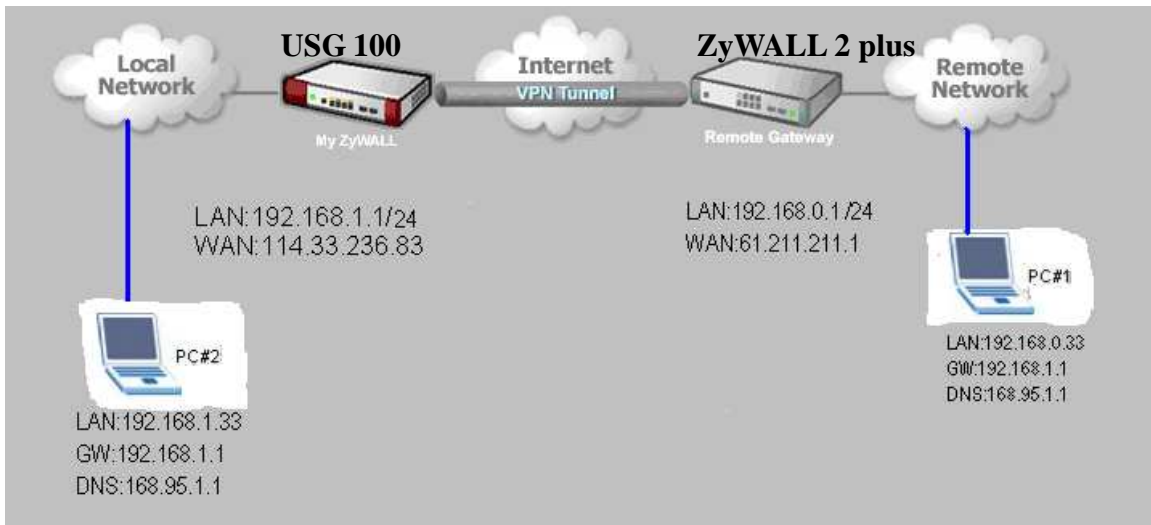


## USG 100 VS ZyWALL 2 PLUS VPN IPsec 設定



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 為標準的 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 值改設為 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

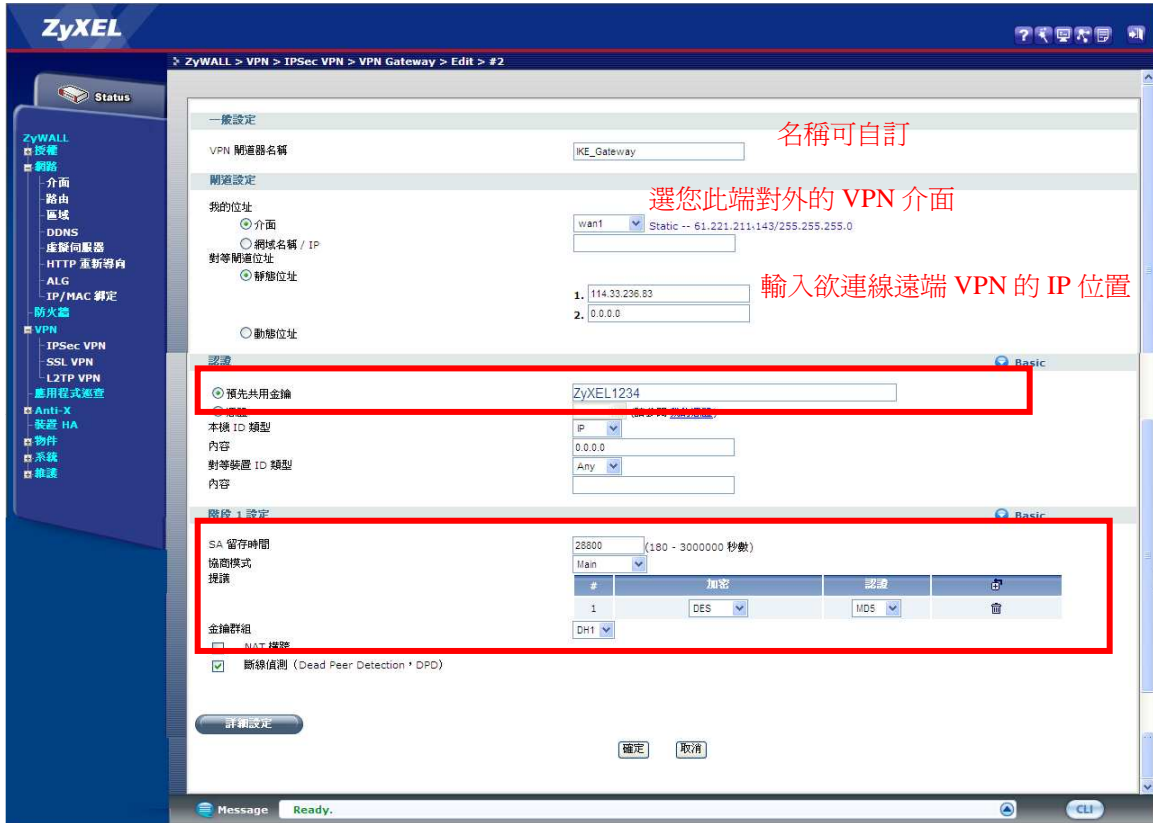
步驟 1: 查看 WAN 及 LAN 的設定值, 點選 “網路” → 點選 “介面” → 點選 “狀態”



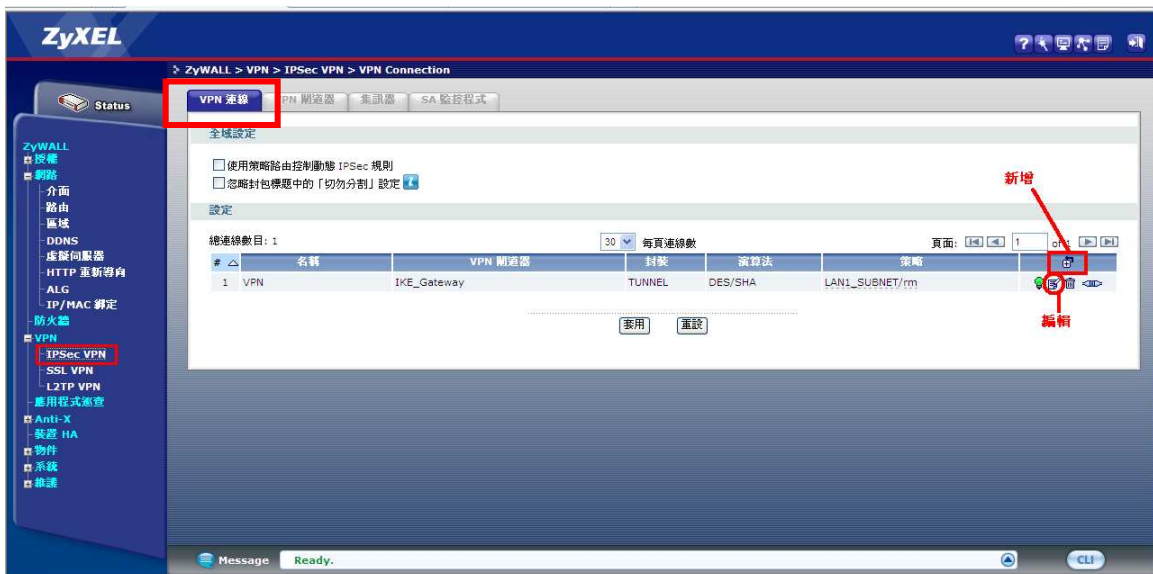
步驟 2: ZyWALL → 點選 “VPN” → 點選 “IPsec VPN” → 點選 “VPN 閘道器” → 按下 “新增”



步驟 3：設定一個名稱來識別此通道要連線對外的 VPN 通道  
紅色框框為兩端設備皆需相同的值。



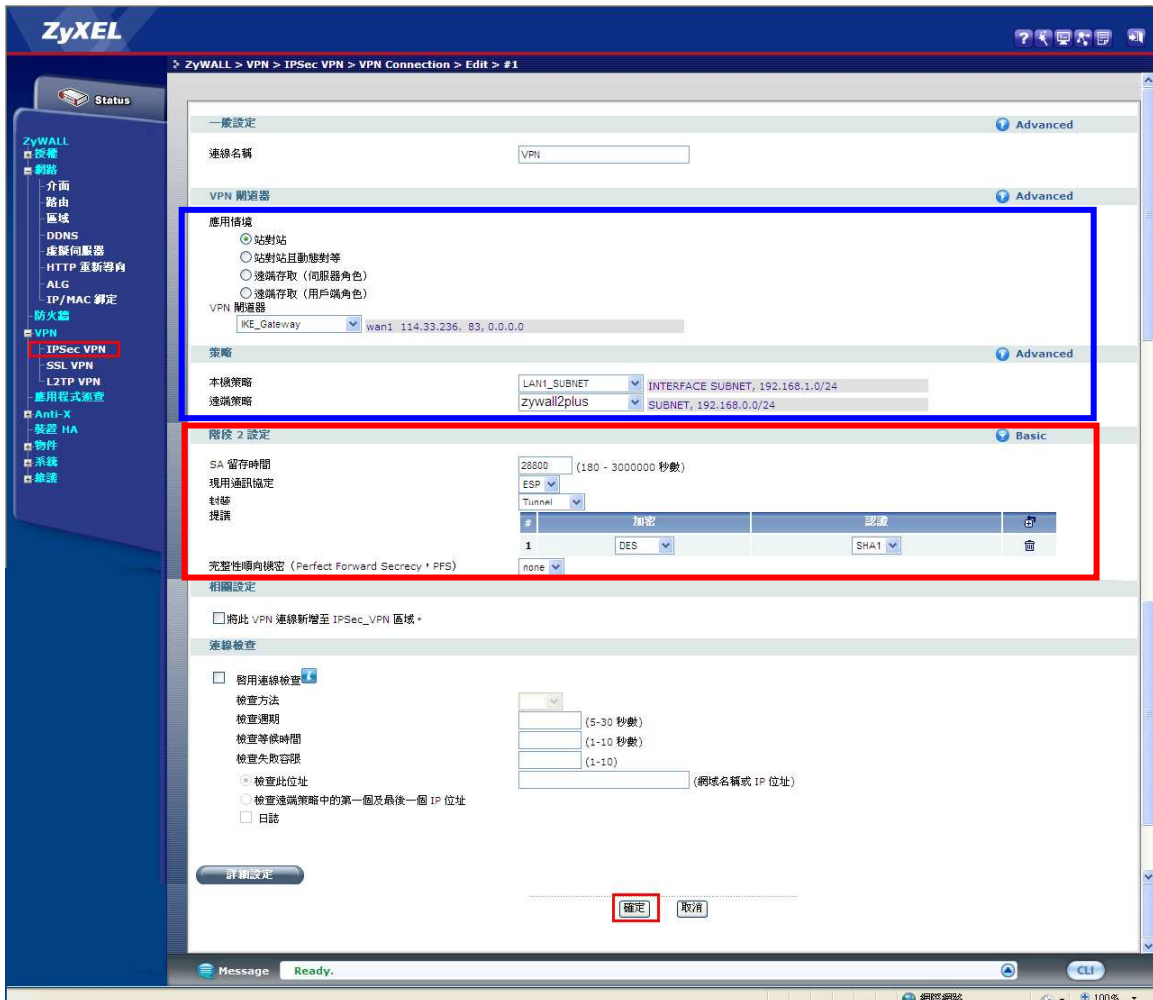
步驟 4：ZyWALL →點選“VPN”→點選“IPsec VPN”→點選“VPN 連線”→按下“新增”



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)

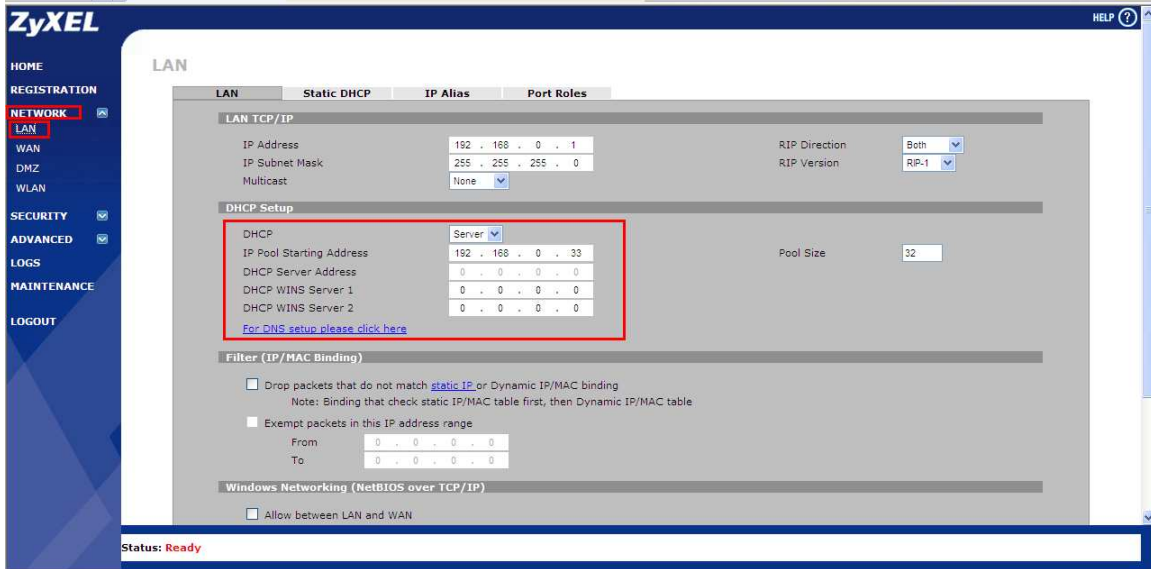
紅色框框為兩端設備皆需相同的值。

最後按下套用即完成 USG 100 端的設定。

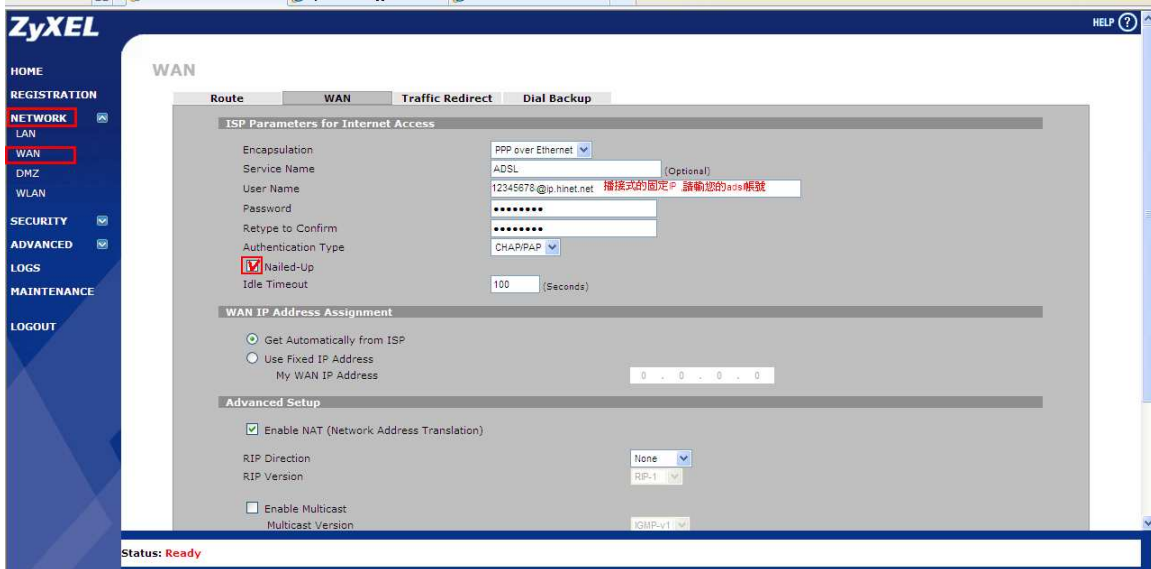


### ZyWALL 2 PLUS

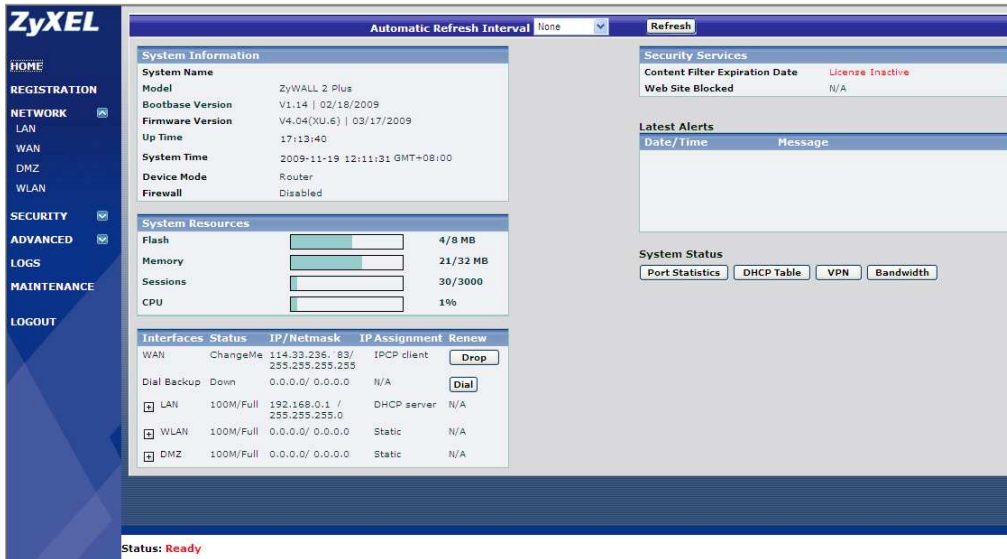
步驟 6：查看 LAN 的設定值，點選 NETWORK→點選 LAN 端。  
避開原本的 192.168.1.1 的網段。



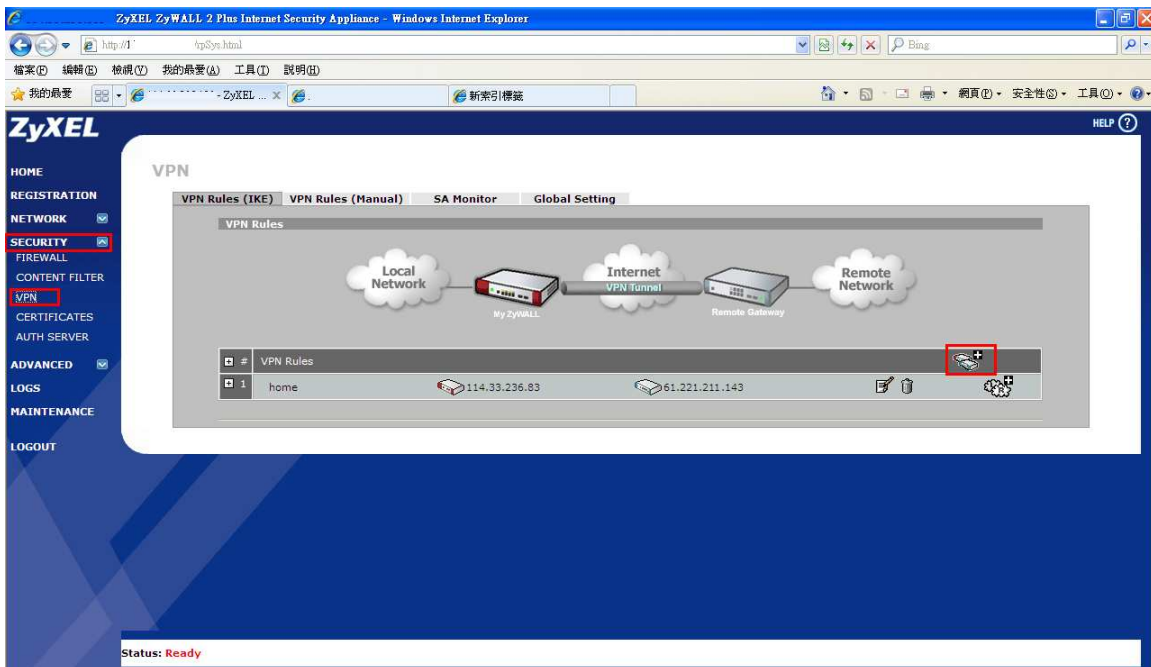
步驟 7：查看 WAN 的設定值，點選 NETWORK→點選 WAN 端。  
此範例為播接式的固定 IP 制的對外網路。



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(認證、階段 1 設定的值)完全相同, 並按下 Apply 套用。

The screenshot shows the ZyXEL configuration interface for a VPN gateway. The left sidebar contains navigation options like HOME, REGISTRATION, NETWORK, SECURITY, FIREWALL, CONTENT FILTER, VPN, CERTIFICATES, AUTH SERVER, ADVANCED, LOGS, MAINTENANCE, and LOGOUT. The main content area is divided into several sections:

- Property:** Name: home, NAT Traversal: checked.
- Gateway Policy Information:** My ZyWALL: 114.33.236.83 (zywall 2 plus的wan ip), My Address: My Domain Name, Primary Remote Gateway: 61.221.211.143 (卻連入設備的wan ip).
- Authentication Key:** Pre-Shared Key: ZyXE1234, Local ID Type: auto\_generated\_self\_signed\_cert, Content: 0.0.0.0, Peer ID Type: IP, Content: 0.0.0.0. A red box highlights this section with a blue arrow pointing to the text "2個端點的密碼要相同, 大小寫有區別".
- Extended Authentication:** Client Mode selected, User Name and Password fields.
- IKE Proposal:** Negotiation Mode: Main, Encryption Algorithm: DES, Authentication Algorithm: MD5, SA Life Time (Seconds): 28800, Key Group: DH1.
- Associated Network Policies:** A table with columns #, Name, Local Network, and Remote Network. The table contains one entry: vpn-p2 with Local Network 192.168.0.0 / 255.255.255.0 and Remote Network 192.168.1.0 / 255.255.255.0. The Apply button is highlighted with a red box.

步驟 11: 點選“新增 VPN 連線規則”

The screenshot shows the ZyXEL VPN Rules configuration page. The left sidebar is the same as in the previous screenshot. The main content area is titled "VPN" and has tabs for VPN Rules (IKE), VPN Rules (Manual), SA Monitor, and Global Setting. The "VPN Rules (IKE)" tab is active, showing a diagram of a VPN tunnel connecting a Local Network (My ZyWALL) to a Remote Network (Remote Gateway) via an Internet VPN Tunnel. Below the diagram is a table of VPN Rules:

#	Name	Local Network	Remote Network	Actions
1	home	114.33.236.83	61.221.211.143	edit, delete, refresh
	vpn	192.168.0.0 / 255.255.255.0	192.168.1.0 / 255.255.255.0	edit, delete, refresh, add

The "add" icon (a gear with a plus sign) in the table is highlighted with a red box, indicating the step to click "Add VPN Connection Rule".

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。

**VPN - NETWORK POLICY - EDIT**

**Property**

- Active
- Name: vpn
- Protocol: 0
- Nailed-Up
- Allow NetBIOS broadcast Traffic Through IPSec Tunnel
- Check IPSec Tunnel Connectivity
- Log
- Ping this Address: 0 . 0 . 0 . 0

**Gateway Policy Information**

- Gateway Policy: home

**Virtual Address Mapping Rule:**

- Active
- Virtual Address Mapping Rule: Port Forwarding Rules
- Type: One-to-One
- Private Starting IP Address: 0 . 0 . 0 . 0
- Private Ending IP Address: 0 . 0 . 0 . 0
- Virtual Starting IP Address: 0 . 0 . 0 . 0
- Virtual Ending IP Address: 0 . 0 . 0 . 0

**Local Network** zywall 2 plus LAN 網段 允許透過vpn存取 ip 範圍

- Address Type: Subnet Address
- Starting IP Address: 192 . 168 . 0 . 0
- Ending IP Address / Subnet Mask: 255 . 255 . 255 . 0
- Local Port: Start 0 End 0

**Remote Network** 卻連接VPN設備的LAN 網段 允許本端透過vpn存取的另一端 ip 範圍

- Address Type: Subnet Address
- Starting IP Address: 192 . 168 . 1 . 0
- Ending IP Address / Subnet Mask: 255 . 255 . 255 . 0
- Remote Port: Start 0 End 0

**IPSec Proposal**

- Encapsulation Mode: Tunnel
- Active Protocol: ESP
- Encryption Algorithm: DES
- Authentication Algorithm: SHA1
- SA Life Time (Seconds): 28800
- Perfect Forward Secrecy (PFS): NONE
- Enable Replay Detection
- Enable Multiple Proposals

2端設備,務必要設相同的值

Apply Cancel

Status: Ready

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

**VPN**

查看是否 Tunnel 是否為建立成功.

VPN Rules (IKE) VPN Rules (Manual) SA Monitor Global Setting

**Security Associations Table**

#	Name	Local Network	Remote Network	Encapsulation	IPSec Algorithm
1	vpn	192.168.0.0 / 255.255.255.0	192.168.1.0 / 255.255.255.0	Tunnel	ESP DES--SHA1

Refresh Disconnect

有看到此筆,即代表建立成功