the limit is reached:

Firebox Authentication Groups

Member:

Available: 3.

4.

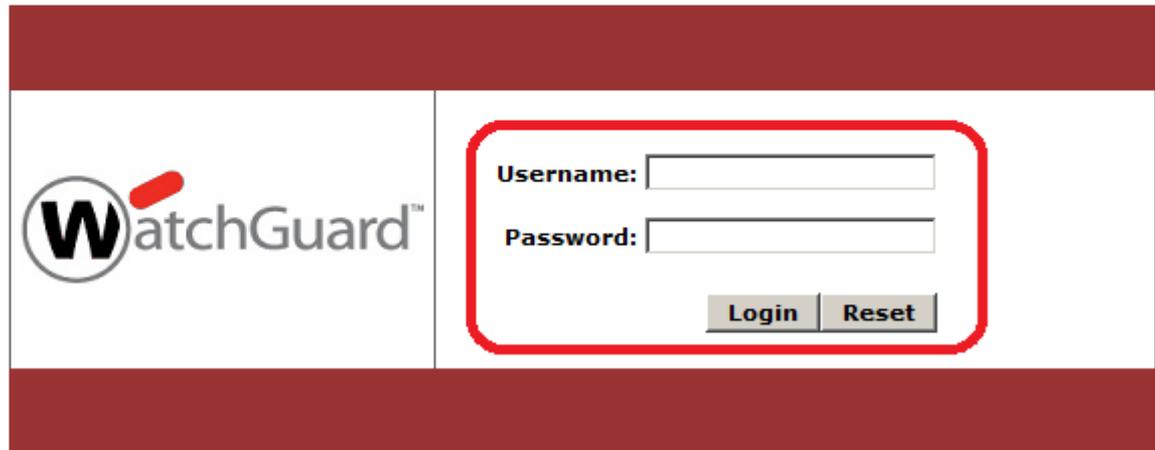
5.

Step 2 :

1. 輸入帳號名稱
2. 輸入帳號的密碼
3. 點選Available下方SSL VPN-Users
4. 點選向左方箭頭
5. 點選OK

SSL VPN Client安裝

連線Download SSL VPN Client



The screenshot displays the WatchGuard login page. On the left is the WatchGuard logo. On the right, there is a login form with two input fields: "Username:" and "Password:". Below the fields are two buttons: "Login" and "Reset". The entire login form area is highlighted with a red rounded rectangle.

在網址列 <https://Firewall External IP Address/sslvpn.html>
之後輸入帳號密碼

下載您所需的軟體

Items available to download



Download

Mobile VPN with SSL client software for Windows

Use this client to make a secure VPN connection to the company network from a Windows computer.



Download

Mobile VPN with SSL client software for Mac

Use this client to make a secure VPN connection to the company network from a Mac computer.



Download

Mobile VPN with SSL client profile

Import this profile to enable a secure VPN connection from any SSL VPN client that supports .ovpn configuration files.

Logout

依您的作業系統下載所需的軟體

安裝完成SSL VPN Client



下載安裝完成之後會在桌面出現SSL VPN Client的圖示，點擊兩下

安裝完成SSL VPN Client



WatchGuard Mobile VPN with SSL

WatchGuard
Firebox[®] SSL

Server: 59.120.145.169

User name:

Password:

Automatically reconnect

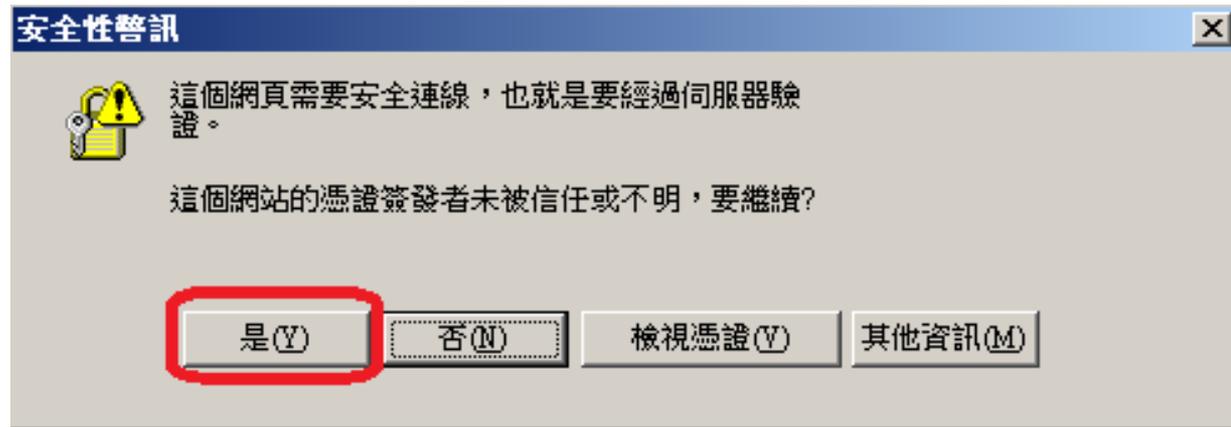
Remember password

Connect Cancel

Version 12.2.0 (Build 597644)

輸入Firewall External IP Address以及帳號密碼，之後按下Connect

安全憑證點選



安全憑證部分點選”是”

連線成功畫面

```
C:\Windows\system32\cmd.exe

乙太網路卡 區域連線 2:

連線特定 DNS 尾碼 . . . . . :
描述 . . . . . : TAP-Win32 Adapter V9
實體位址 . . . . . : 00-FF-95-AF-74-E9
DHCP 已啟用 . . . . . : 是
自動設定啟用 . . . . . : 是
連結-本機 IPv6 位址 . . . . . : fe-80::2-f4:768::480::d53%38<偏好選項>
IPv4 位址 . . . . . : 192.168.100.2<偏好選項>
子網路遮罩 . . . . . : 255.255.255.0
租用取得 . . . . . : 2012年7月17日 下午 03:15:52
租用到期 . . . . . : 2013年7月17日 下午 03:15:56
預設閘道 . . . . . :
DHCP 伺服器 . . . . . : 192.168.100.254
DHCPv6 IAID . . . . . : 520159125
DHCPv6 用戶端 DUID. . . . . : 00-01-00-01-15-92-24-0A-00-1F-16-2F-0A-AF

DNS 伺服器 . . . . . : fec0:0:0:ffff::1%1
                        fec0:0:0:ffff::2%1
                        fec0:0:0:ffff::3%1
NetBIOS over Tcpip . . . . . : 啟用

乙太網路卡 區域連線:
```

VPN連線成功後會得到一組192.168.100.x網段的IP位置

Dimension Report 安裝



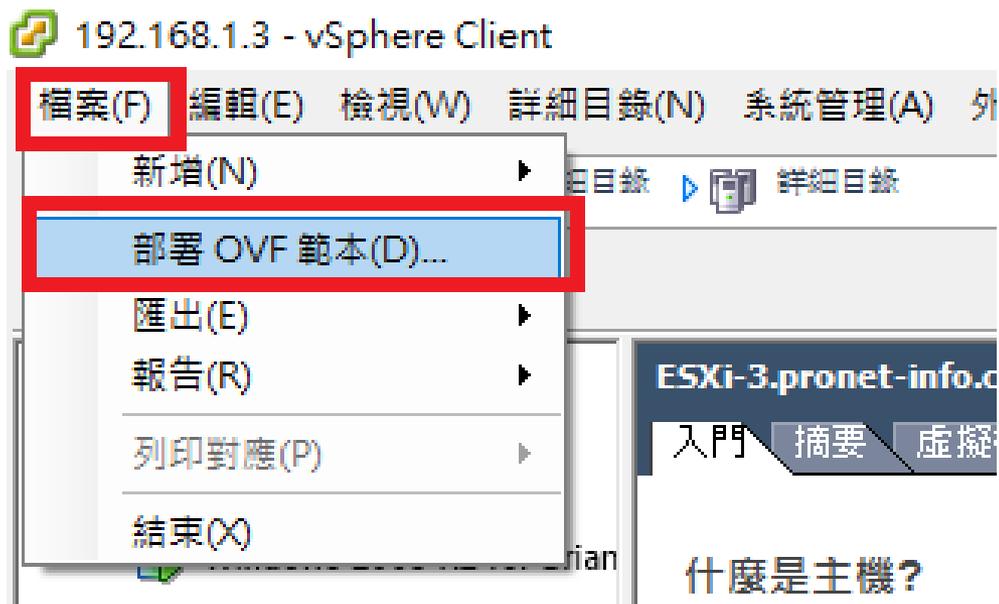
WatchGuard Dimension Report說明

WatchGuard Dimension Reporting System可安裝於下列作業系統中

1. VMware ESX
2. VMware ESXI
3. Windows Hyper-V

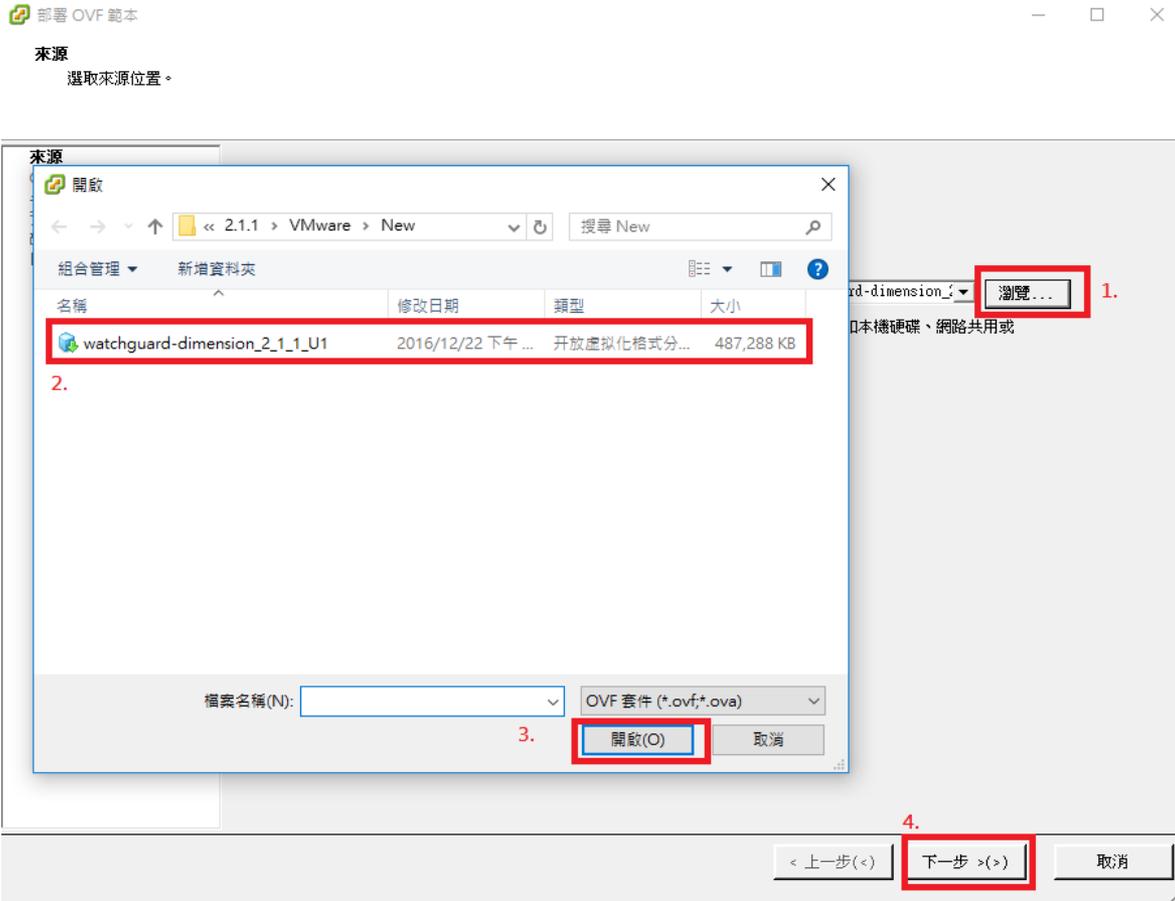
除了上面幾種作業系統外，WatchGuard提供舊版Report System可安裝於一般Windows作業系統中。

部屬 Dimension Report OVF



檔案 → 部屬 OVF 範本

選擇 Dimension Report OVF 檔案



1. 點選瀏覽
2. 選擇 Dimension OVF 檔案
3. 點選開啟
4. 點選下一步

Dimension Report OVF檔案詳細資料

部署 OVF 範本

- □ ×

OVF 範本詳細資料

驗證 OVF 範本詳細資訊。

來源

OVF 範本詳細資料

- 使用者授權合約
- 名稱和位置
- 資源集區
- 磁碟格式
- 網路對應
- 即將完成

產品:	Dimension
版本:	2.1.1 U1
廠商:	WatchGuard Technologies, Inc.
發佈者:	WatchGuard Technologies, Inc. (無效的憑證)
下載大小:	475.7 MB
磁碟大小:	1.0 GB (精簡佈建) 43.0 GB (完整佈建)
說明:	WatchGuard Dimension is the next-generation platform for managing WatchGuard physical and virtual integrated security solutions. It is delivered as a virtual appliance for simple deployment and configuration. WatchGuard Dimension offers a rich set of dashboards and reports, as well as log viewing capability, bringing the power of business intelligence to network security.

< 上一步(<) **下一步(>)** 取消

點選下一步

Dimension Report 合約選項

部署 OVF 範本

使用者授權合約

接受使用者授權合約。

來源

[OVF 範本詳細資料](#)

使用者授權合約

名稱和位置

資源集區

磁碟格式

網路對應

即將完成

WatchGuard End-User License Agreement

This WatchGuard End-User License Agreement (the "AGREEMENT") is a legal agreement between you and WatchGuard Technologies, Inc. ("WATCHGUARD") and contains the terms that govern your downloading, installation, copying and use of the SOFTWARE PRODUCT. As used herein, "you" or "your" means the person, company or other entity using the SOFTWARE PRODUCT. Capitalized terms used in this AGREEMENT are defined in accordance with Section 1 below.

PLEASE CAREFULLY READ THE TERMS OF THIS AGREEMENT BEFORE YOU CLICK "I AGREE" OR OTHER SIMILARLY WORDED BUTTON. BY CHECKING THE BOX INDICATING THAT YOU AGREE TO THE TERMS OF THIS AGREEMENT, OR BY DOWNLOADING, INSTALLING, COPYING OR USING THE SOFTWARE PRODUCT, YOU (A) HEREBY CONSENT AND AGREE TO BE BOUND BY THIS AGREEMENT; AND (B) HEREBY REPRESENT AND WARRANT THAT YOU ARE LAWFULLY ABLE TO ENTER INTO THIS AGREEMENT. IF THIS AGREEMENT IS BEING AGREED TO BY A COMPANY OR OTHER ENTITY, THEN THE PERSON AGREEING TO THIS AGREEMENT ON BEHALF OF THAT COMPANY OR ENTITY HEREBY REPRESENTS AND WARRANTS THAT (I) HE OR SHE IS DULY AUTHORIZED AND LAWFULLY ABLE TO BIND THAT COMPANY OR ENTITY TO THIS AGREEMENT; (II) THE COMPANY OR ENTITY HAS THE FULL POWER, CORPORATE OR OTHERWISE, TO ENTER INTO THIS AGREEMENT AND PERFORM ITS OBLIGATIONS UNDER THIS AGREEMENT; AND (III) THIS AGREEMENT AND THE PERFORMANCE OF THE COMPANY'S OR ENTITY'S OBLIGATIONS UNDER THIS AGREEMENT DO NOT VIOLATE ANY THIRD-PARTY AGREEMENT TO WHICH THE COMPANY OR ENTITY IS A PARTY.

IF YOU DISAGREE WITH ANY OF THE TERMS OF THIS AGREEMENT, WATCHGUARD DOES NOT GRANT YOU A LICENSE AND YOU MUST NOT DOWNLOAD, INSTALL, COPY OR USE THE SOFTWARE PRODUCT.

1) Definitions. As used in this AGREEMENT, each of the following capitalized terms shall have the meaning ascribed to such terms in this Section 1. All capitalized terms not defined in this Section 1 shall have the meaning ascribed to such terms in the body of this AGREEMENT.

a. "DOCUMENTATION" means any pages, schedules, policies, guidelines, specifications, user manuals, guides, support materials and other documents, materials and information relating to installation and use of the SOFTWARE PRODUCT, including without limitation, those describing the operational and functional capabilities, use limitations, technical and engineering requirements, and testing and performance criteria relevant to proper use of the SOFTWARE PRODUCT, which are referenced in this AGREEMENT, provided to you by WATCHGUARD or posted on the SITE from time to time.

b. "LICENSED MACHINE" means a virtual machine in a hypervisor environment.

c. "OPEN SOURCE SOFTWARE" means certain operating system and other software distributed by WatchGuard under an open source licensing model (e.g., the GNU General Public License, BSD or a license similar to those approved by the Open Source Initiative) in connection with the SOFTWARE PRODUCT. Notwithstanding anything set forth in this AGREEMENT to the contrary, Customer's use of OPEN SOURCE SOFTWARE shall in all ways be governed by the open source license indicated as applicable to the OPEN SOURCE SOFTWARE at <http://www.watchguard.com/wgrdlic/xtmv.asp>, elsewhere on the SITE or in the DOCUMENTATION.

接受(A)

1.

2.

< 上一步(<)

下一步 >(>)

取消

1. 點選接受

2. 點選下一步

輸入Dimension Report OVF 名稱

部署 OVF 範本

名稱和位置
為已部署的範本指定名稱和位置

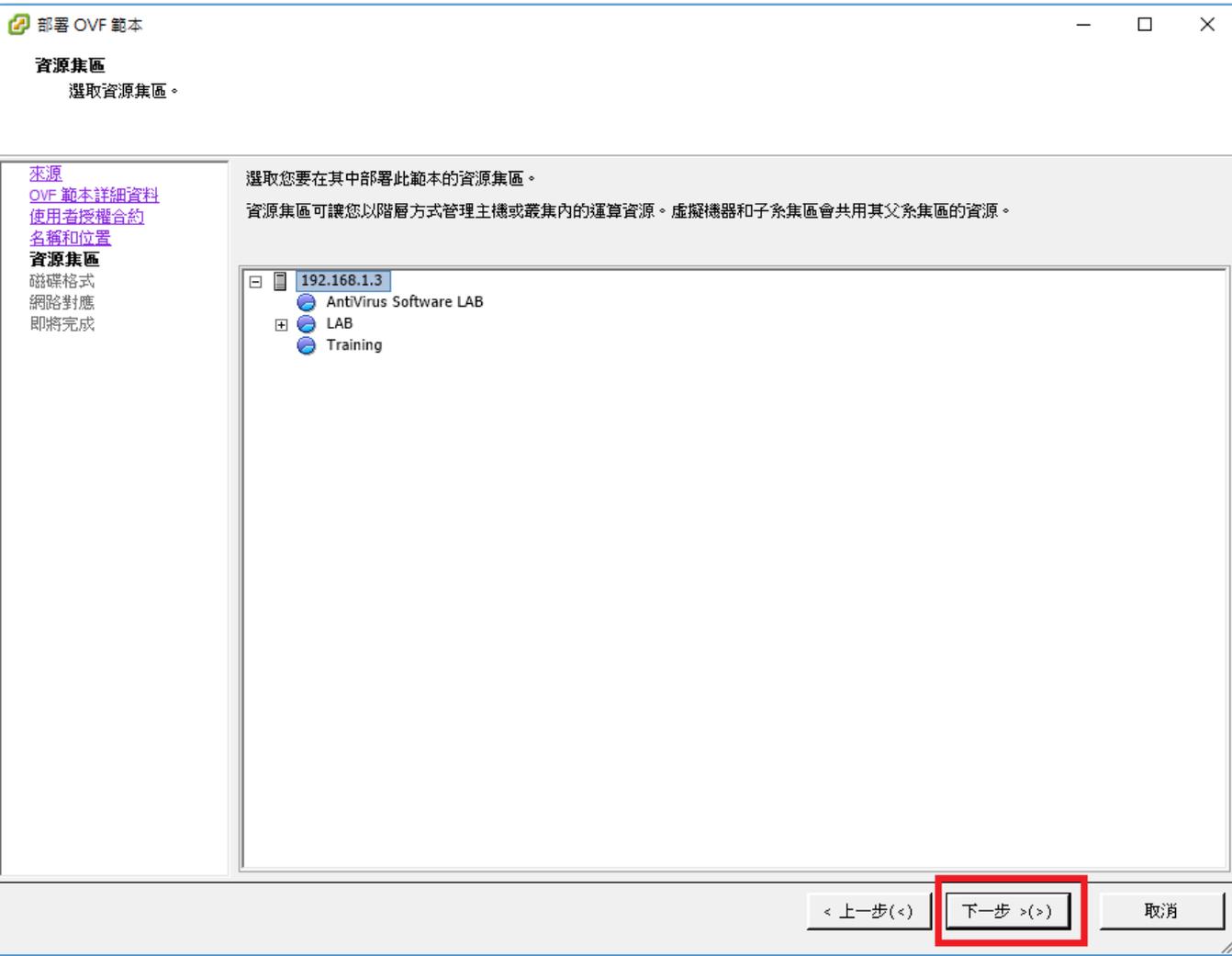
來源
OVF 範本詳細資料
使用者授權合約
名稱和位置
資源集區
磁碟格式
網路對應
即將完成

名稱: 1.
[Dimension]
名稱最多可包含 80 個字元，並且在詳細目錄資料夾中必須是唯一的。

2.
< 上一步(<) 下一步 >(>) 取消

1. 輸入Guest OS名稱
2. 點選下一步

選擇 Dimension Report OVF 資料夾位置



點選下一步

Dimension Report OVF硬碟使用方式

部署 OVF 範本

磁碟格式
您想要以什麼格式儲存虛擬磁碟?

來源
[OVF 範本詳細資料](#)
[使用者授權合約](#)
[名稱和位置](#)
[資源集區](#)
磁碟格式
[網路對應](#)
即將完成

資料存放區:

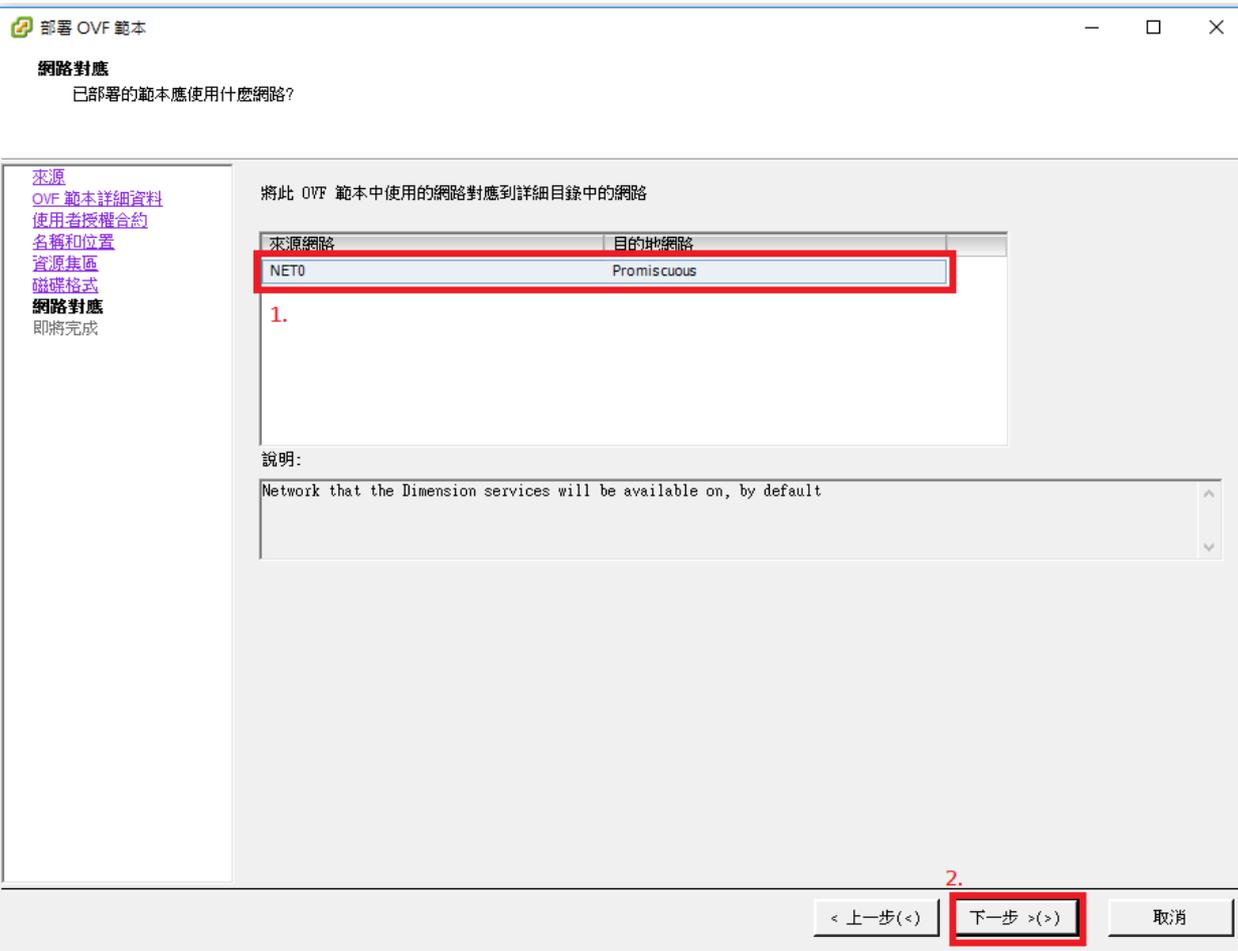
可用空間 (GB):

完整佈建消極式歸零
 完整佈建積極式歸零
 精簡佈建

< 上一步(<) **下一步 >(>)** 取消

使用預設值，點選下一步

選擇 Dimension Report OVF 網卡



1. 選擇網路卡
2. 點選下一步

完成 Dimension Report OVF 匯入設定

部署 OVF 範本

即將完成
這些是您要使用的選項嗎？

[來源](#)
[OVF 範本詳細資料](#)
[使用者授權合約](#)
[名稱和位置](#)
[資源集區](#)
[磁碟格式](#)
[網路對應](#)
即將完成

按一下「完成」後，將開始部署工作。

部署設定：

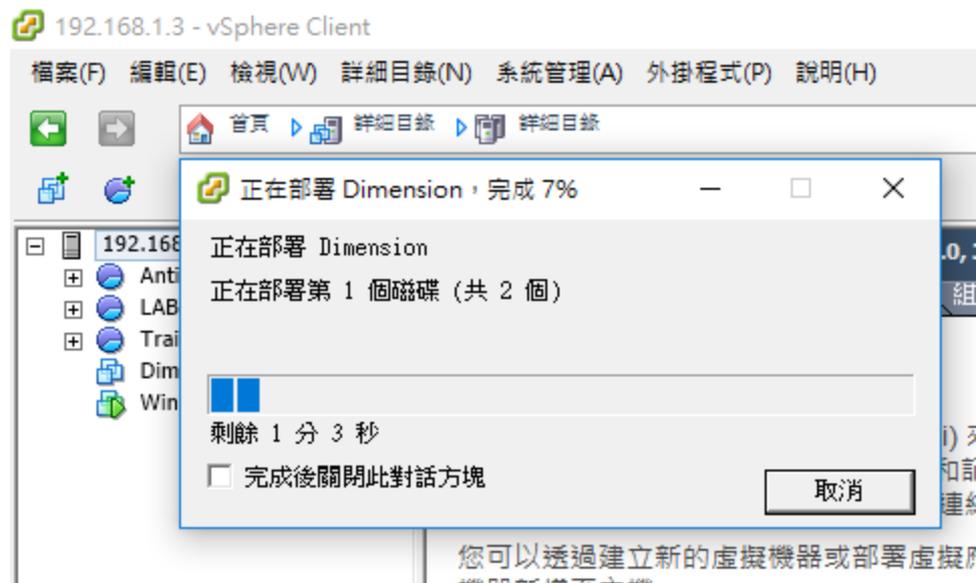
OVF 檔案：	D:\My document\resource\WatchGuard\Dimension\2.1.1\VMware\New\watchguard-dimension_2...
下載大小：	475.7 MB
磁碟大小：	43.0 GB
名稱：	Dimension
主機/叢集：	ESXi-3.pronet-info.com.tw
資料存放區：	datastore1
磁碟佈建：	完整佈建消極式歸零
網路對應：	[NET0] 至 [Promiscuous]

部署後開啟電源(P)

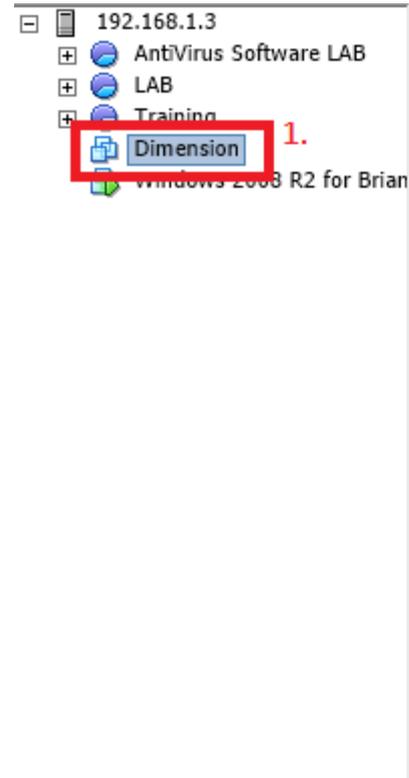
< 上一步(<) **完成** 取消

點選完成開始匯入

開始匯入 Dimension Report OVF



開啟 Dimension Report OVF 虛擬機器



192.168.1.3

- AntiVirus Software LAB
- LAB
- Training
 - Dimension** 1.
 - Windows 2008 R2 for Brian

Dimension

入門 摘要 資源配置 效能 事件 主控台 權限

什麼是虛擬機器?

虛擬機器是一種軟體電腦，可以像實體電腦一樣執行作業系統和應用程式。安裝在虛擬機器上的作業系統稱為客體作業系統。

由於每台虛擬機器都是一個隔離的運算環境，因此，您可以將虛擬機器用作桌面/工作站環境或測試環境，或用來整併伺服器應用程式。

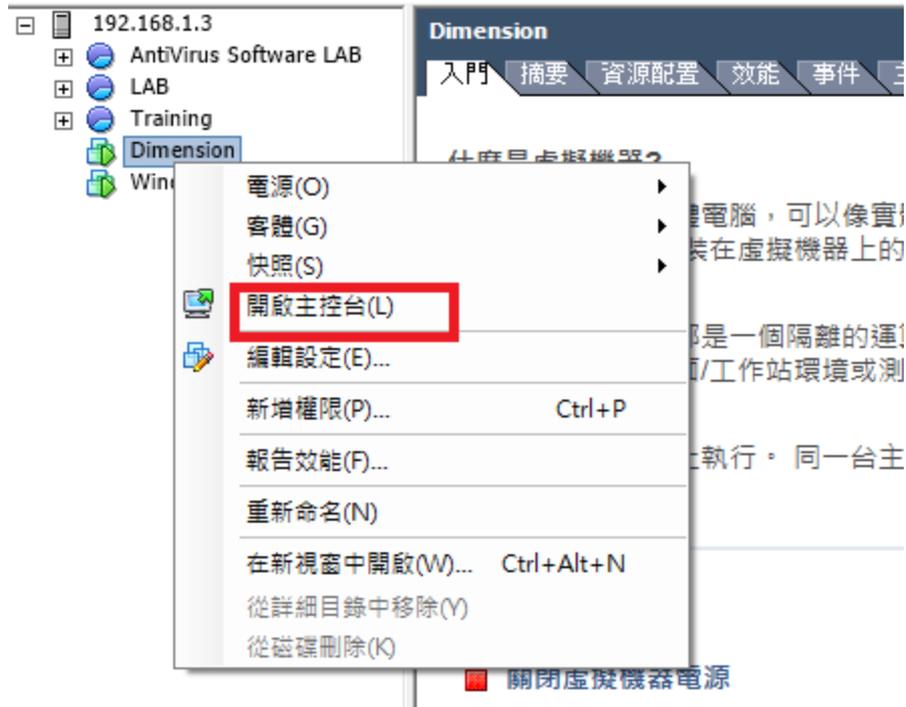
虛擬機器是在主機上執行。同一台主機可執行多台虛擬機器。

基本工作

- ▶ 開啟虛擬機器電源** 2.
- 編輯虛擬機器設定

1. 點選匯入的機器
2. 點選開啟虛擬機器店源

開啟虛擬機器主控台



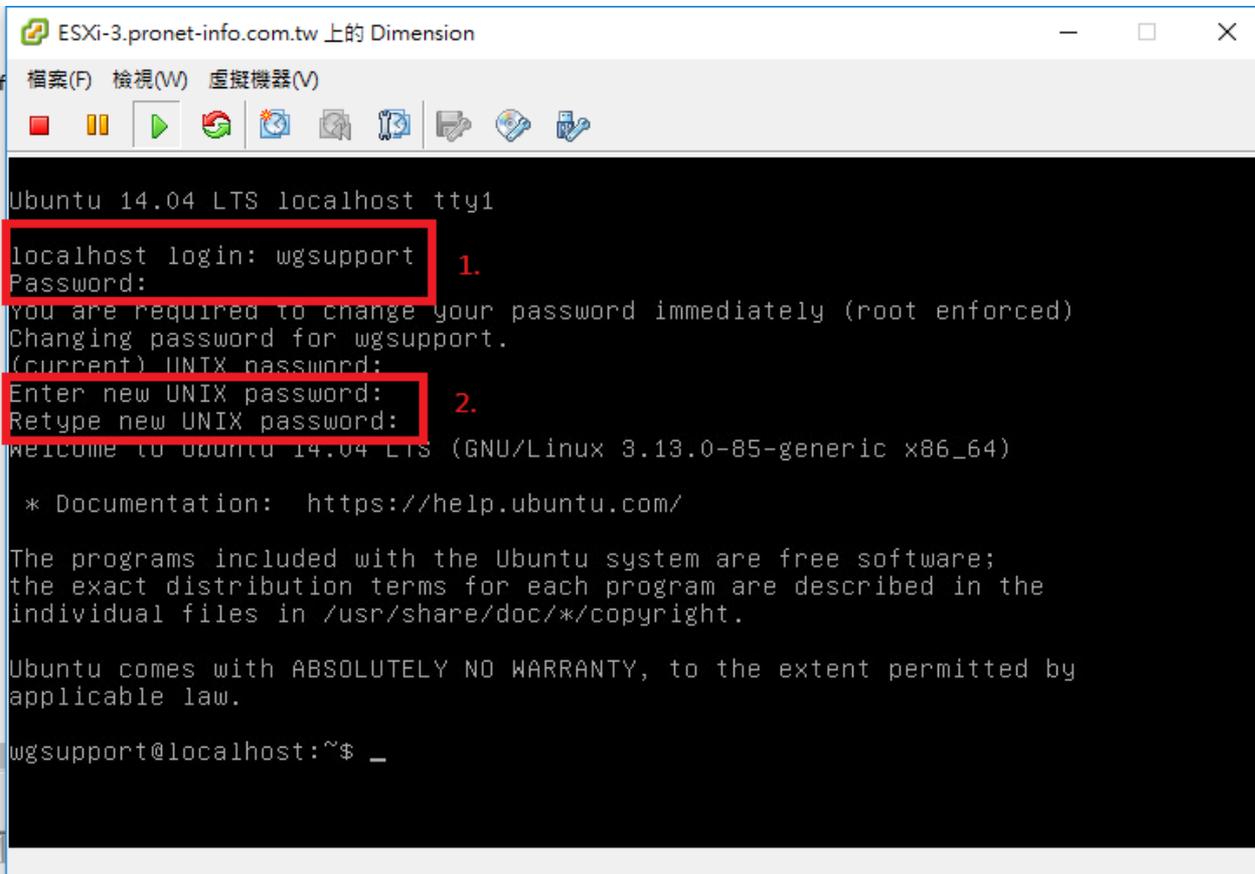
點選虛擬機器案右鍵 → 開啟主控台

登錄虛擬機器主控台

1. 輸入帳號密碼
2. 修改預設密碼

帳號：wgsupport

密碼：readwrite



```
ESXi-3.pronet-info.com.tw 上的 Dimension
檔案(F) 檢視(W) 虛擬機器(V)
localhost login: wgsupport 1.
Password:
you are required to change your password immediately (root enforced)
Changing password for wgsupport.
(current) UNIX password:
Enter new UNIX password: 2.
Retype new UNIX password:
welcome to Ubuntu 14.04 LTS (GNU/Linux 3.13.0-85-generic x86_64)

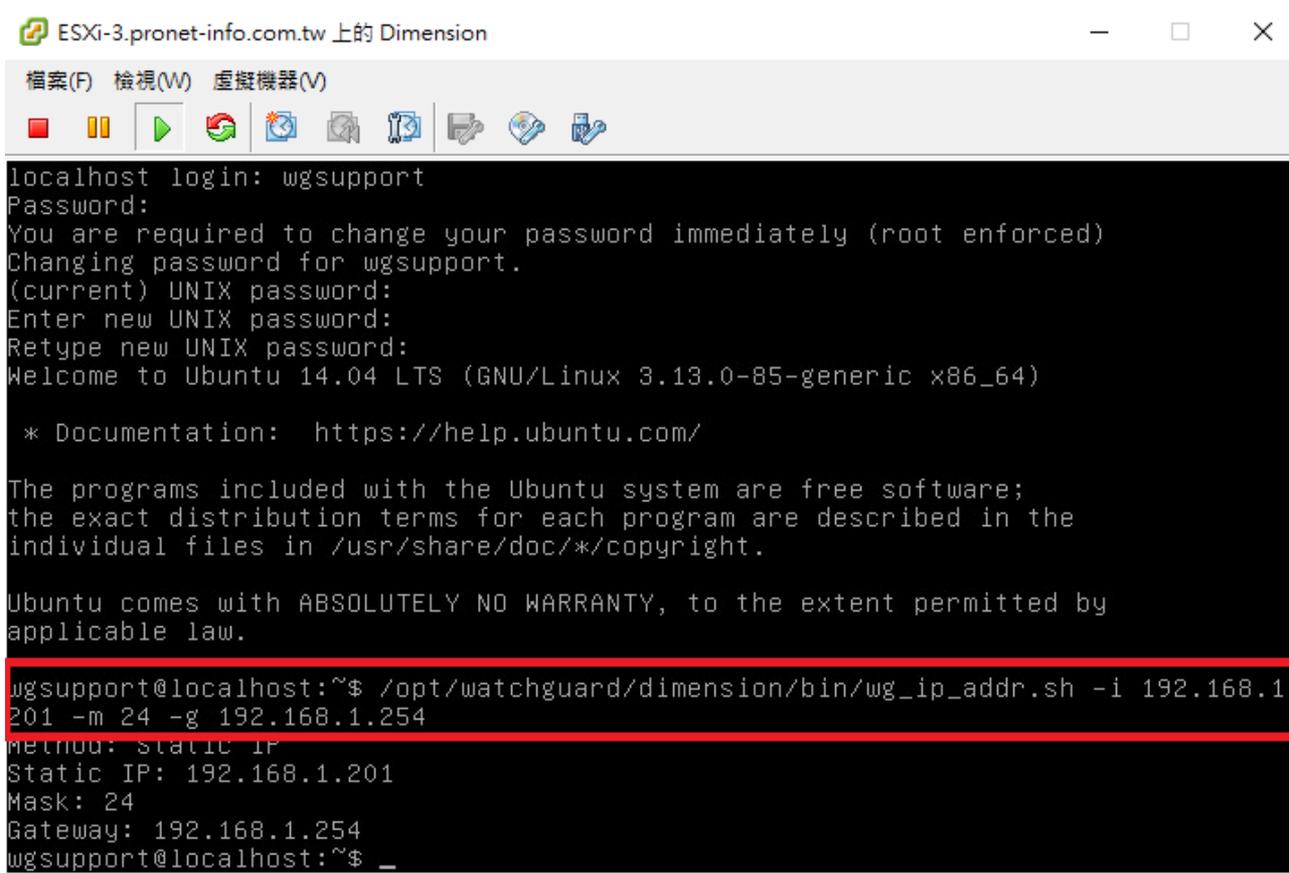
* Documentation:  https://help.ubuntu.com/

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

wgsupport@localhost:~$ _
```

修改 Dimension Report IP



```
ESXi-3.pronet-info.com.tw 上的 Dimension
檔案(F) 檢視(W) 虛擬機器(V)
localhost login: wgsupport
Password:
You are required to change your password immediately (root enforced)
Changing password for wgsupport.
(current) UNIX password:
Enter new UNIX password:
Retype new UNIX password:
Welcome to Ubuntu 14.04 LTS (GNU/Linux 3.13.0-85-generic x86_64)

* Documentation:  https://help.ubuntu.com/

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

wgsupport@localhost:~$ /opt/watchguard/dimension/bin/wg_ip_addr.sh -i 192.168.1.
201 -m 24 -g 192.168.1.254
method: Static IP
Static IP: 192.168.1.201
Mask: 24
Gateway: 192.168.1.254
wgsupport@localhost:~$ _
```

子網路遮罩

`/opt/watchguard/dimension/bin/wg_ip_addr.sh -i 192.168.1.201 -m 24 -g 192.168.1.254`

要修改的IP

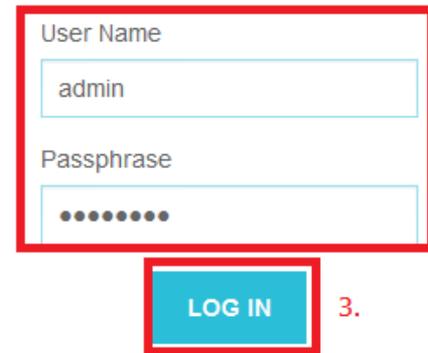
Default Gateway

修改IP將此行指令輸入虛擬機主控台中

登錄Dimension



1.



User Name
admin

Passphrase
●●●●●●

LOG IN

2.

3.

User Name : admin

Passphrase : readwrite

開啟瀏覽器

1. 輸入 https://dimension_ip
2. 輸入帳號密碼
3. 點選LOG IN

啟動Dimension設定精靈

WatchGuard Dimension Setup Wizard

Before you begin, make sure you have this information:

Setting up the System

1. Host name for Dimension
2. IPv4 address settings for eth0 interface
3. Administrator passphrase

Database Location Setting

1. By default location is set to the built-in database
2. To switch to an external database, make sure it's configured and accessible

Setting up Public Addresses (Optional)

1. Add Public FQDNs or IP Addresses

Visibility Setting

1. Log Encryption Key
2. Anonymize Reports (Optional)

Do not power off Dimension before the Setup Wizard completes.

BACK

NEXT

首次登錄系統會啟動Dimension設定精靈

更改Dimension網路設定

System Information

Host Name	<input type="text" value="localhost"/>
IP Address Method	<input type="text" value="Static"/>
IPv4 Address / Mask	<input type="text" value="192.168.1.201"/> / <input type="text" value="24"/>
Default Gateway	<input type="text" value="192.168.1.254"/>
DNS Server	<input type="text" value="192.168.1.100"/> 1.
Domain Name	<input type="text" value="Domain Name"/> (Optional)
	<input type="checkbox"/> Send feedback to WatchGuard ? 2.

We recommend that you specify a static IPv4 address for the default IP address to use to connect to Dimension.

3.

1. 輸入DNS IP
2. 將Send feedback to WatchGuard的勾拿掉
3. 點選Next

選擇 Dimension Database 位置

Database Location Setting

Database location

Default path `/var/opt/watchguard/dimension/data/db`

Select an 'External' database location, if you want to point Dimension to an external PostgreSQL database. Make sure it's ready to use and is accessible.

選擇 Dimension IP 型態

Public Addresses

Is this instance of Dimension publicly accessible to your Firebox devices?

Yes, the Dimension server has a public IP address

No, the Dimension server is behind a NAT device

Your Dimension instance has a public IP address and can be reached successfully.

[BACK](#) [NEXT](#)

使用預設值，點選下一步

修改Administrator密碼

Set Administrator Passphrase

Administrator User Name

Administrator Passphrase

Confirm Passphrase
Passphrase cannot be empty.

The Administrator passphrase gives you read-write access to Dimension, so you can modify your settings. The Administrator passphrase must have at least 8 characters.

修改密碼後點選下一步

輸入Firebox和Dimension間資料加密的密碼

Visibility Setting — Logging Encryption Key

Encryption Key

••••••••

1.

Confirm Encryption Key

••••••••

The encryption key is used to establish a secure connection between Dimension and your Firebox or WatchGuard server

BACK

2.
NEXT

1. 輸入Firebox和Dimension間資料傳遞時，加密的密碼
2. 點選NEXT

匿名登錄設定

Visibility Setting — Anonymize Reports

Do you want to enable Anonymized Mode?

Yes No

When you enable Anonymized Mode, user names, IP addresses, host names, and mobile device names are masked in reports, and log messages and detail reports are not available.

BACK

NEXT

確認Dimension設定

Review Dimension Settings

System Information	<i>Host name:</i> localhost <i>IPv4 address:</i> 192.168.1.201/24 <i>Default Gateway:</i> 192.168.1.254 <i>DNS Server:</i> 192.168.1.100 <i>Domain Name:</i>
Database location	/var/opt/watchguard/dimension/data/db
Administrator	Administrator passphrase set
Visibility Settings	Encryption key set

Review your settings. To change any settings, click **Back**. You cannot make changes after you click **Next**.

確認Dimension設定後點選NEXT

進行Dimension設定初始化

Progress Page

- ✔ System successfully configured.
- ✔ Administrator passphrase is set.
- ✔ PostgreSQL database is configured.
- ✔ Visibility Setting is configured.

The WatchGuard Dimension Setup Wizard is complete. Click **Next** to continue.

BACK

NEXT

完成Dimension設定

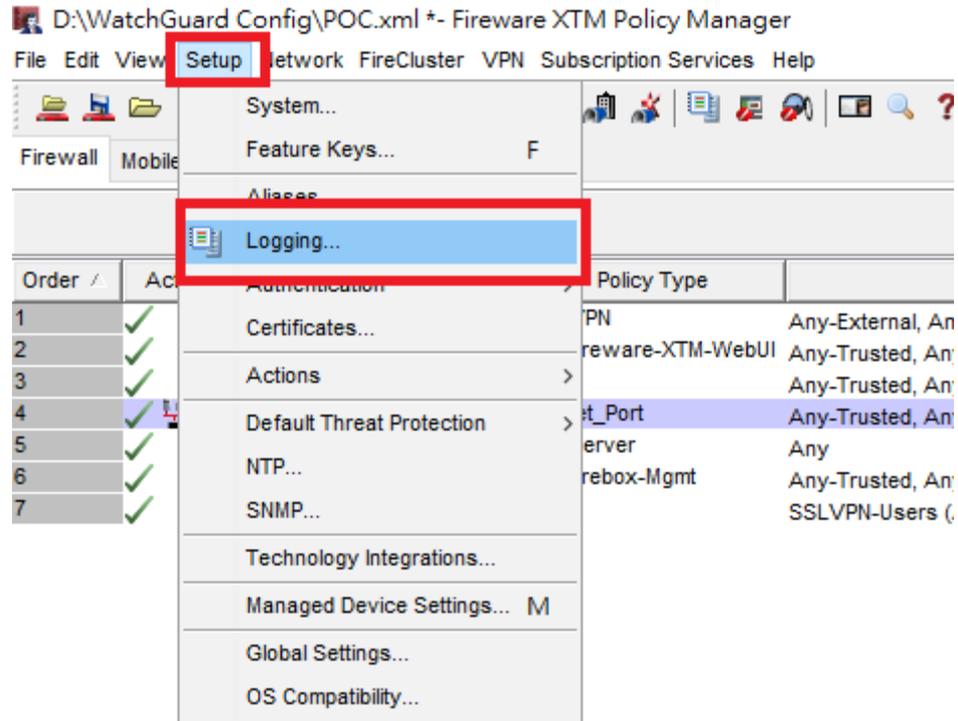
WatchGuard Dimension Setup Wizard

WatchGuard Dimension setup is complete.

To complete the Dimension Setup Wizard, click **Finish**. The WatchGuard Dimension login page will appear.

點選FINISH完成Dimension設定

Firebox和Dimension同步設定



Step 1 :

Setup → Logging

Logging Setup

Use these settings to configure where the device sends log messages.

This device can send log messages to more than one destination at the same time. Select one or more check boxes to specify where log messages are sent: WatchGuard Log Server, syslog server, or Firebox internal storage.

WatchGuard Log Server

Send log messages to these WatchGuard Log Servers: 1.

Log Servers 1 Log Servers 2

2.

The servers you specify on the **Log Servers 2** tab are only available for devices with Fireware XTM OS v11.10 and higher.

Syslog Server

Send log messages to this syslog server:

IP address: . . .

Port: 514

Log format: Syslog

Firebox Internal Storage

Send log messages to Firebox internal storage

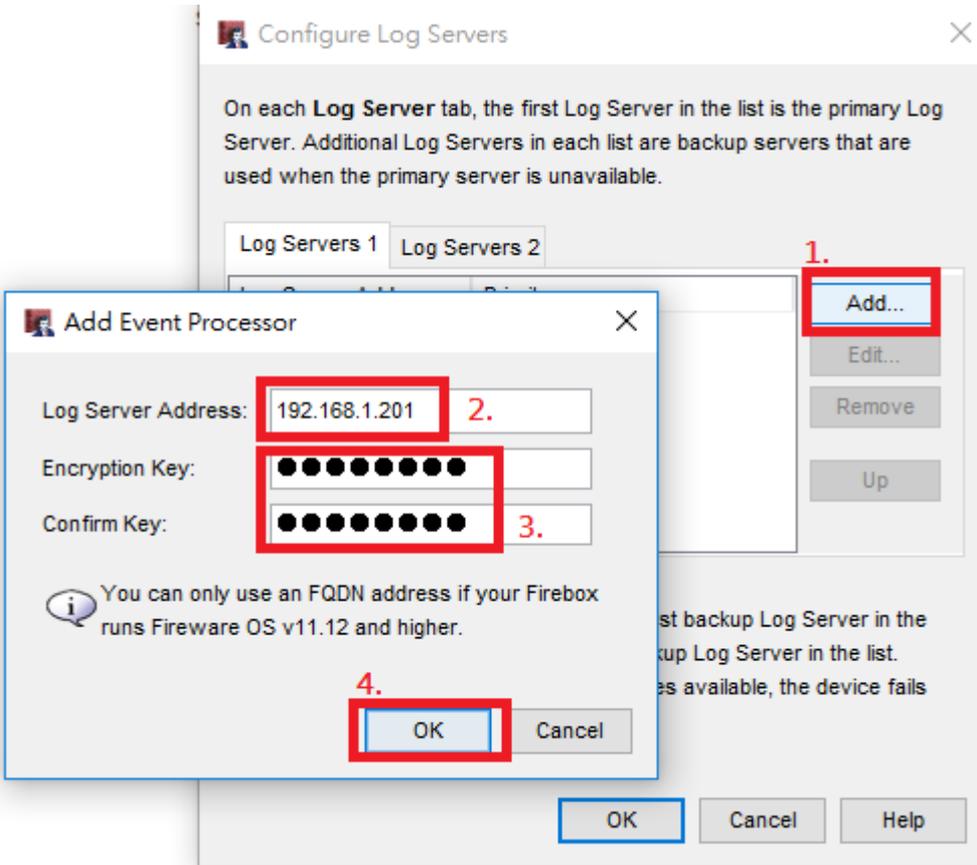
Send log messages when the configuration for this device is changed

OK Cancel Help

Step 2 :

1. 勾選Send log message to these WatchGuard Log Server
2. 點選Configure

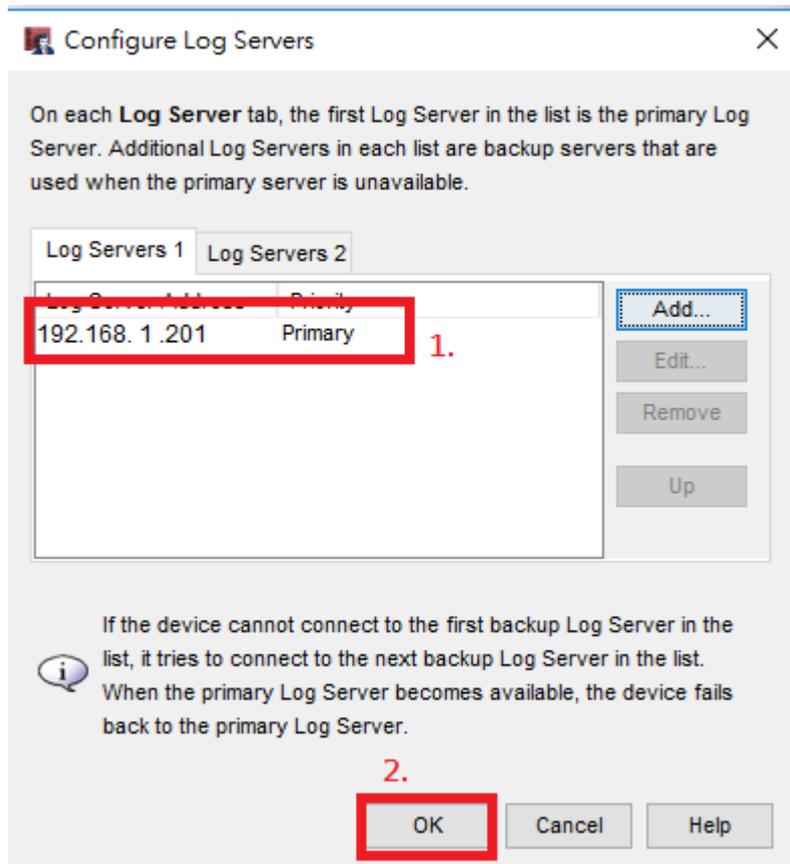
新增Dimension Report Server



Step 3 :

1. 點選Add
2. 輸入Dimension Server IP
3. 輸入Dimension和Firebox同步的密碼
4. 點選OK

確認Firebox Dimension Server設定

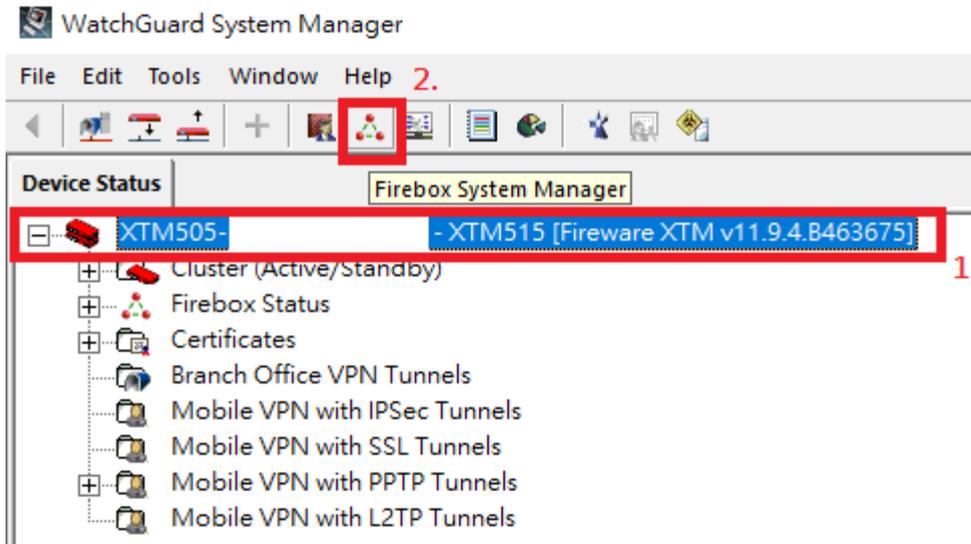


1. 確認Dimension IP設定
2. 點選OK

最後確認Firebox 和Dimension Server同步完成

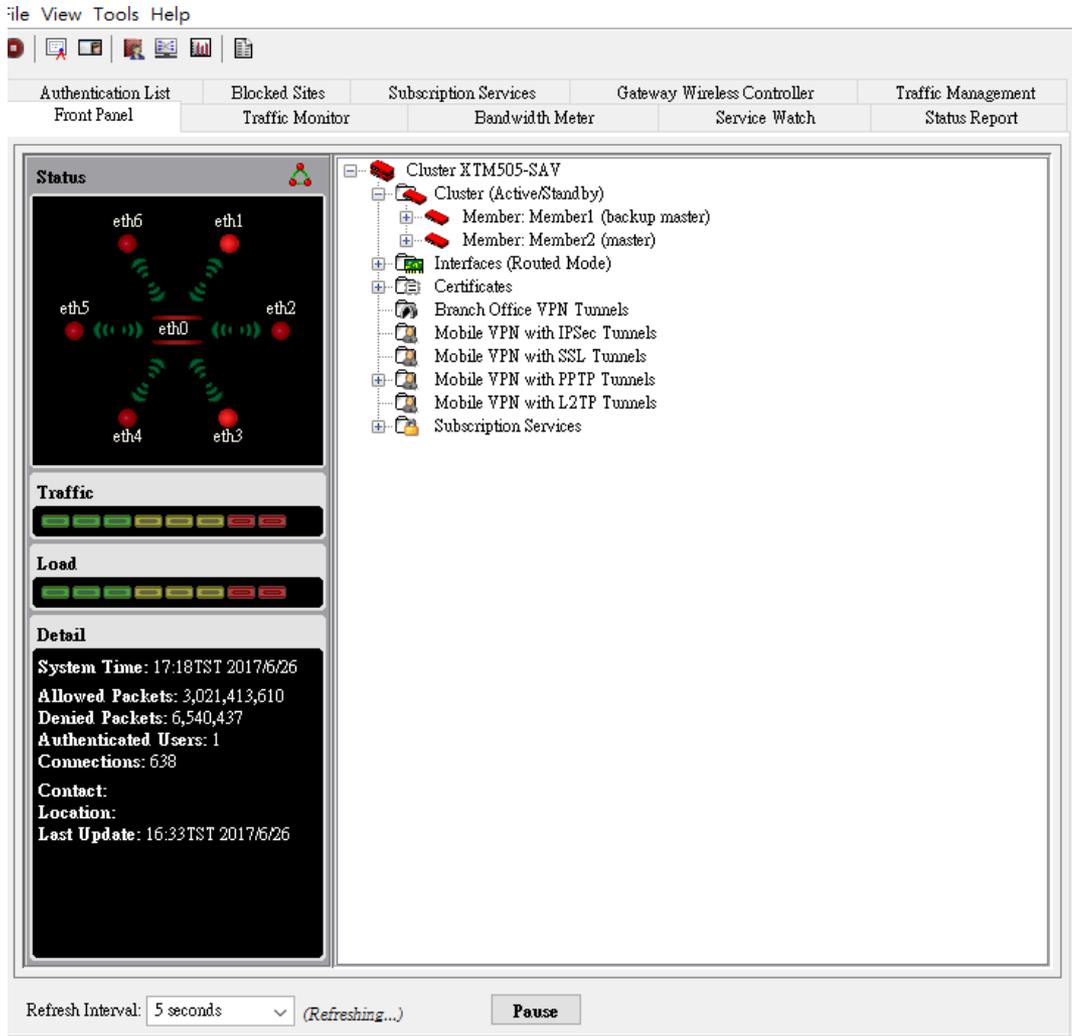
WatchGuard 監看工具

開啟Firebox System Manager



1. 點選防火牆

2. 點選Firebox System Manager



The screenshot displays the Firebox System Manager web interface. At the top, there is a menu bar with 'file View Tools Help' and a set of icons. Below this is a navigation pane with tabs: 'Authentication List', 'Blocked Sites', 'Subscription Services', 'Gateway Wireless Controller', and 'Traffic Management'. Underneath these are sub-tabs: 'Front Panel', 'Traffic Monitor', 'Bandwidth Meter', 'Service Watch', and 'Status Report'. The main content area is divided into three sections: 'Status', 'Traffic', and 'Detail'. The 'Status' section shows a network diagram with interfaces eth0 through eth6 and a central cluster icon. The 'Traffic' section contains two progress bars. The 'Detail' section displays system statistics: System Time: 17:18TST 2017/6/26, Allowed Packets: 3,021,413,610, Denied Packets: 6,540,437, Authenticated Users: 1, and Connections: 638. At the bottom, there is a 'Refresh Interval' dropdown set to '5 seconds' and a 'Pause' button.

Firebox System Manager 首頁
顯示防火牆詳細資訊，包括開
機時間、HA 狀態、防火牆使
用狀況、VPN 使用者登錄狀態
以及介面資訊..... 等等。



Traffic Monitor

The screenshot displays the Traffic Monitor interface with a list of network traffic events. A context menu is open over a selected entry, showing options such as 'Copy Selection', 'Copy All', 'Select All', and 'Block Site: 224.0.0.18...'. The 'Block Site' option is highlighted with a red box. The interface also includes a 'Refresh Interval' dropdown set to '5 seconds' and a 'Continue' button.

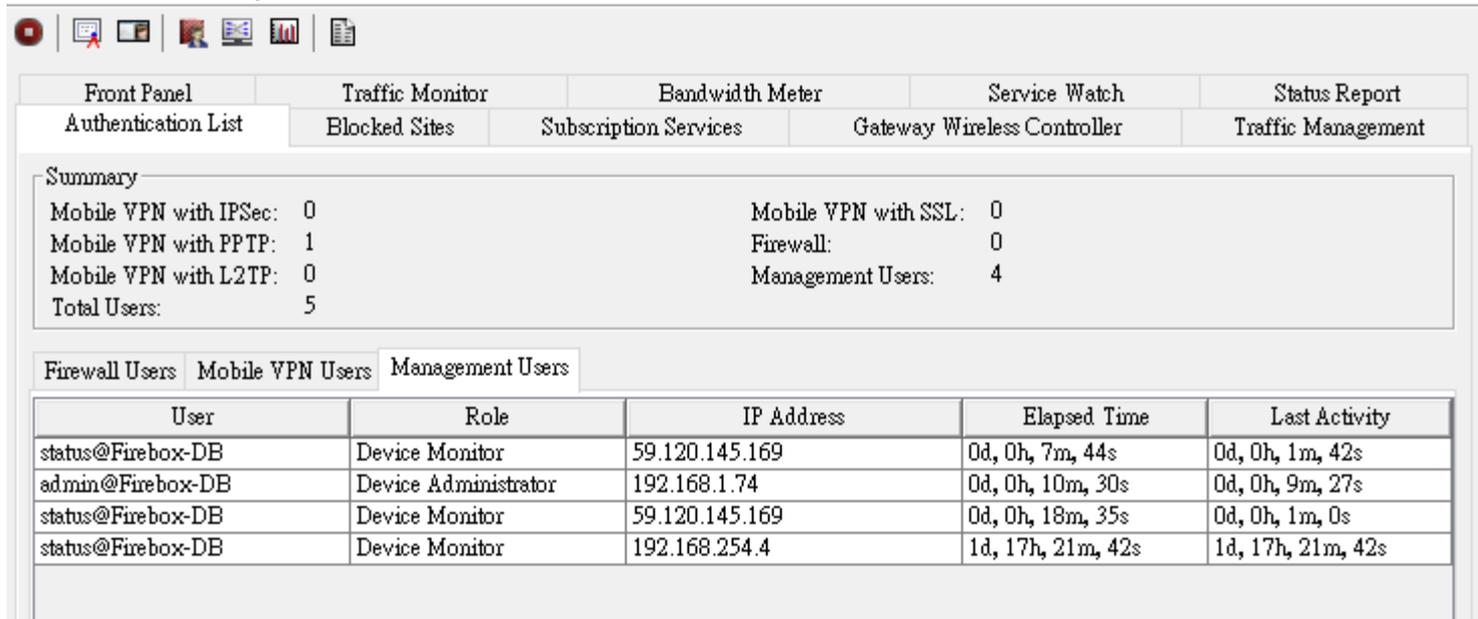
Authentication List	Blocked Sites	Subscription Services	Gateway Wireless Controller	Traffic Management
Front Panel	Traffic Monitor	Bandwidth Meter	Service Watch	Status Report

```
2017-06-26 17:21:07 Member2 Allow src_ip=61.216.4.55 dst_ip=168.95.1.1 pr=dns/udp src_port=46981 dst_port=53 src_intf=Fi
2017-06-26 17:21:07 Member2 Allow src_ip=61.216.4.55 dst_ip=168.95.1.1 pr=dns/udp src_port=46981 dst_port=53 src_intf=Fi
2017-06-26 17:21:07 Member2 Allow src_ip=61.216.4.55 dst_ip=23.99.53.216 pr=https/tcp src_port=44436 dst_port=443 src_int
2017-06-26 17:21:07 Member2 Deny src_ip=74.86.162.134 dst_ip=61.216.4.55 pr=3390/tcp src_port=53337 dst_port=3390 src_
2017-06-26 17:21:09 Member2 Allow src_ip=10.0.6.2 dst_ip=224.0.0.18 pr=vrrp src_port= dst_port= src_intf=Firebox dst_intf=6-H
2017-06-26 17:21:09 Member2 Allow src_ip=192.168.1.151 dst_ip=162.125.82.3 pr=https/tcp src_port=53962 dst_port=443 src_
2017-06-26 17:21:09 Member2 Allow src_ip=192.168.1.238 dst_ip=168.95.1.1 pr=dns/udp src_port=60128 dst_port=53 src_intf=
2017-06-26 17:21:09 Member2 Allow src_ip=192.168.1.24 dst_ip=52.76.222.244 pr=https/tcp src_port=53893 dst_port=443 src_
2017-06-26 17:21:09 Member2 Allow src_ip=192.168.1.253 dst_ip=192.168.1.60 pr=bootpc/udp src_port=67 dst_port=68 src_int
2017-06-26 17:21:09 Member2 Allow src_ip=192.168.1.60 dst_ip=255.255.255.255 pr=bootps/udp src_port=68 dst_port=67 src_
2017-06-26 17:21:09 Member2 Deny src_ip=192.168.1.195 dst_ip=255.255.255.255 pr=17500/udp src_port=17500 dst_port=17
2017-06-26 17:21:10 Member2 Allow src_ip=10.0.6.2 dst_ip=224.0.0.18 pr=vrrp src_port= dst_port= src_intf=Firebox dst_intf=6-H
2017-06-26 17:21:10 Member2 Allow src_ip=125.253.123.183 dst_ip=61.216.4.57 pr=rdp/tcp src_port=64221 dst_port=3389 src_
2017-06-26 17:21:10 Member2 Allow src_ip=192.168.1.24 dst_ip=17.252.157.7 pr=https/tcp src_port=49233 dst_port=443 src_in
2017-06-26 17:21:10 Member2 Allow src_ip=192.168.1.53 dst_ip=168.95.1.1 pr=dns/udp src_port=12888 dst_port=53 src_intf=1
2017-06-26 17:21:10 Member2 Allow src_ip=192.168.1.53 dst_ip=168.95.1.1 pr=dns/udp src_port=15188 dst_port=53 src_intf=1
2017-06-26 17:21:10 Member2 Allow src_ip=192.168.1.53 dst_ip=168.95.1.1 pr=dns/udp src_port=53252 dst_port=53 src_intf=1
2017-06-26 17:21:10 Member2 Allow src_ip=192.168.1.53 dst_ip=168.95.1.1 pr=dns/udp src_port=55530 dst_port=53 src_intf=1
2017-06-26 17:21:11 Membe
Diagnostic Tasks...
2.102.148 pr=http/tcp src_port=53435 dst_port=80 src_
2017-06-26 17:21:11 Membe
Source IP Address: 10.0.6.2
7.1 pr=https/tcp src_port=57393 dst_port=443 src_intf=
2017-06-26 17:21:11 Membe
Destination IP Address: 224.0.0.18
1.1 pr=dns/udh src_port=12715 dst_port=53 src_intf=1
Copy Destination IP Address
dst_port=443 sr
dst_port=110 src_
2017-06-26 17:21:12 Membe
Copy Selection
rebox dst_intf=6-H
2017-06-26 17:21:12 Membe
Copy All
rebox dst_intf=6-H
2017-06-26 17:21:12 Membe
Select All
traceroute...
2 dst_port=161 sr
dst_port=443 src_in
2017-06-26 17:21:12 Membe
Event Notifications...
53 src_intf=1-Ins
2017-06-26 17:21:12 Membe
Clear Traffic Monitor
38.254.3 pr=wg-firebox-mgmt/tcp src_port=33822 dst_p
38.254.3 pr=wg-firebox-mgmt/tcp src_port=38673 dst_p
2017-06-26 17:21:12 Membe
Settings...
38.254.3 pr=wg-firebox-mgmt/tcp src_port=58055 dst_p
38.254.3 pr=wg-firebox-mgmt/tcp src_port=60528 dst_p
2017-06-26 17:21:12 Member2 Deny src_ip=91.241.13.27 dst_ip=61.216.4.55 pr=microsoft-ds/tcp src_port=45031 dst_port=445
2017-06-26 17:21:12 Member2 Deny src_ip=91.241.13.27 dst_ip=61.216.4.56 pr=microsoft-ds/tcp src_port=15611 dst_port=445
```

Traffic Monitor顯示進出防火牆的所有流量，以及正在使用那些應用程式等等資訊。當在此頁面發現異常流量時，可直接按右鍵阻擋特定IP。

Authentication List

File View Tools Help



The screenshot shows a web interface with a navigation menu at the top containing: Front Panel, Authentication List, Traffic Monitor, Blocked Sites, Bandwidth Meter, Subscription Services, Service Watch, Gateway Wireless Controller, Status Report, and Traffic Management. Below the menu is a 'Summary' section with the following data:

Mobile VPN with IPsec:	0	Mobile VPN with SSL:	0
Mobile VPN with PPTP:	1	Firewall:	0
Mobile VPN with L2TP:	0	Management Users:	4
Total Users:	5		

Below the summary is a tabbed interface with three tabs: Firewall Users, Mobile VPN Users, and Management Users. The 'Firewall Users' tab is active, displaying a table with the following columns: User, Role, IP Address, Elapsed Time, and Last Activity.

User	Role	IP Address	Elapsed Time	Last Activity
status@Firebox-DB	Device Monitor	59.120.145.169	0d, 0h, 7m, 44s	0d, 0h, 1m, 42s
admin@Firebox-DB	Device Administrator	192.168.1.74	0d, 0h, 10m, 30s	0d, 0h, 9m, 27s
status@Firebox-DB	Device Monitor	59.120.145.169	0d, 0h, 18m, 35s	0d, 0h, 1m, 0s
status@Firebox-DB	Device Monitor	192.168.254.4	1d, 17h, 21m, 42s	1d, 17h, 21m, 42s

透過此頁面可顯示目前登錄防火牆使用者狀態，包括VPN使用者以及防火牆管理員登錄狀態。