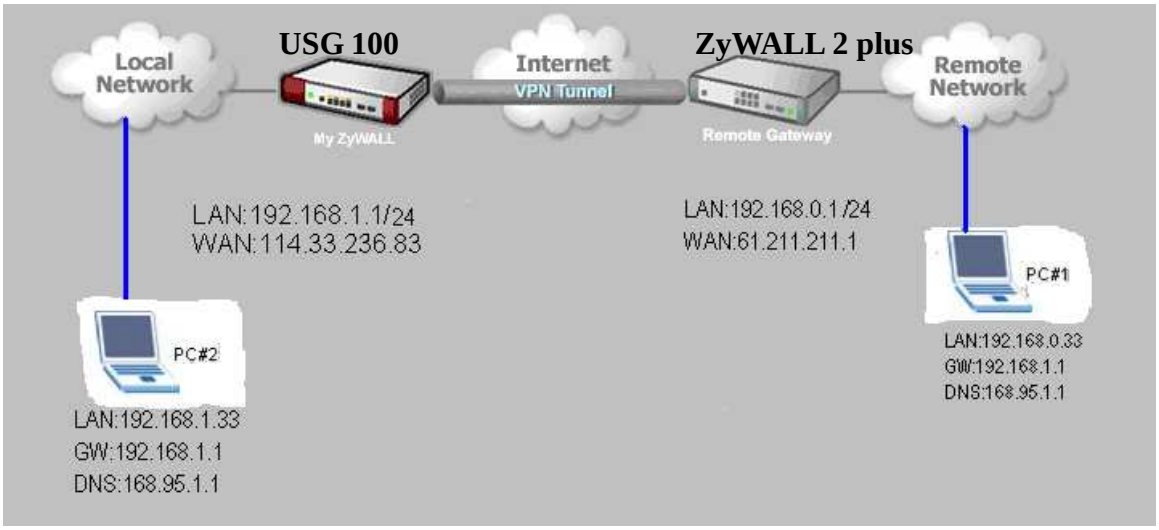
USG 100 VS ZyWALL 2 PLUS　　VPN IPsec 設定



虛擬私人網路利用現有的網路連線提供安全的通道傳輸,不需要租借昂貴的專線
一個安全的 VPN 通道必須組合一連串的加密認證方式,稽核跟規則開放 ZyWALL 所提供的 IPSec 爲標準的 IPSec 通訊協定, 包含一些標準的加密及認證方式讓您在網際網路上建立安全的加密通道.

設定前 注意事項

1. 兩端設備的 LAN 網段需不同，避免路由規則上的錯亂·
2. 兩端設備設定的加密方式需相同。
3. 兩端底下電腦的防火牆請暫時關閉。
4. USG100 的另一端設備，建議避開 USG 100 預設網段 192.168.1.0/24 ~192.168.3.0/24，若另一端無法改的話，且使用的是 USG 100 的中預設網段，且該網段 USG 100 並未使用的話，請於介面的 IP 值改設爲 0.0.0.0，避免路由發生錯誤。

設定值

設定相關所需要 USG 100 與 ZyWALL 2 plus 的 WAN 及 LAN & IPsec VPN

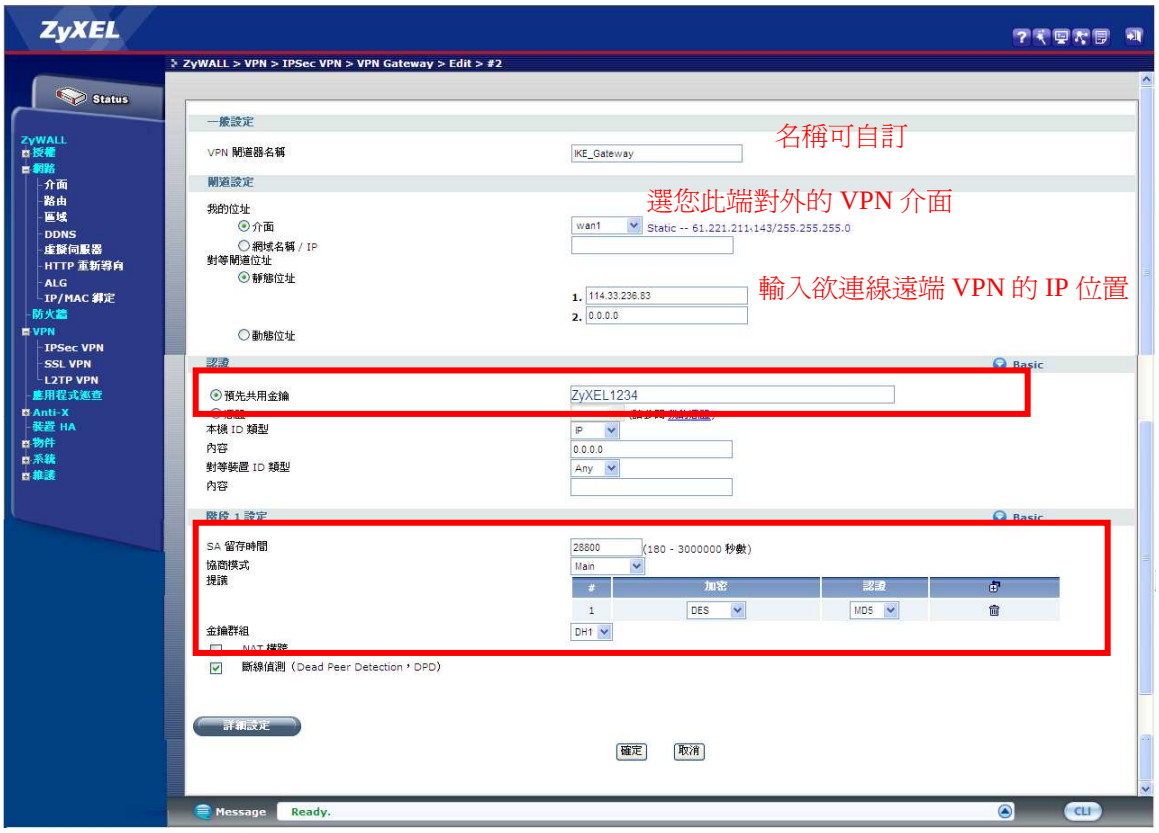
USG 100 端的設定

步驟 1：查看 WAN 及 LAN 的設定值，點選“網路”→點選“介面”→點選“狀態”

步驟 2：ZyWALL →點選“VPN”→點選“IPsec VPN”→點選“VPN 閘道器“→按下“新增”

步驟 3：設定一個名稱來識別此通道要連線對外的 VPN 通道

紅色框框爲兩端設備皆需相同的值。



步驟 4：ZyWALL →點選 “VPN” →點選 “IPsec VPN” →點選 “VPN 連線”→按下 “新增”

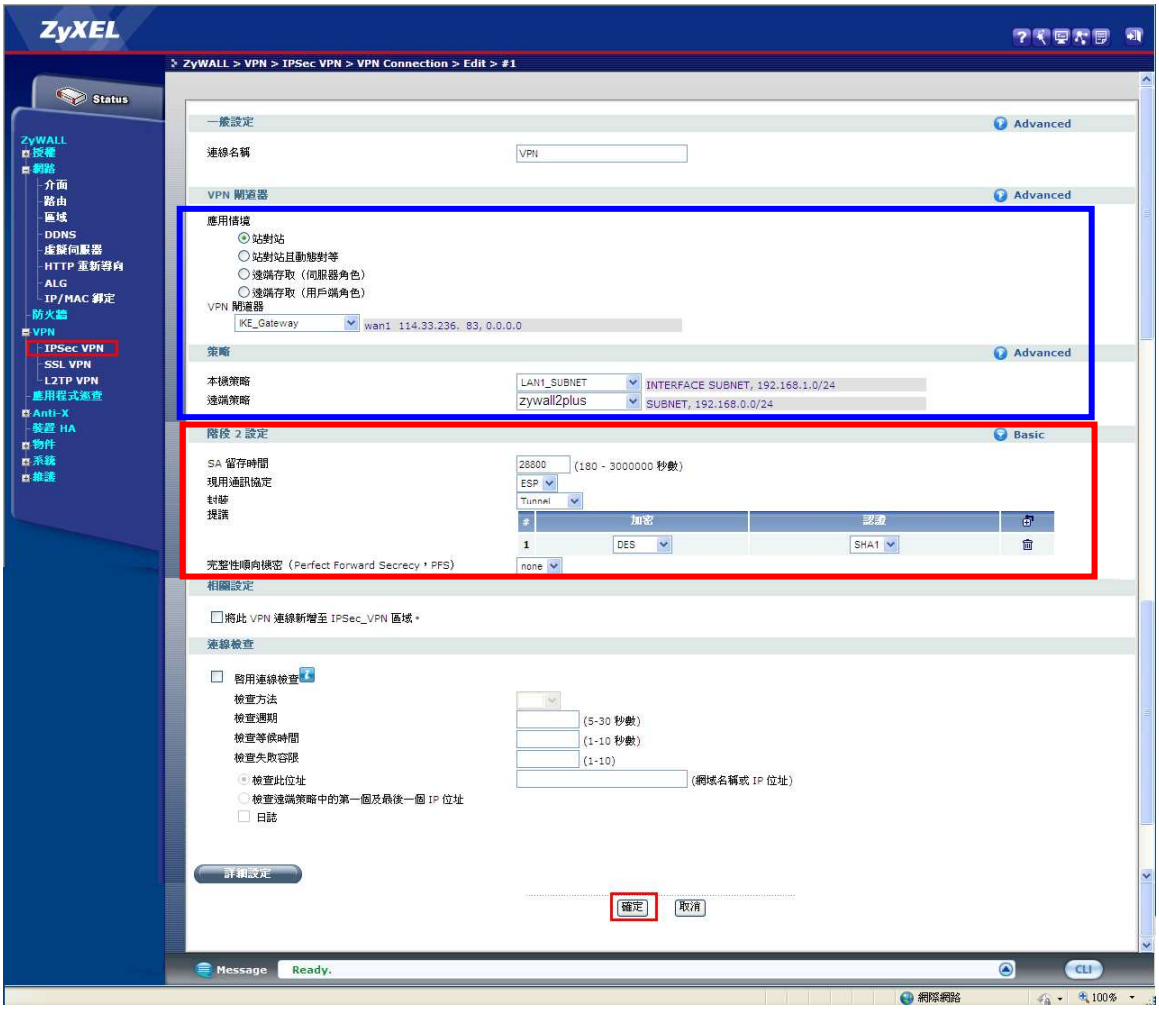
步驟 5：設定連線規則，點選“站對站 Site to Site”，選擇已建立的 VPN 閘道器。

本機策略：選擇允許本端 LAN 網路可存取遠端 VPN 的網段(USG 50H LAN)

遠端策略：選擇遠端網路可存取網段位置 (ZyWALL 2 PLUS LAN)

紅色框框爲兩端設備皆需相同的值。

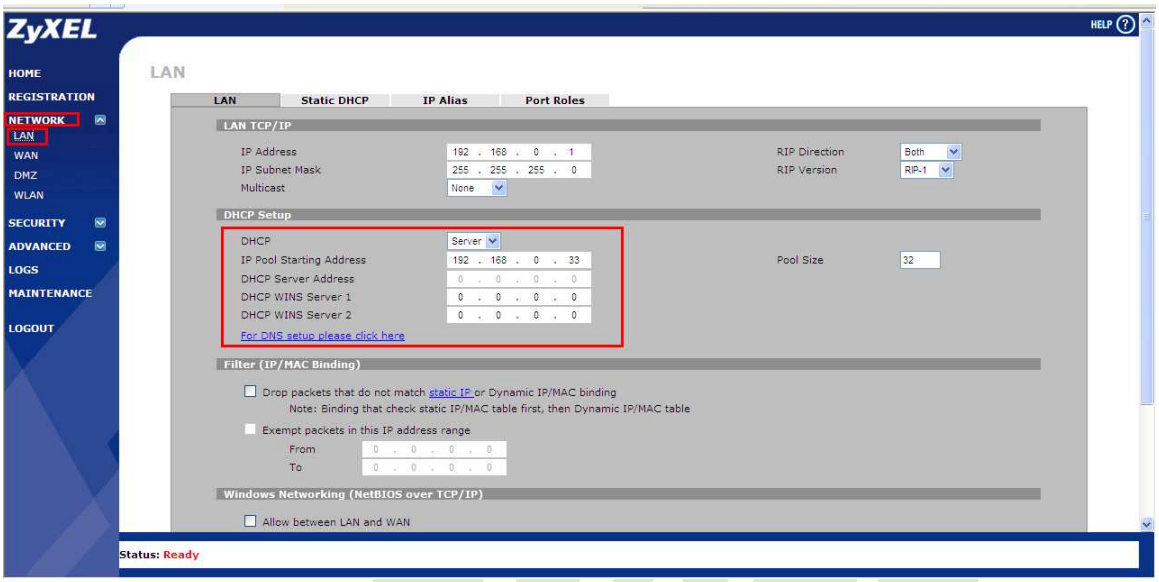
最後按下**套用**即完成 USG 100 端的設定。



ZyWALL 2 PLUS

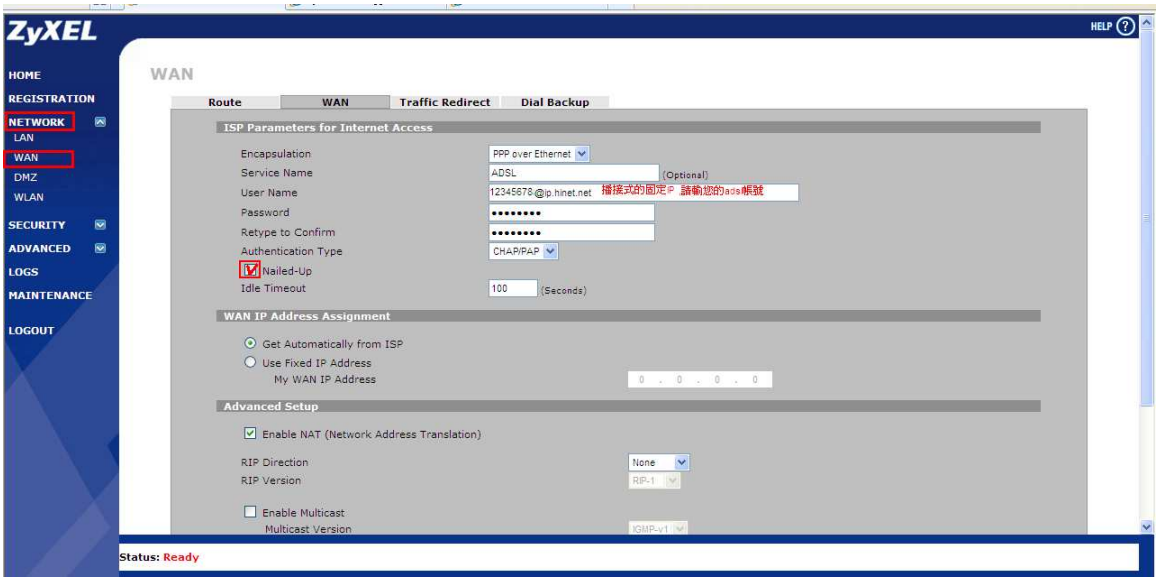
步驟 6：查看 LAN 的設定值，點選 NETWORK→點選 LAN 端。

避開原本的 192.168.1.1 的網段。

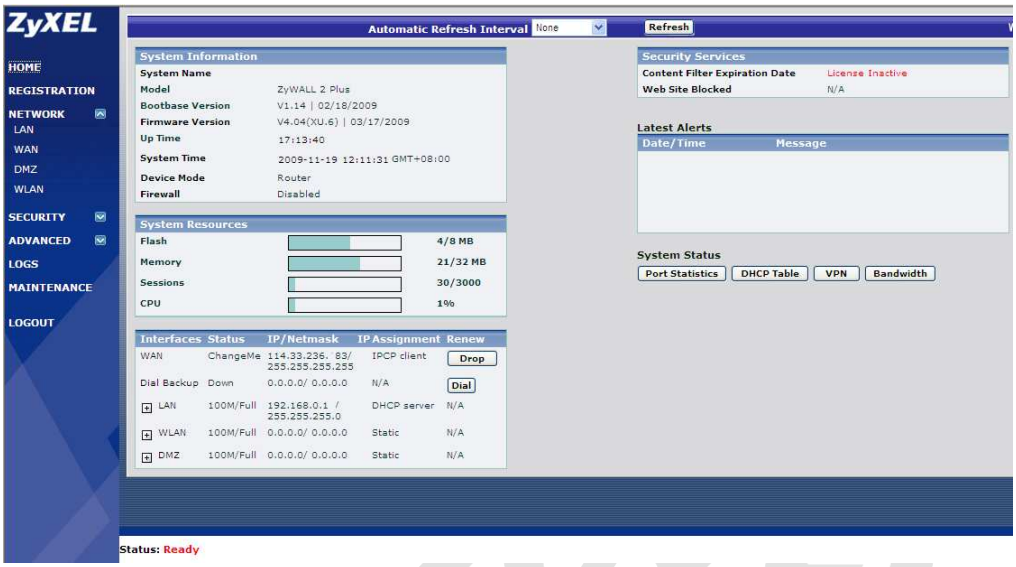


步驟 7：查看 WAN 的設定值，點選 NETWORK→點選 WAN 端。

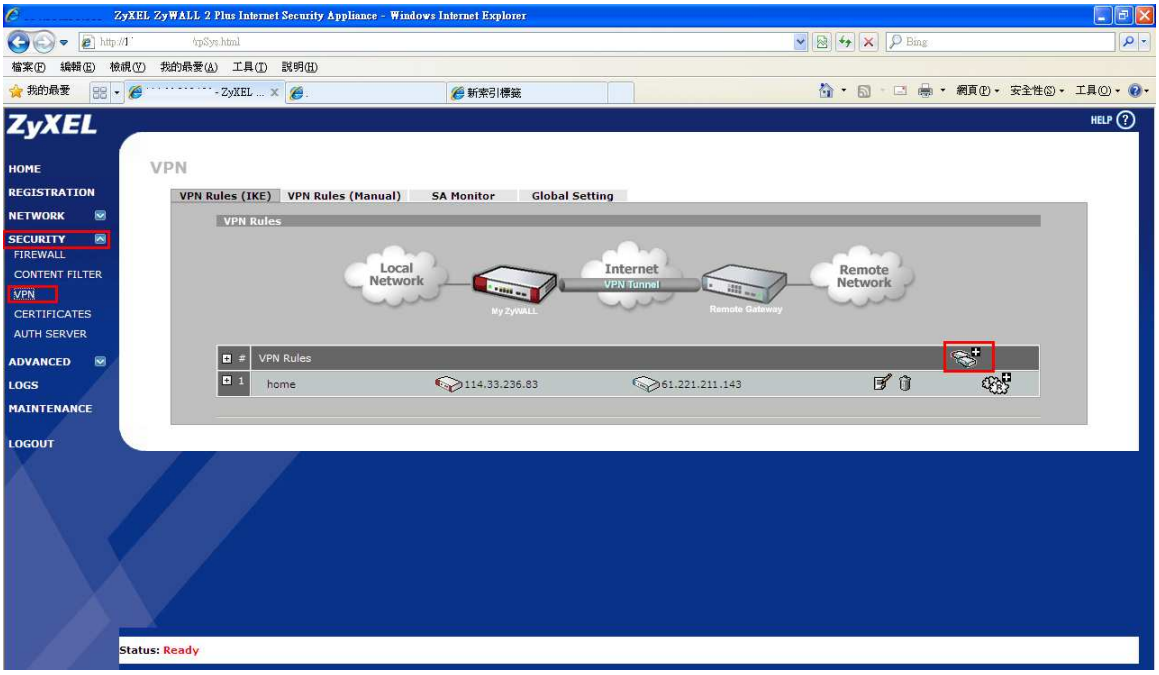
此範例爲播接式的固定 IP 制的對外網路。



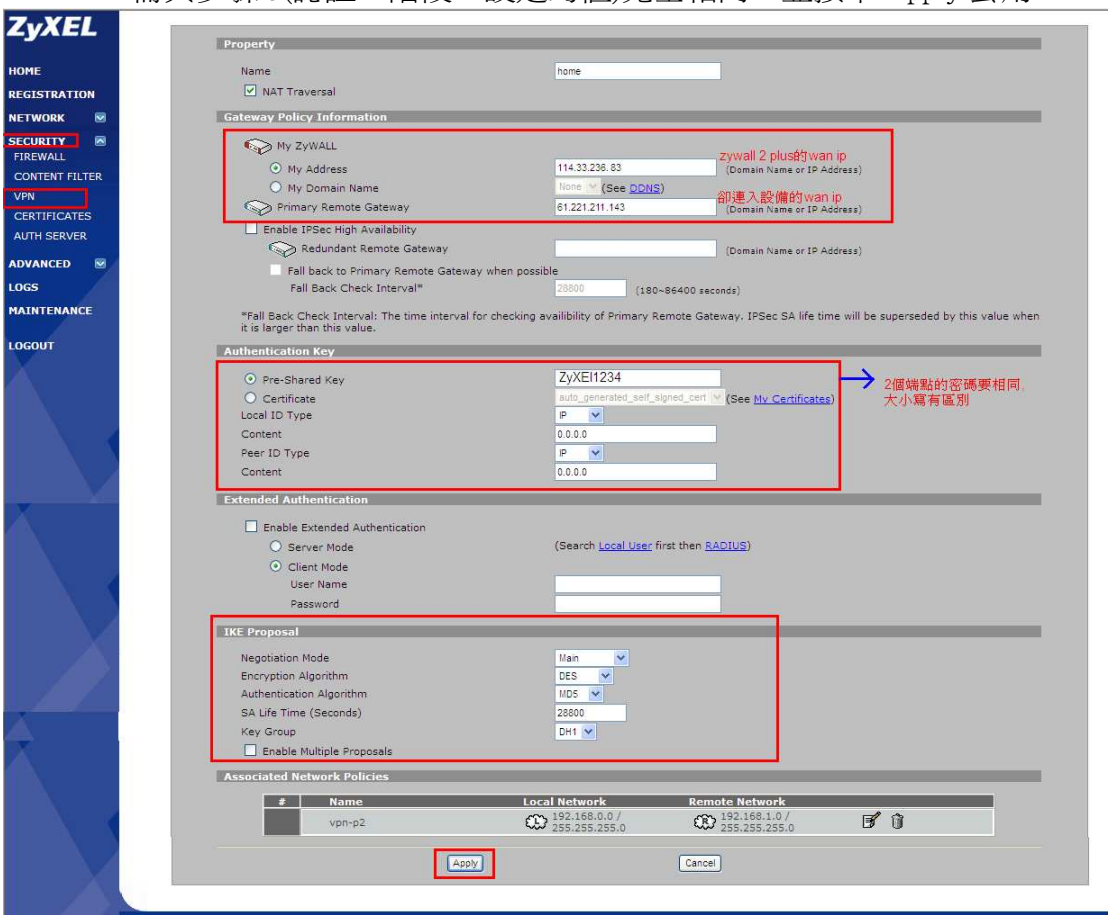
步驟 8：查看 WAN IP 是否正確取得。



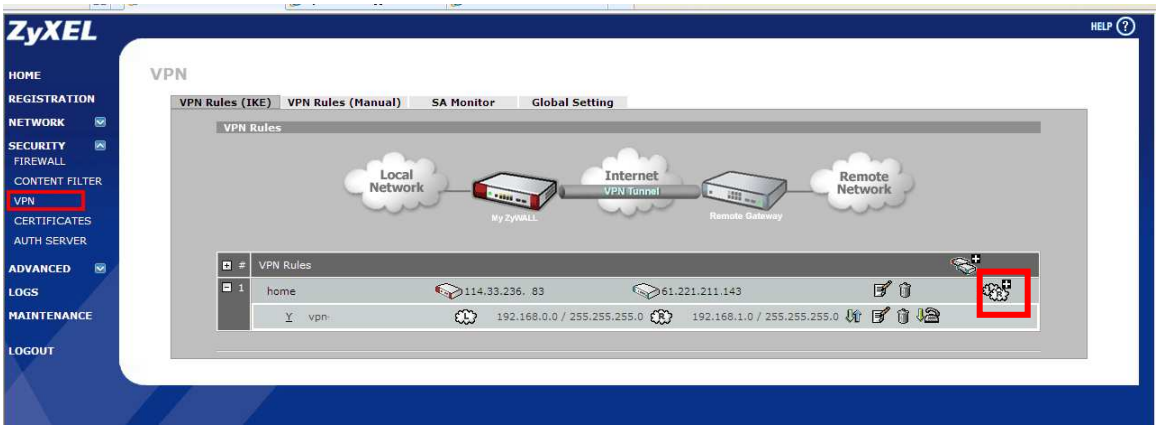
步驟 9：VPN 建立通道，點選 SECURITY→點選 VPN→按下 “新增”  。



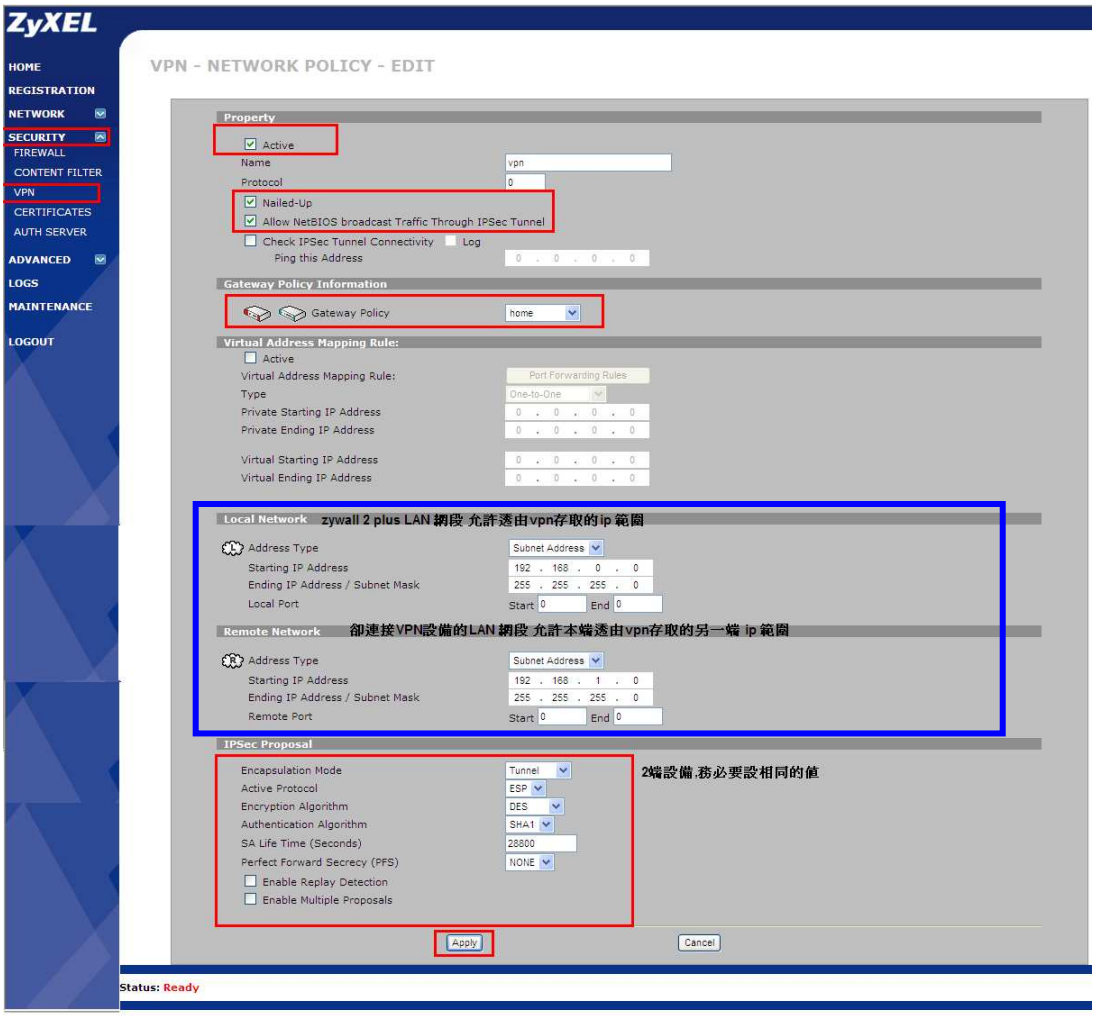
步驟 10：VPN 建立通道(Gateway)，**Authentication Key** 的 **Pre-Shared Key** and **IKE Proposal** 需與步驟 3(認証、階段 1 設定的值)完全相同，並按下 Apply 套用。



步驟 11：點選 “新增 VPN 連線規則”



步驟 12：勾選 Active 點選，自訂一個 VPN 連線規則名稱，並選已建立的 VPN Gateway(home)剛剛步驟 10 所建立的，IPSec Proposal 需與步驟 5(階段 2 的值)完全相同，並按下 Apply 套用。



步驟 13：點選 VPN→點選 SA Monitor 查看 VPN tunnel 是否建立成功。