Application Notes
SL1000/500 VPN with SafeNet SoftRemote VPN Client

Version 1.3

Revision History

Version	Author	Date	Status
1.0	Julian Chang	08/20/2003	Initial draft
1.1	Nicole Lin	12/02/2004	
1.2	Martin Su	06/27/2005	

Table of Contents

1 Introduction

This application note will detail all of the steps to create a working IKE IPSec VPN tunnel between an ASUS SL1000 device (also be applied to SL500) and SafeNet SoftRemote VPN Client. All setting and screen dumps contained within this application notes are taken from a SafeNet SoftRemote running version 10.3.5(build 6), and a SL1000 device running firmware 1.1.68A.410.

2 Network Setup:

Figure 2.1 Overview of Network Connections

2.1 Connecting to the SL1000/500 Security Gateway using an IPSec Client

2.1.1 Provisioning Remote Access Groups and Users

Step 1: Create a remote access user group and add a remote access user to the user group.

Step 2: Verifying the users and the groups added in Step 1.

Step3: Under **Firewall→ Advanced→ Self Access**, add a Self Access Rule for remote user to login--**Allow TCP port 80 from WAN**. See Figure 2.3.

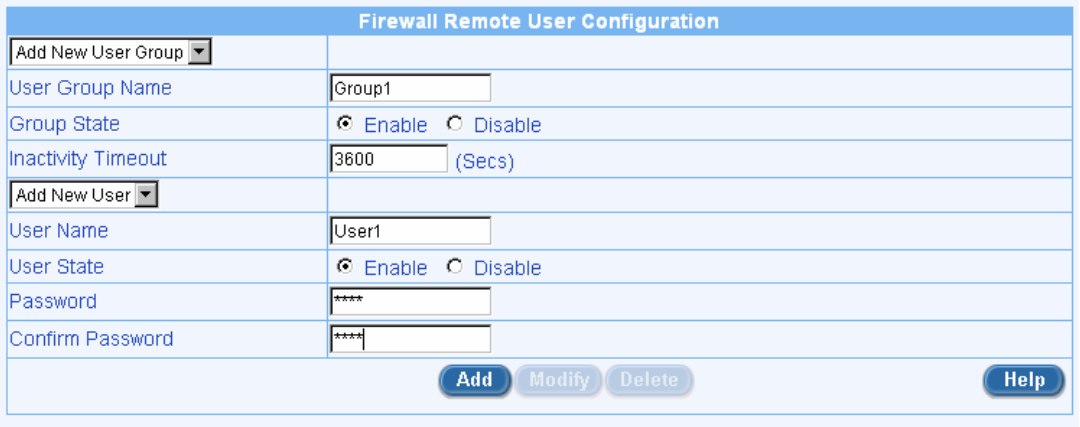

Figure 2.2 Remote User Configuration page

Figure 2.3 Self Access Rule Allowing Remote Users to Login

2.1.2 Configuring SL1000/500 VPN Policies for Aggressive Mode Remote Access

Aggressive Mode remote access with Xauth is a mechanism where the remote access client is prompted for an additional login (the Xauth login). This form of remote access is more secure since an intruder cannot access the corporate resources through a connected Laptop, which belongs to a valid employee. In addition, normal HTTP login by the remote user is used to instantiate appropriate firewall policies on the SL1000/500 security gateway. Once these policies are instantiated then the remote user is allowed secure access by the gateway.

2.1.2.1 Steps to configure SL1000 system

The main configuration activities required on SL1000 system to configure remote access users are:

- Group and User Administration
- VPN Policy configuration for the group

  Once the group and users are defined, the policies required in VPN are added and associated with the group.
- Firewall Policy Configuration for the group

  If secure access is required, a inbound firewall rule is needed for the group.

Step 1: Adding VPN specific policies for group "Group1"

Use option sequence **Remote Access -> VPN Tunnel**

Field	Purpose	Value
Tunnel Name	Enter a unique name to identify the connection	group_ra
Remote Access radio button	Make it as remote access connection	Selected
Local Secure Group	Select IP address, subnet or range	192.168.2.0/24
Preshared Key	A hexadecimal or ASCII shared secret	12345678
Remote ID	Match domain name of SafeNet	User1

Table 2.1 Adding VPN policy for the group "Group1" (Aggressive mode)

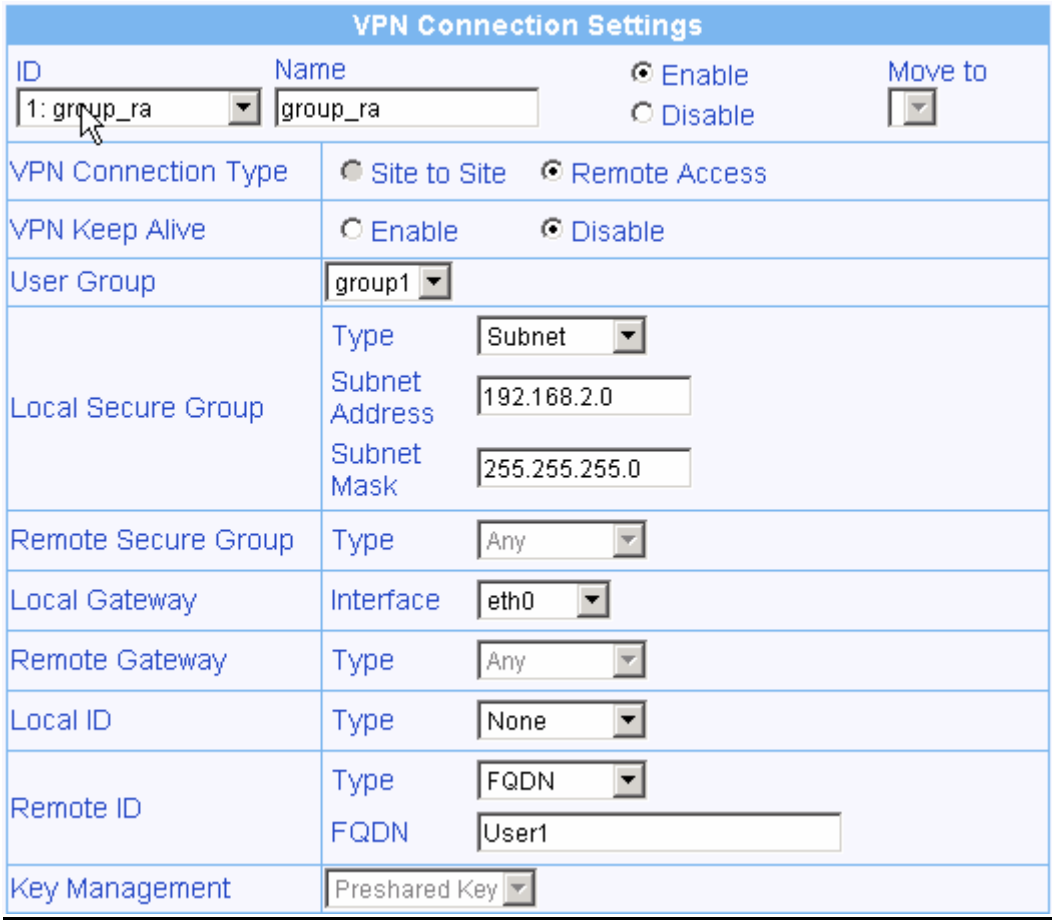

Figure 2.4 VPN policy configuration page

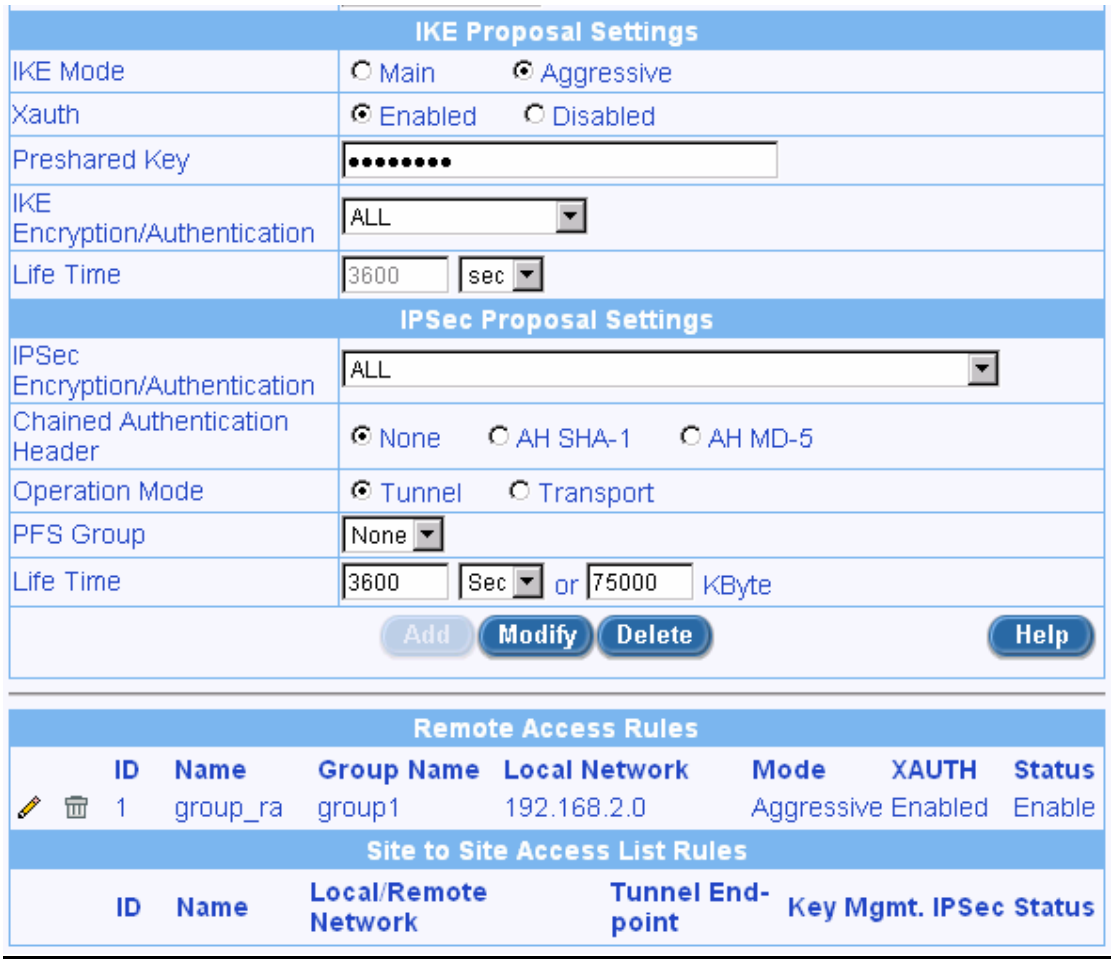

Figure 2.5 VPN policy configuration page(cont.)

Step 2: Verify VPN policies added for groups "Group1"

Figure 2.6 Verify VPN policy added for the group "Group1"

Step 3: Verify Virtual IP Address for user "User1"

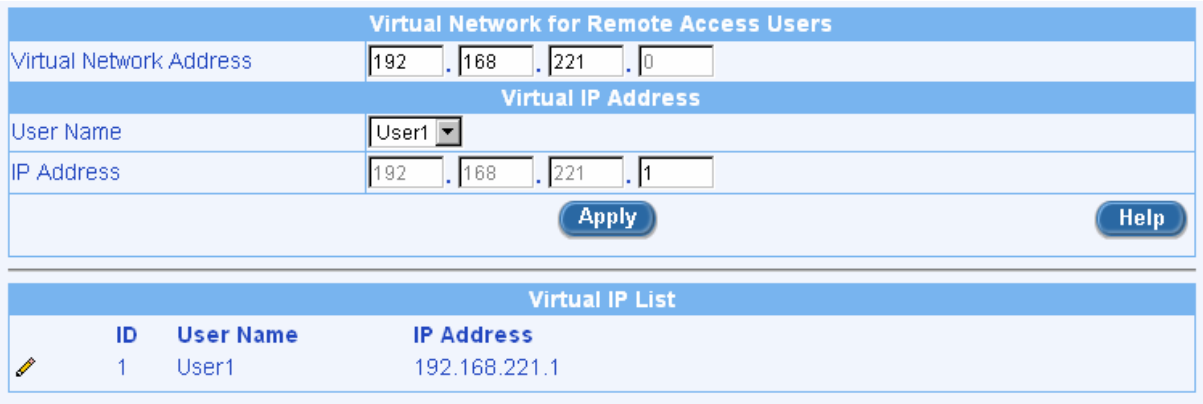

Figure 2.7 Configure virtual IP address for remote user "User1"

Step 4: Adding Firewall specific policies for group "Group1"

Field	Purpose	Value
Action		Allow
Rule Type		Inbound
User Group		Group1
Source IP		ANY
Destination IP		Subnet: 192.168.2.0/24
VPN		Enable

Table 2.2 Adding firewall policy for group "Group1"

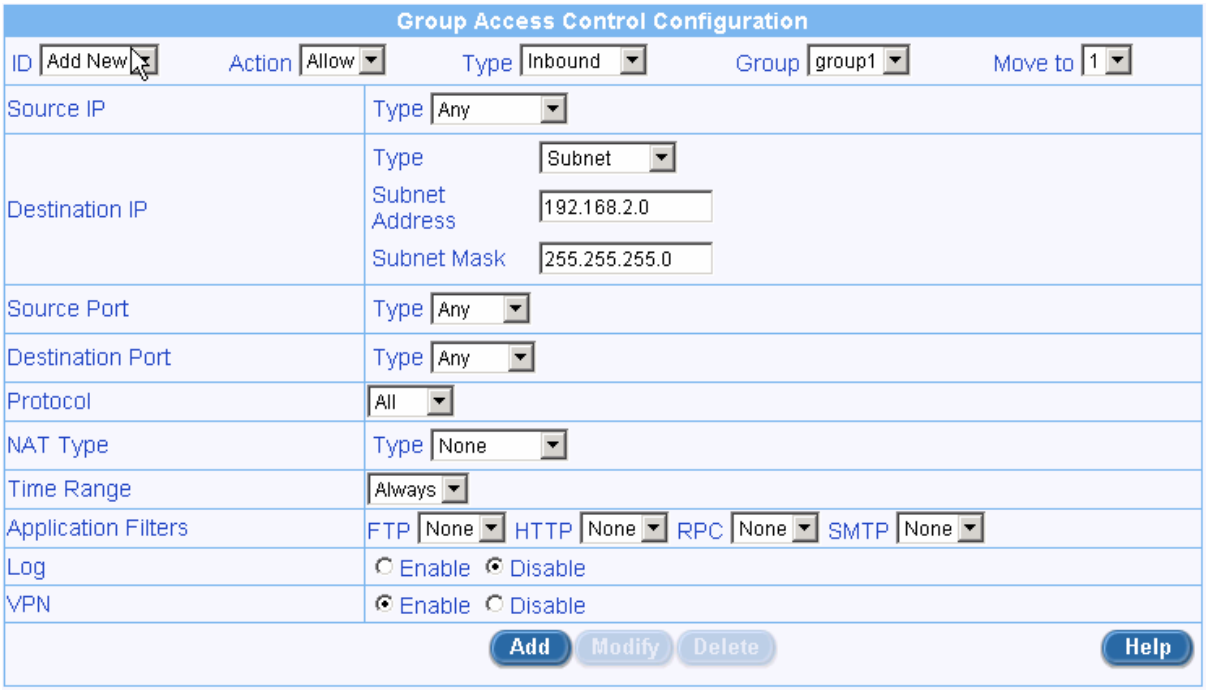

Figure 2.8 Firewall group policy configuration page

2.1.2.2 Steps to configure Remote Client

Each of the remote PC's should have VPN client software installed. The following configuration steps described assuming SafeNet SoftRemote 10.3.5 (Build 6) is installed in each of the user's PC.

Step 1: SafeNet Configuration for User1

Open the Security Policy Editor.

1. Addition of policy
   - ✓ Use options **My Connections -> (right click) -> Add -> Connection**

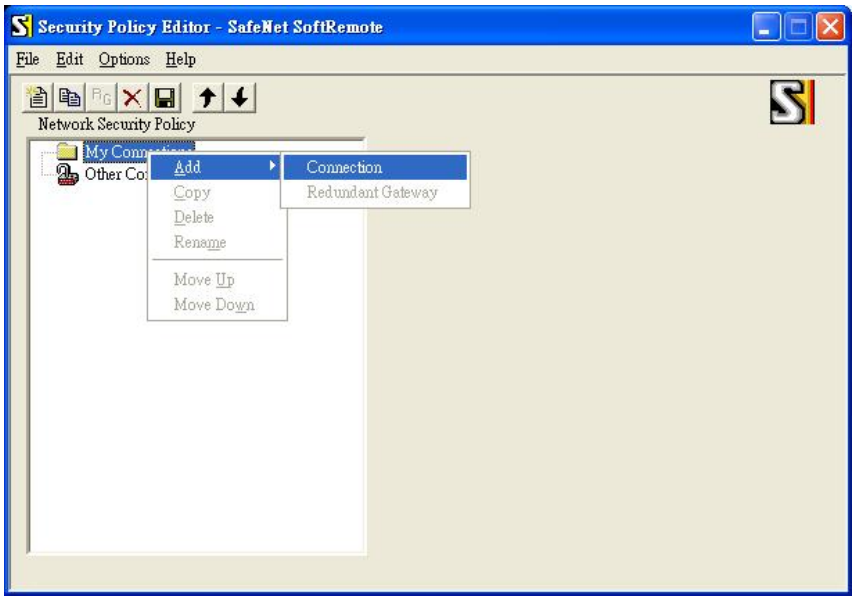

Figure 2.9 SoftRemote configuration for "SL1000" as My Connection

   - ✓ A connection **"New Connection"** will be shown.

- ✓ Use options **My Connection -> New Connection -> (right click) -> Rename**
- ✓ The connection name will become editable. Edit it to SL1000

Figure 2.9 SoftRemote configuration for "SL1000" as My Connection (cont.)

- ✓ In **Remote Party Identity and Address** block, select **IP Subnet** in **ID Type** and specify subnet 192.168.2.0 and mask 255.255.255.0 in the text box.
- ✓ Check **Connect using** and select **Secure Gateway Tunnel**.
- ✓ In **ID Type**, select **IP Address** and type 220.135.200.51 as remote VPN gateway.

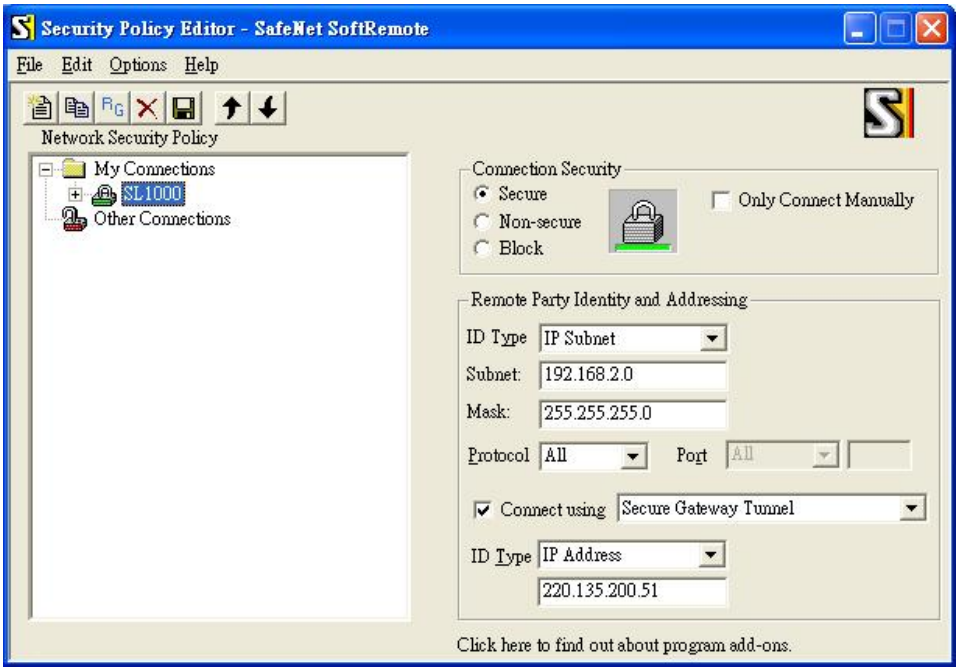

Figure 2.10 Configure ID type and addressing for remote party

- ✓ Use Options **My Connections -> SL1000 -> My Identity**

  On the right hand side, go to the **Internet Interface** block. Ensure that the IP Address field shows IP address 192.168.19.89 (this will be the case unless your PC has multiple. In that case, from the Name drop down box, choose appropriate interface to get the IP address 192.168.19.89.)

  Go to the My Identity block at the top.
- ✓ Select **Domain Name** in **ID Type** and type User1 here.
- ✓ From the **Certificate** drop-down list, choose None. **Pre-Shared Key** button will appear on at the right hand top corner. Click on the **Pre-Shared Key** button. A dialogue box as shown will appear.
- ✓ Disable **Virtual Adapter** if no certain programs that work with the client are "IP address-aware". If you configure a virtual IP for User1 in SL1000, you can choose **Required** to let the client accept a virtual IP assigned from SL1000.

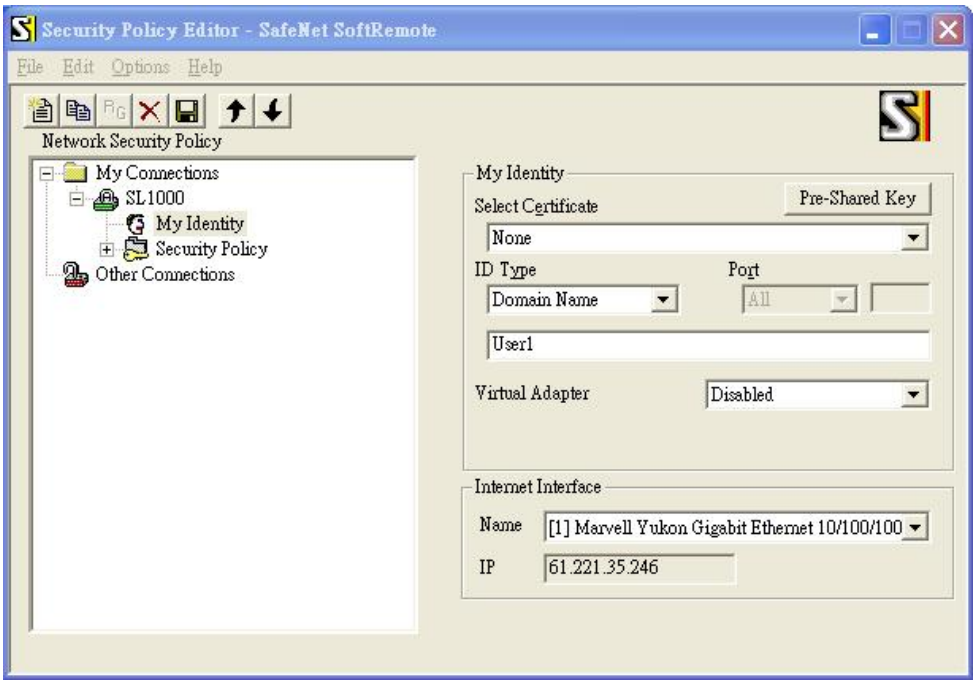

Figure 2.11 Setup pre-shared secret and local ID type

✓ Click on the **Enter Key** button to enable the text box. Enter 12345678 into the text box and click on OK.

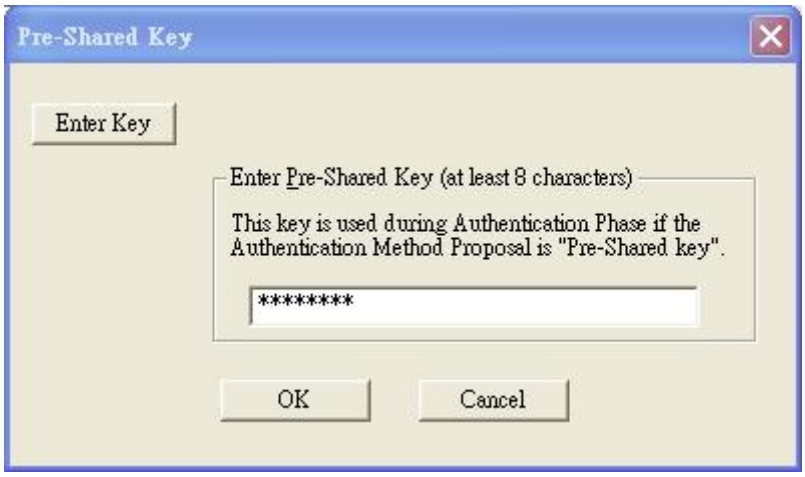

Figure 2.102 Enter pre-shared key

- ✓ Use options **My Connection -> SL1000 -> Security Policy**
- ✓ Choose **Aggressive Mode**

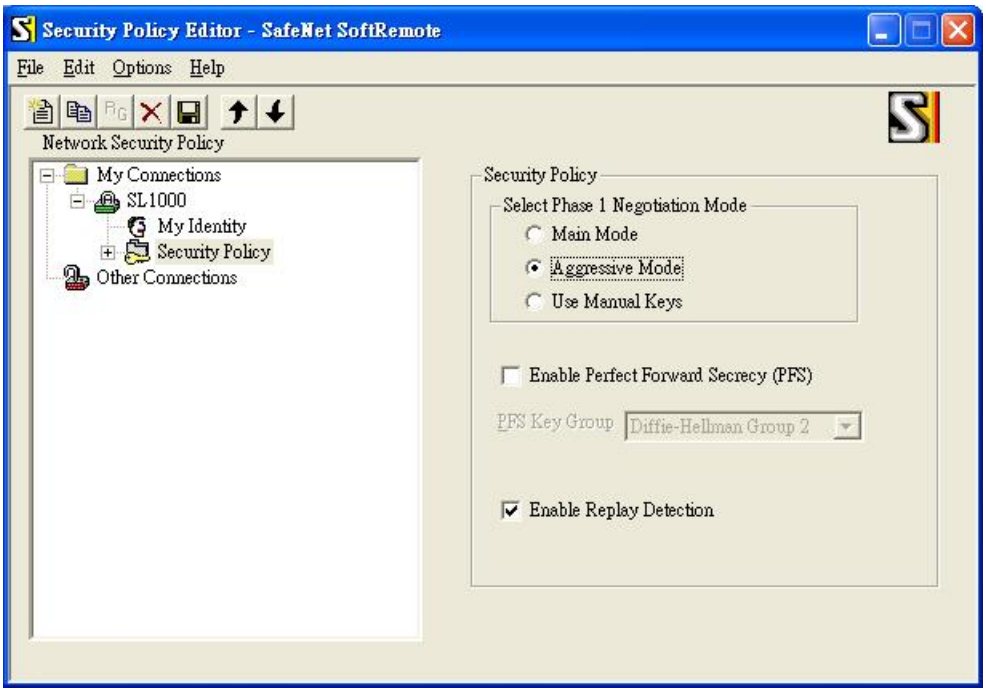

Figure 2.113 Configure IKE phase 1 negotiation mode as "Aggressive mode"

- ✓ Use option sequence: **My Connection -> SL1000 -> Security Policy -> Authentication (Phase 1) -> Proposal 1**
- ✓ On the right hand side, select **Diffie-Hellman Group 2** option from the Key Group drop-down list.

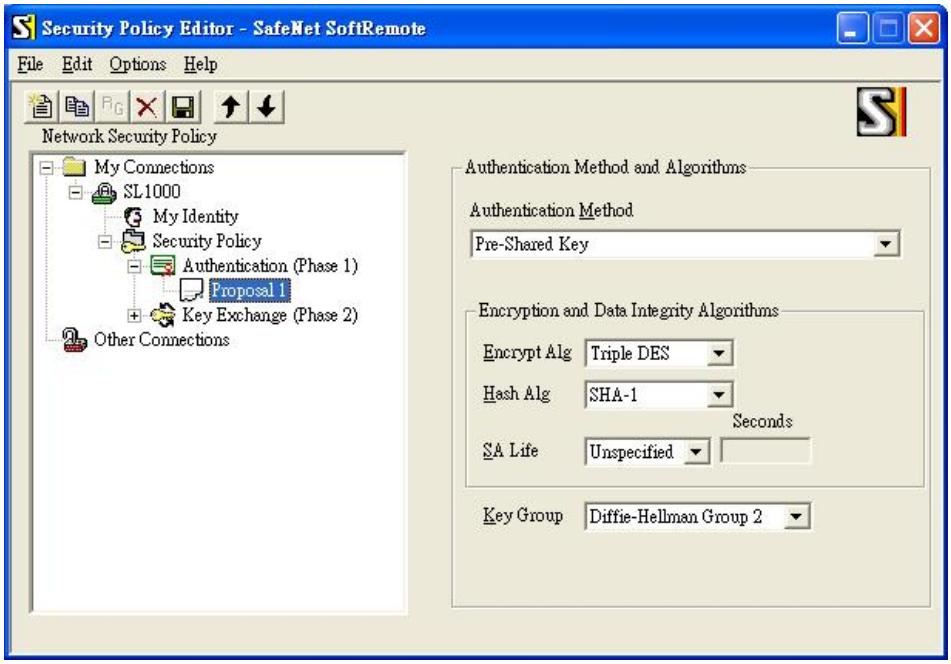

Figure 2.124 Configuration IKE phase 1 authentication method and algorithms

- ✓ Save the configuration.

2.1.2.3 Establishing VPN connection

Step 1: Activate IPSec Dial Client

In remote PC, right click the SafeNet SoftRemote Icon on the right bottom corner of desktop. Choose **"Activate Security Policy".** Left click the Icon again. Now choose **"Connect"** and connect to **"My Connection\SL1000"**. A popup window appears on PC1 asking for the XAUTH username and password. Enter User1 as username and 1234 as password.

Figure 2.135 Pop-up window for XAUTH user authentication

Type User1 into the **Username** text box and 1234 into the **Password** text box and click **OK**. A successfully connection message will come up.

Figure 2.146 VPN connection is established

Step 2: Login "User1" to activate inbound ACL rule in SL1000

Start Internet Explorer (5.0 or higher) web browser. In the Address box, enter: "http://220.135.200.51/login". A dialogue box as shown will appear:

Figure 2.17 User login for "User1"

Type User1 into the **User Name** text box and 1234 into the **Password** text box and click OK. Then, browser will display successful login message along with Logout button as shown.

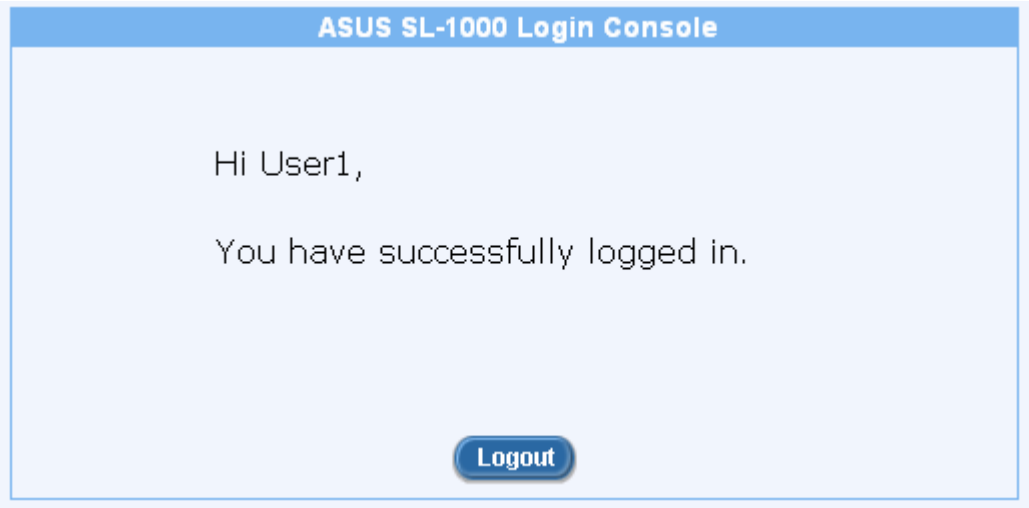

Figure 2.18 Successful login message for "User1"

Step 3: Verify Connection

On the SL1000/500 system side,

Use options **Remote Access -> Remote Access User**

You will see the details of the users logged in as below:

Figure 2.19 Remote Users Login Details

Ping from PC1 to PC4. See that the tunnel gets established.

```
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

C:\>ping 192.168.2.10

Pinging 192.168.2.10 with 32 bytes of data:

Reply from 192.168.2.10: bytes=32 time=10ms TTL=126
Reply from 192.168.2.10: bytes=32 time<10ms TTL=126
Reply from 192.168.2.10: bytes=32 time<10ms TTL=126
Reply from 192.168.2.10: bytes=32 time=10ms TTL=126

Ping statistics for 192.168.2.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum =  10ms, Average =  5ms

C:\>
```

Figure 2.20 Verify VPN connection by using Ping command