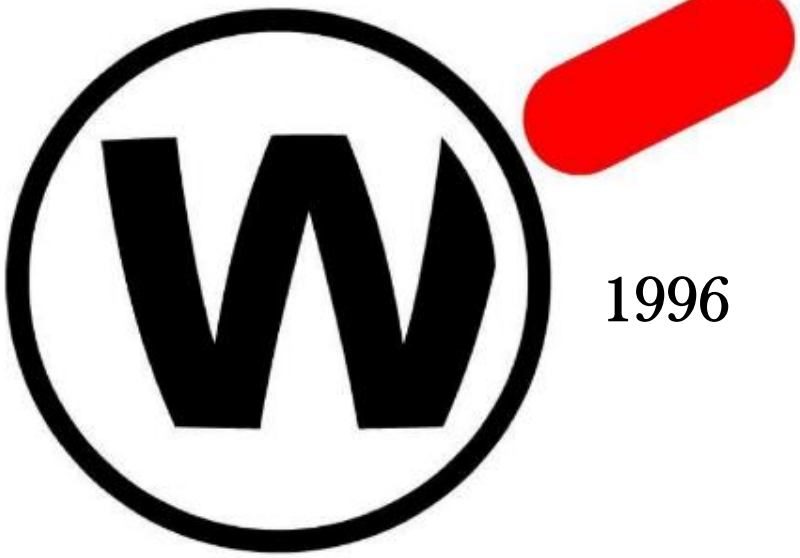
管理課程



1996

Enterprise Grade Security
企業級防護

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 :

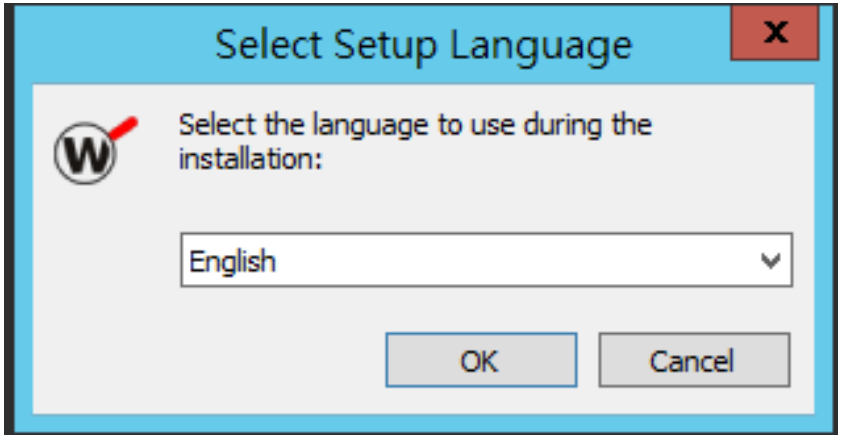
執行WSM安裝軟體

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”

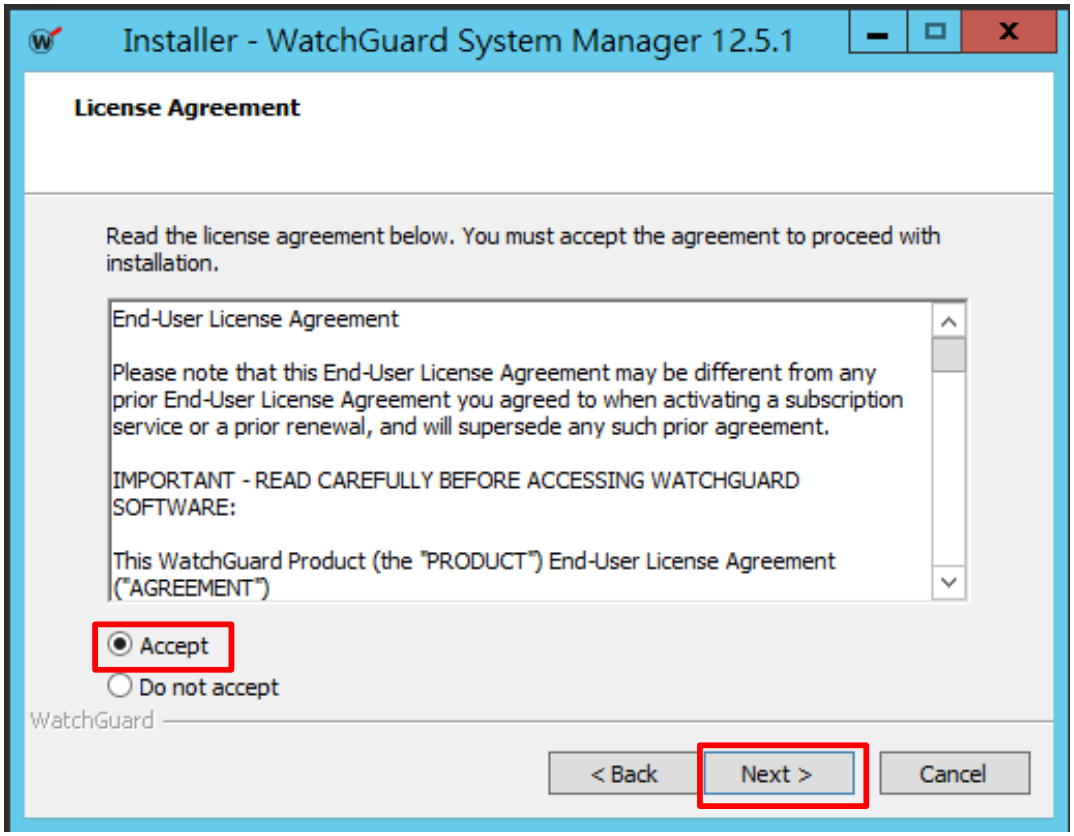


WatchGuard System Manager 安裝

Step 3 :

點選“Next”開始進行安裝精靈

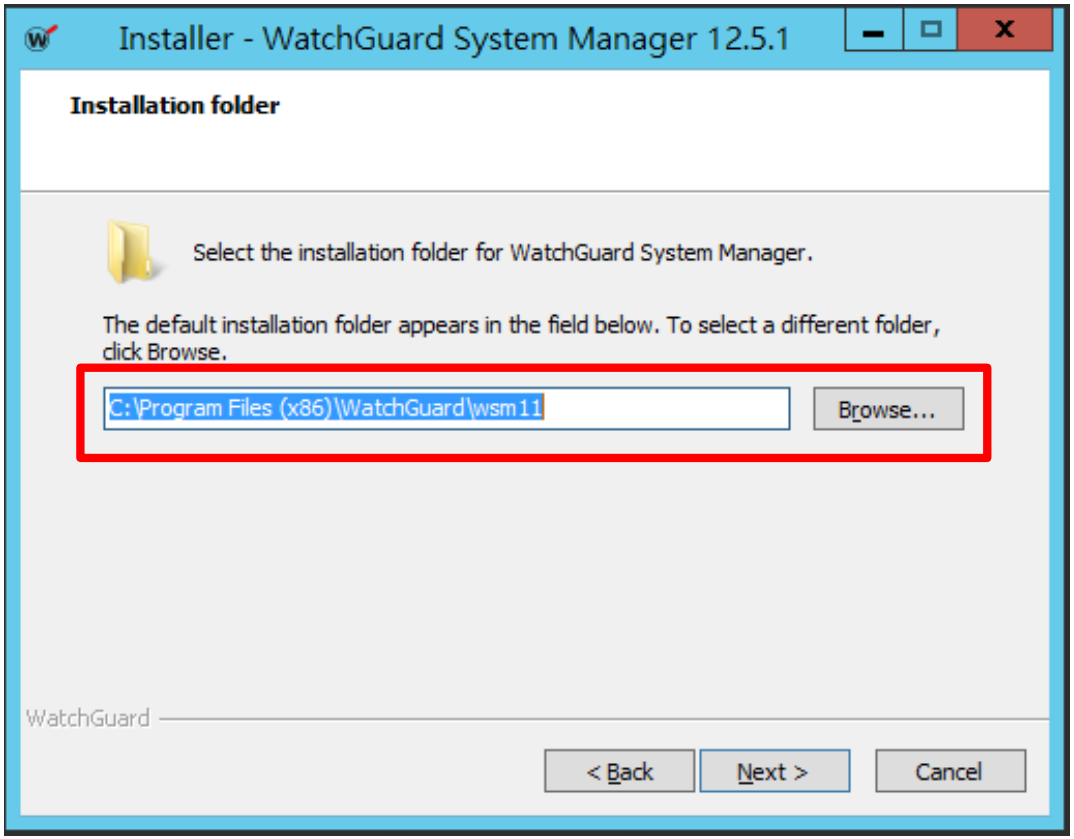
WatchGuard System Manager 安裝



Step 4 :

點選“Accept”接受合約內容，並點選“Next”下一步

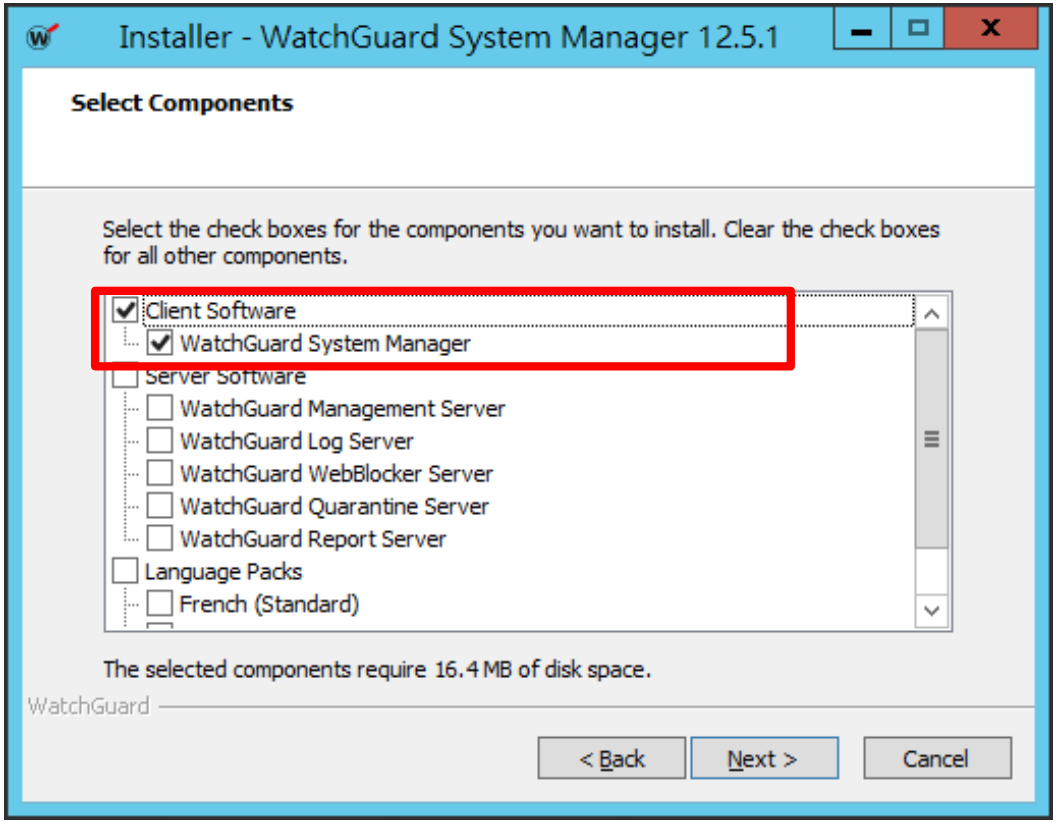
WatchGuard System Manager 安裝



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

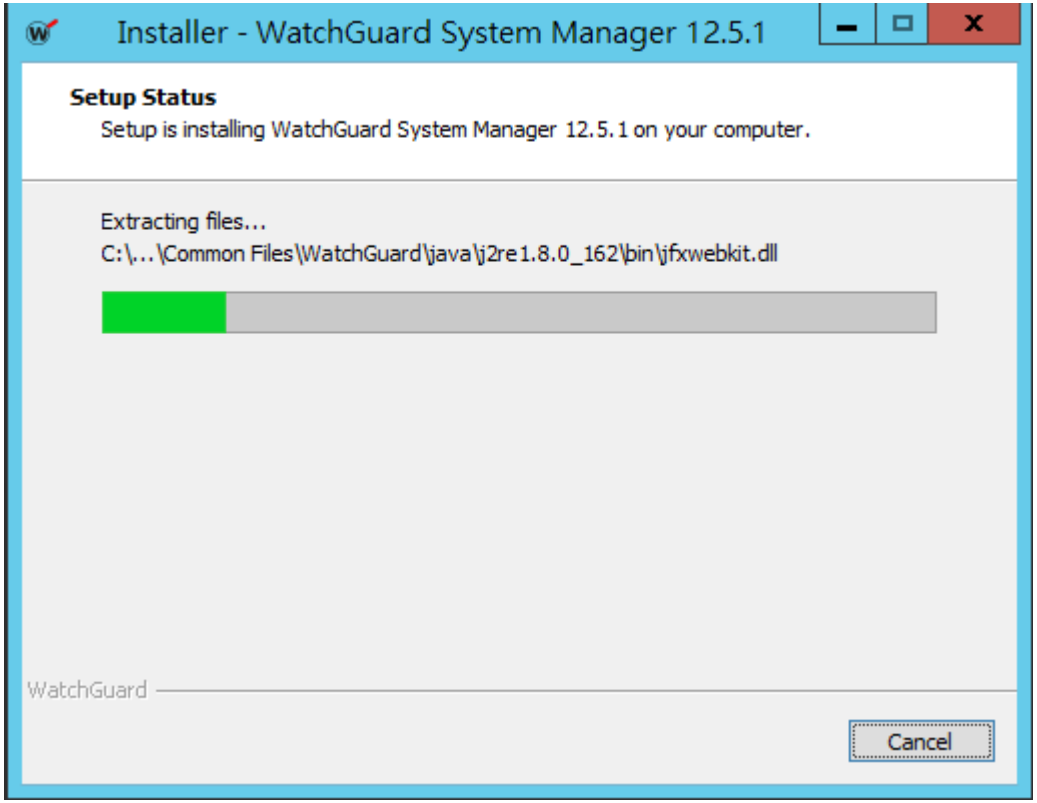
WatchGuard System Manager 安裝



Step 6 :

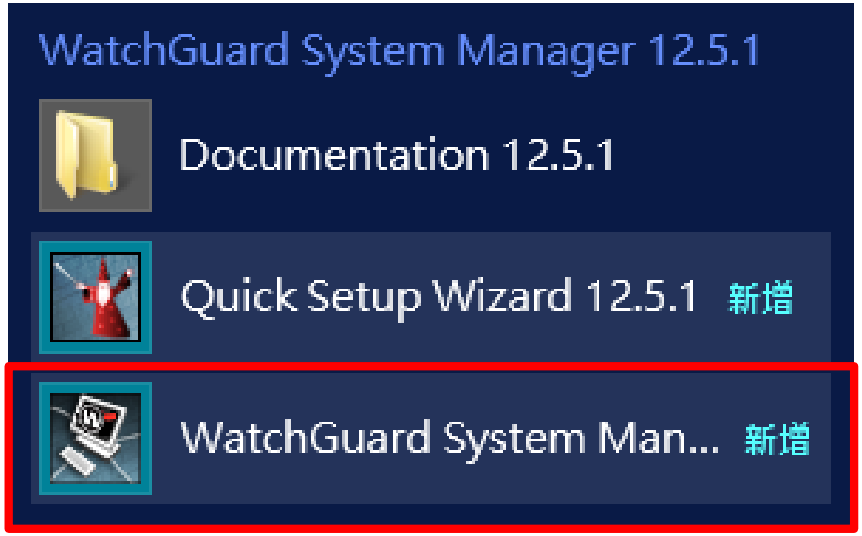
只需要選擇安裝第一個選項”WatchGuard System Manager”

WatchGuard System Manager 安裝



Wait For Installation

執行WSM



安裝完成後在程式集中將出現

WatchGuard System Manager

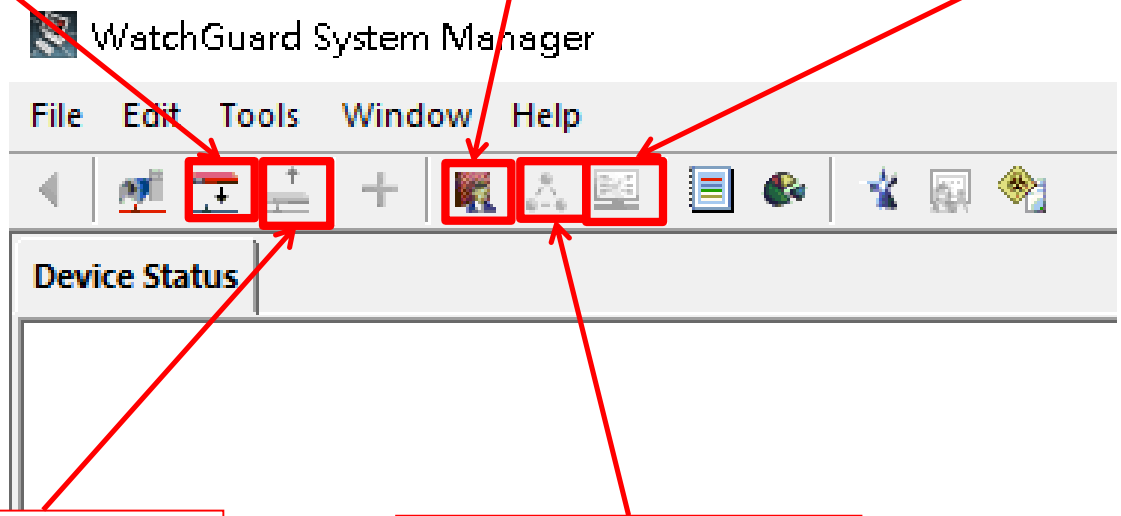
點選此Icon開啟WSM

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

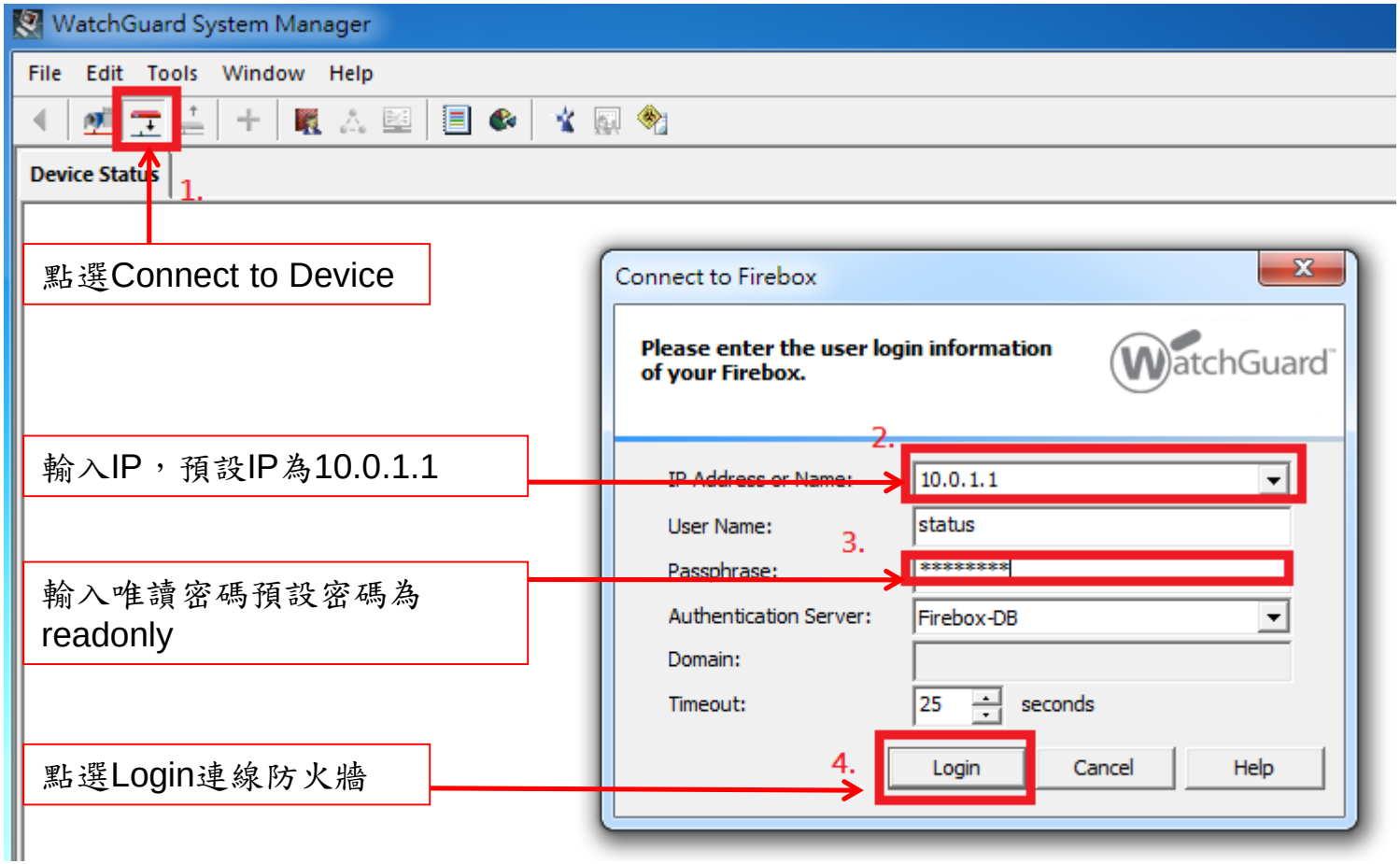
Eth2 Optional
IP : 10.0.2.1

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

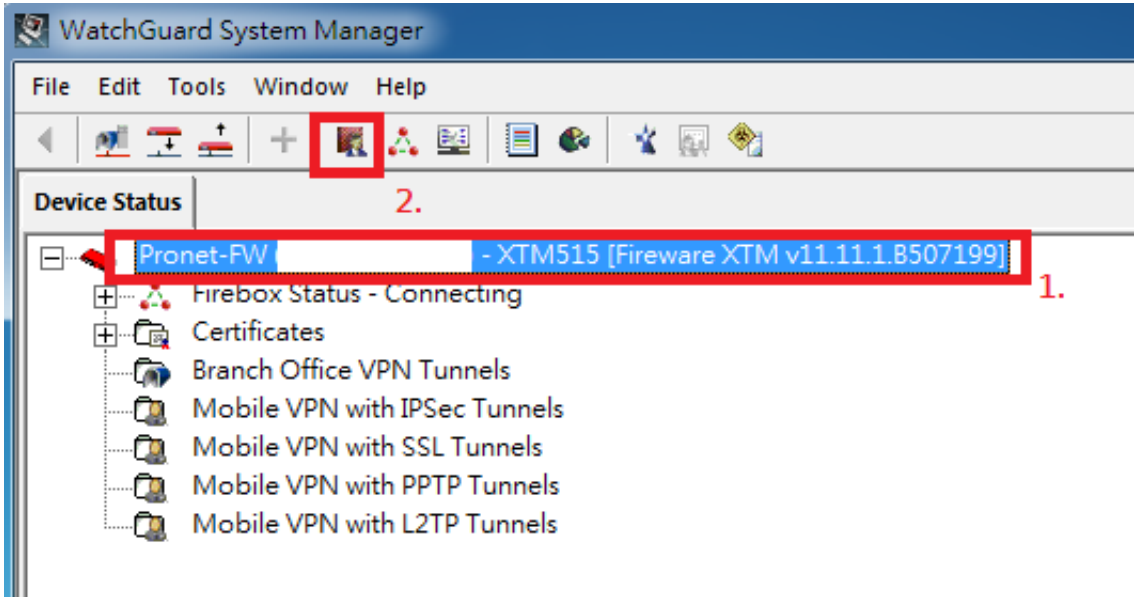
連線管理Firebox Firewall

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



開啟Firewall Policy Manager



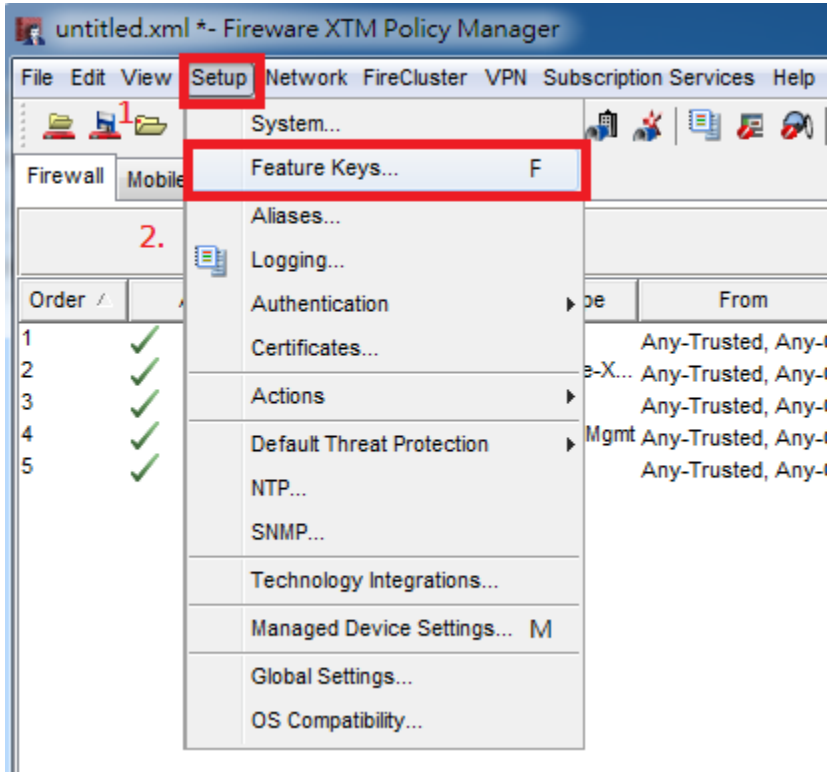
連線防火牆後

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

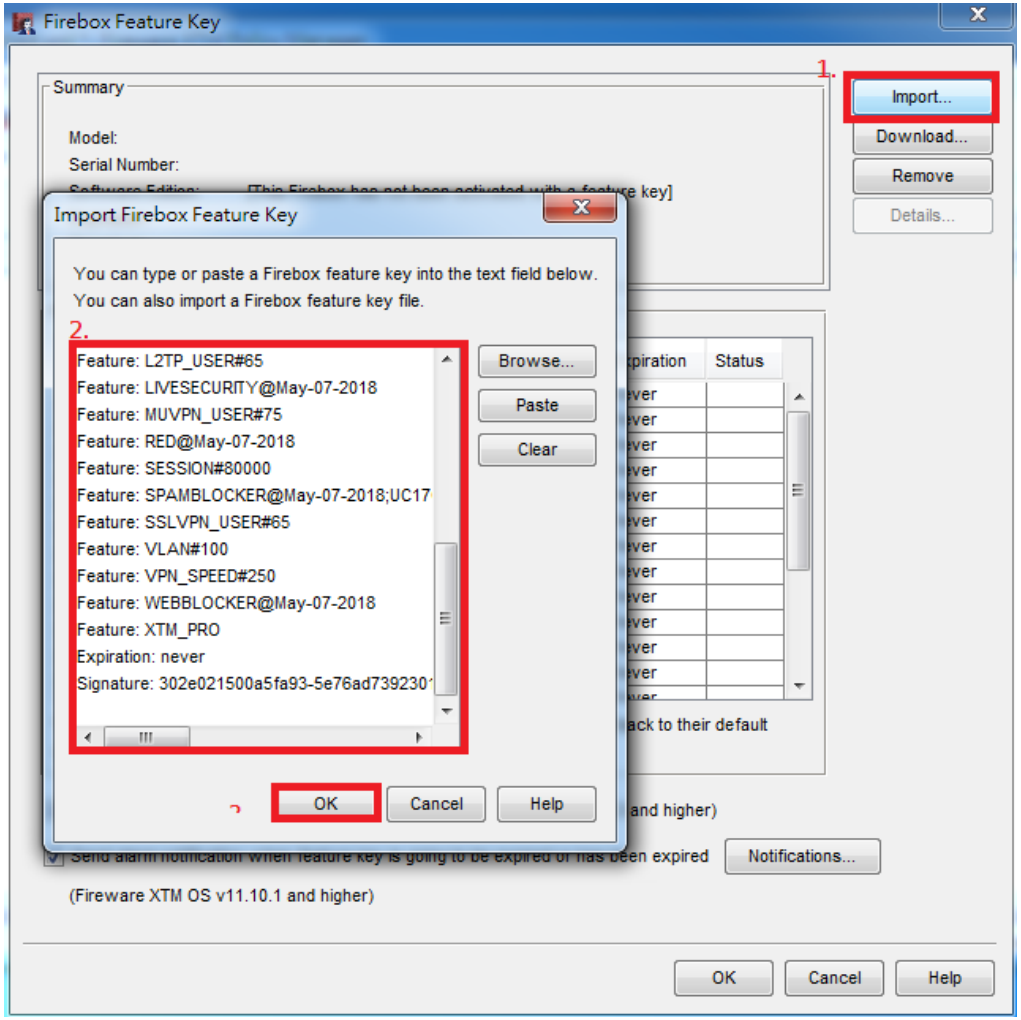


Step 1 :

點選Setup → Feature Keys

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

匯入Feature Key



Step 2 :

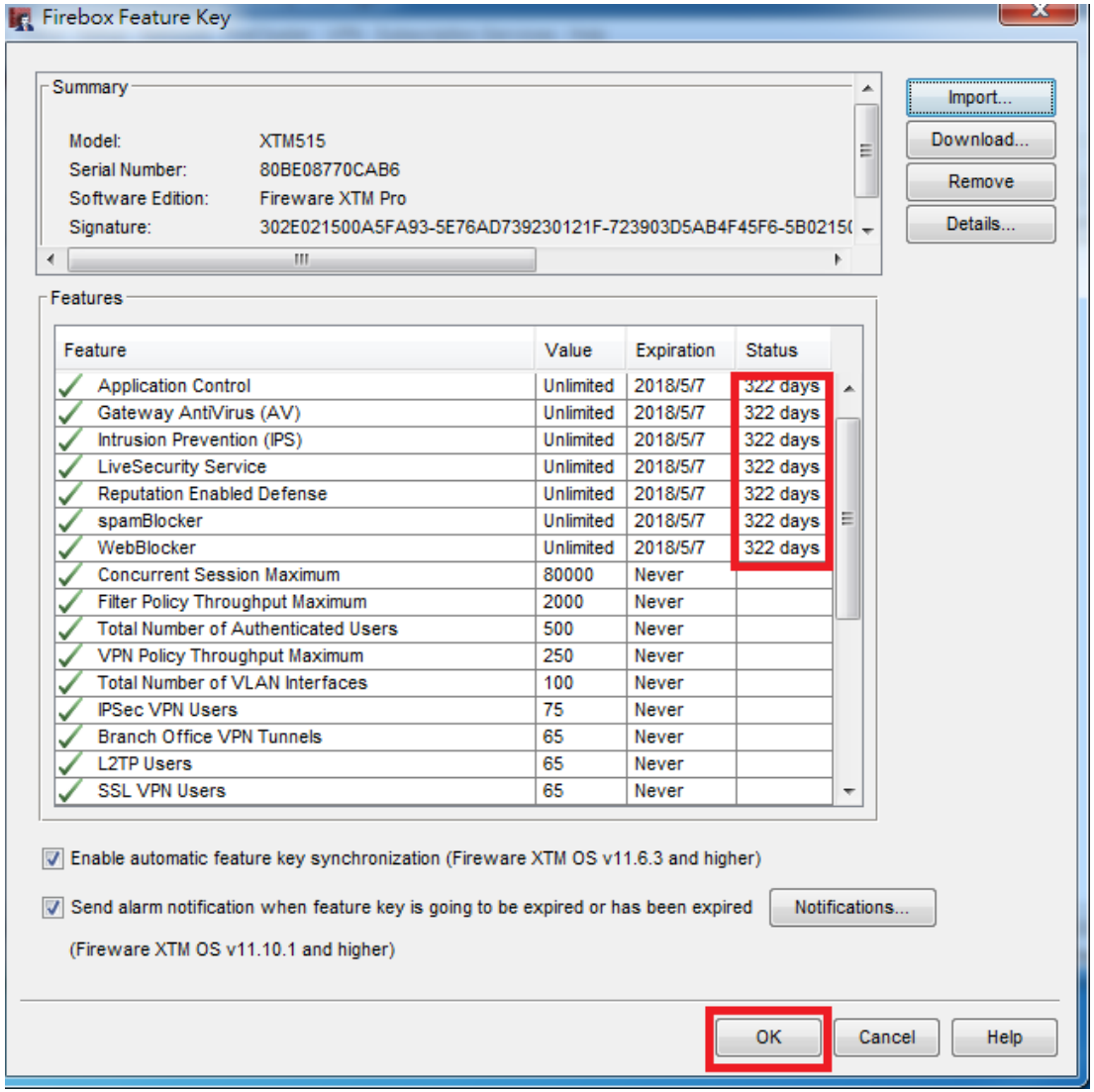
1.點選Import，點選後會彈跳出Import Firebox Feature Key的視窗

2.於框內貼上事先下載的Feature Key

Feature Key可於WatchGuard網站上下載，或是由代理商提供

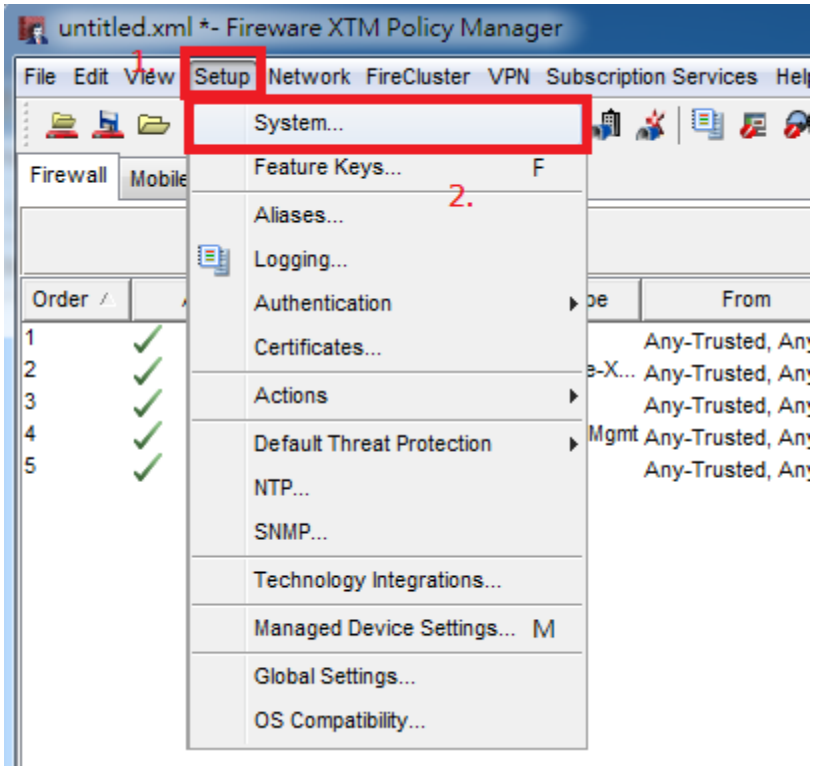
3.點選OK

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

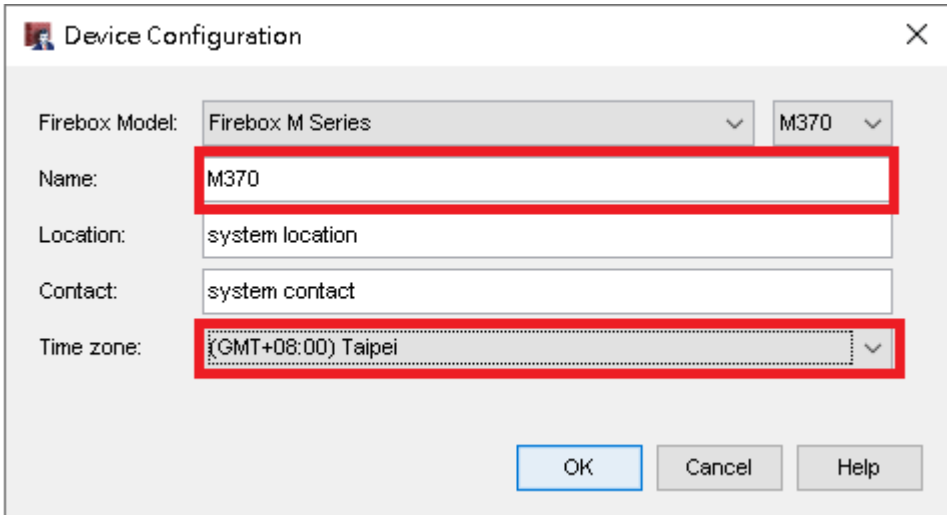


Step 1 :

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

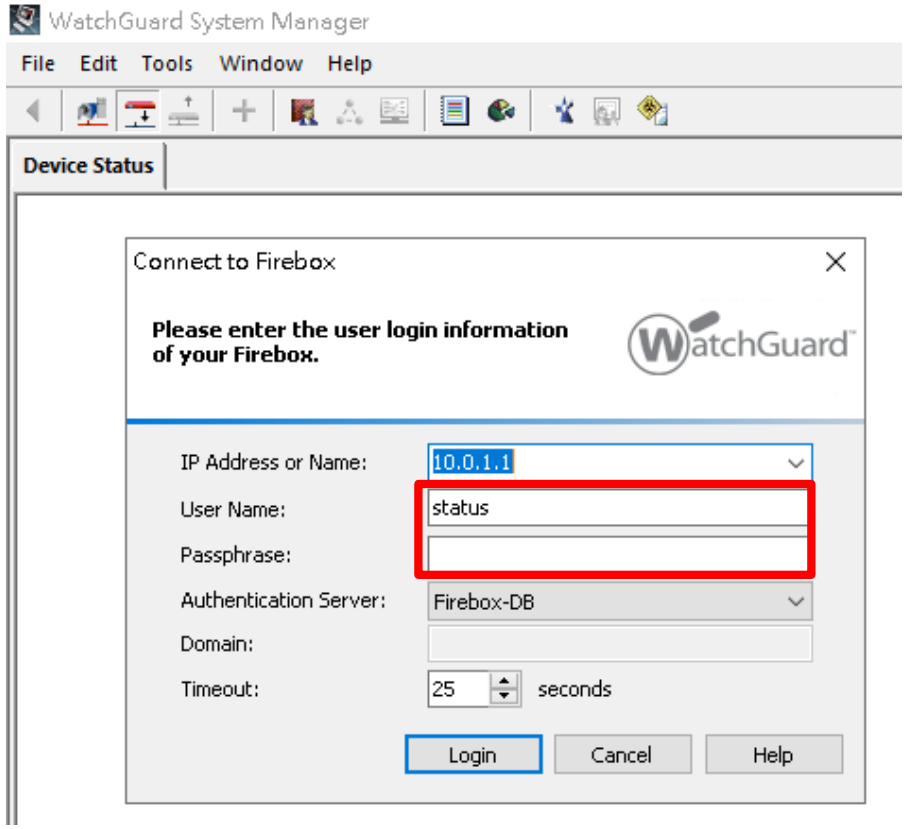


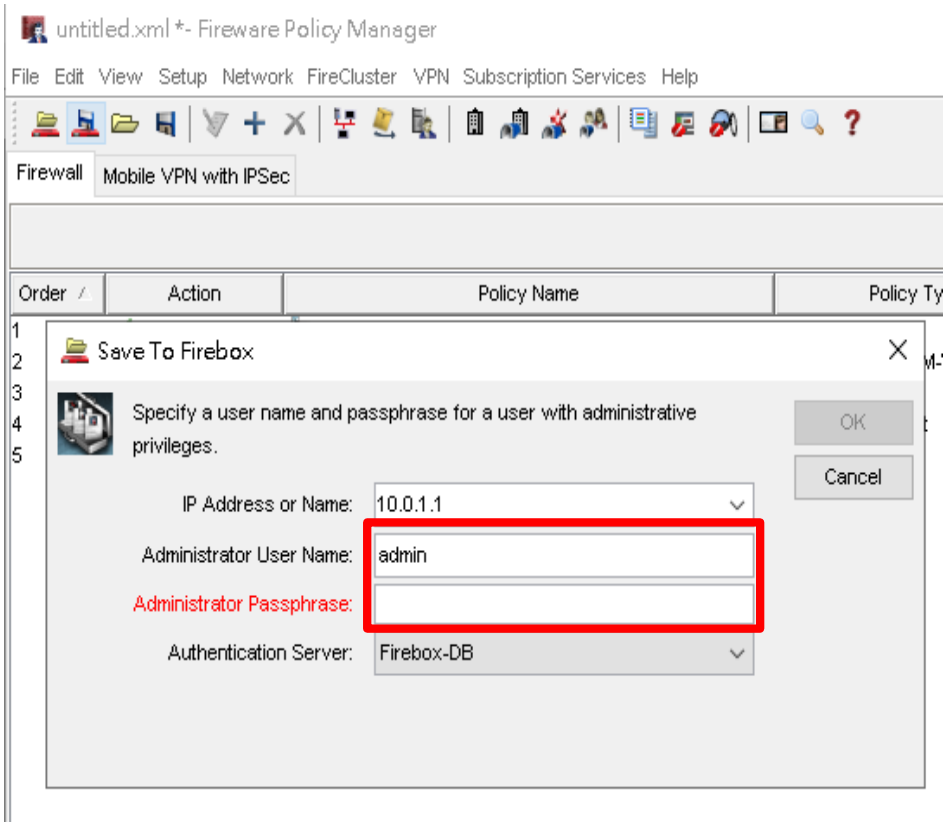
Step 2 :

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

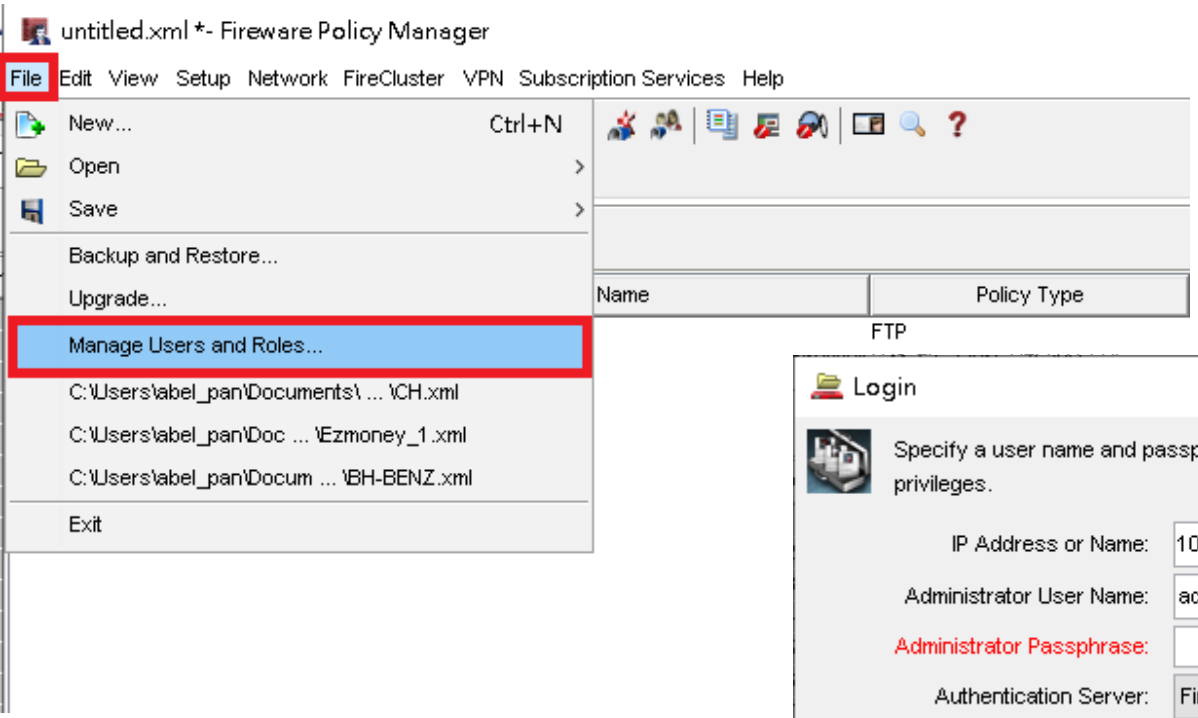
預設密碼

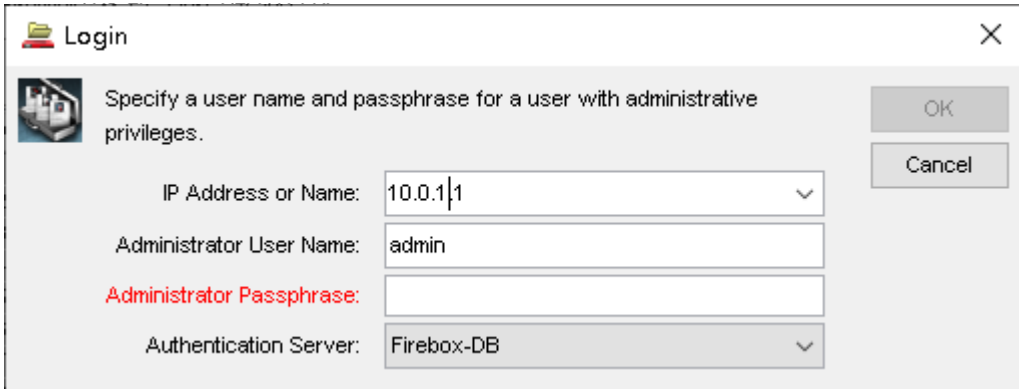
readonly

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



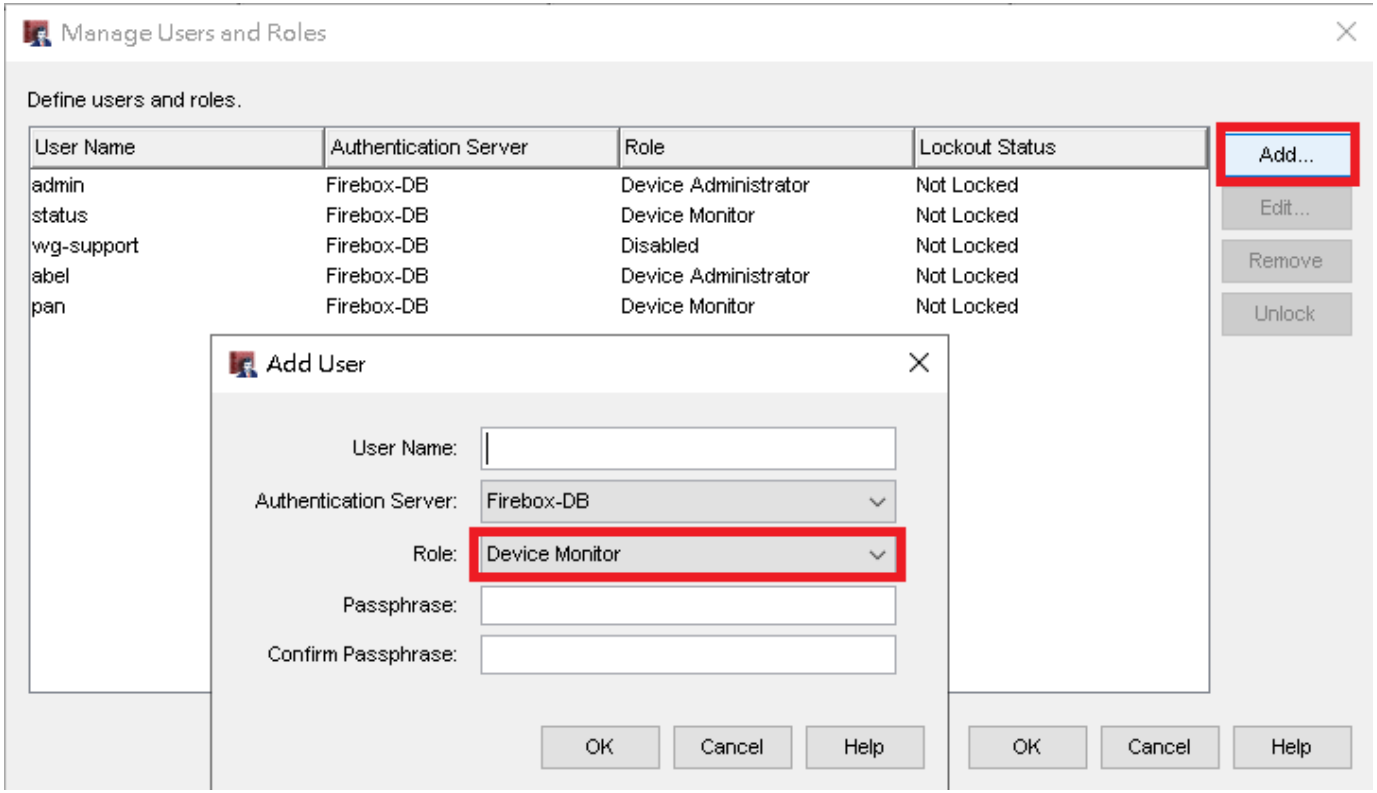


Step 1 :

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

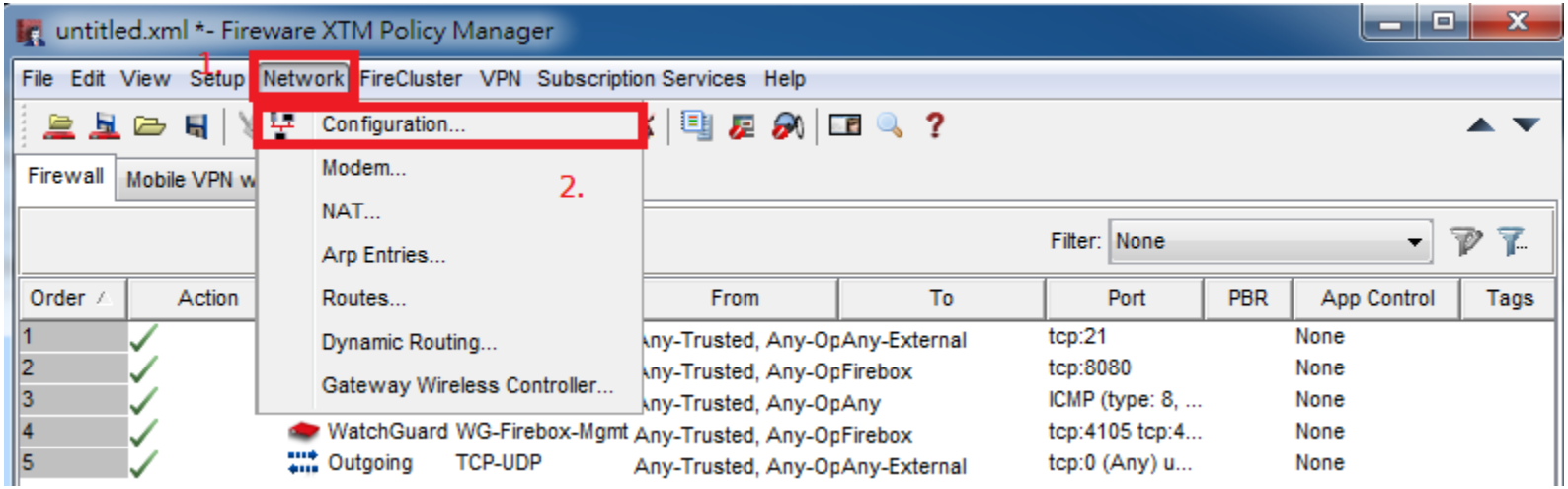


Step 2 : 1. 點選Add 新增帳號

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

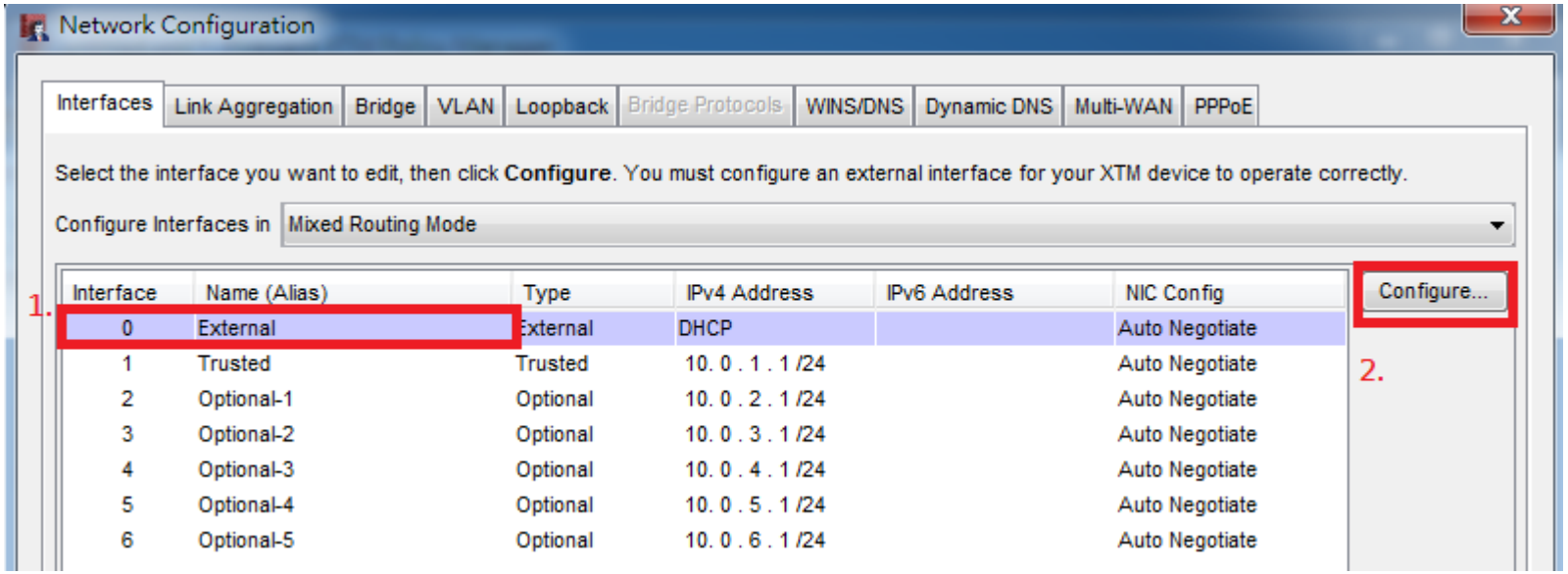
Network 參數設定

網路介面設定



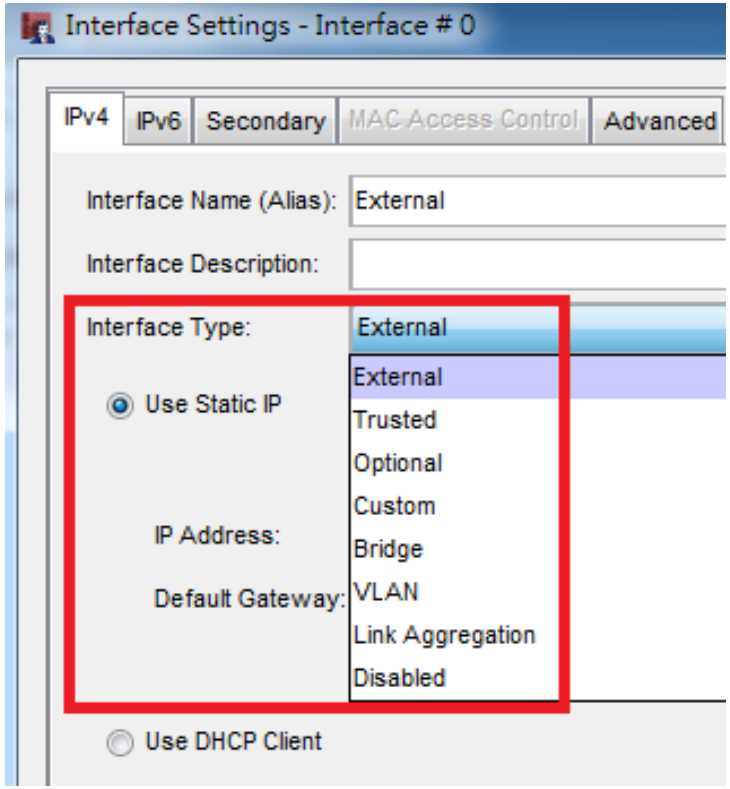
點選Network → Configuration

網路介面設定



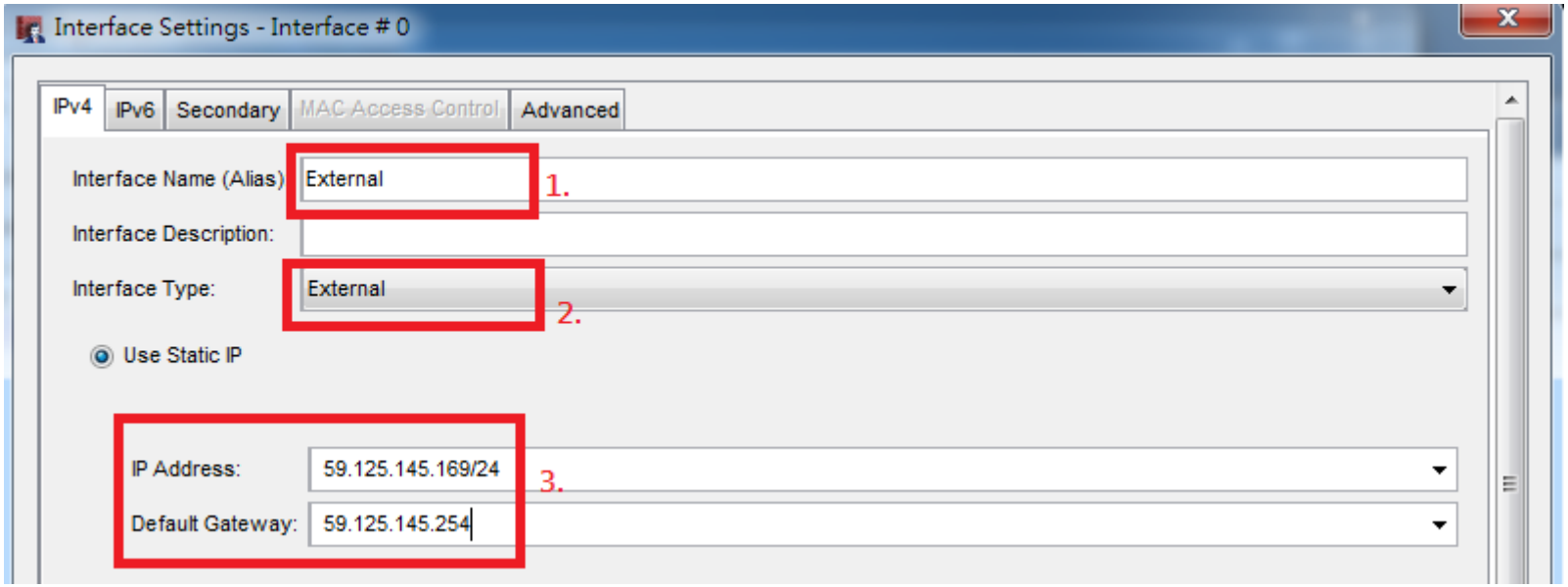
點選要設定的介面→ Configure

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



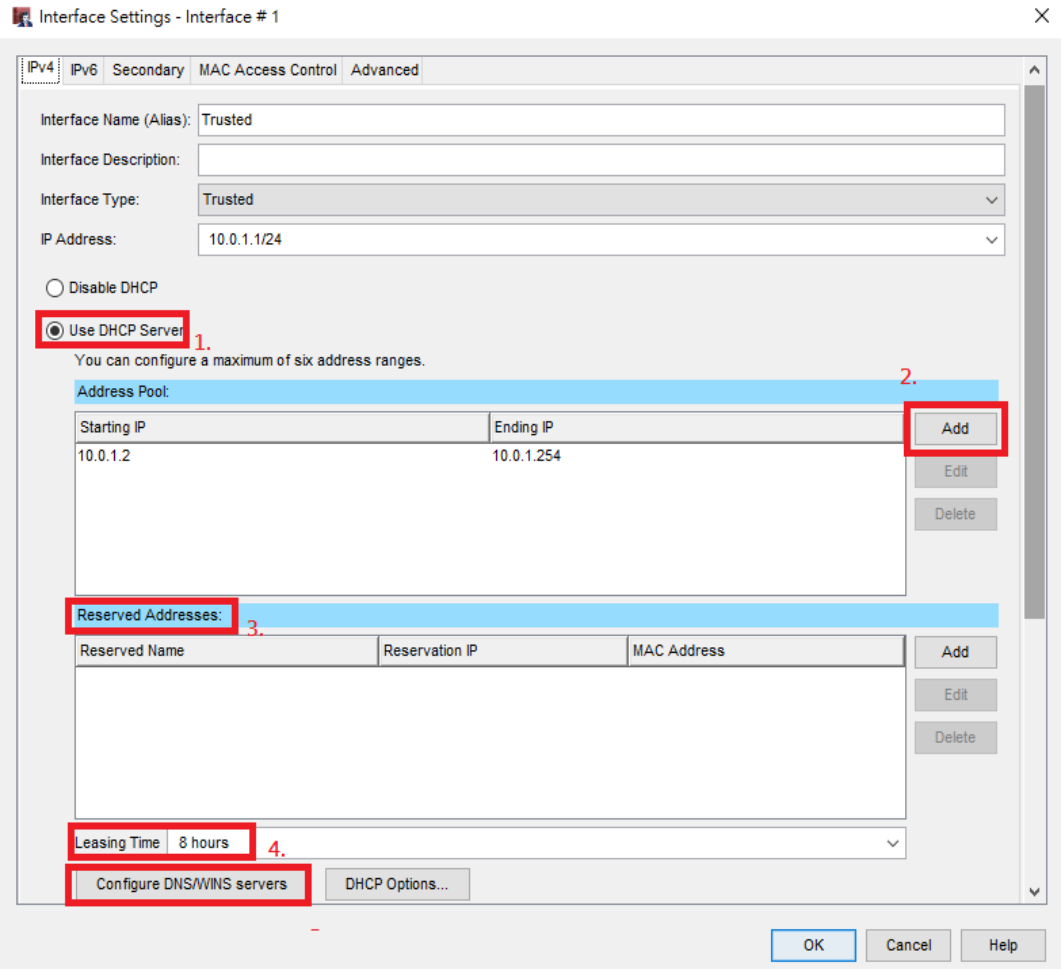
1.輸入名稱，以方便後續識別介面

2.選擇Interface Type

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

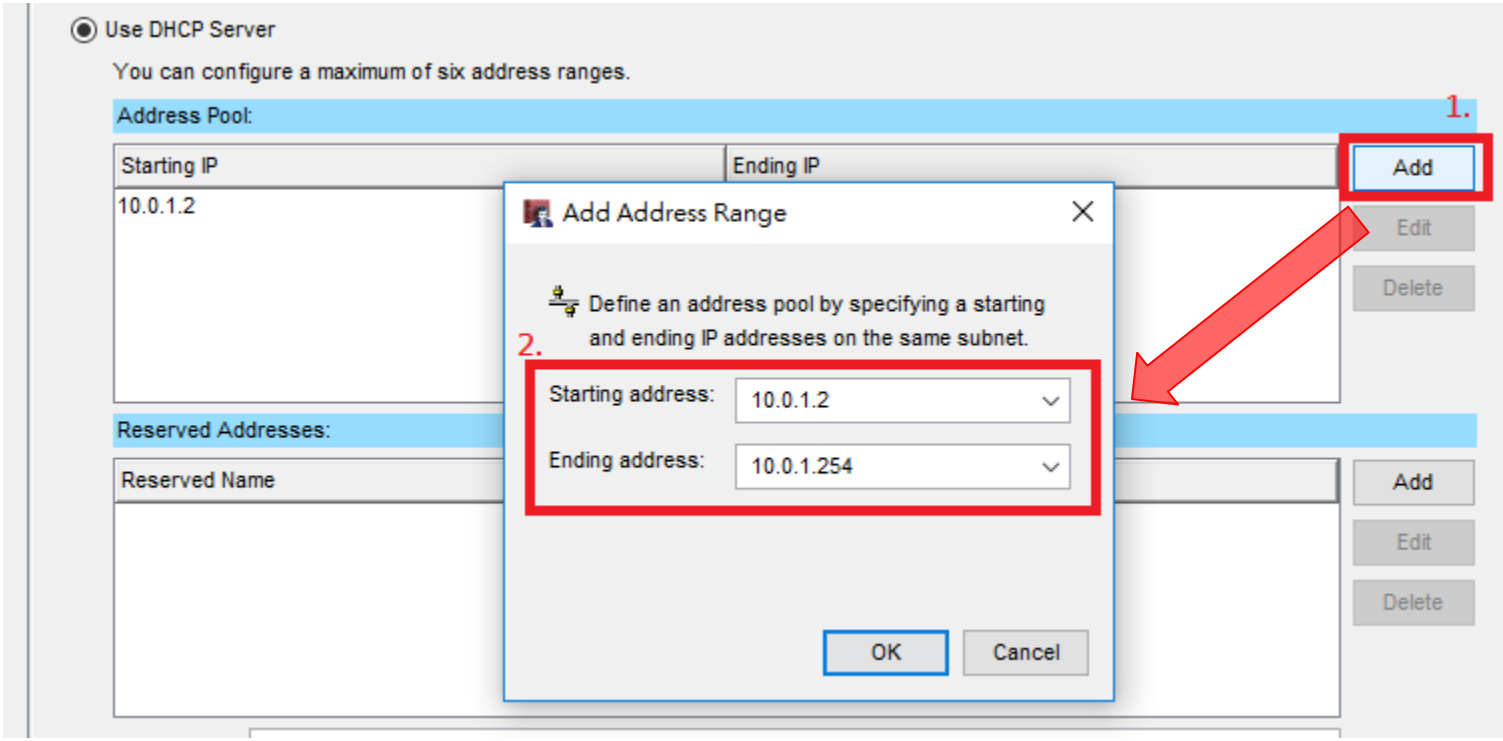
Note ：WatchGuard Firewall所有型號皆可介接4條對外線路

設定DHCP Server



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

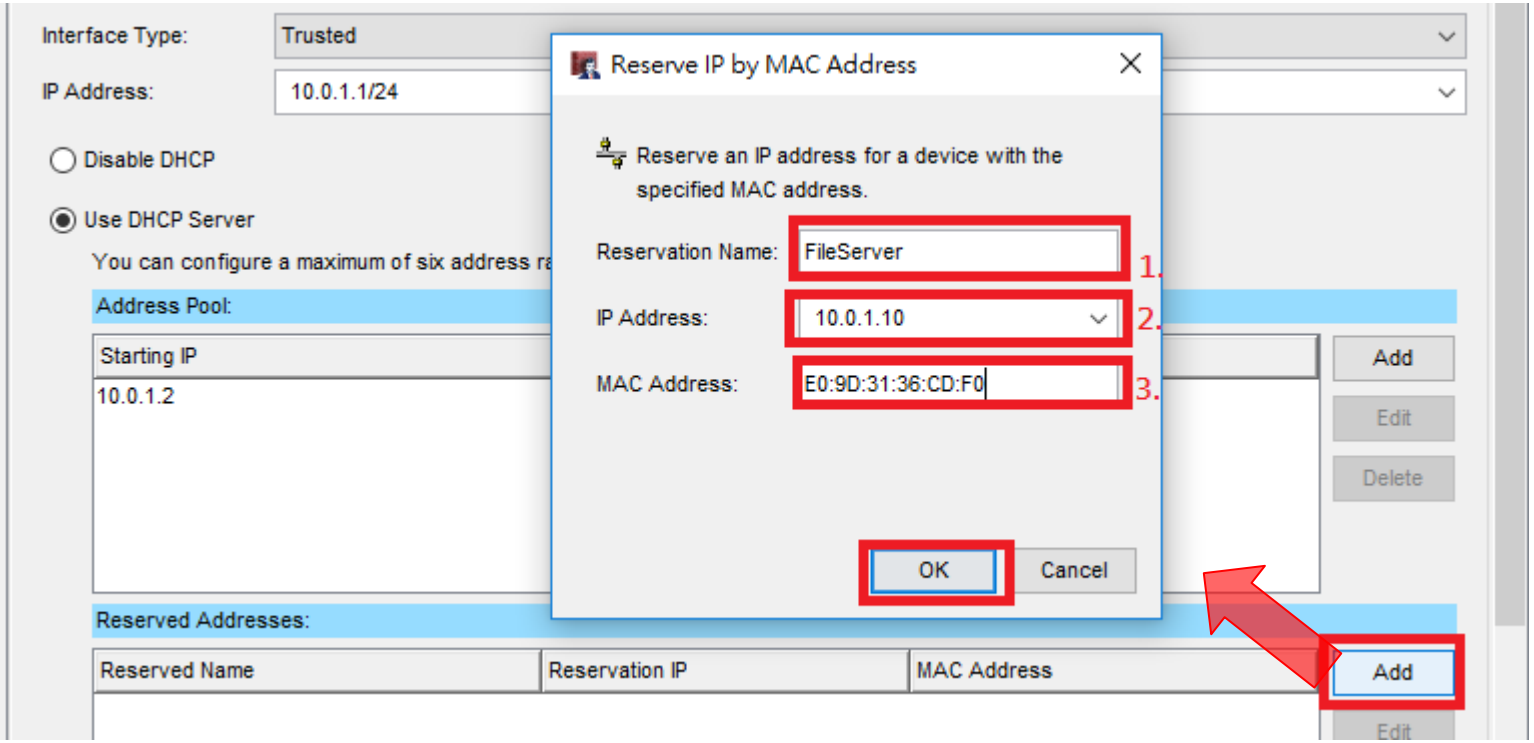
設定DHCP Pool



點選Add新增DHCP Pool

Note：DHCP Pool必須和介面同一個網段

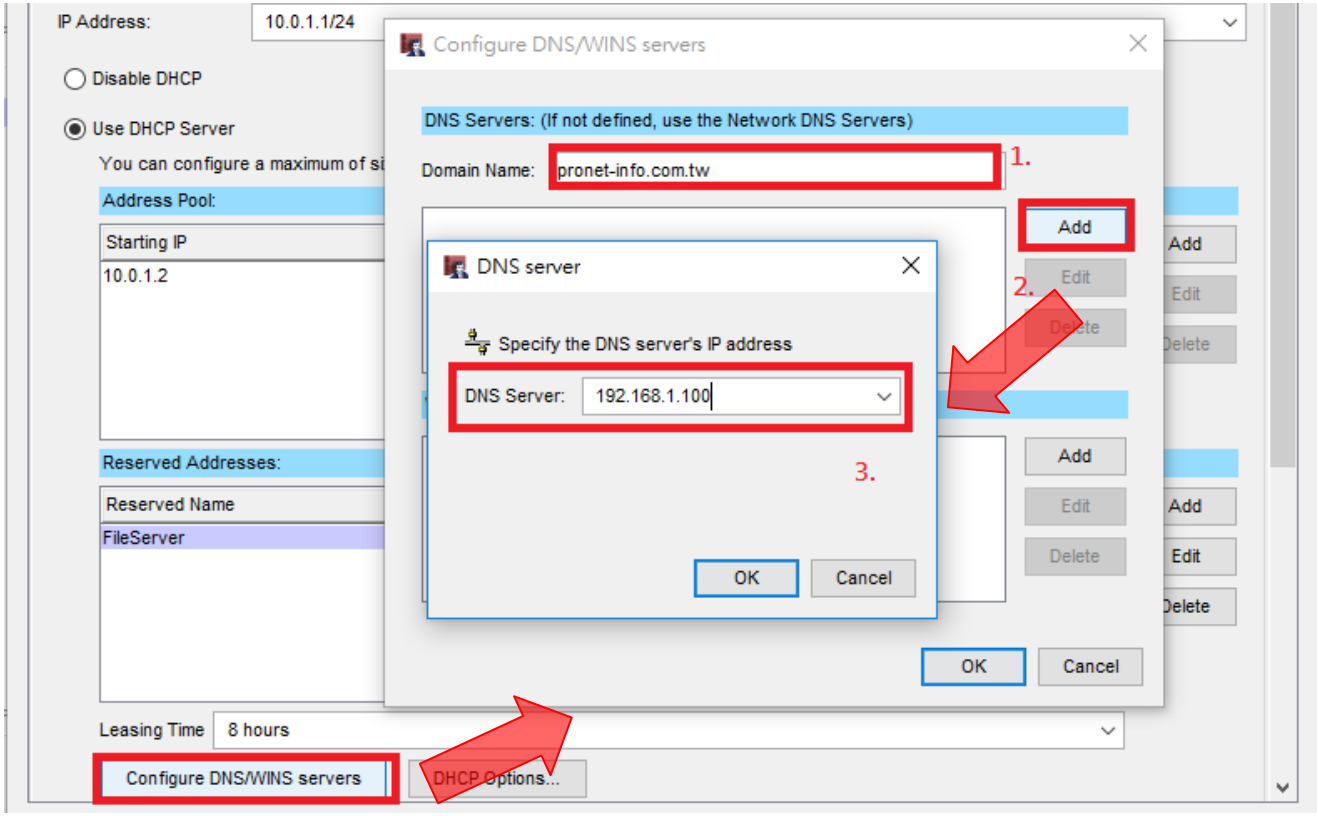
設定Reserved Addressed



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

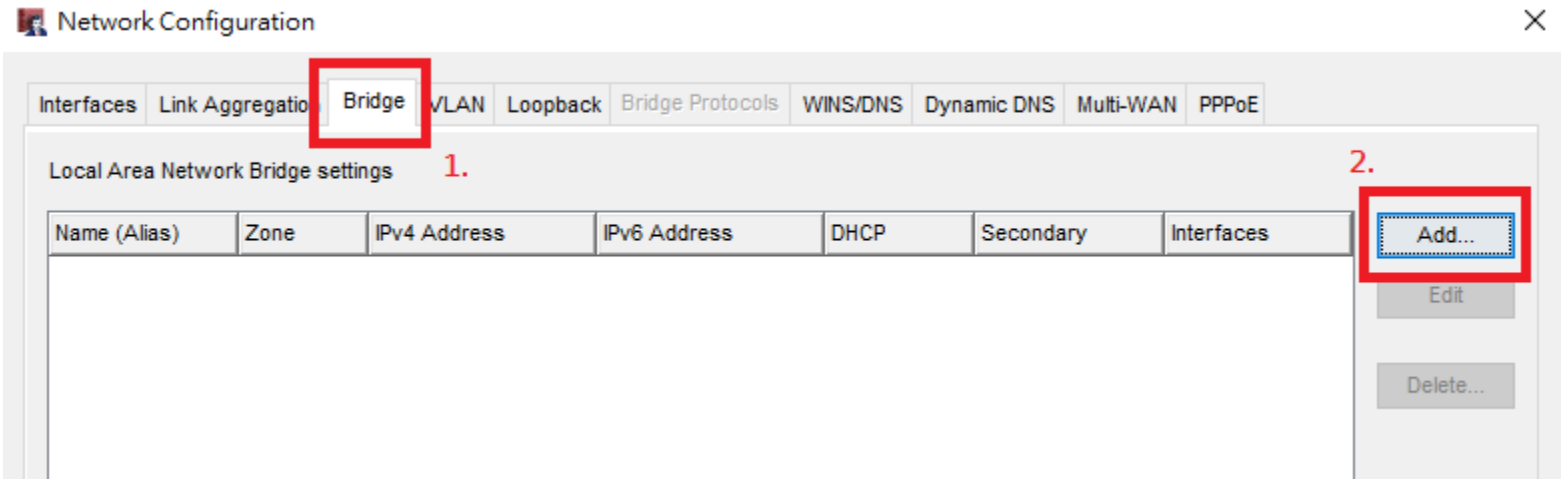
1. 輸入Domain Name (Option)
2. 點選Add
3. 輸入DNS IP Address

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

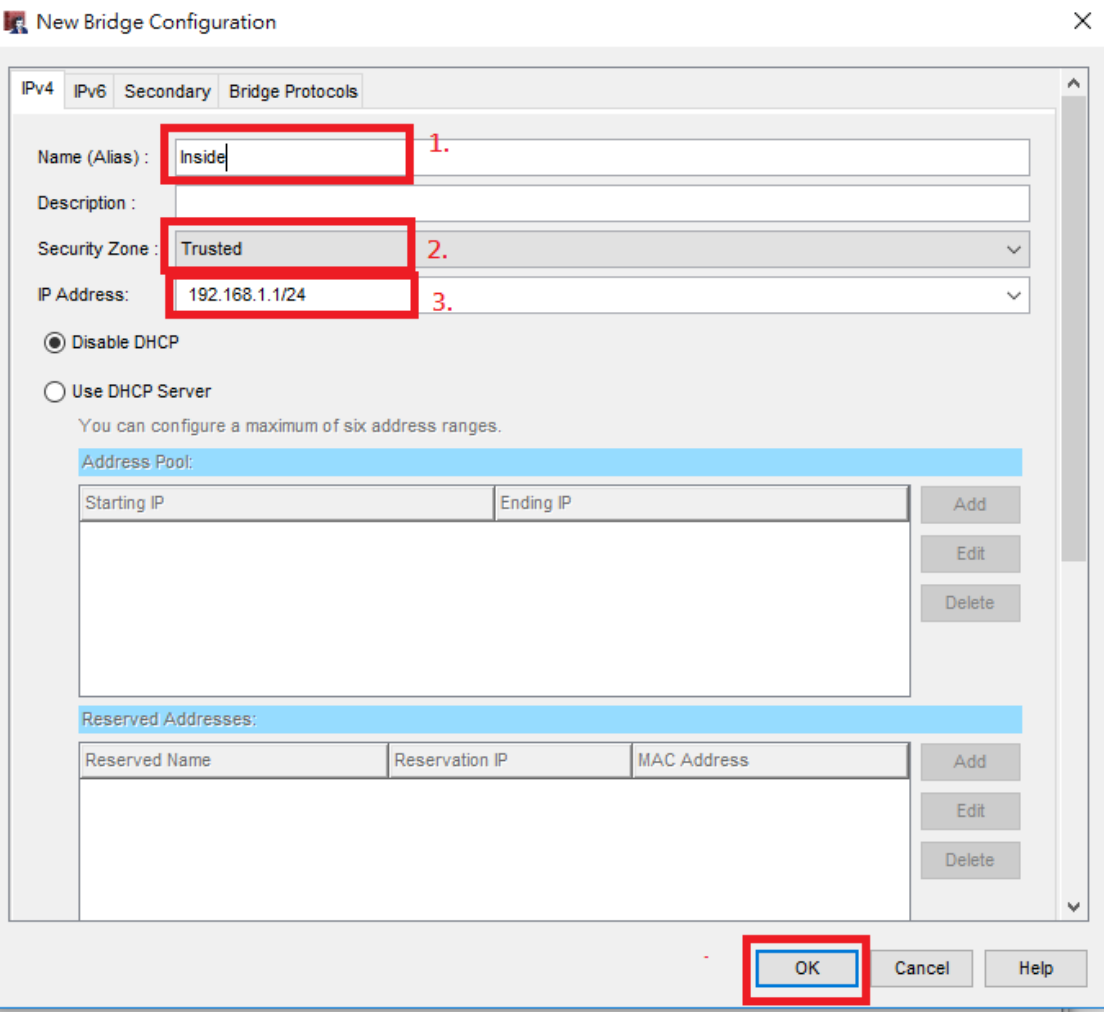


Step 1 :

Network → Configuration

1. 選擇上方頁簽 Bridge
2. 點選Add

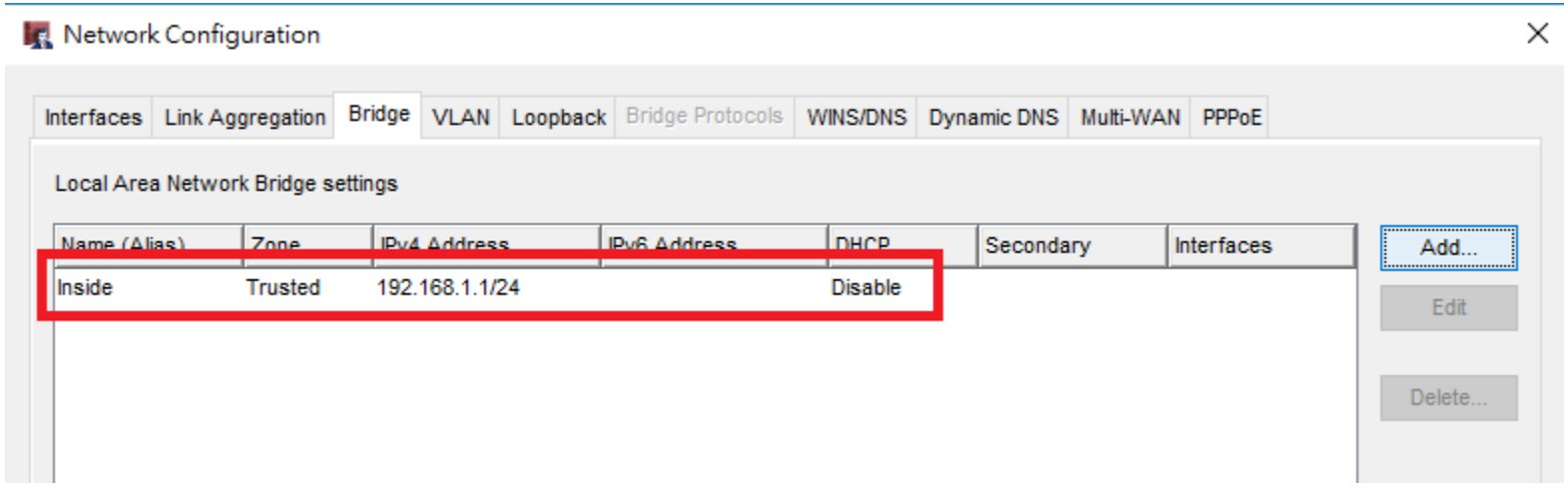
Interface Bridge 設定



Step 2 :

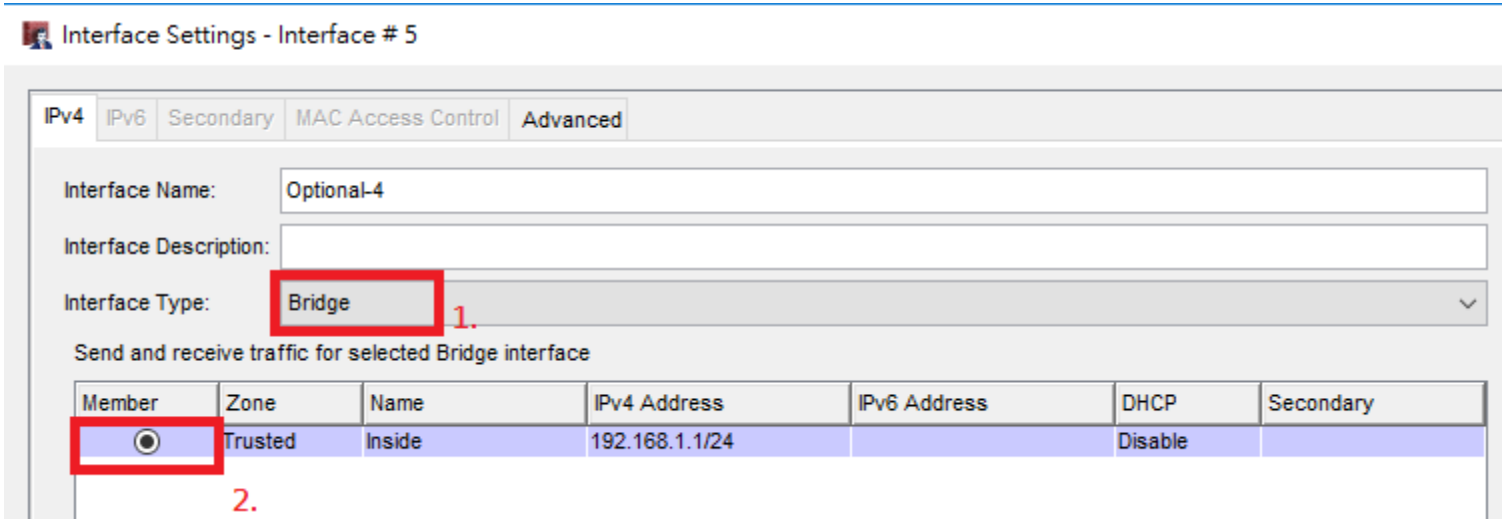
1. 設定介面名稱
2. 選擇Security Zone，External 介面不可設定Bridge
3. 輸入IP Address
4. 點選OK

確認Interface Bridge 設定



Bridge介面資訊設定完成後顯示於Bridge頁面

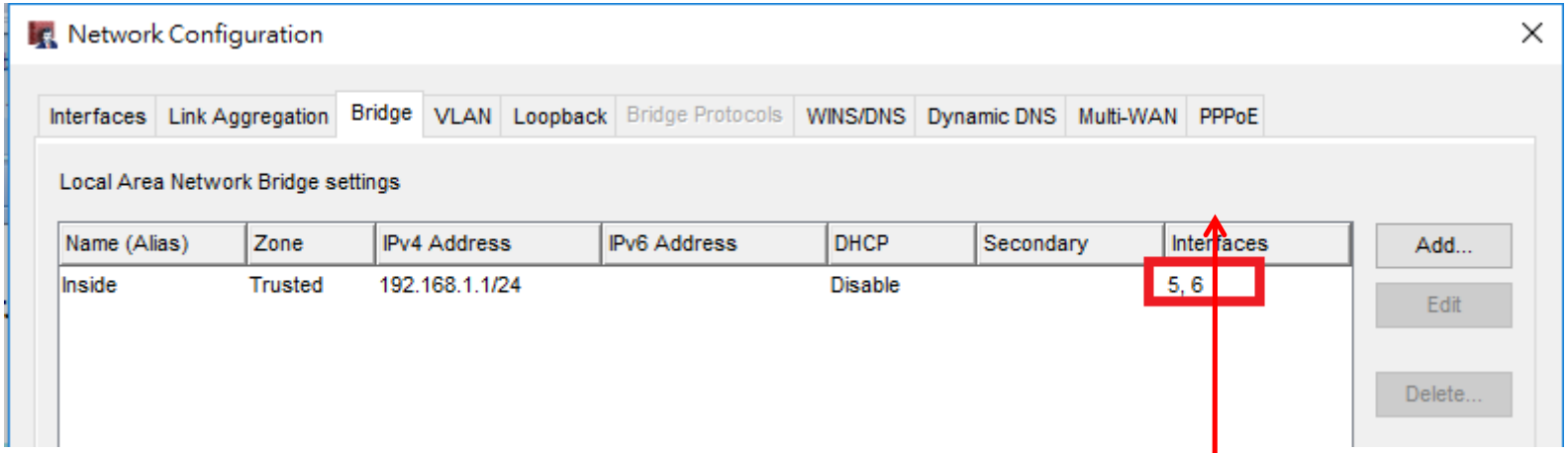
將實體介面加入Interface Bridge



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

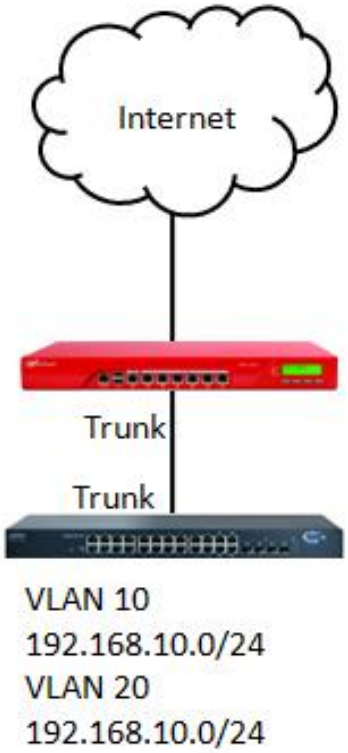
確認Interface Bridge 設定完成



Eth5以及Eth6設定完成加入到同一個Bridge

VLAN設定

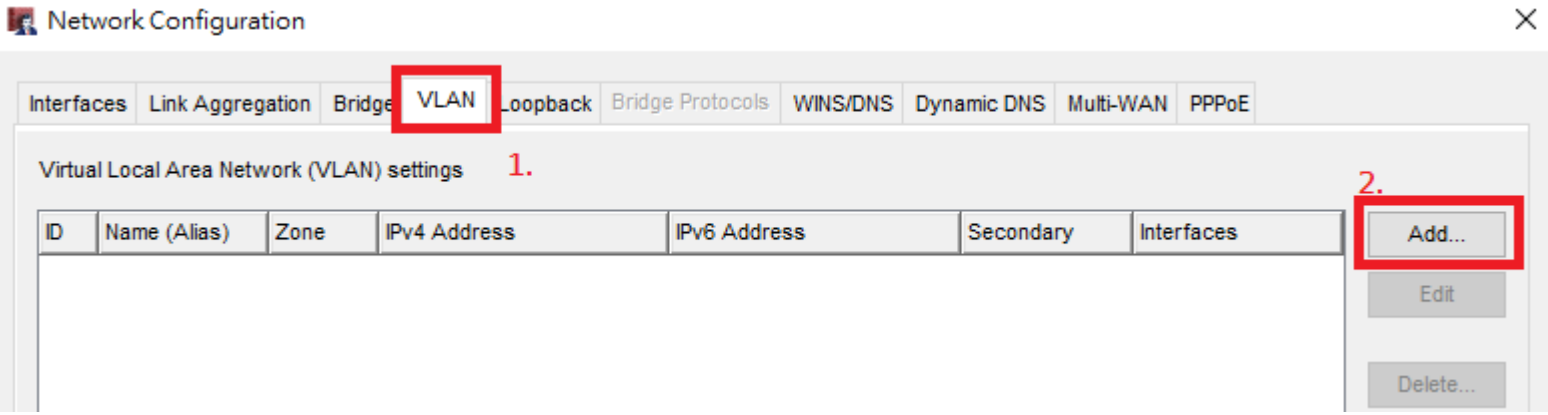
範例情境



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

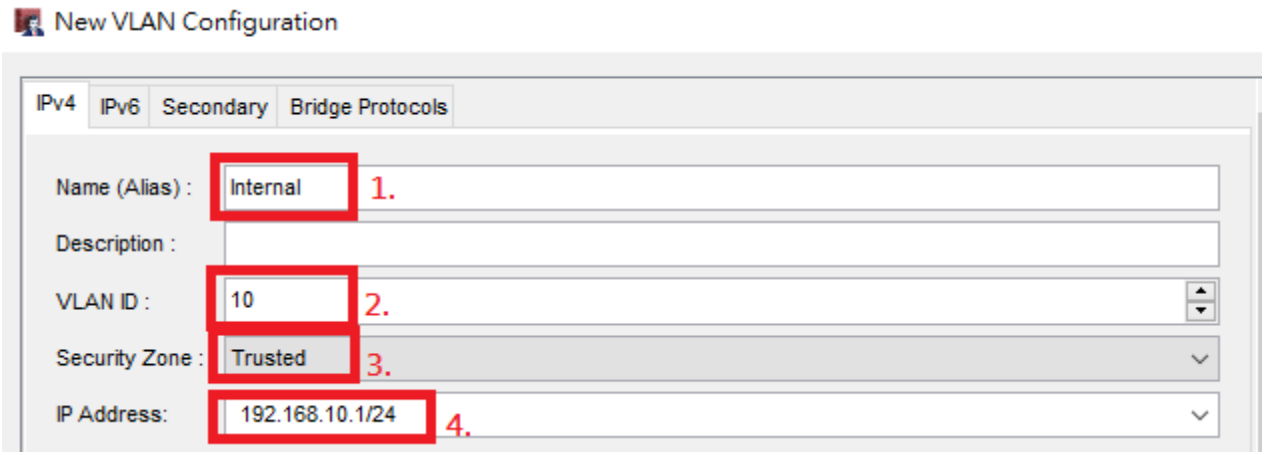
VLAN設定



Network → Configuration

1. 選擇上方頁簽 VLAN
2. 點選Add

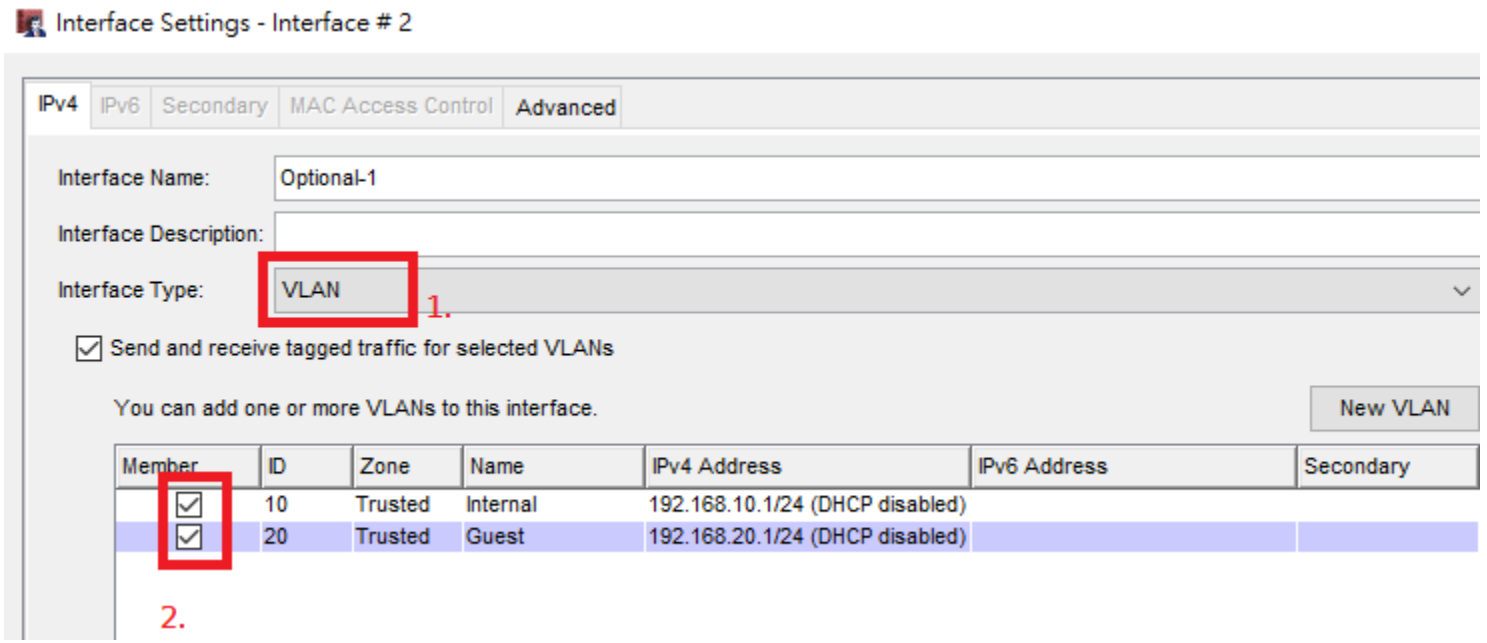
VLAN介面設定



VLAN設定說明

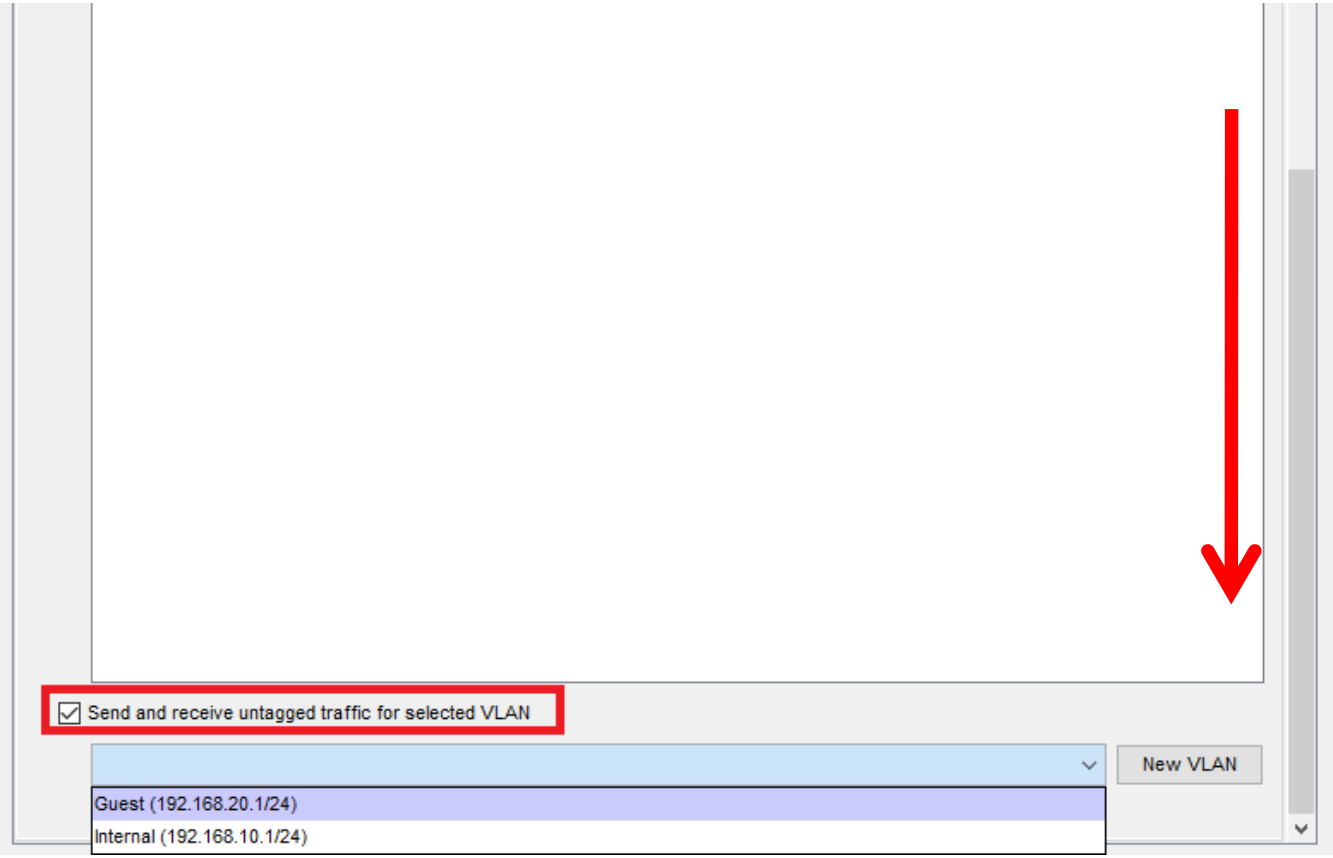
1. Name : 輸入VLAN名稱
2. VLAN ID : 此為VLAN Tag設定，如果此VLAN為VLAN 10，此欄位要輸入10
3. Security Zone : 選擇該VLAN所屬的型態
4. IP Address : 輸入此Interface VLAN IP位置

實體介面VLAN設定



1. Interface Type選擇VLAN
2. 將下方Member VLAN勾選起來

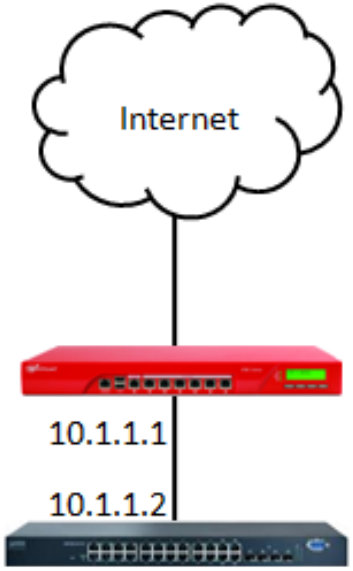
Native VLAN設定



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

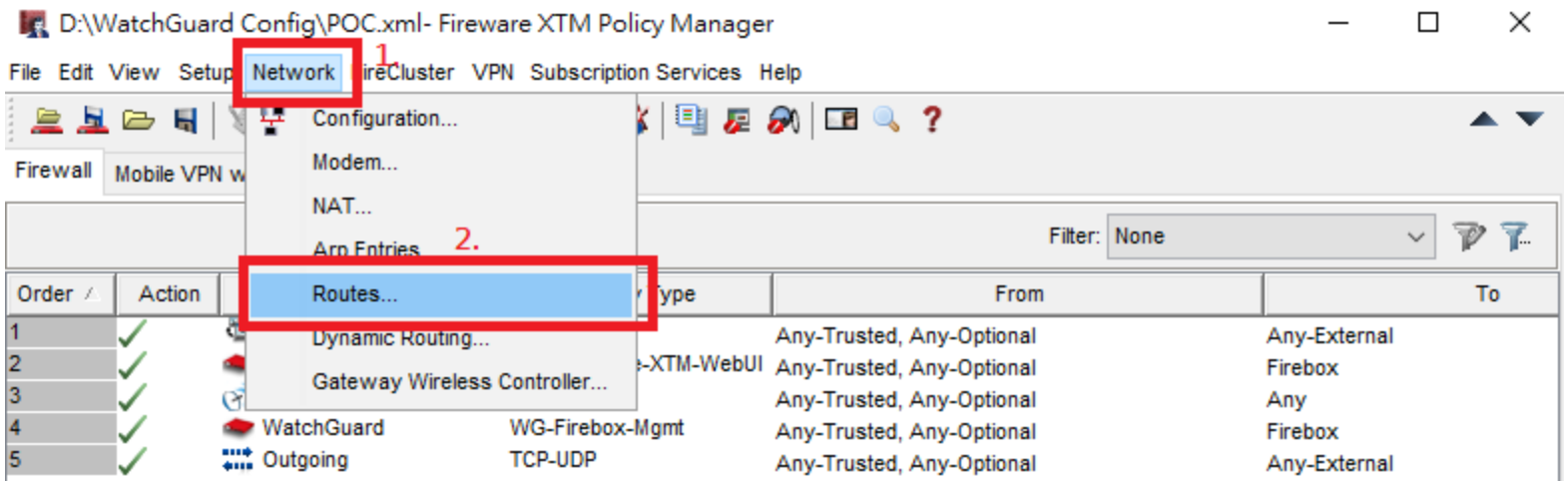
範例情境二



架構說明

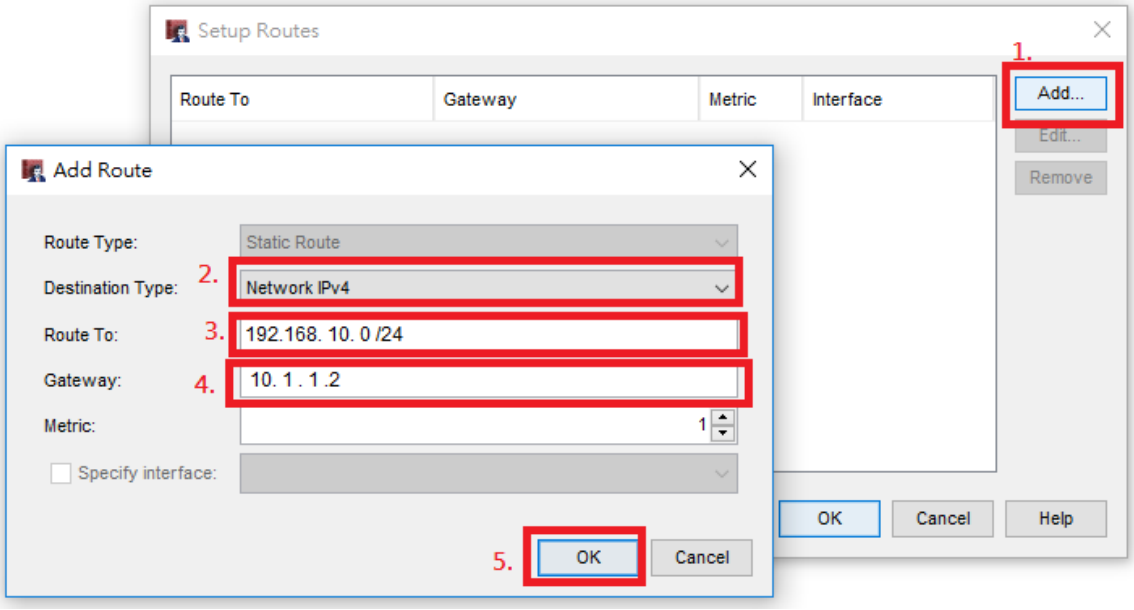
1. WatchGuard 下方介接的Switch為L3 Switch
2. 內部網段路由在Core Switch完成
3. WatchGuard必須設定靜態路由江內部網段指回Core Switch

Static Route設定



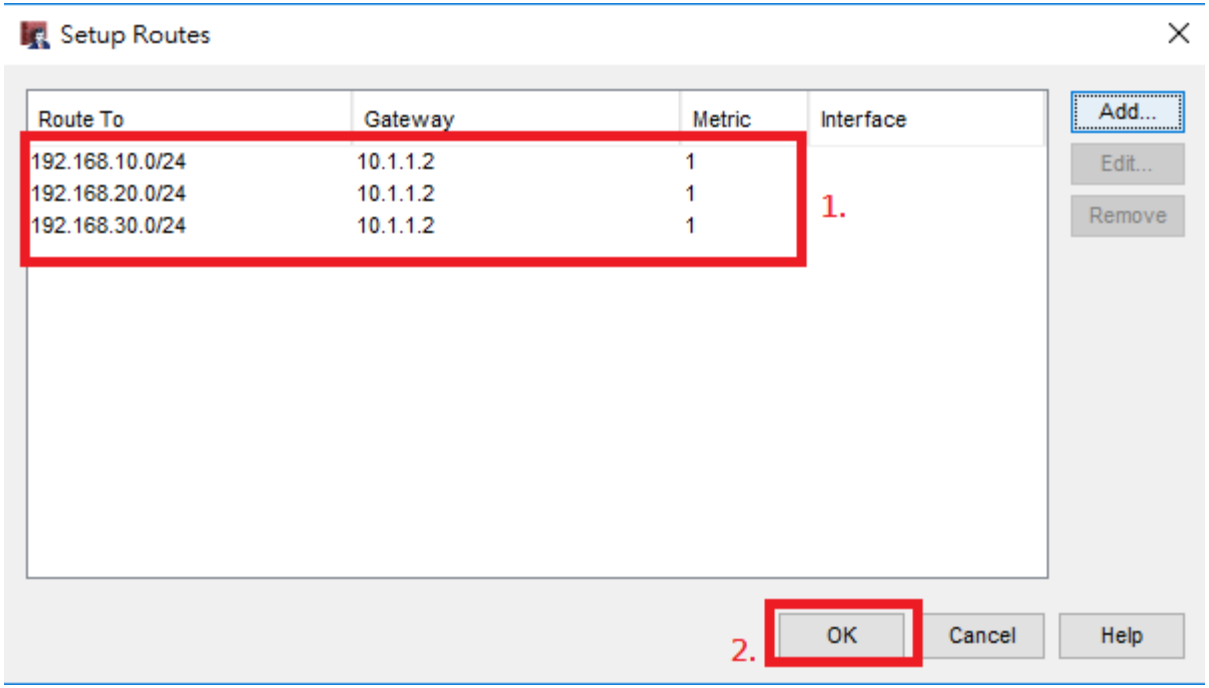
點選Network → Routes

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

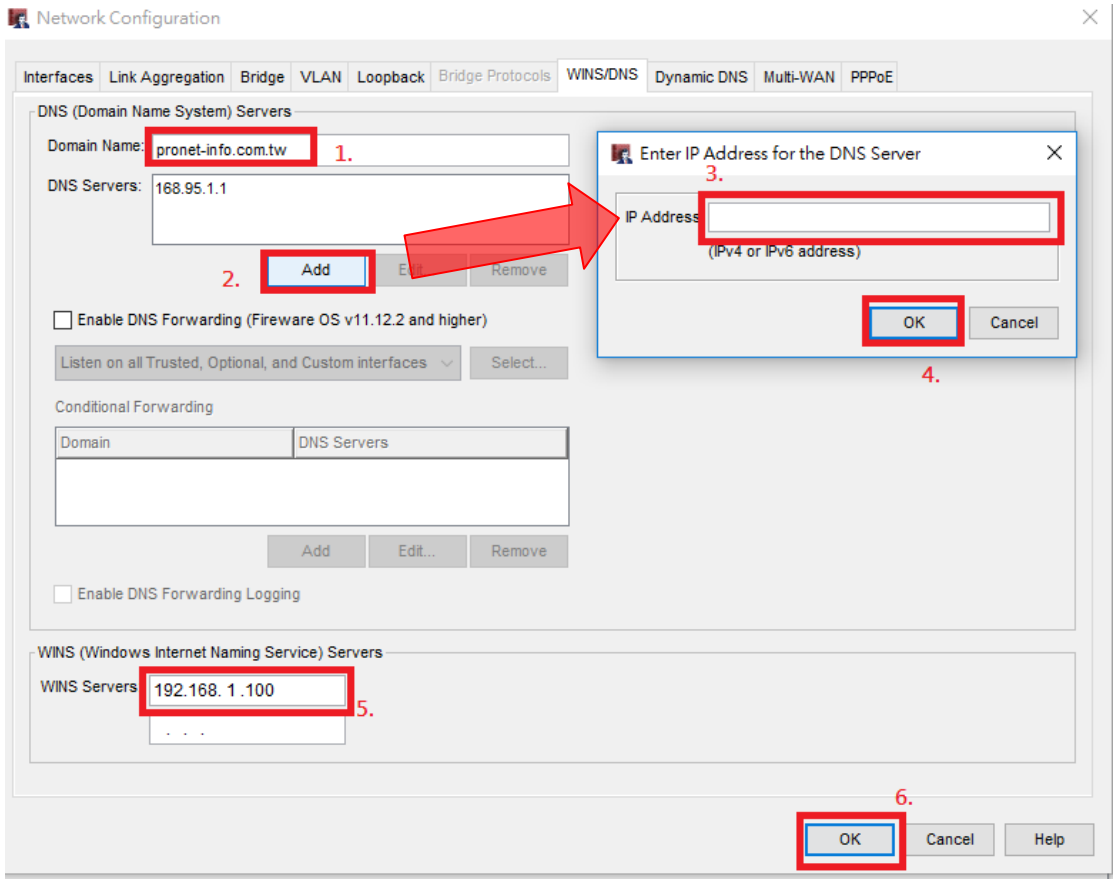
Static Route設定確認



1. 確認Static Route設定
2. 點選OK

DNS Server 設定

Firewall DNS 、WINS設定

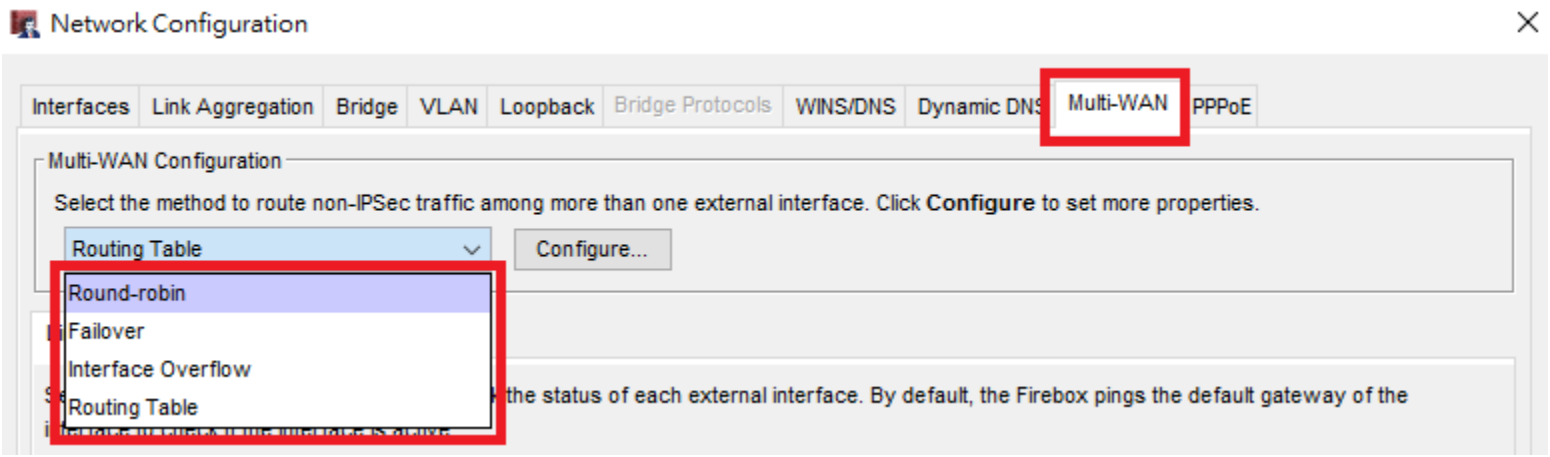


防火牆必需設定DNS特徵碼才可進行更新

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

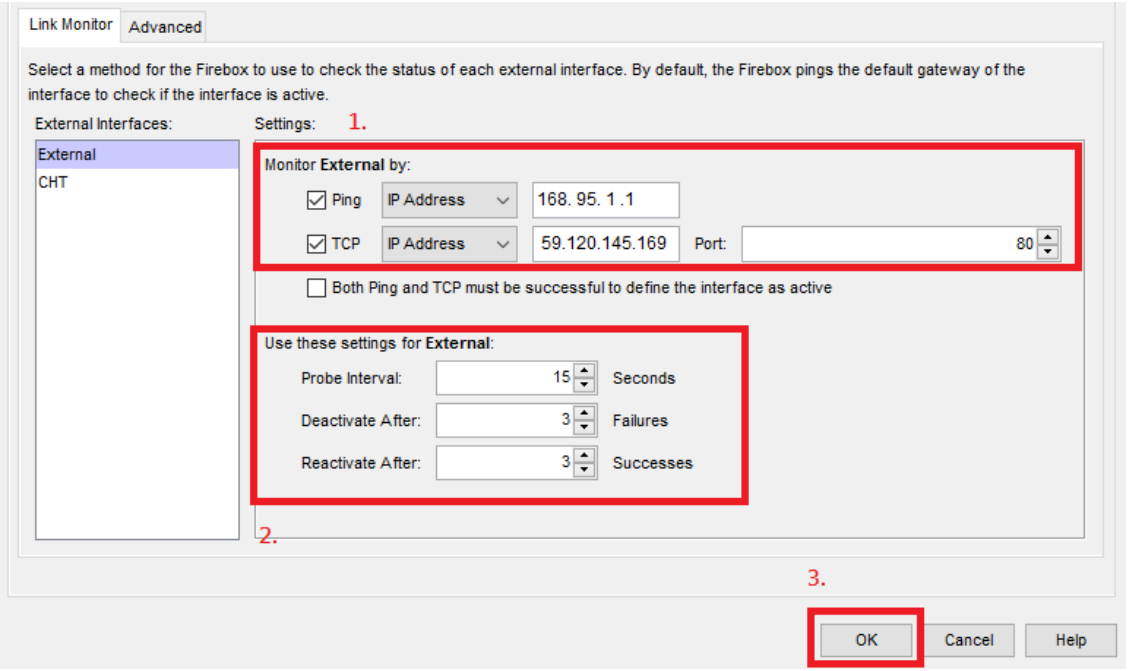
Muti-WAN設定



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

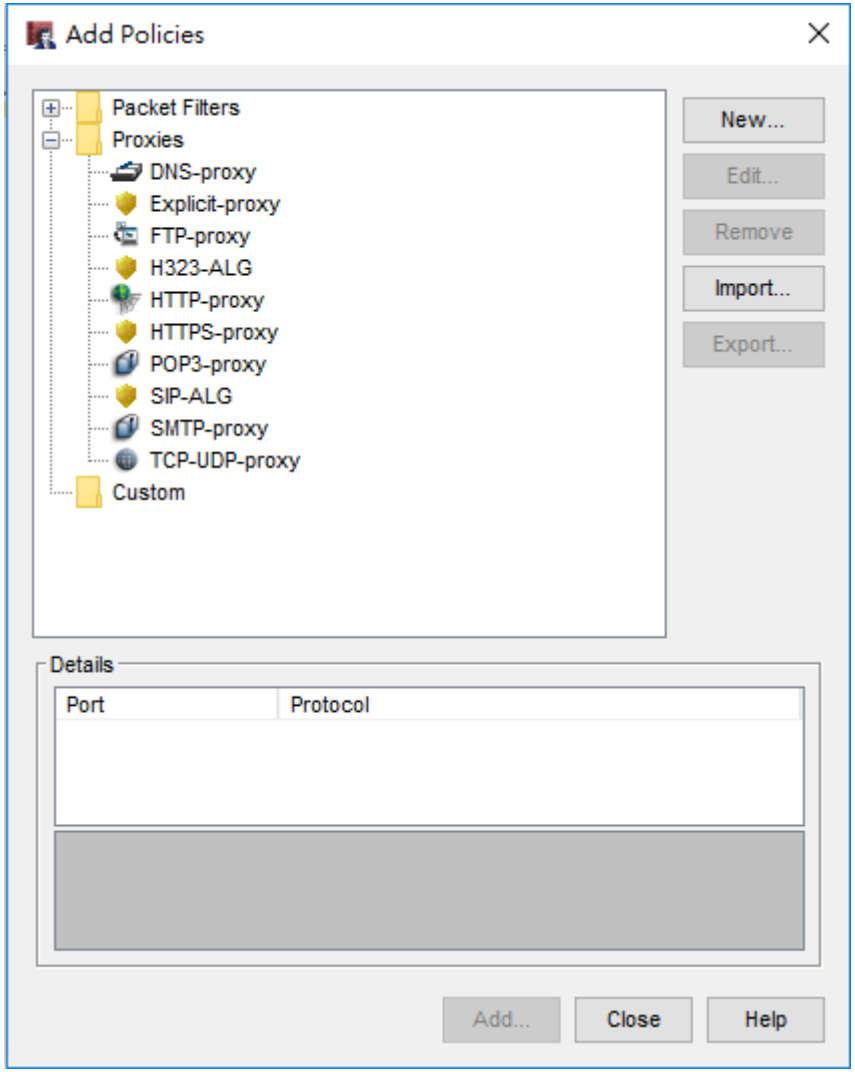
   每15秒測試一次

   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

Policy 設定

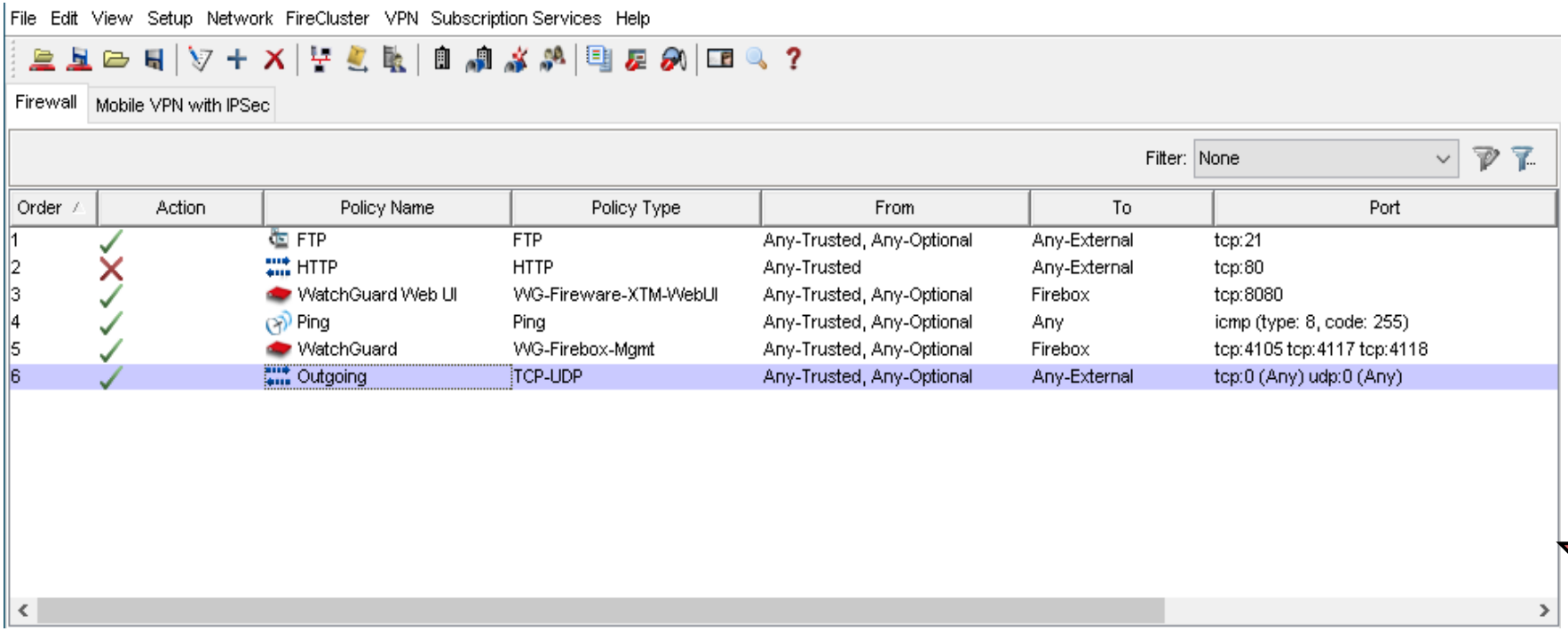
WatchGuard Policy種類



WatchGuard Policy分為下列三種

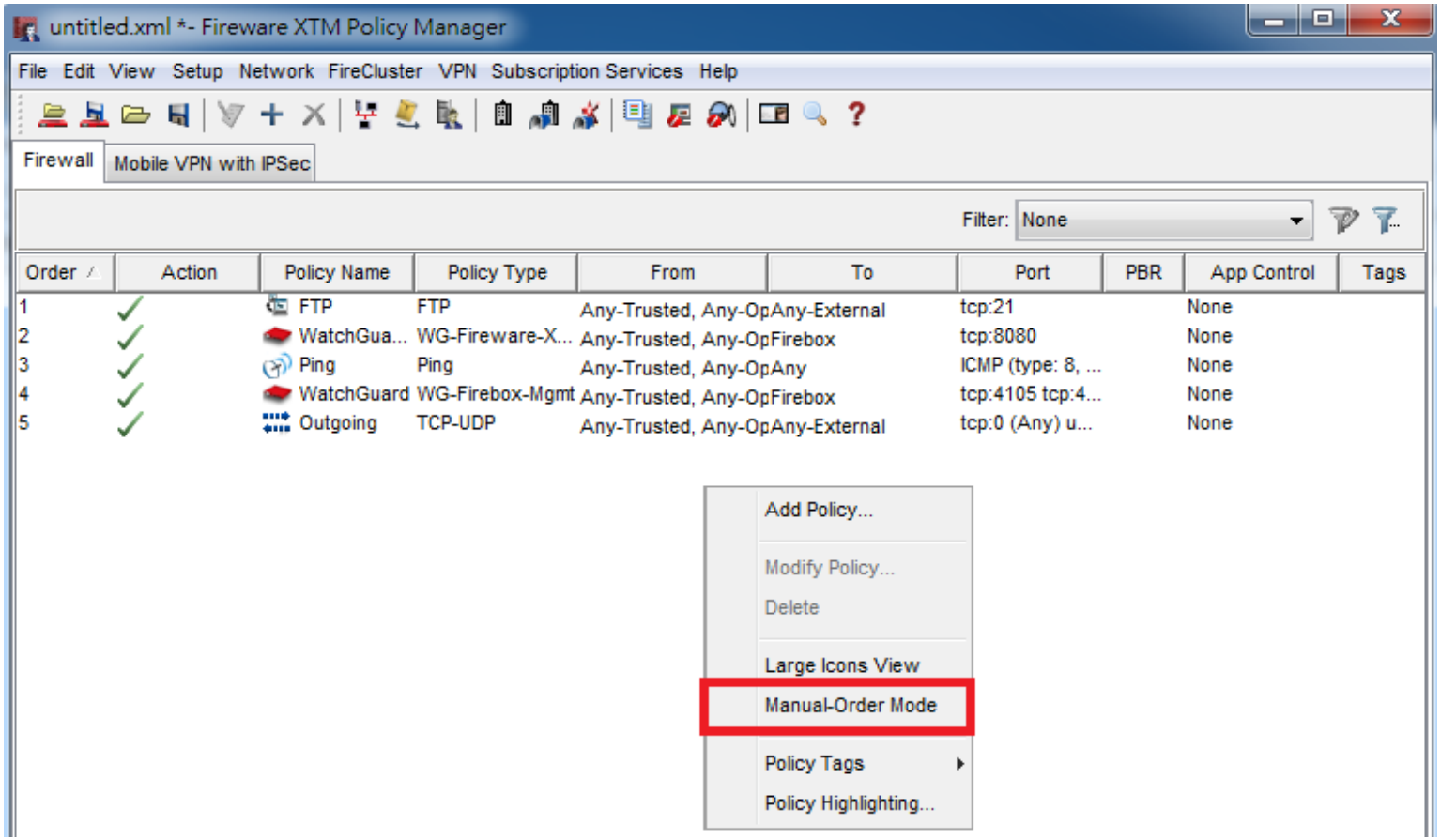
1. **Packet Filters** – WatchGuard已建立好多種常用的Service，使用者可依據需求找到要設定的服務。
2. **Proxies** – Proxy Policy可設定內容過濾，包含閘道防毒以及網頁過濾需要使用Proxy Policy進行設定。
3. **Custom** – 可自行建立要設定的Port或是服務群組。

WatchGuard Policy 特性



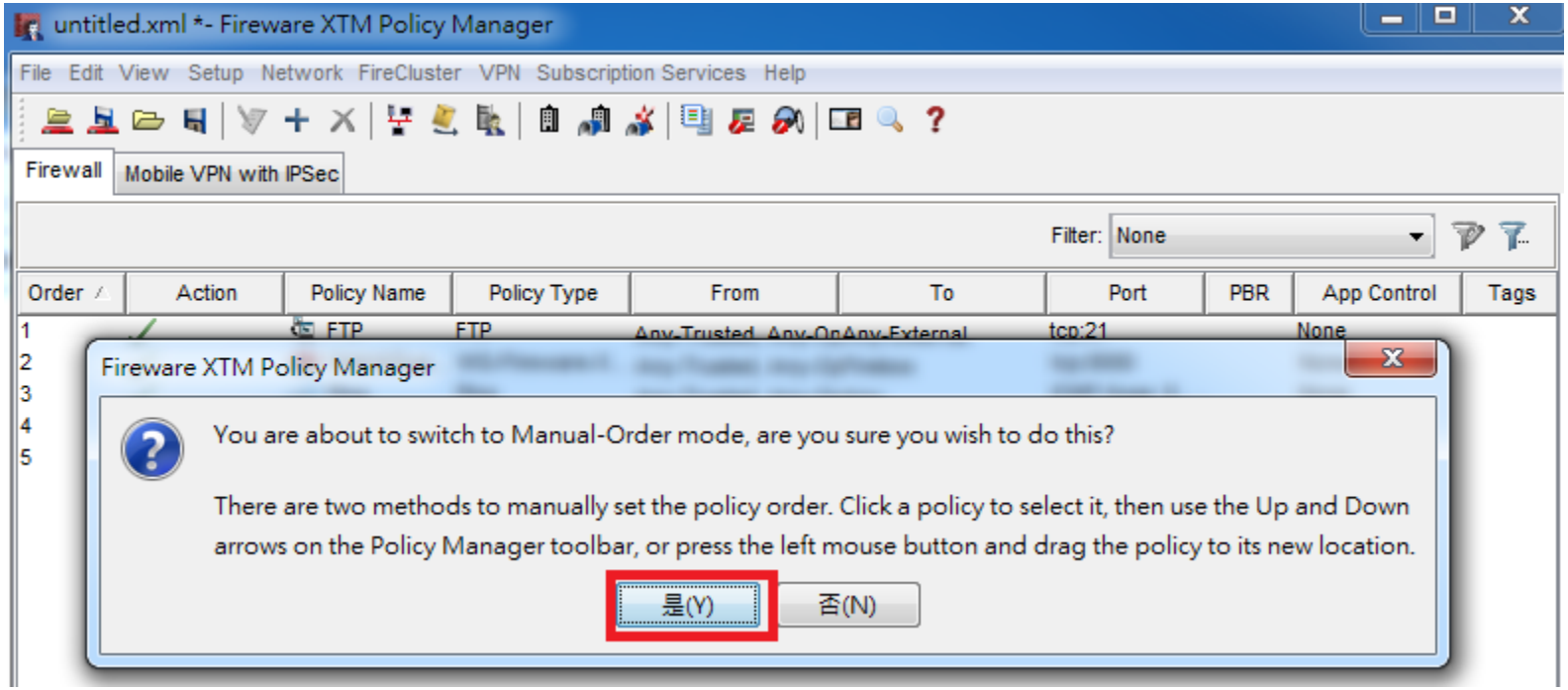
*WatchGuard Firewall 會依據order 數字順序進行作用

Policy Manual Order Mode



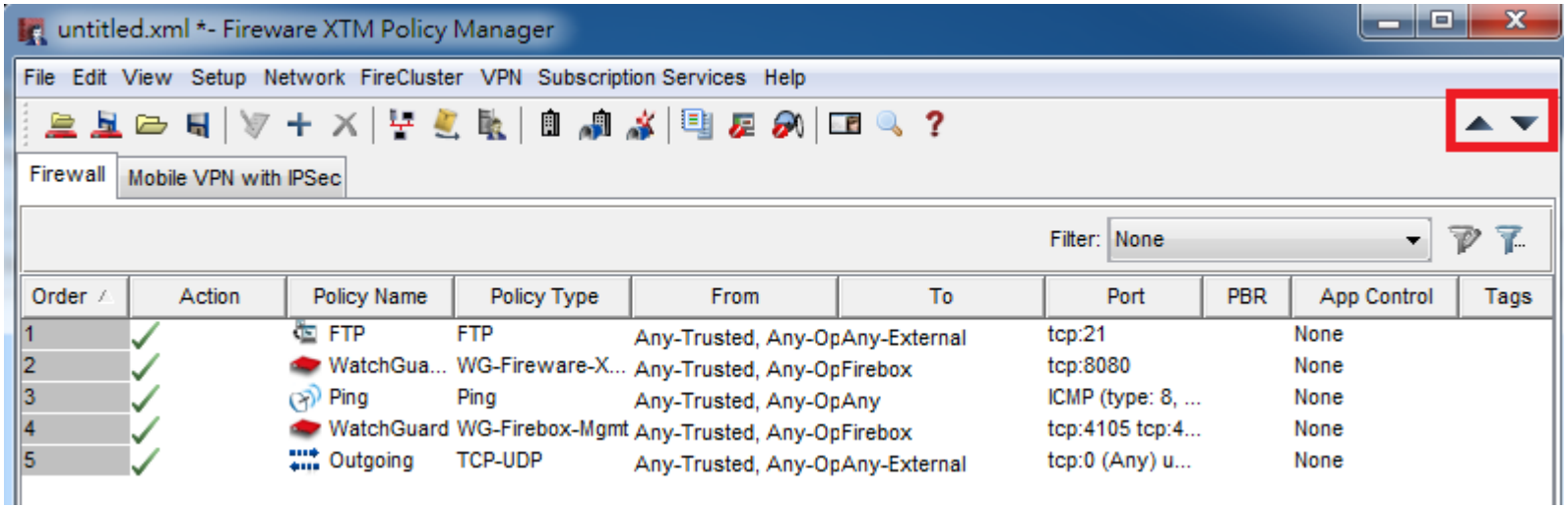
Step 1 : WatchGuard Policy預設會自動設定Policy順序，必須先調整成手動排序，在空白處按右鍵點選“Manual-Order Mode”

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”。

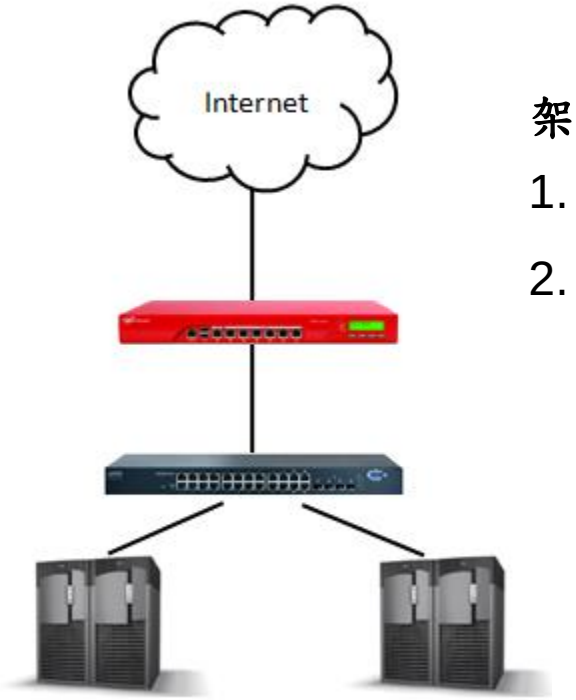
Policy Manual Order Mode 設定完成



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

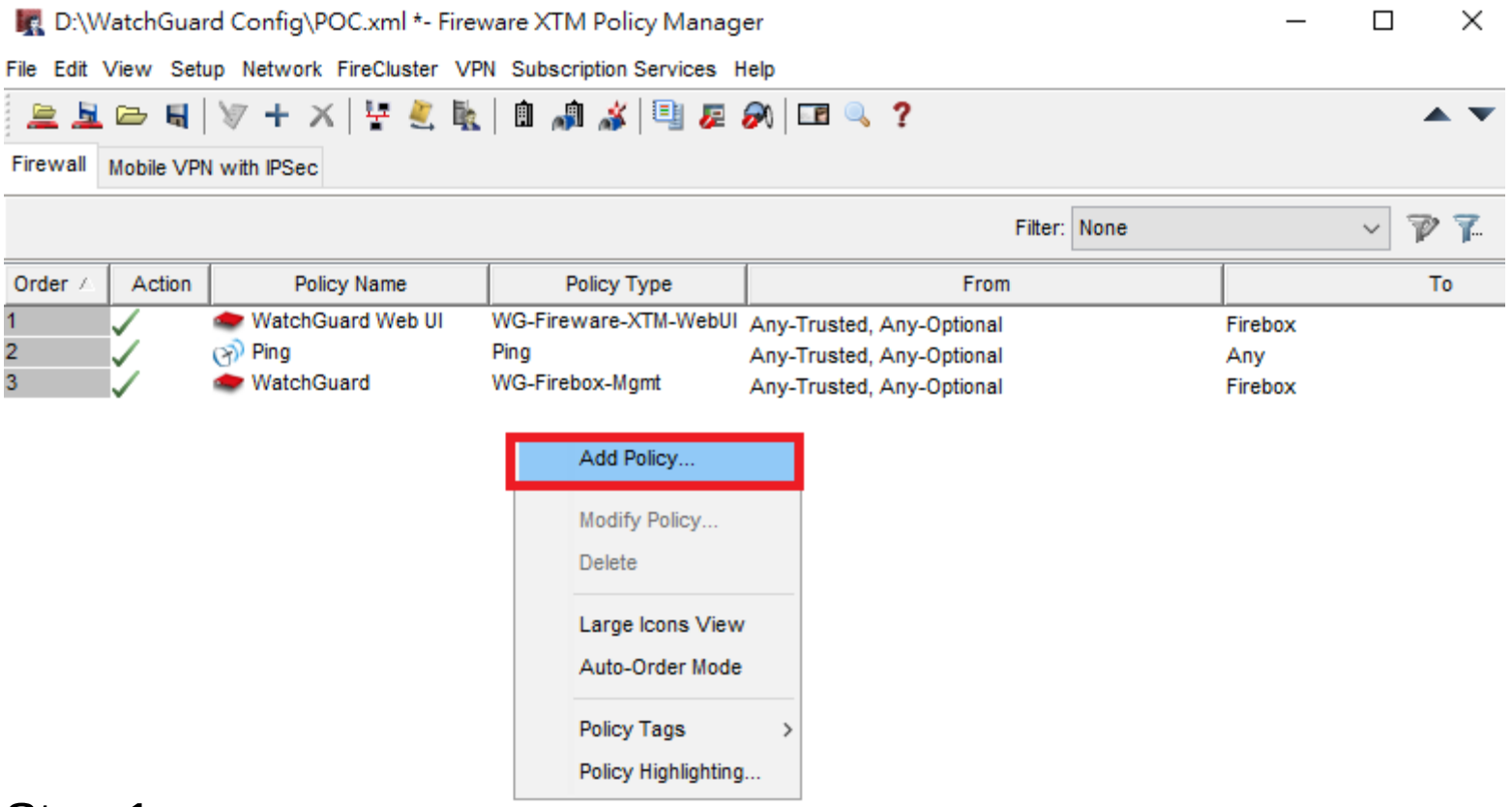
原則範例情境一



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

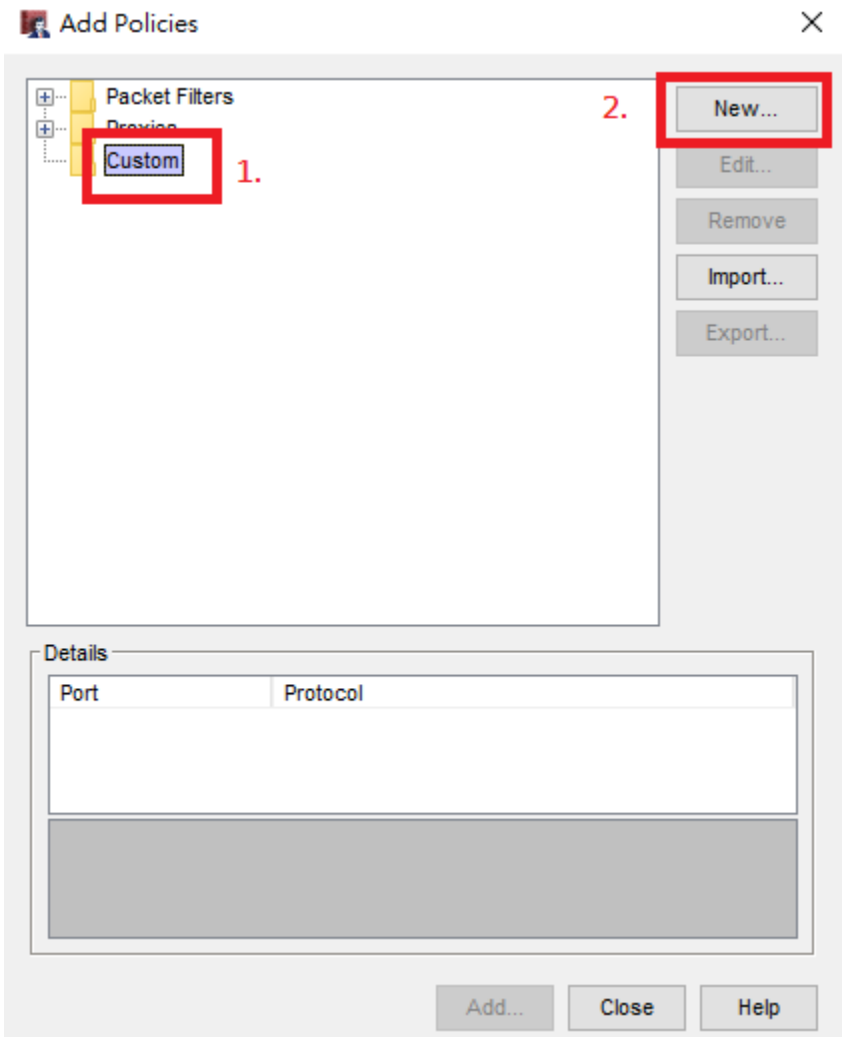
設定Service Group



Step 1 :

Policy Manager空白處按右鍵點選Add Policy

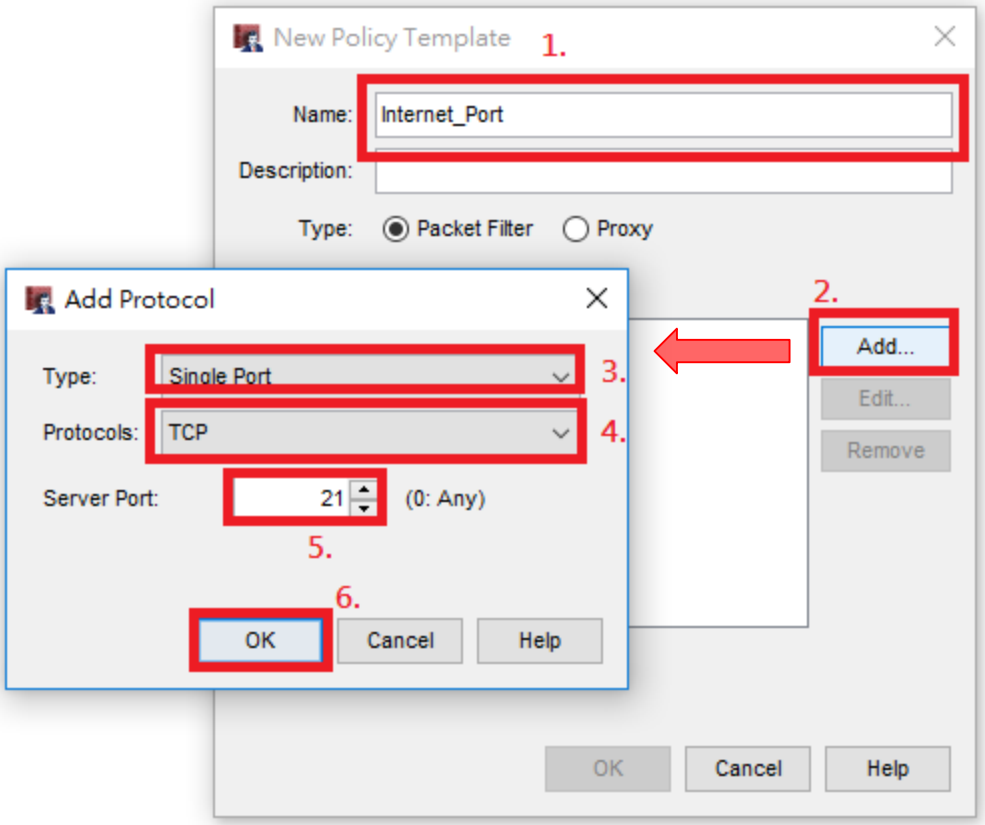
設定Service Group



Step 2 :

1. 點選Custom
2. 點選New

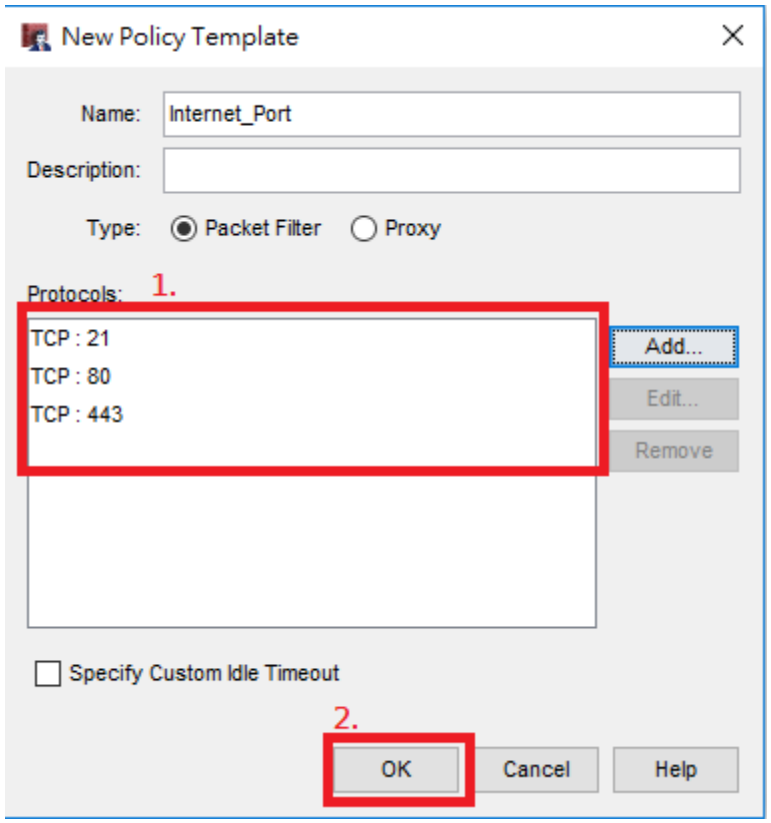
設定Service Group



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

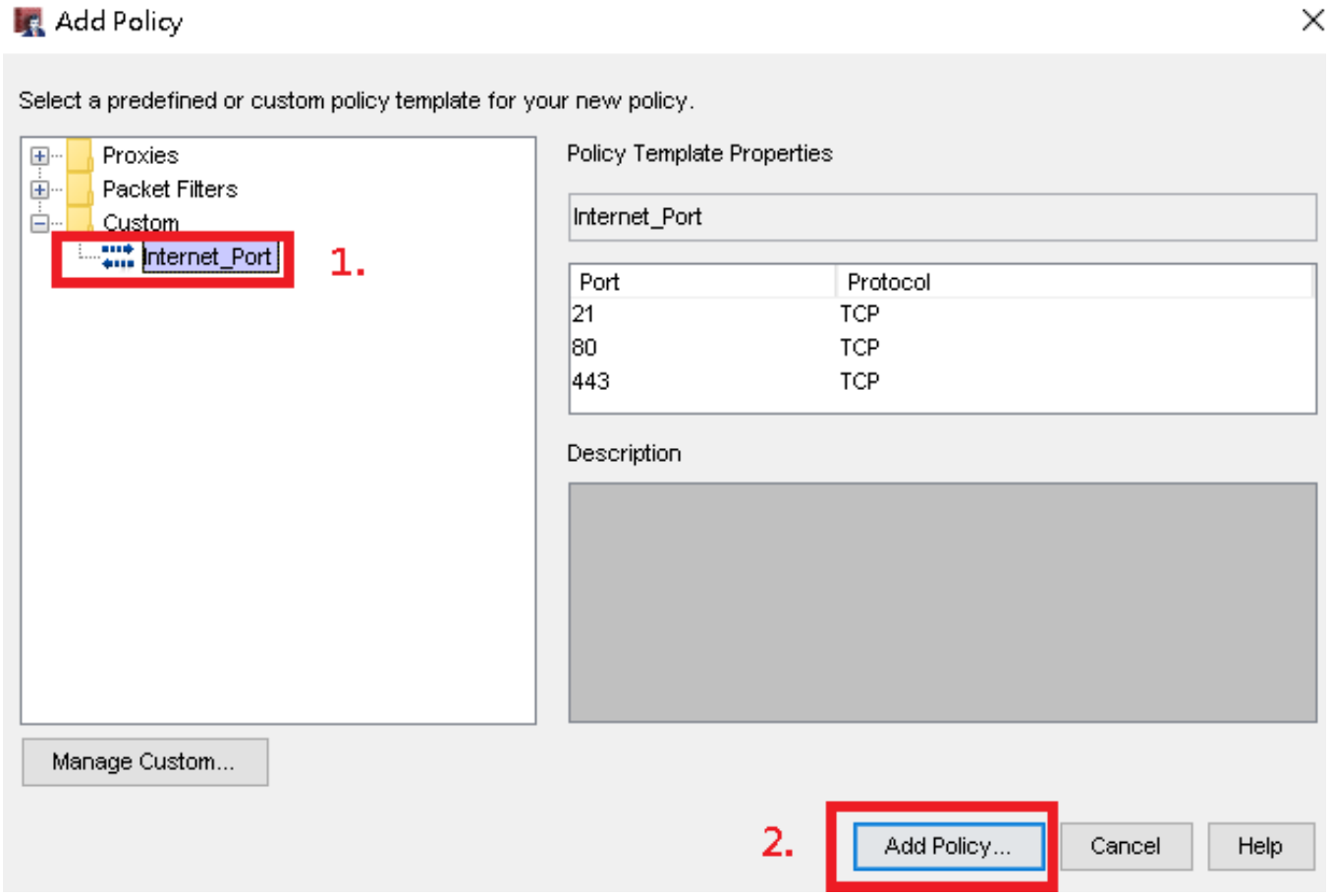
設定Service Group



Step 4 :

1. 確認要控制的Port輸入完成
2. 點選OK

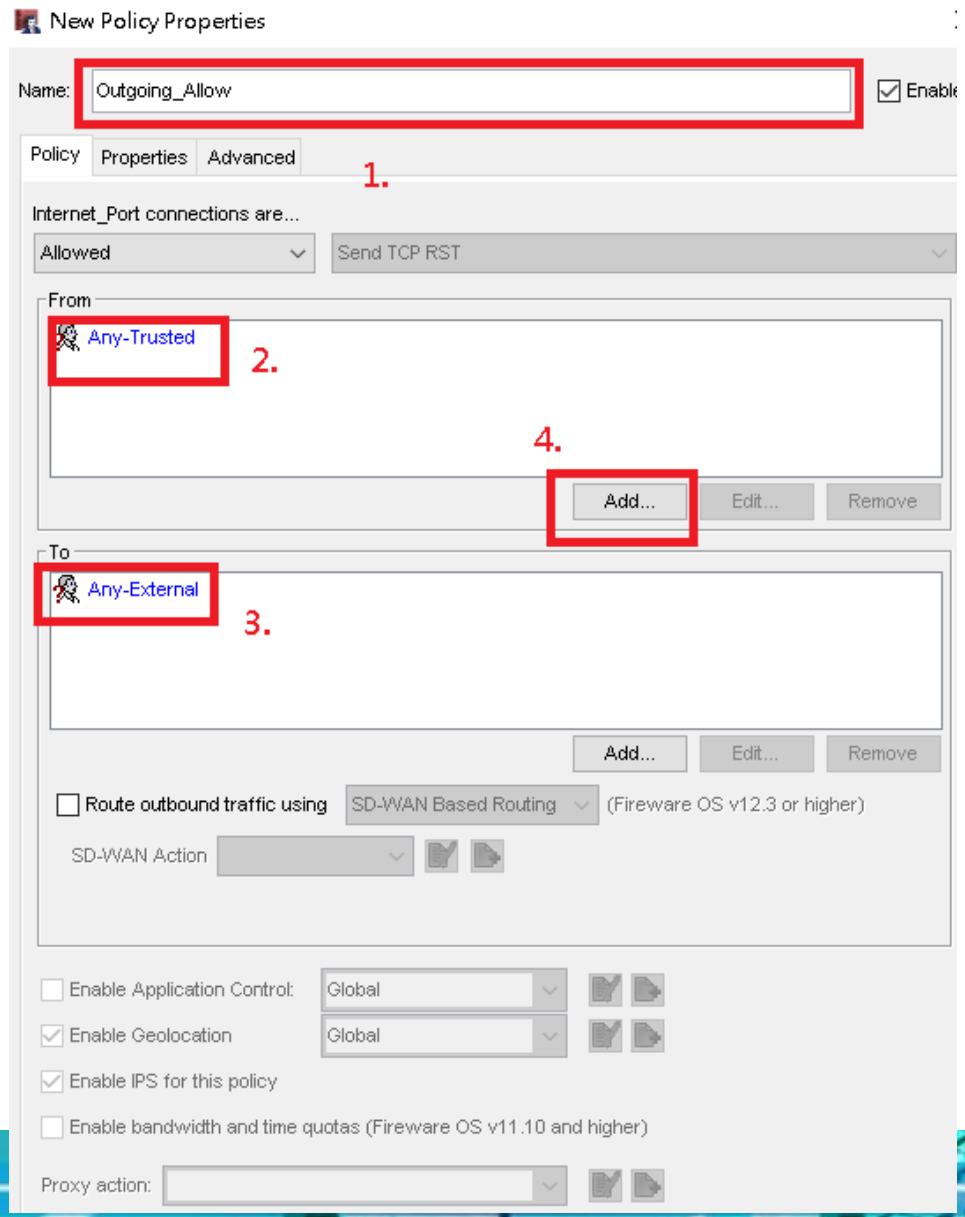
新增Policy



Step 1 :

1. 點選先前所新增的Custom Port
2. 點選下方Add

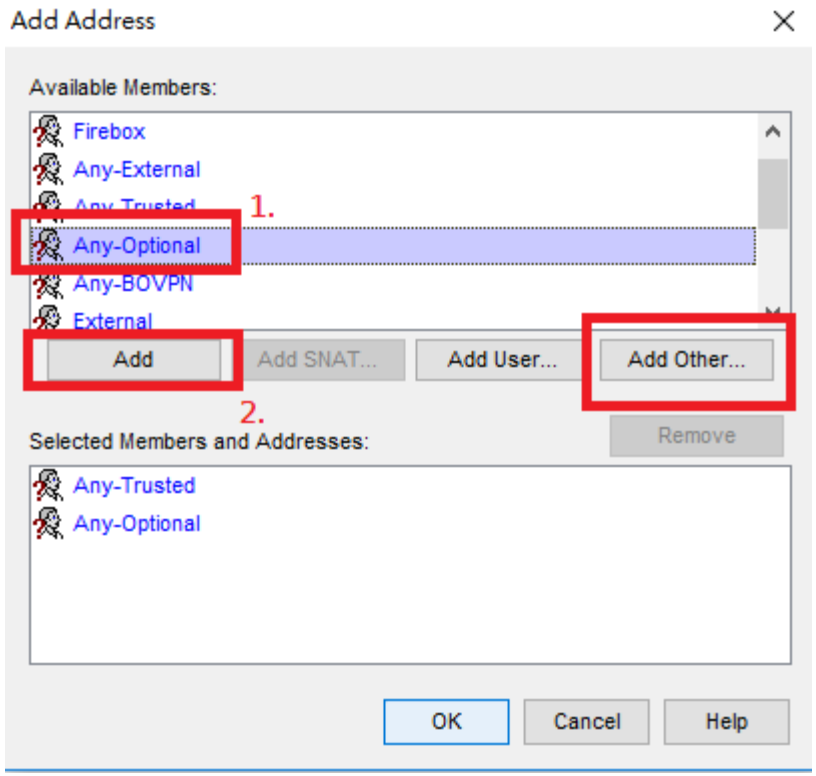
新增Policy



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



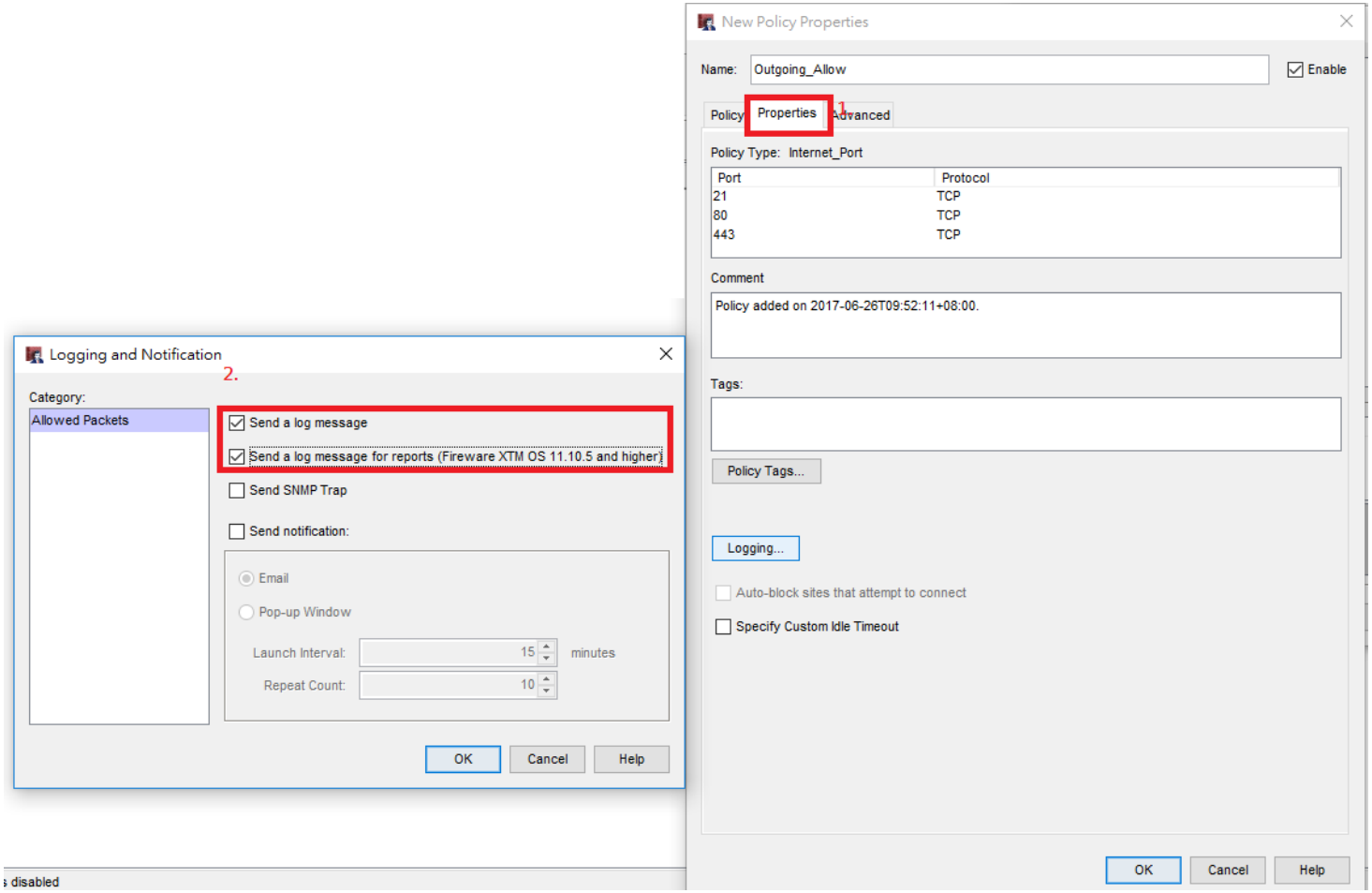
Step 3 :

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

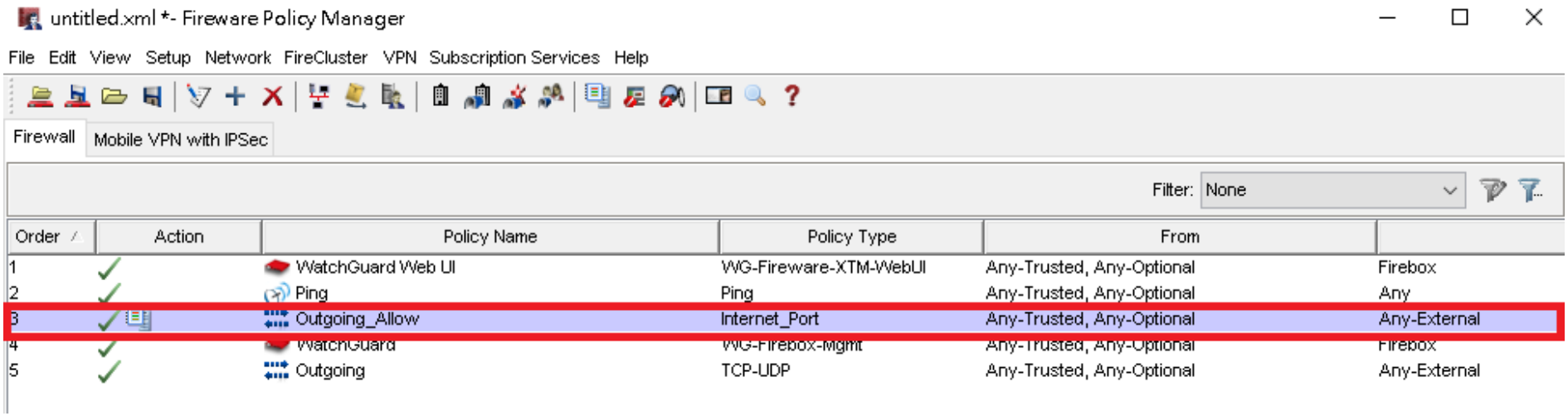
如需要加入其他型態的來源時，點選Add Other來選擇。

設定Policy Log



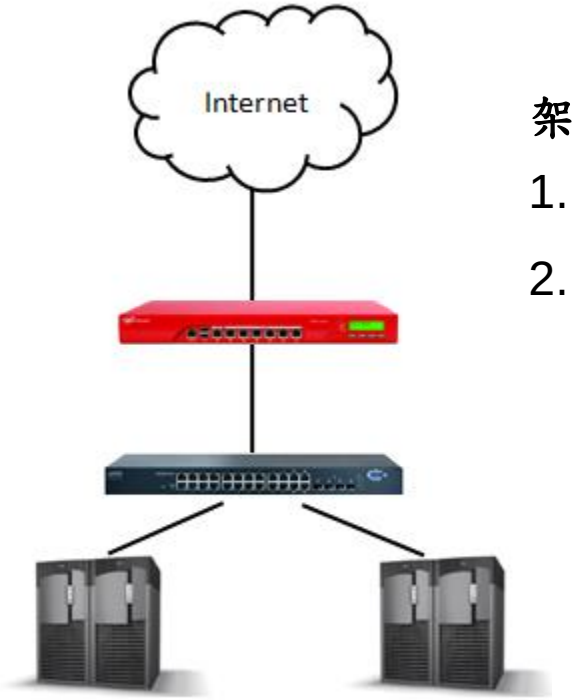
1. 點選Properties
2. 將Send a log message以及Send log message for report

確認Policy設定



Policy設定完成後顯示於Policy Manager

原則範例情境二

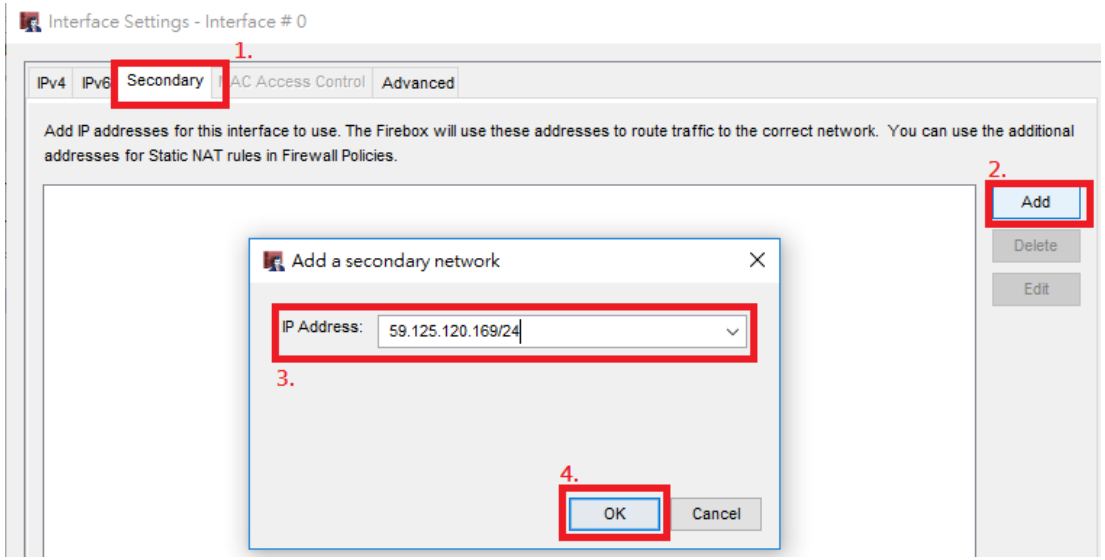


架構說明

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

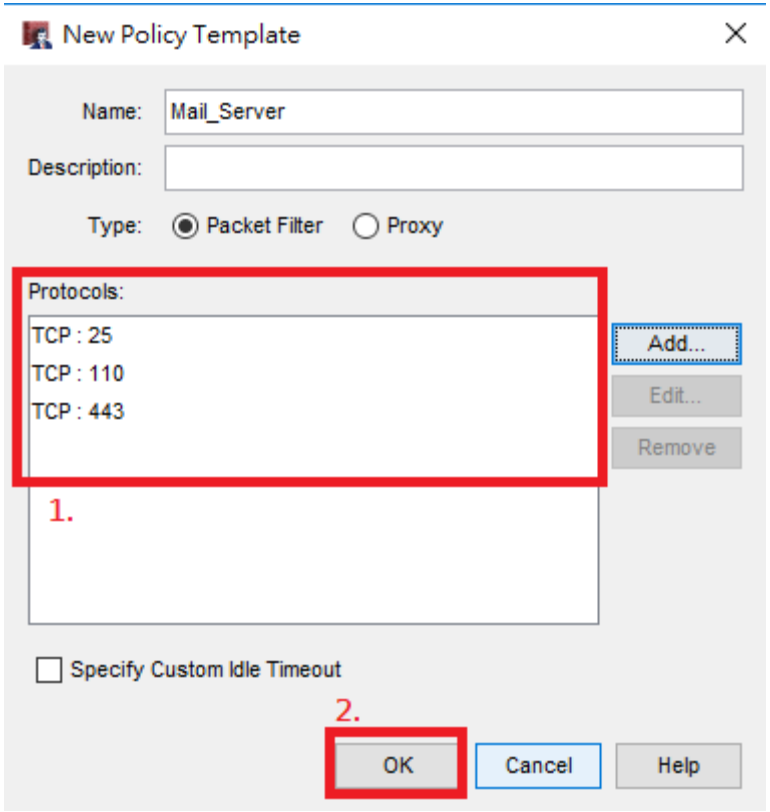
設定Secondary IP Address



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

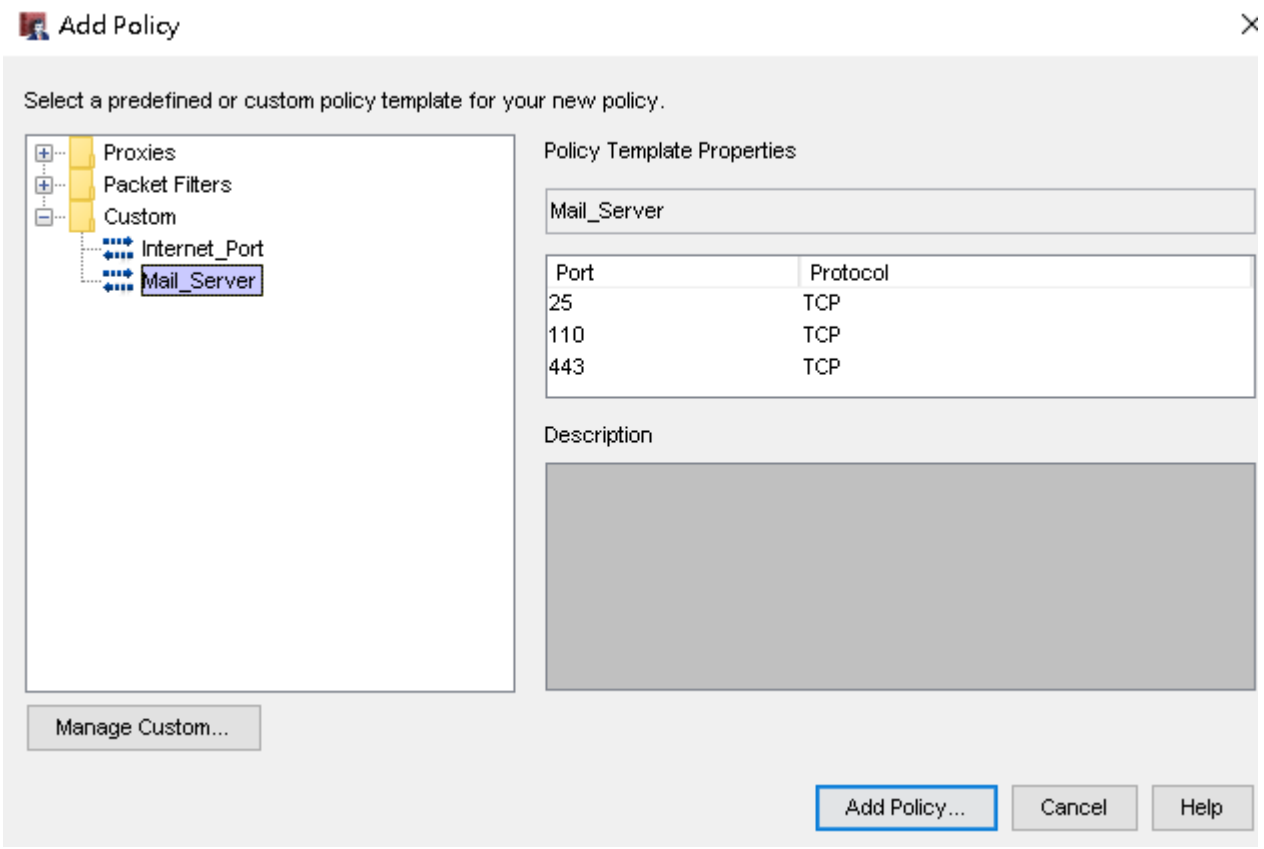
Note：要開放對外服務的IP必須事先設定好External Secondary IP Address

新增Service Group



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

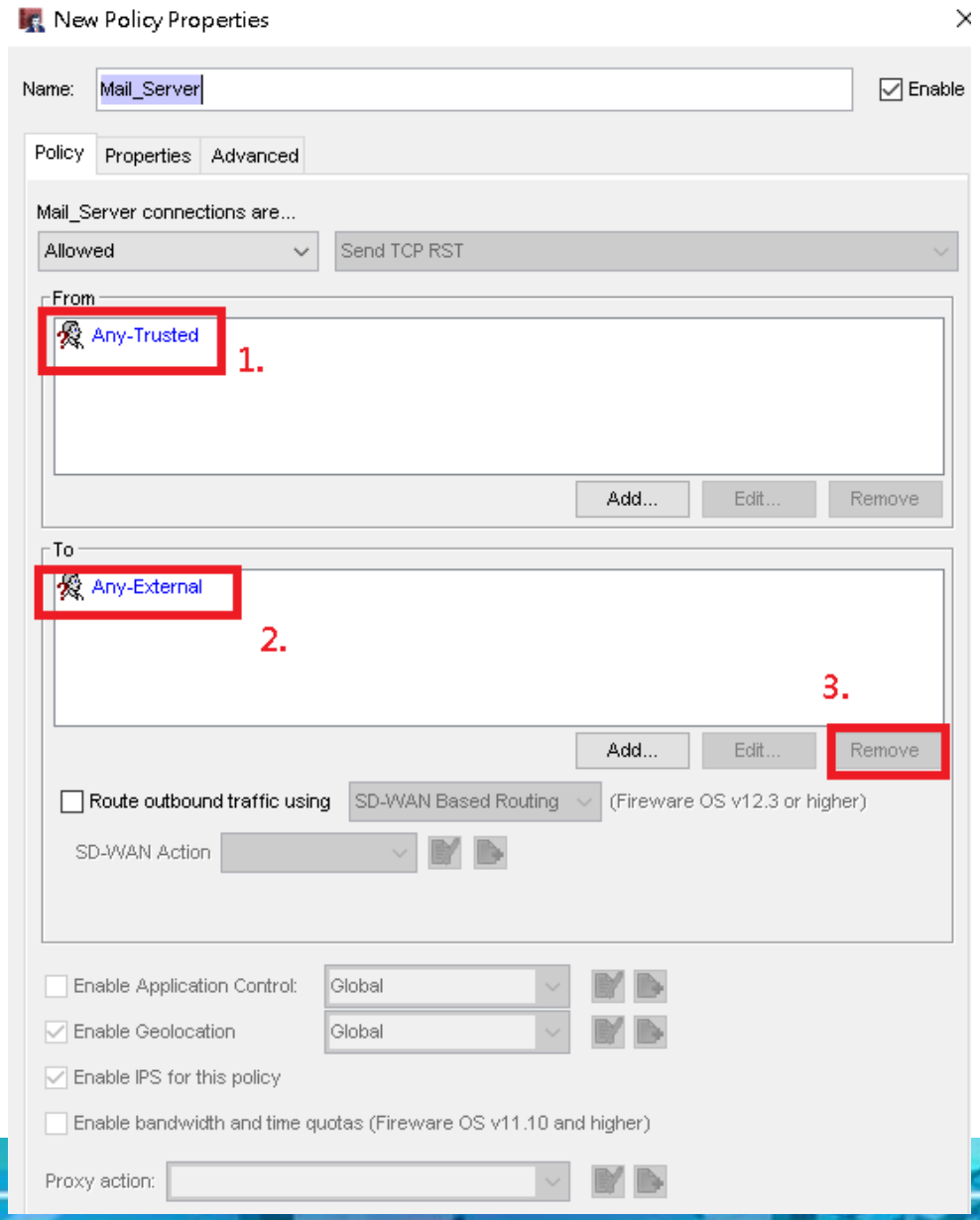
新增對外服務Policy



Step 1 :

1. 點選新增的Service Group
2. 點選Add

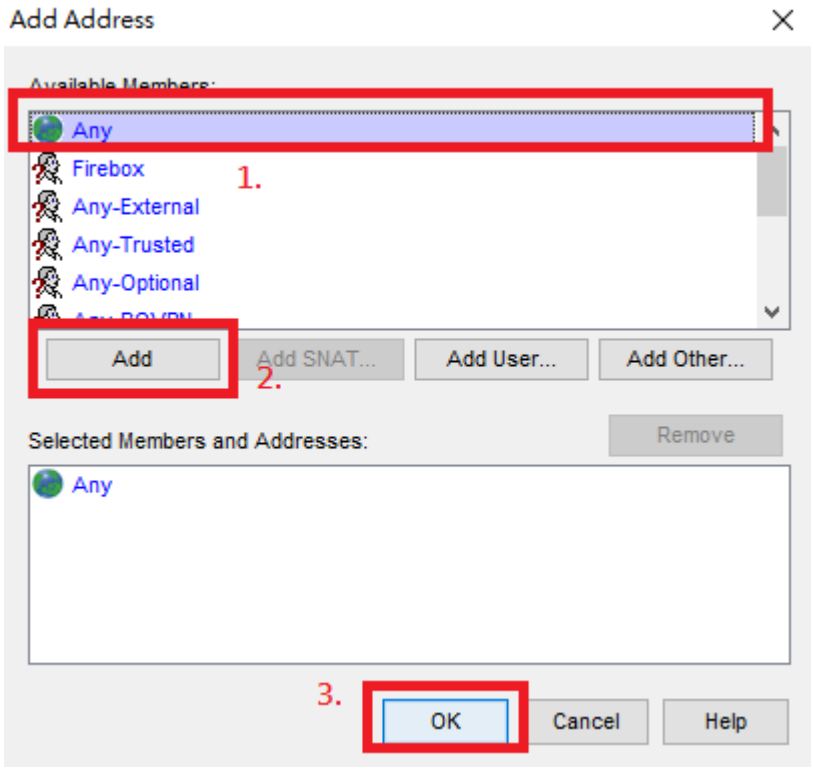
新增對外服務Policy



Step 2 :

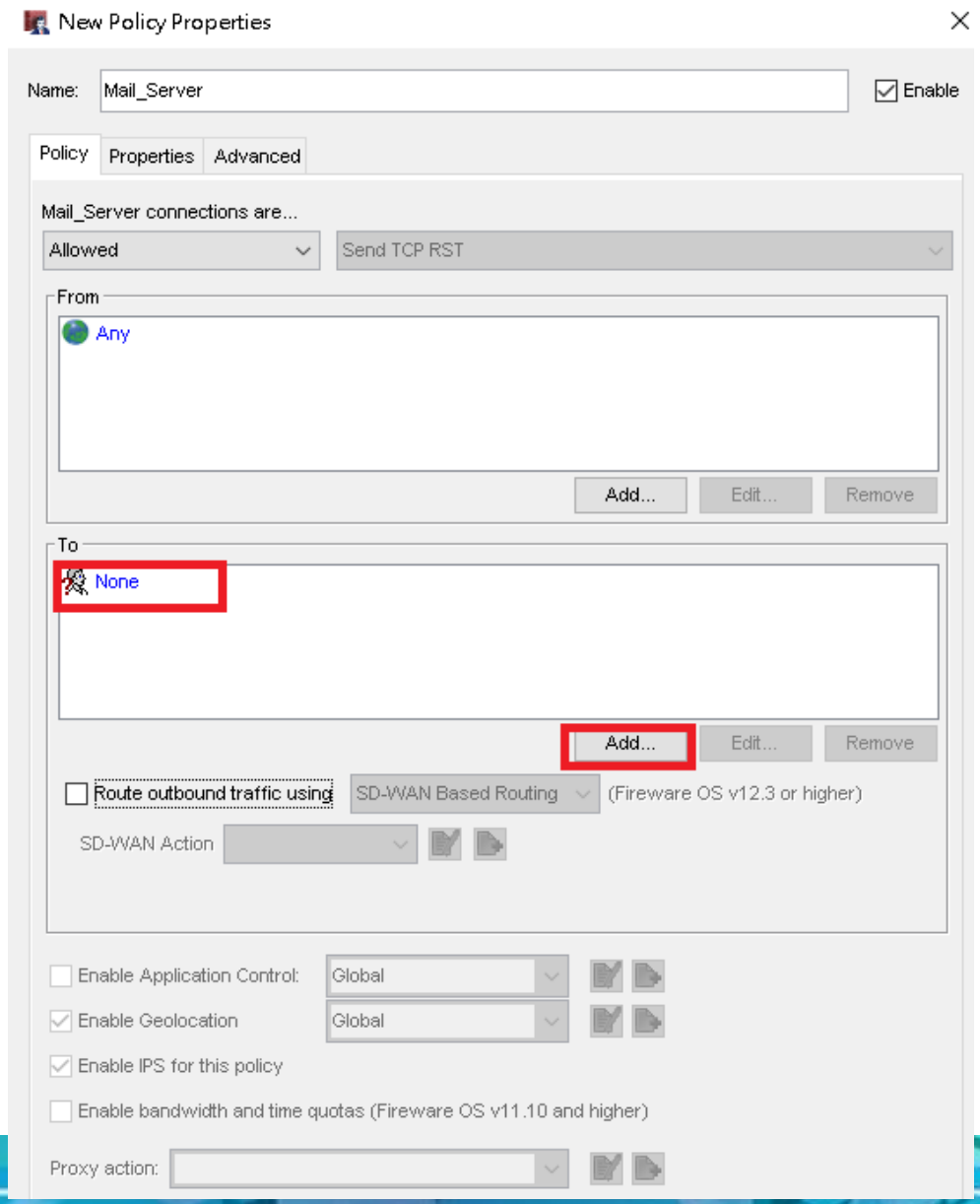
1. Name : 輸入Policy名稱
2. 點選Any-External
3. 點選Remove
4. 點選From欄位下方Add

選擇來源位置



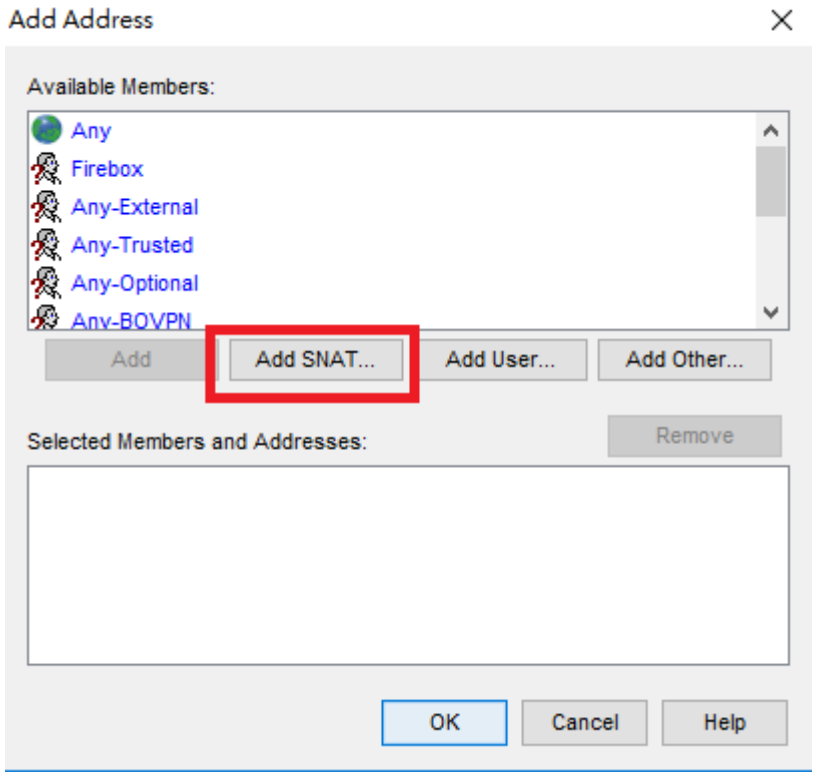
1. 此要開起對外服務的Policy，來源位置選擇Any
2. 點選Add
3. 點選OK

設定SNAT



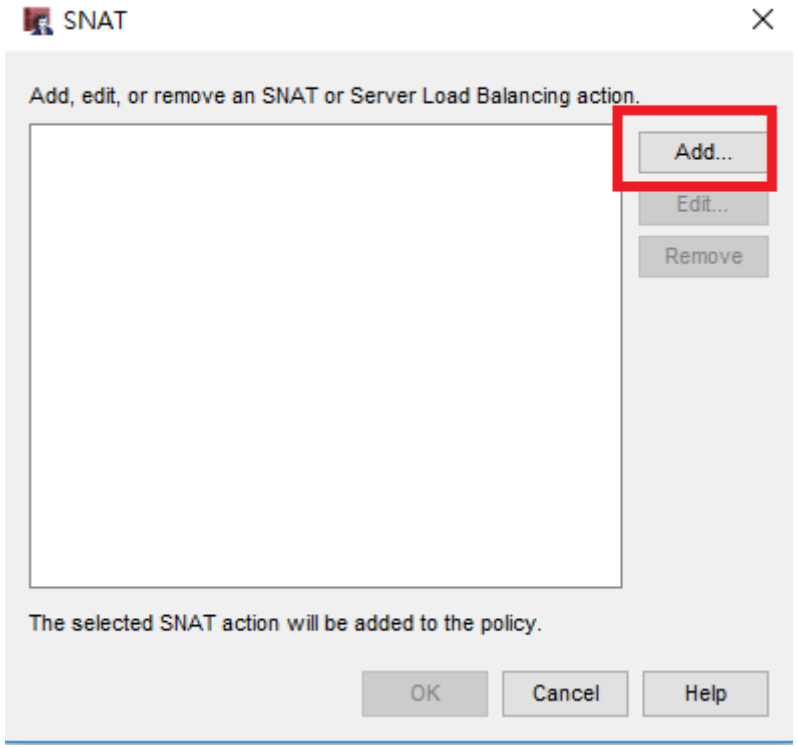
點選To欄位下方Add

設定SNAT



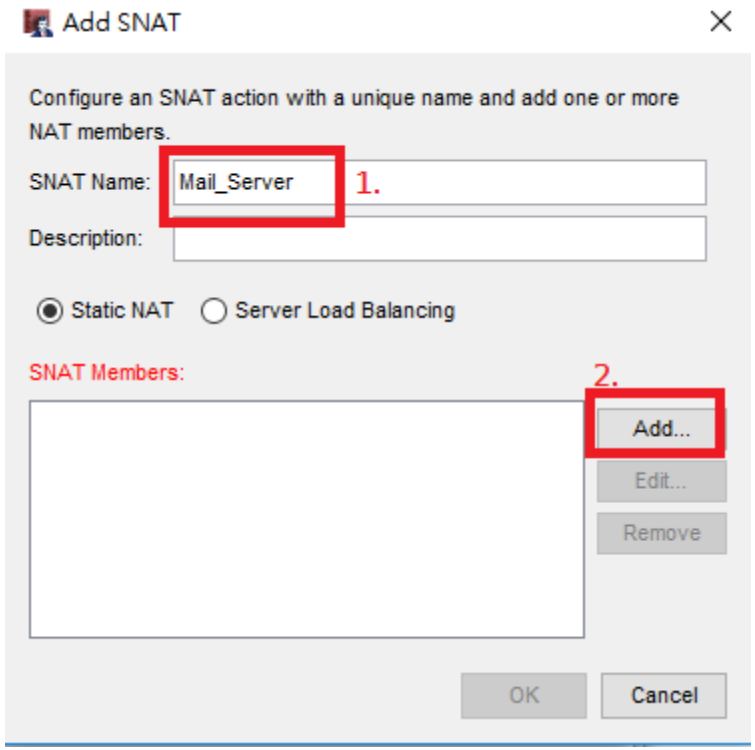
點選Add SNAT

設定SNAT



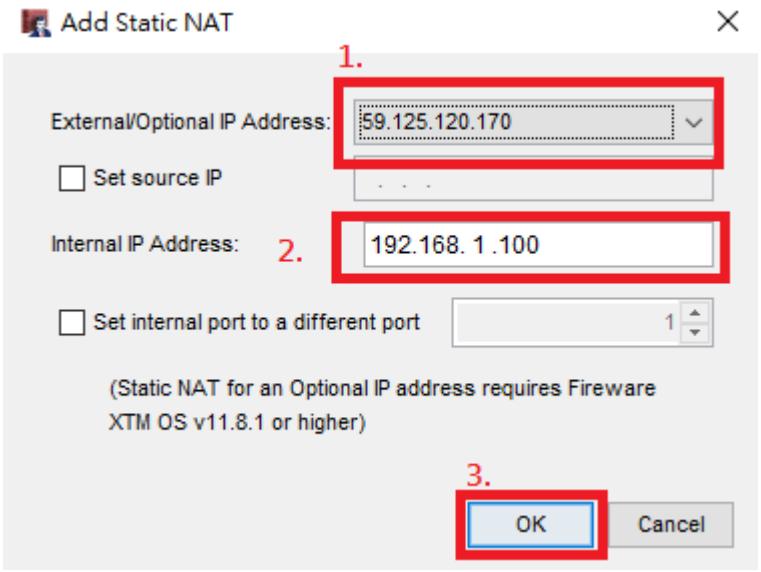
SNAT視窗點選Add

設定SNAT



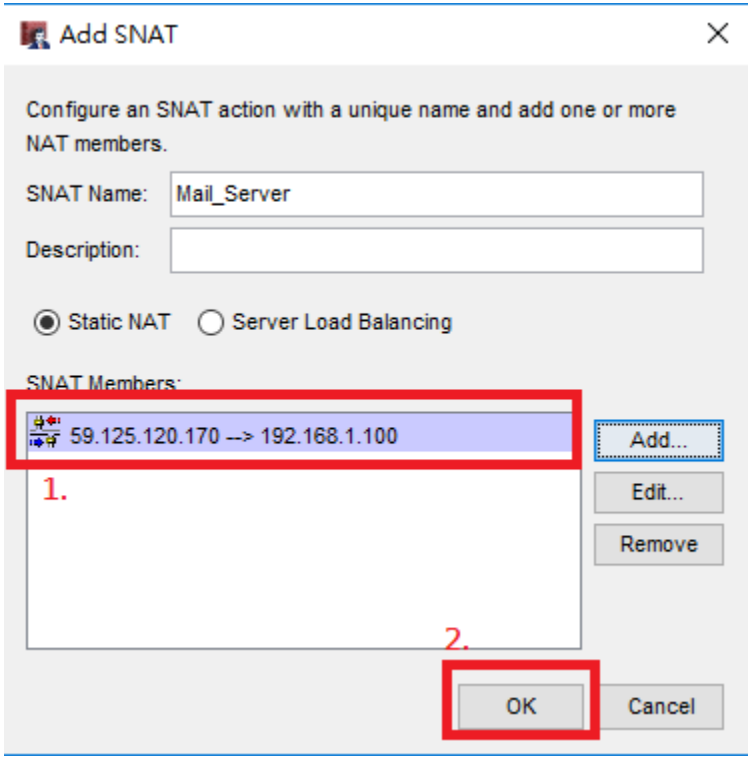
1. 設定SNAT名稱
2. 點選Add

設定SNAT



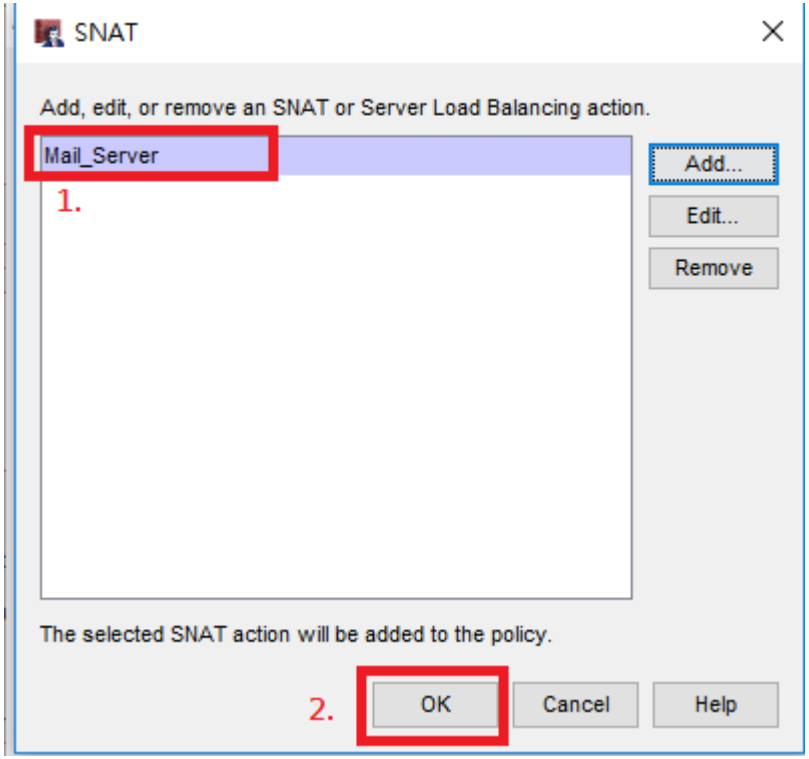
1. 於下拉式選單選擇外部IP Address
2. 輸入Server Private IP Address
3. 點選OK

確認內外部IP對應設定



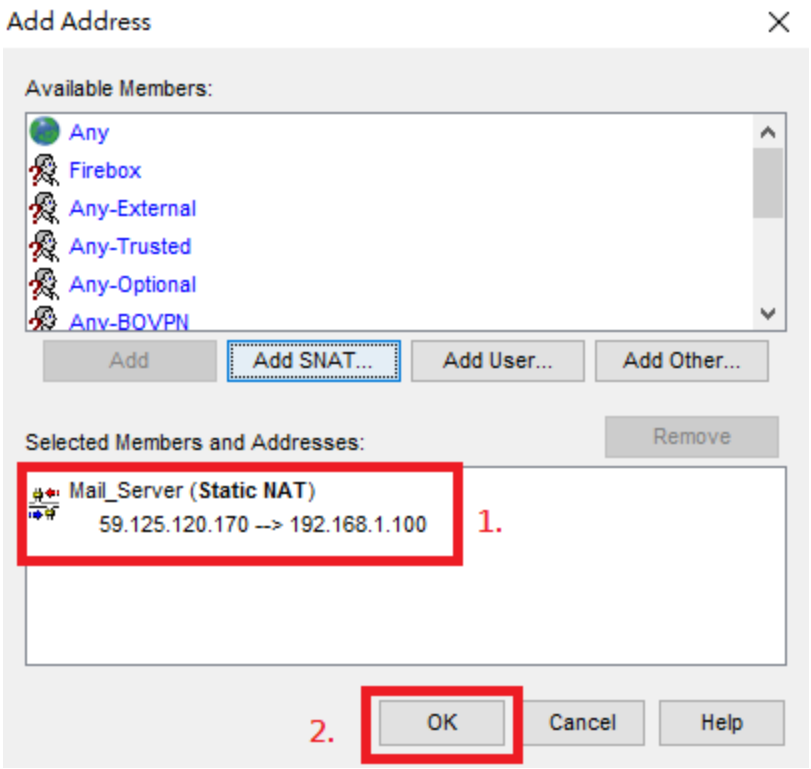
1. 確認內外部IP對應設定
2. 點選OK

完成SNAT設定



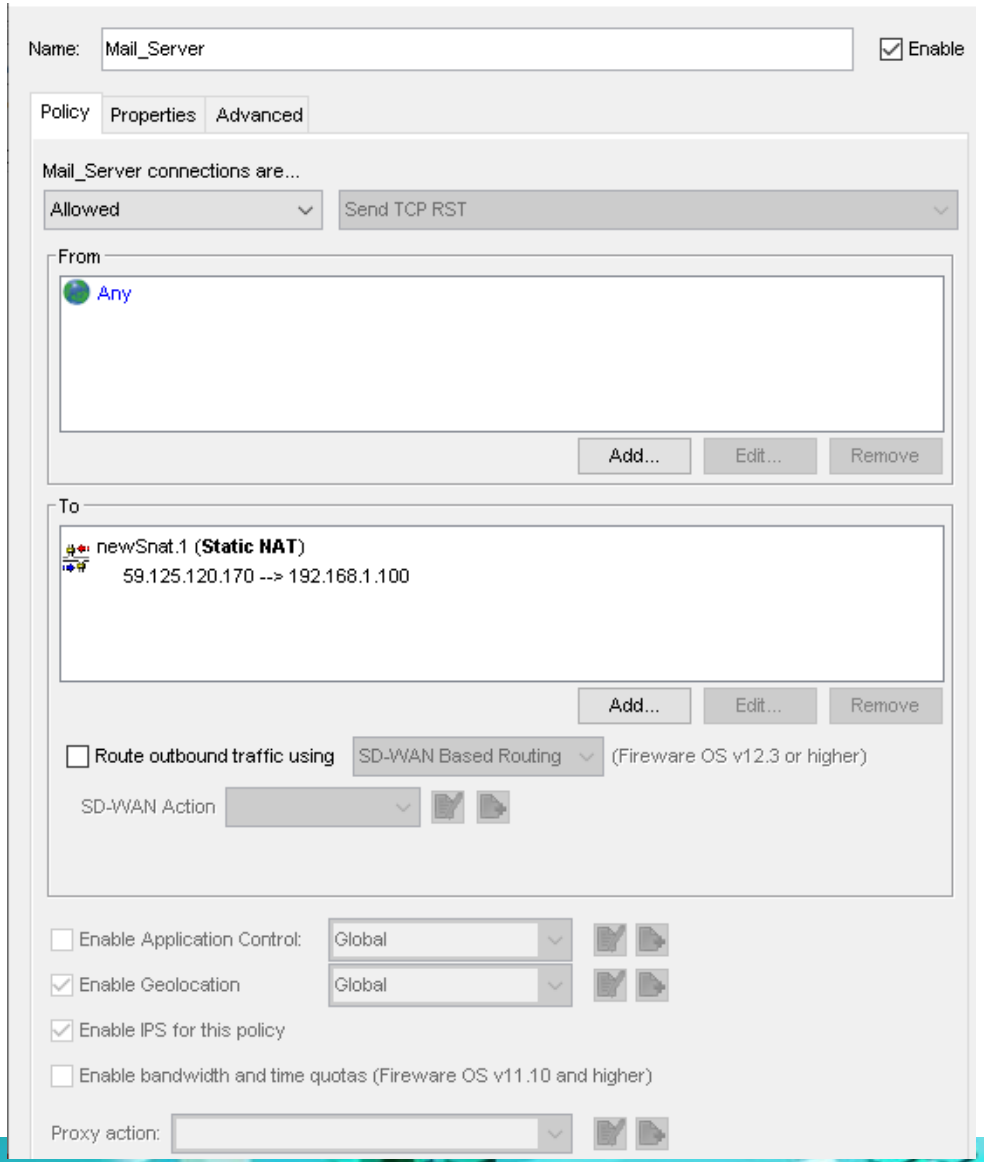
1. 確認SNAT名稱
2. 點選OK

確認目的地SNAT設定



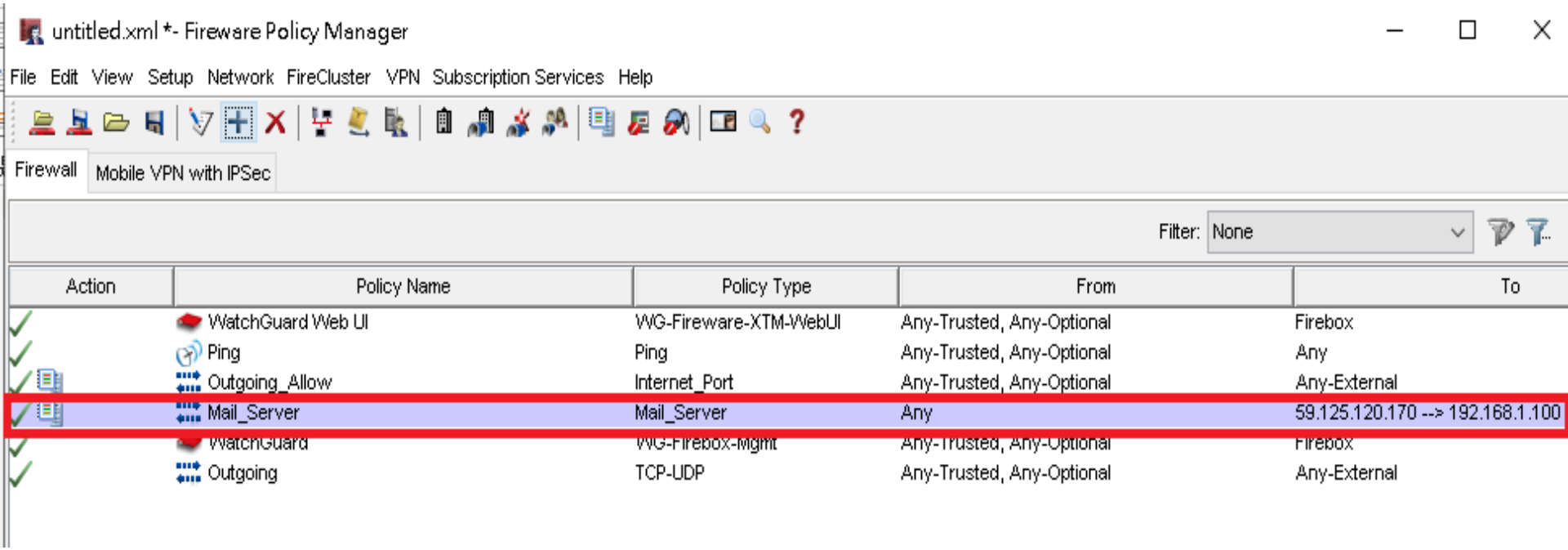
1. 確認目的地SNAT設定
2. 點選OK

完成對外服務Policy設定



1. 確認Policy設定
2. 點選OK

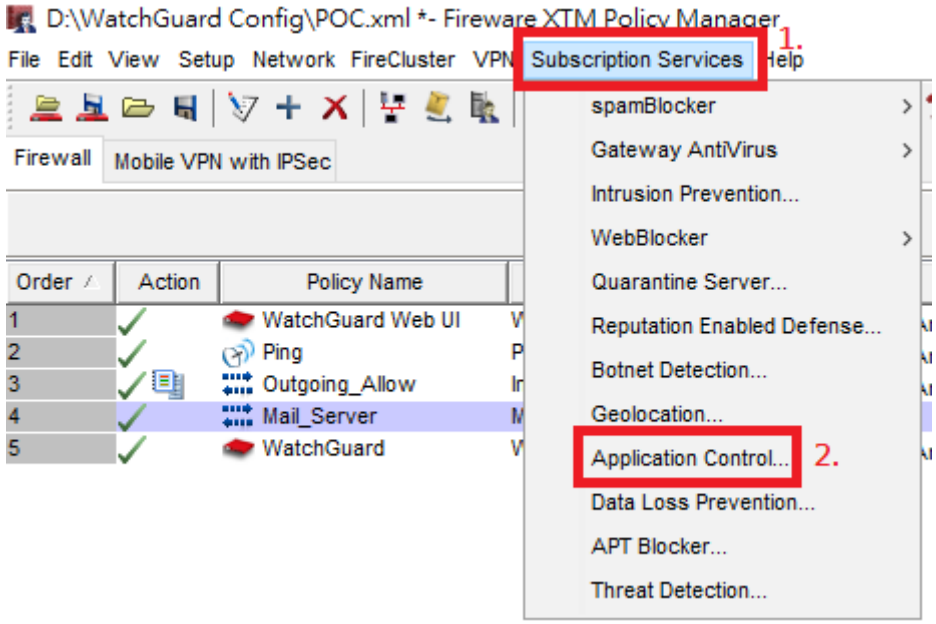
完成SNAT POLICY 畫面



UTM 設定

Application Control設定

設定Application Control

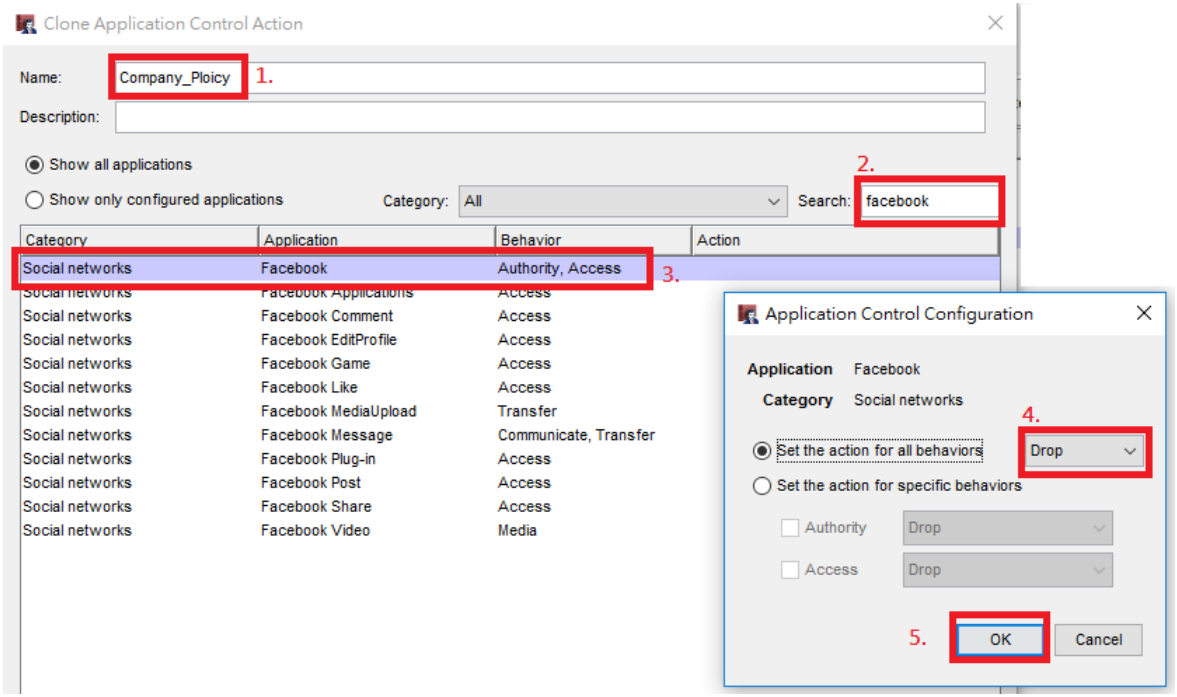


1. Subscription Service
2. 點選Application Control

複製Global Policy

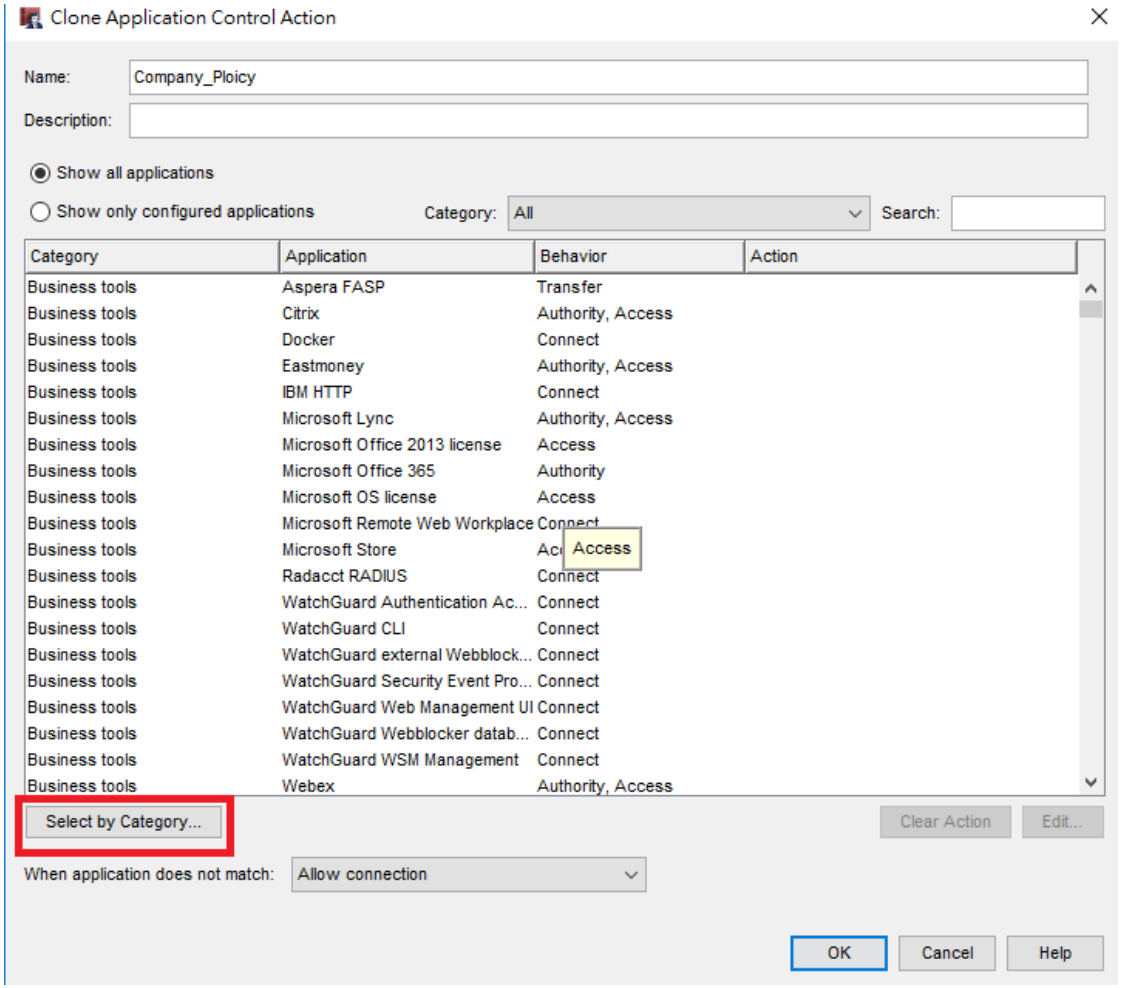
1. 點選Global
2. 點選Clone

設定要封鎖的Application Control



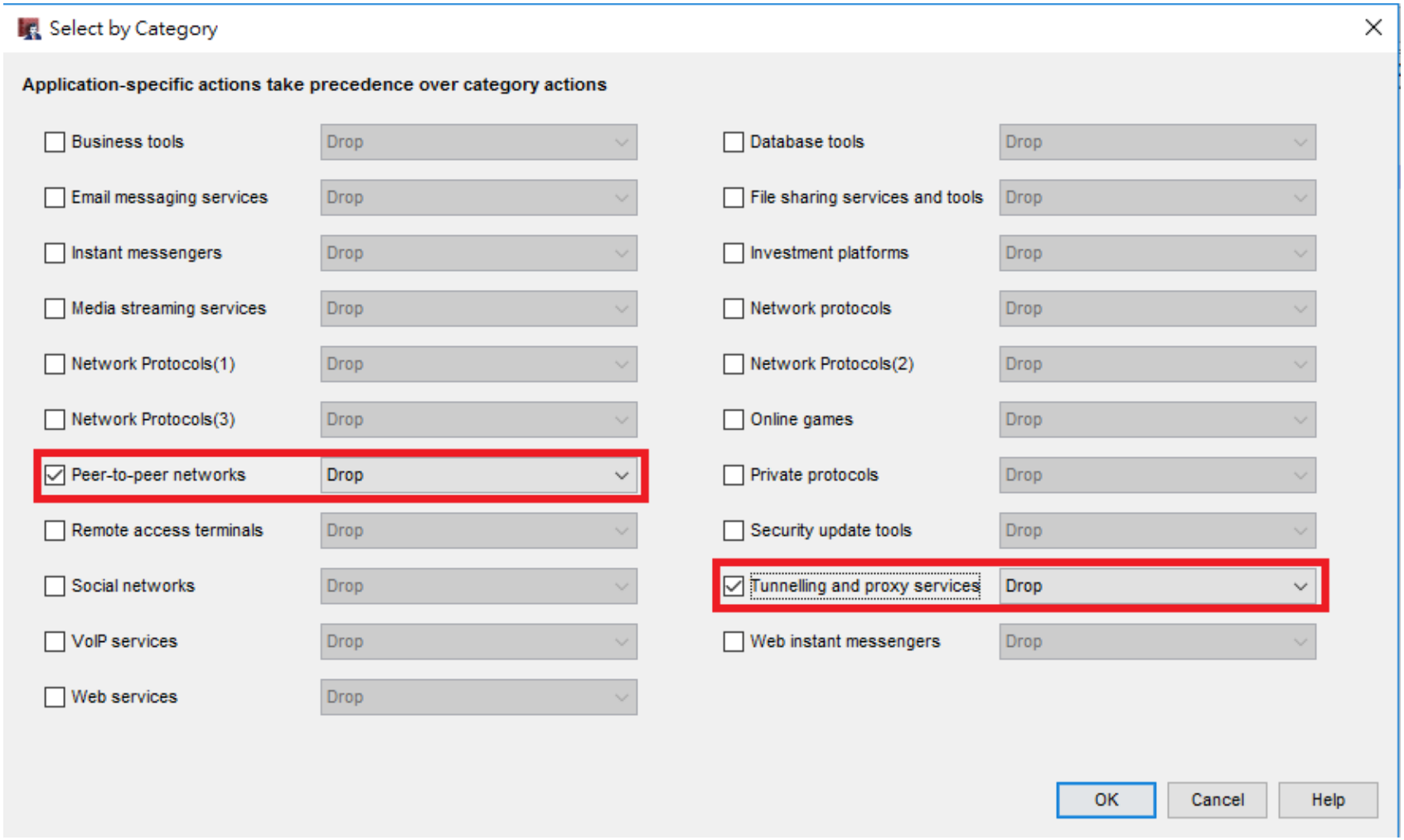
1. 設定Application Control政策名稱
2. 搜尋要管控的應用程式
3. 連續點選兩下要控管的應用程式
4. 於下拉式選單選擇要控管的方式
5. 點選OK

依據分類設定封鎖



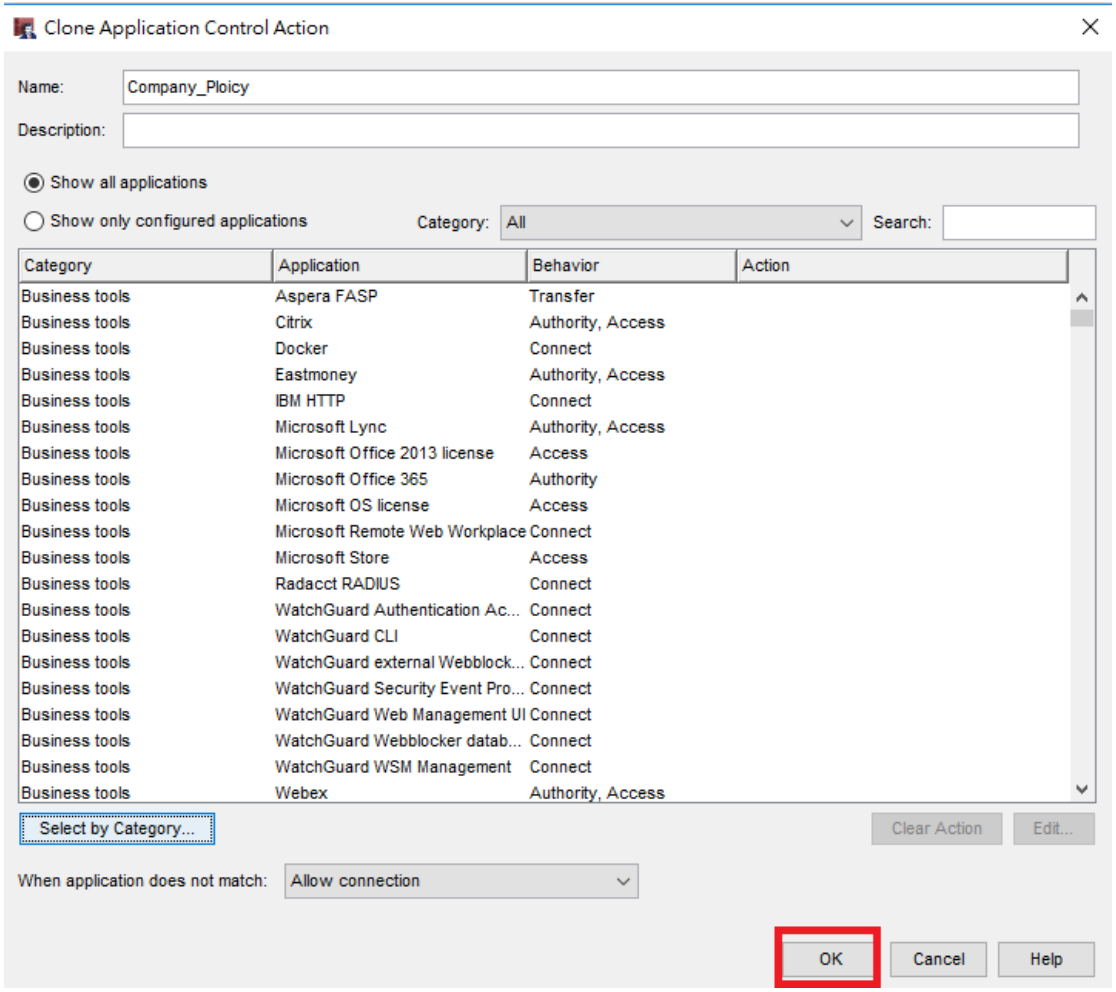
點選下方Select by category

勾選要封鎖的應用程式分類



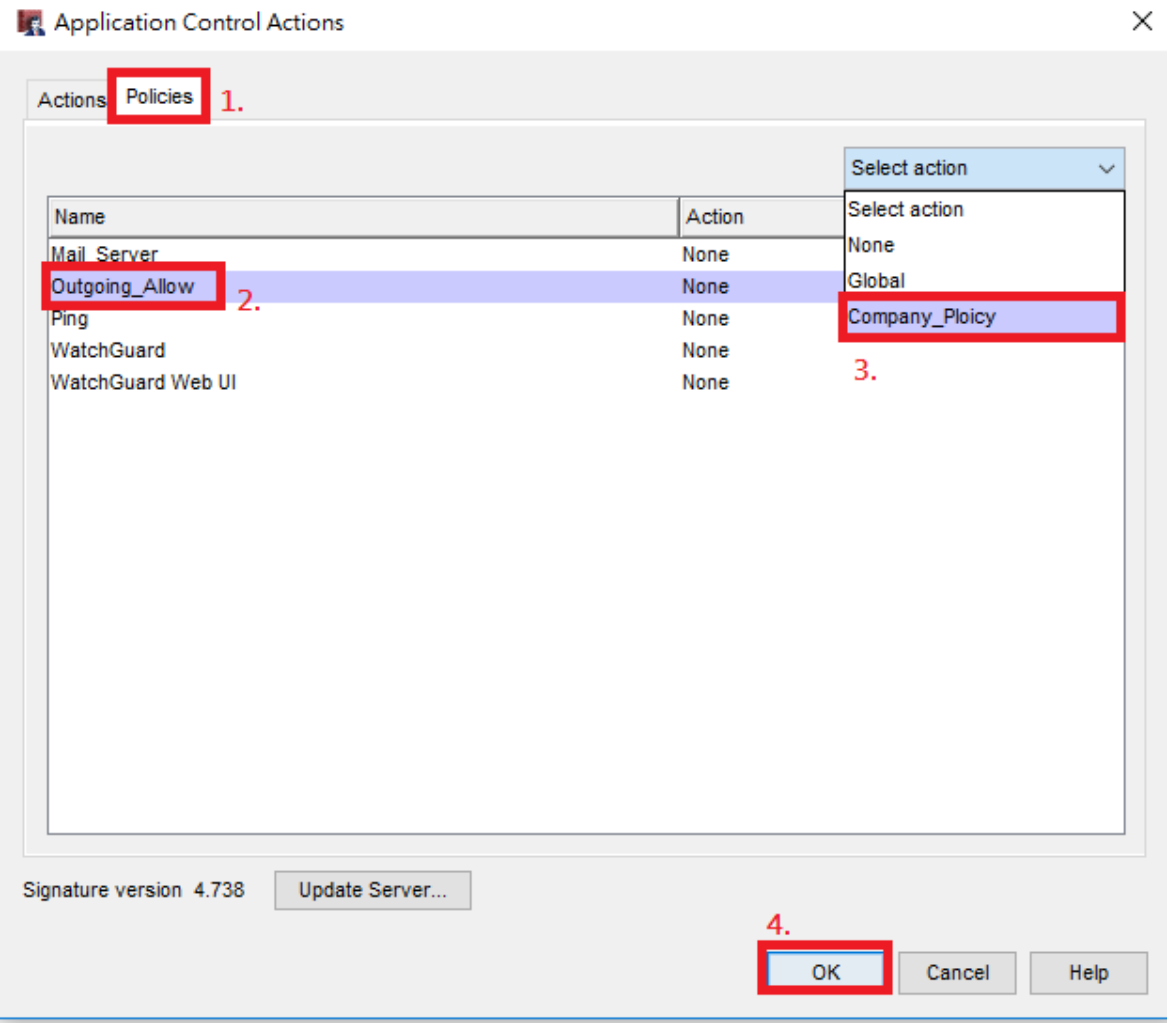
勾選要封鎖的應用程式分類

Application Control Profile設定完成



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

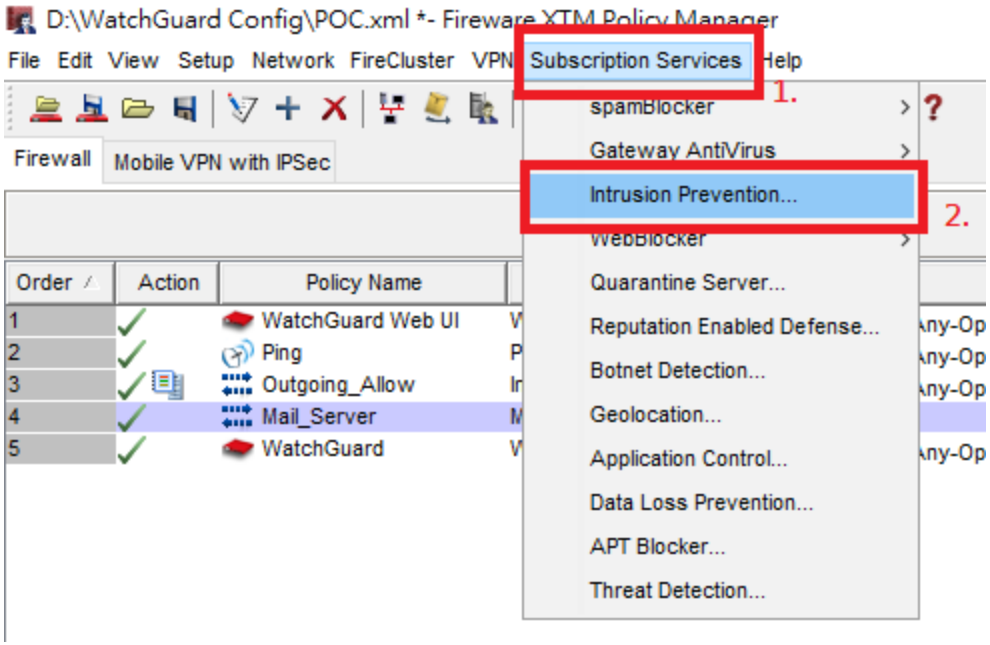
設定Application Control要套用的Policy



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

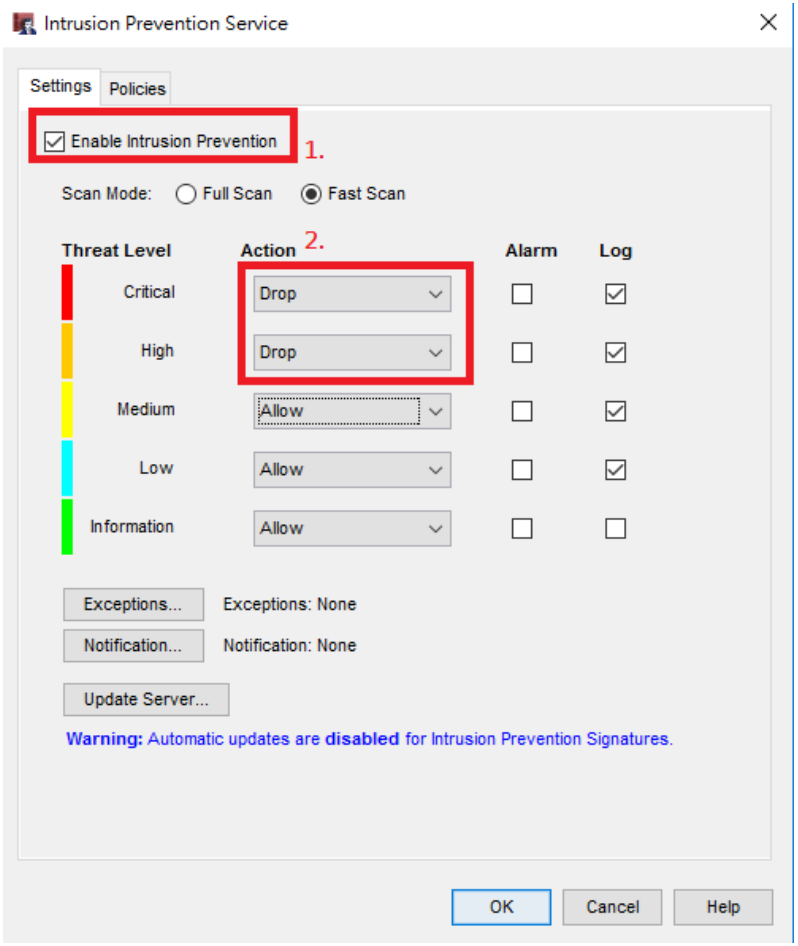
IPS設定

設定IPS



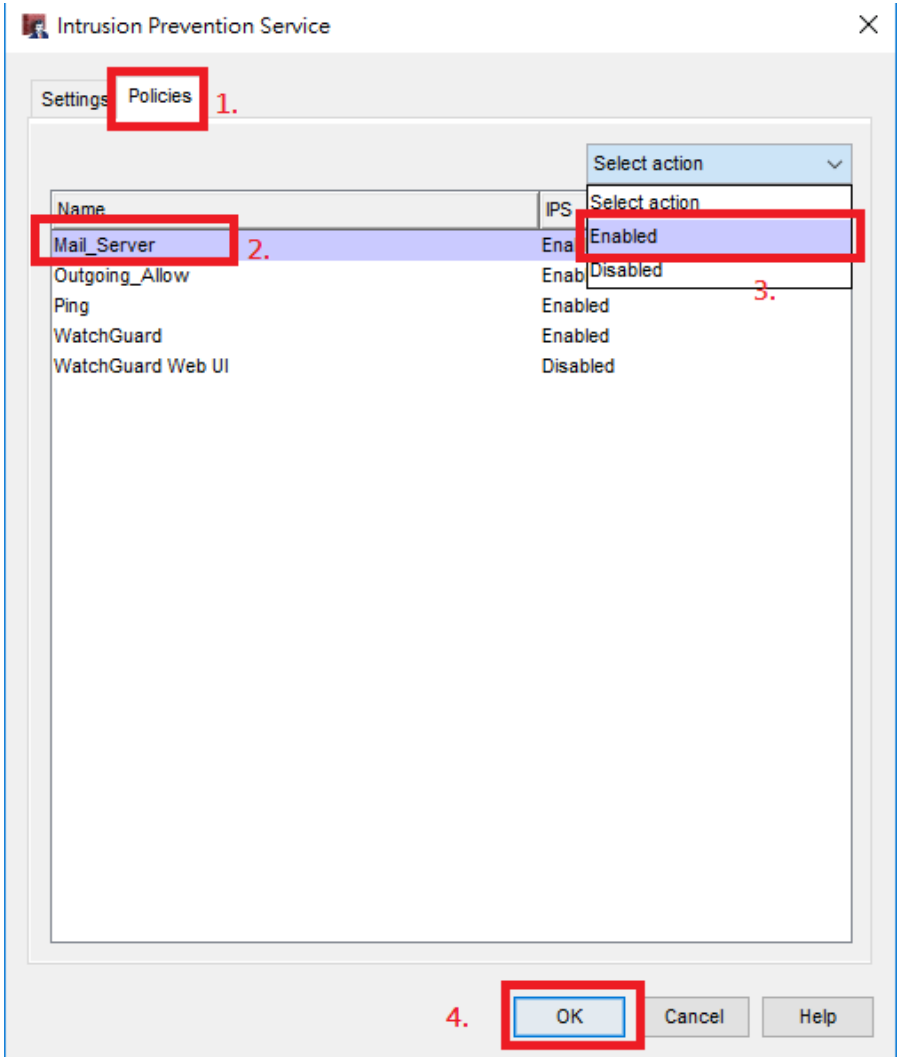
1. Subscription Service
2. 點選Intrusion Prevention

封鎖風險等級設定



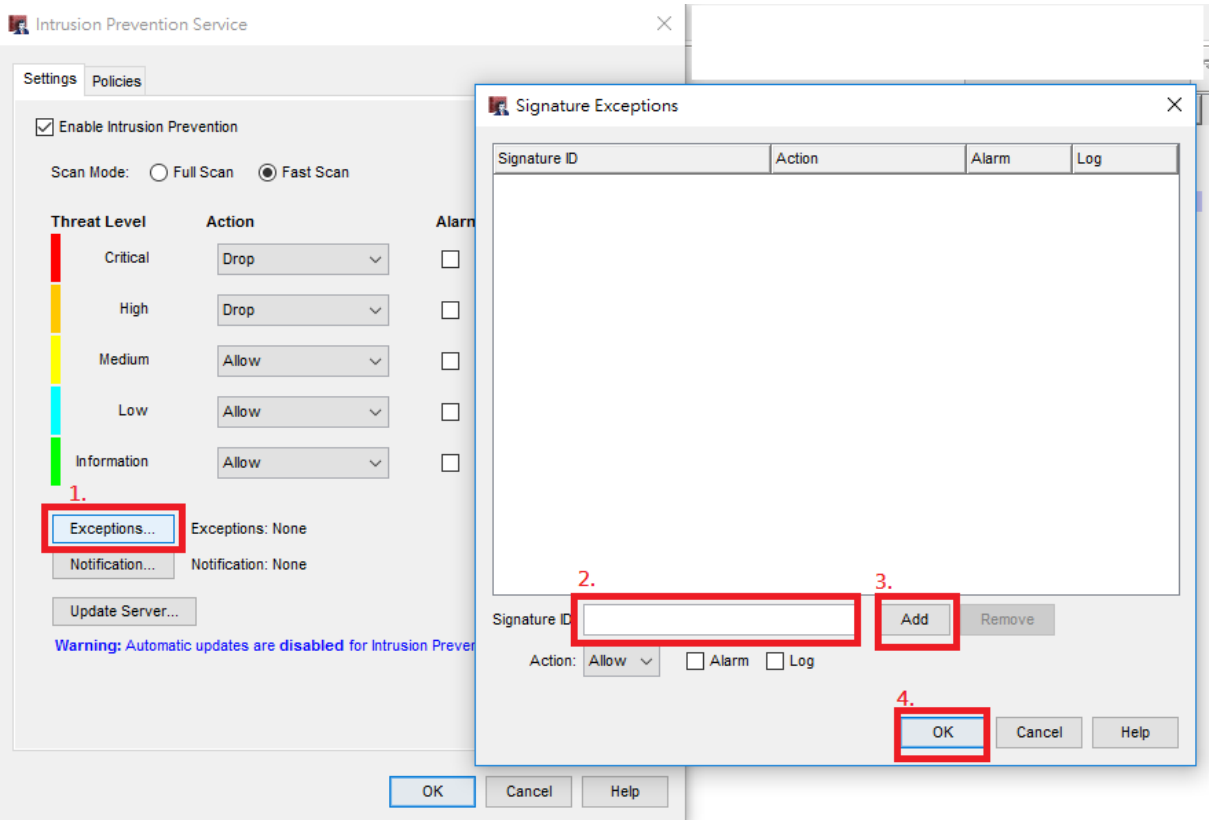
1. 勾選Enable Intrusion Prevention
2. 將要風選的風險等級選擇Drop

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

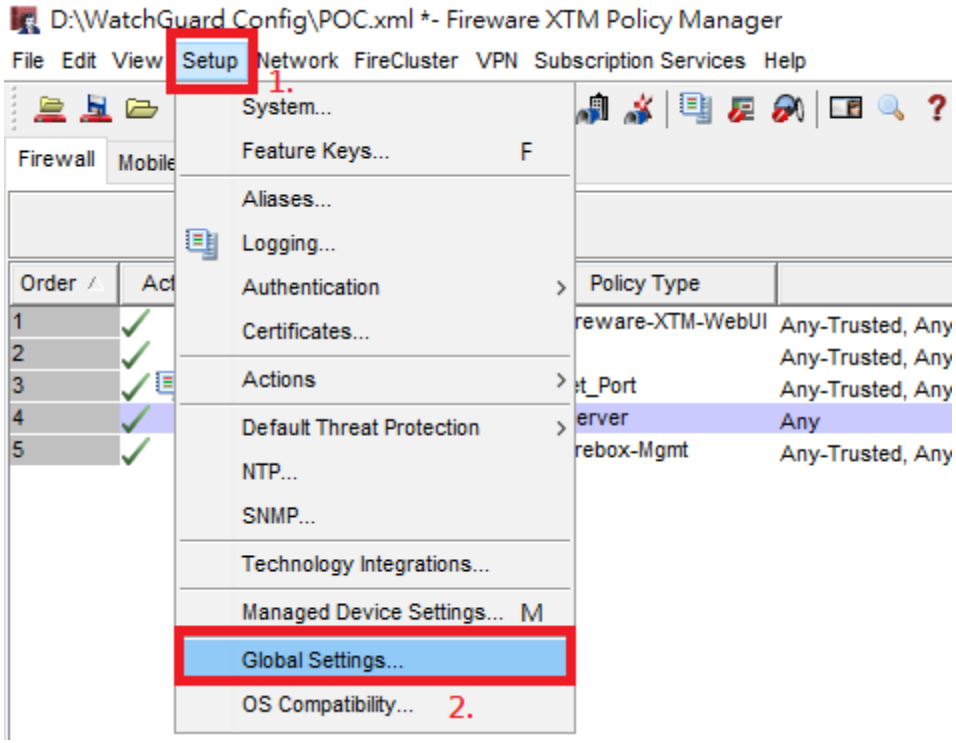
Traffic Manager設定

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

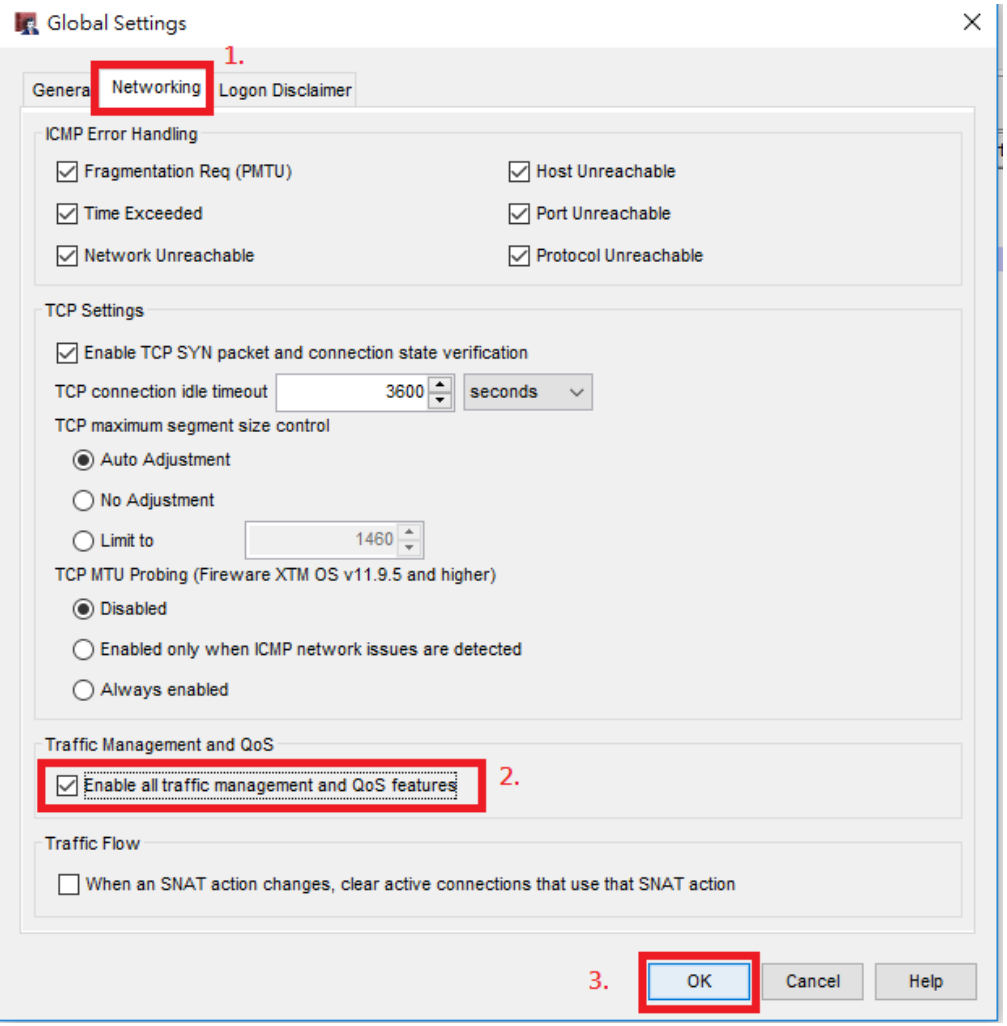
啟用Traffic Manager



Step 1 :

1. 點選Setup
2. 點選Global Settings

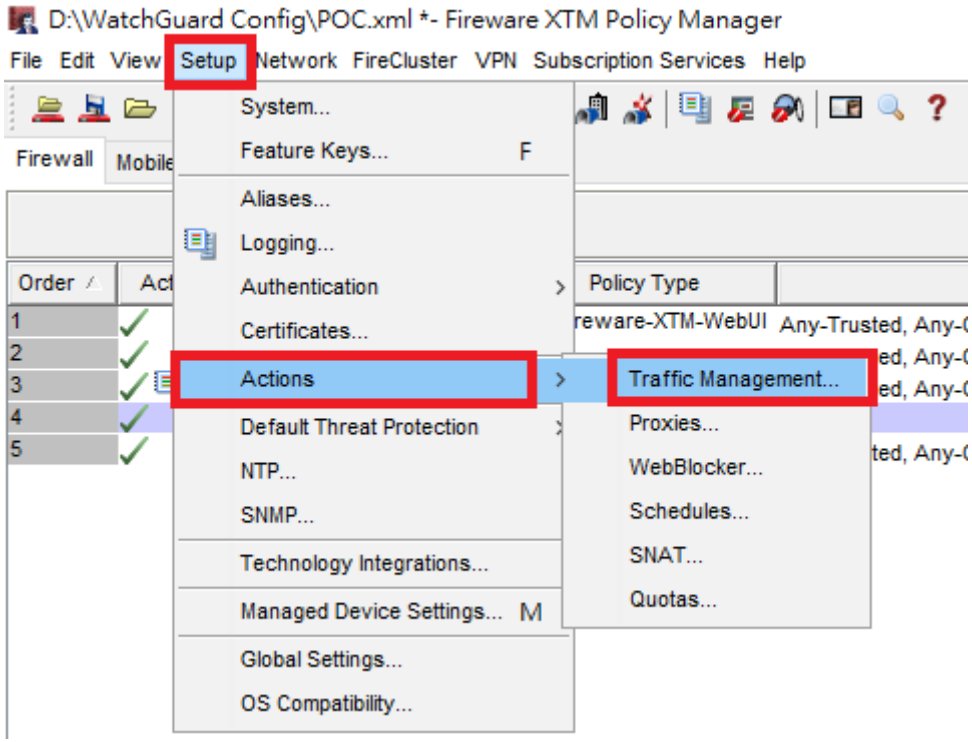
啟用Traffic Manager



Step 2 :

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

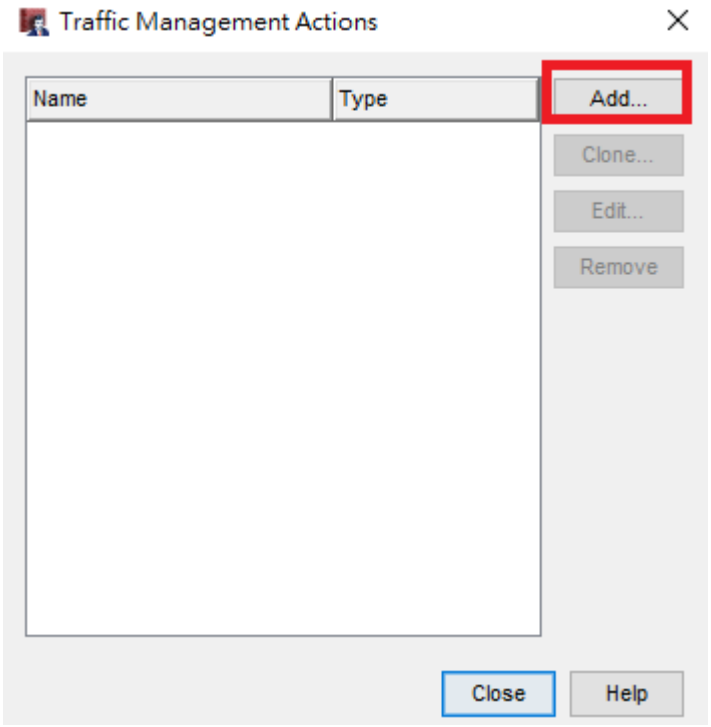
設定Traffic Manager Profile



Step 1 :

Setup → Actions → Traffic Management

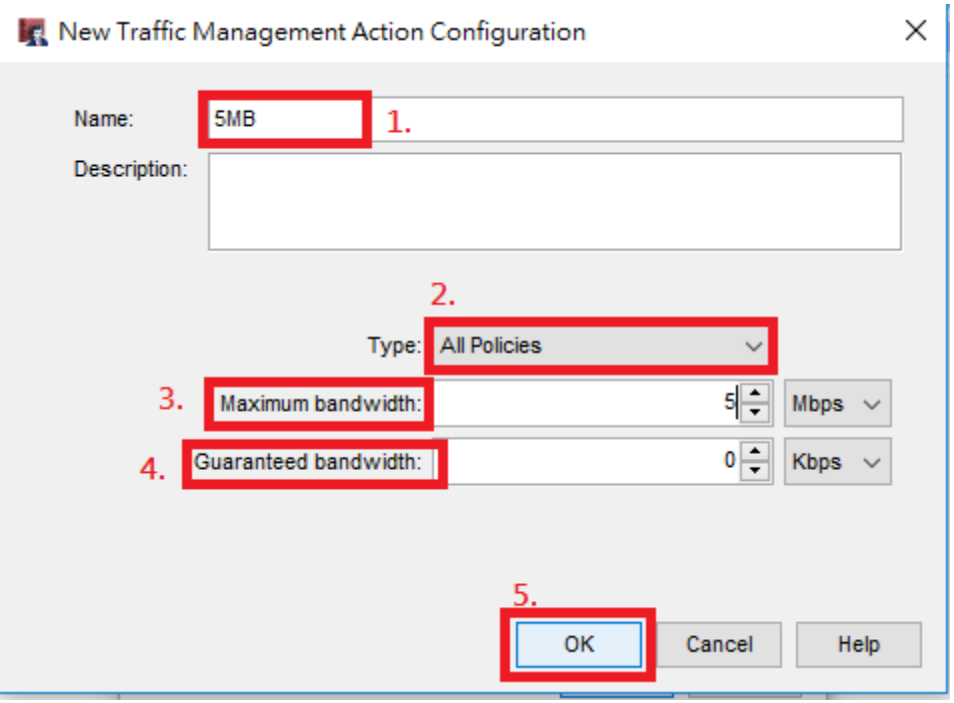
設定Traffic Manager Profile 2



Step 2 :

點選Add

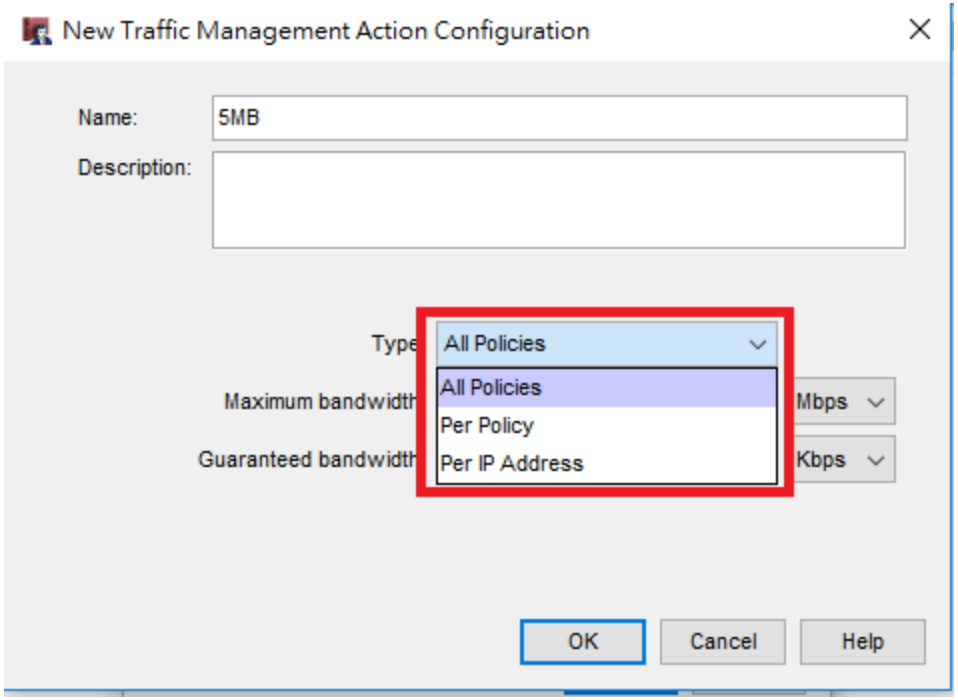
設定Traffic Manager Profile



Step 3 :

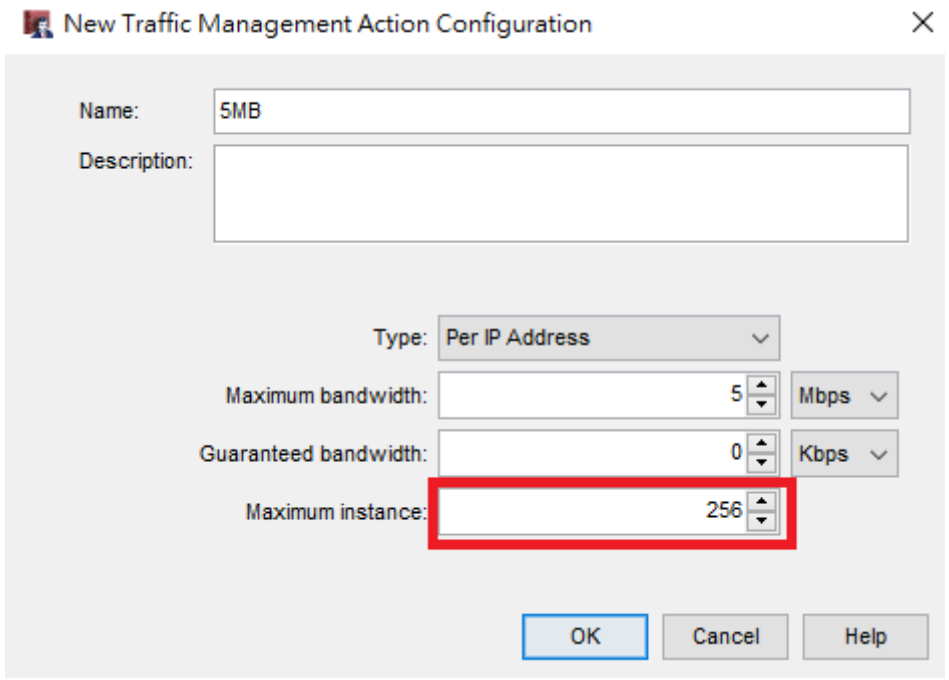
1. 設定Traffic management Profile名稱
2. 選擇Profile Type
3. Maximum Bandwidth：最大頻寬，套用此Profile Policy可使用的頻寬上限
4. Guaranteed Bandwidth：保證頻寬，套用到此Profile的Policy至少可使用的頻寬下限。
5. 點選OK

Traffic Manager Profile Type說明



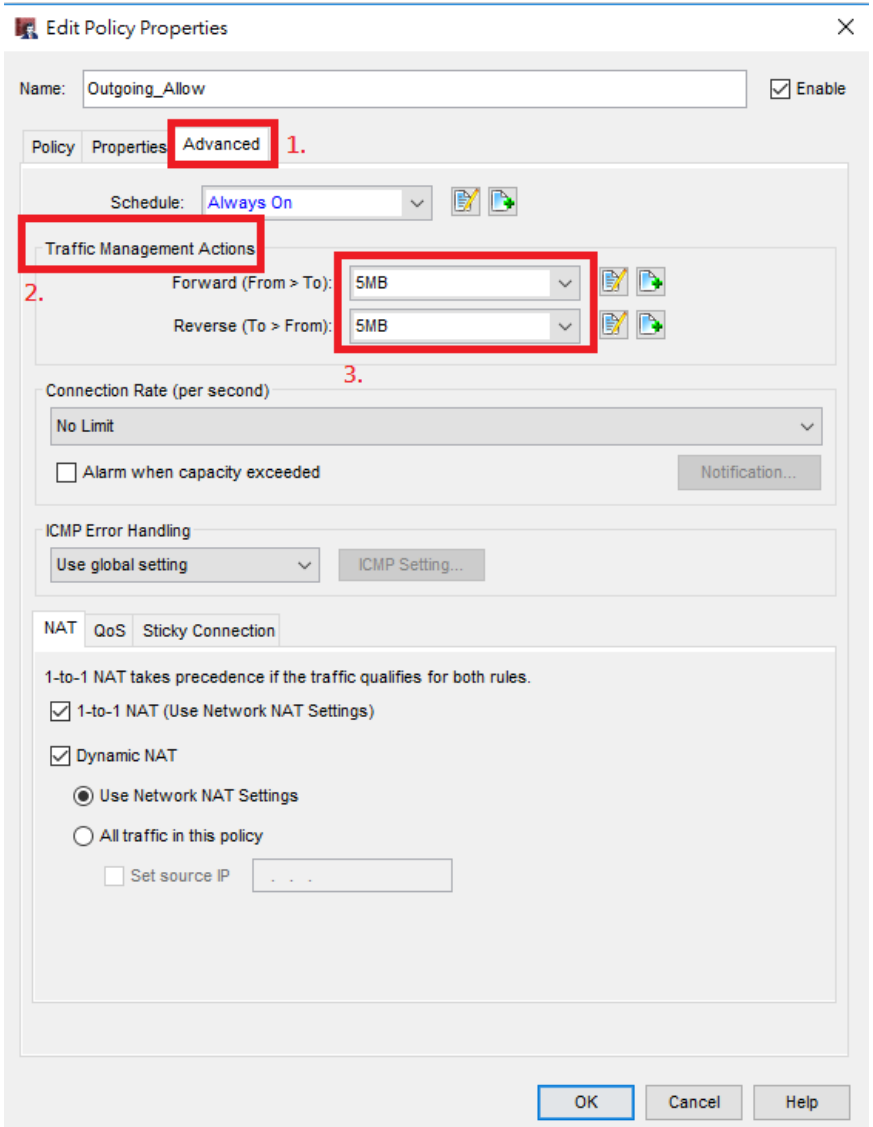
1. **All Policies** – 整台防火牆只要套用到這個Profile的Policy共同Share所設定的頻寬
2. **Per Policy** – 防火牆中個別Policy套用到這個Profile皆獨立可使用所設定的頻寬
3. **Per IP Address** – Policy中每一個IP都可以獨立使用所設定的頻寬。

Per IP Address設定



Type 設定Per IP Address時，Maximum instance設定256

Traffic Manager Profile 套用至Policy



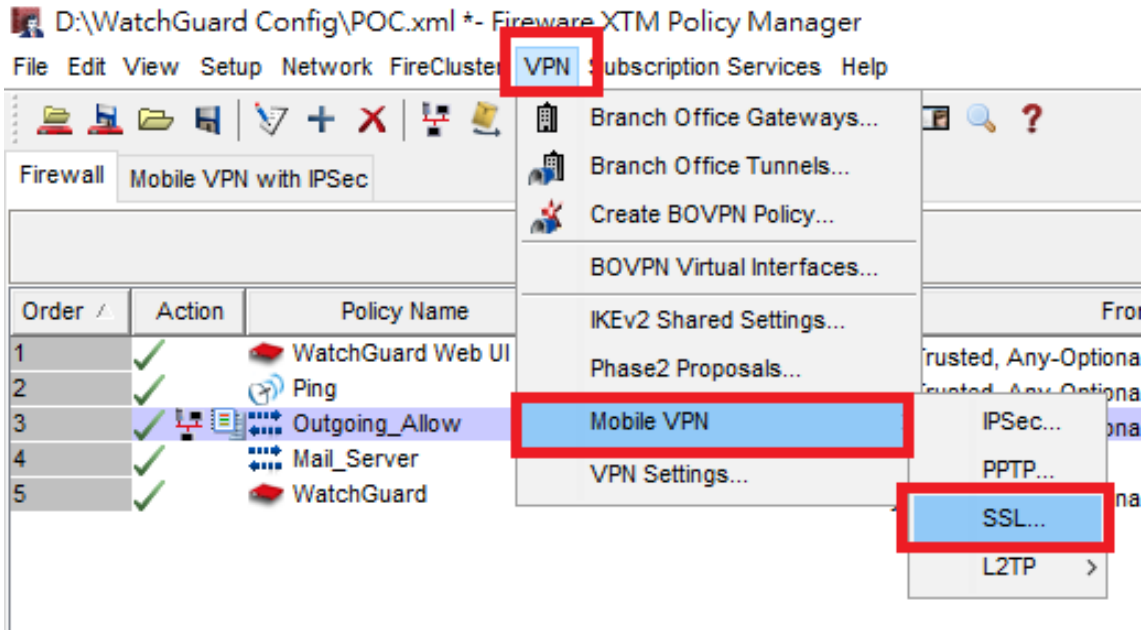
1. 編輯Policy點選Advance
2. Traffic Management Action中選擇設定好的Profile

Forward – 上傳頻寬

Reverse – 下載頻寬

VPN 設定

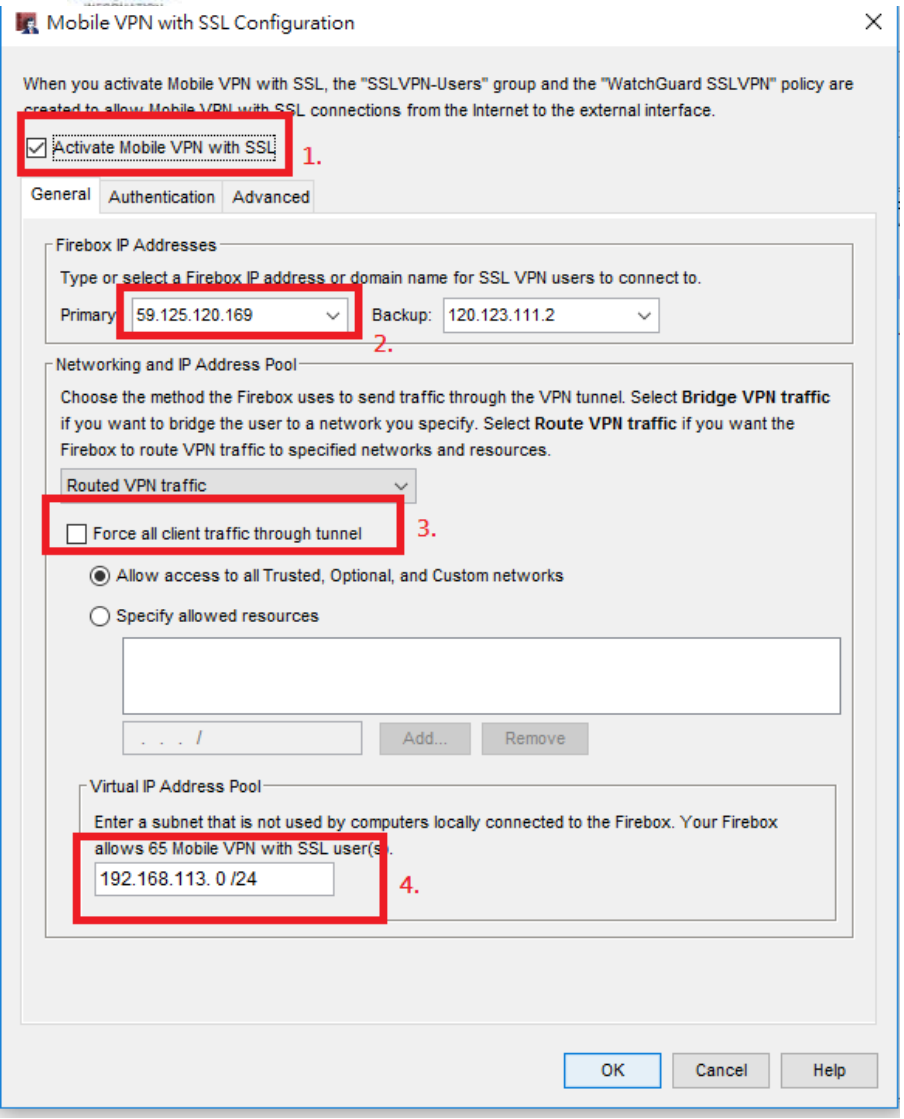
啟用SSL VPN設定



Step 1 :

VPN → Mobile VPN → SSL

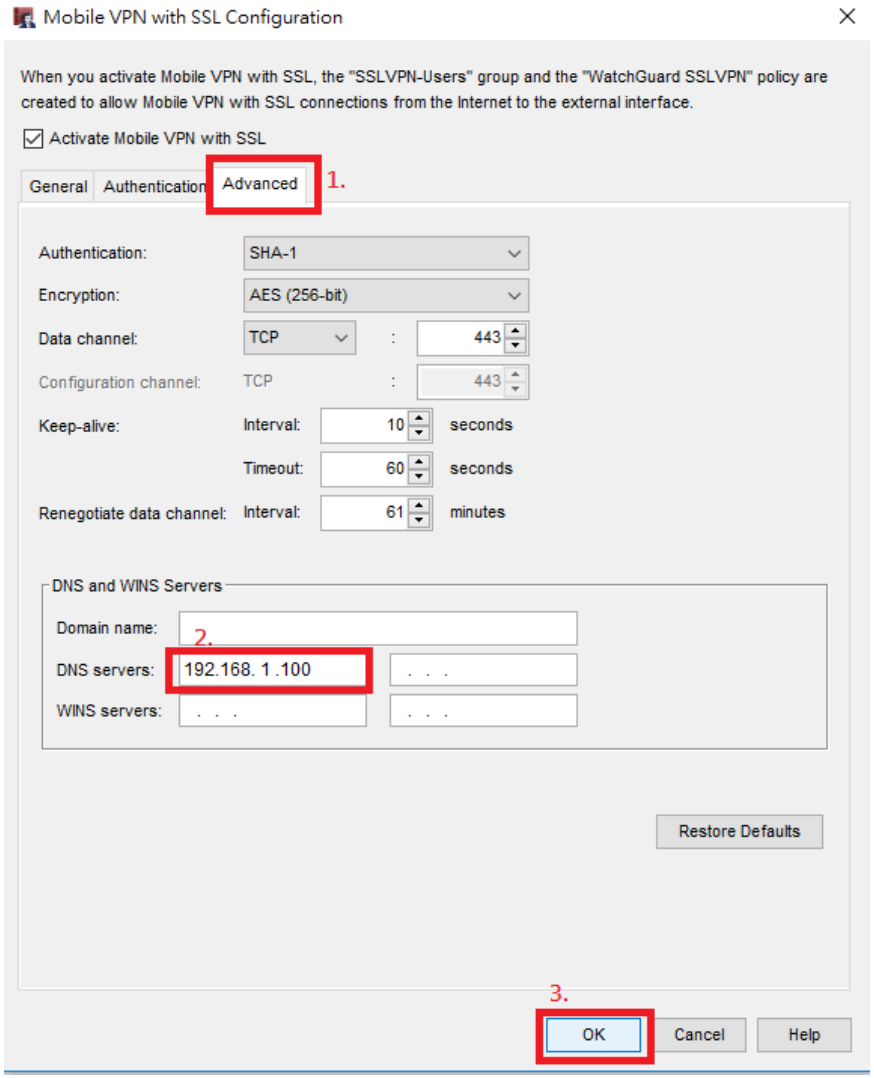
啟用SSL VPN設定



Step 2 :

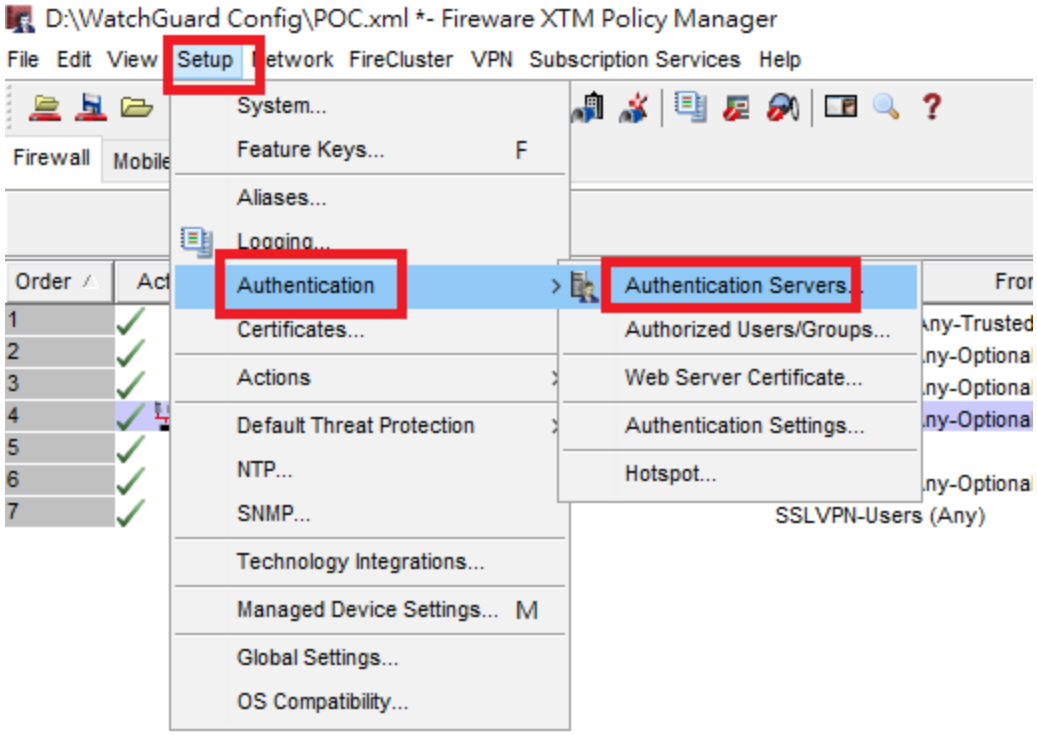
1. 勾選Active Mobile VPN with SSL
2. 選擇要提供給SSL VPN連線的IP
3. Force all client traffic through tunnel – 勾選此選項，連線SSL VPN的電腦所有流量都會經過VPN Tunnel。
4. 輸入SSL VPN所可以取得的IP Pool

SSL VPN DNS參數設定



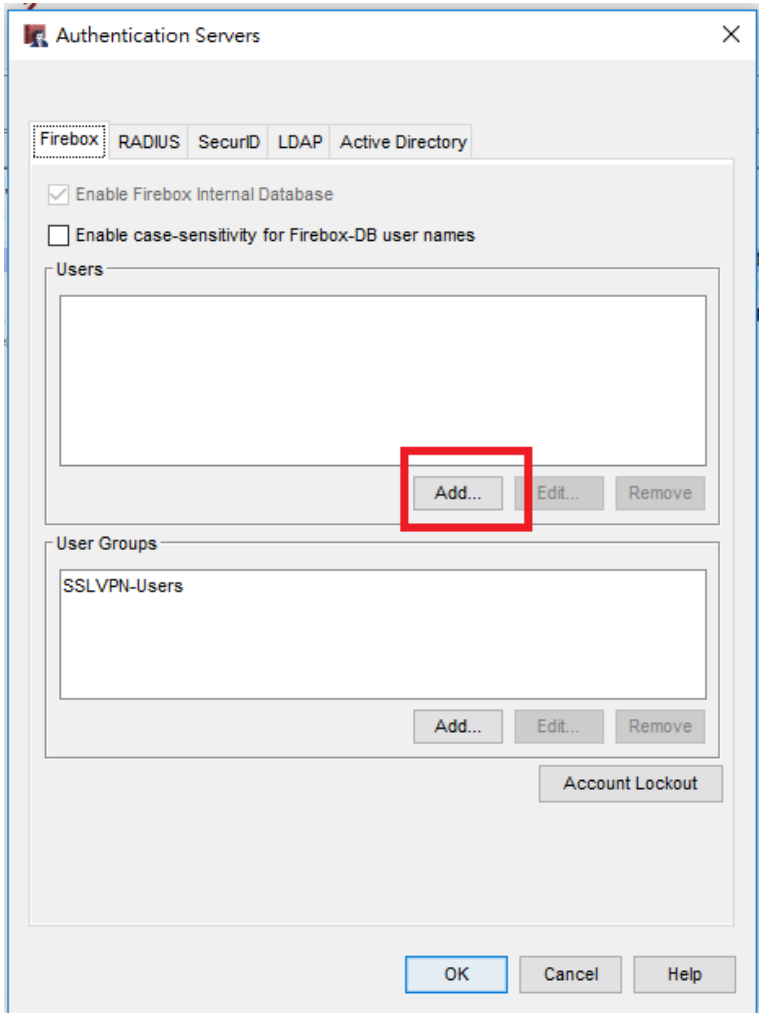
1. 點選Advance
2. 輸入DNS Server IP，Client連線SSL VPN後所會取得的DNS IP

設定SSL VPN連線帳號



Setup → Authentication → Authentication Server

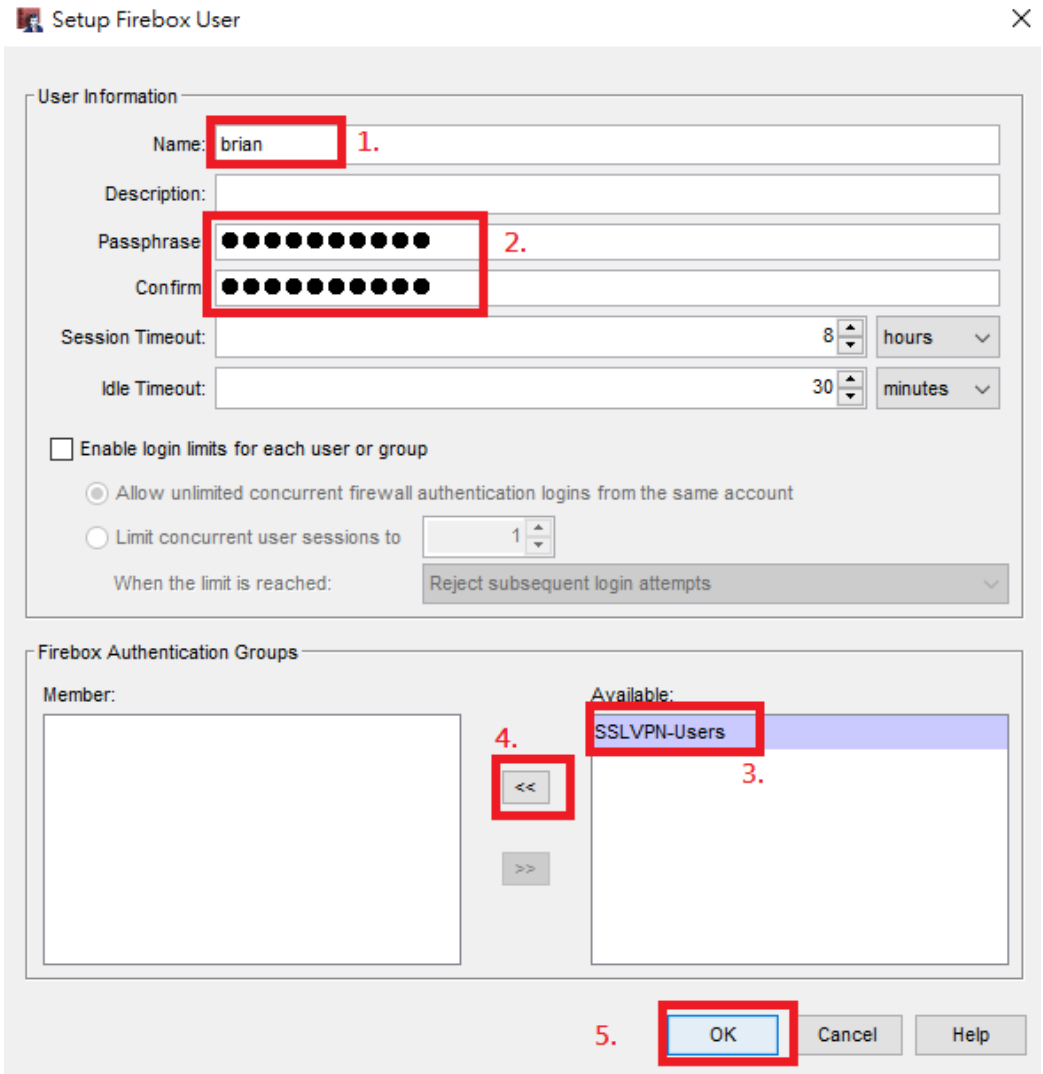
新增SSL VPN連線帳號



Step 1 :

點選Add

新增SSL VPN連線帳號

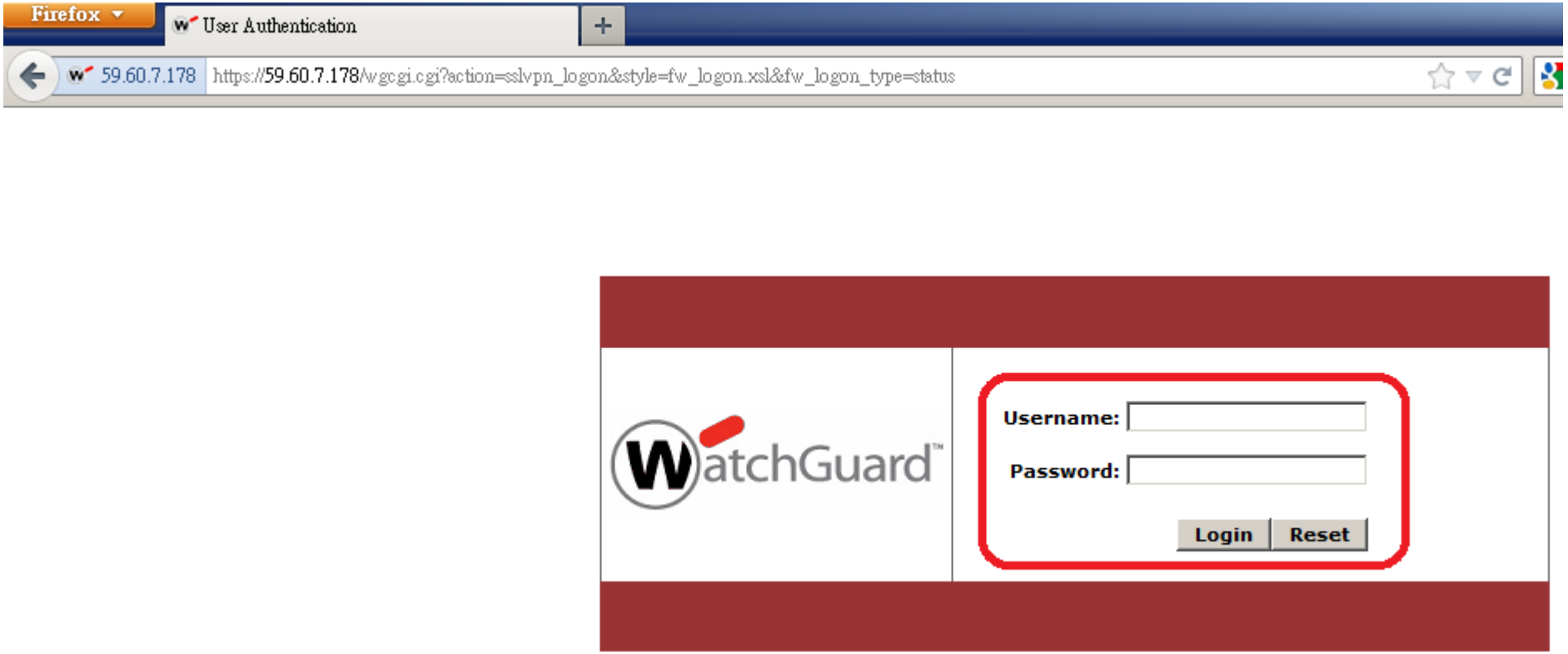


Step 2 :

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

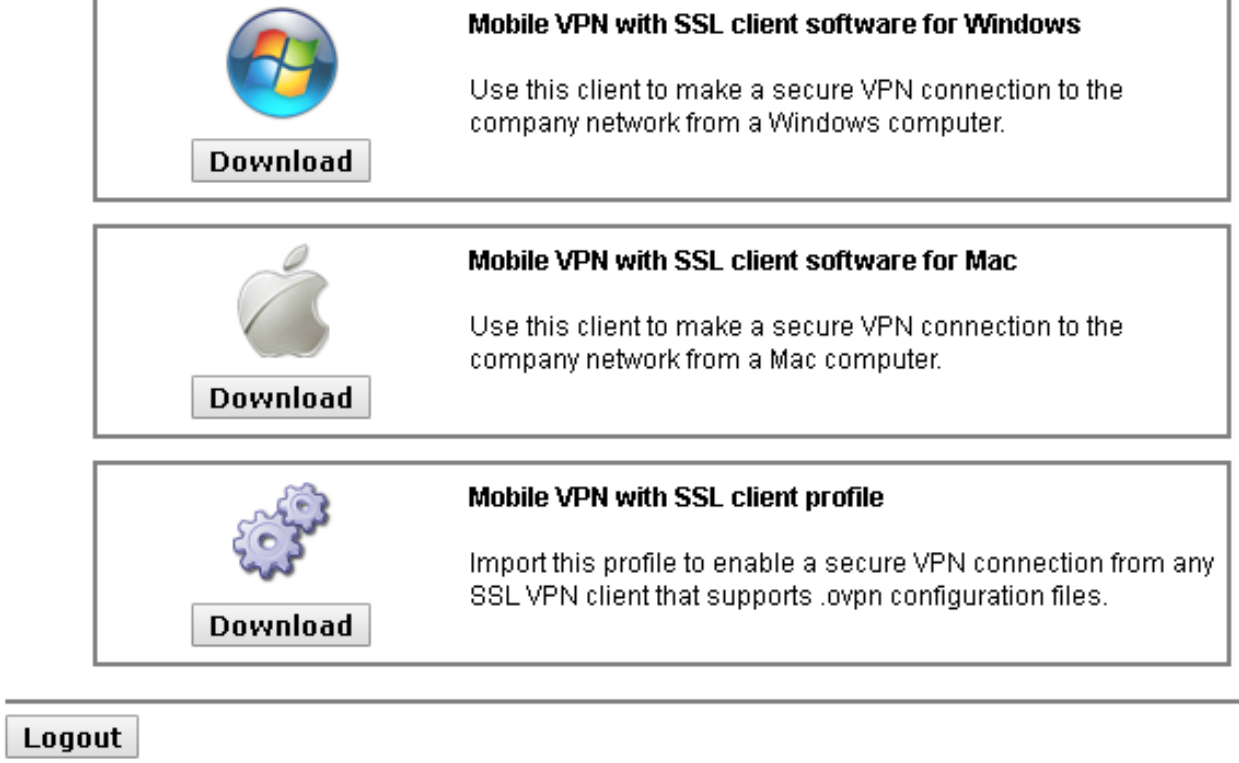
SSL VPN Client安裝

連線Download SSL VPN Client



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



依您的作業系統下載所需的軟體

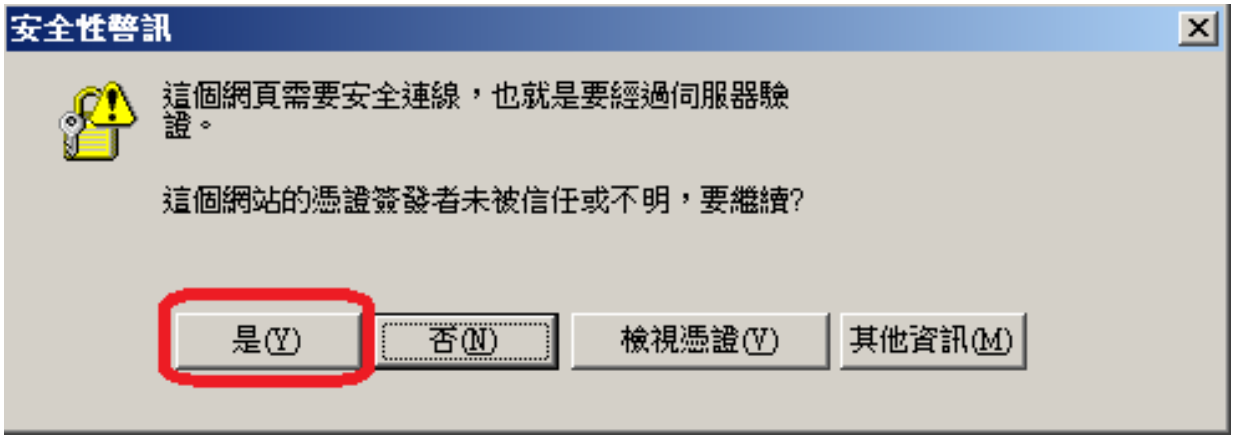
安裝完成SSL VPN Client

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

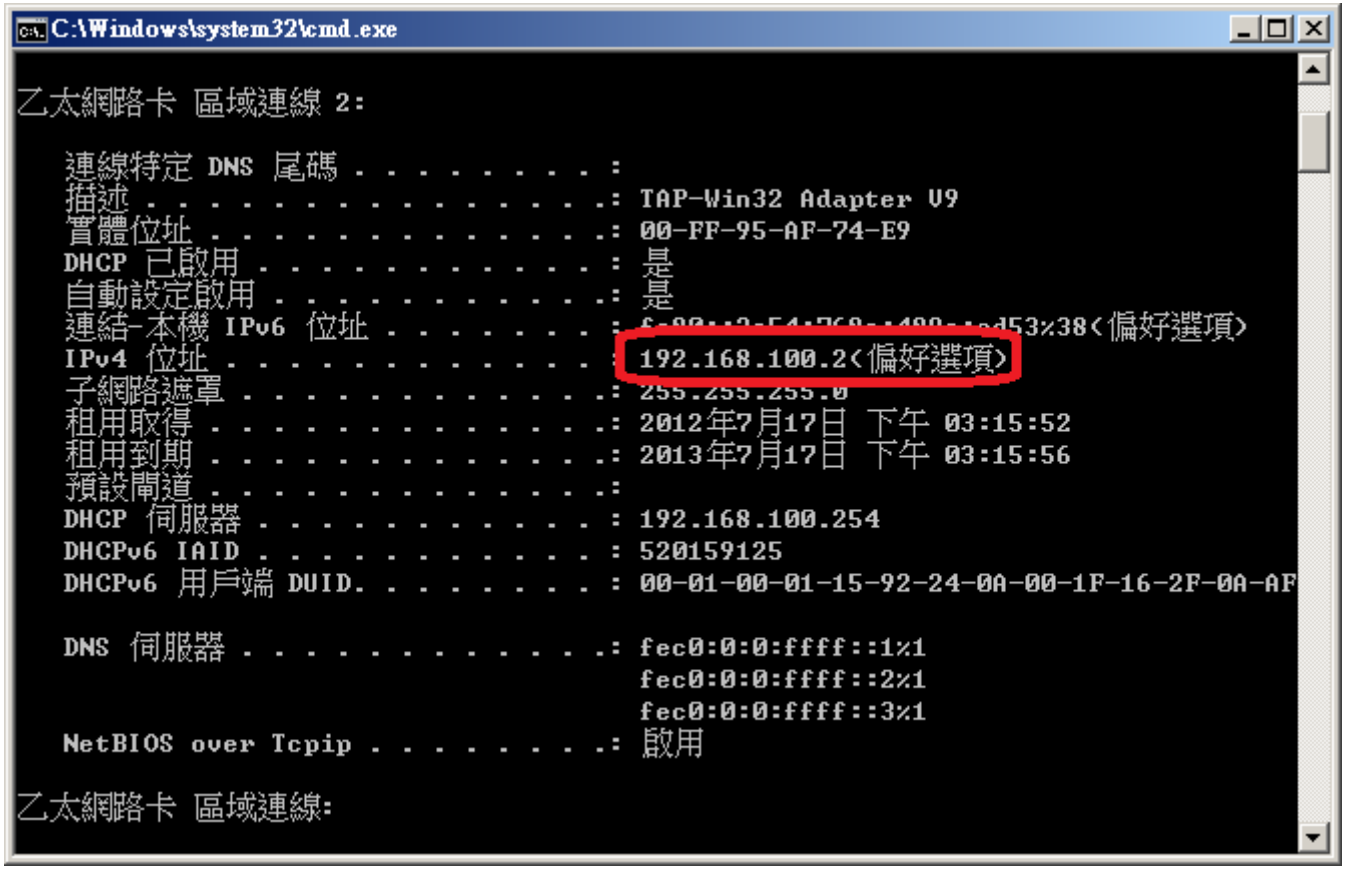
輸入Firewall External IP Address以及帳號密碼，之後按下Connect

安全憑證點選



安全憑證部分點選”是”

連線成功畫面



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

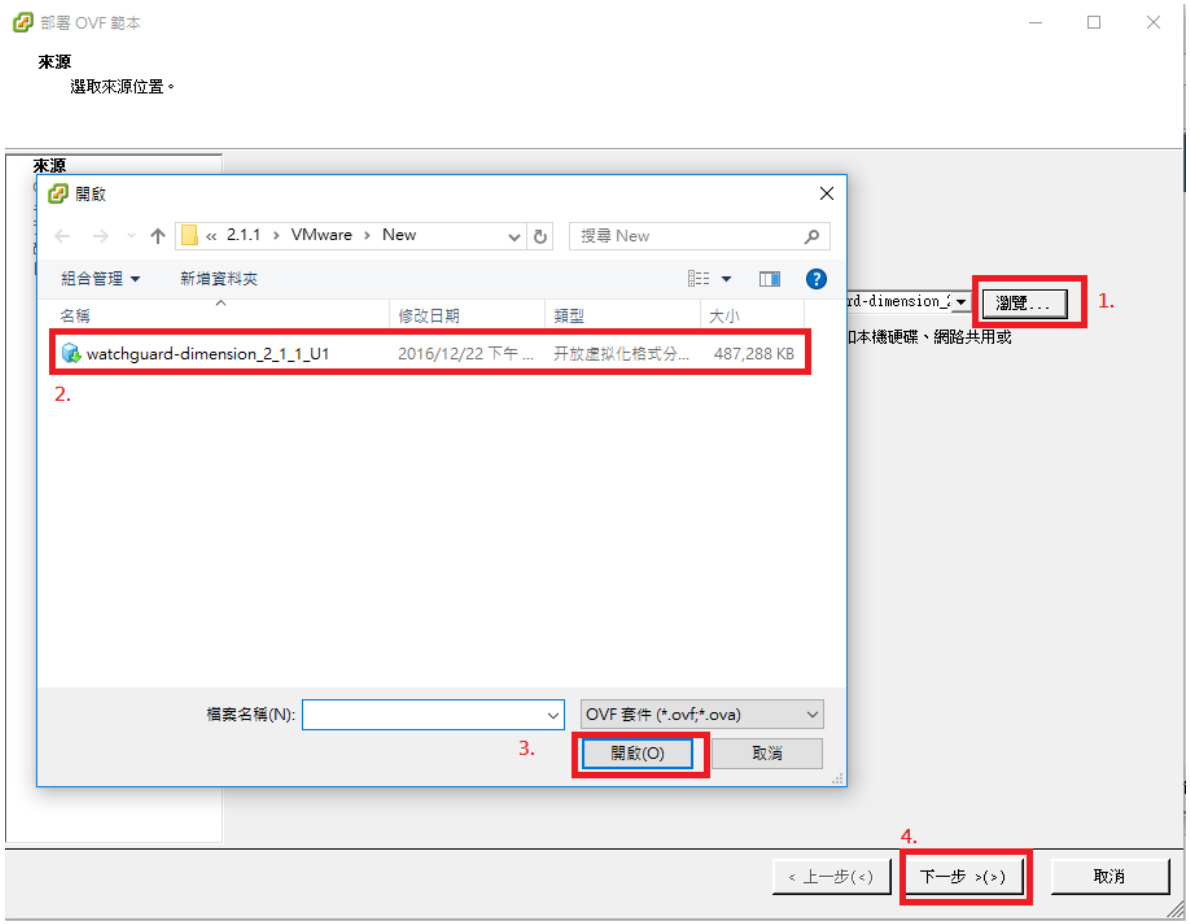
1. VMware ESX
2. VMware ESXI
3. Windows Hyper-V

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

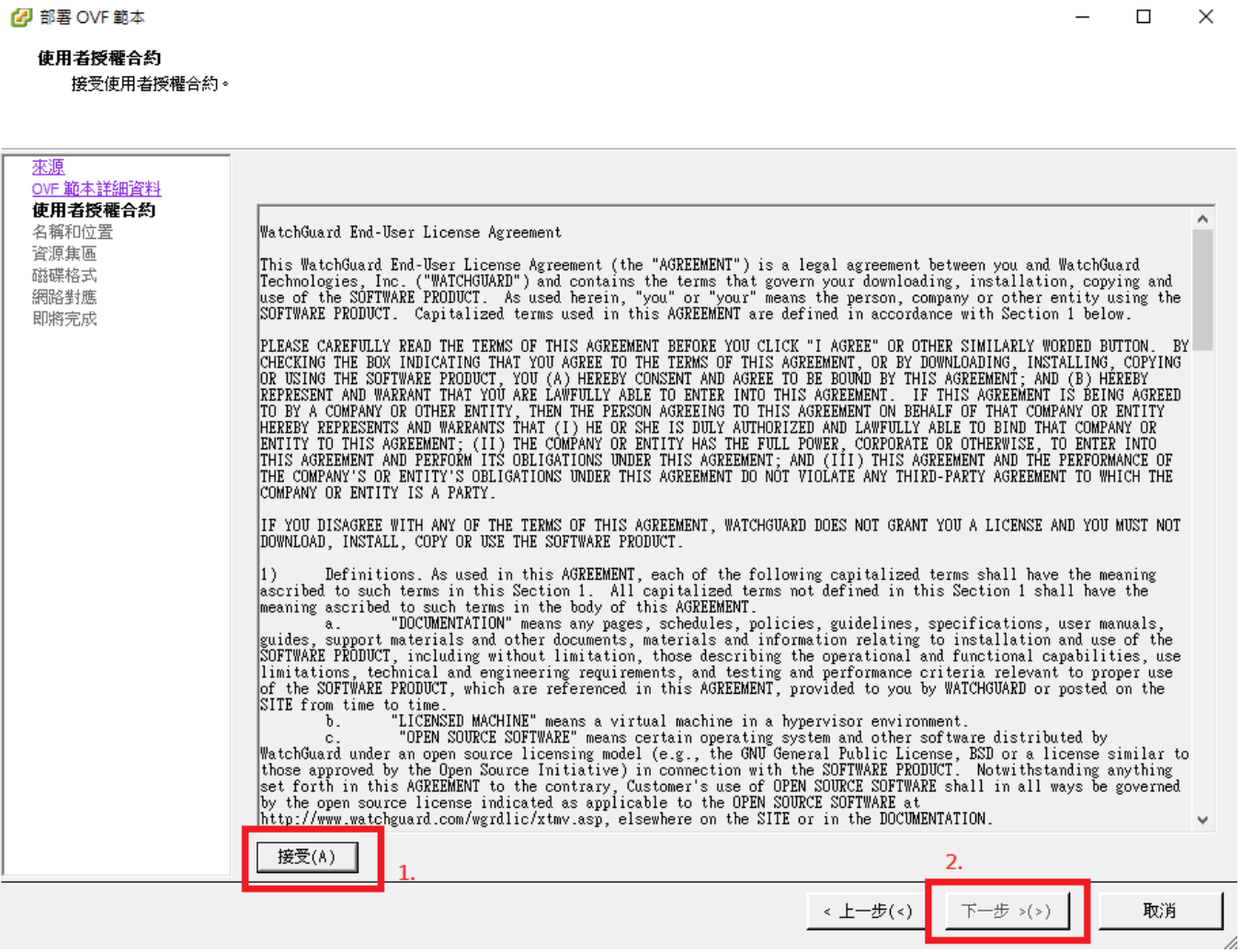


1. 點選瀏覽
2. 選擇Dimension OVF檔案
3. 點選開啟
4. 點選下一步

Dimension Report OVF檔案詳細資料

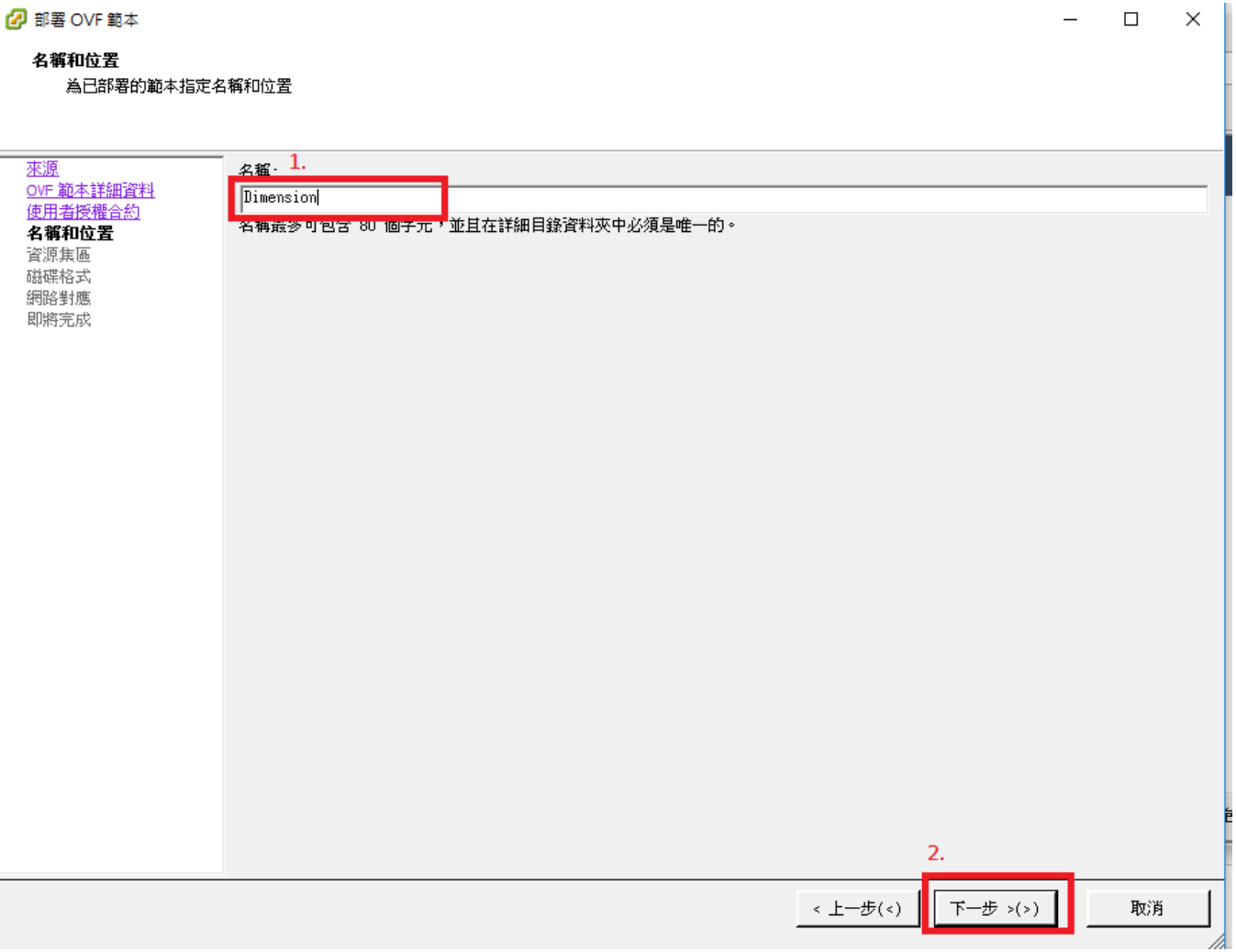
點選下一步

Dimension Report合約選項



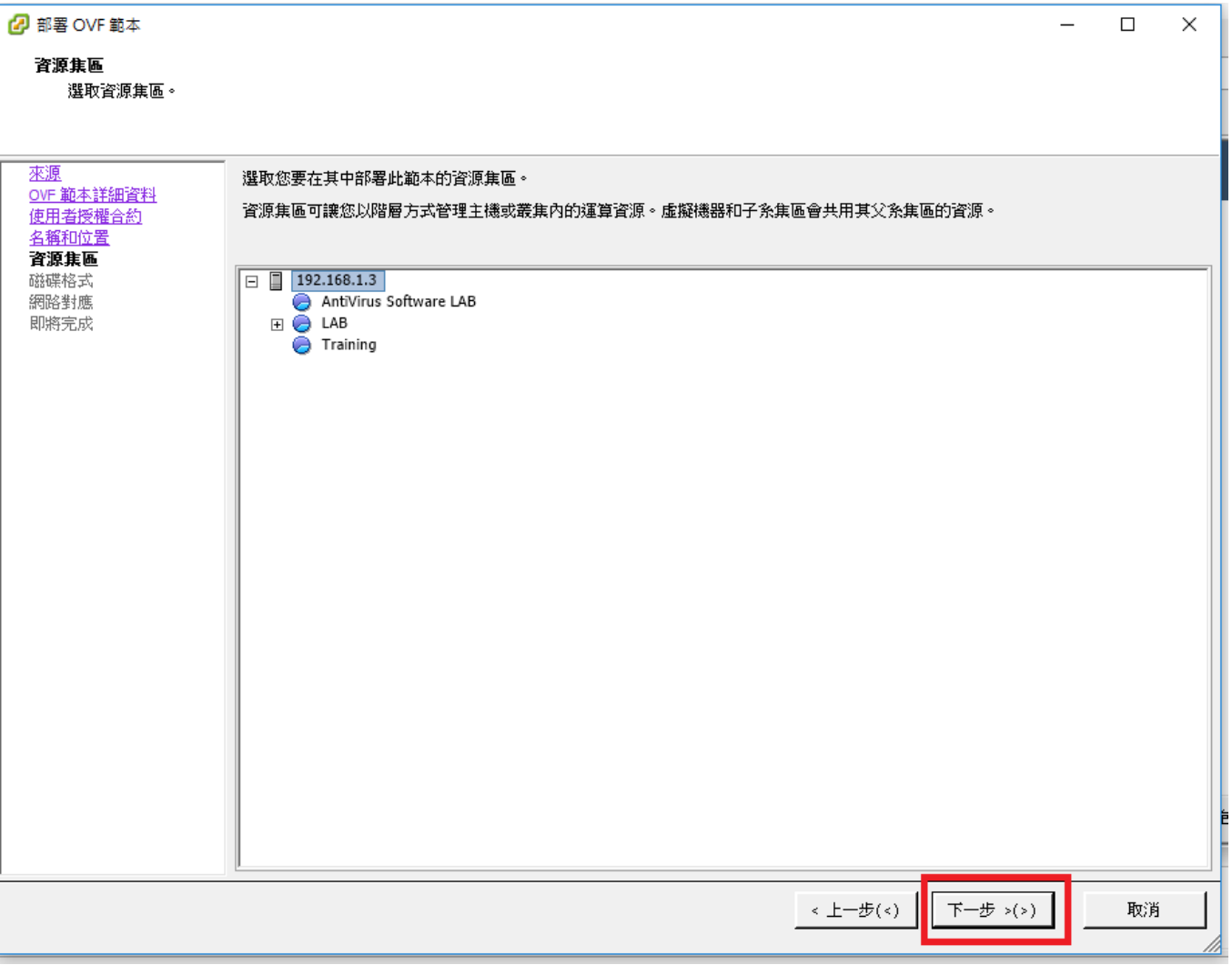
1. 點選接受
2. 點選下一步

輸入Dimension Report OVF 名稱



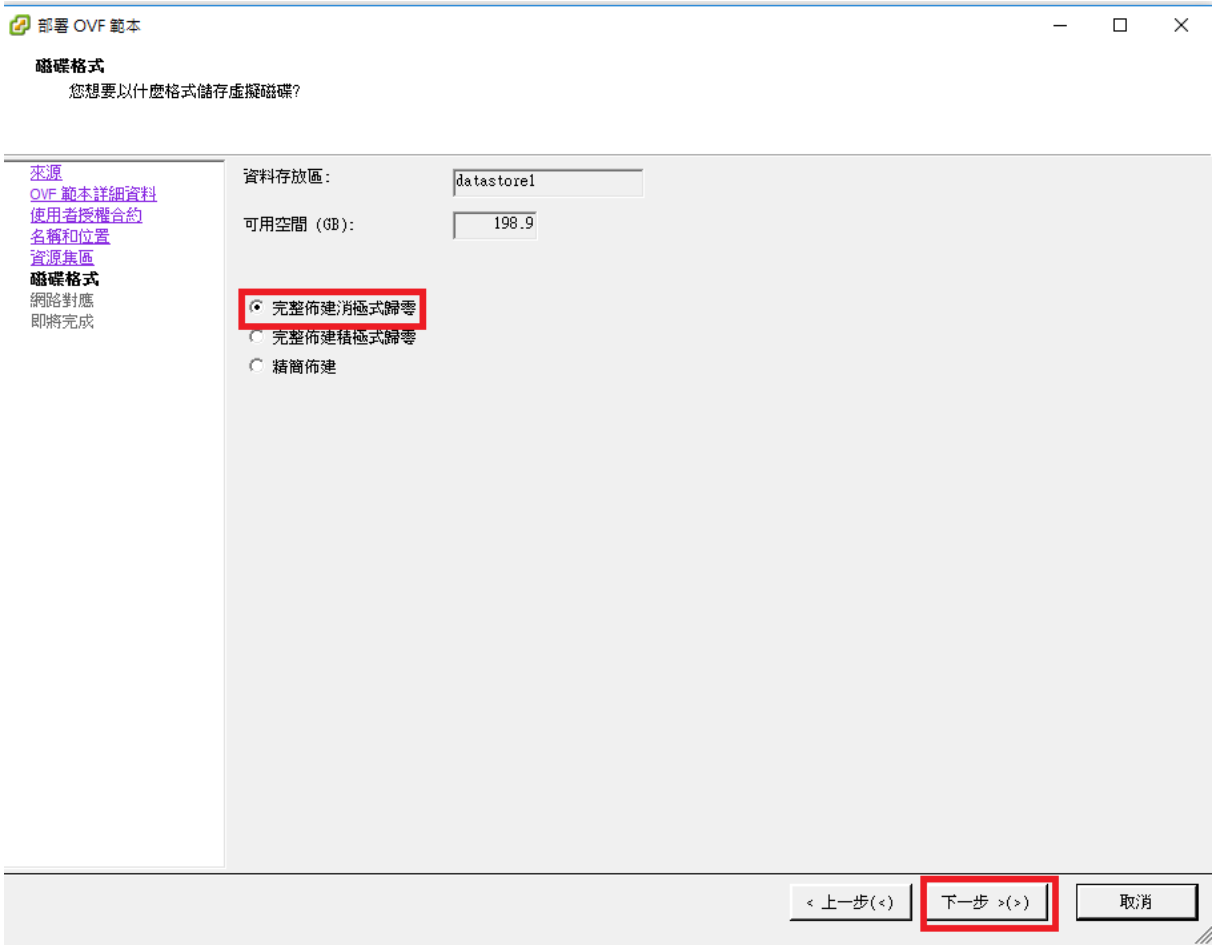
1. 輸入Guest OS名稱
2. 點選下一步

選擇Dimension Report OVF資料夾位置



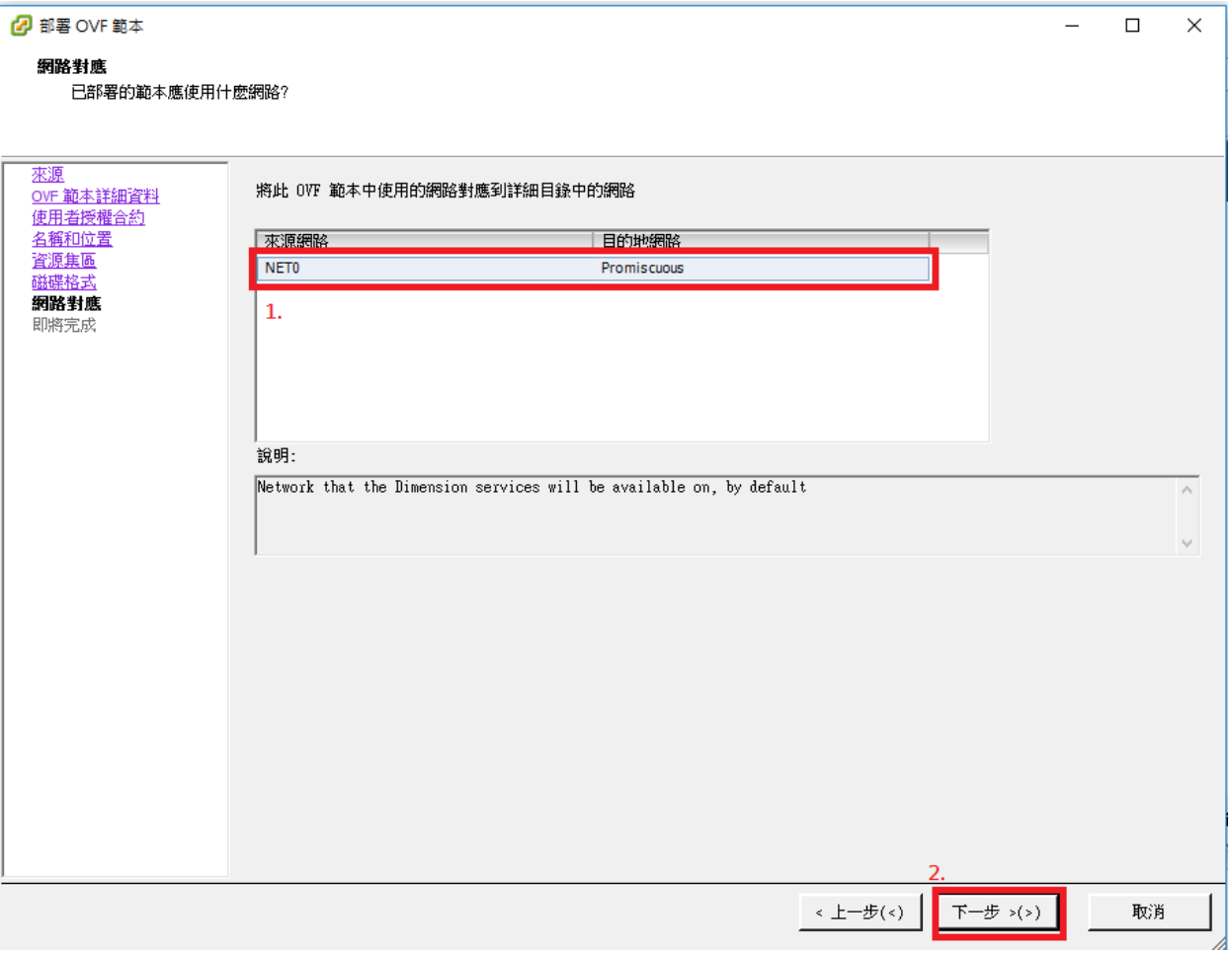
點選下一步

Dimension Report OVF硬碟使用方式



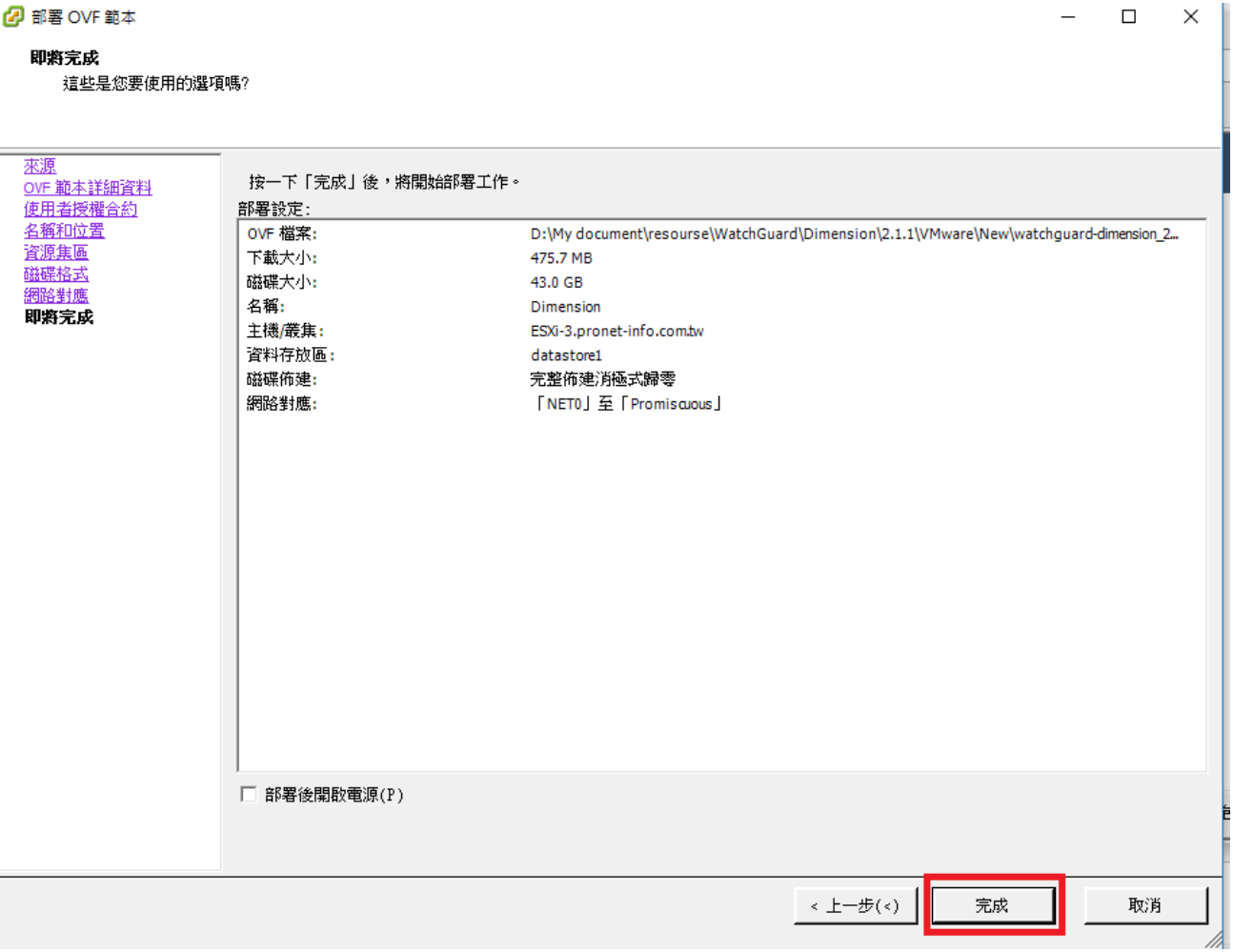
使用預設值，點選下一步

選擇Dimension Report OVF網卡



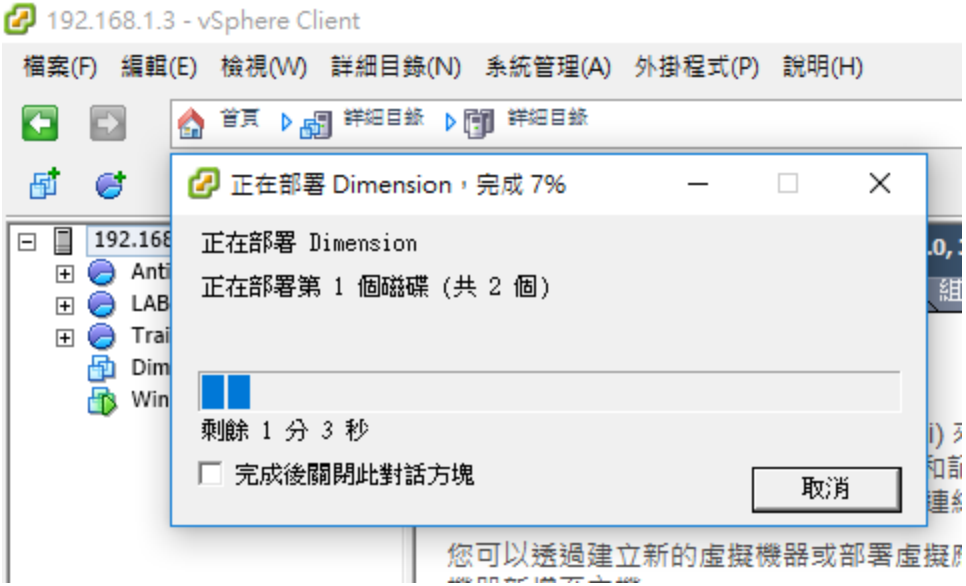
1. 選擇網路卡
2. 點選下一步

完成Dimension Report OVF匯入設定



點選完成開始匯入

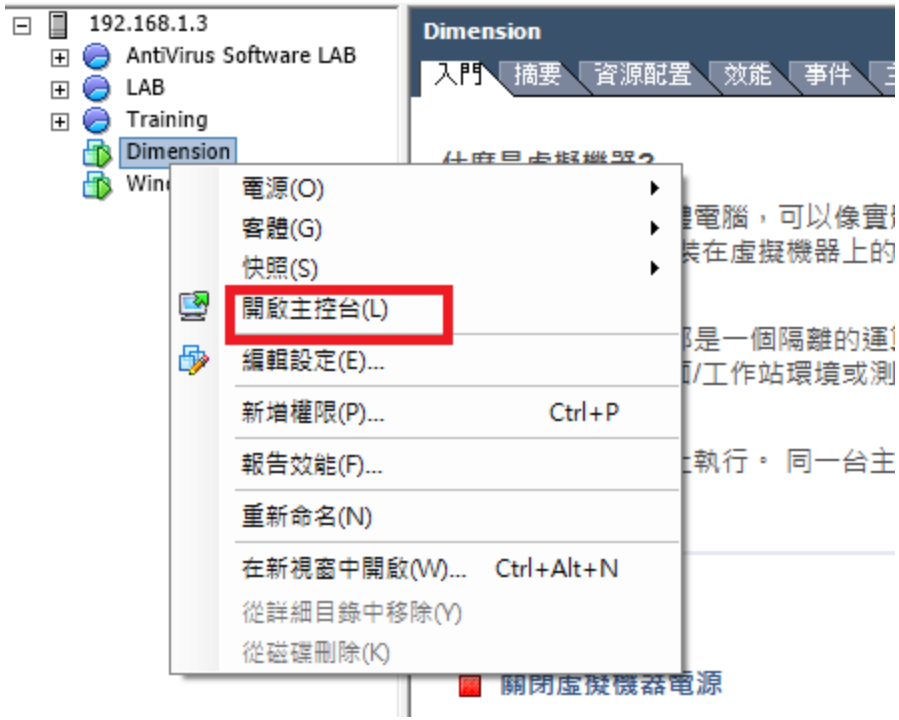
開始匯入 Dimension Report OVF



開啟Dimension Report OVF虛擬機器

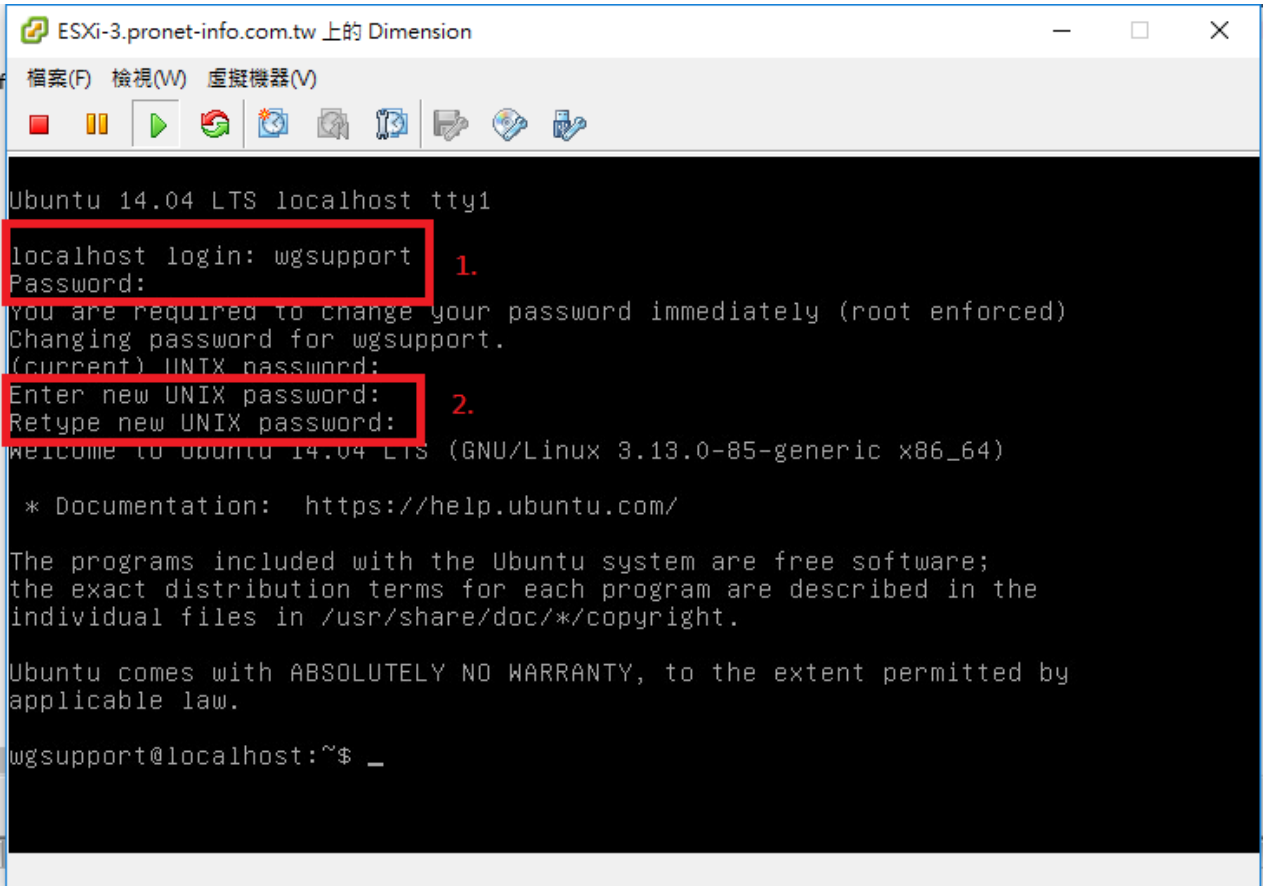
1. 點選匯入的機器
2. 點選開啟虛擬機器店源

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

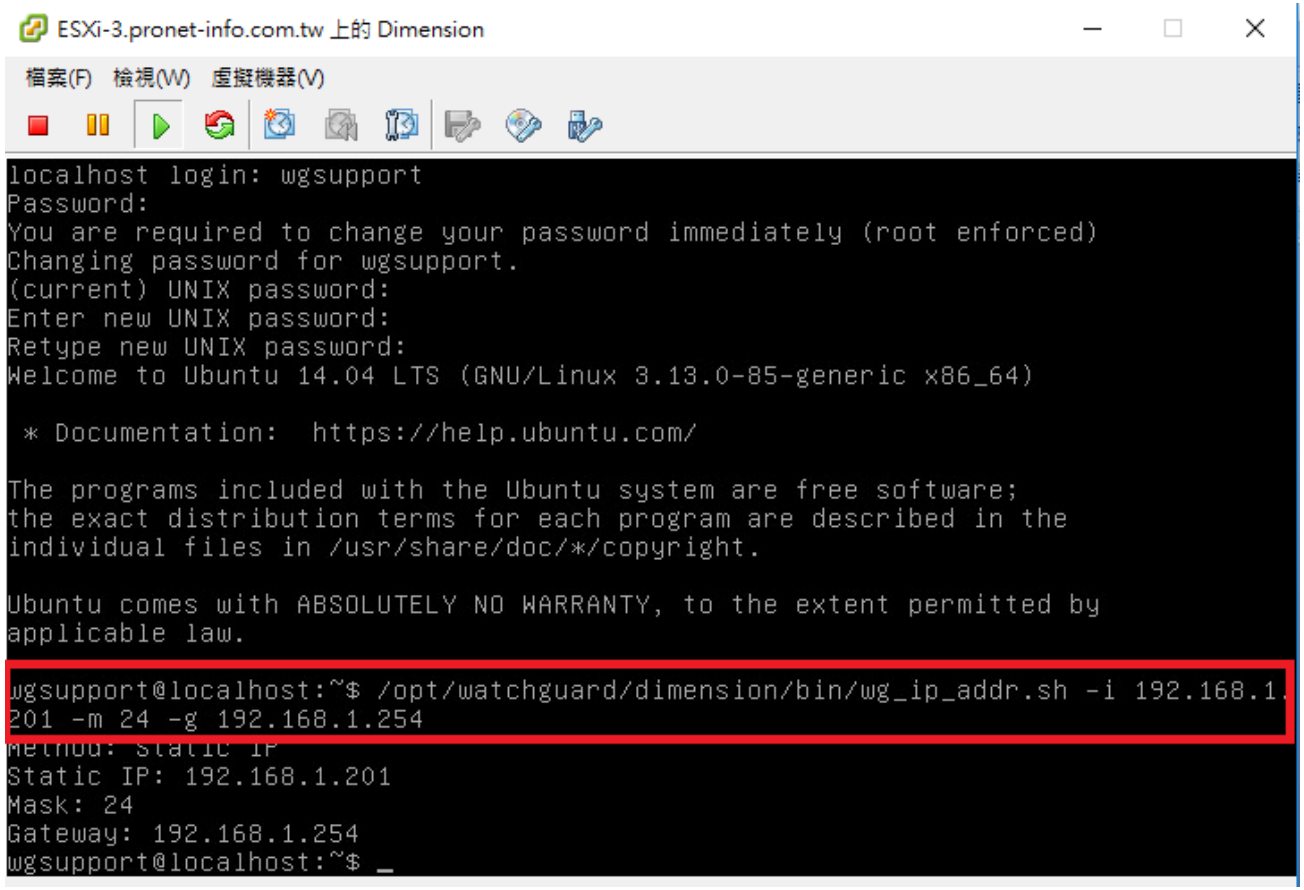


1. 輸入帳號密碼
2. 修改預設密碼

帳號：wgsupport

密碼：readwrite

修改Dimension Report IP



子網路遮罩

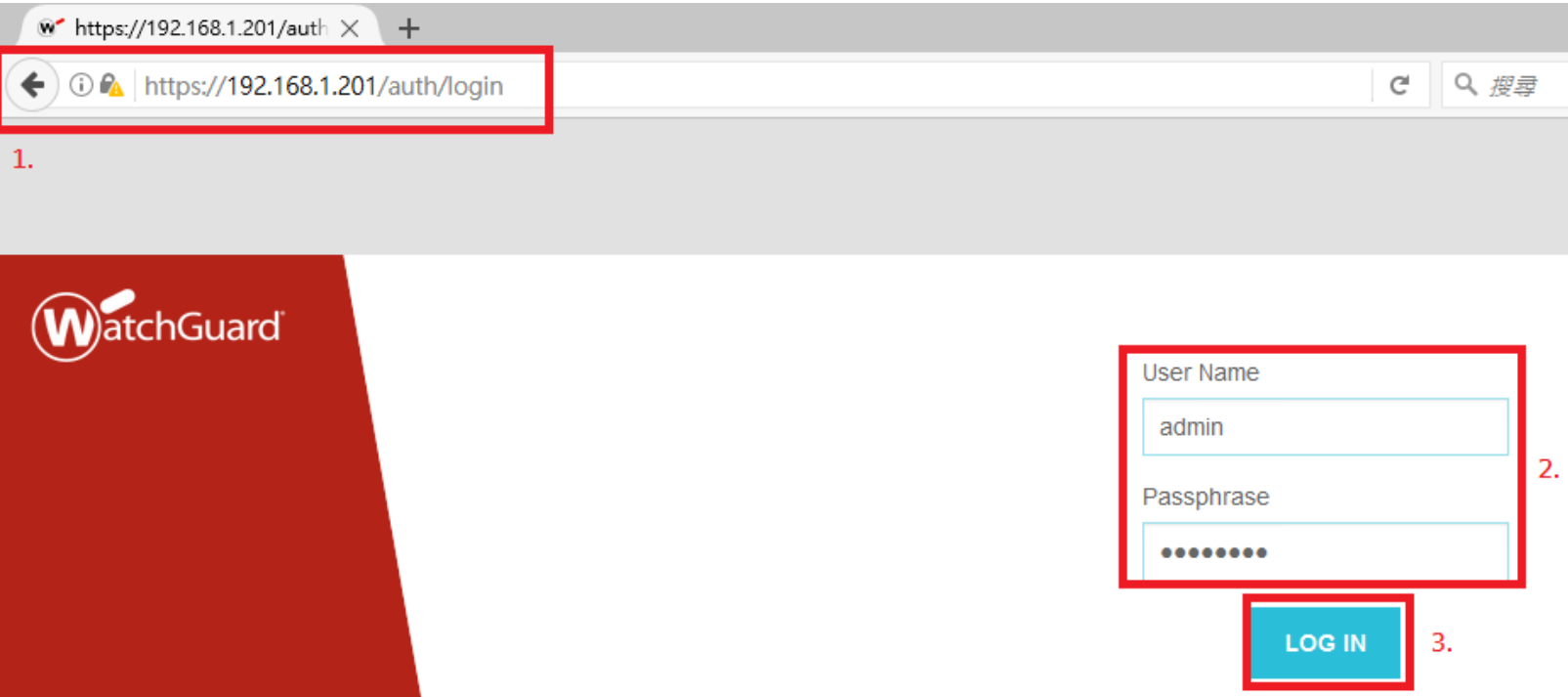
/opt/watchguard/dimension/bin/wg_ip_addr.sh -i 192.168.1.201 -m 24 -g 192.168.1.254

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



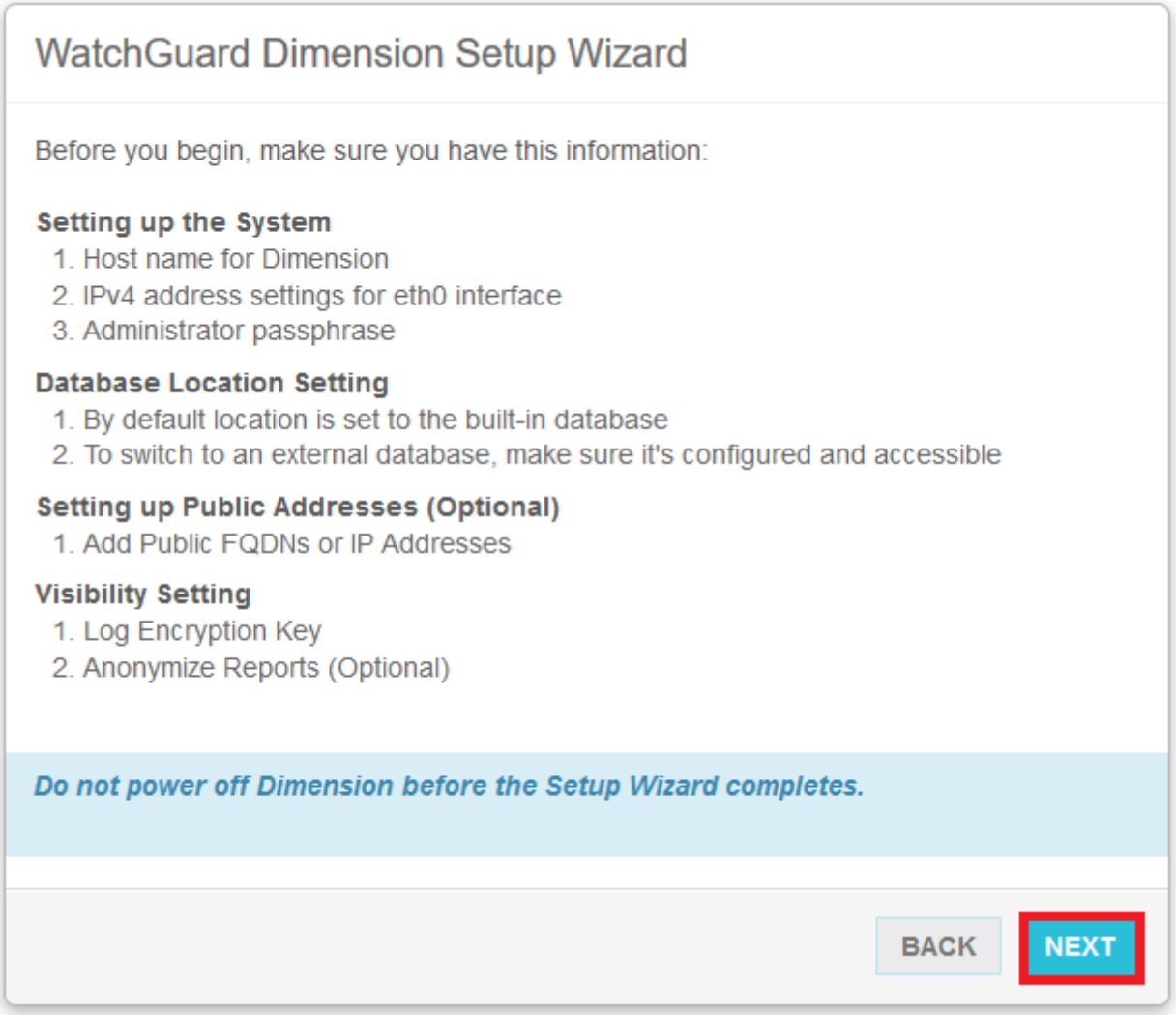
開啟瀏覽器

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

User Name : admin

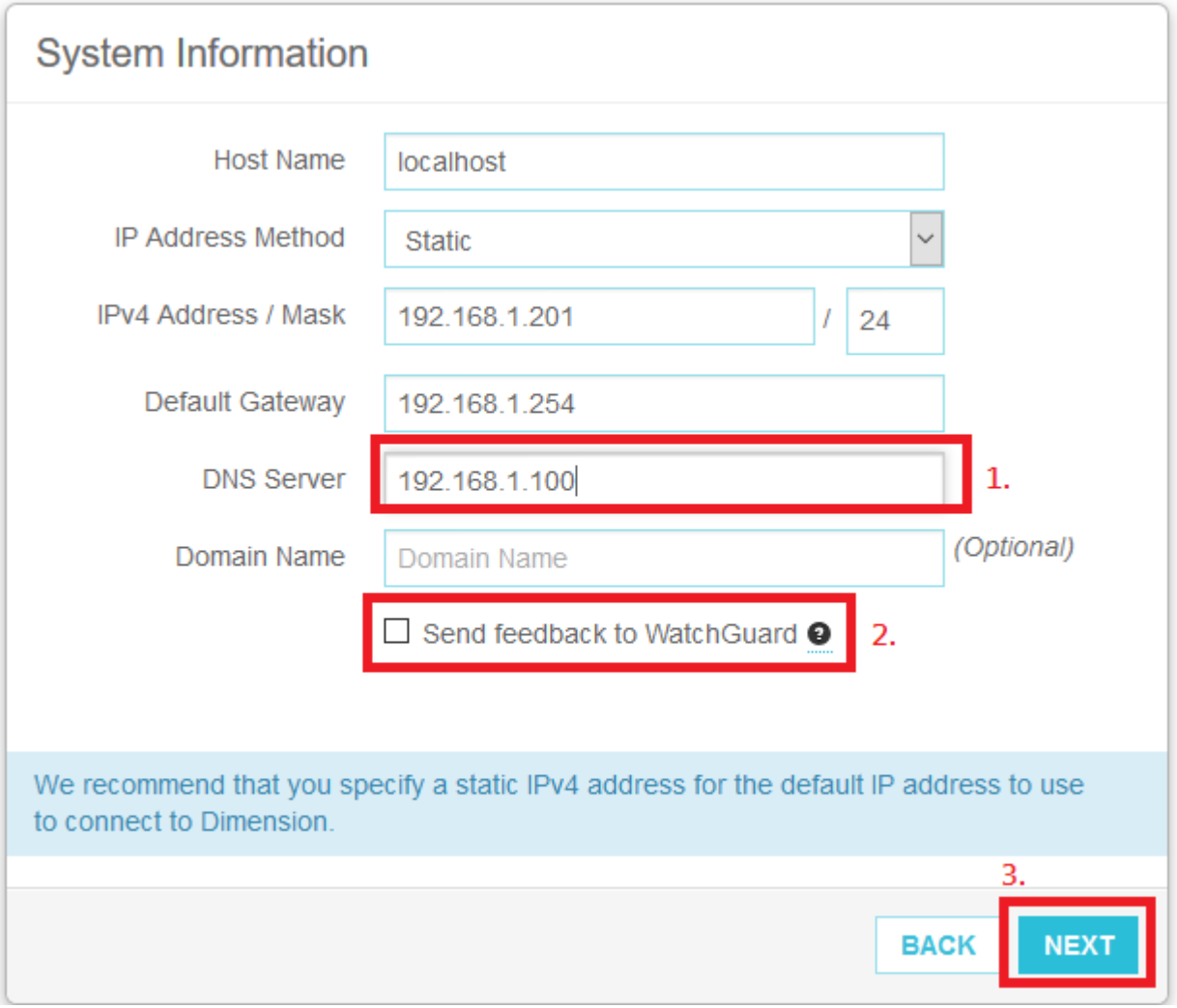
Passphrase : readwrite

啟動Dimension設定精靈



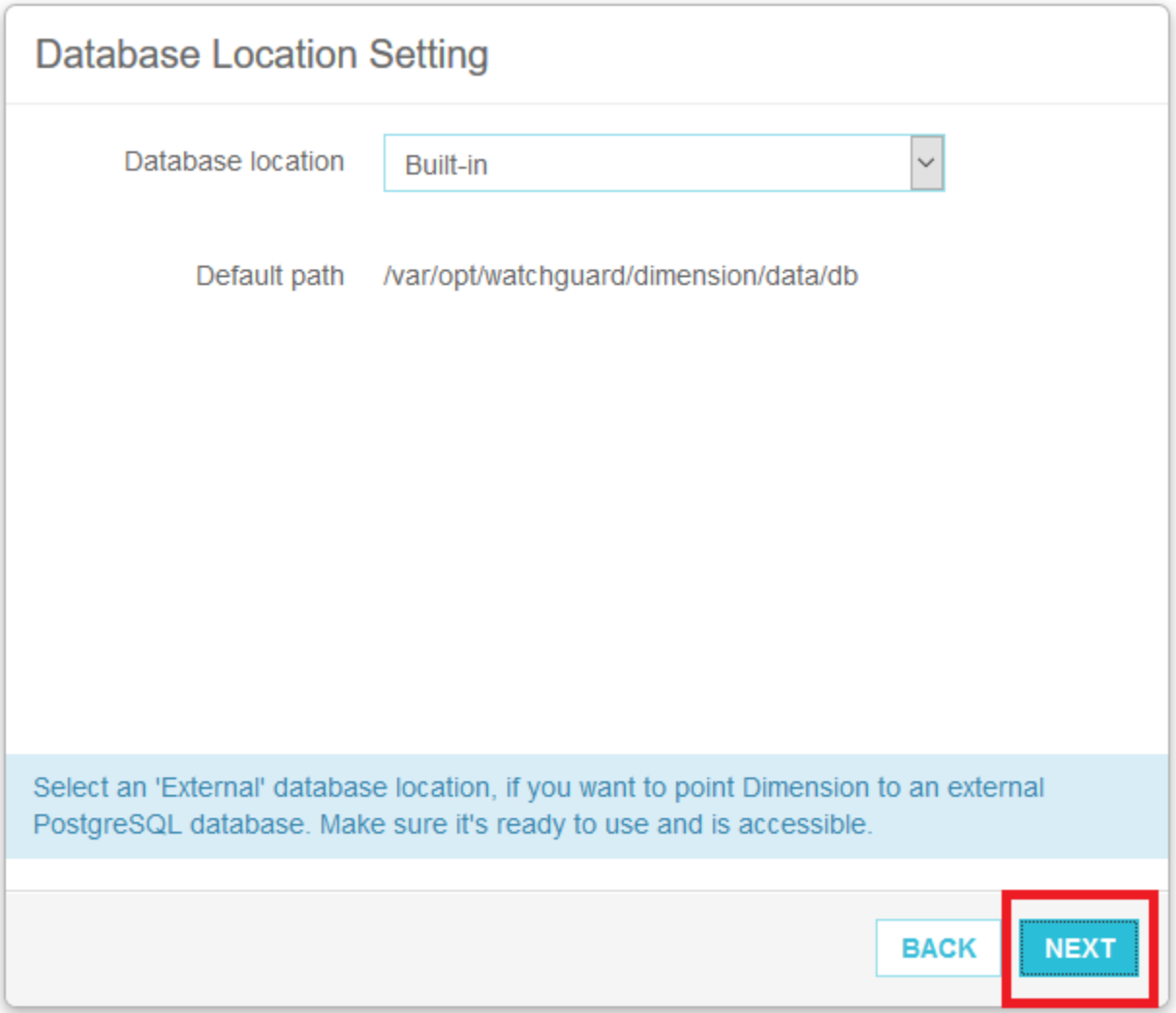
首次登錄系統會啟動Dimension設定精靈

更改Dimension網路設定

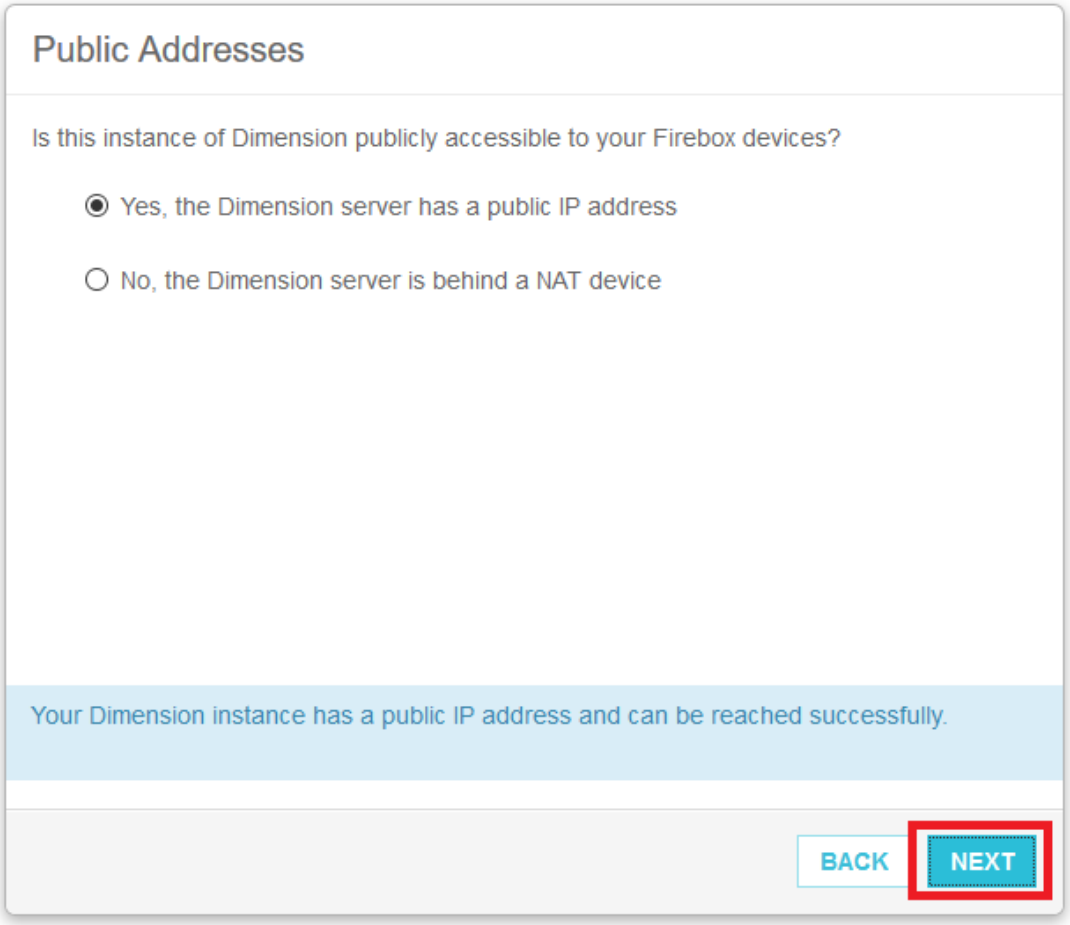


1. 輸入DNS IP
2. 將Send feedback to WatchGuard的勾拿掉
3. 點選Next

選擇Dimension Database位置

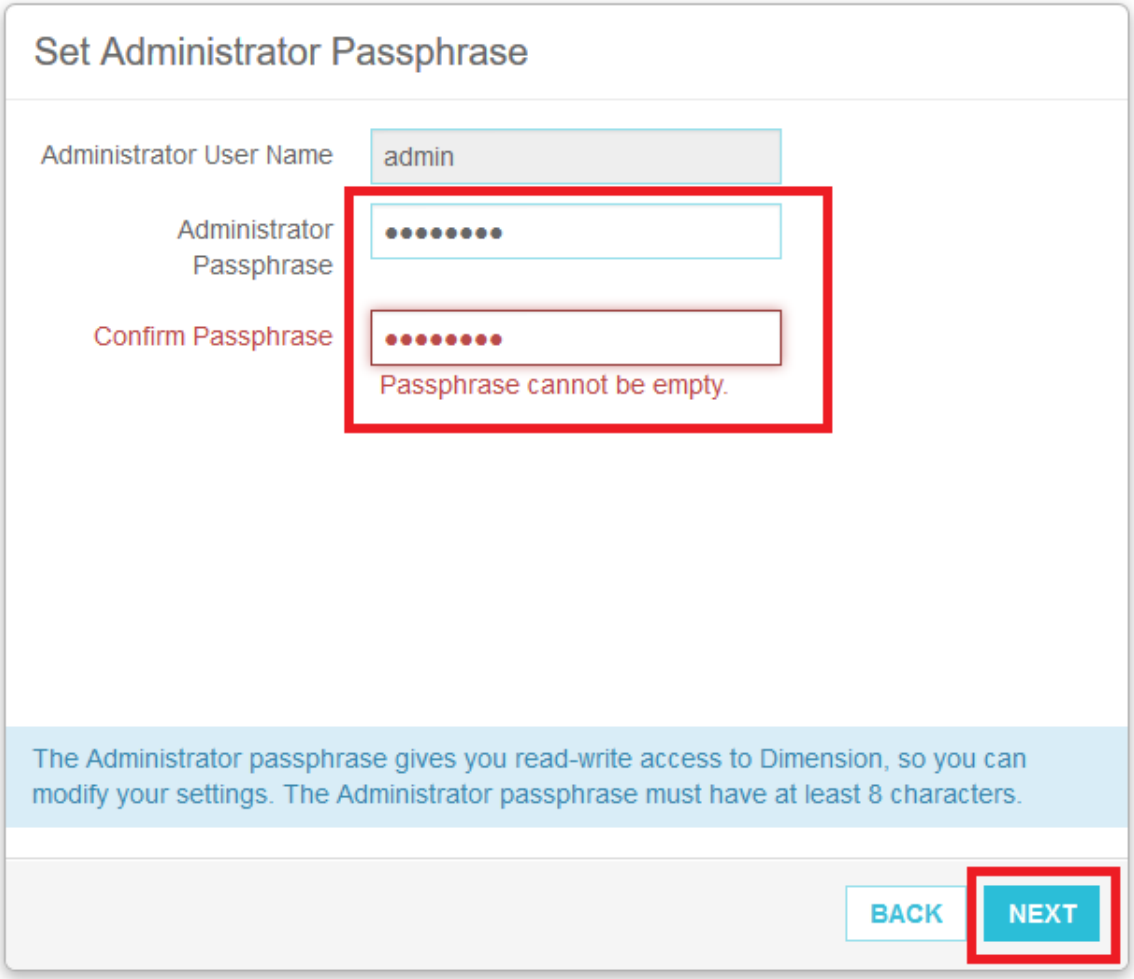


選擇Dimension IP型態



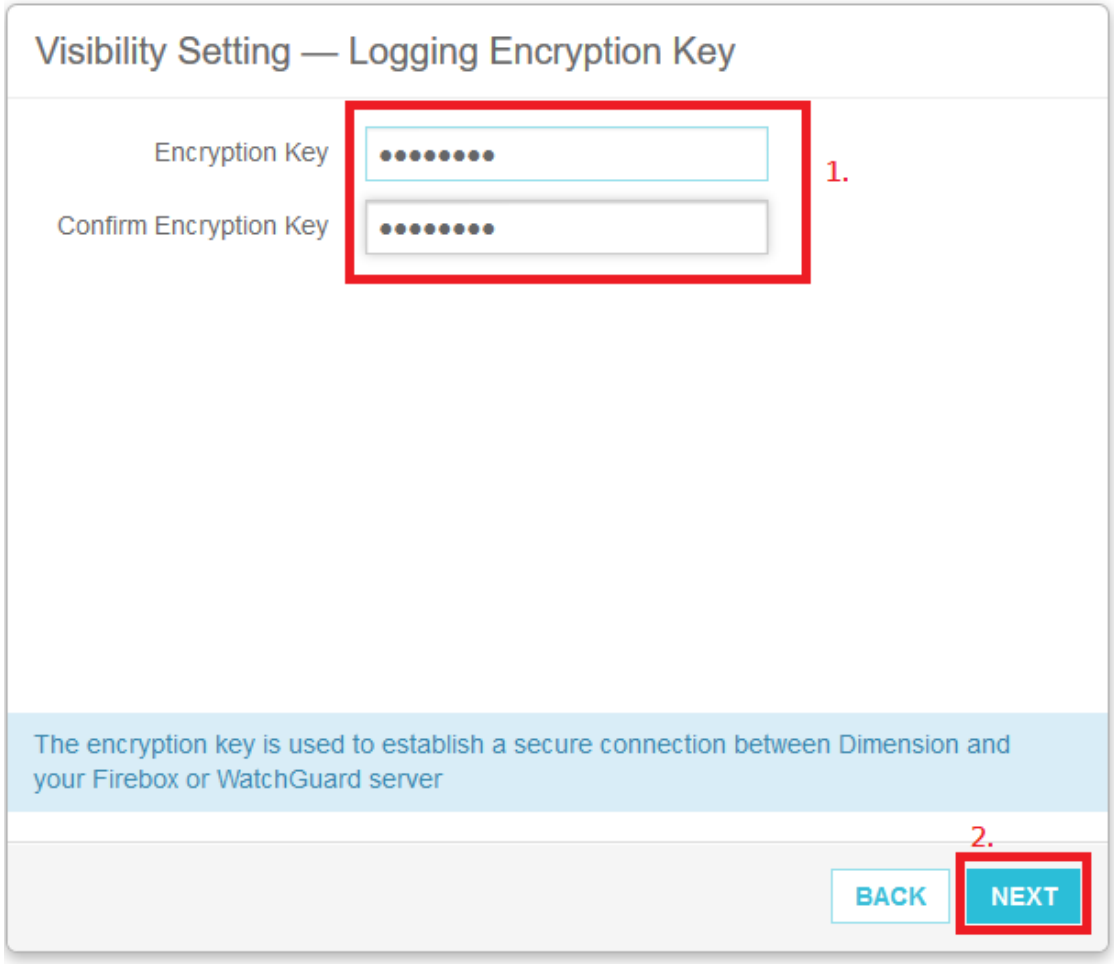
使用預設值，點選下一步

修改Administrator密碼



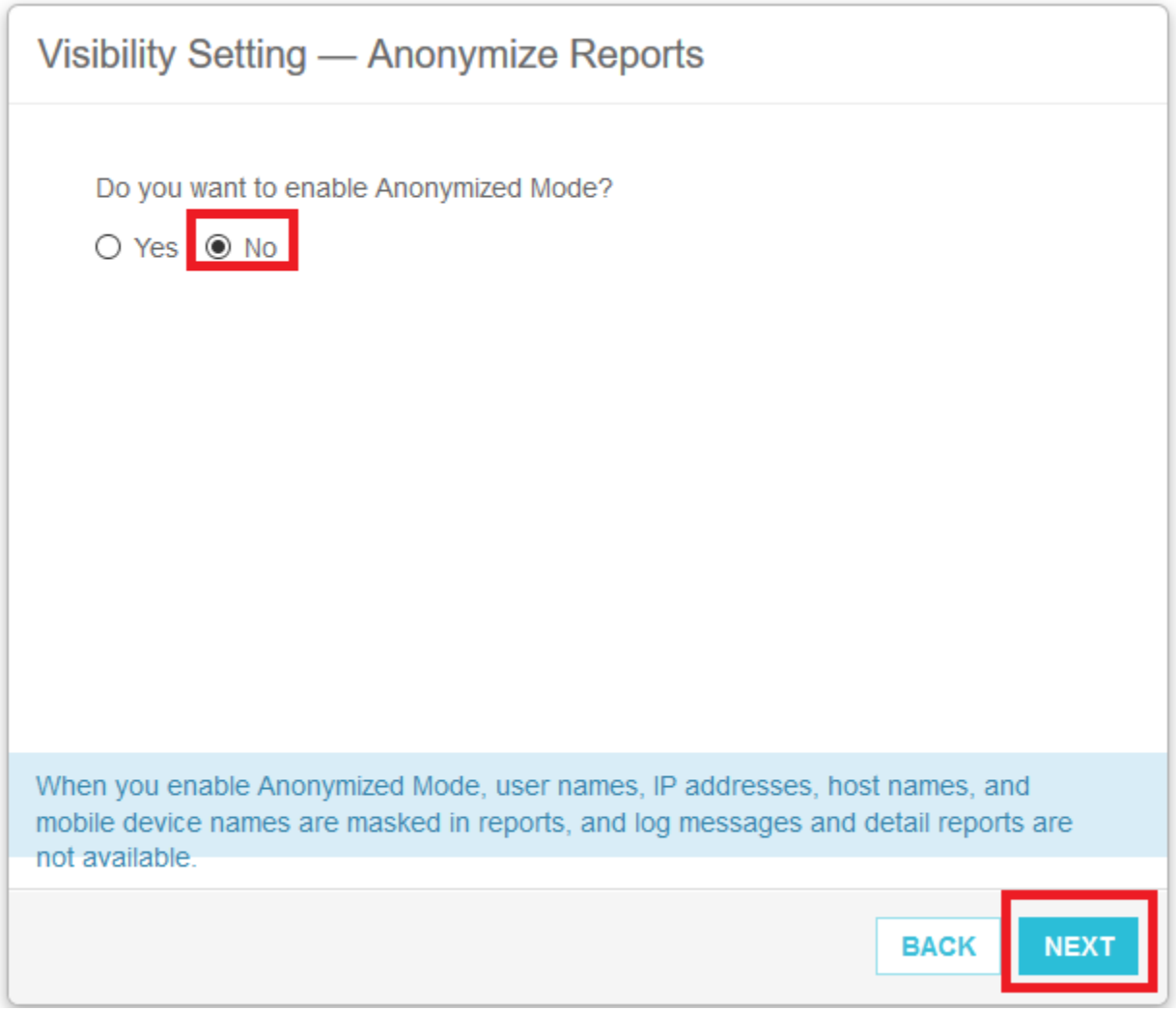
修改密碼後點選下一步

輸入Firebox和Dimension間資料加密的密碼

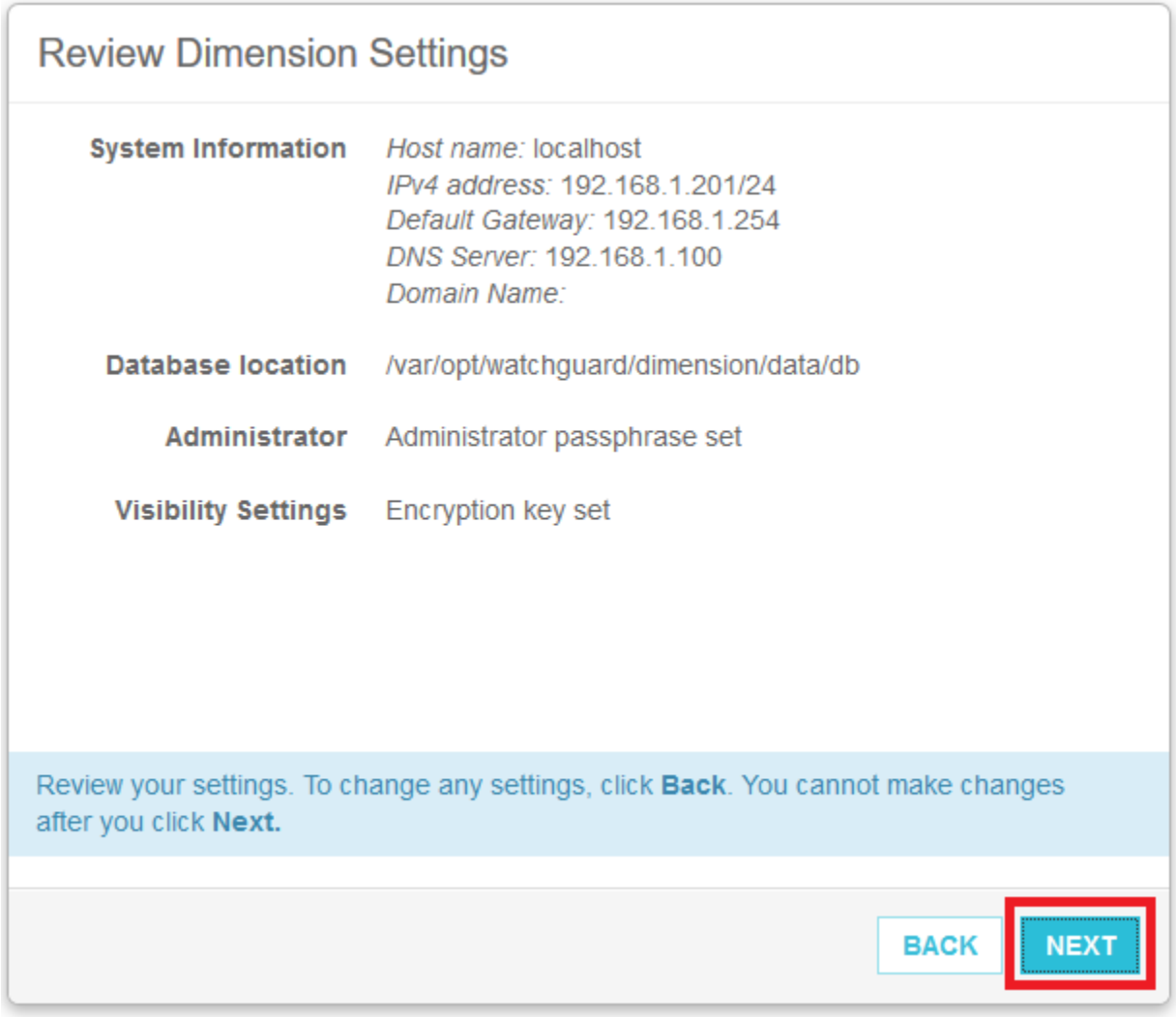


1. 輸入Firebox和Dimension間資料傳遞時，加密的密碼
2. 點選NEXT

匿名登錄設定

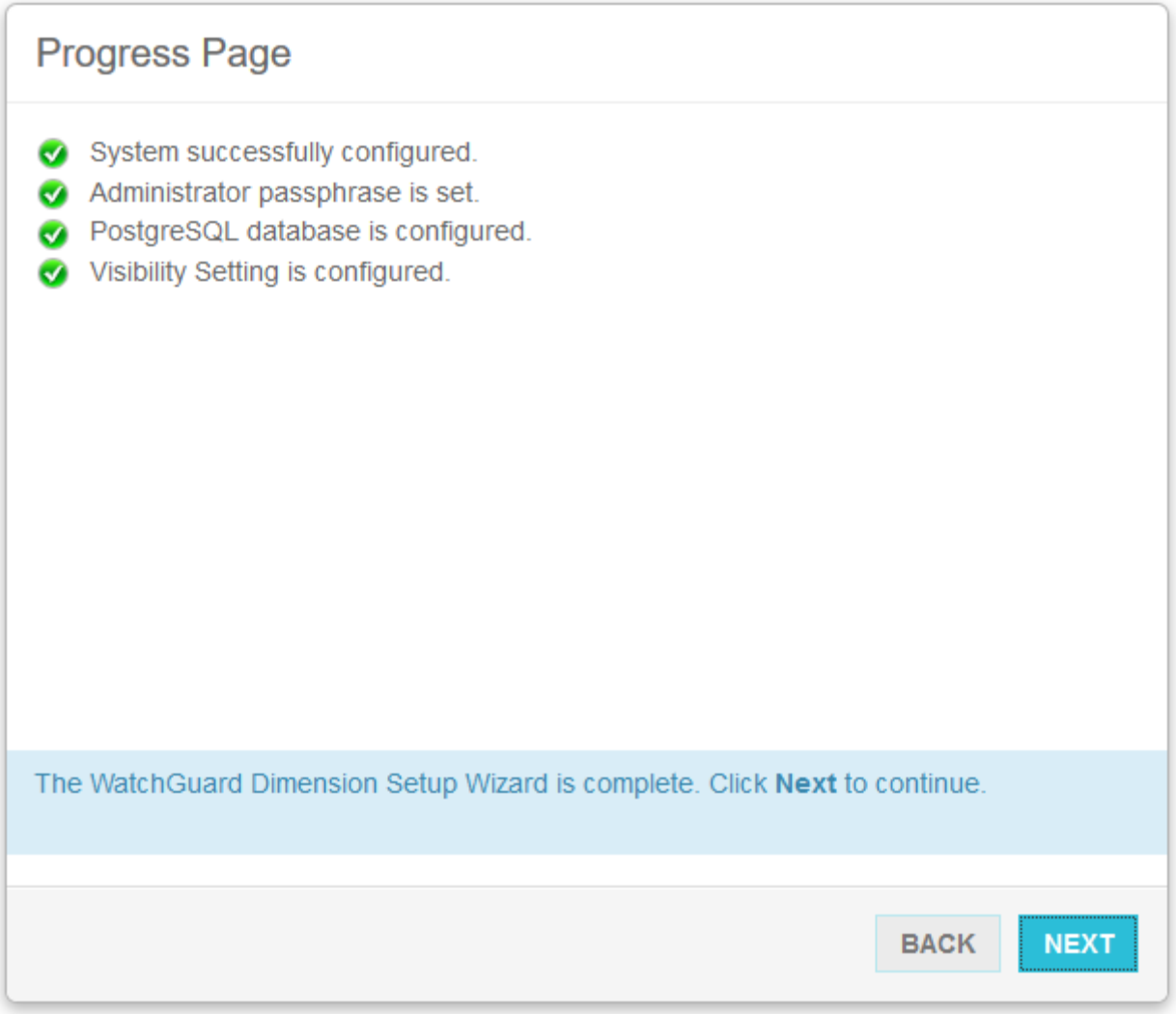

Visibility Setting — Anonymize Reports
Do you want to enable Anonymized Mode?
Yes
No
When you enable Anonymized Mode, user names, IP addresses, host names, and mobile device names are masked in reports, and log messages and detail reports are not available.
BACK
NEXT

確認Dimension設定

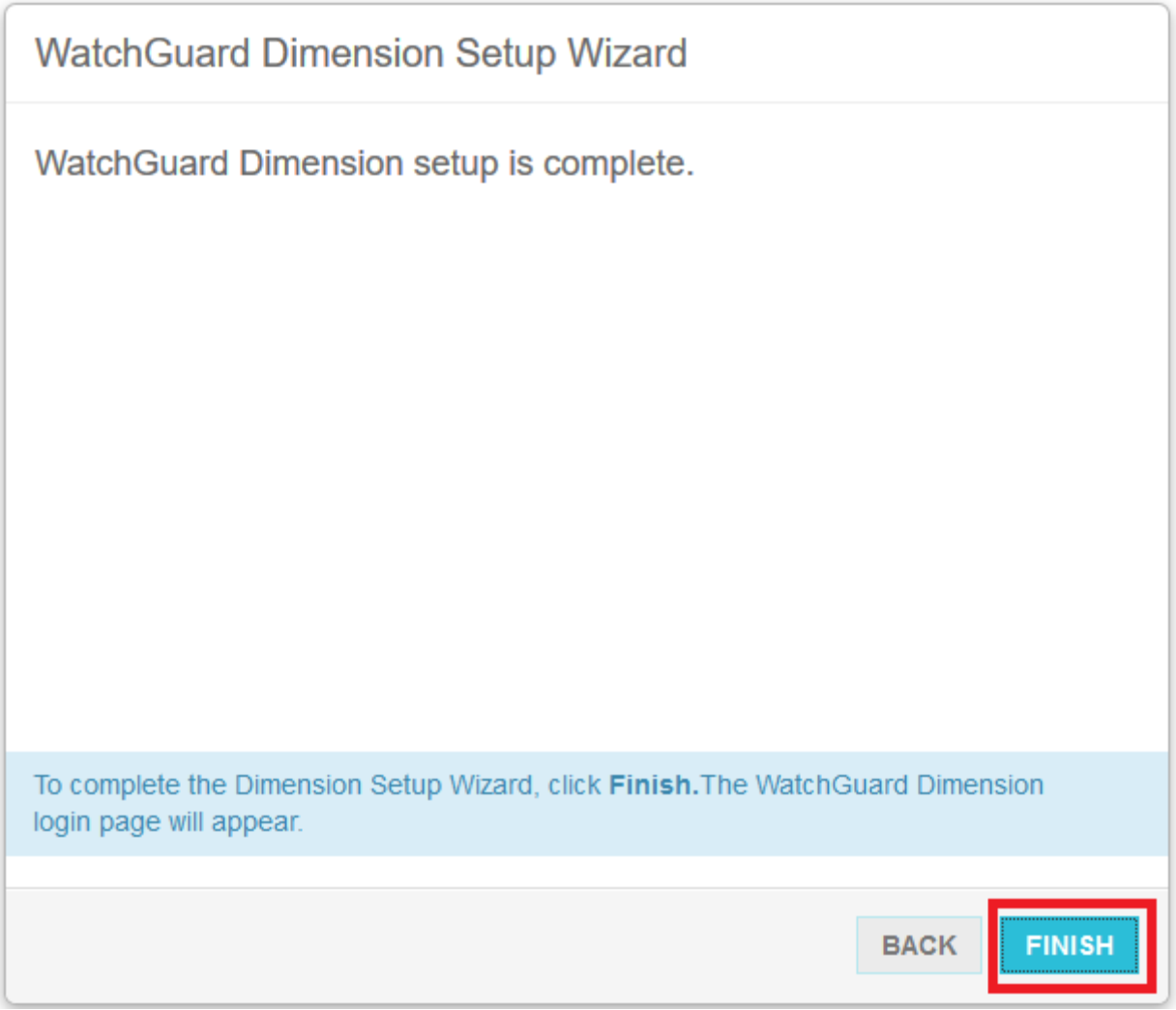


確認Dimension設定後點選NEXT

進行Dimension設定初始化

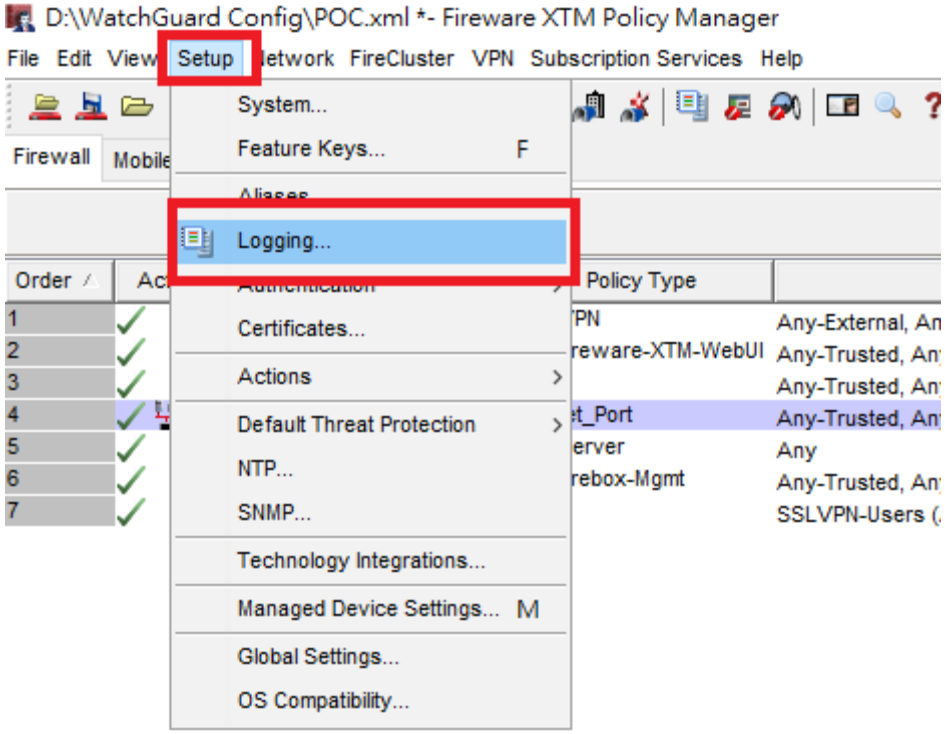


完成Dimension設定



點選FINISH完成Dimension設定

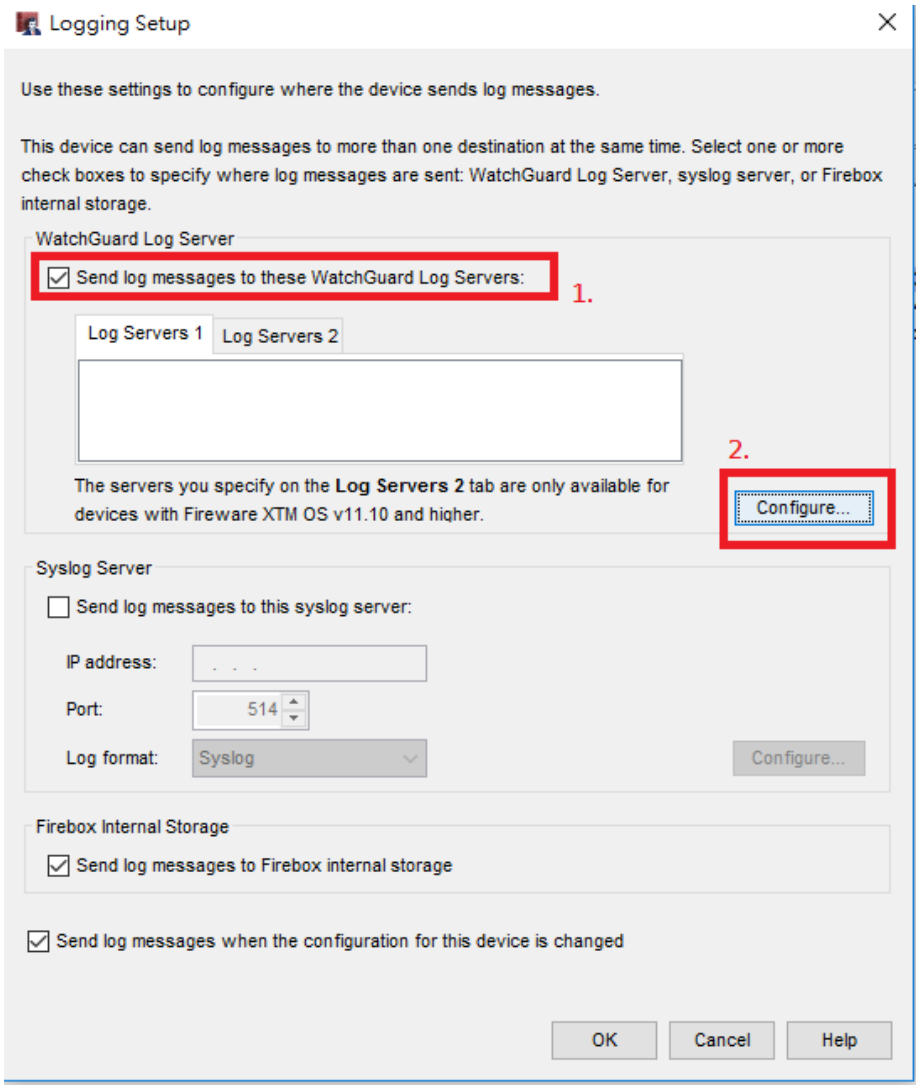
Firebox和Dimension同步設定



Step 1 :

Setup → Logging

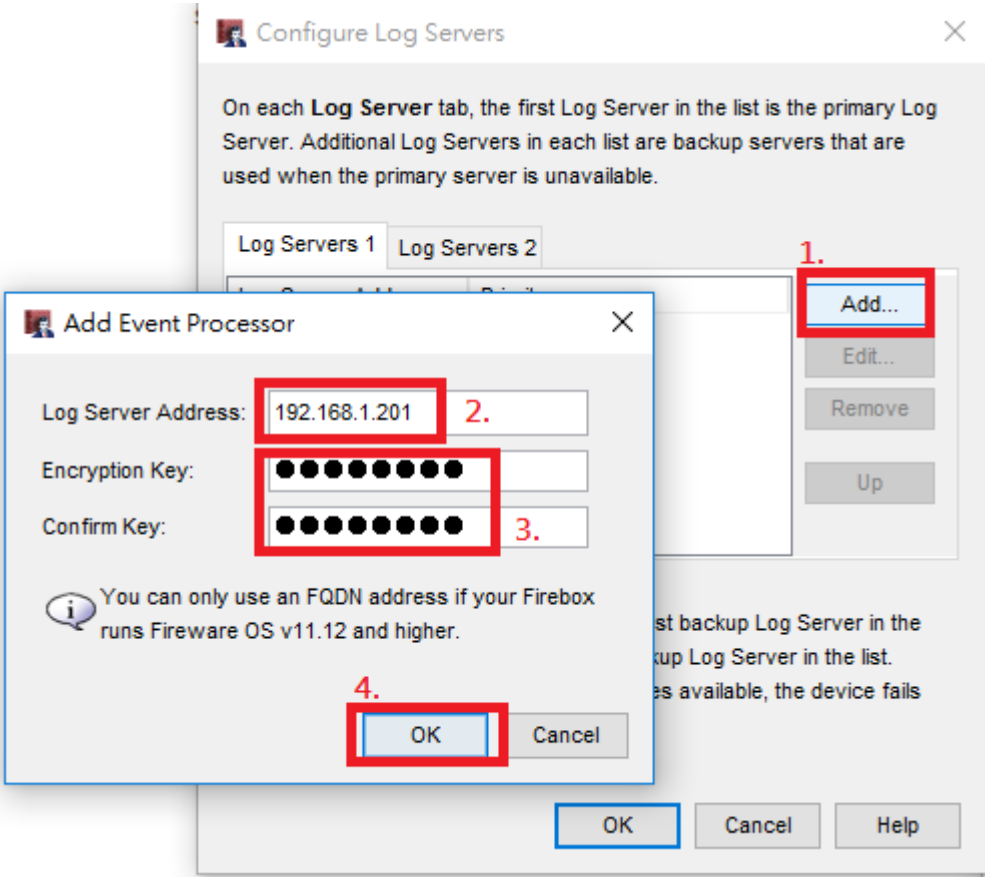
Firebox和Dimension同步設定



Step 2 :

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

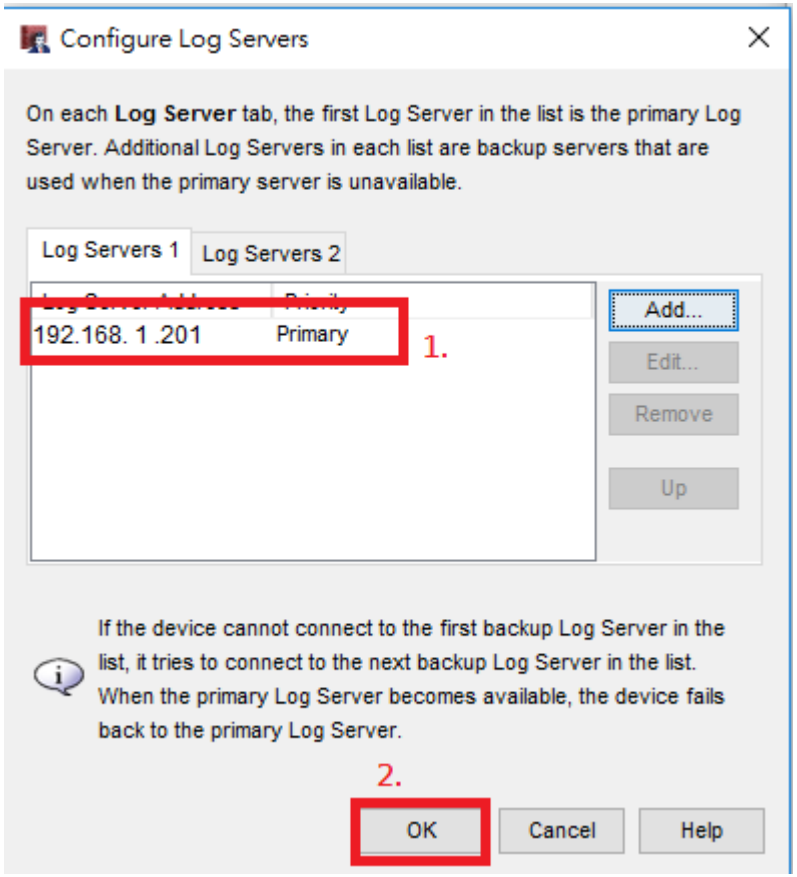
新增Dimension Report Server



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

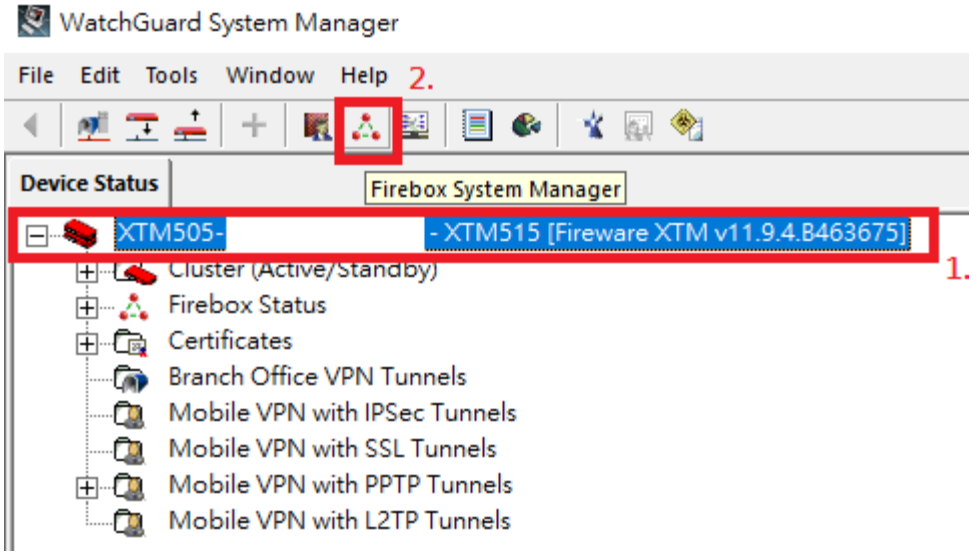


1. 確認Dimension IP設定
2. 點選OK

最後確認Firebox 和Dimension Server同步完成

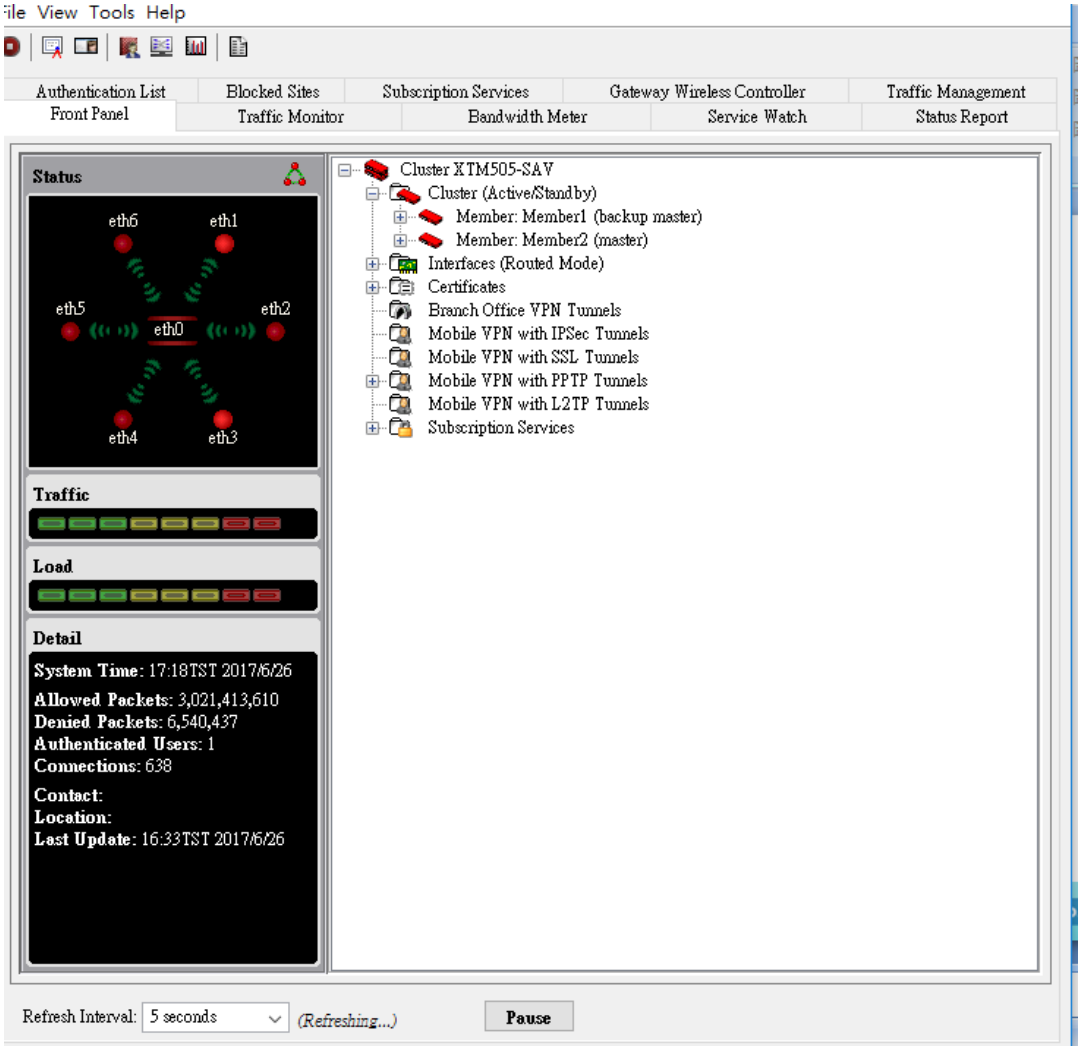
WatchGuard監看工具

開啟Firebox System Manager



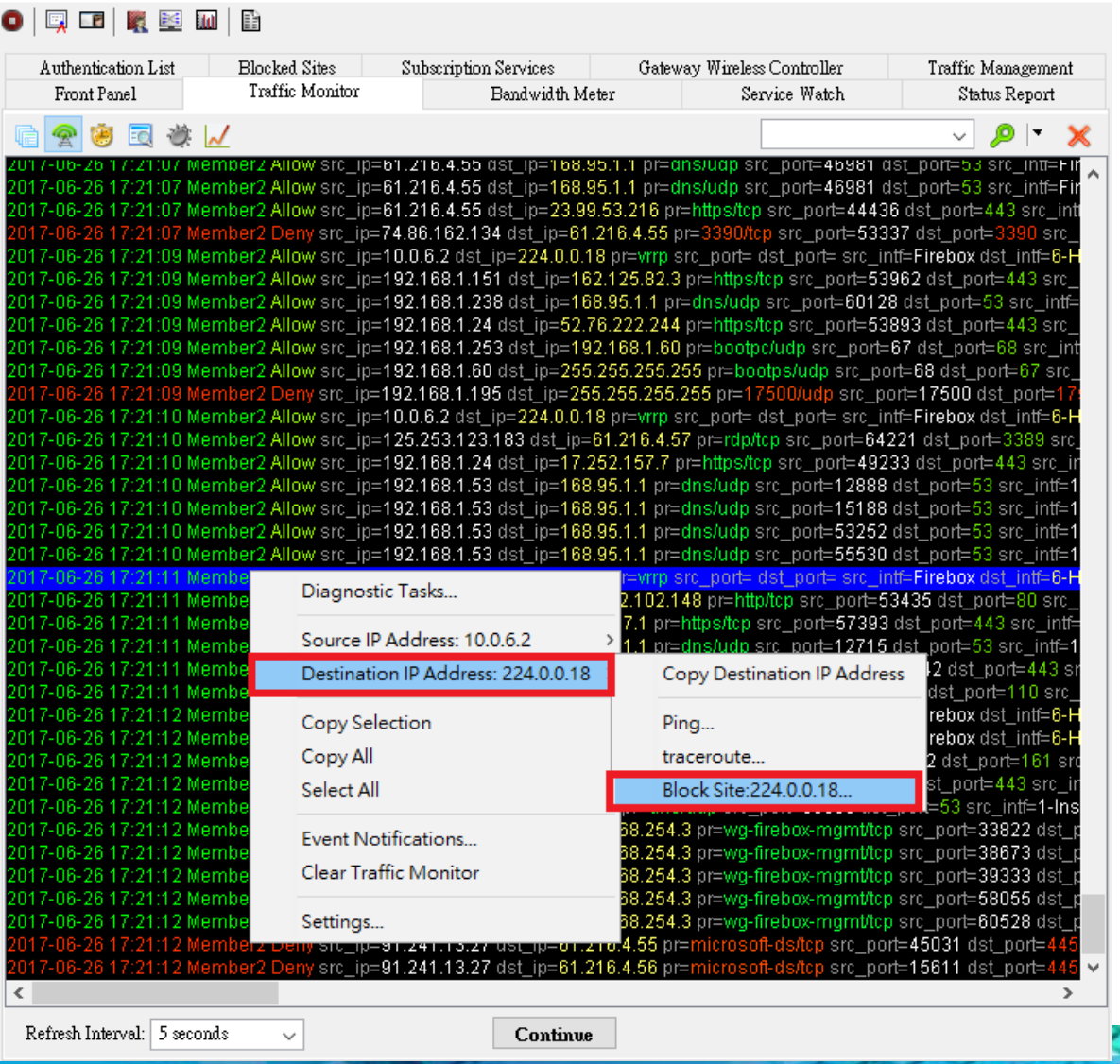
1. 點選防火牆
2. 點選Firebox System Manager

Firebox System Manager首頁



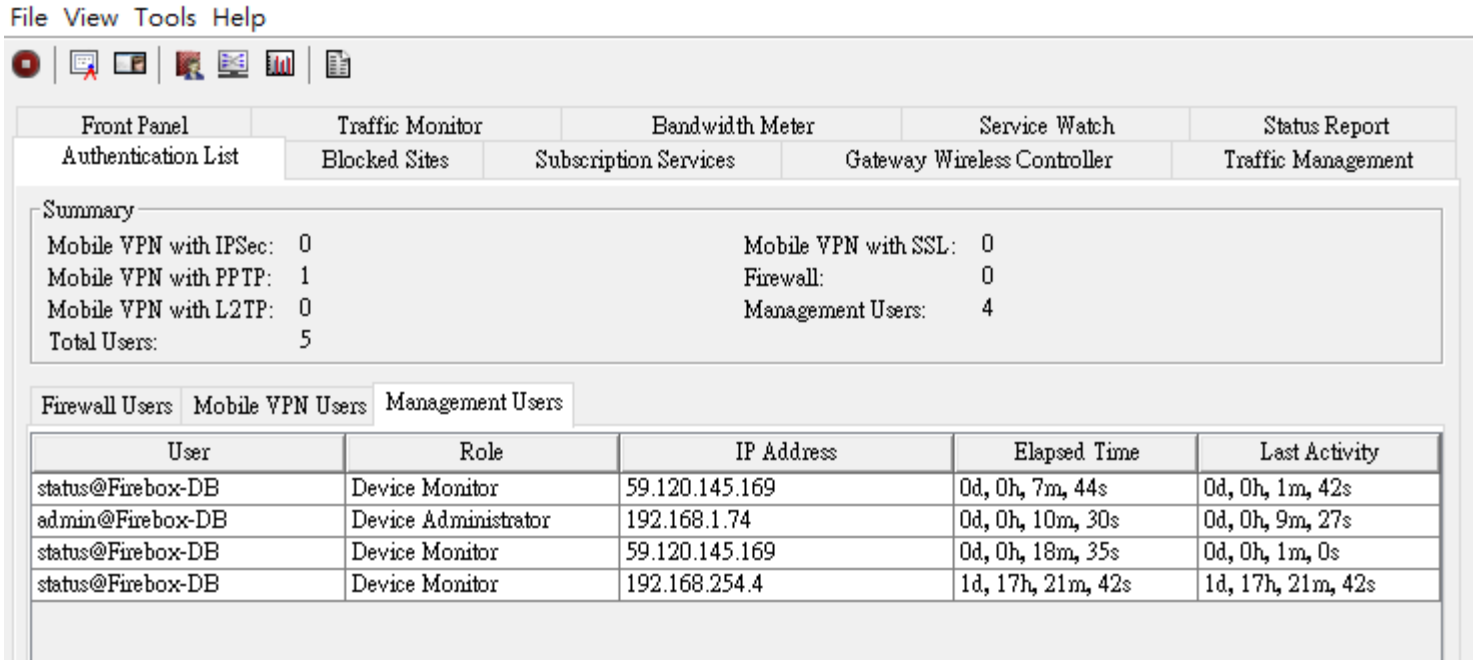
Firebox System Manager首頁顯示防火牆詳細資訊，包括開機時間、HA狀態、防火牆使用狀況、VPN使用者登錄狀態以及介面資訊.....等等。

Traffic Monitor



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



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。