



Proxicast IPSec VPN Client Example

Technote LCTN0013

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

© Copyright 2005-2009, Proxicast LLC. All rights reserved.

Proxicast is a registered trademark and LAN-Cell, and LAN-Cell Mobile Gateway are trademarks of Proxicast LLC. All other trademarks mentioned herein are the property of their respective owners.

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.

Document Revision History:

Date	Comments
February 2, 2009	First release

Introduction

The Proxicast IPSec VPN Client is a low-cost, easy to use software VPN client application for Microsoft Windows. A fully-function 30 day Evaluation Version of the software may be download from the Proxicast website:

http://www.proxicast.com/vpnclient/VPN_Client_Download.htm

This Technote documents how to use the VPN Configuration Wizards built into the LAN-Cell 2 and the VPN Client for Windows to quickly create a secure remote access connection from a Windows PC to the LAN-Cell's remote LAN devices.

The Proxicast VPN Client for Windows and the LAN-Cell can be configured for other IPSec settings depending upon your requirements. Also, the Proxicast VPN Client for Windows is fully IPSec-standard compliant and can be used to establish VPN tunnels to many other vendors' IPSec devices. Please consult the *LAN-Cell User's Guide* and the *Proxicast IPSec VPN Client for Windows User's Guide* for more information.

This Technote is for illustration purposes only.

Example Network Topology

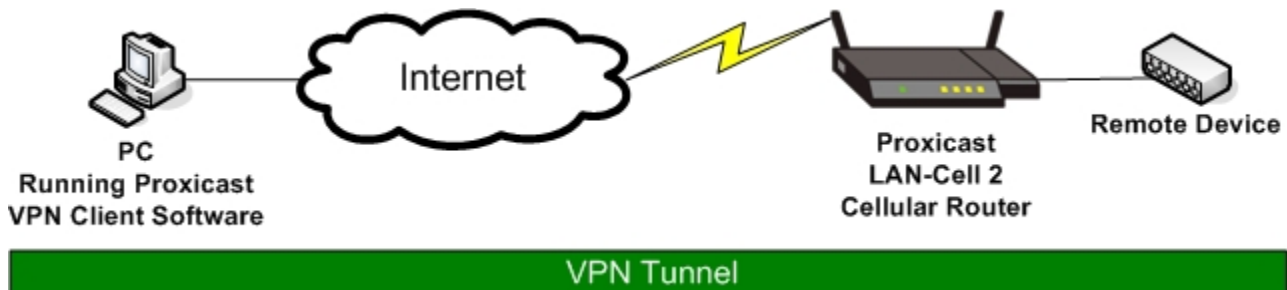


Figure 1: Example Network Topology

Usage Notes

- This example was created using the Proxicast IPSec VPN Client for Windows version 4.51.001 and LAN-Cell 2 firmware version 4.02(AQP.3).
- 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. If your LAN-Cell has a dynamic IP address, the same configuration is possible by replacing the static IP address with a fully qualified dynamic DNS name (FQDN) such as *myrouter.dyndns.org* (see the Advanced->DNS->DDNS screen).
- Your PC and any intervening firewalls must be configured to allow IKE (UDP:500) packets to flow between your PC and the LAN-Cell in order for the IPSec tunnel to be negotiated. If there is a NAT router between your PC and the Internet, you may need to enable NAT-Traversal (NAT-T) on both the LAN-Cell and the VPN Client software.
- This example demonstrates a Single Address VPN connection to a remote subnet via a VPN Tunnel (LAN-Cell's LAN subnet). The Proxicast 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, Juniper, SonicWall, ZyXEL, etc.

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 Proxicast VPN Client connection parameters on the LAN-Cell 2. To reach this screen, select **SECURITY** then **VPN Wizard** from the left side menu (Figure 2).

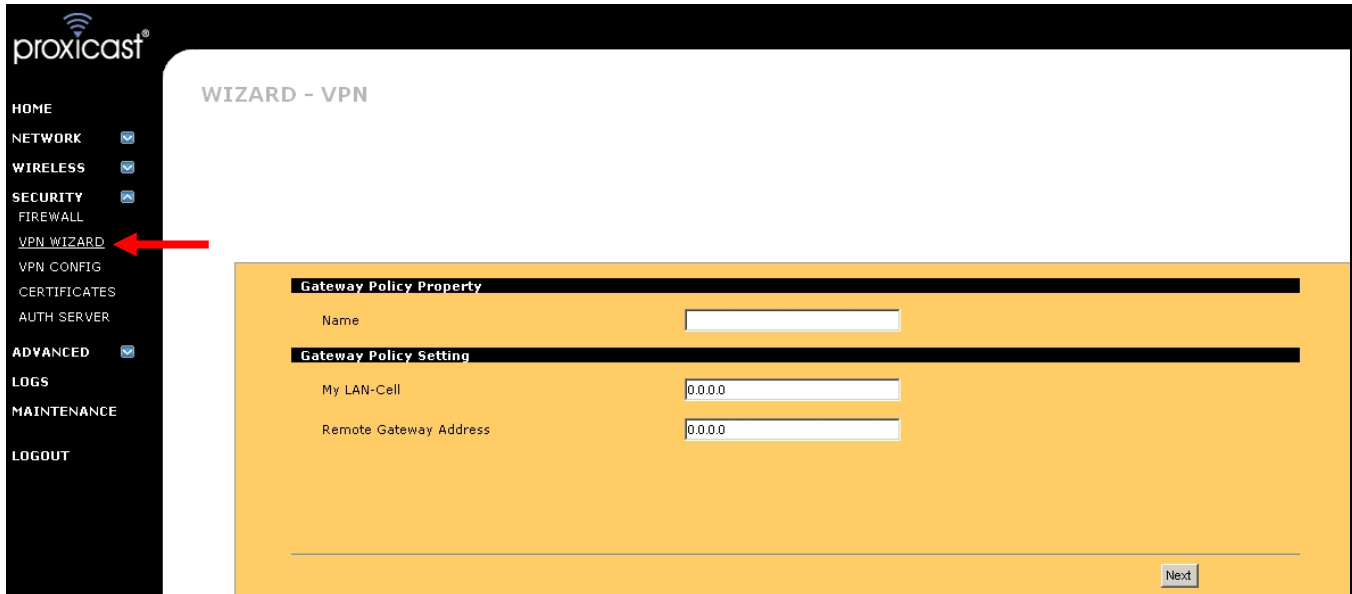


Figure 2: LAN-Cell 2 VPN Wizard

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 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 parameter in the Proxicast VPN 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 Proxicast VPN Clients from multiple PCs. Also, when the Proxicast 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 Proxicast VPN 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 *LAN-Cell User's Guide* for more information on creating firewall rules.

Gateway Policy Property

Name: Proxicast VPN Clients

Gateway Policy Setting

My LAN-Cell: 166.139.37.157

Remote Gateway Address: 0.0.0.0

Next

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 Proxicast VPN Clients

Network Policy Setting

Local Network

Starting IP Address: 192 . 168 . 1 . 0

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

Remote Network

Starting IP Address: 0 . 0 . 0 . 0

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

Back Next

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 Proxicast VPN Client.

Next, we define the IKE Phase 1 parameters that will be used to negotiate the initial VPN tunnel connection between the Proxicast VPN 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: (Seconds)

Pre-Shared Key:

Back Next

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 as they match the default IKE parameters in the Proxicast VPN Client.

The LAN-Cell and Proxicast VPN Client 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 Proxicast VPN 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: (Seconds)

Perfect Forward Secrecy (PFS): None DH1 DH2

Back Next

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. They match the default Phase 2 configuration settings in the Proxicast VPN Client.

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	Proxicast VPN 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 Proxicast VPN 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

Back Finish

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.

Click on the **LOGS** Menu, clear any existing entries, and then launch the Proxicast VPN Client for Windows software.

Example Proxicast VPN Client for Windows Configuration

After starting the Proxicast VPN Client software for the first time (or by selecting the VPN Configuration/Config. Wizard menu), the VPN Configuration Wizard is displayed (Figure 9).

Figure 9: Proxicast VPN Client Wizard Step 1

The Wizard is pre-filled with a DNS Name of *myrouter.dyndns.org*. You must change this to the FQDN or static IP address of your LAN-Cell. In our example, this is 166.139.37.167 (Figure 10).

Likewise, the default Preshared-key value in the Wizard is *12345678*. Change this to the value entered as the Preshared-key in the LAN-Cell's VPN Wizard.

The Private IP subnet of the remote network is pre-filled to the factory default of the LAN-Cell (*192.168.1.0*). If you changed the LAN-Cell's IP address & subnet, enter the subnet value here.

Note this is the SUBNET ADDRESS of the LAN-Cell's private network, not the IP address of the LAN-Cell. Typically you will have set the LAN-Cell to a Class-C subnet and will specify a "0" in the last octet (In our example this value is 192.168.1.0 reflecting a subnet mask of 255.255.255.0).

Figure 10: Wizard Step 1 Example Values

Click the **NEXT** button in the Wizard to display the Configuration Summary screen (Figure 11).

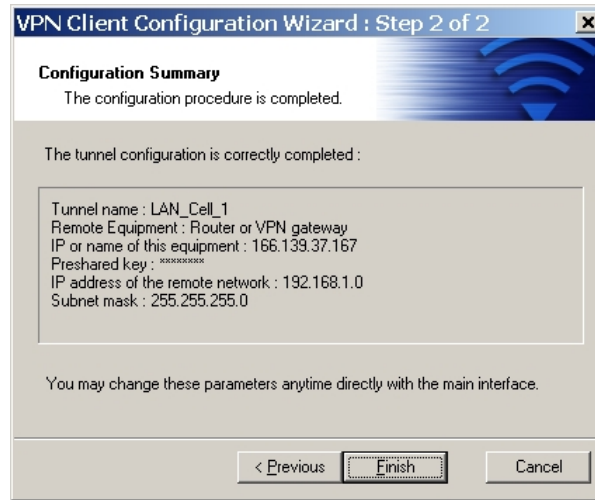


Figure 11: VPN Client Configuration Wizard Step 2

Clicking the **FINISH** button displays the Proxicast VPN Client main Configuration Panel showing the Phase 1 (LAN_Cell_1) and Phase 2 (Tunnel_1) parameter sets created by the Configuration Wizard (Figure 12).

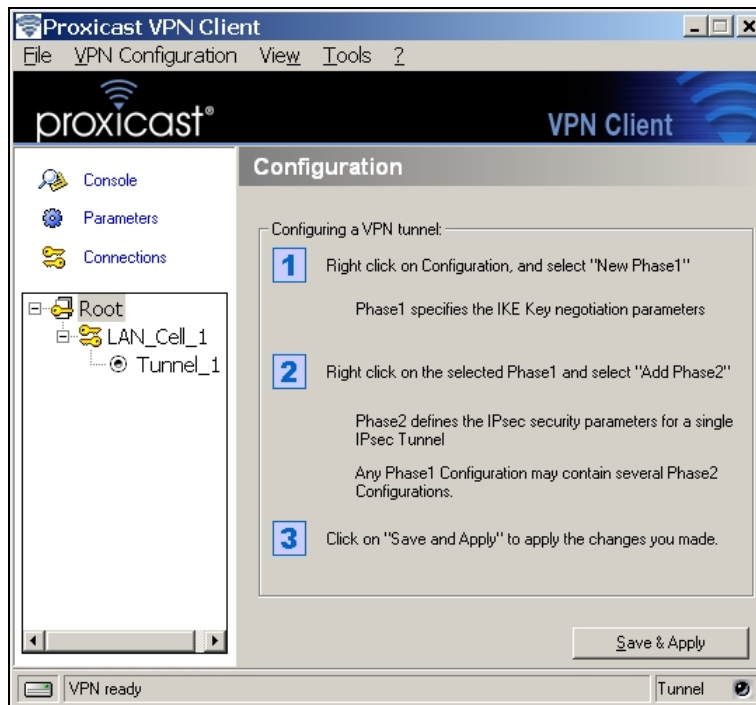


Figure 12: VPN Client Configuration Panel

You are now ready to open a VPN Tunnel to the LAN-Cell. Select Tunnel_1 and click the **Open Tunnel** button on the lower right side of the screen (Figure 13).

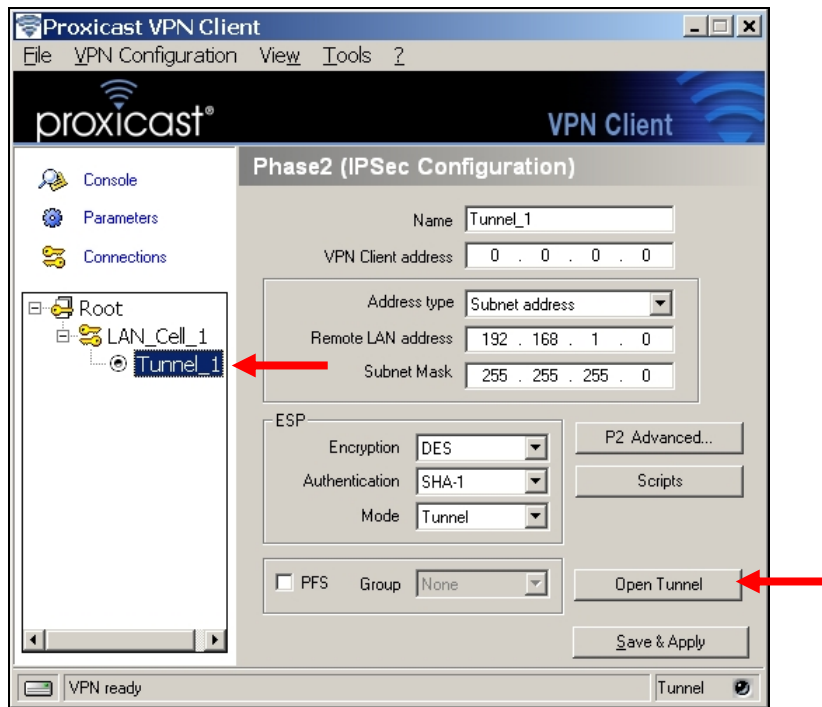


Figure 13: Opening a VPN Tunnel from the Configuration Panel

You can also open a tunnel from the Windows System Tray area of the Taskbar. Right click the red Proxicast VPN Client Tunnel Status Icon and select Open Tunnel from the popup menu (Figure 14).

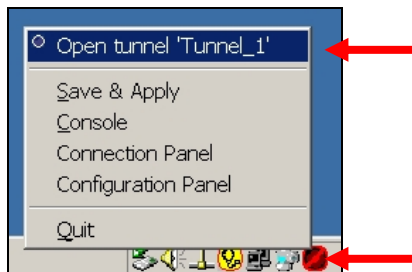


Figure 14: Opening a VPN Tunnel from the System Tray

While the tunnel is being established, you will see several status popups in the System Tray area (Figure 15).

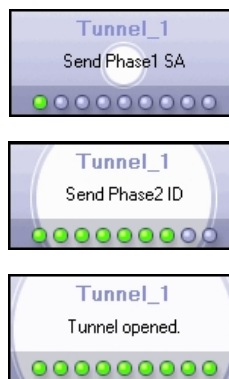


Figure 15: VPN Tunnel Progress Popups

Once the tunnel is established, the System Tray icon will turn green and the VPN Client status bar will indicate *VPN Tunnel Opened* (Figure 16).

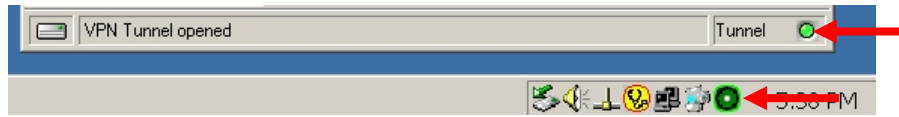


Figure 16: VPN Tunnel Progress Status Icons

You may also view and change the status of the tunnel using the Tunnels View (Figure 17) or Connections Panel (Figure 18).

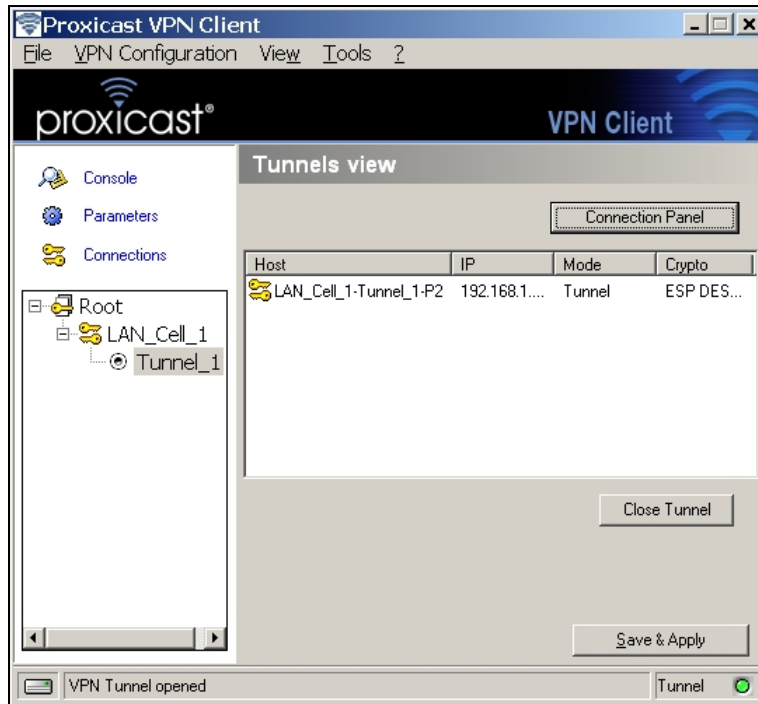


Figure 17: Tunnels View

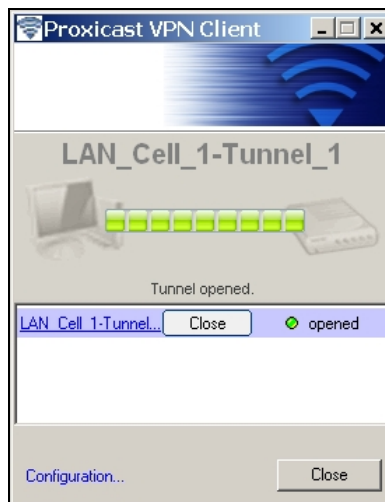
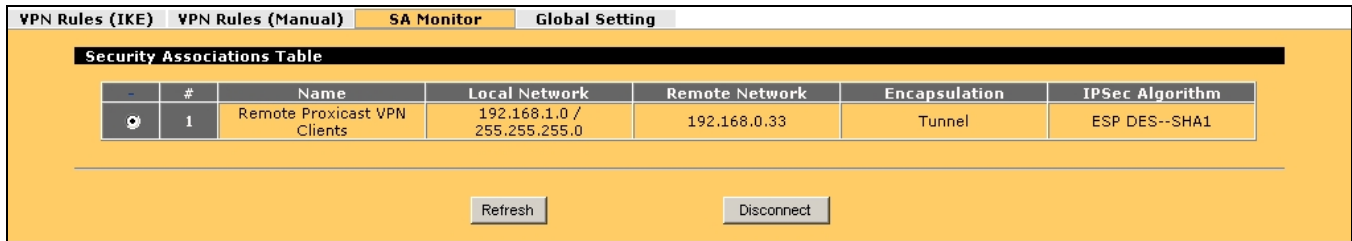


Figure 18: Connections Panel

On the LAN-Cell, you can observe the status of the tunnel using the **VPN** button on the Home Screen or the **SA Monitor** tab under the **VPN CONFIG** menu (Figure 19).



The screenshot shows a web interface with a navigation bar at the top containing four tabs: 'VPN Rules (IKE)', 'VPN Rules (Manual)', 'SA Monitor', and 'Global Setting'. The 'SA Monitor' tab is selected and highlighted in orange. Below the navigation bar is a section titled 'Security Associations Table' with a black header. The table contains one data row with the following details:

#	Name	Local Network	Remote Network	Encapsulation	IPsec Algorithm
1	Remote Proxicast VPN Clients	192.168.1.0 / 255.255.255.0	192.168.0.33	Tunnel	ESP DES--SHA1

Below the table, there are two buttons: 'Refresh' and 'Disconnect'.

Figure 19: LAN-Cell SA Monitor Screen

Reviewing the VPN Tunnel Configuration Parameters

You can review and modify the VPN configuration parameters of the LAN-Cell by using the **VPN Config** option on the LAN-Cell's left side menu (Figure 20).

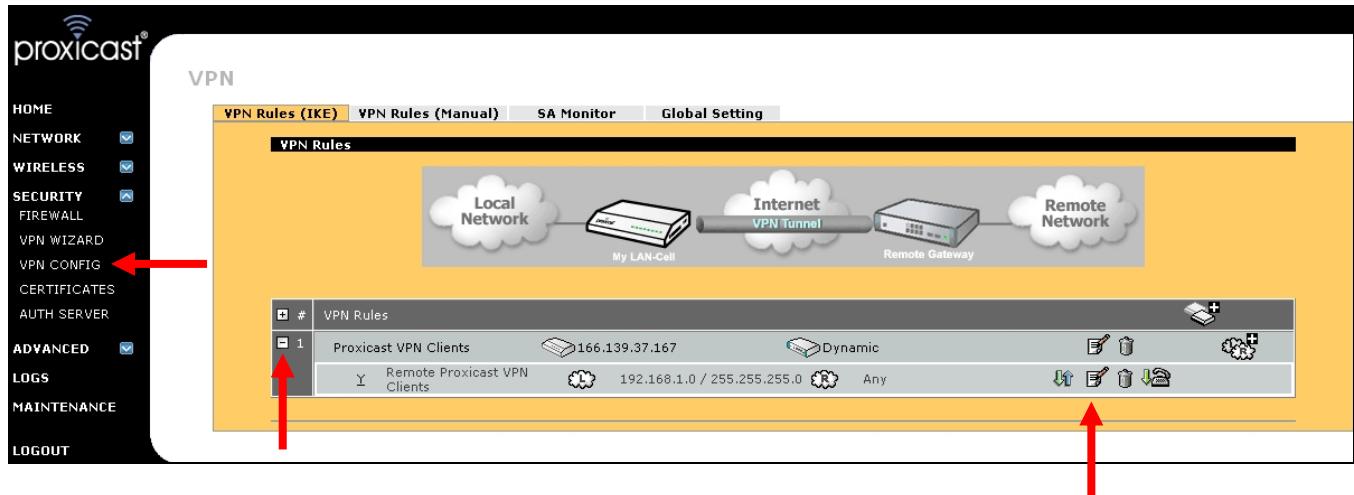


Figure 20: LAN-Cell VPN Configuration Screen


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 20).

Figure 21 shows the VPN Gateway Policy Edit screen.

VPN - GATEWAY POLICY - EDIT

Property

Name:

NAT Traversal

Gateway Policy Information

My LAN-Cell

- My Address: (Domain Name or IP Address)
- My Domain Name: (See [DDNS](#))

Primary Remote Gateway: (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*: (180-86400 seconds)

*Fall Back Check Interval: The time interval for checking availability 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:
- Certificate: (See [My Certificates](#))

Local ID Type:

Content:

Peer ID Type:

Content:

Extended Authentication

Enable Extended Authentication

- Server Mode (Search [Local User](#) first then [RADIUS](#))
- Client Mode

User Name:

Password:

IKE Proposal

Negotiation Mode:

Encryption Algorithm:

Authentication Algorithm:

SA Life Time (Seconds):

Key Group:

Enable Multiple Proposals

Associated Network Policies

#	Name	Local Network	Remote Network	
	Remote Proxicast VPN Clients	192.168.1.0 / 255.255.255.0	Any	

Figure 21: Editing the VPN Gateway Policy Parameters

Figure 22 shows the VPN Network Policy Edit screen.

VPN - NETWORK POLICY - EDIT

Property

Active
 Name: Remote Proxicast VPN 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: Proxicast VPN Clients

Virtual Address Mapping Rule:

Active
 Virtual Address Mapping Rule: Port Forwarding Rules
 Type: One-to-One
 Private Starting IP Address: 0 . 0 . 0 . 0
 Private Ending IP Address: 0 . 0 . 0 . 0
 Virtual Starting IP Address: 0 . 0 . 0 . 0
 Virtual Ending IP Address: 0 . 0 . 0 . 0

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 22: Editing the VPN Network Policy Parameters

In the Proxicast IPSec VPN Client, you can review and modify the Phase 1 and Phase 2 parameters by selecting the corresponding entry in the Configuration Panel as well as the Advanced button (Figures 23 and 24).

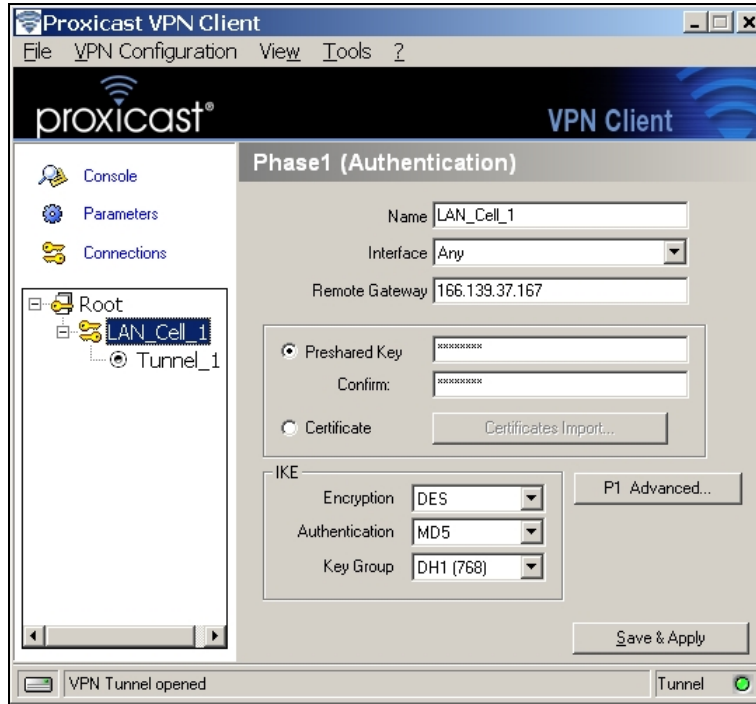


Figure 23: VPN Client Phase 1 Parameters

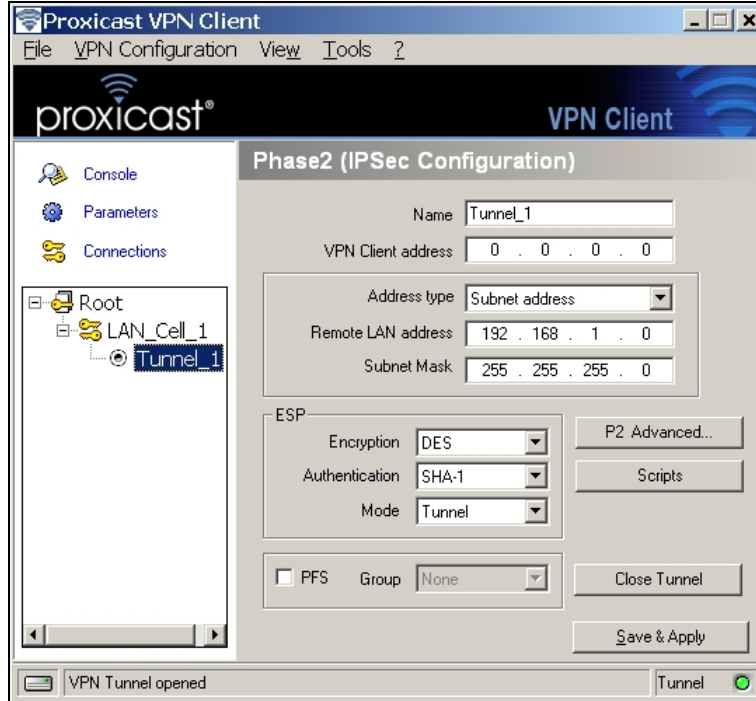


Figure 24: VPN Client Phase 2 Parameters

Troubleshooting

The Proxicast LAN-Cell and the VPN Client software both have extensive error logging features. On the VPN Client, problems during Phase 1 and Phase 2 are indicated in the popup status windows (Figure 25). You can also open the **Console** window in the VPN Client prior to attempting a new tunnel connection (Figure 26).

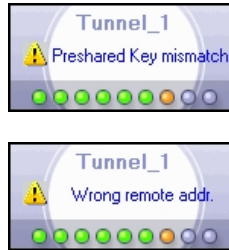


Figure 25: VPN Client Error Examples

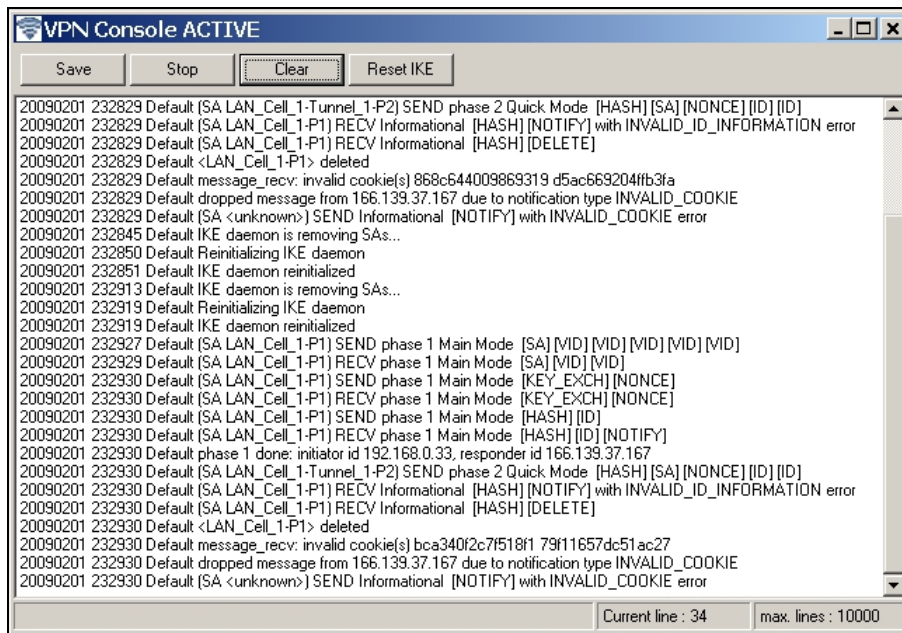


Figure 26: VPN Client Debug Console Messages

The most common issues when VPN tunnels fail to open are:

- Not clicking **Save & Apply** after making configuration changes.
- Not waiting approximately 30 seconds after a connection failure (or tunnel close) to allow both sides to fully reset before reattempting to open a tunnel.
- Entering a Phase 2 VPN Client Address other than 0.0.0.0 which conflicts with the LAN-Cell's subnet.
- Entering a Phase 2 Remote LAN Address/Subnet that does not match the LAN-Cell's subnet.

You can also view the LAN-Cell's log after a connection attempt. Below are some common VPN-related error messages from the LAN-Cell's log:

Successful VPN Tunnel Creation:

1	2009-02-02 04:42:50	Rule [Remote Proxicast VPN Clients] Tunnel built successfully	24.3.147.160	166.139.37.167	IKE
2	2009-02-02 04:42:50	The cookie pair is : 0xE93B3D99ABB4AE1A / 0x2088E8D1ED9C0C40	24.3.147.160	166.139.37.167	IKE
3	2009-02-02 04:42:49	Adjust TCP MSS to 1390	166.139.37.167	24.3.147.160	IKE
4	2009-02-02 04:42:49	Recv:[HASH]	24.3.147.160	166.139.37.167	IKE
5	2009-02-02 04:42:49	The cookie pair is : 0xE93B3D99ABB4AE1A / 0x2088E8D1ED9C0C40	24.3.147.160	166.139.37.167	IKE
6	2009-02-02 04:42:49	Send:[HASH][SA][NONCE][ID][ID]	166.139.37.167	24.3.147.160	IKE
7	2009-02-02 04:42:49	The cookie pair is : 0xE93B3D99ABB4AE1A / 0x2088E8D1ED9C0C40	166.139.37.167	24.3.147.160	IKE
8	2009-02-02 04:42:49	Swap rule to rule [Remote Proxicast VPN Clients]	24.3.147.160	166.139.37.167	IKE
9	2009-02-02 04:42:49	The cookie pair is : 0xE93B3D99ABB4AE1A / 0x2088E8D1ED9C0C40	24.3.147.160	166.139.37.167	IKE
10	2009-02-02 04:42:49	Start Phase 2: Quick Mode	24.3.147.160	166.139.37.167	IKE
11	2009-02-02 04:42:49	The cookie pair is : 0xE93B3D99ABB4AE1A / 0x2088E8D1ED9C0C40	24.3.147.160	166.139.37.167	IKE
12	2009-02-02 04:42:49	Recv:[HASH][SA][NONCE][ID][ID]	24.3.147.160	166.139.37.167	IKE
13	2009-02-02 04:42:49	The cookie pair is : 0xE93B3D99ABB4AE1A / 0x2088E8D1ED9C0C40	24.3.147.160	166.139.37.167	IKE
14	2009-02-02 04:42:48	Phase 1 IKE SA process done	166.139.37.167	24.3.147.160	IKE
15	2009-02-02 04:42:48	The cookie pair is : 0xE93B3D99ABB4AE1A / 0x2088E8D1ED9C0C40	166.139.37.167	24.3.147.160	IKE
16	2009-02-02 04:42:48	Send:[ID][HASH][NOTFY:INIT_CONTACT]	166.139.37.167	24.3.147.160	IKE
17	2009-02-02 04:42:48	The cookie pair is : 0xE93B3D99ABB4AE1A / 0x2088E8D1ED9C0C40	166.139.37.167	24.3.147.160	IKE
18	2009-02-02 04:42:48	Recv:[ID][HASH]	24.3.147.160	166.139.37.167	IKE
19	2009-02-02 04:42:48	The cookie pair is : 0xE93B3D99ABB4AE1A / 0x2088E8D1ED9C0C40	24.3.147.160	166.139.37.167	IKE
20	2009-02-02 04:42:48	Send:[KE][NONCE]	166.139.37.167	24.3.147.160	IKE
21	2009-02-02 04:42:48	The cookie pair is : 0xE93B3D99ABB4AE1A / 0x2088E8D1ED9C0C40	166.139.37.167	24.3.147.160	IKE
22	2009-02-02 04:42:48	Recv:[KE][NONCE]	24.3.147.160	166.139.37.167	IKE
23	2009-02-02 04:42:48	The cookie pair is : 0xE93B3D99ABB4AE1A / 0x2088E8D1ED9C0C40	24.3.147.160	166.139.37.167	IKE
24	2009-02-02 04:42:48	Send:[SA][VID][VID]	166.139.37.167	24.3.147.160	IKE
25	2009-02-02 04:42:48	The cookie pair is : 0xE93B3D99ABB4AE1A / 0x2088E8D1ED9C0C40	166.139.37.167	24.3.147.160	IKE
26	2009-02-02 04:42:48	Recv:[SA][VID][VID][VID][VID][VID]	24.3.147.160	166.139.37.167	IKE
27	2009-02-02 04:42:48	The cookie pair is : 0xE93B3D99ABB4AE1A / 0x2088E8D1ED9C0C40	24.3.147.160	166.139.37.167	IKE
28	2009-02-02 04:42:48	Recv Main Mode request from [24.3.147.160]	24.3.147.160	166.139.37.167	IKE

Phase 1 Parameter Mismatch:

#	Time ▲	Message	Source	Destination	Note
1	2009-02-02 04:45:27	Send:[NOTFY:NO_PROP_CHOSEN]	166.139.37.167	24.3.147.160	IKE
2	2009-02-02 04:45:27	The cookie pair is : 0x917DC8B116521D0A / 0x56466B9C5A896D70	166.139.37.167	24.3.147.160	IKE
3	2009-02-02 04:45:27	[SA] : No proposal chosen	24.3.147.160	166.139.37.167	IKE
4	2009-02-02 04:45:27	[SA] : Rule [Proxicast VPN Clients] Phase 1 key group mismatch	24.3.147.160	166.139.37.167	IKE
5	2009-02-02 04:45:27	The cookie pair is : 0x917DC8B116521D0A / 0x56466B9C5A896D70	24.3.147.160	166.139.37.167	IKE
6	2009-02-02 04:45:27	Recv:[SA][VID][VID][VID][VID][VID]	24.3.147.160	166.139.37.167	IKE
7	2009-02-02 04:45:27	The cookie pair is : 0x917DC8B116521D0A / 0x56466B9C5A896D70	24.3.147.160	166.139.37.167	IKE
8	2009-02-02 04:45:27	Recv Main Mode request from [24.3.147.160]	24.3.147.160	166.139.37.167	IKE
9	2009-02-02 04:45:27	Rule [Proxicast VPN Clients] Receiving IKE request	24.3.147.160	166.139.37.167	IKE
10	2009-02-02 04:45:27	The cookie pair is : 0x917DC8B116521D0A / 0x56466B9C5A896D70	24.3.147.160	166.139.37.167	IKE

Compare the Phase 1 parameters on both the LAN-Cell VPN Gateway Policy Edit page and the Proxicast VPN 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	2009-02-02 04:49:35	Rule[Proxicast VPN Clients] receives duplicate packet	24.3.147.160	166.139.37.167	IKE
2	2009-02-02 04:49:35	The cookie pair is : 0x6D900A98AB697E31 / 0x8F49BA5C0BDD11FE	24.3.147.160	166.139.37.167	IKE
3	2009-02-02 04:49:29	Send:[HASH][NOTFY:ERR_ID_INFO]	166.139.37.167	24.3.147.160	IKE
4	2009-02-02 04:49:29	The cookie pair is : 0x6D900A98AB697E31 / 0x8F49BA5C0BDD11FE	166.139.37.167	24.3.147.160	IKE
5	2009-02-02 04:49:29	[ID] : ID type mismatch. Local / Peer: IP / E-MAIL	24.3.147.160	166.139.37.167	IKE
6	2009-02-02 04:49:29	The cookie pair is : 0x6D900A98AB697E31 / 0x8F49BA5C0BDD11FE	24.3.147.160	166.139.37.167	IKE
7	2009-02-02 04:49:29	[ID] : Rule [Proxicast VPN Clients] Phase 1 ID mismatch	24.3.147.160	166.139.37.167	IKE
8	2009-02-02 04:49:29	The cookie pair is : 0x6D900A98AB697E31 / 0x8F49BA5C0BDD11FE	24.3.147.160	166.139.37.167	IKE
9	2009-02-02 04:49:29	Send:[HASH][NOTFY:ERR_ID_INFO]	166.139.37.167	24.3.147.160	IKE
10	2009-02-02 04:49:29	The cookie pair is : 0x6D900A98AB697E31 / 0x8F49BA5C0BDD11FE	166.139.37.167	24.3.147.160	IKE
11	2009-02-02 04:49:29	[ID] : Rule [Proxicast VPN Clients] Phase 1 ID mismatch	24.3.147.160	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 Proxicast VPN 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 = PC Remote.

Phase 2 Parameter Mismatch:

#	Time ▲	Message	Source	Destination	Note
1	2009-02-02 04:51:57	Send:[HASH][DEL]	166.139.37.167	24.3.147.160	IKE
2	2009-02-02 04:51:57	The cookie pair is : 0x4C09888FC8AA9965 / 0x705259D351E2779C	166.139.37.167	24.3.147.160	IKE
3	2009-02-02 04:51:57	Send:[HASH][NOTFY:NO_PROP_CHOSEN]	166.139.37.167	24.3.147.160	IKE
4	2009-02-02 04:51:57	The cookie pair is : 0x4C09888FC8AA9965 / 0x705259D351E2779C	166.139.37.167	24.3.147.160	IKE
5	2009-02-02 04:51:57	[SA] : No proposal chosen	24.3.147.160	166.139.37.167	IKE
6	2009-02-02 04:51:57	The cookie pair is : 0x4C09888FC8AA9965 / 0x705259D351E2779C	24.3.147.160	166.139.37.167	IKE
7	2009-02-02 04:51:57	Swap rule to rule [Remote Proxicast VPN Clients]	24.3.147.160	166.139.37.167	IKE
8	2009-02-02 04:51:57	The cookie pair is : 0x4C09888FC8AA9965 / 0x705259D351E2779C	24.3.147.160	166.139.37.167	IKE
9	2009-02-02 04:51:57	Start Phase 2: Quick Mode	24.3.147.160	166.139.37.167	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 VPN Client's Phase 2 settings.

Frequently Asked Questions

Q: Can more than 1 Proxicast VPN Client 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. You can either create 1 default rule (as in this example) or 5 specific rules, one for each remote computer (using specific VPN Client IP addresses). The LAN-Cell 2 supports 5 simultaneous VPN tunnels; the original LAN-Cell Mobile Gateway supports 2 VPN tunnels.

Q: Can the Proxicast VPN Client PC make VPN connections to more than 1 LAN-Cell at the same time?

A: Yes. Simply re-run the Configuration Wizard in the VPN Client software and enter the information for each additional LAN-Cell.

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

A: Yes. The Proxicast VPN Client software supports a fully qualified domain name (FQDN) as a remote gateway. You must first create a host and domain name using a Dynamic DNS Service (such as DynDNS.com) and configure the LAN-Cell to update the DDNS 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 using a "default rule" approach. However, the Proxicast VPN Client for Windows can act as a responder and open a tunnel initiated by a LAN-Cell if both sides have been properly configured.

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 Proxicast VPN 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.

###