Proxicast IPSec VPN Client Example

Technote LCTN3013

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 3:
LC3-52U

Document Revision History:

Date	Comments
February 2, 2009	First release
February 11, 2013	Updated for LAN-Cell 3

Note: There is a version of this TechNote for the LAN-Cell 2. See:
http://www.proxicast.com/support/files/LCTN0013%20Proxicast%20IPSec%20VPN%20Client%20Example.pdf

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 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

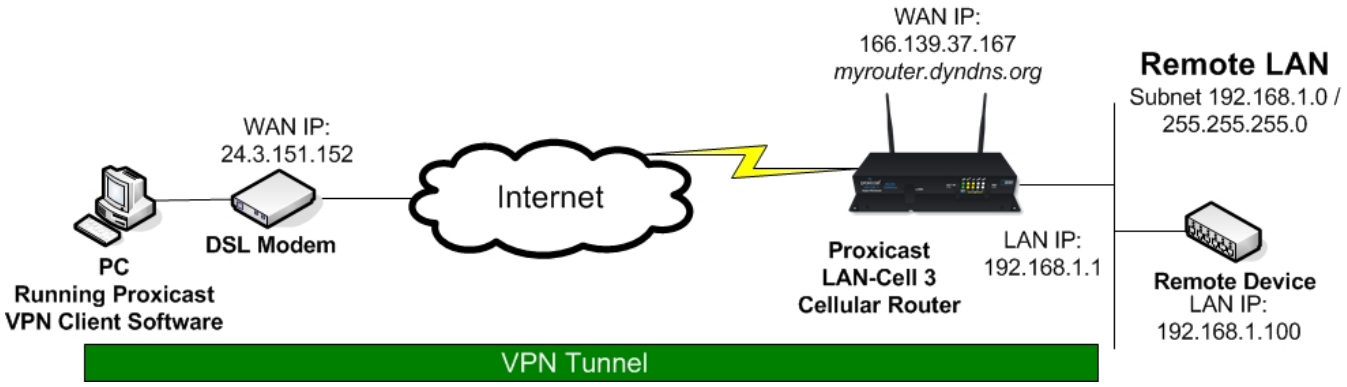

Figure 1: Example Network Topology

Usage Notes

- This example was created using the Proxicast IPSec VPN Client for Windows version 5.51.001 and LAN-Cell 3 firmware version 5.2.0.
- 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 *serial#.proxidns.com* or *myrouter.dyndns.org* (see the Setup->DDNS screen).
- The LAN-Cell's WAN connection (USB or Ethernet) must have a public IP address.
- 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 "net-to-net" tunnels that interconnect two different subnets. The LAN-Cell does support net-to-net 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 3 uses a single IPSec VPN screen to create the VPN authentication rule and network definition. To reach this screen, select **SECURITY** then **VPN** from the menu (Figure 2).

Figure 2: LAN-Cell 3 VPN / IPSec Summary Screen

Select **Enable** to activate the LAN-Cell's IPSec feature. Then click the **Add** button to open the VPN rule screen (See Figure 3).

Figure 3: LAN-Cell 3 IPSec Rule Default Screen

Begin by entering a descriptive Connection Name for this rule. This name is just for local identification purposes. The name may not contain spaces.

For the VPN Mode, select "Remote User". This will change the VPN Rule screen as shown in Figure 4.

Figure 4: Remote User IPSec Rule

Confirm that the Local External Interface matches the currently active LAN-Cell WAN. If the LAN-Cell has both a wired Ethernet and USB WAN connection, separate IPSec rules must be created for each interface.

The Local Subnet IP and Netmask fields will be automatically populated with the settings from the LAN-Cell. In general, you will not need to change these values.

Enter a Preshared Key that is at least an 8 character string. Avoid non-alphanumeric characters such as dashes, underscores, asterisks, etc. In our example, the Preshared Key is 12345678.

The remainder of the settings on this screen are the LAN-Cell defaults and do not need to be changed for our example. They match the default configuration settings in the Proxicast VPN Client.

Click **Confirm** on the rule screen to save the VPN configuration. The new rule will now be shown on the IPSec Summary on screen as shown in Figure 5.

***** Remember to click Save Settings at the bottom of the screen to save your new IPSec rule.**

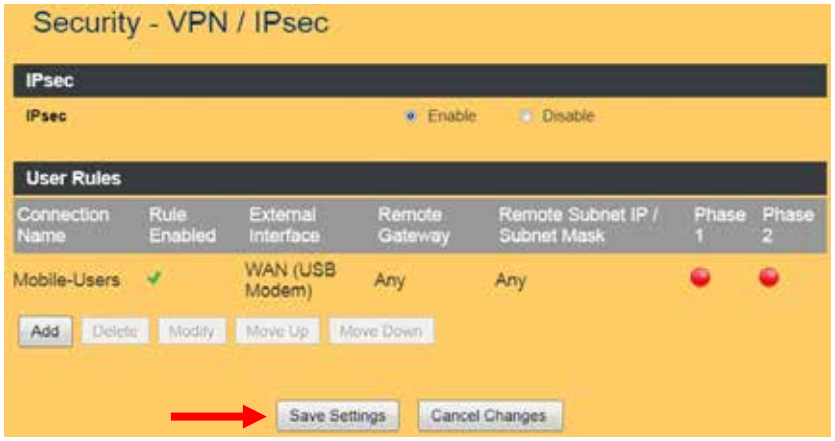

Figure 5: IPSec Rule Summary

Configuration of the LAN-Cell is now complete.

Example Proxicast VPN Client for Windows Configuration

After starting the Proxicast VPN Client software for the first time (or by selecting the Configuration->Wizard menu), the VPN Configuration Wizard is displayed (Figure 6).

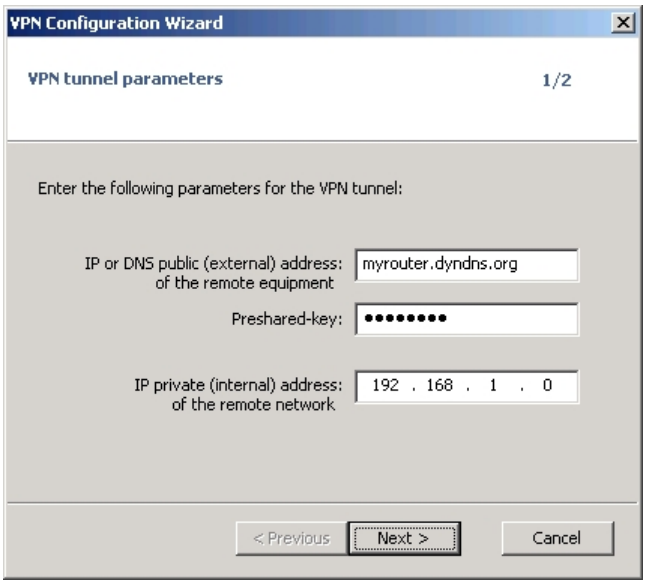

Figure 6: Proxicast VPN Client Wizard Step 1

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.

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).

Click the **NEXT** button in the Wizard to display the Configuration Summary screen (Figure 7).

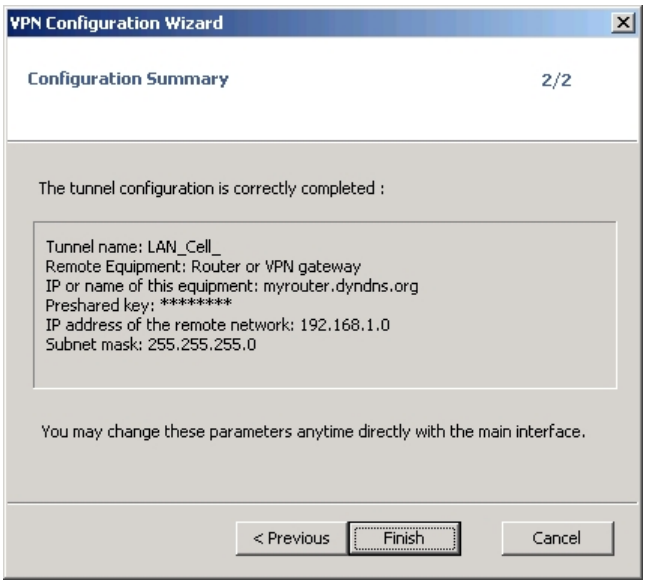

Figure 7: VPN Client Configuration Wizard Step 2

Clicking the **FINISH** button displays the Proxicast VPN Client main Configuration Panel showing the Phase 1 (LAN_Cell) and Phase 2 (Tunnel) parameter sets created by the Configuration Wizard (Figure 8).

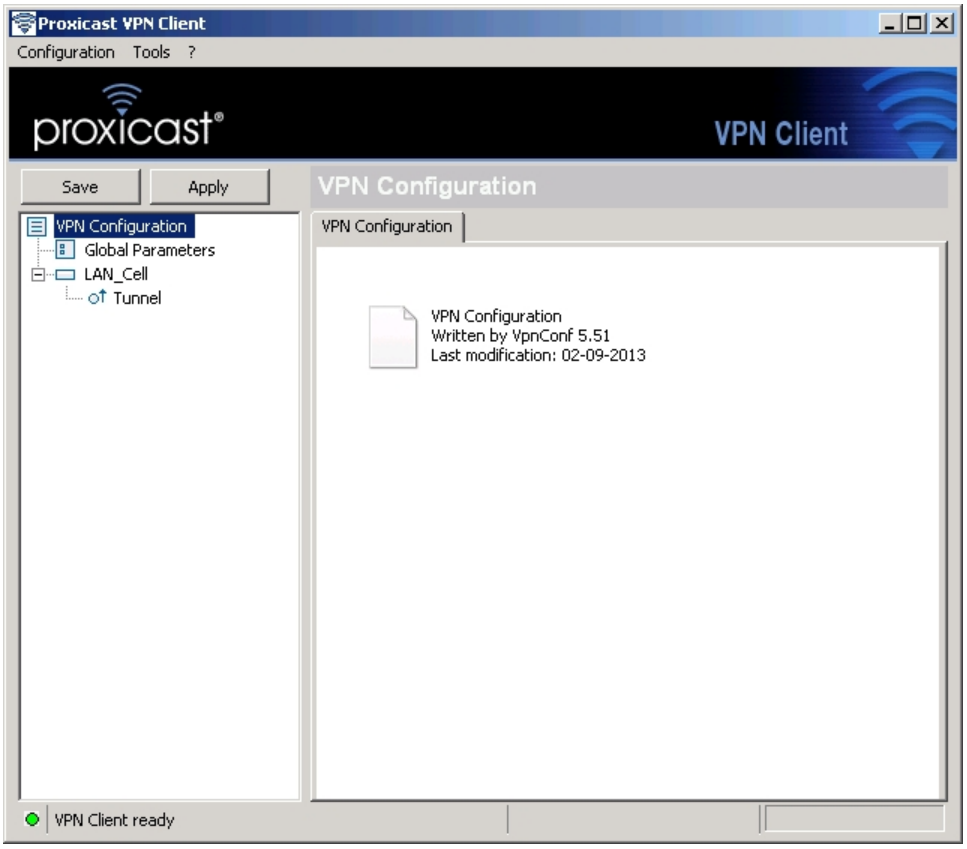

Figure 8: VPN Client Configuration Panel

You are now ready to open a VPN Tunnel to the LAN-Cell. Double-click **Tunnel** in the left pane to begin negotiating the IPSec tunnel.

You can also open a tunnel from the Windows System Tray area of the Taskbar. Right click the Proxicast VPN Client Tunnel Status Icon in the system tray and select Open Tunnel from the popup menu (Figure 9).

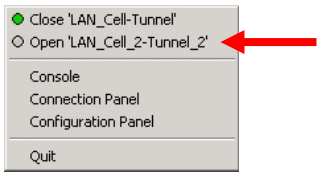

Figure 9: Opening a VPN Tunnel from the System Tray

While the tunnel is being established, you will see several status popups in the System Tray area (Figure 10).

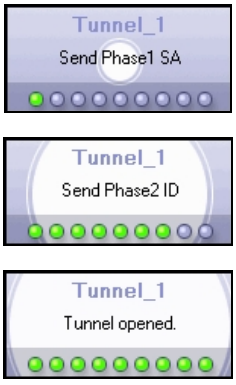

Figure 10: VPN Tunnel Progress Popups

Once the tunnel is established, the System Tray icon will turn green (Figure 11).

Figure 11: VPN Tunnel Progress Status Icons

You may also view and change the status of the tunnel using the Connections Panel (Figure 12).

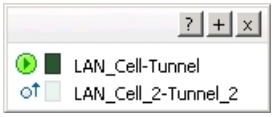

Figure 12: Connections Panel

On the LAN-Cell, you can observe the status of the tunnel on the VPN / IPSec summary screen (Figure 13).

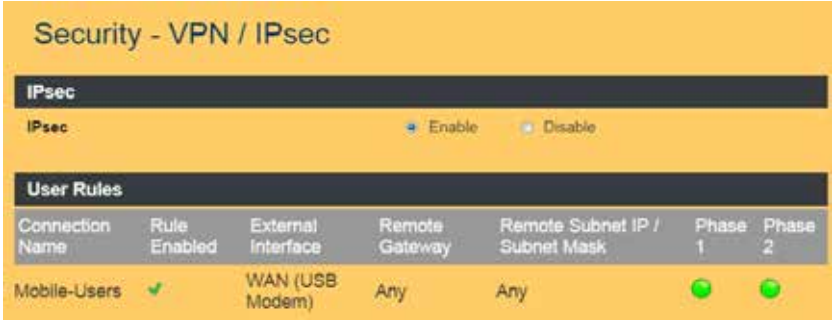

Figure 13: LAN-Cell IPSec Status Screen

Reviewing the VPN Tunnel Configuration 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 14 and 15).

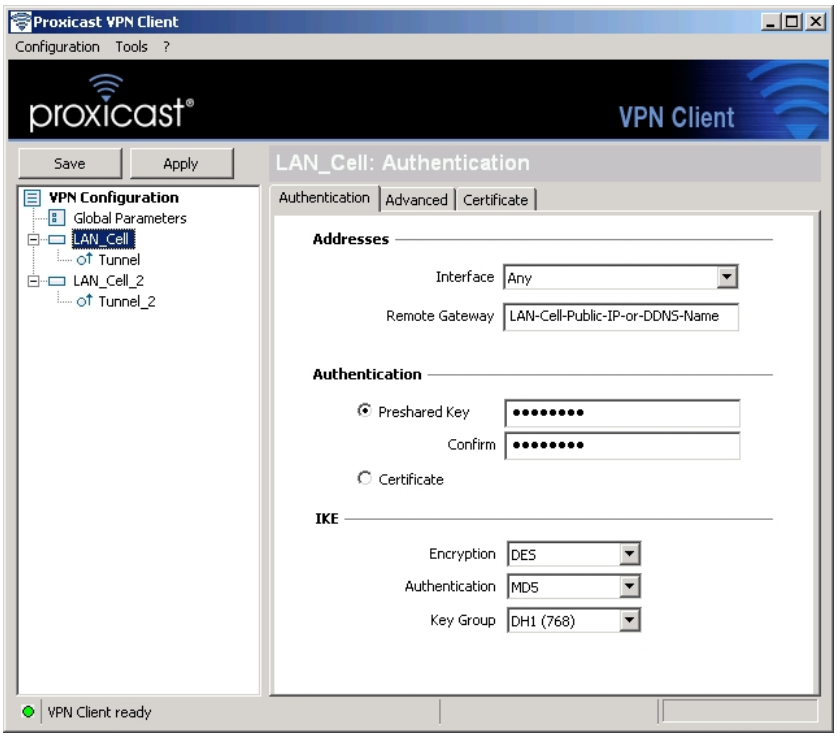

Figure 14: VPN Client Phase 1 Parameters

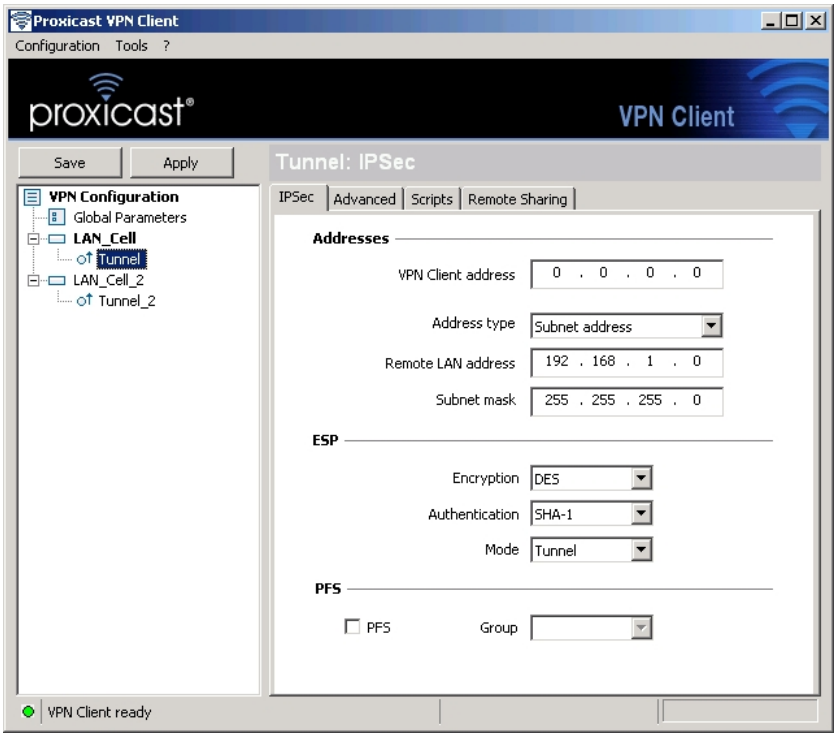

Figure 15: VPN Client Phase 2 Parameters

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 16). You can also open the **Console** window in the VPN Client prior to attempting a new tunnel connection (Figure 17).

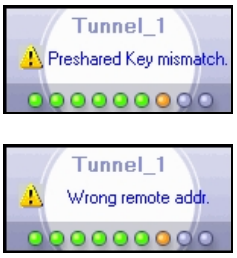

Figure 16: VPN Client Error Examples

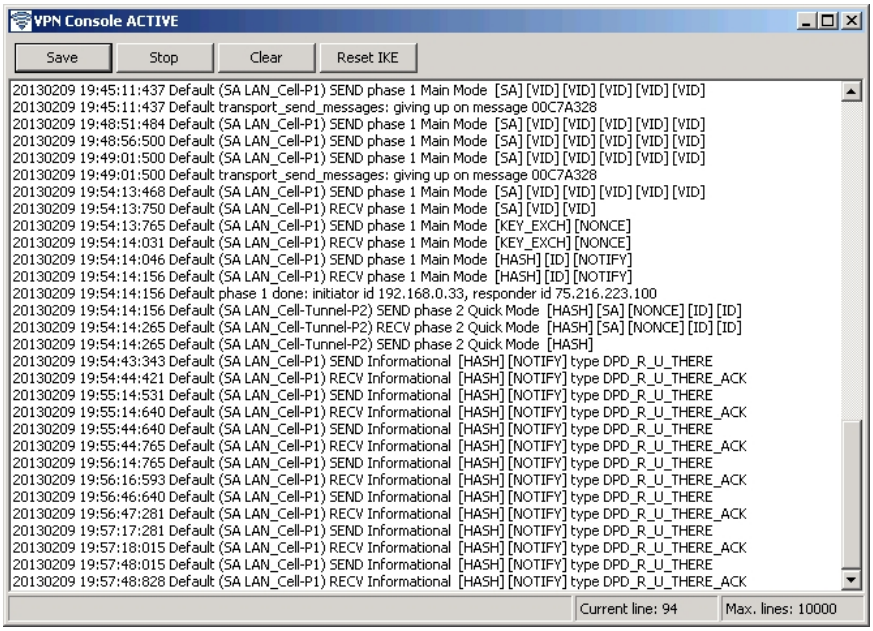

Figure 17: VPN Client Debug Console Messages

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

- Not clicking **Save or 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:

<IPSEC> Feb 10 19:02:00 Mobile-Users [4] 24.3.151.152 #4: STATE_QUICK_R2: IPsec SA established tunnel mode {ESP=>0x177bf496 <0x37ed6f8c xfrm=DES_0-HMAC_SHA1 NATOA=none NATD=24.3.151.152:19318 DPD=enabled}
<IPSEC> Feb 10 19:02:00 Mobile-Users [4] 24.3.151.152 #4: transition from state STATE_QUICK_R1 to state STATE_QUICK_R2
<IPSEC> Feb 10 19:02:00 Mobile-Users [4] 24.3.151.152 #4: Dead Peer Detection (RFC 3706): enabled
<IPSEC> Feb 10 19:02:00 Mobile-Users [4] 24.3.151.152 #4: STATE_QUICK_R1: sent QR1 inbound IPsec SA installed expecting QI2
<IPSEC> Feb 10 19:02:00 Mobile-Users [4] 24.3.151.152 #4: transition from state STATE_QUICK_R0 to state STATE_QUICK_R1
<IPSEC> Feb 10 19:02:00 Mobile-Users [4] 24.3.151.152 #4: them: 24.3.151.152[192.168.0.33 +S=C]===192.168.0.33/32
<IPSEC> Feb 10 19:02:00 Mobile-Users [4] 24.3.151.152 #4: us: 192.168.1.0/24===166.139.37.167<166.139.37.167>[+S=C]
<IPSEC> Feb 10 19:02:00 Mobile-Users [4] 24.3.151.152 #4: responding to Quick Mode proposal {msgid:0ae46eec}
<IPSEC> Feb 10 19:02:00 Mobile-Users [4] 24.3.151.152 #3: the peer proposed: 192.168.1.0/24:0/0 -> 192.168.0.33/32:0/0
<IPSEC> Feb 10 19:02:00 Mobile-Users [4] 24.3.151.152 #3: Dead Peer Detection (RFC 3706): enabled
<IPSEC> Feb 10 19:02:00 Mobile-Users [4] 24.3.151.152 #3: STATE_MAIN_R3: sent MR3 ISAKMP SA established {auth=OAKLEY_PRESHARED_KEY cipher=oakley_des_cbc_64 prf=oakley_md5 group=modp768}
<IPSEC> Feb 10 19:02:00 Mobile-Users [4] 24.3.151.152 #3: new NAT mapping for #3 was 24.3.151.152:500 now 24.3.151.152:19318
<IPSEC> Feb 10 19:02:00 Mobile-Users [4] 24.3.151.152 #3: transition from state STATE_MAIN_R2 to state STATE_MAIN_R3
<IPSEC> Feb 10 19:02:00 Mobile-Users [4] 24.3.151.152 #3: deleting connection Mobile-Users instance with peer 24.3.151.152 {isakmp=#0/ipsec=#0}
<IPSEC> Feb 10 19:02:00 Mobile-Users [3] 24.3.151.152 #3: switched from Mobile-Users to Mobile-Users
<IPSEC> Feb 10 19:02:00 Mobile-Users [3] 24.3.151.152 #3: Main mode peer ID is ID_IPV4_ADDR: 192.168.0.33
<IPSEC> Feb 10 19:02:00 Mobile-Users [3] 24.3.151.152 #3: ignoring informational payload type IPSEC_INITIAL_CONTACT msgid=00000000
<IPSEC> Feb 10 19:02:00 Mobile-Users [3] 24.3.151.152 #3: STATE_MAIN_R2: sent MR2 expecting MI3
<IPSEC> Feb 10 19:02:00 Mobile-Users [3] 24.3.151.152 #3: transition from state STATE_MAIN_R1 to state STATE_MAIN_R2
<IPSEC> Feb 10 19:02:00 Mobile-Users [3] 24.3.151.152 #3: NAT-Traversal: Result using RFC 3947 (NAT-Traversal): peer is NATed
<IPSEC> Feb 10 19:01:59 Mobile-Users [3] 24.3.151.152 #3: STATE_MAIN_R1: sent MR1 expecting MI2
<IPSEC> Feb 10 19:01:59 Mobile-Users [3] 24.3.151.152 #3: transition from state STATE_MAIN_R0 to state STATE_MAIN_R1
<IPSEC> Feb 10 19:01:59 Mobile-Users [3] 24.3.151.152 #3: responding to Main Mode from unknown peer 24.3.151.152
<IPSEC> Feb 10 19:01:59 packet from 24.3.151.152:500: received Vendor ID payload [Dead Peer Detection]
<IPSEC> Feb 10 19:01:59 packet from 24.3.151.152:500: received Vendor ID payload [RFC 3947] method set to=109
<IPSEC> Feb 10 19:01:59 packet from 24.3.151.152:500: received Vendor ID payload [draft-ietf-ipsec-nat-t-ike-03] method set to=108
<IPSEC> Feb 10 19:01:59 packet from 24.3.151.152:500: received Vendor ID payload [draft-ietf-ipsec-nat-t-ike-02_n] method set to=106
<IPSEC> Feb 10 19:01:59 packet from 24.3.151.152:500: received Vendor ID payload [draft-ietf-ipsec-nat-t-ike-00]

Phase 1 Parameter Mismatch:

<IPSEC> Feb 10 20:13:01 Mobile-Users [4] 24.3.151.152: deleting connection Mobile-Users instance with peer 24.3.151.152 {isakmp=#0/ipsec=#0}
<IPSEC> Feb 10 20:13:01 Mobile-Users #20: deleting state (STATE_MAIN_I1)
<IPSEC> Feb 10 20:13:01 Mobile-Users [4] 24.3.151.152: terminating SAs using this connection
<IPSEC> Feb 10 20:12:40 Mobile-Users [4] 24.3.151.152 #21: sending notification NO_PROPOSAL_CHOSEN to 24.3.151.152:500
<IPSEC> Feb 10 20:12:40 Mobile-Users [4] 24.3.151.152 #21: no acceptable Oakley Transform
<IPSEC> Feb 10 20:12:40 Mobile-Users [4] 24.3.151.152 #21: Oakley Transform [OAKLEY_DES_CBC (64) OAKLEY_MD5 OAKLEY_GROUP_MODP1024] refused due to insecure key_len and enc. alg. not listed in ike string
<IPSEC> Feb 10 20:12:40 Mobile-Users [4] 24.3.151.152 #21: responding to Main Mode from unknown peer 24.3.151.152
<IPSEC> Feb 10 20:12:40 packet from 24.3.151.152:500: received Vendor ID payload [Dead Peer Detection]
<IPSEC> Feb 10 20:12:40 packet from 24.3.151.152:500: received Vendor ID payload [RFC 3947] method set to=109
<IPSEC> Feb 10 20:12:40 packet from 24.3.151.152:500: received Vendor ID payload [draft-ietf-ipsec-nat-t-ike-03] method set to=108
<IPSEC> Feb 10 20:12:40 packet from 24.3.151.152:500: received Vendor ID payload [draft-ietf-ipsec-nat-t-ike-02_n] method set to=106
<IPSEC> Feb 10 20:12:40 packet from 24.3.151.152:500: received Vendor ID payload [draft-ietf-ipsec-nat-t-ike-00]
<IPSEC> Feb 10 20:12:40 Mobile-Users [4] 24.3.151.152 #20: initiating Main Mode
<IPSEC> Feb 10 20:12:40 Mobile-Users [4] 24.3.151.152 #19: starting keying attempt 14 of an unlimited number
<IPSEC> Feb 10 20:12:40 Mobile-Users [4] 24.3.151.152 #19: max number of retransmissions (2) reached STATE_QUICK_I1. No acceptable response to our first Quick Mode message: perhaps peer likes no proposal

<IPSEC> Feb 10 20:12:12 packet from 24.3.151.152:19318: received and ignored informational message
<IPSEC> Feb 10 20:12:12 Mobile-Users [4] 24.3.151.152 #5: received Delete SA payload: deleting ISAKMP State #5
<IPSEC> Feb 10 20:12:12 Mobile-Users [4] 24.3.151.152 #5: received and ignored informational message
<IPSEC> Feb 10 20:12:12 Mobile-Users [4] 24.3.151.152 #5: received Delete SA(0x89c07690) payload: deleting IPSEC State #7

Compare the Phase 1 parameters on both the LAN-Cell 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:

<IPSEC> Feb 10 20:48:37 Mobile-Users #24: deleting state (STATE_MAIN_R3)
<IPSEC> Feb 10 20:48:37 Mobile-Users [8] 24.3.151.152 #24: deleting connection Mobile-Users instance with peer 24.3.151.152 {isakmp=#24/ipsec=#0}
<IPSEC> Feb 10 20:48:37 Mobile-Users [8] 24.3.151.152 #24: DPD: Restarting Connection
<IPSEC> Feb 10 20:48:37 Mobile-Users [8] 24.3.151.152 #24: DPD: No response from peer - declaring peer dead<IPSEC> Feb 10 20:47:27 Mobile-Users [8] 24.3.151.152 #24: Dead Peer Detection (RFC 3706): enabled
<IPSEC> Feb 10 20:47:27 Mobile-Users [8] 24.3.151.152 #24: STATE_MAIN_R3: sent MR3 ISAKMP SA established {auth=OAKLEY_PRESHARED_KEY cipher=oakley_des_cbc_64 prf=oakley_md5 group=modp768}
<IPSEC> Feb 10 20:47:27 Mobile-Users [8] 24.3.151.152 #24: new NAT mapping for #24 was 24.3.151.152:500 now 24.3.151.152:21229
<IPSEC> Feb 10 20:47:27 Mobile-Users [8] 24.3.151.152 #24: transition from state STATE_MAIN_R2 to state STATE_MAIN_R3
<IPSEC> Feb 10 20:47:27 Mobile-Users [8] 24.3.151.152 #24: deleting connection Mobile-Users instance with peer 24.3.151.152 {isakmp=#0/ipsec=#0}
<IPSEC> Feb 10 20:47:27 Mobile-Users [7] 24.3.151.152 #24: switched from Mobile-Users to Mobile-Users
<IPSEC> Feb 10 20:47:27 Mobile-Users [7] 24.3.151.152 #24: Main mode peer ID is ID_USER_FQDN: user@test.com
<IPSEC> Feb 10 20:47:27 Mobile-Users [7] 24.3.151.152 #24: ignoring informational payload type IPSEC_INITIAL_CONTACT msgid=00000000
<IPSEC> Feb 10 20:47:27 Mobile-Users [7] 24.3.151.152 #24: STATE_MAIN_R2: sent MR2 expecting MI3
<IPSEC> Feb 10 20:47:27 Mobile-Users [7] 24.3.151.152 #24: transition from state STATE_MAIN_R1 to state STATE_MAIN_R2
<IPSEC> Feb 10 20:47:27 Mobile-Users [7] 24.3.151.152 #24: NAT-Traversal: Result using RFC 3947 (NAT-Traversal): peer is NATed
<IPSEC> Feb 10 20:47:26 Mobile-Users [7] 24.3.151.152 #24: STATE_MAIN_R1: sent MR1 expecting MI2
<IPSEC> Feb 10 20:47:26 Mobile-Users [7] 24.3.151.152 #24: transition from state STATE_MAIN_R0 to state STATE_MAIN_R1
<IPSEC> Feb 10 20:47:26 Mobile-Users [7] 24.3.151.152 #24: responding to Main Mode from unknown peer 24.3.151.152
<IPSEC> Feb 10 20:47:26 packet from 24.3.151.152:500: received Vendor ID payload [Dead Peer Detection]
<IPSEC> Feb 10 20:47:26 packet from 24.3.151.152:500: received Vendor ID payload [RFC 3947] method set to=109
<IPSEC> Feb 10 20:47:26 packet from 24.3.151.152:500: received Vendor ID payload [draft-ietf-ipsec-nat-t-ike-03] method set to=108
<IPSEC> Feb 10 20:47:26 packet from 24.3.151.152:500: received Vendor ID payload [draft-ietf-ipsec-nat-t-ike-02_n] method set to=106
<IPSEC> Feb 10 20:47:26 packet from 24.3.151.152:500: received Vendor ID payload [draft-ietf-ipsec-nat-t-ike-00]

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:

<IPSEC> Feb 10 20:56:24 packet from 24.3.151.152:21229: received and ignored informational message
<IPSEC> Feb 10 20:56:24 packet from 24.3.151.152:21229: ignoring informational payload type INVALID_COOKIE on st==NULL (deleted?)
<IPSEC> Feb 10 20:56:23 packet from 24.3.151.152:21229: received and ignored informational message
<IPSEC> Feb 10 20:56:23 Mobile-Users [8] 24.3.151.152: deleting connection Mobile-Users instance with peer 24.3.151.152 {isakmp=#0/ipsec=#0}
<IPSEC> Feb 10 20:56:23 Mobile-Users [8] 24.3.151.152 #7: received Delete SA payload: deleting ISAKMP State #7
<IPSEC> Feb 10 20:56:22 Mobile-Users [8] 24.3.151.152 #8: sending encrypted notification NO_PROPOSAL_CHOSEN to 24.3.151.152:21229
<IPSEC> Feb 10 20:56:22 Mobile-Users [8] 24.3.151.152 #8: no acceptable Proposal in IPsec SA
<IPSEC> Feb 10 20:56:22 Mobile-Users [8] 24.3.151.152 #8: IPsec Transform [ESP_DES (64) AUTH_ALGORITHM_HMAC_MD5] refused due to insecure key_len and enc. alg. not listed in esp string
<IPSEC> Feb 10 20:56:22 Mobile-Users [8] 24.3.151.152 #7: the peer proposed: 192.168.1.0/24:0/0 -> 192.168.0.33/32:0/0
<IPSEC> Feb 10 20:56:22 Mobile-Users [8] 24.3.151.152 #7: Dead Peer Detection (RFC 3706): enabled
<IPSEC> Feb 10 20:56:22 Mobile-Users [8] 24.3.151.152 #7: STATE_MAIN_R3: sent MR3 ISAKMP SA established {auth=OAKLEY_PRESHARED_KEY cipher=oakley_des_cbc_64 prf=oakley_md5 group=modp768}

<IPSEC> Feb 10 20:56:22 Mobile-Users [8] 24.3.151.152 #7: new NAT mapping for #7 was 24.3.151.152:500 now 24.3.151.152:21229
<IPSEC> Feb 10 20:56:22 Mobile-Users [8] 24.3.151.152 #7: transition from state STATE_MAIN_R2 to state STATE_MAIN_R3
<IPSEC> Feb 10 20:56:22 Mobile-Users [8] 24.3.151.152 #7: deleting connection Mobile-Users instance with peer 24.3.151.152 {isakmp=#0/ipsec=#0}
<IPSEC> Feb 10 20:56:22 Mobile-Users [7] 24.3.151.152 #7: switched from Mobile-Users to Mobile-Users
<IPSEC> Feb 10 20:56:22 Mobile-Users [7] 24.3.151.152 #7: Main mode peer ID is ID_IPV4_ADDR: 192.168.0.33
<IPSEC> Feb 10 20:56:22 Mobile-Users [7] 24.3.151.152 #7: ignoring informational payload type IPSEC_INITIAL_CONTACT msgid=00000000
<IPSEC> Feb 10 20:56:22 Mobile-Users [7] 24.3.151.152 #7: STATE_MAIN_R2: sent MR2 expecting MI3
<IPSEC> Feb 10 20:56:22 Mobile-Users [7] 24.3.151.152 #7: transition from state STATE_MAIN_R1 to state STATE_MAIN_R2
<IPSEC> Feb 10 20:56:22 Mobile-Users [7] 24.3.151.152 #7: NAT-Traversal: Result using RFC 3947 (NAT-Traversal): peer is NATed
<IPSEC> Feb 10 20:56:22 Mobile-Users [7] 24.3.151.152 #7: STATE_MAIN_R1: sent MR1 expecting MI2
<IPSEC> Feb 10 20:56:22 Mobile-Users [7] 24.3.151.152 #7: transition from state STATE_MAIN_R0 to state STATE_MAIN_R1
<IPSEC> Feb 10 20:56:22 Mobile-Users [7] 24.3.151.152 #7: responding to Main Mode from unknown peer 24.3.151.152
<IPSEC> Feb 10 20:56:22 packet from 24.3.151.152:500: received Vendor ID payload [Dead Peer Detection]
<IPSEC> Feb 10 20:56:22 packet from 24.3.151.152:500: received Vendor ID payload [RFC 3947] method set to=109
<IPSEC> Feb 10 20:56:22 packet from 24.3.151.152:500: received Vendor ID payload [draft-ietf-ipsec-nat-t-ike-03] method set to=108
<IPSEC> Feb 10 20:56:22 packet from 24.3.151.152:500: received Vendor ID payload [draft-ietf-ipsec-nat-t-ike-02_n] method set to=106
<IPSEC> Feb 10 20:56:22 packet from 24.3.151.152:500: received Vendor ID payload [draft-ietf-ipsec-nat-t-ike-00]

Similar to a Phase 1 proposal error, this indicates that the Phase 2 parameters do not match. Check the LAN-Cell's VPN 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 25 simultaneous clients to establish VPN tunnels with the LAN-Cell at the same time. You can either create 1 default rule (as in this example) or 25 specific rules, one for each remote computer (using specific VPN Client IP addresses). The LAN-Cell supports 25 simultaneous 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. There is no limit to the number tunnels that can be defined.

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 use the LAN-Cell's permanent DDNS name (serial#.proxidns.com) or 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 **SETUP->DDNS** screen in the LAN-Cell 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 net-to-net 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.

# # #