

VPN SSL VPN 連線設定範例

ZyWALL SSL VPN 支援隧道模式。當遠端使用者建立虛擬連線時，ZyWALL USG 50-H 會配發一組虛擬 IP 位址，並將虛擬連線視為內部網路，即可以存取區網的資源。

SSL VPN 允許使用網頁瀏覽器以安全的方式，由遠端讓使用者登入；遠端的使用者不需要額外加裝 VPN 路由器或是 VPN 用戶端軟體。

煩請登入 USG 50H 的管理畫面，並點選 VPN --> SSL VPN --> 並按下新增按鈕建立完整通道 SSL VPN

1 勾選啟用

2 輸入名稱 (如: SSL_Policy1)

3 建立新使用者物件

4 在“可選取的使用者/群組物件中即會出現 test 可供選擇，請選擇 test 按壓 >> 將 test 選取至“選取的使用者/群組物件

輸入使用者名稱/密碼
使用者類型選擇 User

5 配置 IP 集區，選擇 (Create Object)

建立 SSL VPN 的虛擬 IP 範圍

設定

名稱	SSL_Add
位址類型	RANGE
起始 IP 位址	10.0.0.1
結束 IP 位址	10.0.0.5

.....

- ⑥ DNS 伺服器 1 (可以略過不建立)或選擇 User Defined,輸入您欲對應的 DNS 伺服器位址(如: 172.24.68.100)
- ⑦ 請在網路表選擇可選取允許存取的位址物件
- ⑧ 設定完成,請按下**“確定”**

網路延伸:

啟用網路延伸

配置 IP 集區	SSL_Add	RANGE 10.0.0.1 - 10.0.0.5
DNS 伺服器 1	User Defined	172.24.68.100
DNS 伺服器 2	none	
WINS 伺服器 1	none	
WINS 伺服器 2	none	

.....

網路表

可選取的位址物件	選取的位址物件
	DMZ_SUBNET LAN1_SUBNET LAN2_SUBNET WLAN-1-1_SUBNET

.....

將 SSL VPN 加入 SSL_VPN 區域

選擇網路→區域

設定

名稱	封鎖內部區域流量	成員	修改
LAN1	No	lan1	
LAN2	No	lan2	
WLAN	No	wlan-1-1	
WAN	Yes	wan1, wan2, wan1_ppp, wan2_ppp	
DMZ	Yes	dmz	
SSL_VPN	Yes		
IPSec_VPN	Yes		

在 SSL_VPN 部分點選編輯按鈕

選擇 SSLVPN 成員

群組成員

名稱 SSL_VPN

封鎖內部區域流量

成員清單

可用 SSL_VPN

成員

成員

SSLVPN / SSL_Policy1

>>

<<

成員

SSLVPN / SSL_Policy1

確定

取消

完成將 SSL VPN 加入 SSL_VPN 區域

設定

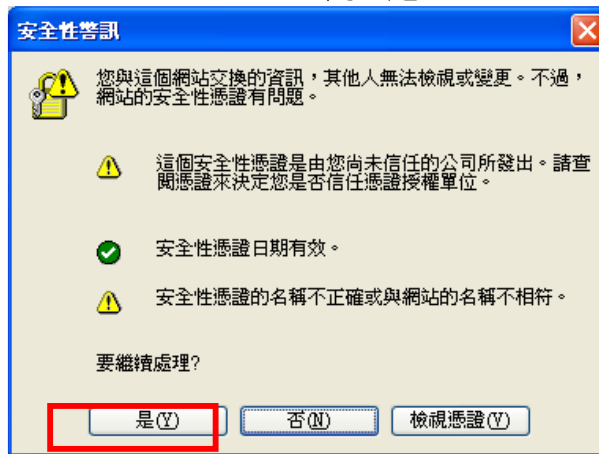
名稱	封鎖內部區域流量	成員	修改
LAN1	No	lan1	
LAN2	No	lan2	
WLAN	No	wlan-1-1	
WAN	Yes	wan1, wan2, wan1_ppp, wan2_ppp	
DMZ	Yes	dmz	
SSL_VPN	Yes	SSL_Policy1	
IPSec_VPN	Yes		

SSL 用戶端登入

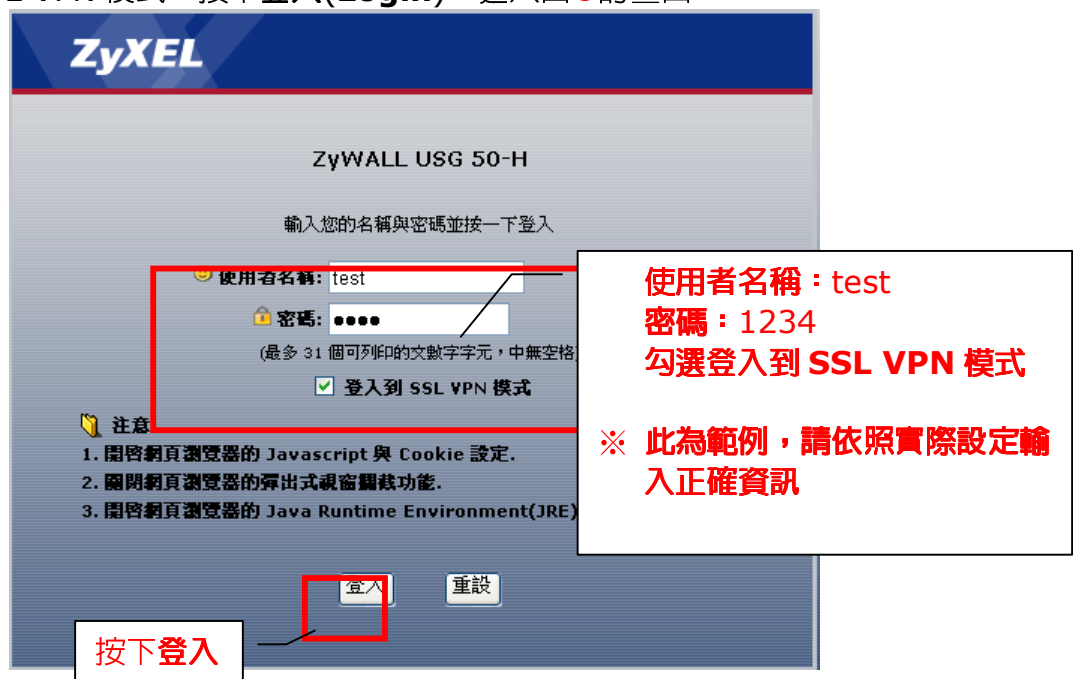
步驟一：使用 Internet Explorer 輸入 ZyWALL USG 50-H 的 WAN IP 位址



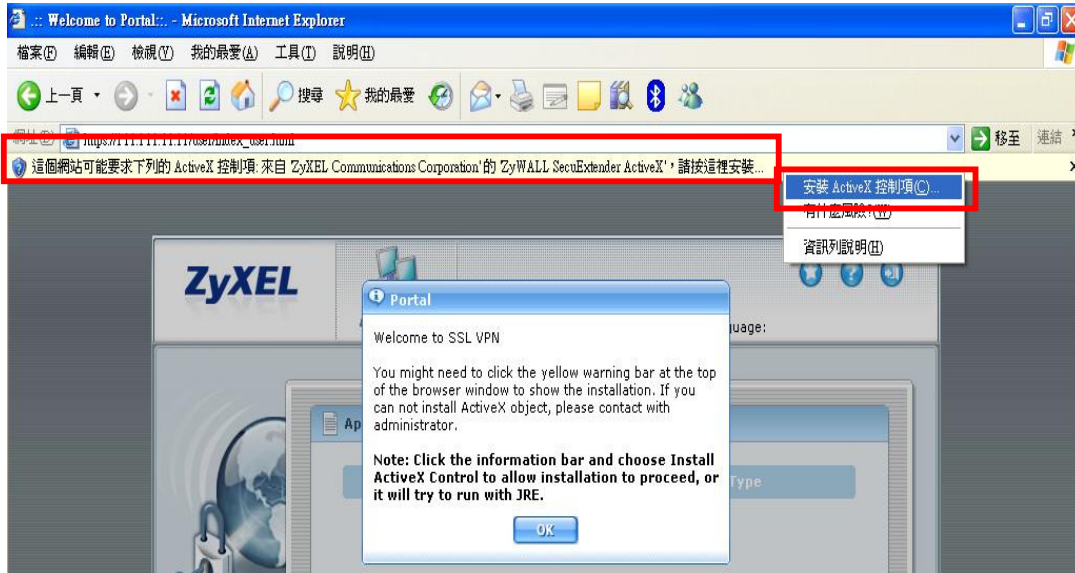
步驟二：當畫面跳出”安全性警訊”，詢問您是否要繼續處理，請按下”是”。



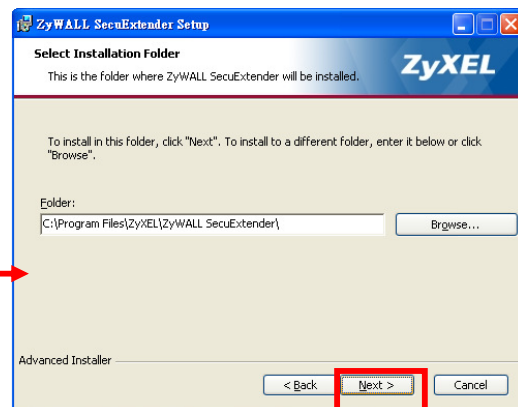
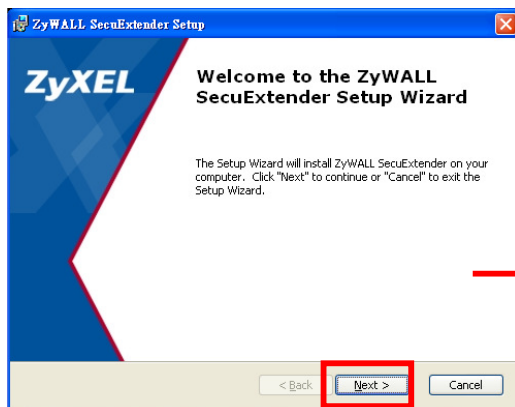
步驟三：輸入預設使用者名稱(User Name)及登入密碼(Password)並勾取登入到 SSL VPN 模式，按下登入(Login)→進入圖 2 的畫面

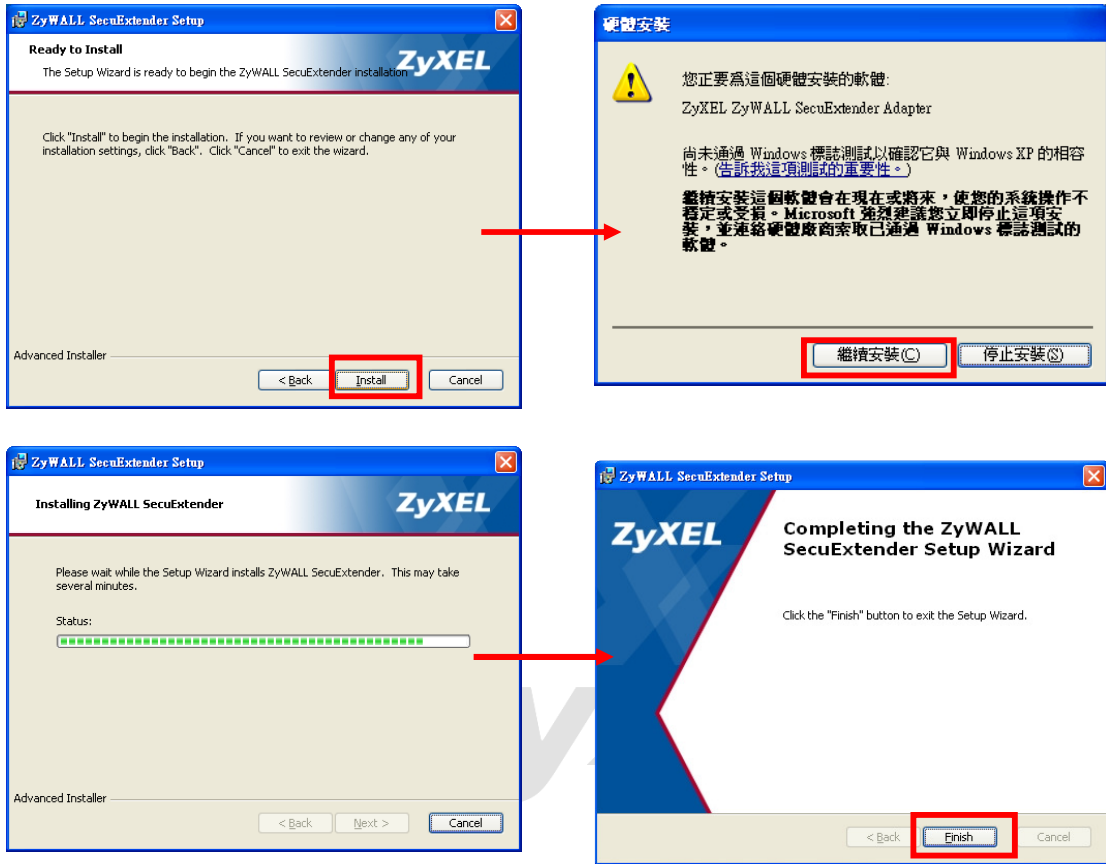


步驟四：登入後，若為首次登入，網頁上則會出現要求您安裝“ZyWALL SecuExtender ActiveX”的控制項，請在該對話框按右鍵，選擇”安裝 ActiveX 控制項”

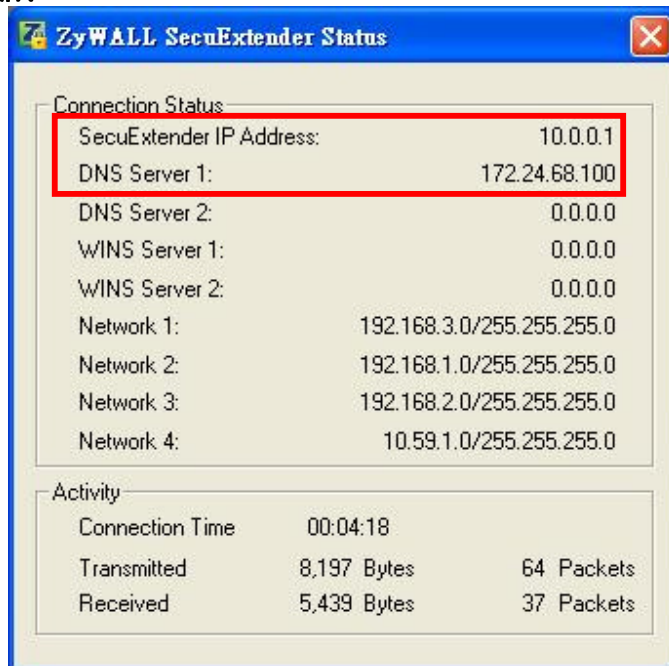


步驟五：安裝 ZyWALL SecuExtender ActiveX 軟體





步驟六：當安裝完成，電腦左下方會出現  圖示，並會顯示您所取得的 IP 及 DNS 相關資訊



步驟七：存取 ZyWALL USG 50-H 中，LAN1(192.168.1.33)所分享的資料

