第二十章

Web VPN / SSL VPN

由於 Internet 的普遍應用，企業遠端安全登入的需求也與日俱增。對於使用者而言， 最方便安全的解決方案莫過於 SSL VPN，用戶端不需要安裝任何軟體或硬體，只要使用標準的瀏覽器，就可通過簡單的 SSL 安全加密協定傳輸資料。

【VPN】專有名詞解釋：

DES 說明如下：

- 資料加密標準（Data Encryption Standard）是一種 NIST 標準安全加密金鑰方法，使用的加密金鑰爲 56 位元。

3DES 說明如下：

- 提供比 DES 更加安全的三重資料加密標準(Triple Data Encryption Standard,3DES)安全加密金鑰方法，使用的加密金鑰爲 168 位元。

AES 說明如下：

- 爲高階加密模式其標準比 DES 的加密標準更加嚴謹，DES 加密金鑰長度爲 56 位元，AES 加密金鑰長度則高達 128 位元、192 位元、以及 256 位元。

【設定】名詞解釋：

用戶端 **VPN IP** 說明如下：

- 可設定用戶端和 NUS-MS3000 建立 SSL VPN 連線時的認證帳號、配發的 IP、加密演算法、通訊協定、使用埠號和連線時間。

 SSL VPN IP 範圍不可和內部(LAN、Multiple Subnet、DMZ)、外部(WAN)及 PPTP 伺服器的網段相同。

伺服器端內部子網路 說明如下：

- 設定用戶端可存取的伺服器端子網路。

【狀態】視窗表格內圖示與名詞名稱定義：

用戶名稱 說明如下：

- 顯示用戶端所使用的認證名稱。

真實 IP 說明如下：

- 顯示用戶端所使用的真實 IP。

VPN IP 說明如下：

- 顯示 NUS-MS3000 配發給用戶端的 IP。

連線歷時 說明如下：

- 顯示用戶端與 NUS-MS3000 的持續連線時間。

變更 說明如下：

- 可中斷和 NUS-MS3000 建立的 SSL VPN 連線。*（如圖 20-1）*

用戶名稱	真實 IP	VPN IP	連線歷時	變更
沒有資料				

圖 20-1 狀態視窗表格

外部用戶端和 NUS-MS3000 設定 Web/SSL VPN 連線的方法

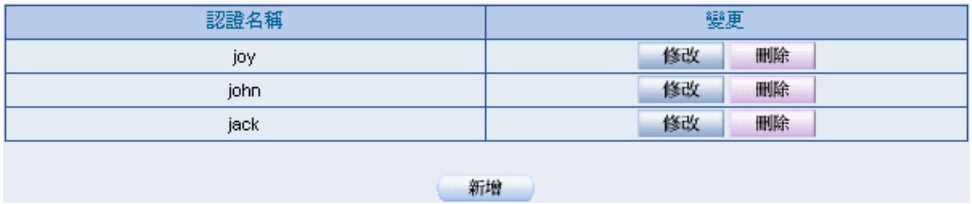
步驟1. 於【介面位址】之【外部網路】功能中，啓動 HTTPS 功能：*（如圖 20-2）*


負載模式: 自動分配 （建議使用 自動分配）

外部網路介面	連線模式	IP位址	飽和連線數	Ping	HTTP	HTTPS	變更	優先權
1	指定 IP 位址	61.11.11.11	1	✓	✓	✓	修改	1
2	指定 IP 位址	211.22.22.22	1	✓	✓	✓	修改	2
3	(關閉)	---	0	---	---	---	修改	0
4	(關閉)	---	0	---	---	---	修改	0

圖 20-2 外部網路界面設定

步驟2. 於【認證表】之【認證用戶】功能中，新增下列設定：*（如圖 20-3）*



認證名稱	變更
joy	修改 刪除
john	修改 刪除
jack	修改 刪除

新增

圖 20-3 認證用戶設定

步驟3. 於【認證表】之【認證群組】功能中，新增下列設定：*（如圖 20-4）*

群組名稱	成員	Radius	POP3	LDAP	變更
laboratory	joy, john, jack				修改 刪除 暫停

新增

圖 20-4 認證群組設定

步驟4. 於【Web VPN / SSL VPN】之【設定】功能中，新增下列設定：

- 按下【修改】鈕。*（如圖 20-5）*
- 【啓動 Web VPN】功能。
- 【VPN IP 範圍】輸入 192.168.222.0 / 255.255.255.0。
- 【加密演算法】選擇 3DES。
- 【通訊協定】選擇 TCP。
- 【伺服器埠號】輸入預設值 1194。
- 【認證用戶或群組】選擇 laboratory。
- 閒置時間設爲 0。
- 按下【確定】鈕。
- 會自動新增內部網路介面位址，爲允許用戶端存取的網段。*（如圖 20-6）*

圖 20-5 啟動Web VPN設定

圖 20-6 Web VPN啟動完成

步驟5. 客戶端於瀏覽器中輸入下列設定：

- 於【網址】輸入 http://61.11.11.11/sslvpn 或 http://61.11.11.11/webvpn（即 NUS-MS3000 介面位址加上 sslvpn 或 webvpn 字串）。
- 按下【Enter】鈕。*（如圖 20-7）*
- 於【安全性警訊】視窗中，按下【是】鈕。
- 於【警告 - 安全】視窗中，按下【是】鈕。
- 於【警告 - HTTPS】視窗中，按下【是】鈕。
- 再次於【警告 - 安全】視窗中，按下【是】鈕。
- 於【Authentication】視窗中，輸入【認證名稱】爲 john 和【認證密碼】爲 123456789。*（如圖 20-8, 圖 20-9, 圖 20-10, 圖 20-11, 圖 20-12）*
- 按下【確定】鈕。*（如圖 20-13, 圖 20-14）*

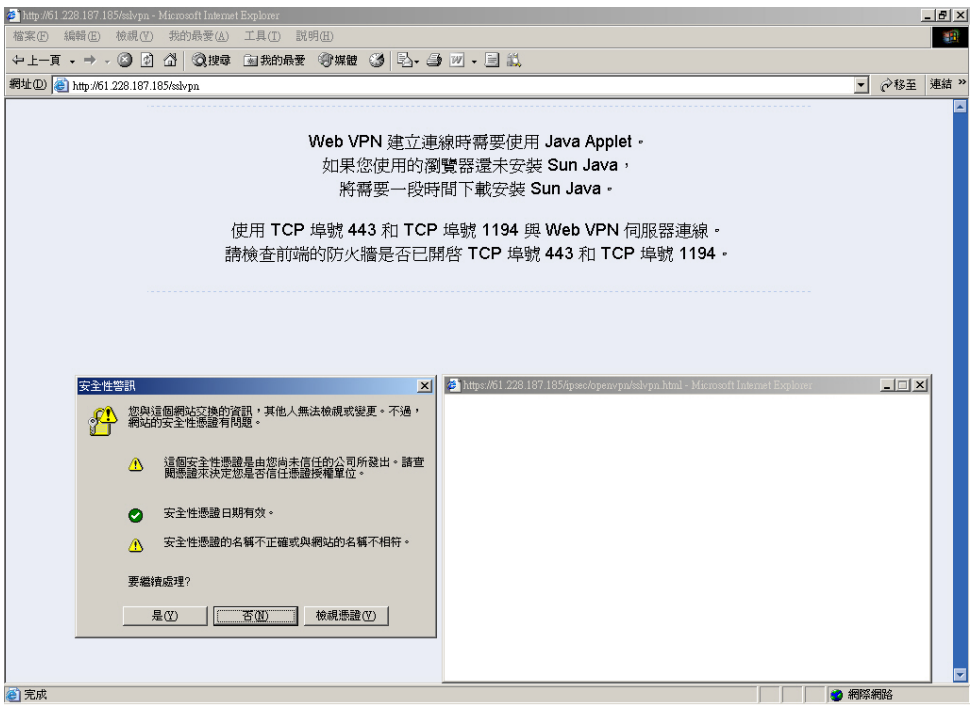


圖 20-7 登入SSL VPN連線畫面

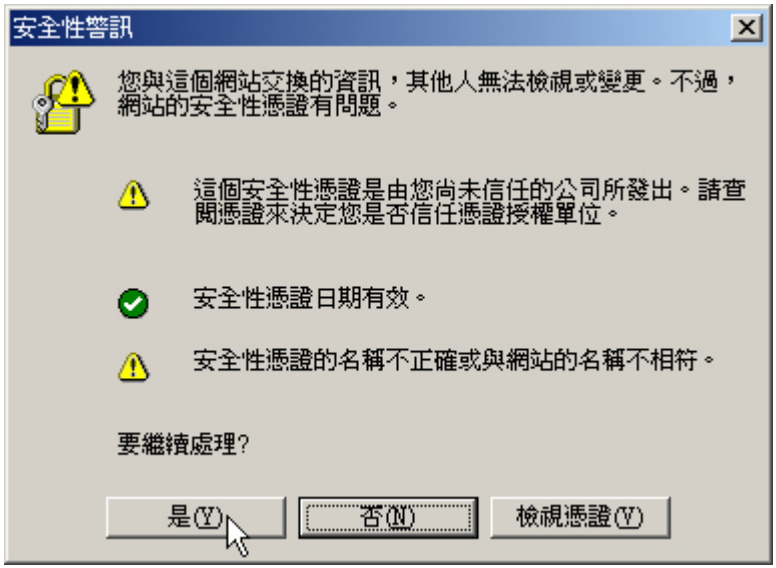


圖 20-8 安全性警訊視窗

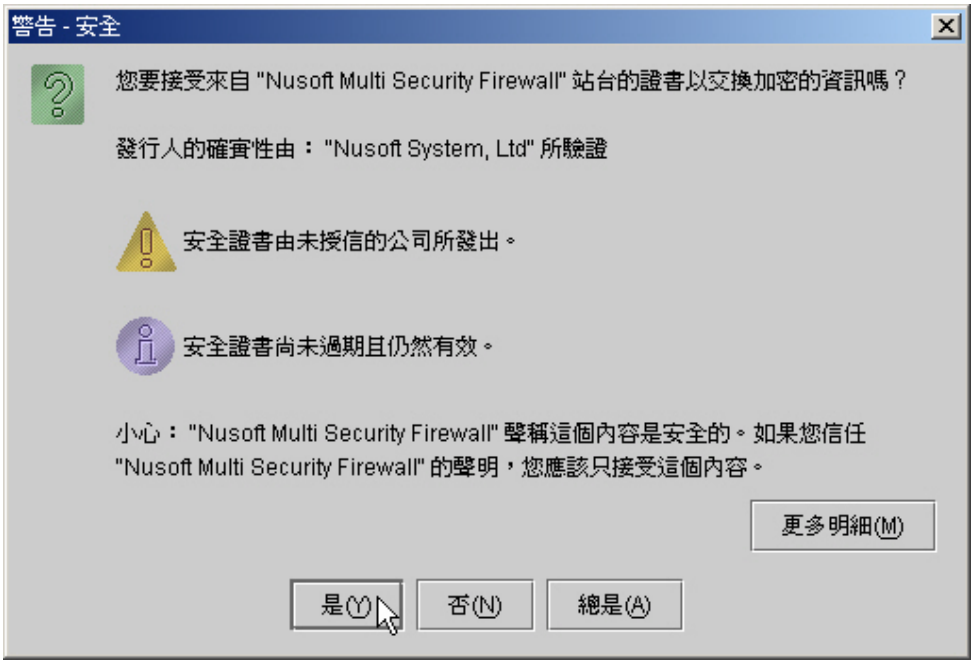


圖 20-9 警告 - 安全視窗

圖 20-10 警告 - HTTPS視窗

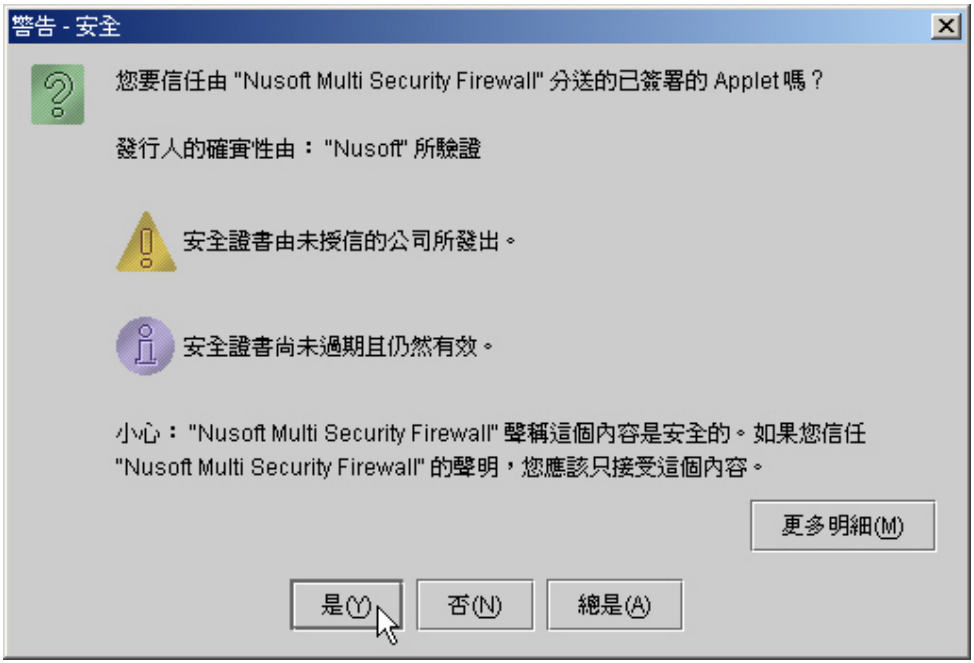


圖 20-11 警告 - 安全視窗

圖 20-12 Authentication視窗

圖 20-13 SSL VPN連線中

圖 20-14 完成SSL VPN連線

步驟6. 於【Web VPN / SSL VPN】之【狀態】功能中，顯示如下連線訊息：*（如圖20-15）*

用戶名稱	眞實 IP	VPN IP	連線歷時	變更
john	220.132.112.108	192.168.222.10	0:01:24	斷線

圖 20-15 SSL VPN連線狀態

當用戶端的 PC 未安裝 SUN JAVA Runtime Environment 軟體，於登入 SSL VPN 連線畫面時，會自動下載安裝此軟體（*如圖 20-16, 圖 20-17*）。

圖 20-16 安裝Java Runtime Environment Plug-in CA確認畫面

圖 20-17 Java Runtime Environment Plug-in安裝中