How to establish a VPN tunnel between WMU9000 VPN and Green Bow VPN Client with DDNS?

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: ovislink.

Procedure:

WMU 9000 DDNS Setting:

Step (1): First, select "Enable" to enable DDNS function,
Second, input DDNS user name and password,
Third, input your host name

Step (2): Make sure the DDNS has worked and has updated the correct IP

WMU 9000 VPN IPSec Setting :

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

IPSec VPN Setting

*Tunnel Name: ovislink (1)
Tunnel Status: Enable (2)

Local Secure Group
IP Address/Mask: 192.168.1.0/24 (3) <A.B.C.D/M>

Remote Secure Group
IP Address/Mask: <A.B.C.D/M>

Remote Secure Gateway (Road Warriors Please Specify 0.0.0.0)
* IP Address / FQDN: 0.0.0.0 (4)

Local ID
Peer ID

Encryption: 3DES (5)
Authentication: MD5 (6)
Encapsulation: Tunnel (7)

Key Management
Key Exchange Method: Auto(IKE)
PFS: Enable (8)
*Pre-Shared Key: ovislink (9)
Key Lifetime: 3600 (10) <1200-28800>

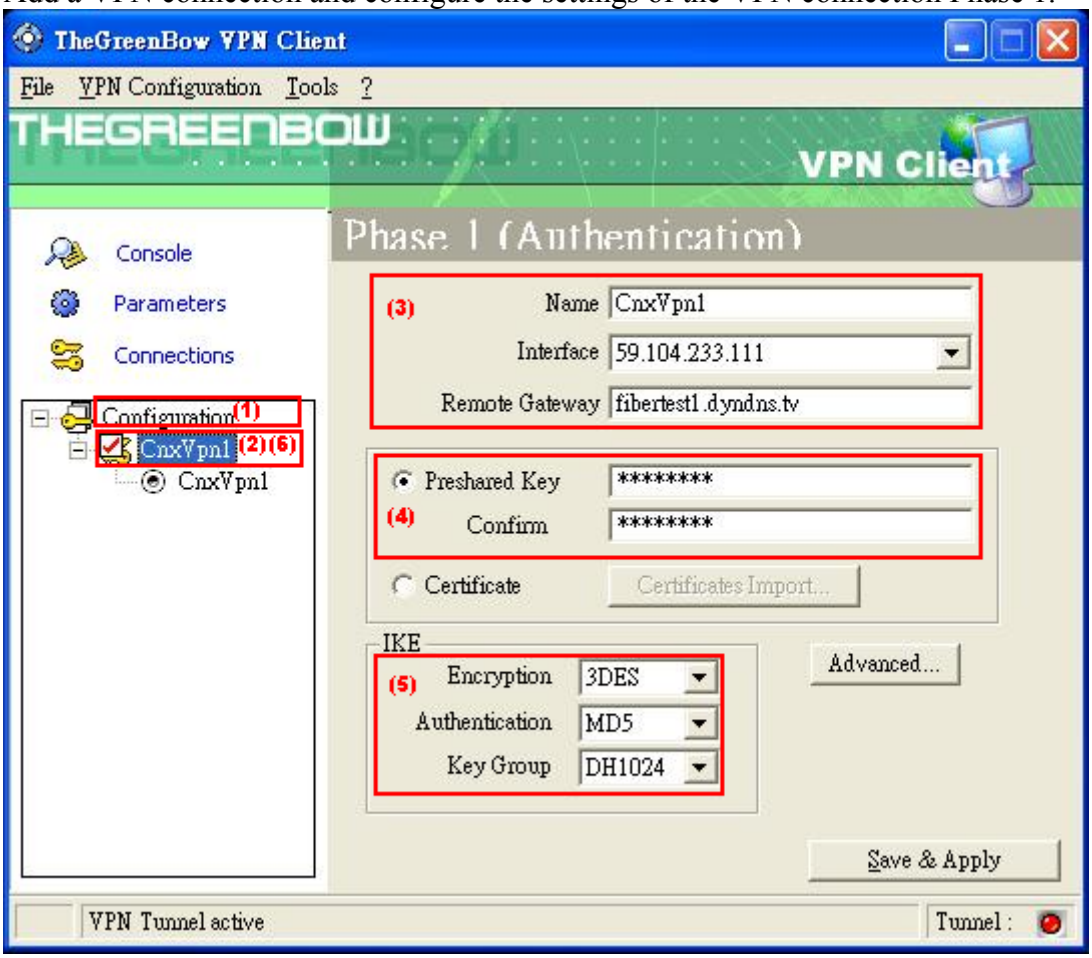
(11) Change | Reset

Delete this tunnel

Step (1): Type the Tunnel name for ***Tunnel name***: [ovislink].
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***: [ovislink].
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 Green Bow VPN Client.

1. Add a VPN connection and configure the settings of the VPN connection Phase 1.

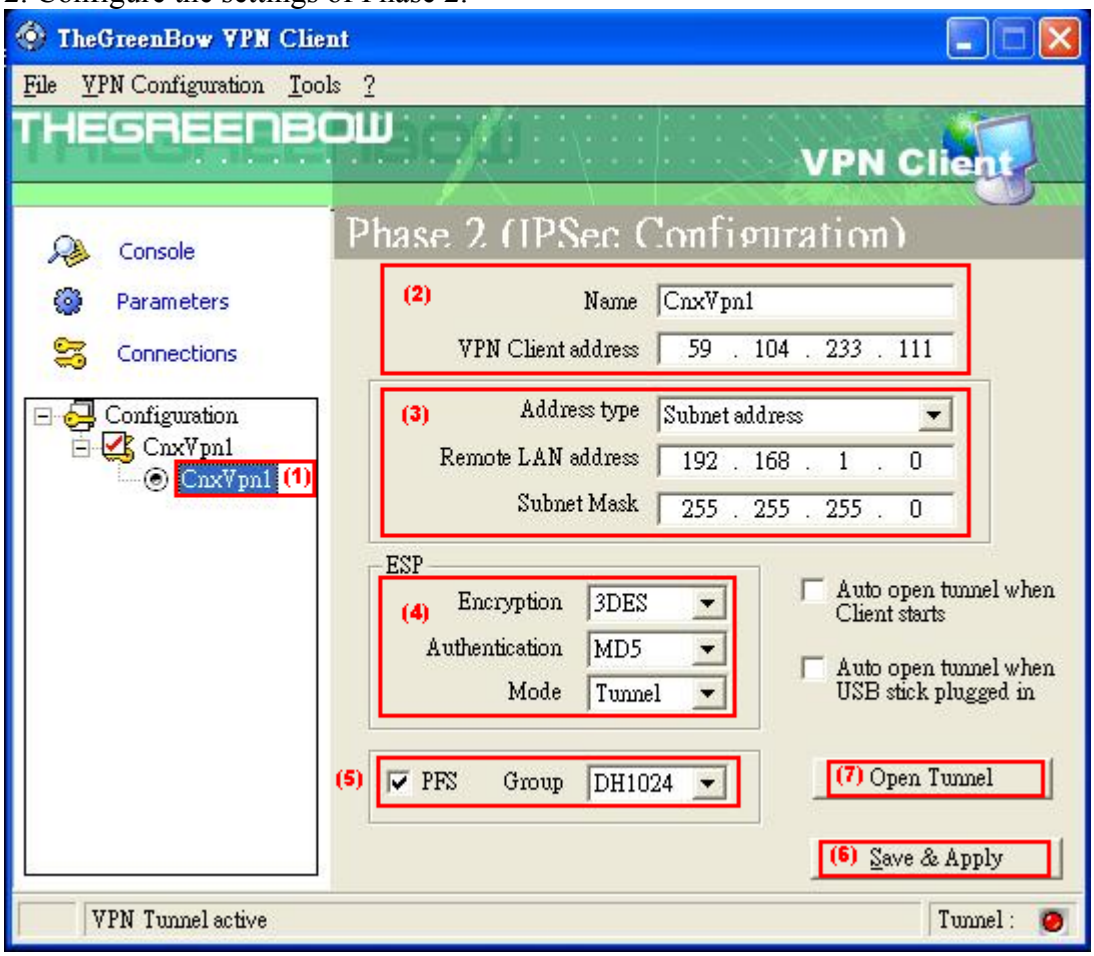


Step (1): Right click on Configuration, and select "New Phase 1"
Step (2): Click on the "CnxVpn1"
Step (3): First, type the name for ***Phase 1***: [CnxVpn1].
Second, select Local Interface:[59.104.233.111]
Third, input Remote Gateway:[fibertest1.dyndns.org]
Step (4): Type the Preshare key: [ovislink].

Step (5): First, select Encryption: [3DES].
Second, select Authentication:[MD5]
Third, select Key Group:[DH1024]

Step (6): Right click on the Phase 1 and select "Add Phase 2"

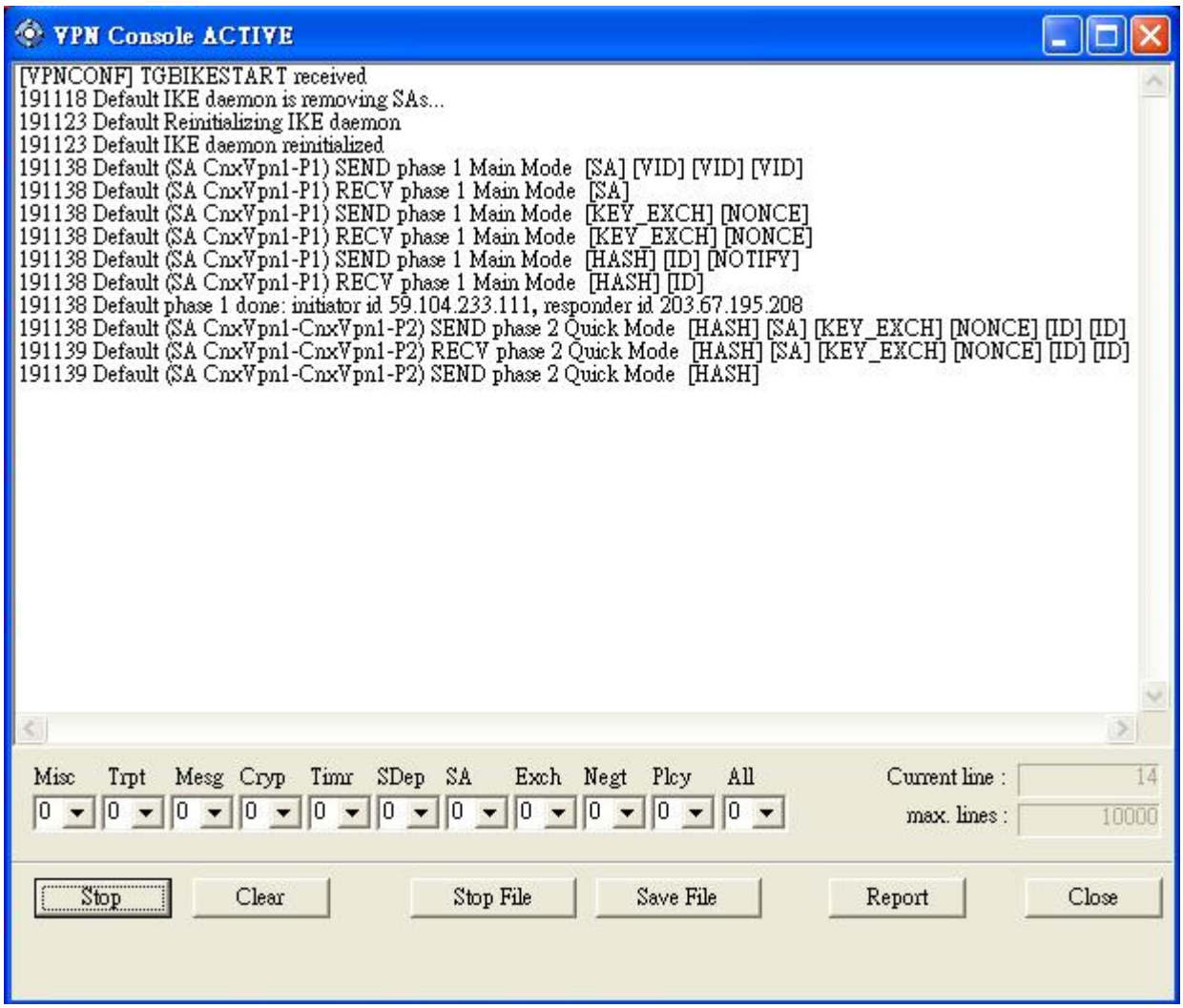
2. Configure the settings of Phase 2.



Step (1): Click on Phase 2

Step (2): First, type the name for ***Phase 1***: [CnxVpn1].
Second, type Local VPN Client address:[59.104.233.111]
Step (3): First, select Remote VPN address type:[Subnet address]
Second, type the ip address of Remote LAN address: [192.168.1.0],
And Remote Subnet Mask:[255.255.255.0]
Step (4): First, select Encryption: [3DES].
Second, select Authentication:[MD5]
Third, select mode:[Tunnel]
Step (5): Enable the PFS check box and select Group:[DH1024]
Step (6): Click on the Save & Apply button
Step (6): Click on the Open Tunnel button to establish the VPN tunnel.

3.The statuses of the IPSec VPN connection.
Step (1): Click on Console in main page, then it will show as bellow


VPN Console ACTIVE
[VPNCONF] TGBIKESTART received
191118 Default IKE daemon is removing SAs...
191123 Default Reinitializing IKE daemon
191123 Default IKE daemon reinitialized
191138 Default (SA CnxVpn1-P1) SEND phase 1 Main Mode [SA] [VID] [VID] [VID]
191138 Default (SA CnxVpn1-P1) RECV phase 1 Main Mode [SA]
191138 Default (SA CnxVpn1-P1) SEND phase 1 Main Mode [KEY_EXCH] [NONCE]
191138 Default (SA CnxVpn1-P1) RECV phase 1 Main Mode [KEY_EXCH] [NONCE]
191138 Default (SA CnxVpn1-P1) SEND phase 1 Main Mode [HASH] [ID] [NOTIFY]
191138 Default (SA CnxVpn1-P1) RECV phase 1 Main Mode [HASH] [ID]
191138 Default phase 1 done: initiator id 59.104.233.111, responder id 203.67.195.208
191138 Default (SA CnxVpn1-CnxVpn1-P2) SEND phase 2 Quick Mode [HASH] [SA] [KEY_EXCH] [NONCE] [ID] [ID]
191139 Default (SA CnxVpn1-CnxVpn1-P2) RECV phase 2 Quick Mode [HASH] [SA] [KEY_EXCH] [NONCE] [ID] [ID]
191139 Default (SA CnxVpn1-CnxVpn1-P2) SEND phase 2 Quick Mode [HASH]
Misc Trpt Mesg Cryp Timr SDep SA Exch Negt Plcy All
0 0 0 0 0 0 0 0 0 0 0
Current line : 14
max. lines : 10000
Stop
Clear
Stop File
Save File
Report
Close