Greenbow VPN Client Example

Technote LCTN0008

Proxicast, LLC
312 Sunnyfield Drive
Suite 200
Glenshaw, PA 15116

1-877-77PROXI
1-877-777-7694
1-412-213-2477

Fax:
1-412-492-9386

E-Mail:
support@proxicast.com

Internet:
www.proxicast.com

This TechNote applies to LAN-Cell models:

LAN-Cell 2:
LC2-411 (firmware 4.02)

CDMA:
1xMG-401
1xMG-401S

GSM:
GPRS-401

Minimum LAN-Cell Firmware Revision: 3.62(XF2).

Note for Original LAN-Cell Model (1xMG & GPRS) Users:

The VPN configuration screens in the original LAN-Cell's Web GUI differ slightly from the examples in this Technote. Please locate the corresponding parameter fields in the VPN Configuration section of the LAN-Cell's user interface under VPN Rules (IKE). See also the LAN-Cell's *User Guide* for more information on VPN configuration. Contact Proxicast Technical Support for previous versions of this TechNote for firmware releases prior to 4.02.

Document Revision History:

Date	Comments
September 22, 2006	First release
July 16, 2007	Updated for LAN-Cell 2
March 3, 2008	Updated LAN-Cell 2 screens for firmware release 4.02 including VPN Wizard example.

Introduction

The Greenbow VPN Client is a low-cost, easy to use VPN client application for Windows. Trial versions of the product may be available for immediate download from the Greenbow website. Proxicast does not sell, support or endorse the Greenbow product.

For more information on Greenbow, please visit their web site: http://www.thegreenbow.com.

This Technote documents one example configuration of the Greenbow VPN client software when used to create a VPN tunnel to a LAN-Cell 2 Cellular Router. Other configurations may also work, depending upon your requirements and network configuration. This Technote is for illustration purposes only.

Example Network Topology

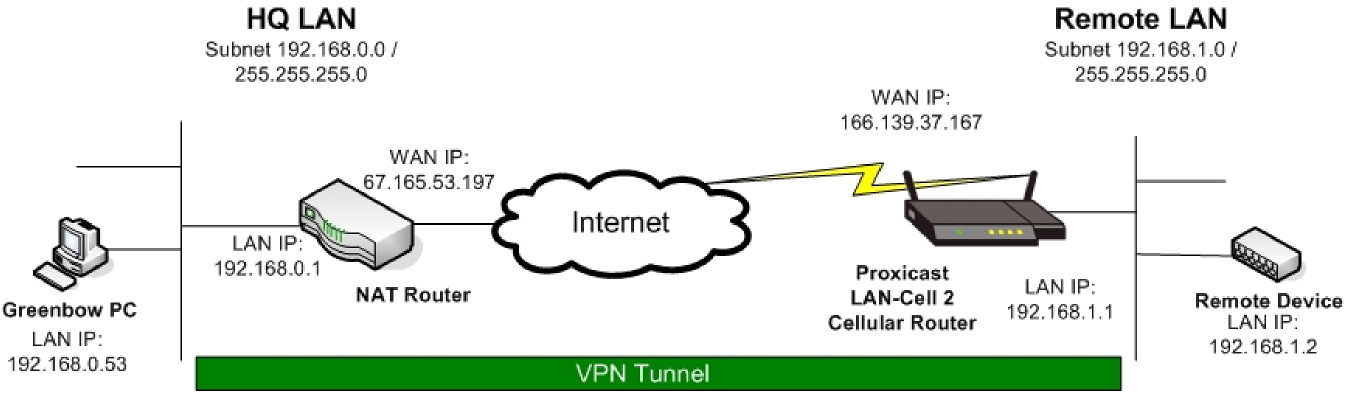


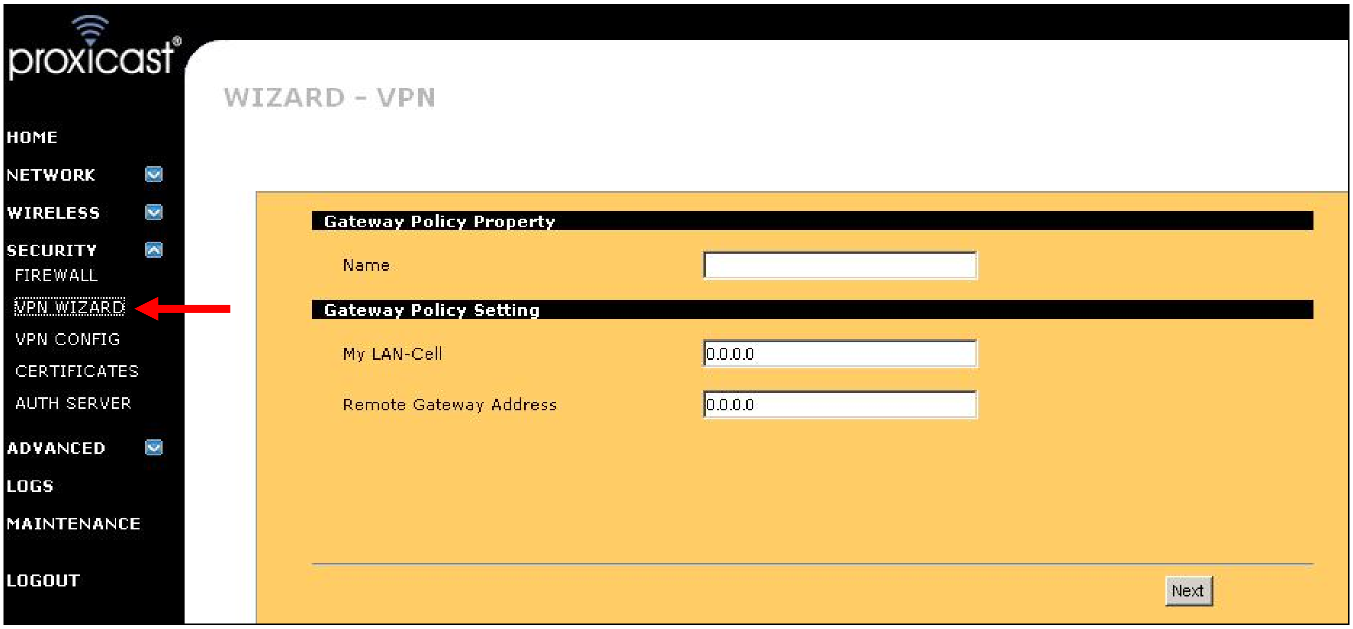
Figure 1: Example Network Topology

Usage Notes

- This example was created using Greenbow version 4.10.010 and LAN-Cell firmware version 4.02(AQP.1).
- When configuring a VPN connection, it is helpful to have the LAN-Cell and your target PC/equipment physically near each other so that you can view the configuration and logs of each device while testing.
- In this example the LAN-Cell has a static WAN IP address. The same configuration is possible by replacing the static IP address (166.139.37.167) with a fully qualified dynamic DNS name.
- Your HQ Router must be configured to allow IKE (UDP:500) packets to flow between your Greenbow PC and the LAN-Cell in order for the IPSec tunnel to be negotiated.
- This example demonstrates a Single Address (Greenbow) VPN connection to a remote Subnet via a VPN Tunnel (LAN-Cell's LAN subnet). The Greenbow VPN Client is not capable of making "site-to-site" tunnels that interconnect two different subnets. The LAN-Cell does support site-to-site VPN tunnels with all of the leading IPSec-compliant VPN routers/concentrators such as Cisco, ZyXEL, SonicWall, etc.
- This example configuration will also work if your Greenbow PC is directly connected to the Internet and your ISP allows VPN requests to pass through their firewall. In the example, replace 192.168.0.51 with the IP address assigned by your ISP. The HQ and Remote LANs must be on different subnets.
- There is additional information on LAN-Cell VPN configuration parameters in the *LAN-Cell User's Guide*.

Example LAN-Cell Configuration

The LAN-Cell 2 includes a **VPN Wizard** feature to step you through the process of creating basic VPN connection rules and network definitions. We will use the VPN Wizard to create the Greenbow client connection parameters on the LAN-Cell 2. To reach this screen, select **SECURITY** then **VPN Wizard** from the left side menu. (See Figure 2).



Gateway Policy Property

Name

Gateway Policy Setting

My LAN-Cell 0.0.0.0

Remote Gateway Address 0.0.0.0

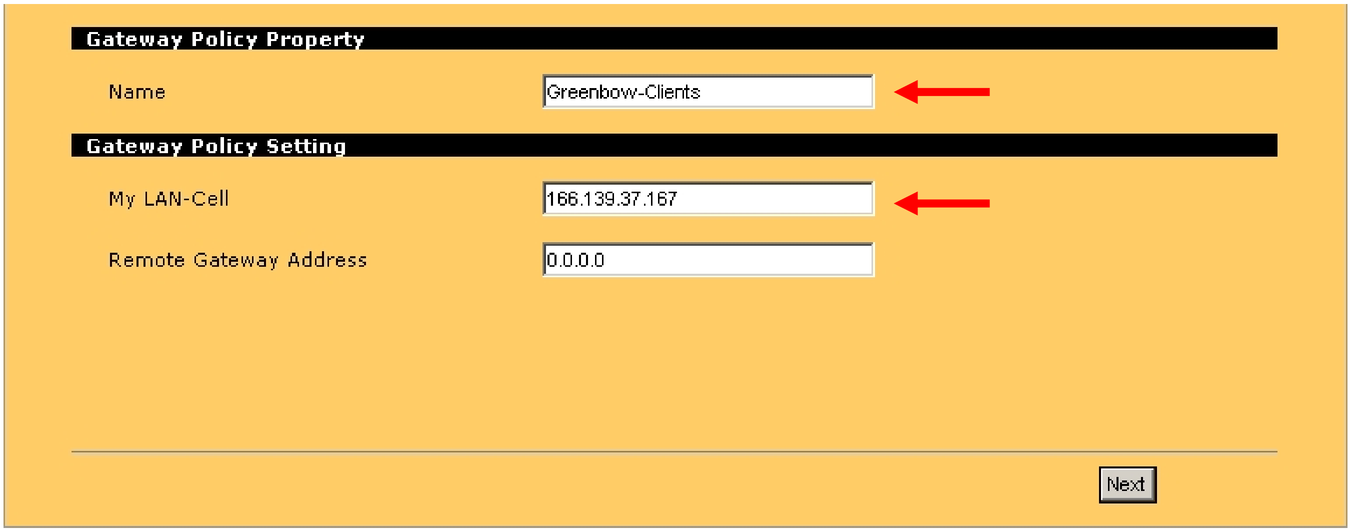
Figure 2: LAN-Cell 2 VPN Wizard

To begin the VPN Wizard, you must give the Gateway Policy a descriptive Name. (See Figure 3).

If your LAN-Cell has a static WAN IP address assigned by your ISP or cellular operator, enter that value as the My LAN-Cell address. Optionally you can enter a Dynamic DNS FQDN that is associated with your LAN-Cell's WAN (see the Advanced->DNS->DDNS screen) or you can enter 0.0.0.0 and the LAN-Cell will use its current WAN IP address. This value must match the Remote Gateway Address parameter in the Greenbow client.

For the Remote Gateway Address, enter 0.0.0.0. This will create a default rule that will accept VPN connections from any remote IP address that presents the correct Phase 1 and Phase 2 parameters and keys. This configuration provides the most flexibility when connecting remote Greenbow clients from multiple PCs. Also, when the Greenbow VPN Client is used on a PC behind a NAT router, it does not present a consistent source IP address during IKE negotiations, preventing the tunnel from being established if either the router's public IP or the Greenbow's client's private IP address is used as the Remote Gateway Address.

Note: If you want to restrict the IP address(es) that can establish a VPN connection using this default global rule, you can add a CELL-CELL/LAN-Cell Firewall Rule to restrict IKE (UDP:500) traffic to a specific IP address or range. See the *User's Guide* for more information on creating firewall rules.



Gateway Policy Property

Name: Greenbow-Clients

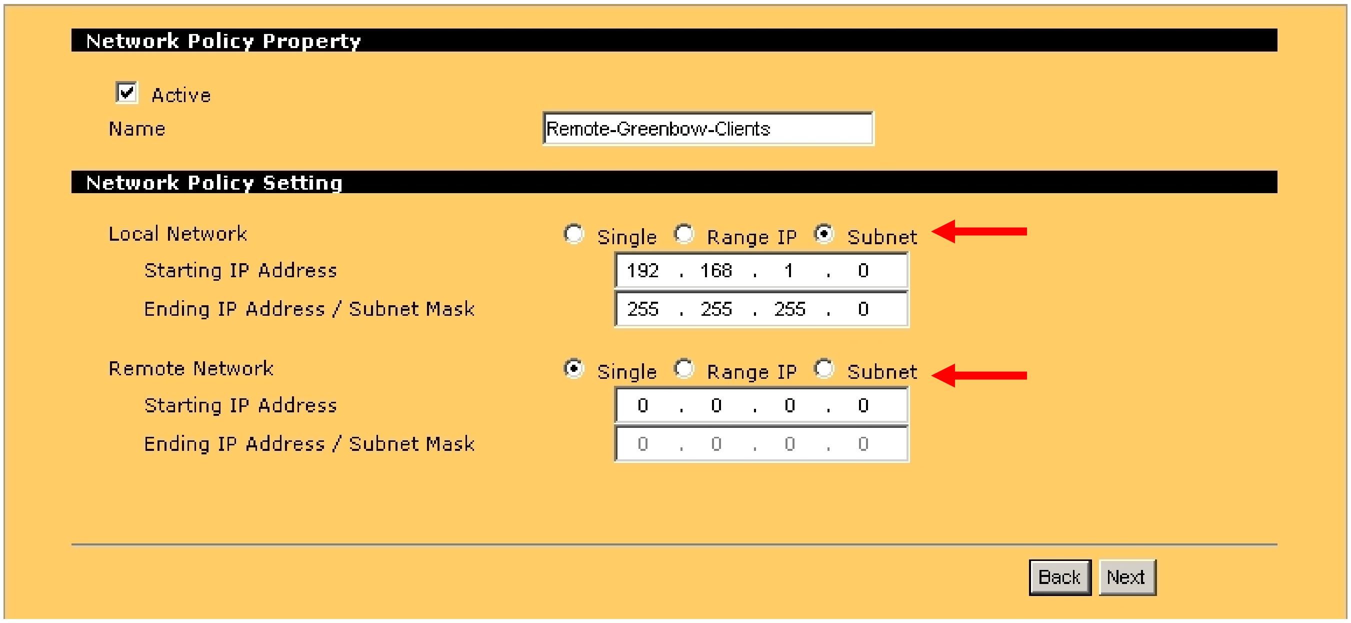
Gateway Policy Setting

My LAN-Cell: 166.139.37.167

Remote Gateway Address: 0.0.0.0

Figure 3: Gateway Policy Parameters

Next, we must create a Network Policy that defines which IP addresses (or subnets) will be used on each end of the VPN tunnel. Figure 4 illustrates the correct settings for our example VPN tunnel.



Network Policy Property

☑ Active

Name: Remote-Greenbow-Clients

Network Policy Setting

Local Network: ○ Single ○ Range IP ● Subnet

Starting IP Address: 192 . 168 . 1 . 0

Ending IP Address / Subnet Mask: 255 . 255 . 255 . 0

Remote Network: ● Single ○ Range IP ○ Subnet

Starting IP Address: 0 . 0 . 0 . 0

Ending IP Address / Subnet Mask: 0 . 0 . 0 . 0

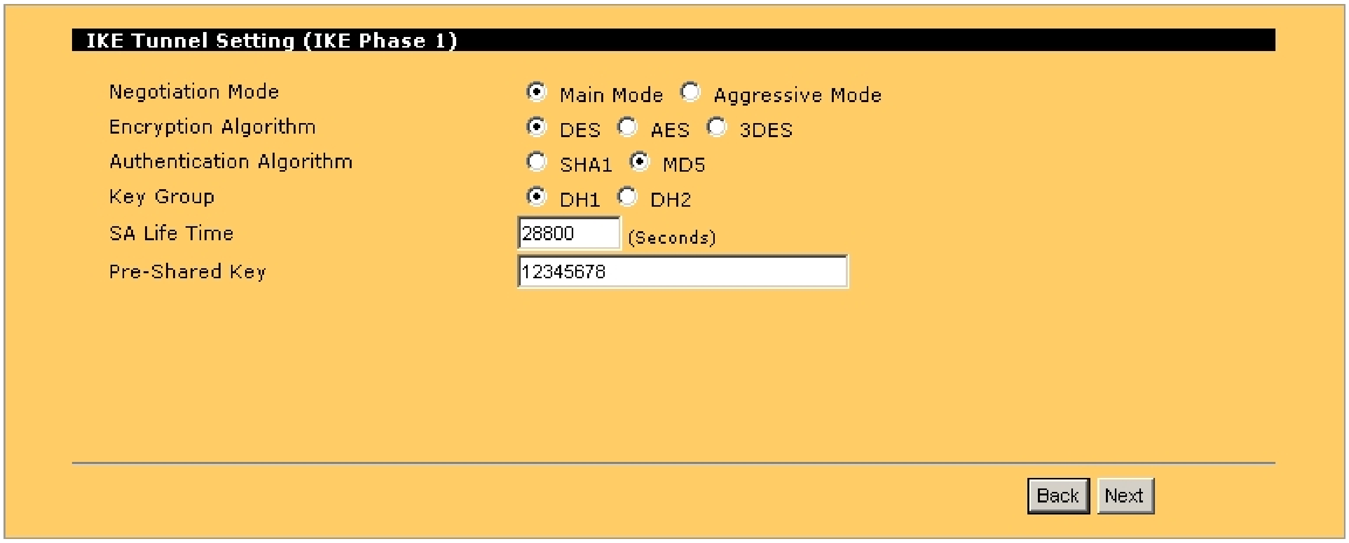
Figure 4: Network Policy Parameters

Be certain to check the Active option. You must also give the Network Policy a descriptive Name.

For the Local Network section, select the Subnet option and enter the LAN-Cell's current LAN subnet and mask. Note that when specifying the subnet, the last octet is 0 for a full Class-C network (255 devices). For our example, the subnet is 192.168.1.0 / 255.255.255.0

For the Remote Network, select Single Address as the type and enter an IP address of 0.0.0.0. This creates a default rule that allows the remote VPN client to have any IP address that is not part of the LAN-Cell's subnet. You can optionally specify the exact remote client IP address that you will assign to the Greenbow Client VPN.

Next, we define the IKE Phase 1 parameters that will be used to negotiate the initial VPN tunnel connection between the Greenbow Client and the LAN-Cell.



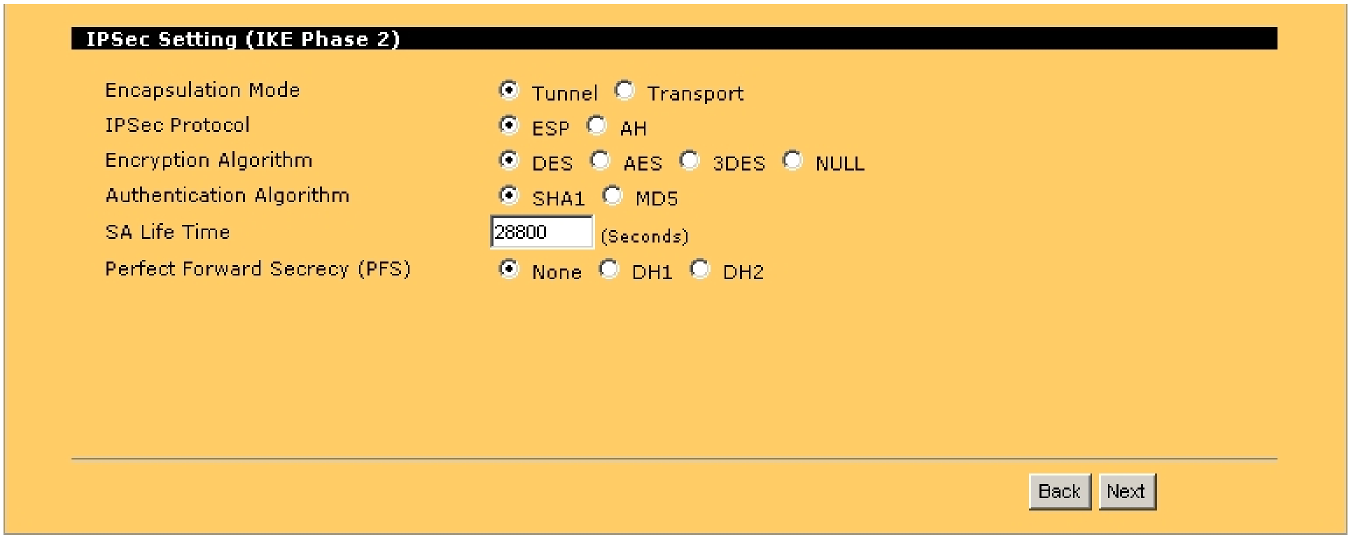
IKE Tunnel Setting (IKE Phase 1)

Negotiation Mode ● Main Mode ○ Aggressive Mode
Encryption Algorithm ● DES ○ AES ○ 3DES
Authentication Algorithm ○ SHA1 ● MD5
Key Group ● DH1 ○ DH2
SA Life Time 28800 (Seconds)
Pre-Shared Key 12345678

Figure 5: IKE Phase 1 Parameters

Figure 5 shows the default values for the IKE Phase 1 parameters. For our example, we will accept the default values and adjust the Greenbow client to match these settings.

The LAN-Cell and Greenbow both support several different types of authentication, including X.509 digital certificates. However, it is easiest to configure the VPN tunnel with Pre-Shared Keys that are the same on both the Greenbow client and the LAN-Cell. Enter a Pre-Shared Key that is at least an 8 character string. Avoid non-alphanumeric characters such as dashes, underscores, asterisks, etc. In our example, the Pre-Shared Key is 12345678.



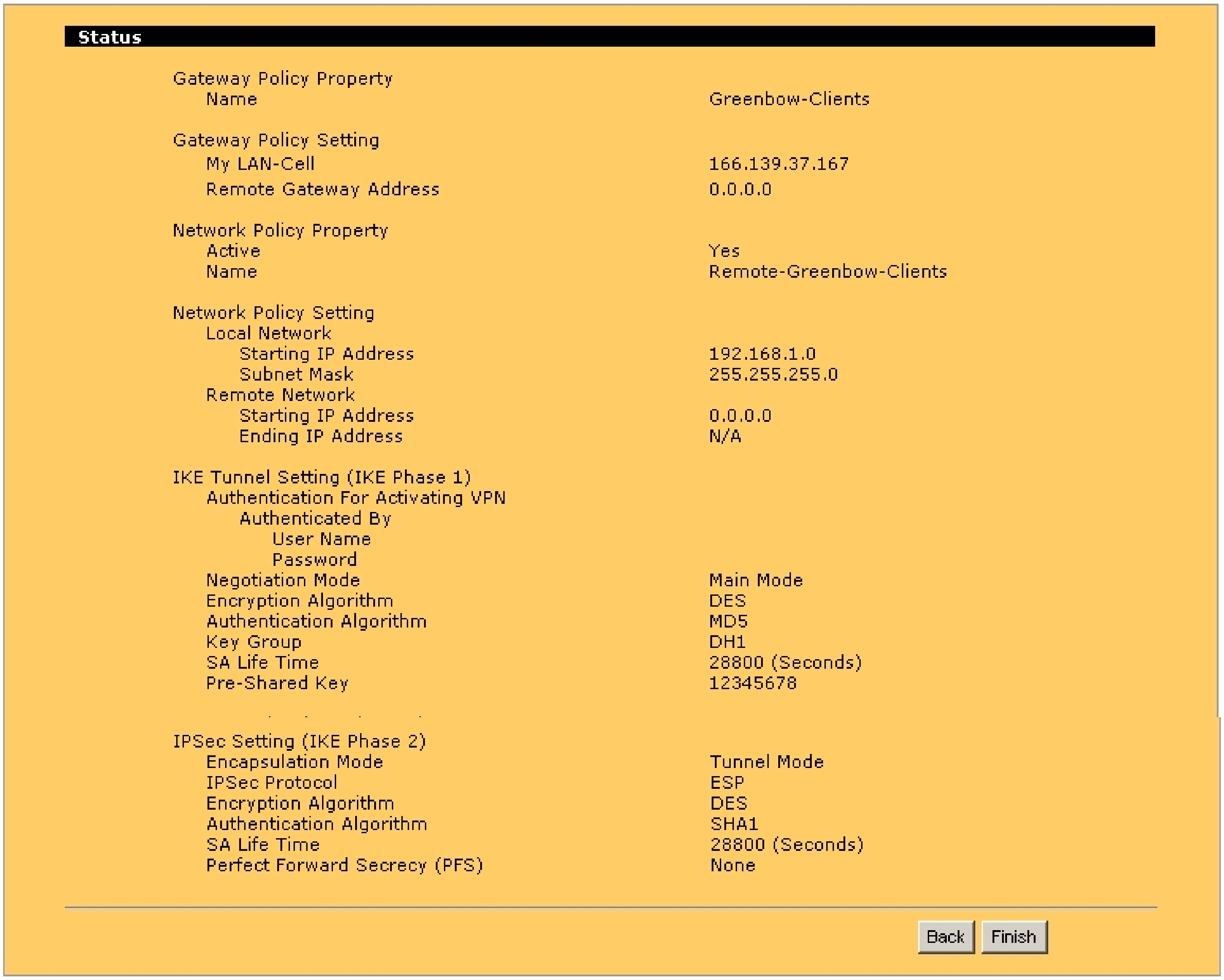
IPSec Setting (IKE Phase 2)

Encapsulation Mode ● Tunnel ○ Transport
IPSec Protocol ● ESP ○ AH
Encryption Algorithm ● DES ○ AES ○ 3DES ○ NULL
Authentication Algorithm ● SHA1 ○ MD5
SA Life Time 28800 (Seconds)
Perfect Forward Secrecy (PFS) ● None ○ DH1 ○ DH2

Figure 6: IKE Phase 2 Parameters

The settings on this screen are the LAN-Cell defaults and do not need to be changed for our example. You will configure the Greenbow VPN Client to match these settings.

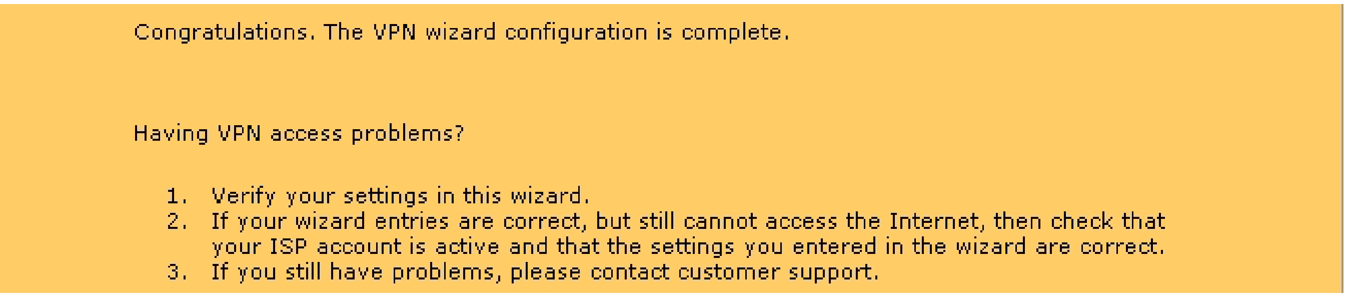
The VPN Wizard will now display a summary screen of all of the parameters you've entered for the VPN tunnel (Figure 7). Review these values and go back through the Wizard if any changes are required. You may wish to print this screen to document the LAN-Cell's VPN configuration parameters.



```
Status

Gateway Policy Property
    Name                                      Greenbow-Clients

Gateway Policy Setting
    My LAN-Cell                               166.139.37.167
    Remote Gateway Address                    0.0.0.0

Network Policy Property
    Active                                    Yes
    Name                                      Remote-Greenbow-Clients

Network Policy Setting
    Local Network
        Starting IP Address                   192.168.1.0
        Subnet Mask                           255.255.255.0
    Remote Network
        Starting IP Address                   0.0.0.0
        Ending IP Address                     N/A

IKE Tunnel Setting (IKE Phase 1)
    Authentication For Activating VPN
        Authenticated By
            User Name
            Password
    Negotiation Mode                          Main Mode
    Encryption Algorithm                      DES
    Authentication Algorithm                  MD5
    Key Group                                 DH1
    SA Life Time                              28800 (Seconds)
    Pre-Shared Key                            12345678

IPSec Setting (IKE Phase 2)
    Encapsulation Mode                        Tunnel Mode
    IPSec Protocol                            ESP
    Encryption Algorithm                      DES
    Authentication Algorithm                  SHA1
    SA Life Time                              28800 (Seconds)
    Perfect Forward Secrecy (PFS)             None
```

Figure 7: VPN Wizard Summary Screen

Click Finish on the summary screen to save the VPN configuration. The confirmation screen shown in Figure 8 will be displayed.



Congratulations. The VPN wizard configuration is complete.

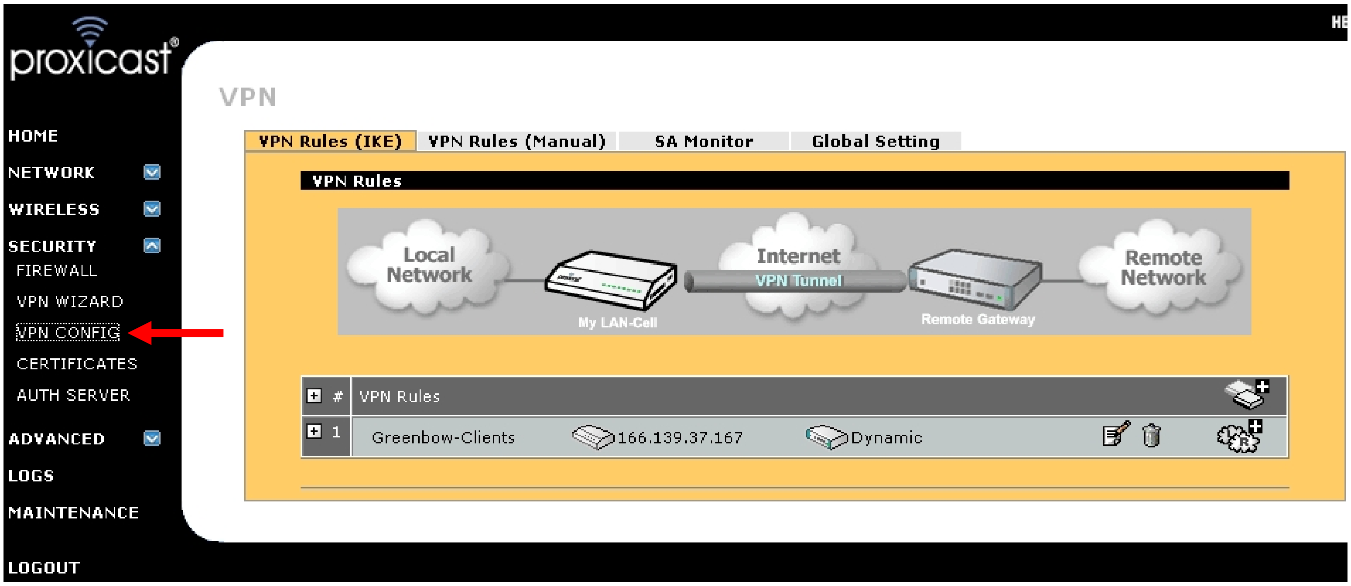
Having VPN access problems?

1. Verify your settings in this wizard.
2. If your wizard entries are correct, but still cannot access the Internet, then check that your ISP account is active and that the settings you entered in the wizard are correct.
3. If you still have problems, please contact customer support.

Figure 8: VPN Wizard Confirmation Screen

Configuration of the LAN-Cell is now complete. You can review and modify the VPN configuration parameters using the **VPN Config** option on the left side menu (Figure 9).

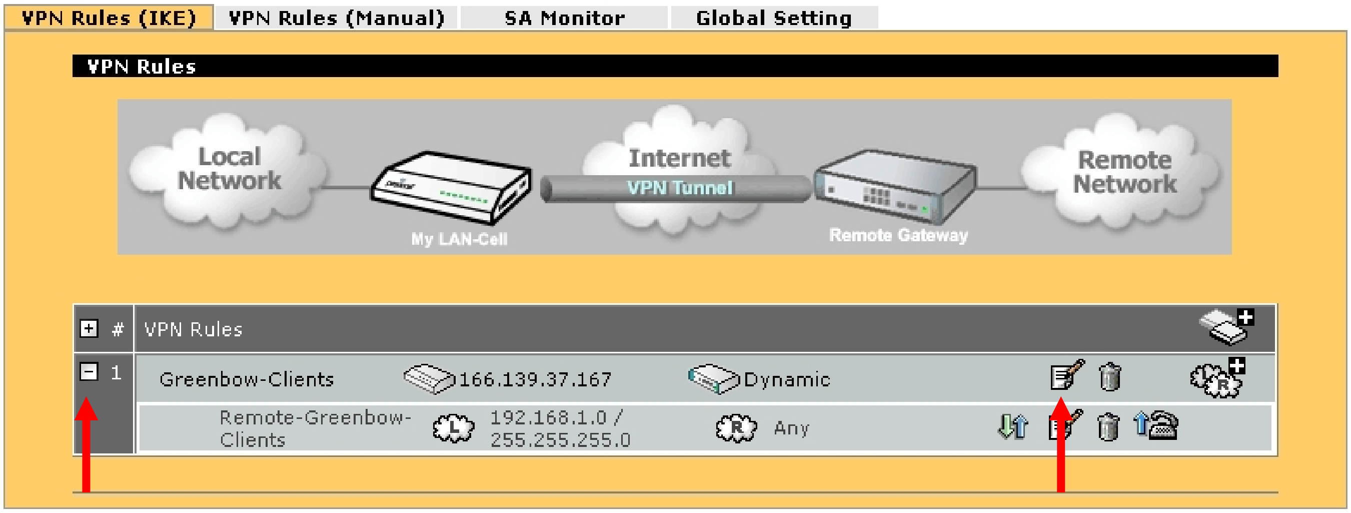
Click on the **LOGS** Menu, clear any existing entries, and then configure the Greenbow VPN Client software.



#	VPN Rules		
1	Greenbow-Clients	166.139.37.167	Dynamic

Figure 9: VPN Configuration Screen

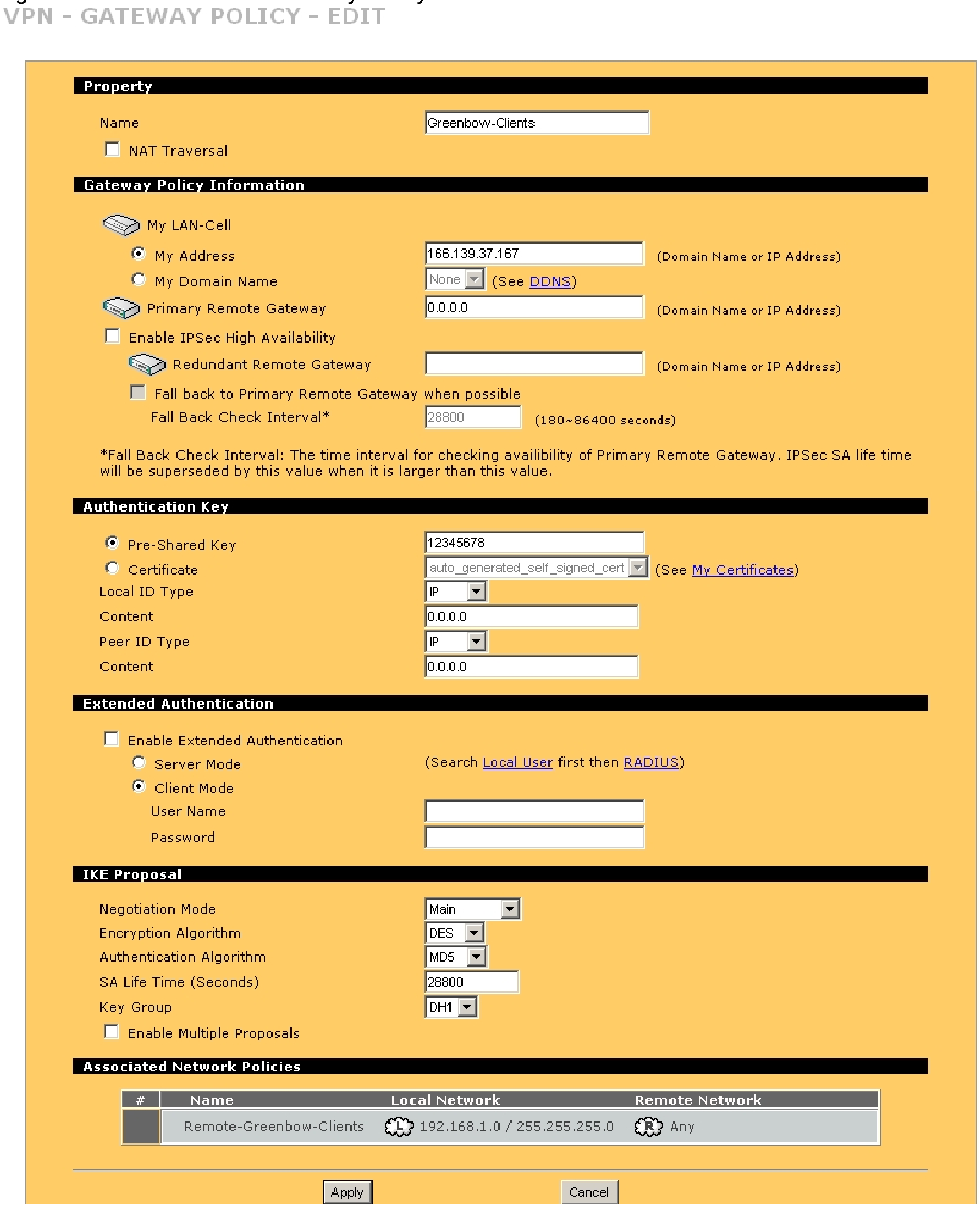
To view the network policies associated with each rule, click the [+] symbol to the left of the Gateway Policy. To edit either the Network or Gateway Policy parameters, click the edit icon ✎ on right of the corresponding line (Figure 10).



#	VPN Rules		
1	Greenbow-Clients	166.139.37.167	Dynamic
	Remote-Greenbow-Clients	192.168.1.0 / 255.255.255.0	Any

Figure 10: Displaying and Editing VPN Rules

Figure 11 shows the VPN Gateway Policy Edit screen.



VPN - GATEWAY POLICY - EDIT

Property

Name: Greenbow-Clients

□ NAT Traversal

Gateway Policy Information

My LAN-Cell

● My Address: 166.139.37.167 (Domain Name or IP Address)

○ My Domain Name: None (See DDNS)

Primary Remote Gateway: 0.0.0.0 (Domain Name or IP Address)

□ Enable IPSec High Availability

Redundant Remote Gateway: (Domain Name or IP Address)

□ Fall back to Primary Remote Gateway when possible

Fall Back Check Interval*: 28800 (180~86400 seconds)

*Fall Back Check Interval: The time interval for checking availibility of Primary Remote Gateway. IPSec SA life time will be superseded by this value when it is larger than this value.

Authentication Key

● Pre-Shared Key: 12345678

○ Certificate: auto_generated_self_signed_cert (See My Certificates)

Local ID Type: IP

Content: 0.0.0.0

Peer ID Type: IP

Content: 0.0.0.0

Extended Authentication

□ Enable Extended Authentication

○ Server Mode (Search Local User first then RADIUS)

● Client Mode

User Name:

Password:

IKE Proposal

Negotiation Mode: Main

Encryption Algorithm: DES

Authentication Algorithm: MD5

SA Life Time (Seconds): 28800

Key Group: DH1

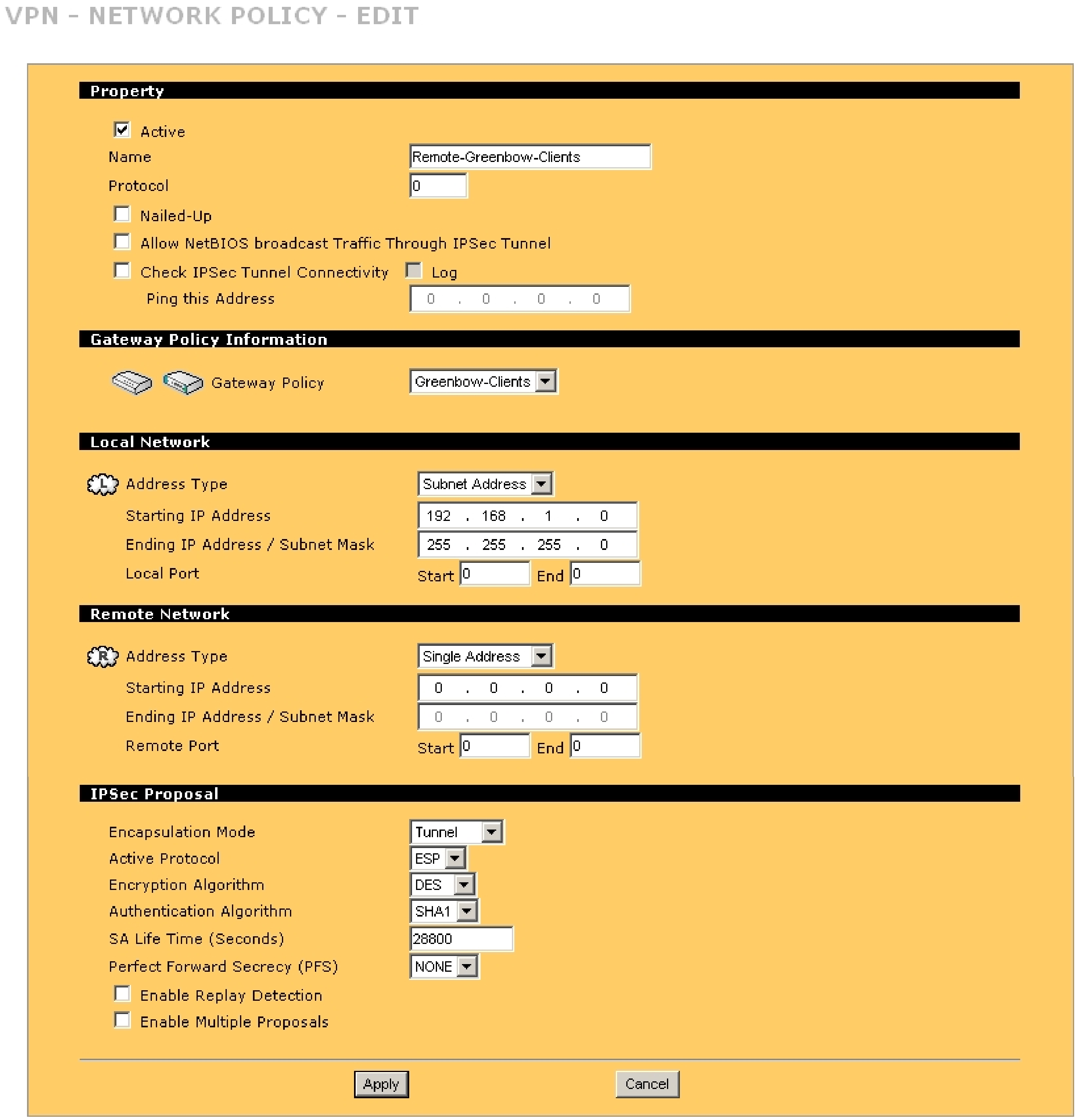
□ Enable Multiple Proposals

Associated Network Policies

#	Name	Local Network	Remote Network
	Remote-Greenbow-Clients	192.168.1.0 / 255.255.255.0	Any

Figure 11: Editing the VPN Gateway Policy Parameters

Figure 12 shows the VPN Network Policy Edit screen.



VPN - NETWORK POLICY - EDIT

Property

☑ Active

Name: Remote-Greenbow-Clients

Protocol: 0

□ Nailed-Up

□ Allow NetBIOS broadcast Traffic Through IPSec Tunnel

□ Check IPSec Tunnel Connectivity □ Log

Ping this Address: 0 . 0 . 0 . 0

Gateway Policy Information

Gateway Policy: Greenbow-Clients

Local Network

Address Type: Subnet Address

Starting IP Address: 192 . 168 . 1 . 0

Ending IP Address / Subnet Mask: 255 . 255 . 255 . 0

Local Port: Start 0 End 0

Remote Network

Address Type: Single Address

Starting IP Address: 0 . 0 . 0 . 0

Ending IP Address / Subnet Mask: 0 . 0 . 0 . 0

Remote Port: Start 0 End 0

IPSec Proposal

Encapsulation Mode: Tunnel

Active Protocol: ESP

Encryption Algorithm: DES

Authentication Algorithm: SHA1

SA Life Time (Seconds): 28800

Perfect Forward Secrecy (PFS): NONE

□ Enable Replay Detection

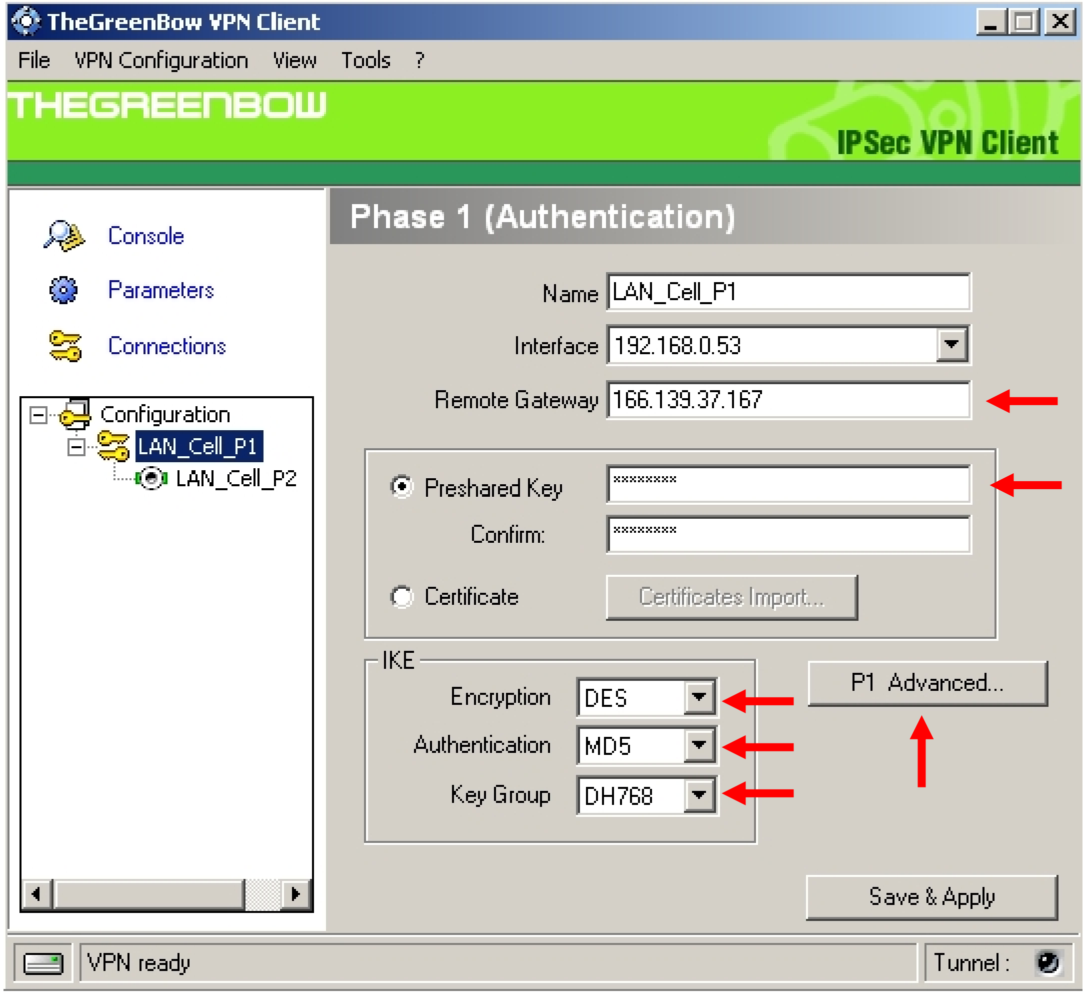
□ Enable Multiple Proposals

Figure 12: Editing the VPN Network Policy Parameters

Example Greenbow Configuration

After starting the Greenbow VPN Client software, select Configuration and right-click to create a new Phase 1 configuration as shown in Figure 13. You may give this connection a descriptive Name of your choosing. Select the LAN Interface that is connected to your HQ LAN. For the Remote Gateway, enter the WAN IP address (or FQDN) of your remote LAN-Cell (166.139.37.167 in our example).

> Note: If your LAN-Cell does not have a static IP address assigned to its 3G or WAN interface, you must define a Fully Qualified Domain Name (FQDN) using the DynDNS.org service and configure the LAN-Cell to update DynDNS each time its WAN IP address changes. See the *LAN-Cell User's Guide* for more information on configuring DynDNS.



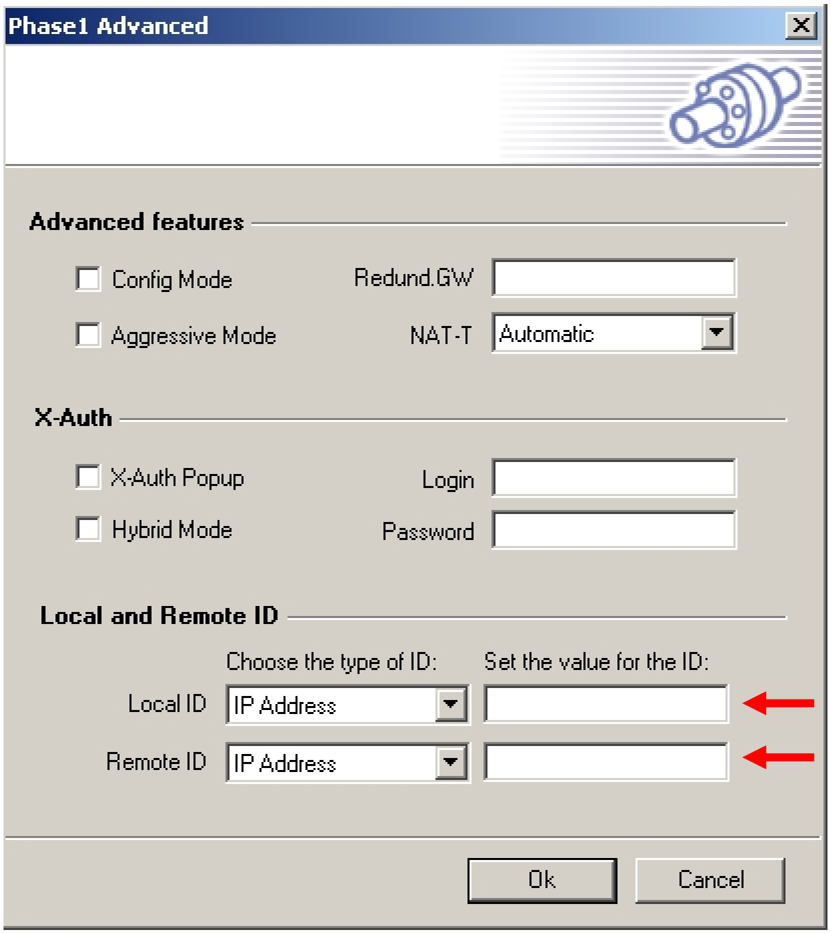
Name: LAN_Cell_P1
Interface: 192.168.0.53
Remote Gateway: 166.139.37.167
● Preshared Key: ********
Confirm: ********
○ Certificate
IKE
Encryption: DES
Authentication: MD5
Key Group: DH768

Figure 13: Greenbow Phase 1

Enter the Pre-Shared Key that you entered on the LAN-Cell (at least 8 characters). Pre-shared keys are case sensitive and they must match EXACTLY on both devices. In our example the pre-shared key is 12345678.

The Phase 1 IKE parameters must also match between on both devices. In our example, we selected DES Encryption, MD5 Authentication and Diffie-Hillman Key Group 1 (768 bits) which are the defaults for the LAN-Cell's Phase 1 parameters.

We must also configure the Phase 1 Local and Remote ID values used during IPSec negotiation. Press the **P1 Advanced** button to reveal the screen shown in Figure 14. For our example, set the Local and Remote ID type to “IP” and leave the Content Values as blank. No other changes to the Greenbow parameters on this screen are necessary for our example. Press **OK** when complete, then **Save & Apply** the Phase 1 settings.



Phase1 Advanced

Advanced features

□ Config Mode   Redund.GW

□ Aggressive Mode   NAT-T Automatic

X-Auth

□ X-Auth Popup   Login

□ Hybrid Mode   Password

Local and Remote ID

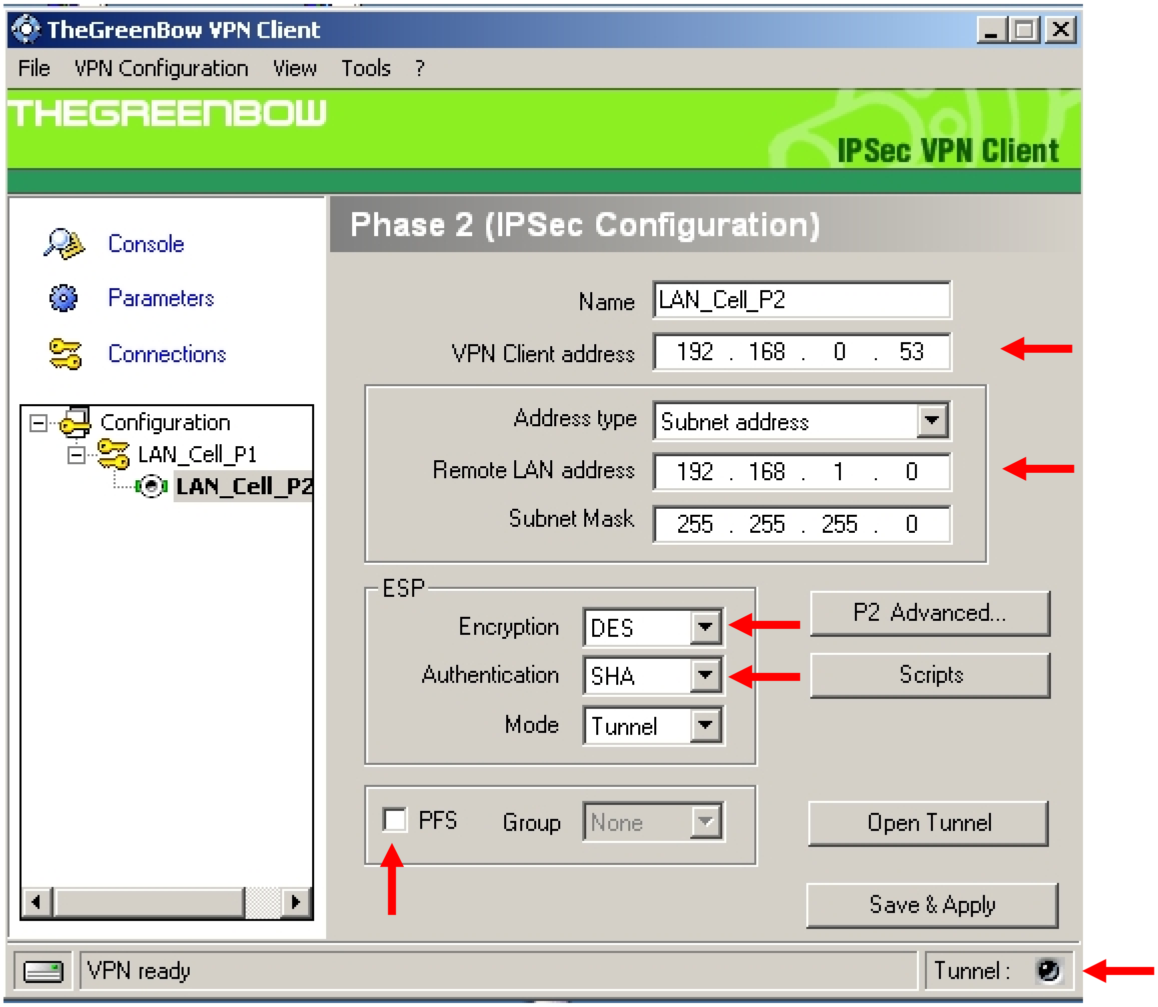
	Choose the type of ID:	Set the value for the ID:
Local ID	IP Address	
Remote ID	IP Address	

Figure 14: Greenbow Phase 1 Advanced

Now select the Phase 1 configuration from the Greenbow main screen and right click to add a Phase 2 configuration as shown in Figure 15.

You may give the Phase 2 parameters their own descriptive Name. Set the VPN Client Address value to the local LAN IP address of your Greenbow PC (192.168.0.53 in our example). Note: With our example, you may use any IP address as the Greenbow VPN Client’s “virtual” IP address as long as the address is NOT within the same subnet as the LAN-Cell’s remote LAN subnet.

The Address Type should be set to “Subnet address” and the Remote LAN Address and subnet must match the LAN address range configured on the remote LAN-Cell. Note that when specifying a subnet, the last octet of the address is 0. In our example this value is 192.168.1.0 / 255.255.255.0.



Name: LAN_Cell_P2

VPN Client address: 192 . 168 . 0 . 53

Address type: Subnet address

Remote LAN address: 192 . 168 . 1 . 0

Subnet Mask: 255 . 255 . 255 . 0

ESP

Encryption: DES

Authentication: SHA

Mode: Tunnel

□ PFS Group: None

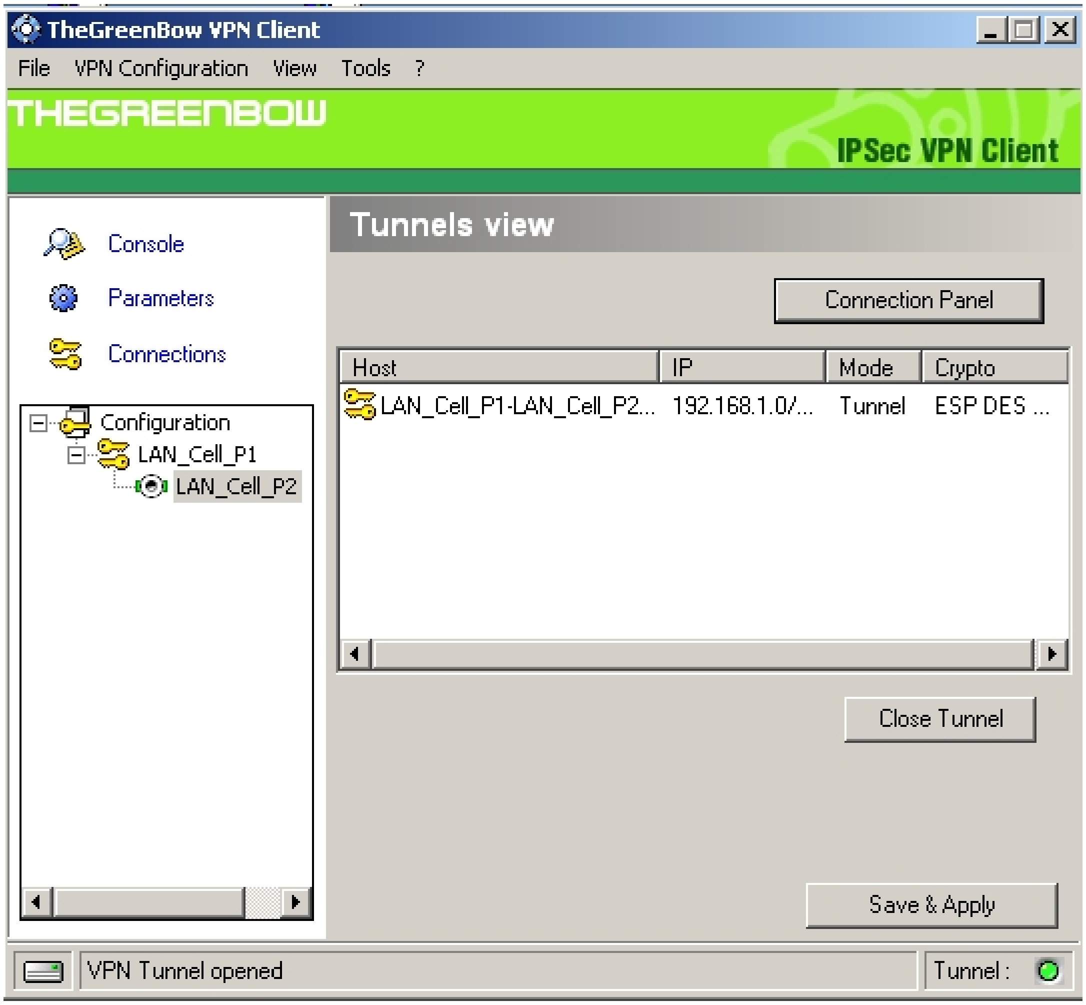
VPN ready

Tunnel :

Figure 15: Greenbow Phase 2

Continuing with the Phase 2 parameters, set the ESP Encryption to DES, the Authentication to SHA, the Mode to Tunnel and uncheck the PFS option to match the LAN-Cell's Phase 2 default values. Press **Save & Apply**. No changes to the Phase 2 Advanced settings are necessary.

You may now press the **Open Tunnel** button to make a connection to the LAN-Cell. In a few seconds, the Tunnel icon in the lower right portion of the Greenbow window should turn green. You can see the status of the tunnel using the Connections menu (see Figure 16).

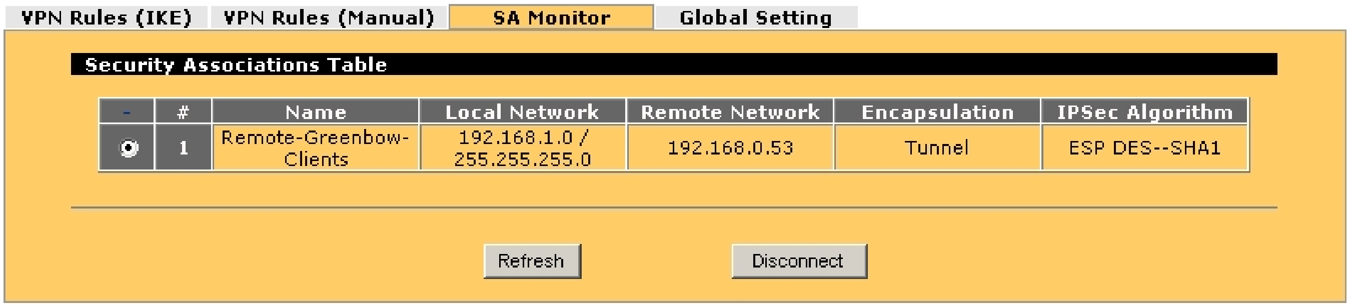


Host	IP	Mode	Crypto
LAN_Cell_P1-LAN_Cell_P2...	192.168.1.0/...	Tunnel	ESP DES ...

VPN Tunnel opened

Figure 16: Greenbow Connections Window

On the LAN-Cell, you can observe the status of the tunnel using the **SA Monitor** tab under the **VPN** menu (see Figure 17).



Security Associations Table

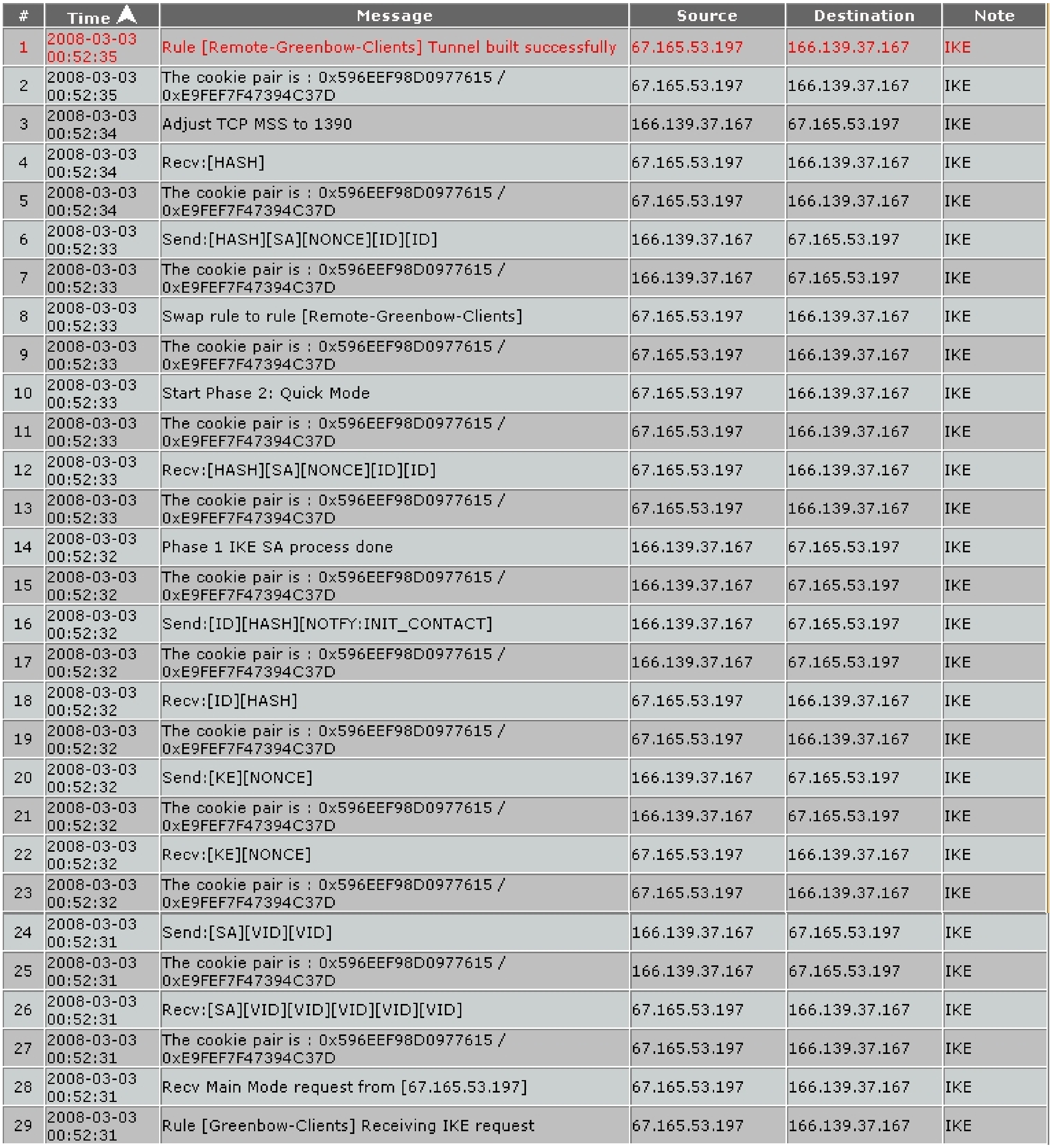
-	#	Name	Local Network	Remote Network	Encapsulation	IPSec Algorithm
●	1	Remote-Greenbow-Clients	192.168.1.0 / 255.255.255.0	192.168.0.53	Tunnel	ESP DES--SHA1

Figure 17: LAN-Cell SA Monitor Screen

Troubleshooting

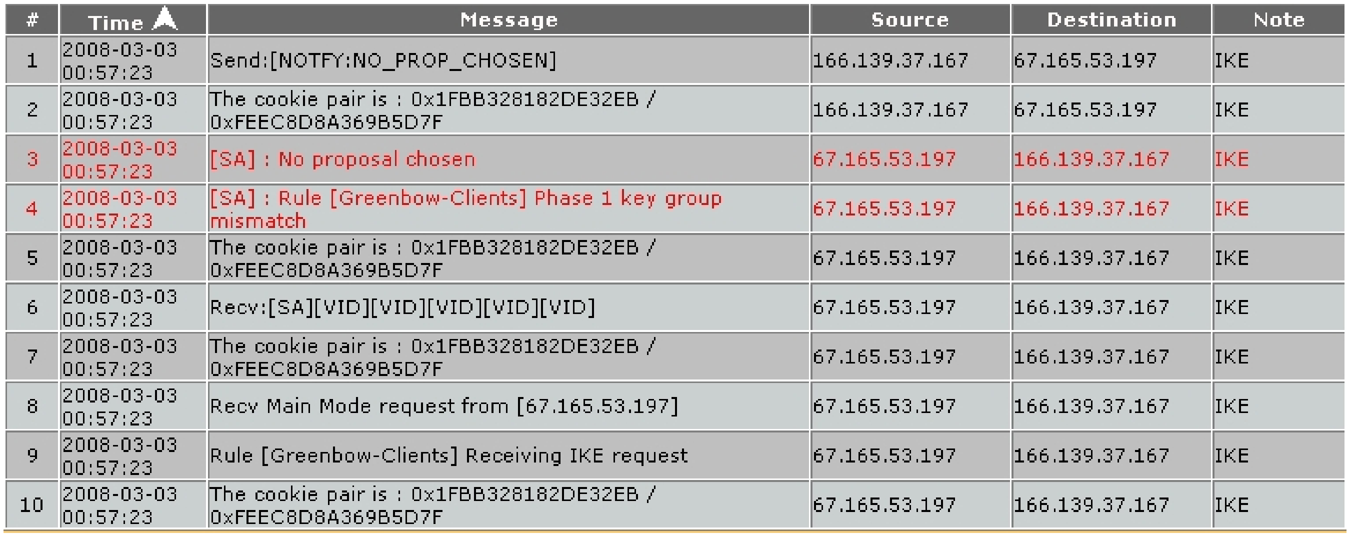
The Greenbow client has extensive error logging features. If your initial attempts at creating the VPN tunnel are unsuccessful, then open the **Console** window and select **Options** to increase the **Debug** level prior to attempting a new tunnel connection. See the Greenbow website for additional documentation and troubleshooting information. Here are some common VPN-related error messages from the LAN-Cell's log:

Successful VPN Tunnel Creation:



#	Time ▲	Message	Source	Destination	Note
1	2008-03-03 00:52:35	Rule [Remote-Greenbow-Clients] Tunnel built successfully	67.165.53.197	166.139.37.167	IKE
2	2008-03-03 00:52:35	The cookie pair is : 0x596EEF98D0977615 / 0xE9FEF7F47394C37D	67.165.53.197	166.139.37.167	IKE
3	2008-03-03 00:52:34	Adjust TCP MSS to 1390	166.139.37.167	67.165.53.197	IKE
4	2008-03-03 00:52:34	Recv:[HASH]	67.165.53.197	166.139.37.167	IKE
5	2008-03-03 00:52:34	The cookie pair is : 0x596EEF98D0977615 / 0xE9FEF7F47394C37D	67.165.53.197	166.139.37.167	IKE
6	2008-03-03 00:52:33	Send:[HASH][SA][NONCE][ID][ID]	166.139.37.167	67.165.53.197	IKE
7	2008-03-03 00:52:33	The cookie pair is : 0x596EEF98D0977615 / 0xE9FEF7F47394C37D	166.139.37.167	67.165.53.197	IKE
8	2008-03-03 00:52:33	Swap rule to rule [Remote-Greenbow-Clients]	67.165.53.197	166.139.37.167	IKE
9	2008-03-03 00:52:33	The cookie pair is : 0x596EEF98D0977615 / 0xE9FEF7F47394C37D	67.165.53.197	166.139.37.167	IKE
10	2008-03-03 00:52:33	Start Phase 2: Quick Mode	67.165.53.197	166.139.37.167	IKE
11	2008-03-03 00:52:33	The cookie pair is : 0x596EEF98D0977615 / 0xE9FEF7F47394C37D	67.165.53.197	166.139.37.167	IKE
12	2008-03-03 00:52:33	Recv:[HASH][SA][NONCE][ID][ID]	67.165.53.197	166.139.37.167	IKE
13	2008-03-03 00:52:33	The cookie pair is : 0x596EEF98D0977615 / 0xE9FEF7F47394C37D	67.165.53.197	166.139.37.167	IKE
14	2008-03-03 00:52:32	Phase 1 IKE SA process done	166.139.37.167	67.165.53.197	IKE
15	2008-03-03 00:52:32	The cookie pair is : 0x596EEF98D0977615 / 0xE9FEF7F47394C37D	166.139.37.167	67.165.53.197	IKE
16	2008-03-03 00:52:32	Send:[ID][HASH][NOTFY:INIT_CONTACT]	166.139.37.167	67.165.53.197	IKE
17	2008-03-03 00:52:32	The cookie pair is : 0x596EEF98D0977615 / 0xE9FEF7F47394C37D	166.139.37.167	67.165.53.197	IKE
18	2008-03-03 00:52:32	Recv:[ID][HASH]	67.165.53.197	166.139.37.167	IKE
19	2008-03-03 00:52:32	The cookie pair is : 0x596EEF98D0977615 / 0xE9FEF7F47394C37D	67.165.53.197	166.139.37.167	IKE
20	2008-03-03 00:52:32	Send:[KE][NONCE]	166.139.37.167	67.165.53.197	IKE
21	2008-03-03 00:52:32	The cookie pair is : 0x596EEF98D0977615 / 0xE9FEF7F47394C37D	166.139.37.167	67.165.53.197	IKE
22	2008-03-03 00:52:32	Recv:[KE][NONCE]	67.165.53.197	166.139.37.167	IKE
23	2008-03-03 00:52:32	The cookie pair is : 0x596EEF98D0977615 / 0xE9FEF7F47394C37D	67.165.53.197	166.139.37.167	IKE
24	2008-03-03 00:52:31	Send:[SA][VID][VID]	166.139.37.167	67.165.53.197	IKE
25	2008-03-03 00:52:31	The cookie pair is : 0x596EEF98D0977615 / 0xE9FEF7F47394C37D	166.139.37.167	67.165.53.197	IKE
26	2008-03-03 00:52:31	Recv:[SA][VID][VID][VID][VID][VID]	67.165.53.197	166.139.37.167	IKE
27	2008-03-03 00:52:31	The cookie pair is : 0x596EEF98D0977615 / 0xE9FEF7F47394C37D	67.165.53.197	166.139.37.167	IKE
28	2008-03-03 00:52:31	Recv Main Mode request from [67.165.53.197]	67.165.53.197	166.139.37.167	IKE
29	2008-03-03 00:52:31	Rule [Greenbow-Clients] Receiving IKE request	67.165.53.197	166.139.37.167	IKE

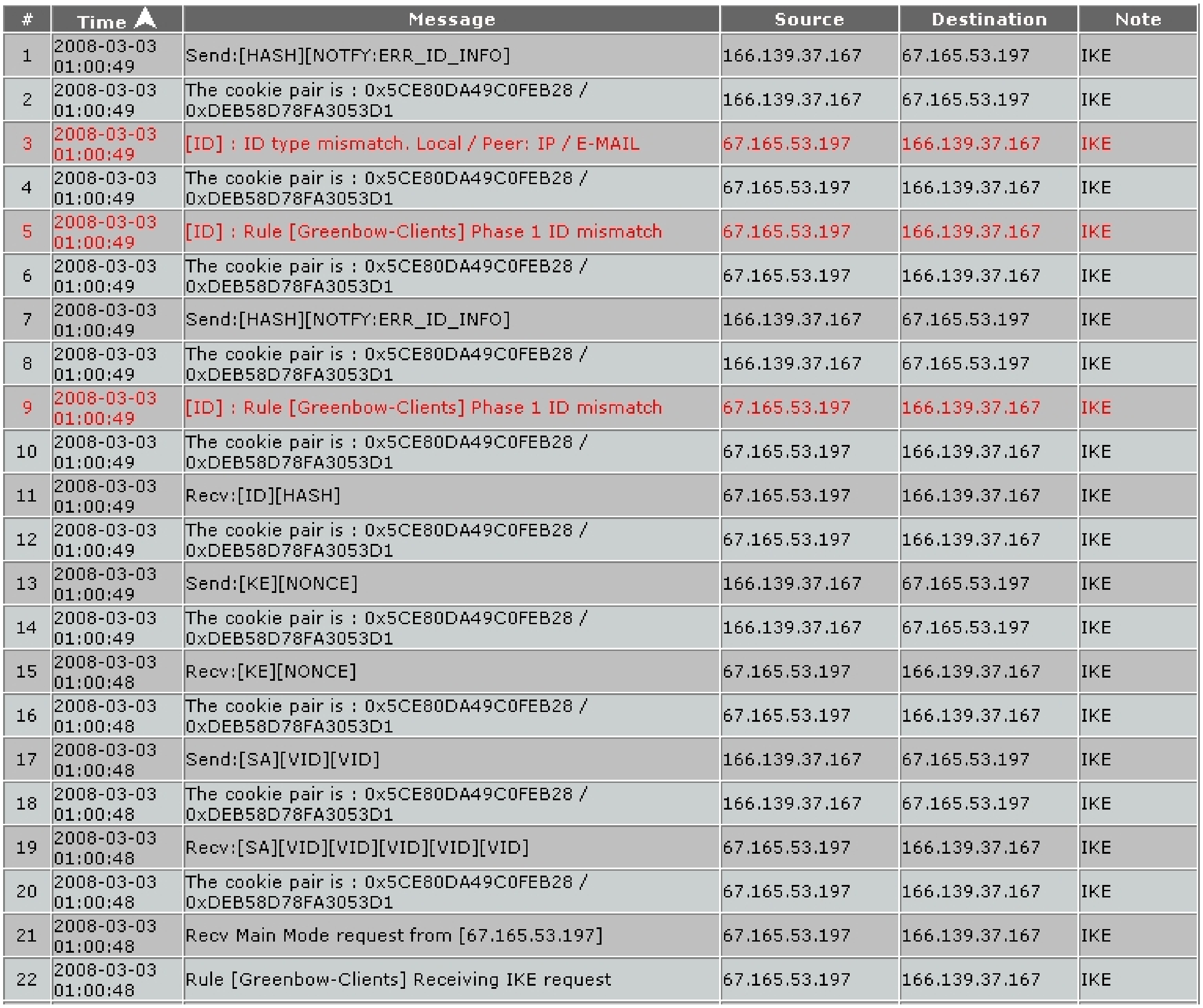
Phase 1 Parameter Mismatch:



#	Time	Message	Source	Destination	Note
1	2008-03-03 00:57:23	Send:[NOTFY:NO_PROP_CHOSEN]	166.139.37.167	67.165.53.197	IKE
2	2008-03-03 00:57:23	The cookie pair is : 0x1FBB328182DE32EB / 0xFEEC8D8A369B5D7F	166.139.37.167	67.165.53.197	IKE
3	2008-03-03 00:57:23	[SA] : No proposal chosen	67.165.53.197	166.139.37.167	IKE
4	2008-03-03 00:57:23	[SA] : Rule [Greenbow-Clients] Phase 1 key group mismatch	67.165.53.197	166.139.37.167	IKE
5	2008-03-03 00:57:23	The cookie pair is : 0x1FBB328182DE32EB / 0xFEEC8D8A369B5D7F	67.165.53.197	166.139.37.167	IKE
6	2008-03-03 00:57:23	Recv:[SA][VID][VID][VID][VID][VID]	67.165.53.197	166.139.37.167	IKE
7	2008-03-03 00:57:23	The cookie pair is : 0x1FBB328182DE32EB / 0xFEEC8D8A369B5D7F	67.165.53.197	166.139.37.167	IKE
8	2008-03-03 00:57:23	Recv Main Mode request from [67.165.53.197]	67.165.53.197	166.139.37.167	IKE
9	2008-03-03 00:57:23	Rule [Greenbow-Clients] Receiving IKE request	67.165.53.197	166.139.37.167	IKE
10	2008-03-03 00:57:23	The cookie pair is : 0x1FBB328182DE32EB / 0xFEEC8D8A369B5D7F	67.165.53.197	166.139.37.167	IKE

Compare the Phase 1 parameters on both the LAN-Cell VPN Gateway Policy Edit page and the Greenbow client's Phase 1 page, in particular the Encryption, Authentication and the Key Group. Note: DH1 = DH768 and DH2 = DH1024.

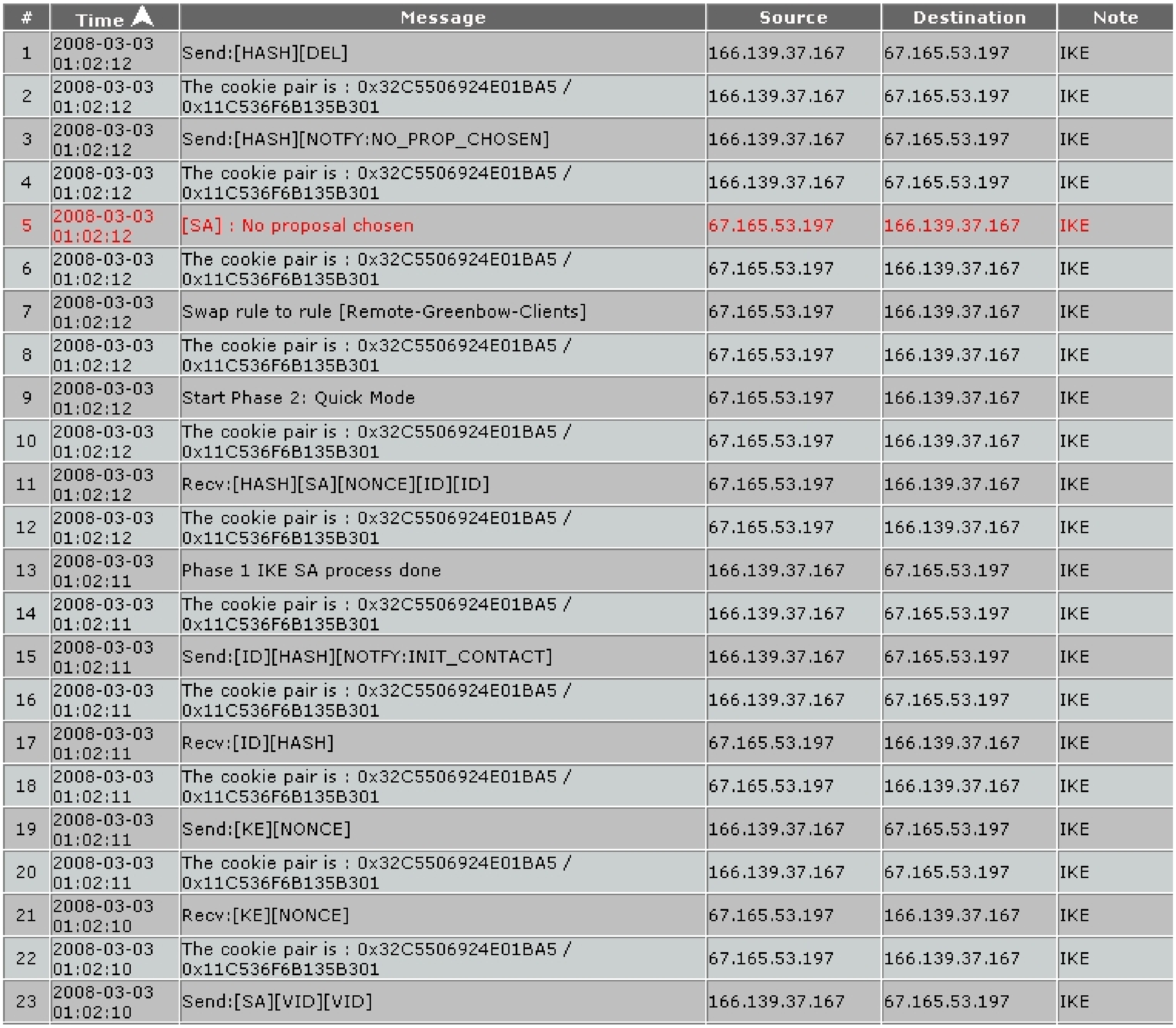
Incorrect ID Type/Content:



#	Time	Message	Source	Destination	Note
1	2008-03-03 01:00:49	Send:[HASH][NOTFY:ERR_ID_INFO]	166.139.37.167	67.165.53.197	IKE
2	2008-03-03 01:00:49	The cookie pair is : 0x5CE80DA49C0FEB28 / 0xDEB58D78FA3053D1	166.139.37.167	67.165.53.197	IKE
3	2008-03-03 01:00:49	[ID] : ID type mismatch. Local / Peer: IP / E-MAIL	67.165.53.197	166.139.37.167	IKE
4	2008-03-03 01:00:49	The cookie pair is : 0x5CE80DA49C0FEB28 / 0xDEB58D78FA3053D1	67.165.53.197	166.139.37.167	IKE
5	2008-03-03 01:00:49	[ID] : Rule [Greenbow-Clients] Phase 1 ID mismatch	67.165.53.197	166.139.37.167	IKE
6	2008-03-03 01:00:49	The cookie pair is : 0x5CE80DA49C0FEB28 / 0xDEB58D78FA3053D1	67.165.53.197	166.139.37.167	IKE
7	2008-03-03 01:00:49	Send:[HASH][NOTFY:ERR_ID_INFO]	166.139.37.167	67.165.53.197	IKE
8	2008-03-03 01:00:49	The cookie pair is : 0x5CE80DA49C0FEB28 / 0xDEB58D78FA3053D1	166.139.37.167	67.165.53.197	IKE
9	2008-03-03 01:00:49	[ID] : Rule [Greenbow-Clients] Phase 1 ID mismatch	67.165.53.197	166.139.37.167	IKE
10	2008-03-03 01:00:49	The cookie pair is : 0x5CE80DA49C0FEB28 / 0xDEB58D78FA3053D1	67.165.53.197	166.139.37.167	IKE
11	2008-03-03 01:00:49	Recv:[ID][HASH]	67.165.53.197	166.139.37.167	IKE
12	2008-03-03 01:00:49	The cookie pair is : 0x5CE80DA49C0FEB28 / 0xDEB58D78FA3053D1	67.165.53.197	166.139.37.167	IKE
13	2008-03-03 01:00:49	Send:[KE][NONCE]	166.139.37.167	67.165.53.197	IKE
14	2008-03-03 01:00:49	The cookie pair is : 0x5CE80DA49C0FEB28 / 0xDEB58D78FA3053D1	166.139.37.167	67.165.53.197	IKE
15	2008-03-03 01:00:48	Recv:[KE][NONCE]	67.165.53.197	166.139.37.167	IKE
16	2008-03-03 01:00:48	The cookie pair is : 0x5CE80DA49C0FEB28 / 0xDEB58D78FA3053D1	67.165.53.197	166.139.37.167	IKE
17	2008-03-03 01:00:48	Send:[SA][VID][VID]	166.139.37.167	67.165.53.197	IKE
18	2008-03-03 01:00:48	The cookie pair is : 0x5CE80DA49C0FEB28 / 0xDEB58D78FA3053D1	166.139.37.167	67.165.53.197	IKE
19	2008-03-03 01:00:48	Recv:[SA][VID][VID][VID][VID][VID]	67.165.53.197	166.139.37.167	IKE
20	2008-03-03 01:00:48	The cookie pair is : 0x5CE80DA49C0FEB28 / 0xDEB58D78FA3053D1	67.165.53.197	166.139.37.167	IKE
21	2008-03-03 01:00:48	Recv Main Mode request from [67.165.53.197]	67.165.53.197	166.139.37.167	IKE
22	2008-03-03 01:00:48	Rule [Greenbow-Clients] Receiving IKE request	67.165.53.197	166.139.37.167	IKE

This error is commonly caused when the Local and Remote ID types and/or Content values are not the same on each device. Check the P1 Advanced page on the Greenbow client to be sure that IP is selected. You can also use E-Mail or DNS ID Types/Content as long as they match the corresponding settings on the LAN-Cell. Remember that the Local and Remote values are relative to each device -- e.g. LAN-Cell Local = Greenbow Remote.

Phase 2 Parameter Mismatch:



#	Time ▲	Message	Source	Destination	Note
1	2008-03-03 01:02:12	Send:[HASH][DEL]	166.139.37.167	67.165.53.197	IKE
2	2008-03-03 01:02:12	The cookie pair is : 0x32C5506924E01BA5 / 0x11C536F6B135B301	166.139.37.167	67.165.53.197	IKE
3	2008-03-03 01:02:12	Send:[HASH][NOTFY:NO_PROP_CHOSEN]	166.139.37.167	67.165.53.197	IKE
4	2008-03-03 01:02:12	The cookie pair is : 0x32C5506924E01BA5 / 0x11C536F6B135B301	166.139.37.167	67.165.53.197	IKE
5	2008-03-03 01:02:12	[SA] : No proposal chosen	67.165.53.197	166.139.37.167	IKE
6	2008-03-03 01:02:12	The cookie pair is : 0x32C5506924E01BA5 / 0x11C536F6B135B301	67.165.53.197	166.139.37.167	IKE
7	2008-03-03 01:02:12	Swap rule to rule [Remote-Greenbow-Clients]	67.165.53.197	166.139.37.167	IKE
8	2008-03-03 01:02:12	The cookie pair is : 0x32C5506924E01BA5 / 0x11C536F6B135B301	67.165.53.197	166.139.37.167	IKE
9	2008-03-03 01:02:12	Start Phase 2: Quick Mode	67.165.53.197	166.139.37.167	IKE
10	2008-03-03 01:02:12	The cookie pair is : 0x32C5506924E01BA5 / 0x11C536F6B135B301	67.165.53.197	166.139.37.167	IKE
11	2008-03-03 01:02:12	Recv:[HASH][SA][NONCE][ID][ID]	67.165.53.197	166.139.37.167	IKE
12	2008-03-03 01:02:12	The cookie pair is : 0x32C5506924E01BA5 / 0x11C536F6B135B301	67.165.53.197	166.139.37.167	IKE
13	2008-03-03 01:02:11	Phase 1 IKE SA process done	166.139.37.167	67.165.53.197	IKE
14	2008-03-03 01:02:11	The cookie pair is : 0x32C5506924E01BA5 / 0x11C536F6B135B301	166.139.37.167	67.165.53.197	IKE
15	2008-03-03 01:02:11	Send:[ID][HASH][NOTFY:INIT_CONTACT]	166.139.37.167	67.165.53.197	IKE
16	2008-03-03 01:02:11	The cookie pair is : 0x32C5506924E01BA5 / 0x11C536F6B135B301	166.139.37.167	67.165.53.197	IKE
17	2008-03-03 01:02:11	Recv:[ID][HASH]	67.165.53.197	166.139.37.167	IKE
18	2008-03-03 01:02:11	The cookie pair is : 0x32C5506924E01BA5 / 0x11C536F6B135B301	67.165.53.197	166.139.37.167	IKE
19	2008-03-03 01:02:11	Send:[KE][NONCE]	166.139.37.167	67.165.53.197	IKE
20	2008-03-03 01:02:11	The cookie pair is : 0x32C5506924E01BA5 / 0x11C536F6B135B301	166.139.37.167	67.165.53.197	IKE
21	2008-03-03 01:02:10	Recv:[KE][NONCE]	67.165.53.197	166.139.37.167	IKE
22	2008-03-03 01:02:10	The cookie pair is : 0x32C5506924E01BA5 / 0x11C536F6B135B301	67.165.53.197	166.139.37.167	IKE
23	2008-03-03 01:02:10	Send:[SA][VID][VID]	166.139.37.167	67.165.53.197	IKE

Similar to a Phase 1 proposal error, this indicates that the Phase 2 parameters do not match. Check the LAN-Cell's VPN Network Policy Edit page settings against the Greenbow's Phase 2 settings.

Frequently Asked Questions

Q: Can I have more than 1 Greenbow PC make a VPN connection to the LAN-Cell at the same time?

A: Yes. The configuration shown will permit up to 5 simultaneous clients to establish VPN tunnels with the LAN-Cell 2 at the same time (using different IP addresses on the HQ LAN network). You can either create 1 default rule (as in this example) or 5 specific rules, one for each remote computer. The LAN-Cell 2 supports 5 simultaneous VPN tunnels; the original LAN-Cell Mobile Gateway supports 2 VPN tunnels.

Q: Can I create a VPN tunnel to my LAN-Cell that has a dynamic IP address?

A: Yes. The Greenbow client supports a fully qualified domain name (FQDN) as a remote gateway. You must first create a host and domain name using the DynDNS.org service and configure the LAN-Cell to update the DynDNS name every time the LAN-Cell's public WAN IP address changes.

See the **ADVANCED->DNS->DDNS** screen in the LAN-Cell 2 as well as the *LAN-Cell User's Guide* for more information.

Q: Can the LAN-Cell initiate the VPN tunnel connection?

A: Not with the configuration shown in this example. The LAN-Cell can initiate a VPN tunnel if it knows the address (or FQDN) of the remote gateway you want to connect with (in either site-to-site or client-to-site mode). This example is strictly for remote client initiated VPN tunnels.

Q: Can I force the remote VPN user to enter a username & password?

A: Yes. This is called "Extended Authentication (X-AUTH)". On the LAN-Cell, you must define a Username and Password for the remote user on the **SECURITY->AUTH SERVER->LOCAL USER DATABASE** screen (or define a link to a RADIUS server that is accessible on the LAN subnet). Next, edit the VPN Gateway Policy settings to enable Extended Authentication in Server mode.

In the Greenbow client, click the Phase 1 Advanced Button and either enable the X-Auth Popup to prompt the user for the username and password defined on the LAN-Cell prior to each connection, or enter the username and password in the fields provided on the P1 Advanced screen. Note, the LAN-Cell does not support Hybrid Mode.

# # #