

USG SSL VPN 翻牆設定

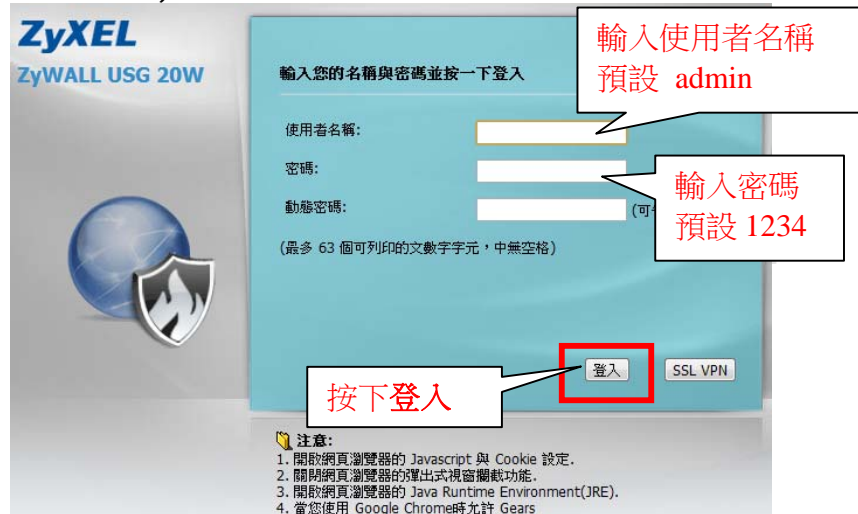
當 User 連入 USG SSL VPN，User 端所有的網路封包皆會改透由 USG 的 SSL VPN 閘道連接至外部網網路，同時也可以存取 SSL VPN 設備之下內部網段的資源。

※ USG 韌體需更新至 3.0 以上。

※ 建議遠端欲連入的使用者 LAN 網段不要與 USG 底下的網段相同。

以下以 USG 20W 為設定範例：


步驟一：登入 USG 設定頁面，預設為 <http://192.168.1.1> 帳號/密碼 (admin/1234)




步驟二：若有詢問您是否要更改密碼，請先按下略過；若無詢問新密碼，表示您已更動過預設密碼，請直接跳至步驟三。

步驟三：看到網路風險警告視窗，請先按下**確定**。



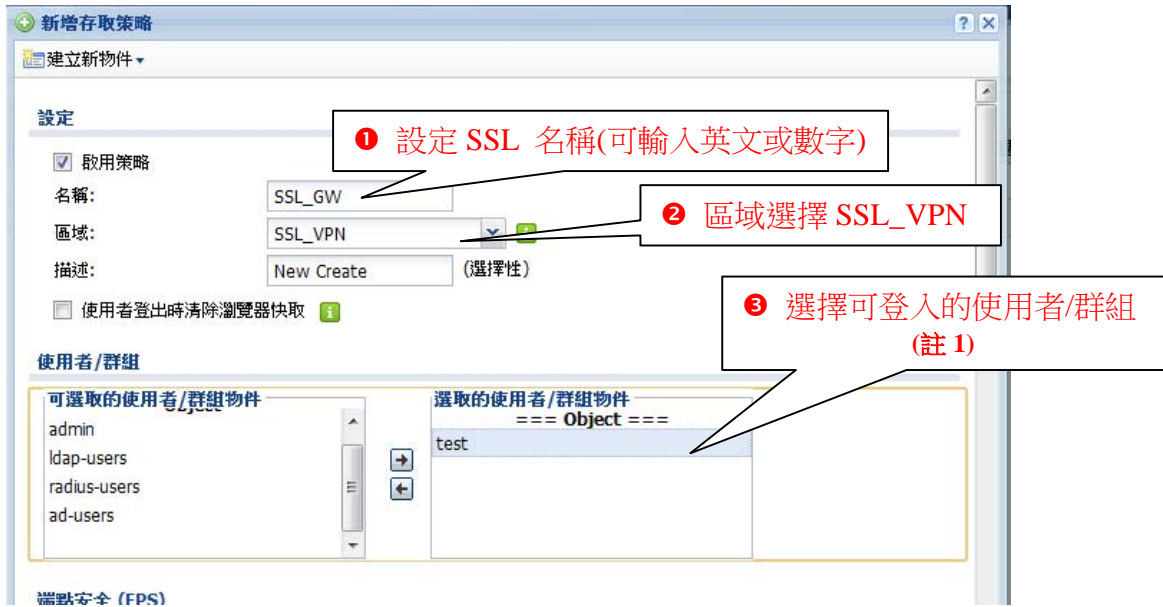
步驟四：按下設定  → VPN → SSL VPN



步驟五：在存取權限中按下新增  新增



步驟六：設定 SSL VPN 條件



接著設定網路延伸（畫面拉至最下方）

強制所有用戶端流量進入 SSL VPN 通道：此功能會強制將所有 SSL VPN 用戶端流量傳送至 SSL VPN 通道，啟用後，可讓 ZyWALL 以 SSL VPN 閘道 IP 位址取代 SSL VPN 用戶端的預設閘道 IP 位址。

網路延伸: (可省略)

啟用網路延伸

強制所有用戶端流量進入 SSL VPN 通道

配置 IP 集區: SSL_Range RANGE 10.100.0.1-10.100.0.5

DNS 伺服器 1: User Defined 168.95.1.1

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: LAN1_SUBNET, LAN2_SUBNET, DMZ_SUBNET, WLAN-1-1_SUBNET, IP6to4-Relay

選取的位址物件:

1 2 個功能皆需打勾，啟用

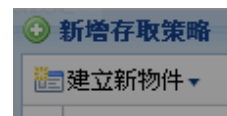
2 配置 IP 集區
選擇派發 SSL VPN 的 IP 範圍
※ 請與 USG 內部其他網段錯開 (註 2)

3 DNS 伺服器 1：選擇 User Defined
輸入欲派發的 DNS 位置
例：168.95.1.1

4 按下確定

確定 取消

新增物件說明：



設定 SSL VPN 條件時，畫面左上方可點選“建立新物件”

註 1：新增使用者/群組

選擇 建立新物件→使用者/群組 ※使用者類型不可為 admin/limit-admin

Add User

設定

使用者名稱: test

使用者類型: user

密碼: ****

重新鍵入: ****

認讀等候時間設定: 使用預設設定 使用手動設定

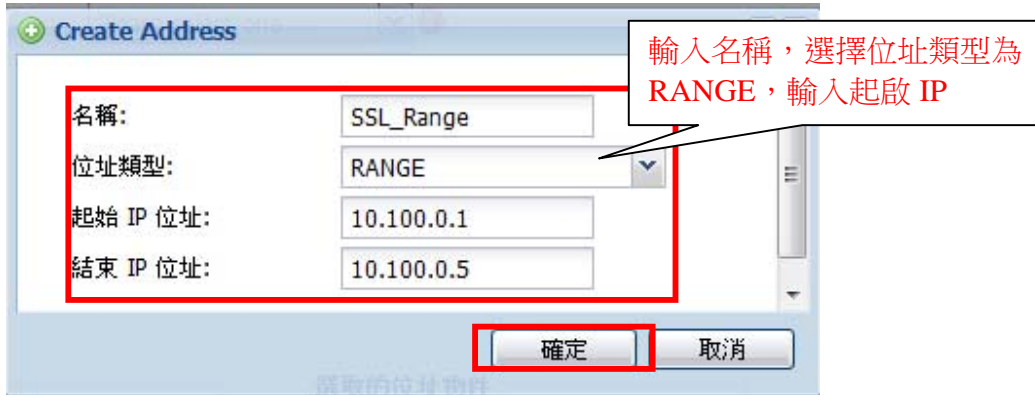
租用時間: 1440 分

再認讀時間: 1440 分

輸入使用者名稱及密碼

確定 取消

註 2：新增 IP 位址範圍
選擇 建立新物件→位址



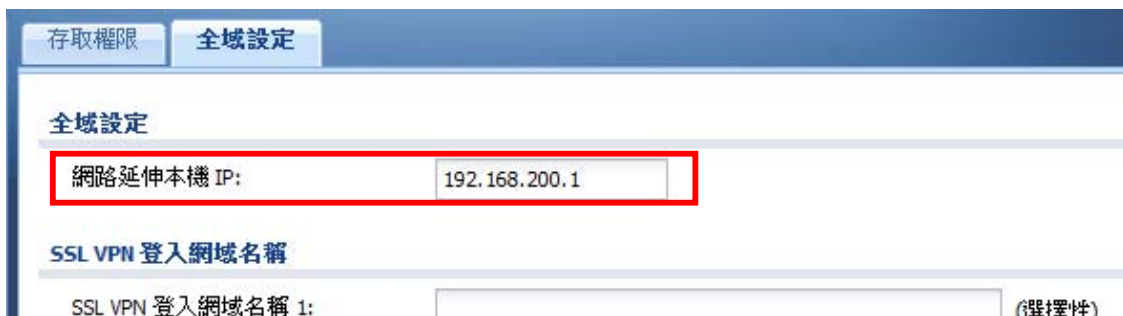
確認 SSL VPN 預設閘道位址

步驟一：按下設定  → VPN → SSL VPN



步驟二：點選全域設定，網路延伸本機 IP 即為 SSL VPN 閘道

※ 若無特殊需求，請保留原設定，勿任意進行更改。



設定完成開始進行驗證！

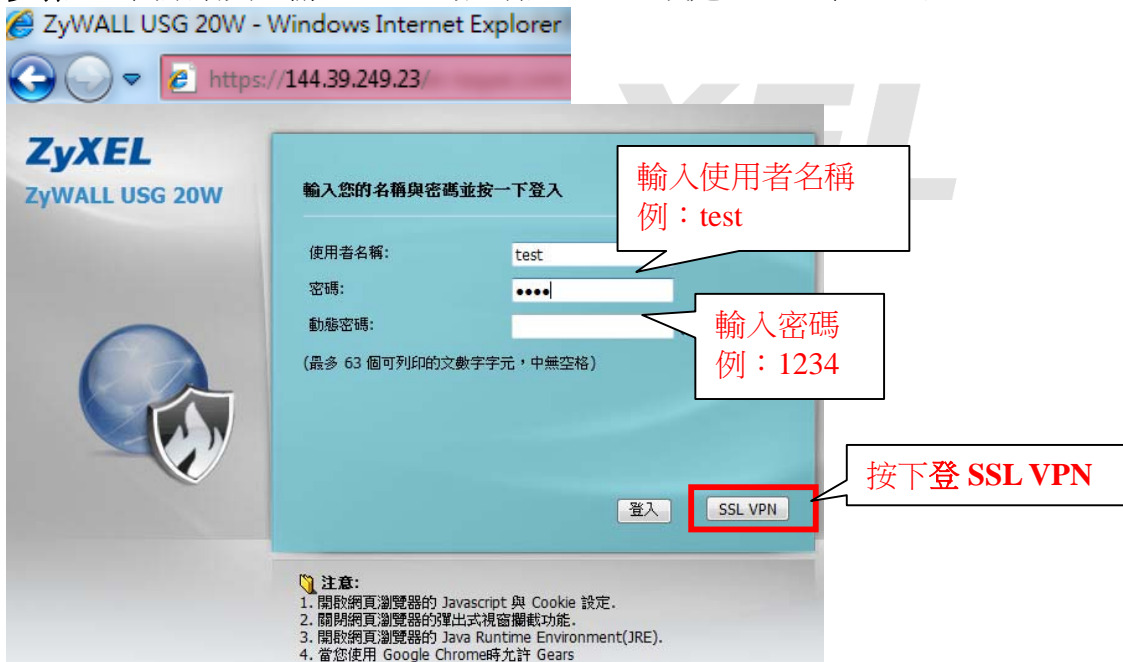
驗證 1

A 電腦，原本不能存取 <http://www.facebook.com> 網站，測試透過 SSL VPN 登入 USG 後，是否可以正常登入！

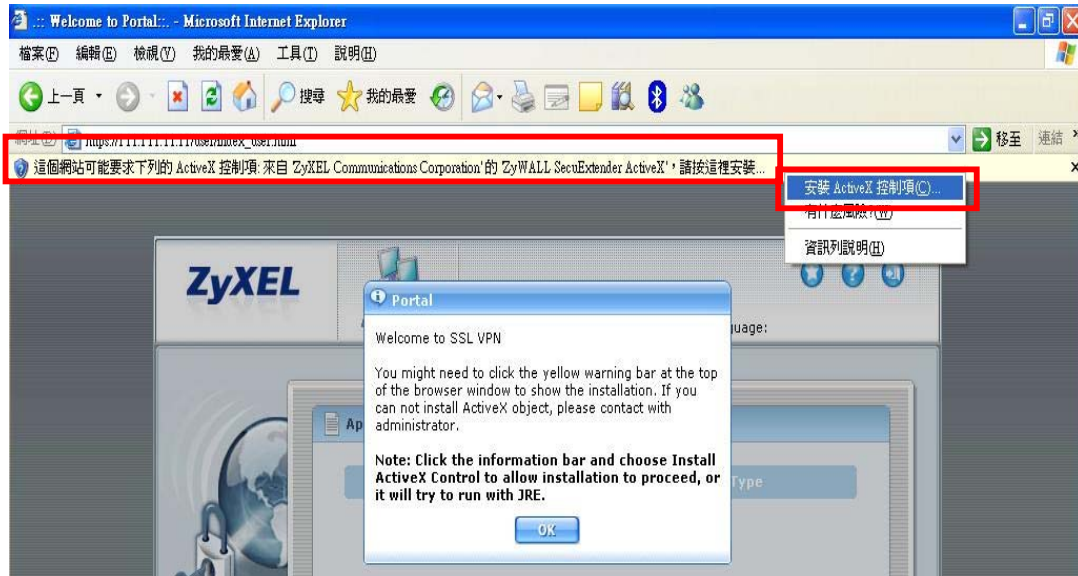
- 確認 A 電腦，無法存取 <http://www.facebook.com>



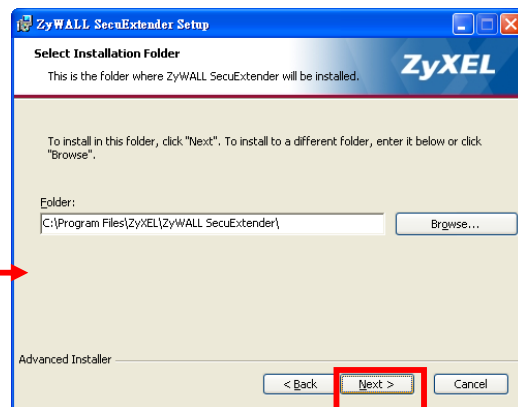
步驟一：開啟網頁，輸入 USG 的遠端登入 IP，或是 DDNS 位置，登入 SSL VPN

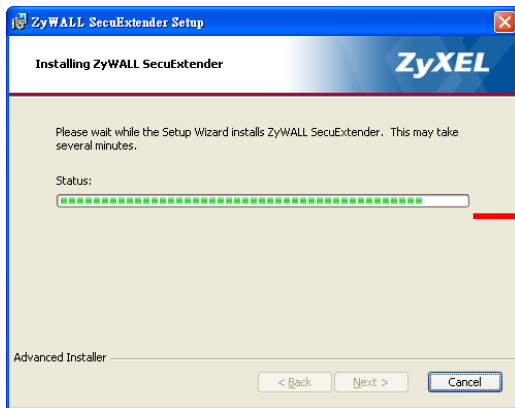
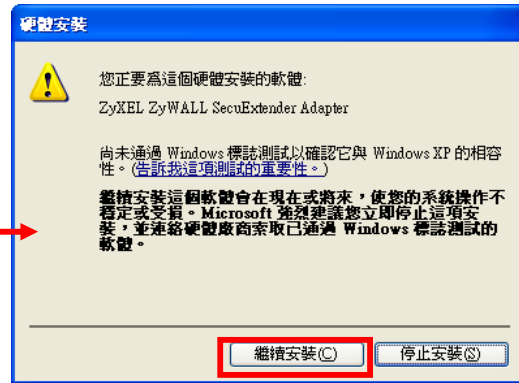
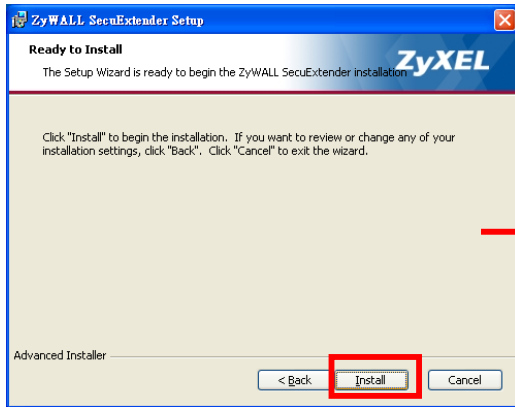


步驟二：登入後，若為首次登入，網頁上則會出現要求您安裝”ZyWALL SecuExtender ActiveX”的控制項，請在該對話框按右鍵，選擇”安裝 ActiveX 控制項

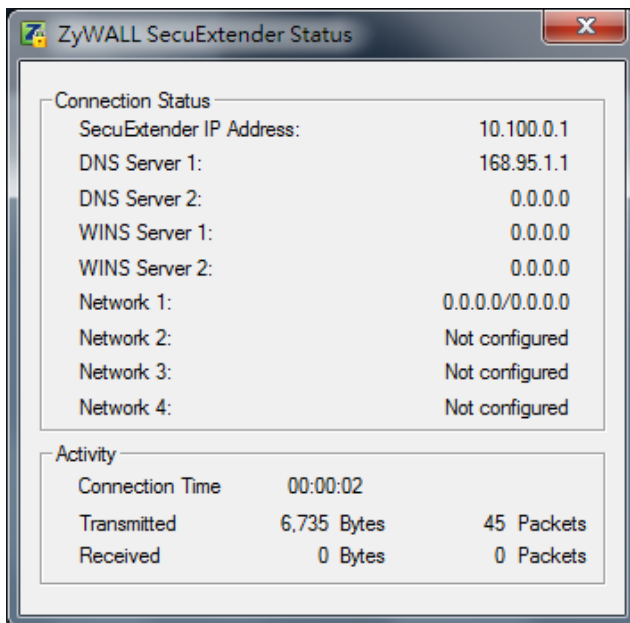


步驟三：安裝 ZyWALL SecuExtender ActiveX 軟體

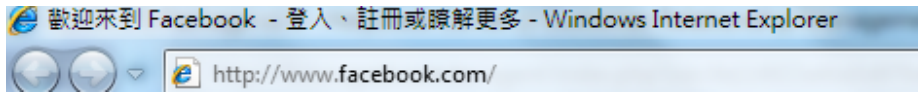




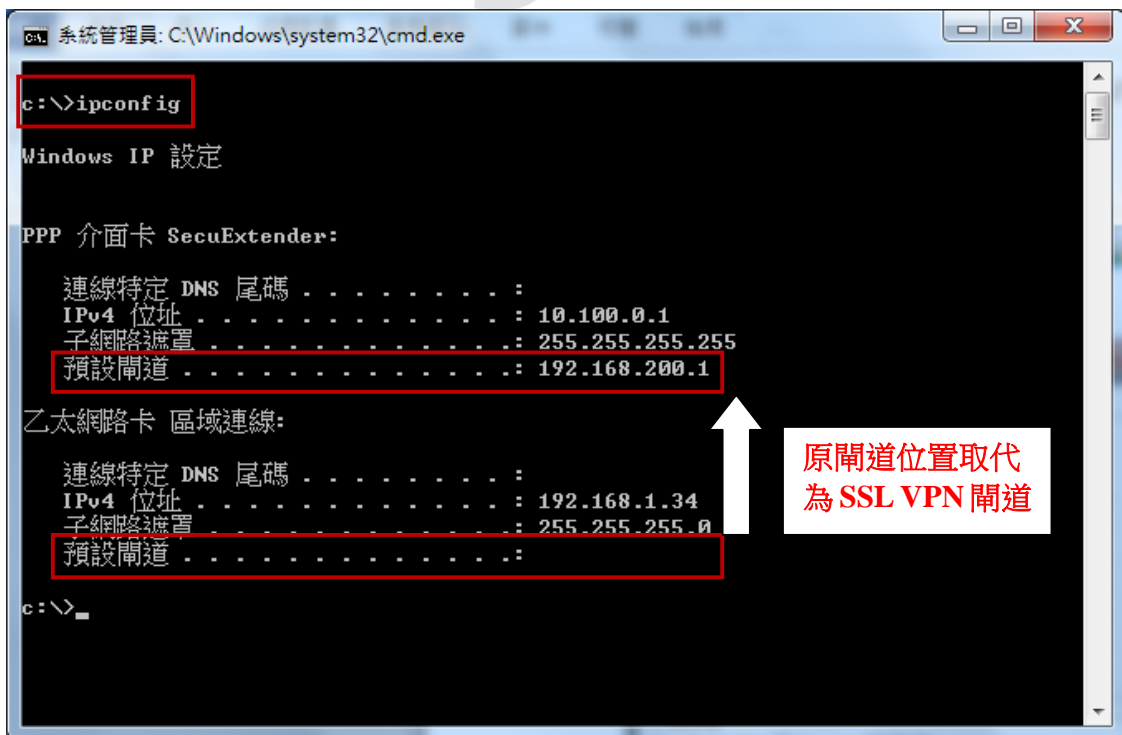
步驟四：當安裝完成，電腦右下方會出現圖示，並會顯示您所取得的 IP 及 DNS 相關資訊



步驟五：重新嘗試開啟 <http://www.facebook.com>



※ 驗證 強制所有用戶端流量進入 **SSL VPN 通道** 功能
確認當由遠端登入 **USG SSL VPN** 後，電腦原預設閘道即會消失，而被 **SSL VPN** 的閘道位置所取代。



驗證 2

存取 USG SSL VPN 底下網段 192.168.2.34 資源

```
系統管理員: C:\Windows\system32\cmd.exe
c:\>ping 192.168.2.34

Ping 192.168.2.34 <使用 32 位元組的資料>:
回覆自 192.168.2.34: 位元組=32 時間=57ms TTL=127
回覆自 192.168.2.34: 位元組=32 時間=85ms TTL=127
回覆自 192.168.2.34: 位元組=32 時間=82ms TTL=127
回覆自 192.168.2.34: 位元組=32 時間=36ms TTL=127

192.168.2.34 的 Ping 統計資料:
    封包: 已傳送 = 4, 已收到 = 4, 已遺失 = 0 (0% 遺失),
    大約的來回時間 <毫秒>:
        最小值 = 36ms, 最大值 = 85ms, 平均 = 65ms
```

可以順利 Ping 到電腦並
可存取網芳資源喔！

