

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

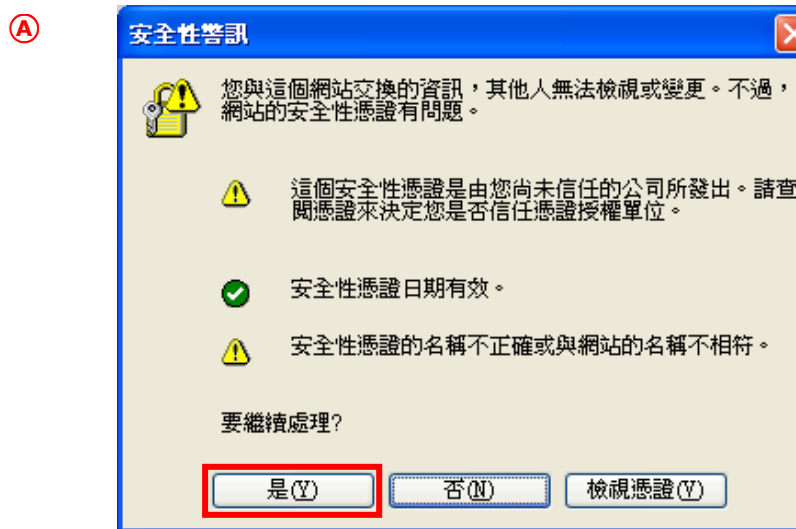
- 第一步：總部端-建立 VPN 閘道器 & 建立 VPN 連線
- 第二步：分支端-建立 VPN 閘道器 & 建立 VPN 連線
- 第三步：檢查建立狀況

第一步：建立總部 VPN 閘道器

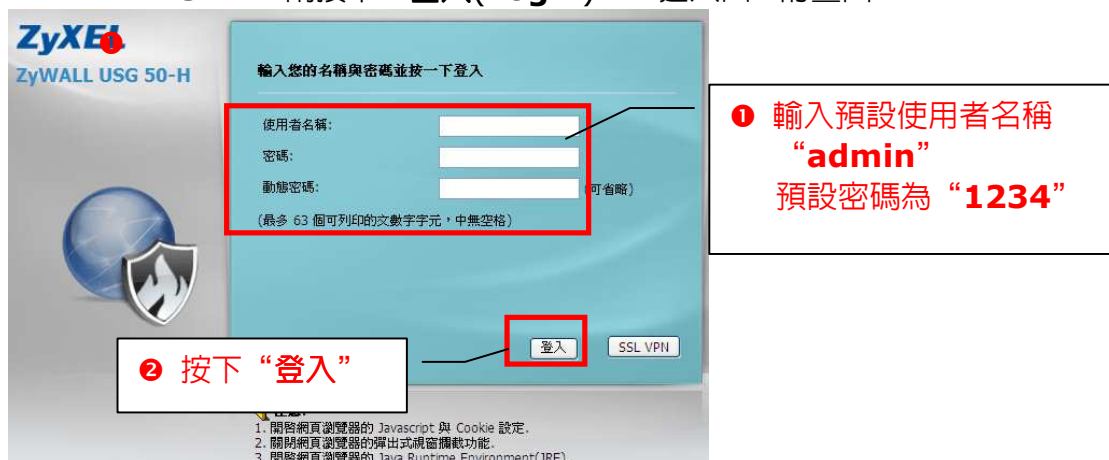
步驟一：開啓您的網頁瀏覽器(Internet Explorer)→請在網址輸入
“192.168.1.1” →會出現步驟二的圖ⓐ畫面



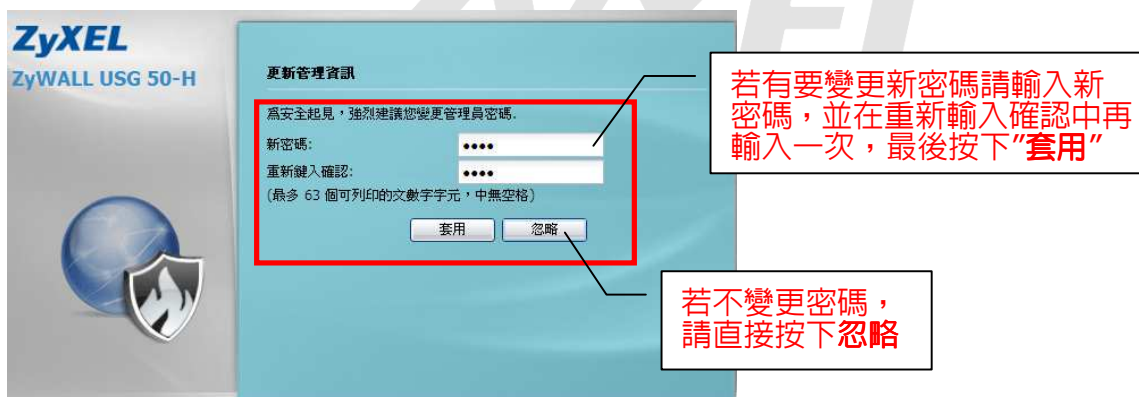
步驟二：當畫面跳出”ⓐ或是ⓑ的安全性警訊/憑證”畫面，詢問您是否要繼續處理，請按下”是”或”繼續瀏覽此網站(不建議)”。



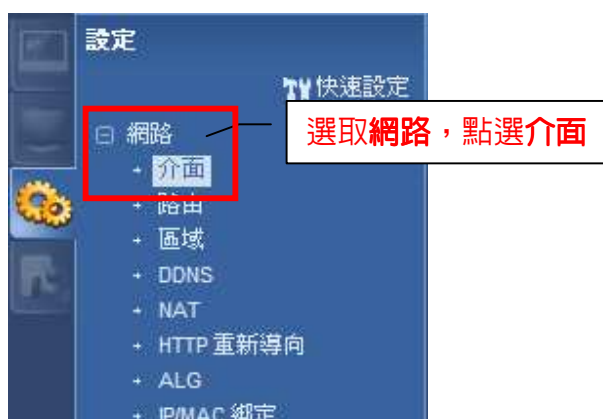
步驟三：輸入預設使用者名稱(User Name)為“admin”及登入密碼(Password)“1234”，請按下“登入(Login)”→進入圖②的畫面



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

#	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

步驟六：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

2 請點選 新增 進行新增規則

#	狀態	名稱	我的位址	安全閘道	VPN 連線
沒有任何資料					

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

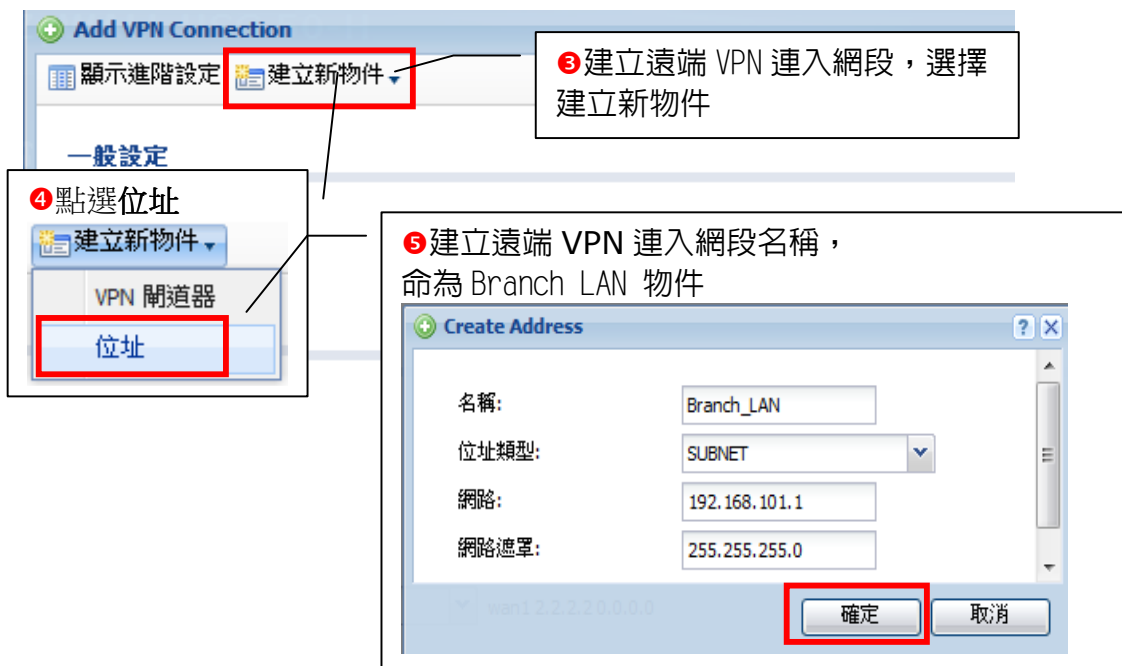
#	狀態	名稱	我的位址	安全閘道	VPN 連線
1		To_Branch_Gateway	wan1	2.2.2.2, 0.0.0.0	

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...

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

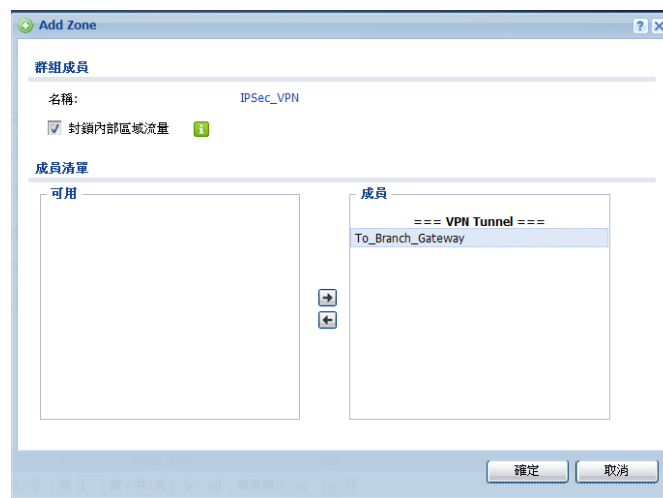
步驟九：請點選“網路”，點選“區域”



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



步驟二：點選網路→介面→點選乙太網路檢視網段狀況

設定

#	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

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

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

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 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 columns: #, 名稱 (Name), 封鎖內部區域流量 (Block Internal Traffic), and 成員 (Members). The table contains 7 rows of data. The 7th row, 'IPSec_VPN', is highlighted with a red box. Above the table, there are buttons for '新增' (Add), '編輯' (Edit), '移除' (Remove), and '參考的物件' (Reference Objects). The '編輯' button is also highlighted with a red box. Below the table, there are navigation controls and a status bar indicating '顯示 1 - 7 行, 共有 7 行' (Display 1 - 7 rows, total 7 rows).

#	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	

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. Below the '成員清單' (Member List) section, there are two panes: '可用' (Available) and '成員' (Members). The '成員' pane contains the entry 'To_HQ_VPN' under the heading '=== VPN Tunnel ==='. There are '確定' (OK) and '取消' (Cancel) buttons at the bottom right.

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

IPsec

使用中的 IPsec 安全性關聯

名稱:

策略:

中斷連線

#	名稱	封裝	策略	演算法	已執行...	等候時間	進向位...	外撥(位...
1	TO_HQ_V... Tunnel		192.168.101.0/24<>1...	esp/des/s...	54	86346	0(0 bytes)	0(0 bytes)

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

也可以從日誌檢查建立的狀態→點選日誌

- 系統狀態
 - 埠統計
 - 介面狀態
 - 流量統計
 - 工作階段監控程式
 - DDNS 狀態
 - IP/MAC 綁定
 - 登入使用者
 - WLAN 狀態
 - Cellular 狀態
 - AppPatrol 統計
- VPN 監視
 - 日誌**

3 選擇日誌

檢視日誌

顯示過濾器

7	2011-01-18 22:38:15	info	IKE	Tunnel [To_Branch:To_Branch_Gateway:0x6061b141] built successfully	1.1.1.1 :500	2.2.2.2 :500	IKE_LOG
8	2011-01-18 22:38:15	info	IKE	[ESP:des_cbc hmac_sha1_96][SPI:0xb4627729/0x6061b141] lifetime: 86420	1.1.1.1 :500	2.2.2.2 :500	IKE_LOG
9	2011-01-18 22:38:15	info	IKE	[Responder:172.24.68.33][Initiator:172.24.68.26][Policy: ipv4(192.168.1.0-19...	1.1.1.1 :500	2.2.2.2 :500	IKE_LOG
10	2011-01-18 22:38:15	info	IKE	Recv:[HASH]	2.2.2.2 :500	1.1.1.1 :500	IKE_LOG
11	2011-01-18 22:38:15	info	IKE	Send:[HASH][SA][NONCE][ID][ID]	1.1.1.1 :500	2.2.2.2 :500	IKE_LOG
12	2011-01-18 22:38:15	info	IKE	Recv:[HASH][SA][NONCE][ID][ID]	2.2.2.2 :500	1.1.1.1 :500	IKE_LOG
13	2011-01-18 22:38:15	info	IKE	Phase 1 IKE SA process done	1.1.1.1 :500	2.2.2.2 :500	IKE_LOG
14	2011-01-18 22:38:15	info	IKE	Send:[ID][HASH]	1.1.1.1 :500	2.2.2.2 :500	IKE_LOG
15	2011-01-18 22:38:15	info	IKE	Recv:[ID][HASH][NOTIFY:INITIAL_CONTACT]	2.2.2.2 :500	1.1.1.1 :500	IKE_LOG
16	2011-01-18 22:38:14	info	IKE	Send:[KE][NONCE]	1.1.1.1 :500	2.2.2.2 :500	IKE_LOG
17	2011-01-18 22:38:14	info	IKE	Recv:[KE][NONCE]	2.2.2.2 :500	1.1.1.1 :500	IKE_LOG
18	2011-01-18 22:38:14	info	IKE	Send:[SA][VID][VID][VID]	1.1.1.1 :500	2.2.2.2 :500	IKE_LOG
19	2011-01-18 22:38:14	info	IKE	The cookie pair is : 0x58c821323ba7774a / 0xdd08d30712a959ff [count=8]	1.1.1.1 :500	2.2.2.2 :500	IKE_LOG
20	2011-01-18 22:38:14	info	IKE	Recv:[SA][VID][VID][VID][VID]	2.2.2.2 :500	1.1.1.1 :500	IKE_LOG
21	2011-01-18 22:38:14	info	IKE	The cookie pair is : 0xdd08d30712a959ff / 0x58c821323ba7774a [count=5]	2.2.2.2 :500	1.1.1.1 :500	IKE_LOG
22	2011-01-18 22:38:14	info	IKE	Recv Main Mode request from [172.24.68.26]	2.2.2.2 :500	1.1.1.1 :500	IKE_LOG
23	2011-01-18 22:38:14	info	IKE	The cookie pair is : 0x58c821323ba7774a / 0x0000000000000000	1.1.1.1 :500		IKE_LOG
24	2011-01-18 22:36:32	info	DHCP	Sending ACK to 192.168.1.33			DHCP ACK

4 即可看到 Tunnel 已建立完成訊息

~ The End ~