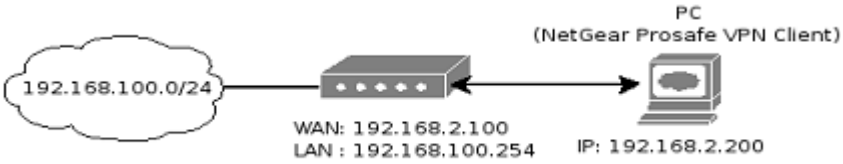
How to establish a VPN tunnel between WMU9000 VPN and NetGear Prosafe VPN Client?



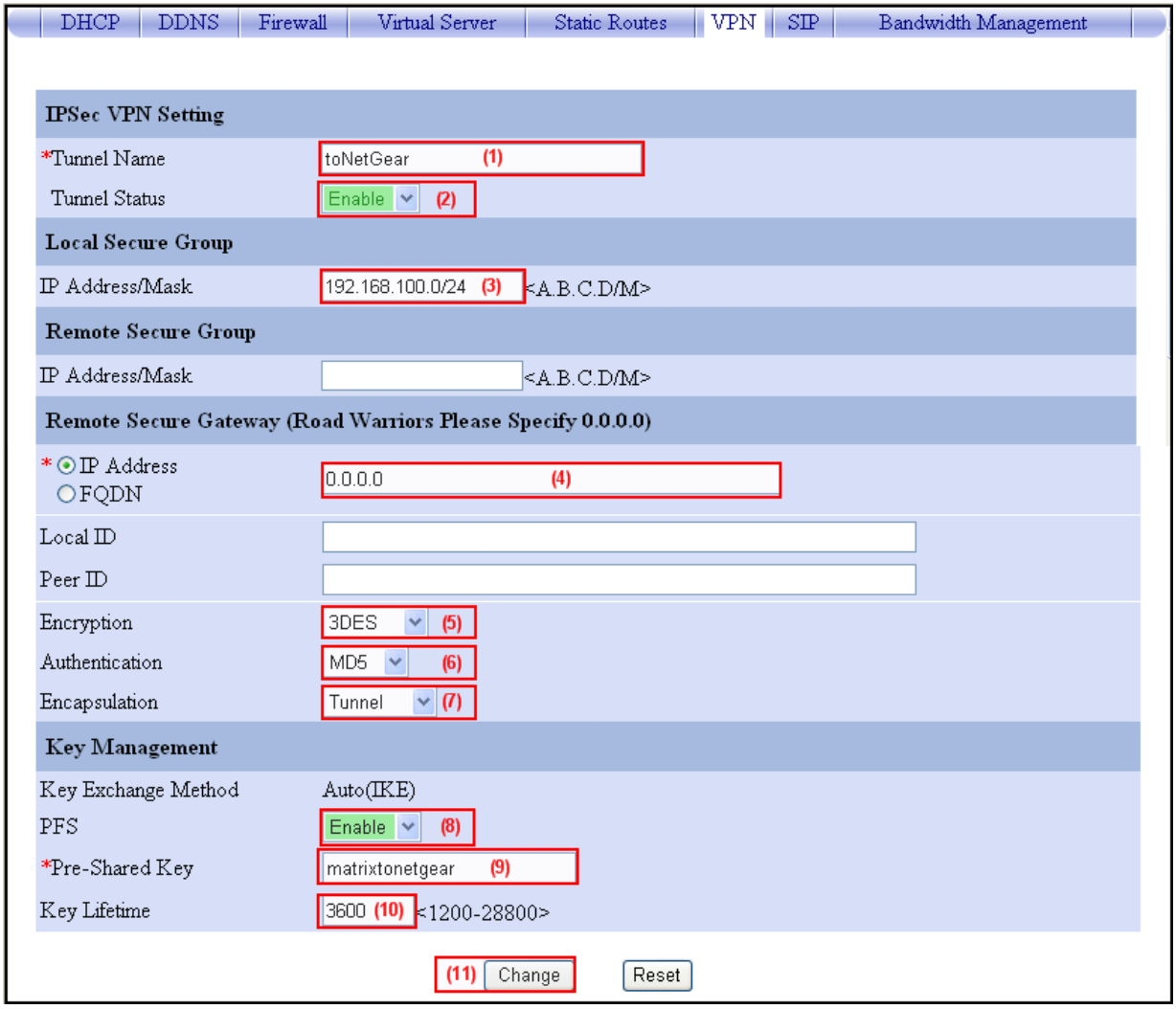
VPN setting Information:

Phase 1 Lifetime: 3600.
Phase 2 Lifetime: 3600.
Data Encryption/ Authentication: esp-3des-md5.
IKE Diffie-Hellman Group: Group 2 (1024-bits).
Perfect Forward Secrecy (PFS): Enable.
Pre-Shared Key: matrixtonetgear.

Procedure:

WMU 9000 VPN IPSec Setting :

1. Configure the IPSec settings of the WMU 9000 VPN.

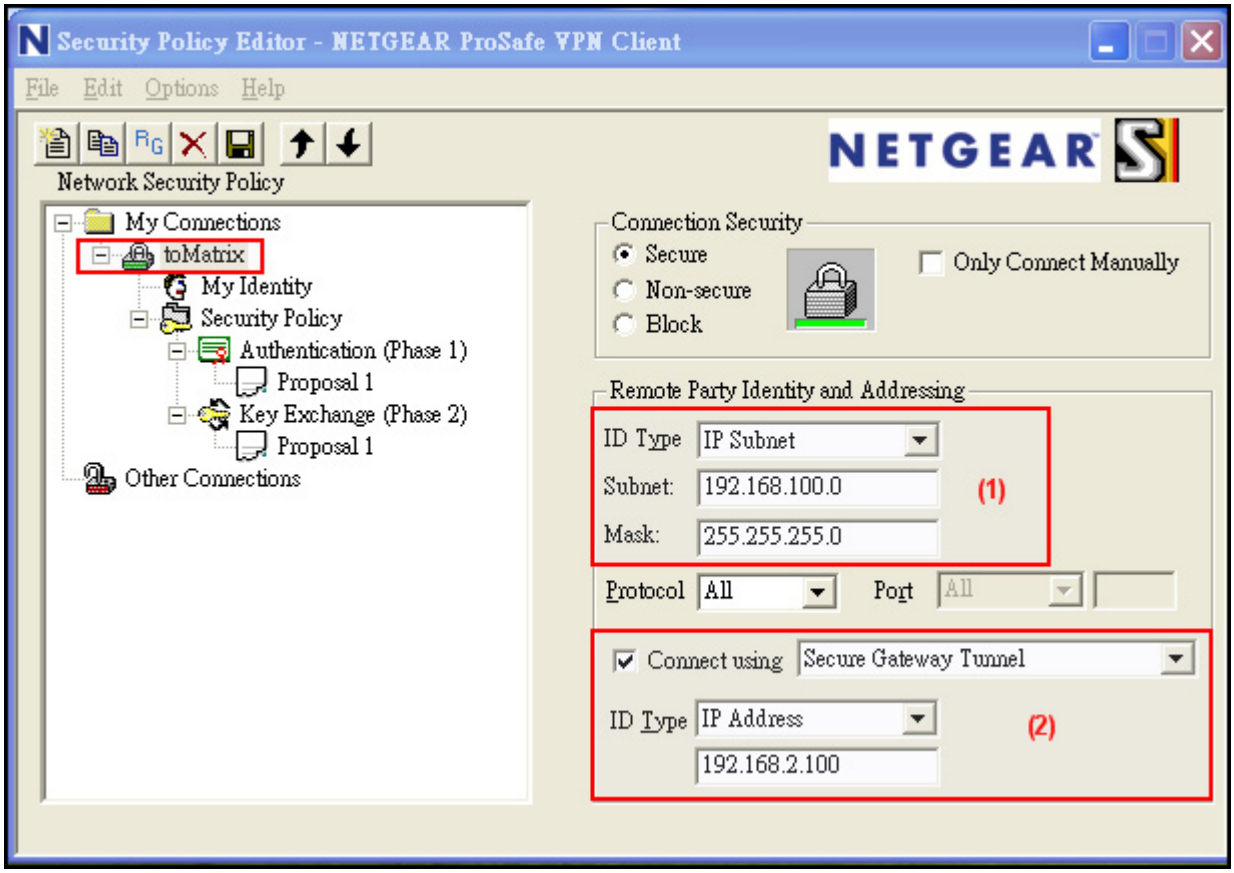


Step (1): Type the Tunnel name for ***Tunnel name***: [toNetGear].
Step (2): Choose the Tunnel Status: [Enable].

Step (3): Type the Local Secure Subnet IP address and maskbit for ***Local Secure Group***: [192.168.1.0/24].
Step (4): Type the Peer VPN Gateway IP Address for ***Remote Secure Gateway***: [0.0.0.0].
Step (5): Choose the Data Encryption Algorithm: [3DES].
Step (6): Choose the Data Authentication Algorithm: [MD5].
Step (7): Choose the mode of the Encapsulation: [Tunnel].
Step (8): Choose the Perfect Forward Secrecy (PFS): [Enable]
Step (9): Type the Pre-Shared Key for ***Pre-Shared Key***: [matrixtonetgear].
Step (10): Type the IKE (Phase 1) lifetime for ***Key Lifetime***: [3600].
Step (11): Click "Change" button to setup this IPSec VPN setting.

Now, in the following, we describe the procedure to set up the IPSec VPN in the NetGear Prosafe VPN Client.

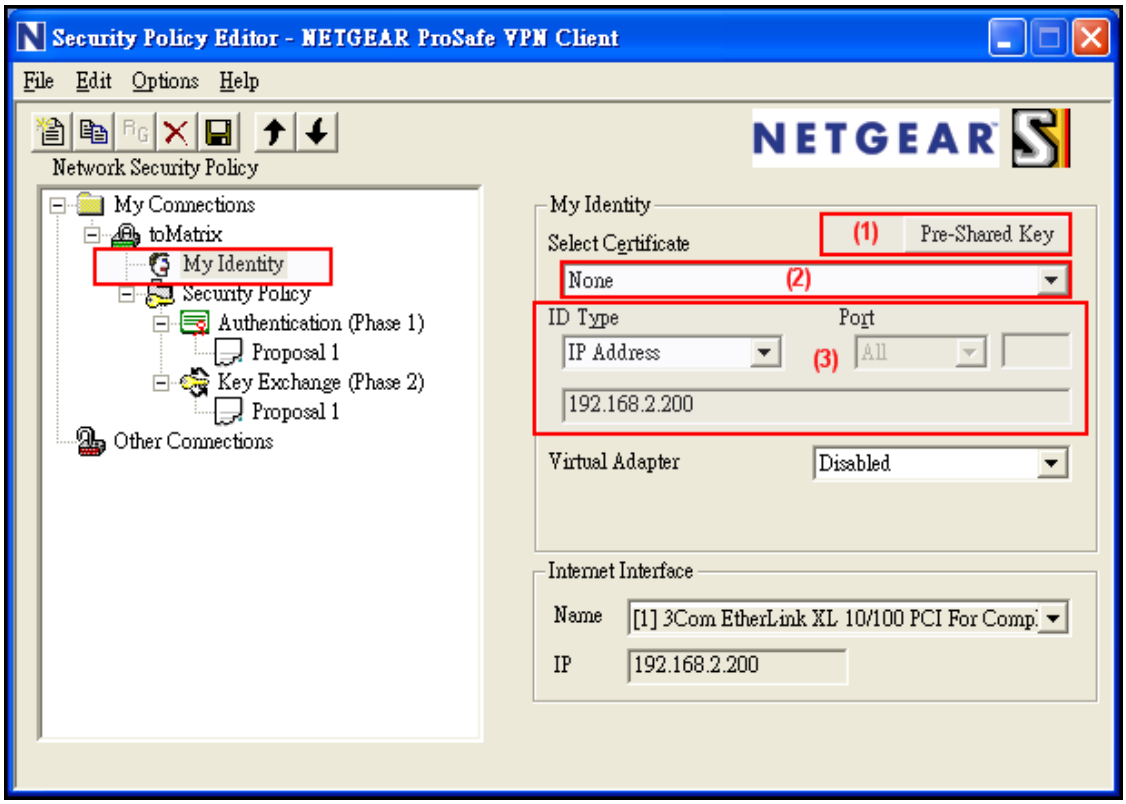
1. Add an VPN connection and configure the settings of the VPN connection.



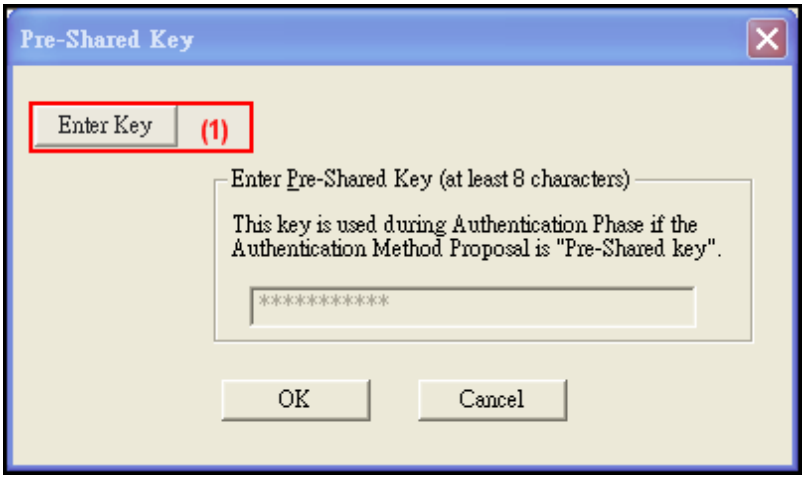
Step (1): First, choose the ID Type of the Remote Secure Subnet: [IP Subnet].
Second, type the Remote Secure Subnet IP address for ***Subnet***: [192.168.100.0].
Finally, type the Remote Secure Subnet Mask for ***Mask***: [255.255.255.0]

Step (2): First, enable the check box and choose the connect type: [Secure Gateway Tunnel].
Second, choose the ID Type of the Remote VPN Gateway: [IP Address].
Finally, type the ip address of the Remote VPN Gateway: [192.168.2.100].

2. Configure the settings of my identity.



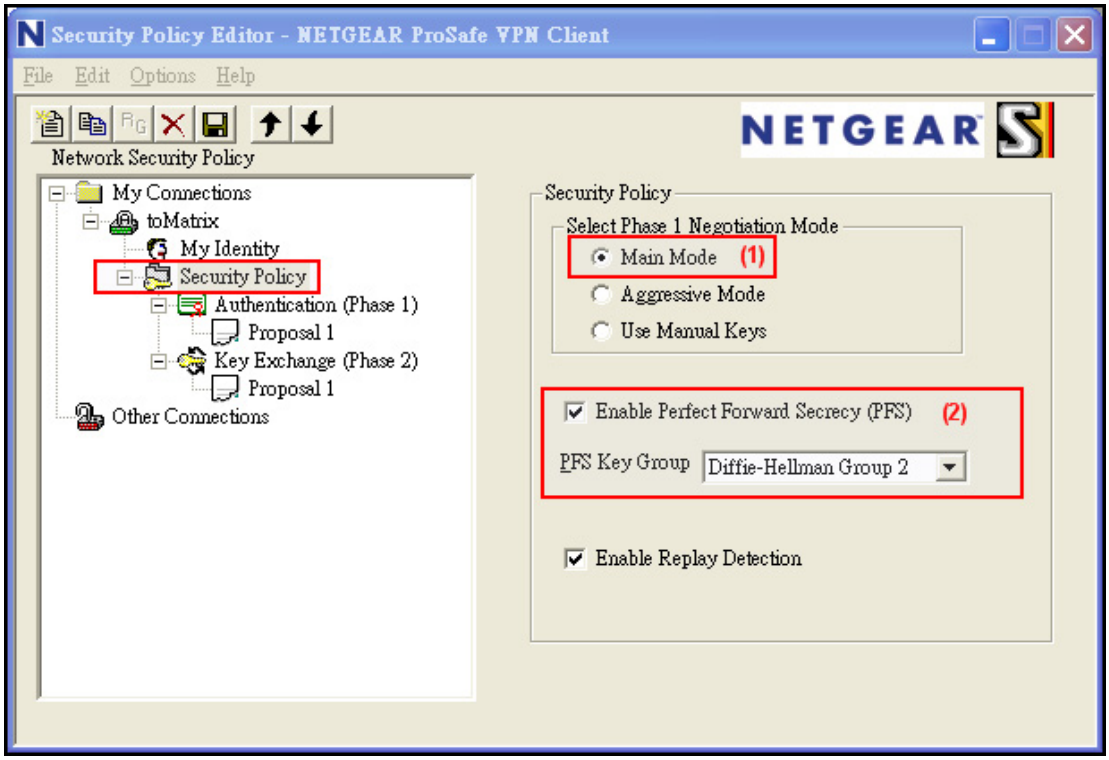
Step (1): Click "Pre-Shared Key" button to enter the Pre-Shared Key. Please refer to the following figure.



1.1: Click the "Enter Key" button to enter the Pre-Shared Key: [matrixtonetgear].

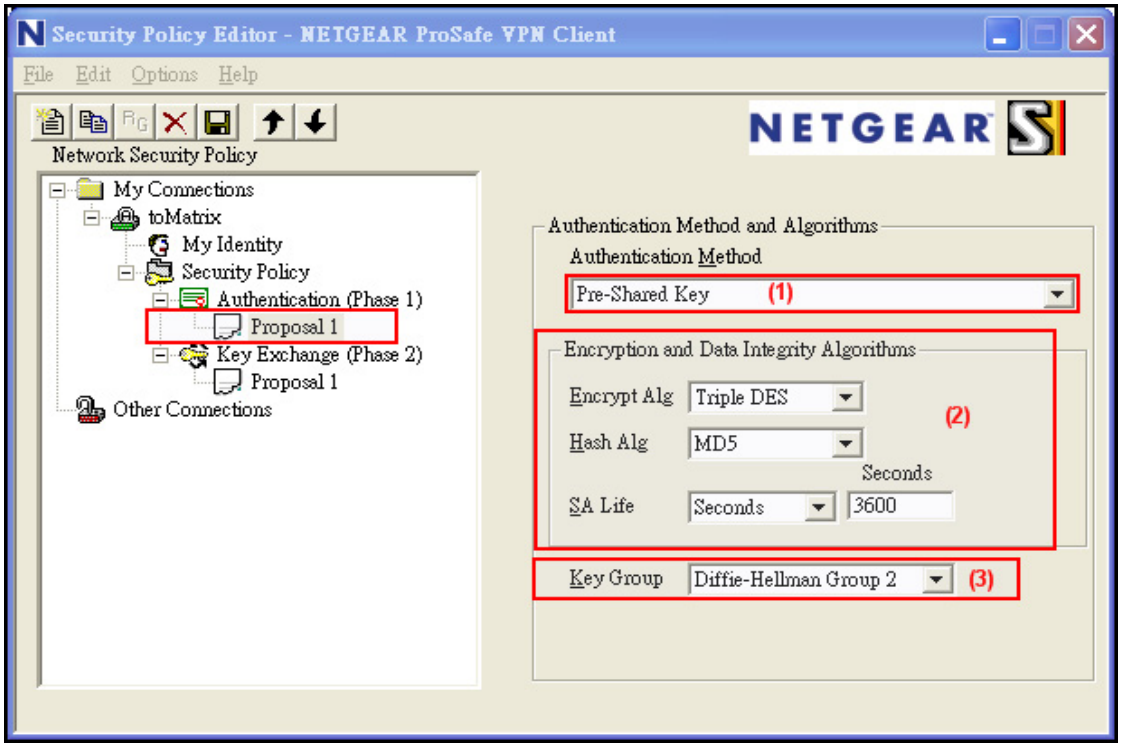
Step (2): Choose the Certificate:[None].
Step (3): Choose the ID Type of the Local VPN Gateway: [IP Address].
And, type the ip address of the Local VPN Gateway: [192.168.2.200].

3. Configure the settings of the Security Policy.



Step (1): Select the Phase 1 Negotiation Mode: [Main Mode].
Step (2): Enable the ***Enable Perfect Forward Secrecy (PFS)*** check box. And, choose the PFS Key Group: [Diffie-Hellman Group 2].

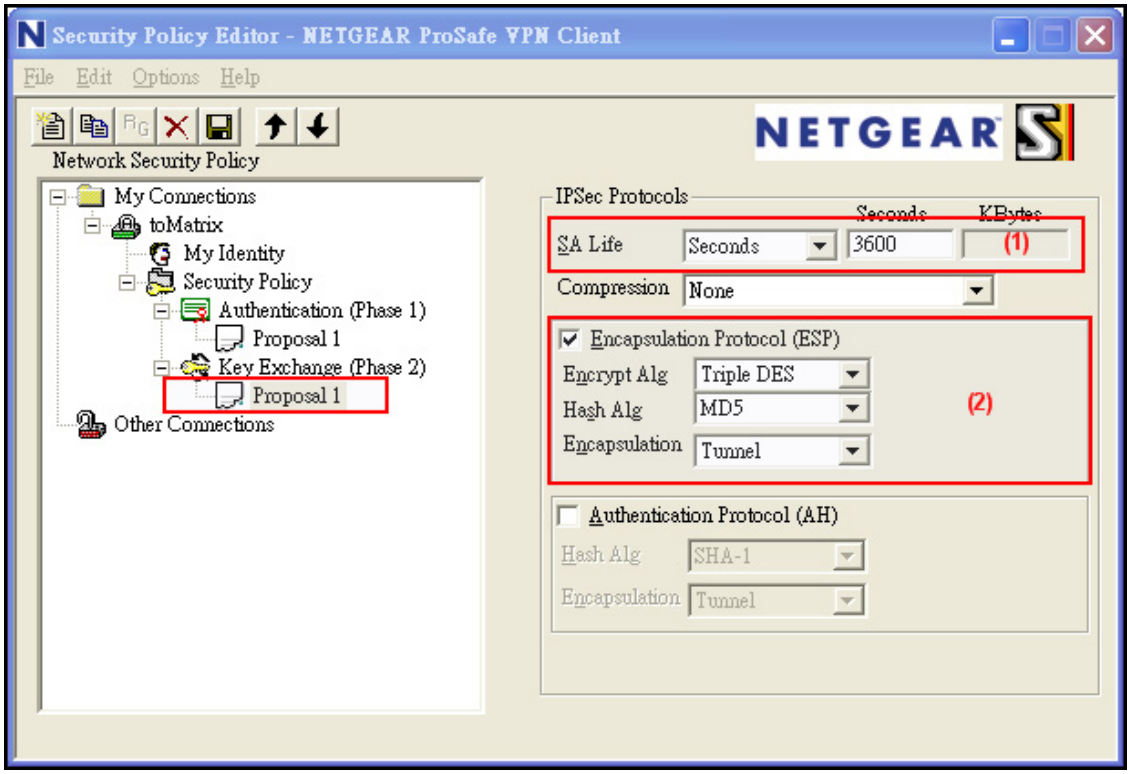
4. Configure the settings of the Phase 1 (Authentication).



Step (1): Choose the Authentication Method: [Pre-Shared Key].

Step (2): Configure the Encryption and Data Integrity Algorithms.
First, choose the Encrypt Algorithm: [Triple DES].
Second, choose the Hash Algorithm: [MD5].
Next, choose the SA life type: [Seconds].
Finally, type the lifetime of the Phase 1: [3600].
Step (3): Choose the Key Group: [Diffie-Hellman Group 2].

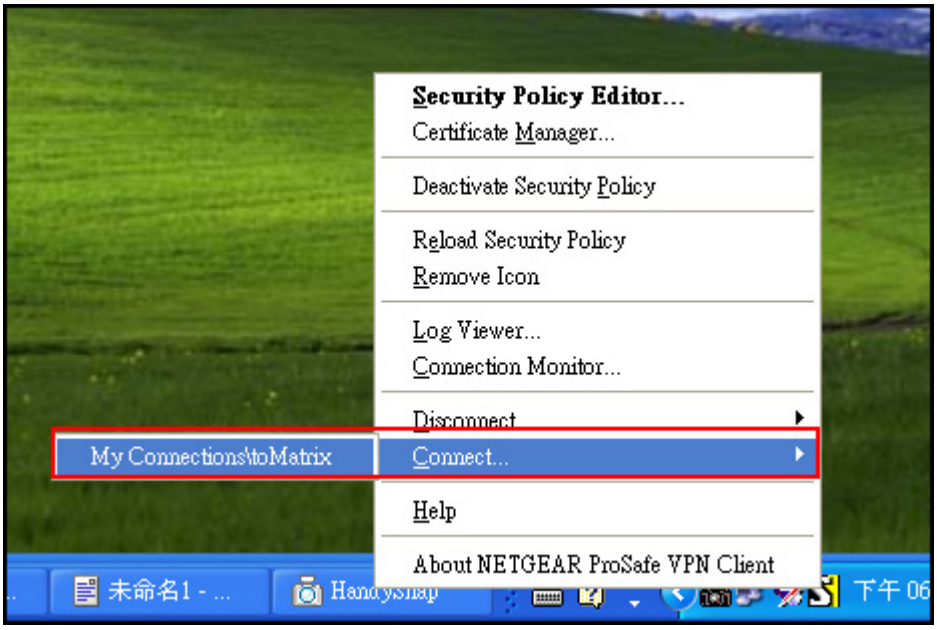
5. Configure the settings of the Phase 2 (Key Exchange).



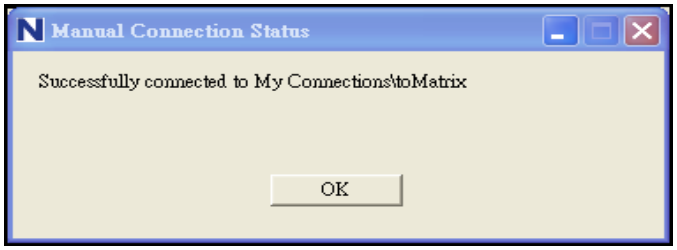
Step (1): Choose the SA life type: [Seconds]. And, type the lifetime of the Phase 1: [3600].

Step (2): First, enable the ***Encapsulation Protocol (ESP)*** check box.
Second, choose the Encrypt Algorithm: [Triple DES].
Next, choose the Hash Algorithm: [MD5].
Finally, choose the mode of the encapsulation: [Tunnel].

6. Connect the VPN connection (toMatrix).



7. Establish the IPSec VPN Tunnel. Please refer the following figure.



8. The statuses of the IPSec VPN connection.