

## ZyWALL USG 50-H IPsec VPN 設定(兩端固定 IP)



### VPN 設定注意事項：

1. 兩端設備 Lan 網段不可重複，若有請修改其中一端網段  
(包含介面已定義網段也不可重複，如 LAN2 192.168.2.X/DMZ 192.168.3.X)
2. 兩端 IKE Phase1 中的 authentication method 值及 phase2 中的值皆要相同。
3. 建立後測試過程，請將底下電腦的防毒或防火牆暫時關閉。
4. USG 50-H 不提供 IPsec VPN 建立後，遠端電腦 Ping USG 50-H 介面 IP。

	總部_LAN1	分支 LAN1
預設 IP	192.168.1.1	192.168.101.1
DHCP 範圍	192.168.1.33~ 192.168.1.133	192.168.101.33~ 192.168.101.233
WAN	1.1.1.1	2.2.2.2

### 設定將 IPsec VPN 設定三步驟

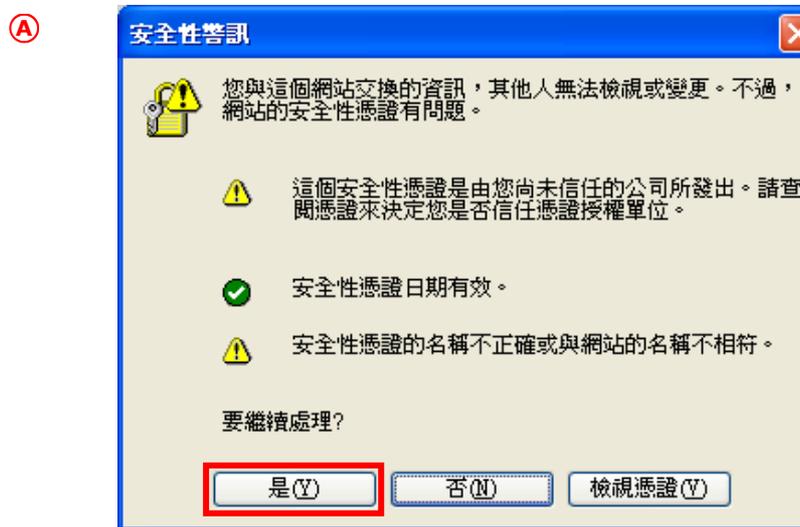
- 第一步：總部端-建立 VPN 閘道器 & 建立 VPN 連線
- 第二步：分支端-建立 VPN 閘道器 & 建立 VPN 連線
- 第三步：檢查建立狀況

## 第一步：建立總部 VPN 閘道器

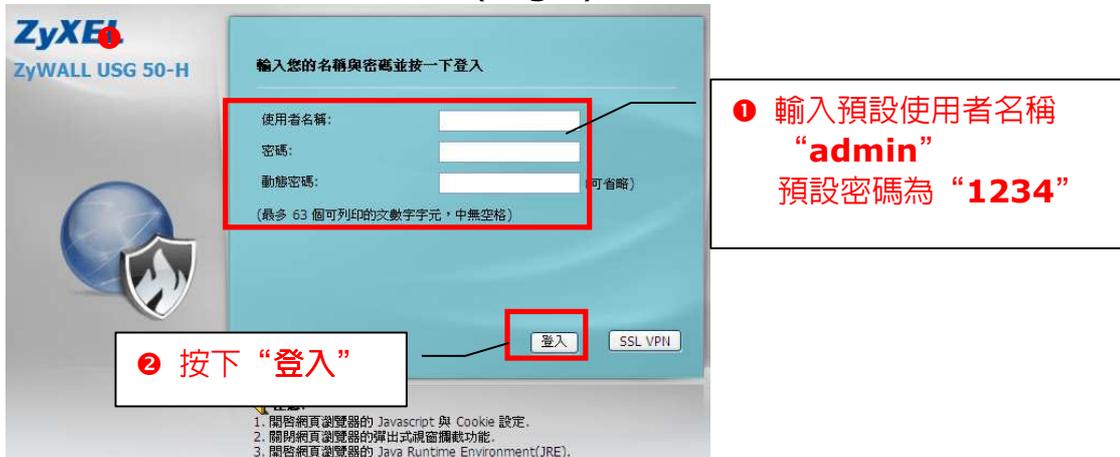
步驟一：開啓您的網頁瀏覽器(Internet Explorer)→請在網址輸入  
“192.168.1.1” →會出現步驟二的圖 ❶ 畫面



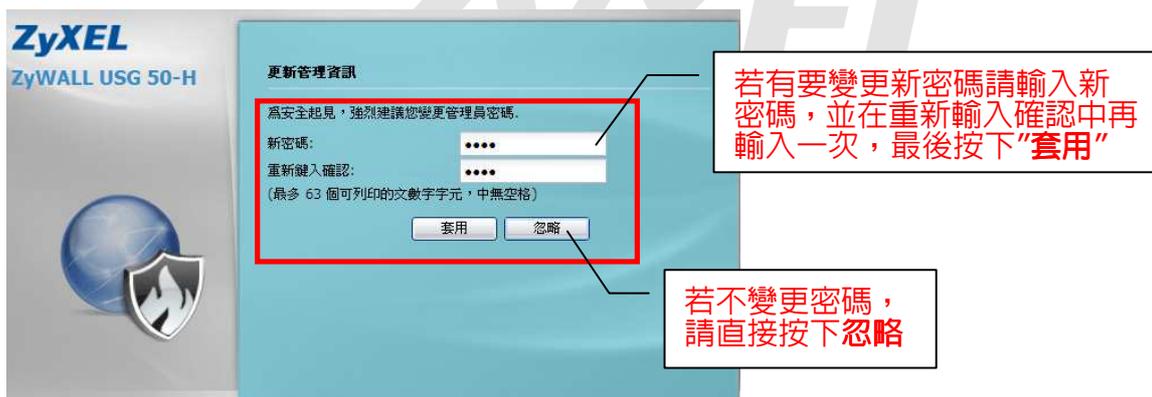
步驟二：當畫面跳出” ❶ 或是 ❷ 的安全性警訊/憑證” 畫面，詢問您是否要繼續處理，請按下” 是 ” 或 ”繼續瀏覽此網站(不建議)”。



步驟三：輸入預設使用者名稱(User Name)為“admin”及登入密碼(Password)“1234”，請按下“登入(Login)”→進入圖②的畫面



② 此時會要求您變更密碼，您可以變更登入的密碼，變更後請點選“套用 (Apply)”，如不變更請直接點選“忽略 (Ignore)”



步驟四：點選網路→介面



### 步驟五：總部網段檢視

連接埠角色 **乙太網路** PPP 行動通信 通道 WLAN VLAN 虛擬區域網路 橋接器 主幹

設定

編輯 刪除 啟動 停用 建立虛擬介面 參考的物件

#	狀態	名稱	IP 位址	遮罩
1	🟡	wan1	STATIC -- 1.1.1.1	255.255.255.0
2	🟡	wan2	DHCP -- 0.0.0.0	0.0.0.0
3	🟡	lan1	STATIC -- 192.168.1.1	255.255.255.0
4	🟡	lan2	STATIC -- 192.168.2.1	255.255.255.0
5	🟡	dmz	STATIC -- 192.168.3.1	255.255.255.0

第 1 頁，共 1 頁 每頁顯示 50 行 顯示 1 - 5 行，共有 5 行

### 步驟六：點選 VPN→點選 IPsec VPN



### 步驟七：點選 VPN 閘道器並新增規則

VPN 連線 **VPN 閘道器** ① 點選 VPN 閘道器

設定

新增 編輯 刪除 啟動 停用 參考的物件

#	狀態	名稱	我的位址	安全閘道	VPN 連線
沒有任何資料					

第 1 頁，共 1 頁 每頁顯示 50 行

② 請點選 新增 進行新增規則

**1** 點選後才能看到階段 1 的設定值

**2** 勾選

**3** 輸入 VPN 閘道器名稱。  
(例：To\_Branch\_Gateway)

**4** 選擇對外上網介面。(例：wan1)

**5** 輸入要連到分支對外固定 IP 位址。  
(例：點選靜態位址，輸入：2.2.2.2 → Branch WAN IP 位址)

**6** 輸入預先共用金鑰。注意：HQ 及 Branch 端都需輸入一樣的金鑰。

**7** 階段 1，選擇兩端 VPN 建立時的密碼演算方式。注意：HQ 及 Branch 端都需選相同一樣。

確定 取消

### VPN 閘道建立完成

VPN 連線    **VPN 閘道器**

### 設定

新增 編輯 移除 啟動 停用 參考的物件

#	狀態	名稱	我的位址	安全閘道	VPN 連線
1		To_Branch_Gateway	wan1	2.2.2.2, 0.0.0.0	

第 1 頁，共 1 頁 | 每頁顯示 50 行 | 顯示 1-1 行，共有 1 行

### 步驟八：建立總部 VPN 連線



建立遠端 VPN 連入網段，建立 Branch LAN 網段位址。



**1** 點選 **啟用**

輸入 VPN 閘道器名稱 (例: To Branch)

**6** 點選 **站對站 (Site to Site)**

**7** 選擇前一步驟建立好的 To\_Branch\_Gateway 規則

**8** 選擇欲與 Branch 連線的網段。(例: LAN1\_SUBNET, 192.168.1.0/24)

**9** 選擇已建立 Branch LAN 物件

**10** 階段 2，選擇兩端 VPN 建立時演算法。注意：HQ 及 Branch 端都需選相同一樣。

確定 取消

### VPN 連線建立完成

VPN 連線 VPN 閘道器

全域設定

- 使用策略路由控制動態 IPsec 規則
- 忽略封包標題中的「切勿分割」設定

設定

新增 編輯 移除 啟動 停用 連接 中斷連線 參考的物件

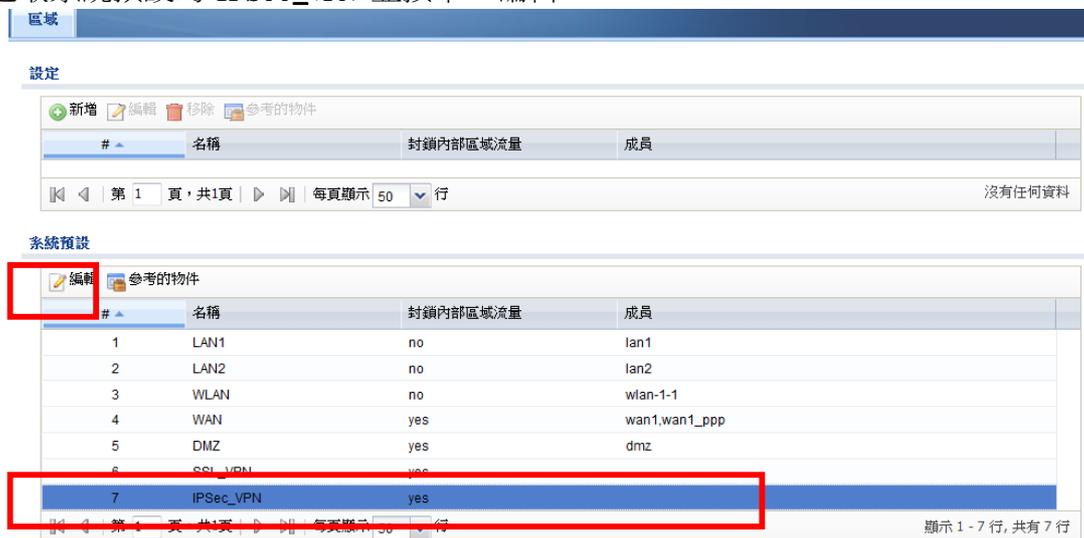
#	狀態	名稱	VPN 閘道器	封裝	演算法	策略
1		To_Branch	To_Branch_Gateway	TUNNEL	DES/SHA1	LAN1_SUBNET/Br...

每頁顯示 50 行 顯示 1 - 1 行, 共有 1 行

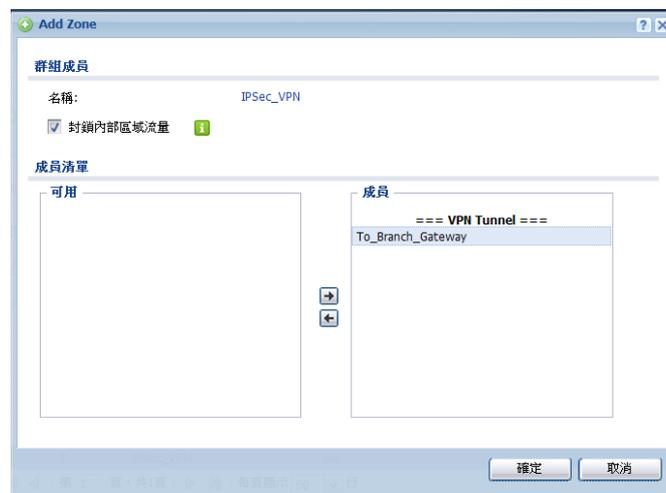
步驟九：請點選“網路”，點選“區域”



選取系統預設的 IPsec\_VPN 並按下“編輯”



將會看到已建立 IPsec VPN Connect 的名稱，請將成員清單的 To\_Branch\_Gateway 加入到成員中並按下確定。



檢查設定後的狀況，將已建立的 IPsec VPN 連線加入到 IPsec\_VPN 的區域成員，是為了讓底下的兩端的區域可以彼此互 PING 的到。

#	名稱	封鎖內部區域流量	成員
1	LAN1	no	lan1
2	LAN2	no	lan2
3	WLAN	no	wlan-1-1
4	WAN	yes	wan1,wan1_ppp
5	DMZ	yes	dmz
6	SSL_VPN	yes	
7	IPSec_VPN	yes	To_Branch_Gateway

## 第二步：建立分支 VPN 閘道器

### 步驟一：點選網路→介面

選取網路，點選介面

步驟二：點選網路→介面→點選乙太網路檢視網段狀況

連接埠角色 | 乙太網路 | PPP | 行動通信 | 通道 | WLAN | VLAN 虛擬區域網路 | 橋接器 | 主幹

設定

編輯 刪除 啟動 停用 建立虛擬介面 參考的物件

#	狀態	名稱	IP 位址	遮罩
1	🟡	wan1	STATIC -- 2.2.2.2	255.255.255.0
2	🟡	wan2	DHCP -- 0.0.0.0	0.0.0.0
3	🟡	lan1	STATIC -- 192.168.101.1	255.255.255.0
4	🟡	lan2	STATIC -- 192.168.202.1	255.255.255.0
5	🟡	dmz	STATIC -- 192.168.88.1	255.255.255.0

第 1 頁，共 1 頁 | 每頁顯示 50 行 | 顯示 1 - 5 行，共有 5 行

步驟三：點選 VPN→點選 IPSec VPN

設定

- 網路
- 認證策略
- 防火牆
- VPN
  - IPSec VPN
  - SSL VPN
  - 應用程式巡查

選取 VPN，點選 IPSec VPN

步驟四：點選 VPN 閘道器並新增規則

VPN 連線 | VPN 閘道器

1 點選 VPN 閘道器

2 請點選 新增 進行新增規則

設定

新增 編輯 刪除 啟動 停用 參考的物件

#	狀態	名稱	我的位址	安全閘道	VPN 連線
---	----	----	------	------	--------

第 1 頁，共 1 頁 | 每頁顯示 50 行 | 沒有任何資料

**3 勾選**

**4 輸入 VPN 閘道器名稱。**  
(例：To\_HQ\_Gateway)

**4 選擇對外上網介面。**(例：wan1)

**5 輸入要連到總部對外固定 IP 位址。**(例：點選靜態位址，輸入：1.1.1.1→HQ WAN IP 位址)

**6 輸入預先共用金鑰。**注意：HQ 及 Branch 端都需輸入一樣的金鑰。

**7 階段 1，選擇兩端 VPN 建立時的密碼演算方式。**注意：HQ 及 Branch 端都需選相同一樣。

### 步驟五：建立 VPN 連線

**1 點選 VPN 連線**

**2 請點選 新增 進行新增規則**

建立遠端 VPN 連入網段，建立 HQ LAN 網段位址。

The image shows a sequence of three screenshots from a ZyXEL web management interface, illustrating the steps to create a remote VPN connection and its associated LAN address.

- Step 3:** In the "Add VPN Connection" window, the "建立新物件" (Create New Object) button is highlighted with a red box. A callout box points to it with the text: "3 建立遠端 VPN 連入網段，選擇建立新物件" (3 Create remote VPN connection, select Create New Object).
- Step 4:** In the "VPN 閘道器" (VPN Gateway) configuration window, the "位址" (Address) button is highlighted with a red box. A callout box points to it with the text: "4 點選位址" (4 Click Address).
- Step 5:** In the "Create Address" window, the "確定" (OK) button is highlighted with a red box. A callout box points to it with the text: "5 建立遠端 VPN 連入網段名稱，命為 HQ\_LAN 物件" (5 Create remote VPN connection name, name it HQ\_LAN object). The form fields are filled with: 名稱: HQ\_LAN, 位址類型: SUBNET, 網路: 192.168.1.0, and 網路遮罩: 255.255.255.0.

**1** 點選啟用

輸入 VPN 閘道器名稱 (例: To\_HQ\_VPN)

**6** 點選站對站 (Site to Site)

**7** 選擇前一步驟建立好的 To\_HQ\_Gateway 規則

**8** 選擇欲與 HQ 連線的網段。(例: LAN1\_SUBNET, 192.168.101.0/24)

**9** 選擇已建立 HQ LAN 物件

**10** 階段 2，選擇兩端 VPN 建立時演算方式。注意：HQ 及 Branch 端都需選相同一樣。

確定 取消

### VPN 連線建立完成

VPN 連線 VPN 閘道器

全域設定

- 使用策略路由控制動態 IPsec 規則
- 忽略封包標題中的「切勿分割」設定

設定

新增 編輯 移除 啟動 停用 連接 中斷連線 參考的物件

#	狀態	名稱	VPN 閘道器	封裝	演算法	策略
1		TO_HQ_VPN	TO_HQ_Gateway	TUNNEL	DES/SHA1	LAN1_SUBNET/H...

第 1 頁，共 1 頁 每頁顯示 50 行 顯示 1 - 1 行，共有 1 行

### 步驟六：手動建立 VPN 連線

全域設定

使用策略路由控制動態 IPsec 規則

忽略封包標題中的「切勿分割」設定

設定

新增 編輯 移除 啟動 停用 連接 中斷連線 參考的物件

#	狀態	名稱	VPN 閘道器	封裝	演算法	策略
1		TO_HQ_VPN	TO_HQ_Gateway	TUNNEL	DES/SHA1	LAN1_SUBNET/...

第 1 頁, 共 1 頁 | 每頁顯示 50 行 | 顯示 1 - 1 行, 共有 1 行

套用 重設

2 按下連接

1 選擇欲建立的 VPN 連線並按下連接

連上的狀況如下圖：

全域設定

使用策略路由控制動態 IPsec 規則

忽略封包標題中的「切勿分割」設定

設定

新增 編輯 移除 啟動 停用 連接 中斷連線 參考的物件

#	狀態	名稱	VPN 閘道器	封裝	演算法	策略
1		TO_HQ_VPN	TO_HQ_Gateway	TUNNEL	DES/SHA1	LAN1_SUBNET/HQ_LAN

第 1 頁, 共 1 頁 | 每頁顯示 50 行 | 顯示 1 - 1 行, 共有 1 行

步驟七：請點選“網路”，點選“區域”

設定

快速設定

- 授權
- 網路
- 介面
- 路由
- 區域
- DDNS
- NAT

選取系統預設的 IPsec\_VPN 並按下“編輯”

The screenshot shows the 'System Preset' section of the ZyXEL management interface. It features a table with the following data:

#	名稱	封鎖內部區域流量	成員
1	LAN1	no	lan1
2	LAN2	no	lan2
3	WLAN	no	wlan-1-1
4	WAN	yes	wan1,wan1_ppp
5	DMZ	yes	dmz
6	SSL_VPN	yes	
7	IPSec_VPN	yes	

The '編輯' (Edit) button and the row for 'IPSec\_VPN' are highlighted with red boxes. The interface also shows navigation controls and a status bar indicating '顯示 1 - 7 行, 共有 7 行'.

將會看到已建立 IPsec VPN Connect 的名稱，請將成員清單的 To\_HQ\_VPN 加入到成員中並按下確定。

The screenshot shows the 'Add Zone' dialog box. The '名稱' (Name) field is set to 'IPSec\_VPN'. The '封鎖內部區域流量' (Block internal traffic) checkbox is checked. The '成員清單' (Member List) section shows a list of available members on the left and a list of selected members on the right. The selected member is 'To\_HQ\_VPN', which is part of a group named '=== VPN Tunnel ==='. The dialog box has '確定' (OK) and '取消' (Cancel) buttons at the bottom.

檢查設定後的狀況，將已建立的 IPsec VPN 連線加入到 IPsec\_VPN 的區域成員，是為了讓底下的兩端的區域可以彼此互 PING 的到。

#	名稱	封鎖內部區域流量	成員
1	LAN1	no	lan1
2	LAN2	no	lan2
3	WLAN	no	wlan-1-1
4	WAN	yes	wan1,wan1_ppp
5	DMZ	yes	dmz
6	SSL_VPN	yes	
7	IPSec_VPN	yes	To_HQ_VPN

### 第三步：檢查建立狀況

步驟一：連線後的可檢查 VPN Tunnel 是否有建立成功。點選**監控** → VPN 監視 → IPsec

1 選擇**監控**

2 選擇 **VPN 監視** → IPsec

即可看到建立成功的 IPsec 通道



也可以從日誌檢查建立的狀態 → 點選日誌



~ The End ~