



LAN-Cell VPN Planner

Tech Note LCTN0002

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 Tech Note applies to LAN-Cell models:

LAN-Cell 2:

LC2-411

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
Februaru 6, 2009	Fixed typographical errors. Added reference to Proxicast VPN Client.
July 14, 2008	First release

Introduction

Configuring an IPSec VPN connection between two devices from different manufacturers can be challenging since manufacturers sometimes use different descriptions for the same parameters. Also, the user must gather a large number of network address and security related parameters in order to complete the configuration. In some instances, it may not be possible or expedient to change the configuration of one VPN end device, necessitating that the other device be configured to match some pre-existing parameters.

The LAN-Cell contains IPSec VPN client and server functionality and is interoperable with most other IPSec VPN equipment and software.

The LAN-Cell can establish “site-to-site” VPN tunnels with other VPN hardware devices; it also supports “client-to-site” tunnels from single remote PC’s running VPN client software. This TechNote includes worksheets for the site-to-site type of VPN setup. See the Proxicast Support website for examples of configuring client-to-site VPN tunnels using the LAN-Cell as the VPN server with VPN client software such as the Proxicast IPSec VPN Client for Microsoft Windows. The LAN-Cell can also be a single-point client to a remote VPN, but this configuration is not common and is not included in the examples.

This TechNote is designed to help you gather the information necessary to configure a virtual private network between your LAN-Cell and your existing VPN equipment. Included are complete VPN example configurations, LAN-Cell VPN default values along with blank worksheets for you to record your specific settings. Use the worksheets in this document to plan your VPN deployment before beginning to make changes to either VPN device.

Getting Started

Some key points to remember when configuring your VPN:

- In general, all VPN parameters much match EXACTLY between the 2 devices.
- It is helpful to can have simultaneous access to the to parameter and log screens of both devices during setup and testing.
- The network on the LAN side of the LAN-Cell and on the “private” side of your other VPN equipment must be on different subnets.
- Most users find it easiest to configure VPNs if both end-points have static public IP addresses. Contact your ISP or cellular network operator to determine if static IP addresses are available. Otherwise, you will need to define a Dynamic DNS hostname for your VPN equipment that has a dynamic IP address.
- The LAN-Cell can be either the VPN initiator or responder for site-to-site VPNs. It is the responder for client-to-site VPNs.
- Ensure that your VPN device is configured for IPSec VPN tunnels and not PPTP, L2TP, or GRE as these are not supported by the LAN-Cell at this time (you can implement these tunneling protocols on a device “behind” the LAN-Cell and configure the LAN-Cell to support “pass-through” tunneling).

Please see the *LAN-Cell User’s Guide* or more detailed information on the VPN parameters and configuration. Also see the Proxicast Support website (<http://www.proxicast.com/support>) for additional VPN information and configuration examples.

Site-to-Site VPNs

Site-to-Site VPNs are probably the most common way to set up a secure connection to a remote site. The IPSec tunnel will be established between the LAN-Cell and a corresponding VPN router/firewall/concentrator on your “headquarters” network (e.g. Cisco PIX/ASA, SonicWall, CheckPoint, etc.).

A site-to-site VPN tunnel results in the “private” subnets behind each VPN device being able to communicate with each other directly and securely as if they were on the same physical network.

Figure 1 shows the IP addressing for our example site-to-site VPN configuration. Note that the remote site (LAN-Cell) has both a static IP address as well as a dynamic DNS name defined. Some VPN devices can establish connections to dynamic DNS devices; others must use static IP addresses. The LAN-Cell supports Dynamic DNS hostnames for its own WAN IP address as well as its peer VPN gateway.

Figure 2 is for you to record the network addresses of the key nodes in your VPN network.

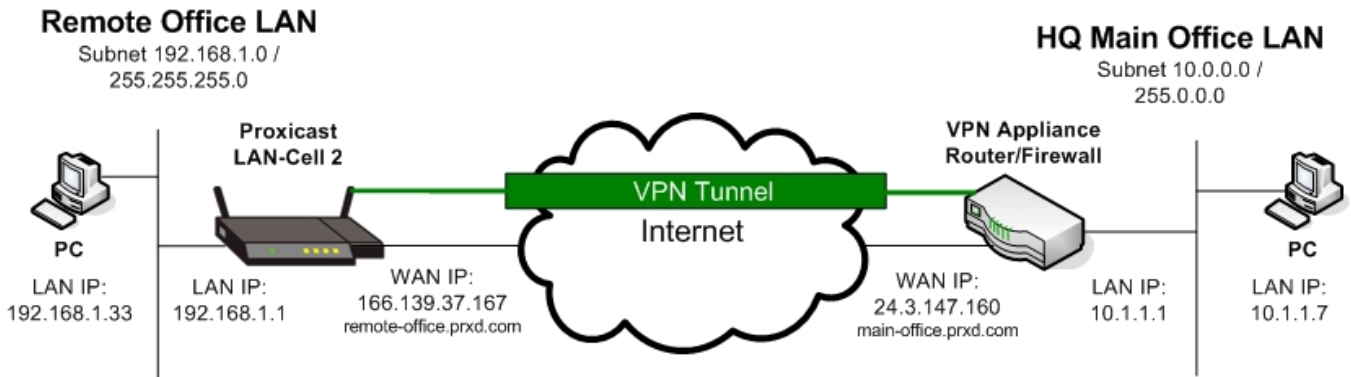


Figure 1: Example Site-to-Site VPN Network Topology

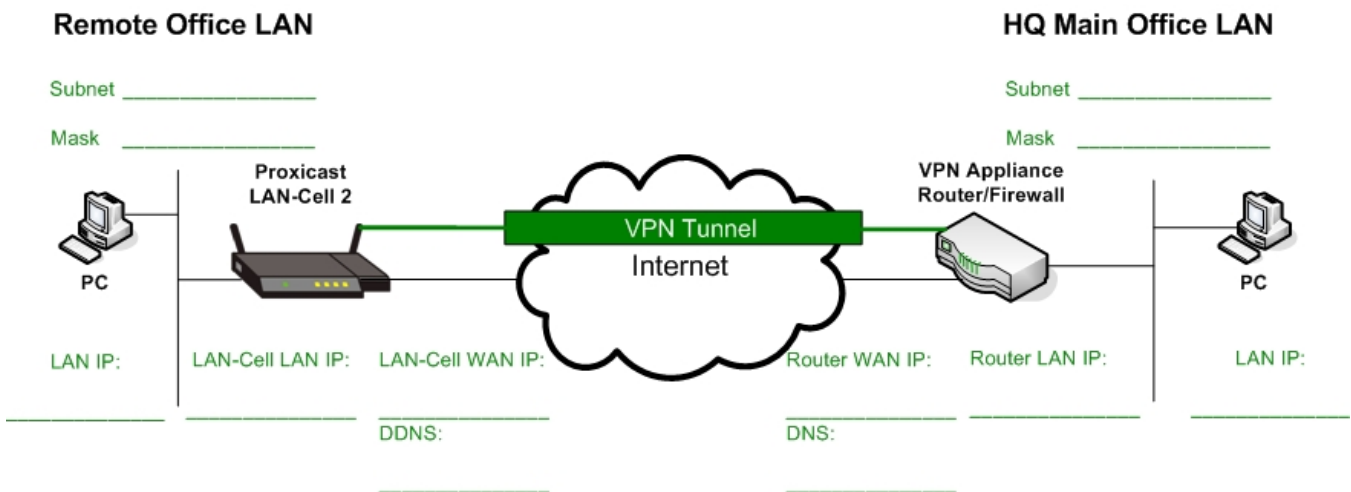


Figure 2: Your Site-to-Site VPN Network Topology

Site-to-Site VPN Parameters

The LAN-Cell's VPN parameters are divided into *Gateway Policy* and *Network Policy* components.

The Gateway Policy (IKE) parameters define how the LAN-Cell and the other VPN device should contact each other over the Internet and the security parameters required for them to establish trusted communications.

Network Policy (IPsec) parameters define which LAN devices are allowed to communicate through the VPN, how each VPN device should integrate the other's private subnet into their routing tables and how communications are to be secured.

The next 2 pages contain worksheets for both the Gateway and Network Policy parameters. Each parameter is shown with its default value, along with the value used in our example site-to-site VPN. Space is also provided for you to record the settings appropriate for your VPN configuration. We recommend that you complete these worksheets before beginning your VPN configuration setup.

Table 1 summarizes the Gateway Policy parameters which must be defined first when creating a new VPN connection with the LAN-Cell. The LAN-Cell 2 supports a number of advanced options such as High Availability (fail-over) tunneling, X.509 PKI certificates and multiple IKE proposals. These have been omitted in the interest of simplicity for this example. This example also assumes that IKE is used rather than manual key exchange.

Table 2 summarizes the Network Policy parameters. Each Gateway Policy can have one or more associated Network Policies and Network Policies can be moved between Gateway Policies if necessary.

Please refer to the notes following each table for additional information on each VPN parameter.

Table 1: Site-to-Site Gateway Policy (IKE) Parameters

#	Parameter	LAN-Cell Default Value	Example LAN-Cell Value	Example HQ VPN Value	Your LAN-Cell	Your HQ VPN
1	Gateway Policy Name	{blank}	Main Office Gateway	N/A		N/A
2	NAT Traversal	Off	Off	Off		
3	My Address	0.0.0.0	166.139.37.167	24.3.147.160		
4	Primary Remote GW	0.0.0.0	24.3.147.160	166.139.37.167		
5	Pre-Shared Key	{blank}	12345678	12345678		
6	Local ID Type	IP	IP	IP		
7	Local ID Content	0.0.0.0	192.168.1.1	10.1.1.1		
8	Peer ID Type	IP	IP	IP		
9	Peer ID Content	0.0.0.0	10.1.1.1	192.168.1.1		
10	Extended Authentication (XAUTH)	Off	Off	Off		
11	Negotiation Mode	Main	Main	Main		
12	Encryption Algorithm	DES	DES	DES		
13	Authentication Algorithm	MD5	MD5	MD5		
14	SA Lifetime	28800	28800	28800		
15	Key Group	DH1 (768)	DH1	DH1		

Table 1 Notes:

- Gateway Policy Name is required.
- NAT Traversal may be necessary if your HQ VPN device is behind a NAT'ing router.
- If My Address is left at 0.0.0.0, the LAN-Cell inserts the current WAN IP address. Use this for dynamic IP situations where you do not have a DDNS name defined, otherwise, select one of the DDNS names you have previously defined in the LAN-Cell for your dynamic IP interface.
- This is the public WAN IP address of your HQ VPN device (or its FQDN).
- Key values must be 8 to 31 case-sensitive ASCII characters or from 16 to 62 hexadecimal ("0-9", "A-F" prefixed by "0x") characters and match exactly on both devices.
- through 9. The ID type can be IP address, domain name, or e-mail address, and the ID content is a specific IP address, domain name, or e-mail address. The ID content is only used for identification; the IP address, domain name, or e-mail address that you enter does not have to actually exist. The LAN-Cell automatically uses the IP address in the My LAN-Cell field if you configure the local Content field to 0.0.0.0 or leave it blank. Local ID type and content refers to the ID type and content that applies to the LAN-Cell itself, and peer ID type and content refers to the other router in the IKE SA. Note: The LAN-Cell's local and peer ID type and ID content must match the remote IPsec router's peer and local ID type and ID content, respectively. IP type is sometimes known as "address matching".
- XAUTH implementations vary by vendor. We suggest setting up your initial VPN without XAUTH to ensure that all other parameters are correct.
- Main mode provides more security; Aggressive mode results in faster tunnel setup.
- DES (56 bit), 3DES (168 bit) and AES (128 bit) are supported. The LAN-Cell and the remote IPsec router must use the same algorithms and keys. Longer keys increase latency and decrease throughput.
- SHA1 is generally considered stronger than MD5, but it is also slower.
- Length of time before an IKE SA automatically renegotiates ranging from 180 to 3,000,000 seconds (almost 35 days). Short SA Lifetimes increase security by forcing the two VPN gateways to update keys. However, every time the VPN tunnel renegotiates, all users accessing remote resources are temporarily disconnected.
- Diffie-Hellman DH1 = 768 bits; DH2 = 1024 bits.

Table 2: Site-to-Site Network Policy (IPSec) Parameters

#	Parameter	LAN-Cell Default Value	Example LAN-Cell Value	Example HQ VPN Value	Your LAN-Cell	Your HQ VPN
1	Active	No	Yes	Yes		
2	Name	{blank}	Main Office LAN	N/A		N/A
3	Protocol	0	0	0		
4	Nailed Up	No	No	No		
5	Allow NetBIOS	No	No	No		
6	Check IPsec Connectivity	No	No	No		
7	Gateway Policy	{current}	To Main Office	N/A		N/A
8	Local Address Type	{Single}	Subnet	Subnet		
9	Local Start IP	0.0.0.0	192.198.1.0	10.0.0.0		
10	Local End IP / Mask	0.0.0.0	255.255.255.0	255.0.0.0		
11	Remote Address Type	{Single}	Subnet	Subnet		
12	Remote Start IP	0.0.0.0	10.0.0.0	192.168.1.0		
13	Remote End IP / Mask	0.0.0.0	255.0.0.0	255.255.255.0		
14	Encapsulation Mode	Tunnel	Tunnel	Tunnel		
15	Active Protocol	ESP	ESP	ESP		
16	Encryption Algorithm	DES	DES	DES		
17	Authentication Algorithm	SHA1	SHA1	SHA1		
18	SA Lifetime	28800	28800	28800		
19	Perfect Forward Secrecy	None	None	None		
20	Enable Replay Detection	No	No	No		
21	Enable Multiple Protocols	No	No	No		

Table 2 Notes:

1. If the Active check box is selected, packets destined for the HQ LAN trigger the LAN-Cell to build the tunnel. The tunnel does not come up automatically until a matching packet is received or Nailed Up is selected.
2. Network Policy Name is required.
3. 0 signifies that any protocol is permitted through the tunnel.
4. Turn on Nailed Up to have the LAN-Cell automatically reinitiate the SA after the SA lifetime times out, even if there is no traffic. The LAN-Cell also reinitiates the SA when it restarts. The LAN-Cell also rebuilds the tunnel if it was disconnected due to the output or input idle timer expiring. This option keeps the tunnel up at all times.
5. If checked, allows NetBIOS traffic to pass through the tunnel.
6. Check this box and configure an IP address in the Ping this Address field to have the LAN-Cell test the VPN tunnel to the remote IPSec router every minute. The LAN-Cell starts the IPSec connection idle timeout timer when it sends the ping packet. If there is no traffic from the remote IPSec router by the time the timeout period expires (default is 2 minutes), the LAN-Cell disconnects the VPN tunnel. Also known as "dead peer detection".
7. Gateway Policy to which this Network Policy is bound.
8. through 13. Specify the IP addresses of the devices behind each VPN device that can use the VPN tunnel. The local IP addresses must correspond to the remote IPSec router's configured remote IP addresses. If "subnet" is selected as the type, be sure to specify a subnet address rather than a specific IP address; for example to specify the entire class-C subnet, specify 192.168.1.0 / 255.255.255.0 as the local subnet and mask.
14. Select Tunnel or Transport.
15. Select ESP or AH.
16. DES (56 bit), 3DES (168 bit) and AES (128 bit) are supported. The LAN-Cell and the remote IPSec router must use the same algorithms and keys. Longer keys increase latency and decrease throughput.

17. SHA1 is generally considered stronger than MD5, but it is also slower.
18. Length of time before an IKE SA automatically renegotiates ranging from 180 to 3,000,000 seconds (almost 35 days). Short SA Lifetimes increase security by forcing the two VPN gateways to update keys. However, every time the VPN tunnel renegotiates, all users accessing remote resources are temporarily disconnected.
19. PFS changes the root key that is used to generate encryption keys for each IPsec SA. It is more secure but takes more time. Diffie-Hellman DH1 = 768 bits; DH2 = 1024 bits.
20. Select to enable replay attack detection (denial of service).
21. Select to allow the LAN-Cell to use any of its phase 2 encryption and authentication algorithms when negotiating an IPsec SA. When you enable multiple proposals, the LAN-Cell allows the remote IPsec router to select which Phase 2 encryption and authentication algorithms to use for the IPsec SA, even if they are less secure than the ones you configured for the VPN rule.

Configuring the LAN-Cell VPN Parameters

The LAN-Cell 2 offers two ways to create a set of Gateway and Network Policies which define a VPN Rule. The **VPN Wizard** can handle basic site-to-site tunnels with pre-shared keys. You can also directly create the Gateway and Network Policies using the **VPN Config** screens which are used to edit existing VPN Rules.

VPN Wizard

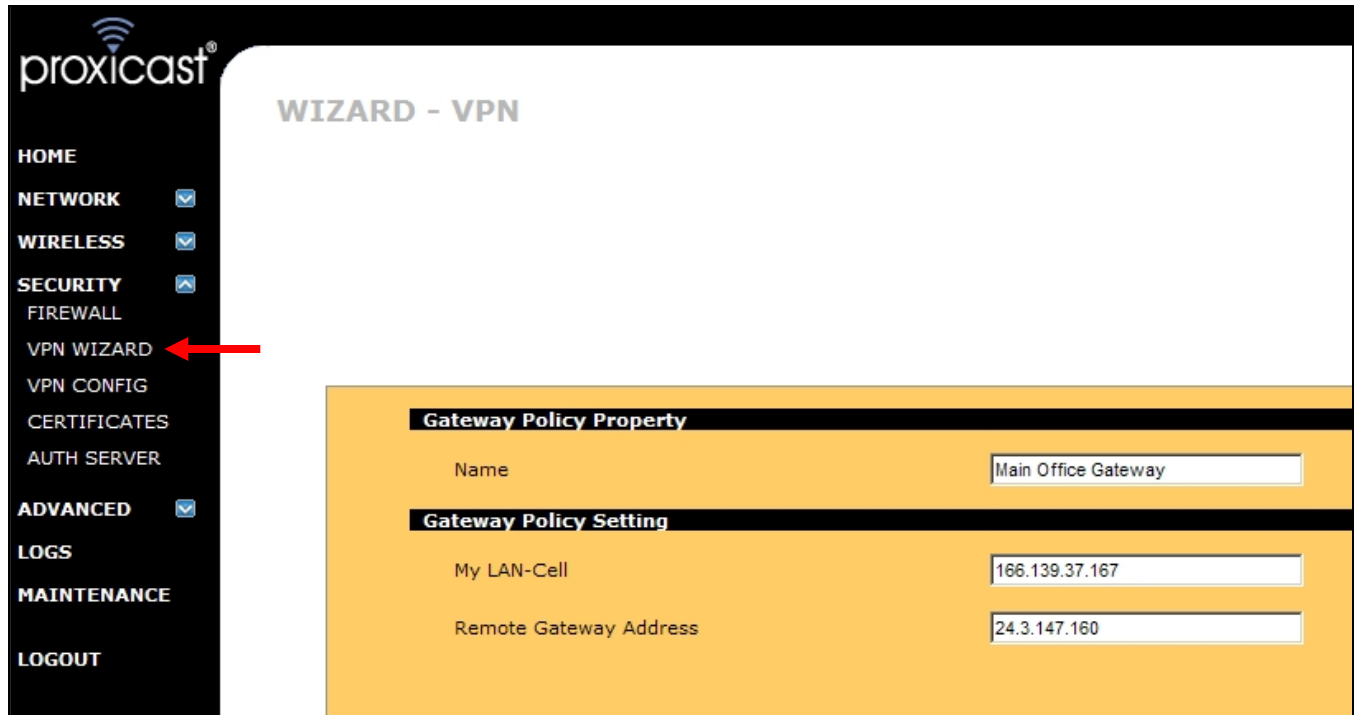


Figure 3: Starting the VPN Wizard & Gateway Policy Parameters

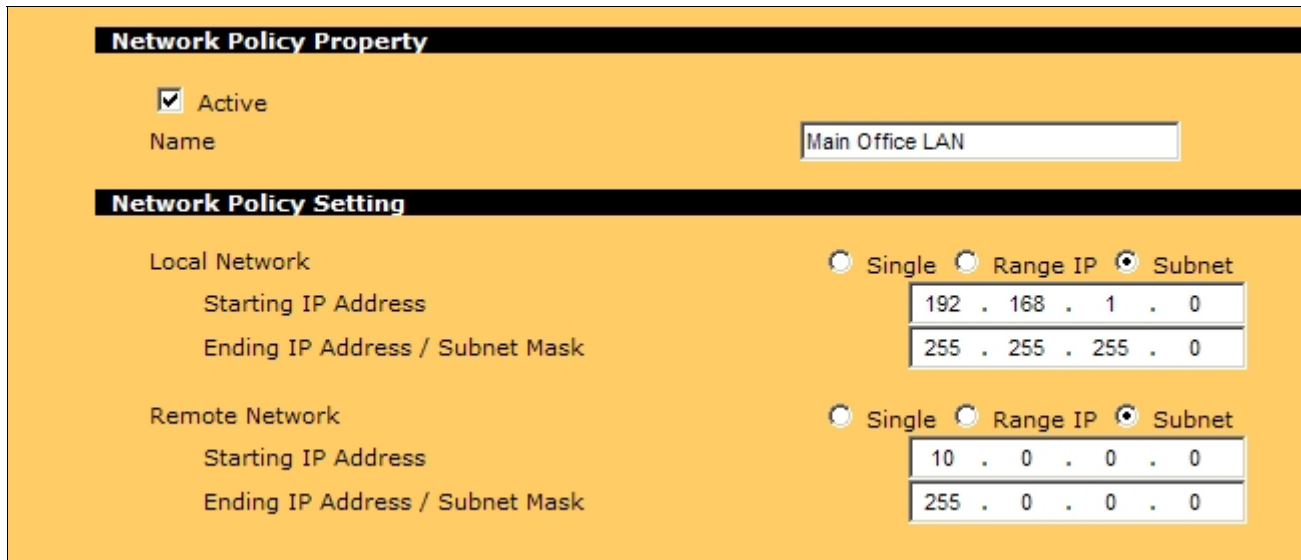


Figure 4: VPN Wizard Network Policy Parameters

IKE Tunnel Setting (IKE Phase 1)	
Negotiation Mode	<input checked="" type="radio"/> Main Mode <input type="radio"/> Aggressive Mode
Encryption Algorithm	<input checked="" type="radio"/> DES <input type="radio"/> AES <input type="radio"/> 3DES
Authentication Algorithm	<input type="radio"/> SHA1 <input checked="" type="radio"/> MD5
Key Group	<input checked="" type="radio"/> DH1 <input type="radio"/> DH2
SA Life Time	<input type="text" value="28800"/> (Seconds)
Pre-Shared Key	<input type="text" value="12345678"/>


Figure 5: VPN Wizard IKE Parameters

Status	
Gateway Policy Property Name	Main Office Gateway
Gateway Policy Setting My LAN-Cell Remote Gateway Address	166.139.37.167 24.3.147.160
Network Policy Property Active Name	Yes Main Office LAN
Network Policy Setting Local Network Starting IP Address Subnet Mask Remote Network Starting IP Address Subnet Mask	192.168.1.0 255.255.255.0 10.0.0.0 255.0.0.0
IKE Tunnel Setting (IKE Phase 1) Authentication For Activating VPN Authenticated By User Name Password Negotiation Mode Encryption Algorithm Authentication Algorithm Key Group SA Life Time Pre-Shared Key	Main Mode DES MD5 DH1 28800 (Seconds) 12345678
IPSec Setting (IKE Phase 2) Encapsulation Mode IPSec Protocol Encryption Algorithm Authentication Algorithm SA Life Time Perfect Forward Secrecy (PFS)	Tunnel Mode ESP DES SHA1 28800 (Seconds) None

Figure 6: VPN Wizard Parameter Summary

Note: The VPN Wizard sets the Local & Remote ID Type to IP Address and the ID Content to 0.0.0.0. You may need to modify this if your HQ VPN device does not support this ID scheme.

VPN Config Screens

You can edit the policies created by the VPN Wizard or enter them directly from the VPN Config screen. Click the **Add Gateway Policy** icon () to begin.

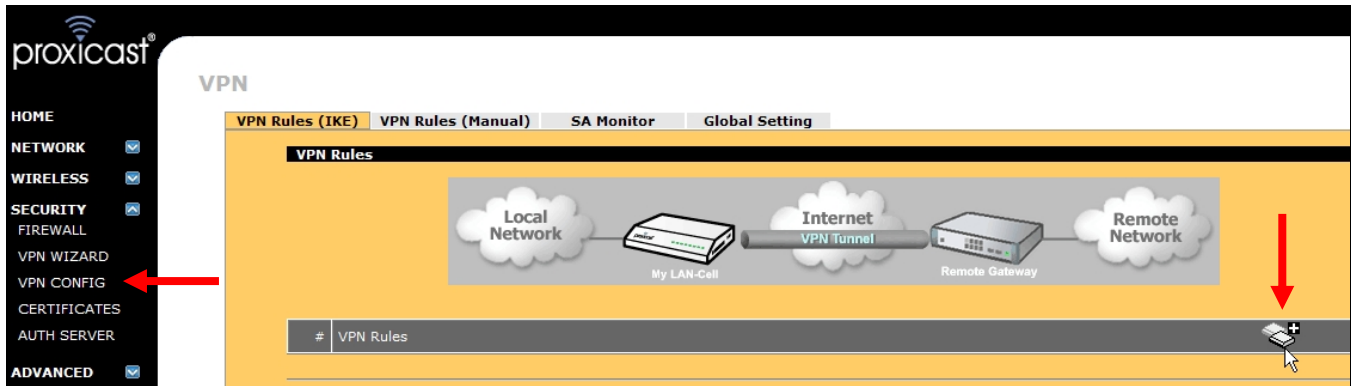


Figure 7: Adding a VPN Gateway Policy


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:

Figure 8: Gateway Policy Parameters

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

Figure 9: IKE Parameters

After saving the Gateway Policy, you are returned to the VPN Rules Summary page. Click the **Add Network Policy** icon (⚙️) to define your Network Policy.

VPN

VPN Rules (IKE)
VPN Rules (Manual)
SA Monitor
Global Setting

VPN Rules

#	VPN Rules					
1	Main Office Gateway	166.139.37.167	mobile.prxd.com			

Figure 10: Adding a VPN Network Policy

VPN - NETWORK POLICY - EDIT

Property

Active
 Name:
 Protocol:
 Nailed-Up
 Allow NetBIOS broadcast Traffic Through IPSec Tunnel
 Check IPSec Tunnel Connectivity Log
 Ping this Address:

Gateway Policy Information

Gateway Policy:

Local Network

Address Type:
 Starting IP Address:
 Ending IP Address / Subnet Mask:
 Local Port: Start End

Remote Network

Address Type:
 Starting IP Address:
 Ending IP Address / Subnet Mask:
 Remote Port: Start End

IPSec Proposal

Encapsulation Mode:
 Active Protocol:
 Encryption Algorithm:
 Authentication Algorithm:
 SA Life Time (Seconds):
 Perfect Forward Secrecy (PFS):
 Enable Replay Detection
 Enable Multiple Proposals

Figure 11: Network Policy Parameters

When complete, a VPN Rule set appears as in Figure 12. Click the [+] icon on the left to expand or collapse the rules as necessary.

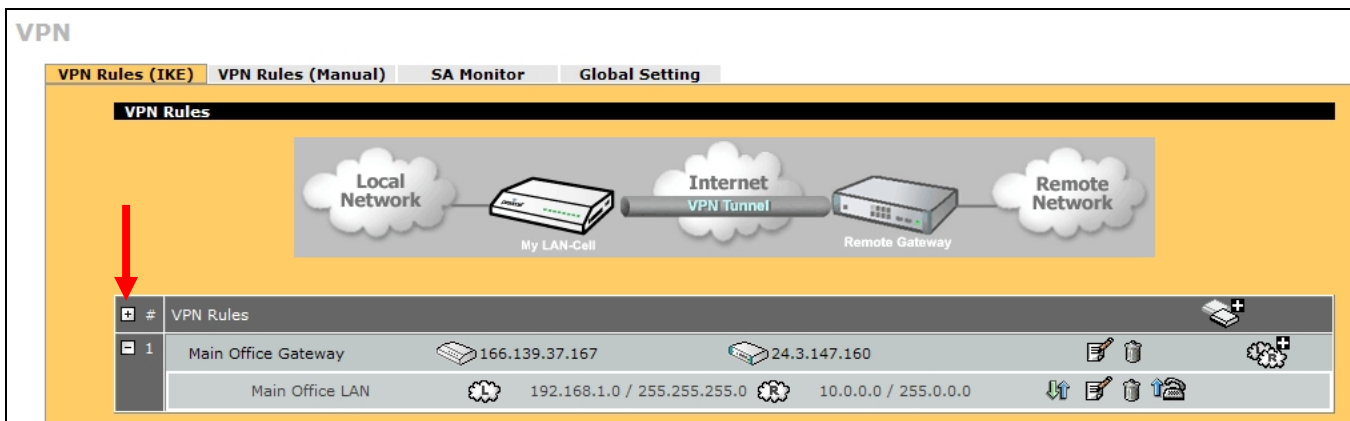


Figure 12: Completed VPN Rule Set

Opening a VPN Tunnel

Once defined, there are several ways to open and test a VPN tunnel.

Always On

If you defined the Network Policy as “Nailed Up”, the VPN tunnel creation will be attempted automatically by the LAN-Cell once the Network Policy has been saved. You can view the current status of the VPN tunnel connections (called Security Associations – SA) using the SA Monitor screen as shown in Figure 13.

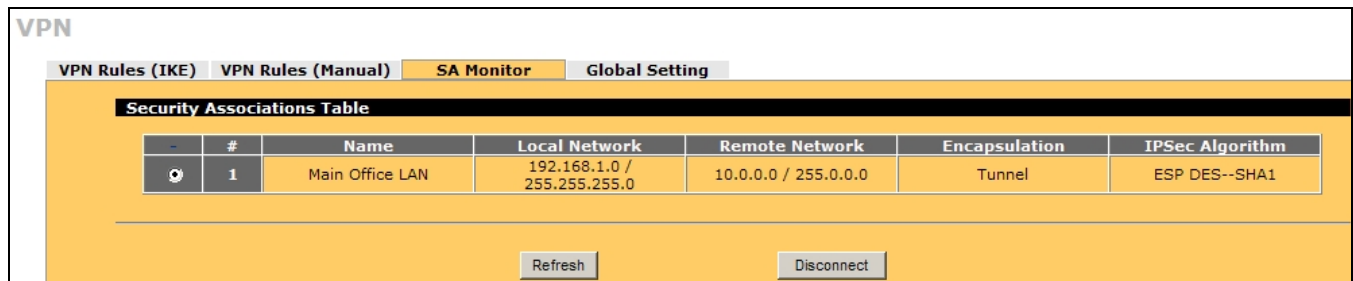


Figure 13: SA Monitor

Manual Connection

You can manually “dial up” the other VPN device by clicking the **Dial** icon (📞) next to the Network Policy rule on the VPN Rule Summary screen (Figure 14). The LAN-Cell will monitor the progress of the tunnel creation and indicate success or failure (Figures 15 & 16). The **Dial** icon can also be used to disconnect an active tunnel.

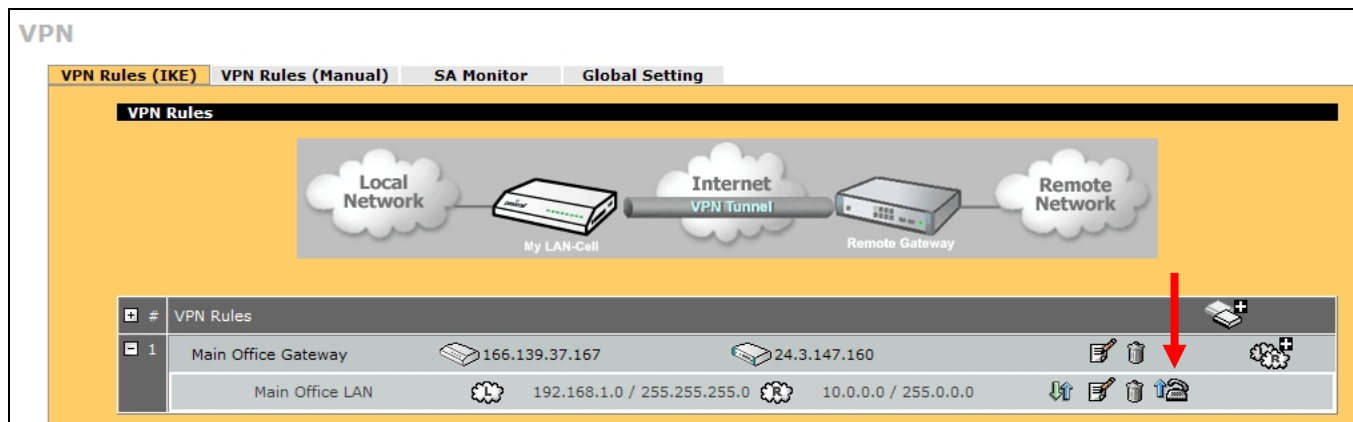


Figure 14: Manually Connecting a VPN

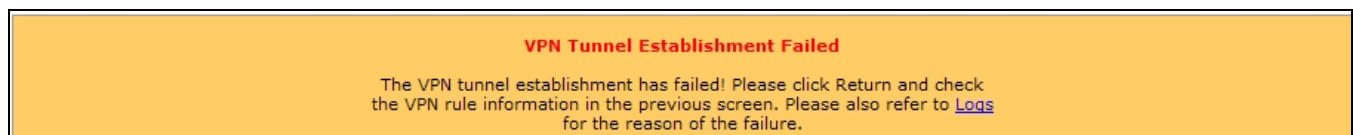


Figure 15: Failed VPN Connection

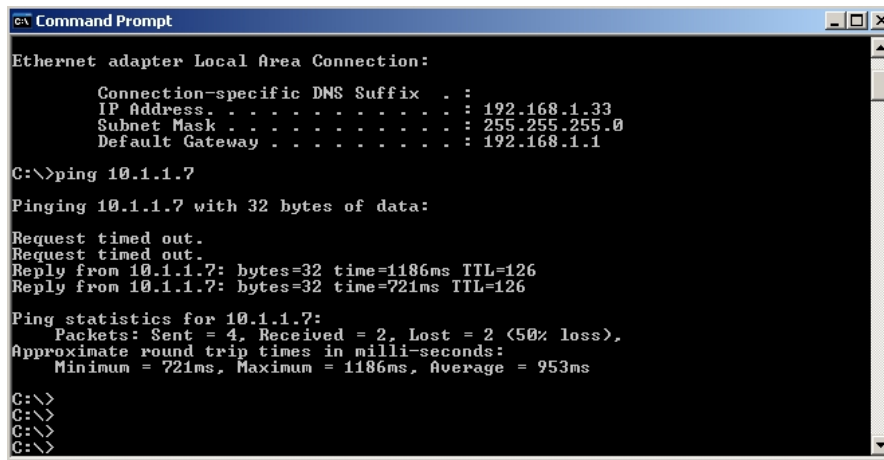


Figure 16: Successful VPN Connection

Traffic Generation

Once your VPN tunnel parameters have been entered, any traffic destined for the other private network will cause the tunnel to be automatically created. For example, a PING from a device on the LAN-Cell's LAN to the HQ LAN will bring up the tunnel. You can also initiate the tunnel from the Main Office LAN by PING'ing a device on the LAN-Cell's LAN.

Note that negotiating the tunnel may take several seconds and your first few PINGS may not be acknowledged (Figure 17). When using this method to test a VPN connection, we do not recommend sending continuous PINGS, as this can create excessive IKE retransmits which may slow down or even prevent tunnel creation.



```
c:\ Command Prompt

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    IP Address . . . . . : 192.168.1.33
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.1

C:\>ping 10.1.1.7

Pinging 10.1.1.7 with 32 bytes of data:

Request timed out.
Request timed out.
Reply from 10.1.1.7: bytes=32 time=1186ms TTL=126
Reply from 10.1.1.7: bytes=32 time=721ms TTL=126

Ping statistics for 10.1.1.7:
    Packets: Sent = 4, Received = 2, Lost = 2 (50% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 721ms, Maximum = 1186ms, Average = 953ms

C:\>
C:\>
C:\>
C:\>
```

Figure 17: Establishing a VPN Tunnel with IP Traffic

Tips

- Backup your LAN-Cell configuration file before beginning to enter the VPN parameters and again after successfully completing the VPN configuration.
- Ensure that you have a reliable Internet connection and that your ISP/Cellular account is provisioned to allow IKE/IPSec traffic in both directions.
- Start by successfully configuring the simplest VPN tunnel possible (e.g. pre-shared keys, no XAUTH, DES/MD5/DH1 security, static IP addresses) before attempting to configure more advanced settings.
- Clear the log on each VPN device after each unsuccessful connection attempt to make it easier to trace the current tunnel session.

Troubleshooting

The most common issues that arise when configuring site-to-site VPN tunnels include:

- *Stuck at Phase 1 ID Mismatch*
It is recommended that you type an IP address other than 0.0.0.0 in the local Content field or use the DNS or E-mail ID type in the following situations:
 - When there is a NAT router between the two IPSec routers.
 - When you want the remote IPSec router to be able to distinguish between VPN connection requests that come in from IPSec routers with dynamic WAN IP addresses.
- *Stuck at Phase 1 No Proposal Chosen*
Try different encryption and authentication settings. Check the Diffie-Hellman key length. Use the Enable Multiple IKE Proposals option to allow the LAN-Cell to automatically match the other VPN device's settings.
- *Phase 2 will not complete*
Most often this is a mismatch with the local and remote network subnet definitions. Ensure that you are specifying a complete subnet (if appropriate). Remember, for a full Class-C subnet, the last octet of the address should be 0 with a subnet mask of 255.255.255.0. Also the private subnets behind each VPN device must be different.

You can also enable Multiple IPSec Proposals to allow the LAN-Cell to match the incoming parameters from the other VPN device.
- *Tunnel goes down after a few minutes*
This is normal behavior if you do not specify "Nailed up" or IPSec Continuity for the Network Policy. By default, the tunnel will be dropped after 2 minutes of inactivity. You can modify the input and output timers on the VPN Config Global Settings screen.
- *Sometimes the tunnel connects and sometimes it doesn't*
Be sure that both VPN devices have completely deleted their security associations before a new tunnel request is initiated. Either manually drop the tunnel or adjust the timer values to drop the tunnel quickly if the VPN peer device does not respond.

Logging

The LAN-Cell has extensive error logging features. If initial attempts at creating the VPN tunnel are unsuccessful, use the **LOGS** menu to obtain more information about the error. You should also consult the logs and documentation for your Main Office VPN appliance for additional troubleshooting assistance.

Here are some common VPN-related error messages from the LAN-Cell's log:

Successful VPN Tunnel Creation:

#	Time ▲	Message	Source	Destination	Note
1	2008-05-14 05:20:38	Rule [Main Office LAN] Tunnel built successfully	166.139.37.167	24.3.147.160	IKE
2	2008-05-14 05:20:38	The cookie pair is : 0x48E8BCA84156C454 / 0xE318DB7902668498	166.139.37.167	24.3.147.160	IKE
3	2008-05-14 05:20:38	Send:[HASH]	166.139.37.167	24.3.147.160	IKE
4	2008-05-14 05:20:38	The cookie pair is : 0x48E8BCA84156C454 / 0xE318DB7902668498	166.139.37.167	24.3.147.160	IKE
5	2008-05-14 05:20:38	Adjust TCP MSS to 1390	166.139.37.167	24.3.147.160	IKE
6	2008-05-14 05:20:37	Recv:[HASH][SA][NONCE][ID][ID]	24.3.147.160	166.139.37.167	IKE
7	2008-05-14 05:20:37	The cookie pair is : 0x48E8BCA84156C454 / 0xE318DB7902668498	24.3.147.160	166.139.37.167	IKE
8	2008-05-14 05:20:37	Send:[HASH][SA][NONCE][ID][ID]	166.139.37.167	24.3.147.160	IKE
9	2008-05-14 05:20:37	The cookie pair is : 0x48E8BCA84156C454 / 0xE318DB7902668498	166.139.37.167	24.3.147.160	IKE
10	2008-05-14 05:20:37	Start Phase 2: Quick Mode	166.139.37.167	24.3.147.160	IKE
11	2008-05-14 05:20:37	The cookie pair is : 0x48E8BCA84156C454 / 0xE318DB7902668498	166.139.37.167	24.3.147.160	IKE
12	2008-05-14 05:20:37	Phase 1 IKE SA process done	166.139.37.167	24.3.147.160	IKE
13	2008-05-14 05:20:37	The cookie pair is : 0x48E8BCA84156C454 / 0xE318DB7902668498	166.139.37.167	24.3.147.160	IKE
14	2008-05-14 05:20:37	Recv:[ID][HASH][NOTFY:INIT_CONTACT]	24.3.147.160	166.139.37.167	IKE
15	2008-05-14 05:20:37	The cookie pair is : 0x48E8BCA84156C454 / 0xE318DB7902668498	24.3.147.160	166.139.37.167	IKE
16	2008-05-14 05:20:37	Send:[ID][HASH][NOTFY:INIT_CONTACT]	166.139.37.167	24.3.147.160	IKE
17	2008-05-14 05:20:37	The cookie pair is : 0x48E8BCA84156C454 / 0xE318DB7902668498	166.139.37.167	24.3.147.160	IKE
18	2008-05-14 05:20:37	Recv:[KE][NONCE]	24.3.147.160	166.139.37.167	IKE
19	2008-05-14 05:20:37	The cookie pair is : 0x48E8BCA84156C454 / 0xE318DB7902668498	24.3.147.160	166.139.37.167	IKE
20	2008-05-14 05:20:37	Send:[KE][NONCE]	166.139.37.167	24.3.147.160	IKE
21	2008-05-14 05:20:37	The cookie pair is : 0x48E8BCA84156C454 / 0xE318DB7902668498	166.139.37.167	24.3.147.160	IKE
22	2008-05-14 05:20:37	Recv:[SA][VID][VID]	24.3.147.160	166.139.37.167	IKE
23	2008-05-14 05:20:37	The cookie pair is : 0x48E8BCA84156C454 / 0xE318DB7902668498	24.3.147.160	166.139.37.167	IKE
24	2008-05-14 05:20:36	Send:[SA][VID][VID]	166.139.37.167	24.3.147.160	IKE
25	2008-05-14 05:20:36	The cookie pair is : 0x48E8BCA84156C454 / 0x0000000000000000	166.139.37.167	24.3.147.160	IKE
26	2008-05-14 05:20:36	Send Main Mode request to [24.3.147.160]	166.139.37.167	24.3.147.160	IKE
27	2008-05-14 05:20:36	Rule [To Main Office] Sending IKE request	166.139.37.167	24.3.147.160	IKE
28	2008-05-14 05:20:36	The cookie pair is : 0x48E8BCA84156C454 / 0x0000000000000000	166.139.37.167	24.3.147.160	IKE

Phase 1 Parameter Mismatch:

#	Time ▲	Message	Source	Destination	Note
1	2008-05-14 05:23:03	Recv:[NOTFY:NO_PROP_CHOSEN]	24.3.147.160	166.139.37.167	IKE
2	2008-05-14 05:23:03	The cookie pair is : 0x942851C0835EB2CE / 0x0000000000000000	24.3.147.160	166.139.37.167	IKE
3	2008-05-14 05:23:03	Send:[SA][VID][VID]	166.139.37.167	24.3.147.160	IKE
4	2008-05-14 05:23:03	The cookie pair is : 0x942851C0835EB2CE / 0x0000000000000000	166.139.37.167	24.3.147.160	IKE
5	2008-05-14 05:23:03	Send Main Mode request to [24.3.147.160]	166.139.37.167	24.3.147.160	IKE
6	2008-05-14 05:23:03	Rule [To Main Office] Sending IKE request	166.139.37.167	24.3.147.160	IKE
7	2008-05-14 05:23:03	The cookie pair is : 0x942851C0835EB2CE / 0x0000000000000000	166.139.37.167	24.3.147.160	IKE

Compare the Phase 1 parameters on the Remote Office LAN-Cell VPN Gateway Policy Edit page with the corresponding Phase 1 parameters on your HQ VPN device, in particular the Encryption, Authentication and the Key Group. Note: DH1 = DH768 and DH2 = DH1024.

Incorrect ID Type or Content:

#	Time ▲	Message	Source	Destination	Note
1	2008-05-14 05:25:36	Recv:[HASH][NOTFY:ERR_ID_INFO]	24.3.147.160	166.139.37.167	IKE
2	2008-05-14 05:25:36	The cookie pair is : 0x7F85DB0F88251197 / 0xFC9802603B3D7737	24.3.147.160	166.139.37.167	IKE
3	2008-05-14 05:25:36	Recv:[HASH][NOTFY:ERR_ID_INFO]	24.3.147.160	166.139.37.167	IKE
4	2008-05-14 05:25:36	The cookie pair is : 0x7F85DB0F88251197 / 0xFC9802603B3D7737	24.3.147.160	166.139.37.167	IKE
5	2008-05-14 05:25:36	Send:[ID][HASH][NOTFY:INIT_CONTACT]	166.139.37.167	24.3.147.160	IKE
6	2008-05-14 05:25:36	The cookie pair is : 0x7F85DB0F88251197 / 0xFC9802603B3D7737	166.139.37.167	24.3.147.160	IKE
7	2008-05-14 05:25:36	Recv:[KE][NONCE]	24.3.147.160	166.139.37.167	IKE
8	2008-05-14 05:25:36	The cookie pair is : 0x7F85DB0F88251197 / 0xFC9802603B3D7737	24.3.147.160	166.139.37.167	IKE
9	2008-05-14 05:25:36	Send:[KE][NONCE]	166.139.37.167	24.3.147.160	IKE
10	2008-05-14 05:25:36	The cookie pair is : 0x7F85DB0F88251197 / 0xFC9802603B3D7737	166.139.37.167	24.3.147.160	IKE
11	2008-05-14 05:25:35	Recv:[SA][VID][VID]	24.3.147.160	166.139.37.167	IKE
12	2008-05-14 05:25:35	The cookie pair is : 0x7F85DB0F88251197 / 0xFC9802603B3D7737	24.3.147.160	166.139.37.167	IKE
13	2008-05-14 05:25:35	Send:[SA][VID][VID]	166.139.37.167	24.3.147.160	IKE
14	2008-05-14 05:25:35	The cookie pair is : 0x7F85DB0F88251197 / 0x0000000000000000	166.139.37.167	24.3.147.160	IKE
15	2008-05-14 05:25:35	Send Main Mode request to [24.3.147.160]	166.139.37.167	24.3.147.160	IKE
16	2008-05-14 05:25:35	Rule [To Main Office] Sending IKE request	166.139.37.167	24.3.147.160	IKE
17	2008-05-14 05:25:35	The cookie pair is : 0x7F85DB0F88251197 / 0x0000000000000000	166.139.37.167	24.3.147.160	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 that both devices are using IP Address as the type and the same IP address values (other than blank or 0.0.0.0). 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. Remote Office LAN-Cell Local = Main Office Remote.

Phase 2 Parameter Mismatch:

#	Time ▲	Message	Source	Destination	Note
1	2008-05-14 05:32:23	Send:[HASH][DEL]	166.139.37.167	24.3.147.160	IKE
2	2008-05-14 05:32:23	The cookie pair is : 0xAF30B1DAB275562 / 0xB6B56A1750E3A218	166.139.37.167	24.3.147.160	IKE
3	2008-05-14 05:32:23	Send:[HASH][DEL]	166.139.37.167	24.3.147.160	IKE
4	2008-05-14 05:32:23	The cookie pair is : 0xAF30B1DAB275562 / 0xB6B56A1750E3A218	166.139.37.167	24.3.147.160	IKE
5	2008-05-14 05:32:23	Recv:[HASH][NOTFY:NO_PROP_CHOSEN]	24.3.147.160	166.139.37.167	IKE
6	2008-05-14 05:32:23	The cookie pair is : 0xAF30B1DAB275562 / 0xB6B56A1750E3A218	24.3.147.160	166.139.37.167	IKE
7	2008-05-14 05:32:23	Send:[HASH][SA][NONCE][ID][ID]	166.139.37.167	24.3.147.160	IKE
8	2008-05-14 05:32:23	The cookie pair is : 0xAF30B1DAB275562 / 0xB6B56A1750E3A218	166.139.37.167	24.3.147.160	IKE
9	2008-05-14 05:32:23	Start Phase 2: Quick Mode	166.139.37.167	24.3.147.160	IKE
10	2008-05-14 05:32:23	The cookie pair is : 0xAF30B1DAB275562 / 0xB6B56A1750E3A218	166.139.37.167	24.3.147.160	IKE
11	2008-05-14 05:32:23	Phase 1 IKE SA process done	166.139.37.167	24.3.147.160	IKE
12	2008-05-14 05:32:23	The cookie pair is : 0xAF30B1DAB275562 / 0xB6B56A1750E3A218	166.139.37.167	24.3.147.160	IKE
13	2008-05-14 05:32:23	Recv:[ID][HASH][NOTFY:INIT_CONTACT]	24.3.147.160	166.139.37.167	IKE
14	2008-05-14 05:32:23	The cookie pair is : 0xAF30B1DAB275562 / 0xB6B56A1750E3A218	24.3.147.160	166.139.37.167	IKE
15	2008-05-14 05:32:23	Send:[ID][HASH][NOTFY:INIT_CONTACT]	166.139.37.167	24.3.147.160	IKE
16	2008-05-14 05:32:23	The cookie pair is : 0xAF30B1DAB275562 / 0xB6B56A1750E3A218	166.139.37.167	24.3.147.160	IKE
17	2008-05-14 05:32:23	Recv:[KE][NONCE]	24.3.147.160	166.139.37.167	IKE
18	2008-05-14 05:32:23	The cookie pair is : 0xAF30B1DAB275562 / 0xB6B56A1750E3A218	24.3.147.160	166.139.37.167	IKE
19	2008-05-14 05:32:22	Send:[KE][NONCE]	166.139.37.167	24.3.147.160	IKE
20	2008-05-14 05:32:22	The cookie pair is : 0xAF30B1DAB275562 / 0xB6B56A1750E3A218	166.139.37.167	24.3.147.160	IKE
21	2008-05-14 05:32:22	Recv:[SA][VID][VID]	24.3.147.160	166.139.37.167	IKE
22	2008-05-14 05:32:22	The cookie pair is : 0xAF30B1DAB275562 / 0xB6B56A1750E3A218	24.3.147.160	166.139.37.167	IKE
23	2008-05-14 05:32:21	Send:[SA][VID][VID]	166.139.37.167	24.3.147.160	IKE
24	2008-05-14 05:32:21	The cookie pair is : 0xAF30B1DAB275562 / 0x0000000000000000	166.139.37.167	24.3.147.160	IKE
25	2008-05-14 05:32:21	Send Main Mode request to [24.3.147.160]	166.139.37.167	24.3.147.160	IKE
26	2008-05-14 05:32:21	Rule [To Main Office] Sending IKE request	166.139.37.167	24.3.147.160	IKE
27	2008-05-14 05:32:21	The cookie pair is : 0xAF30B1DAB275562 / 0x0000000000000000	166.139.37.167	24.3.147.160	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 Main Office's Phase 2 settings.

Frequently Asked Questions

Q: Can I have more than 1 VPN connection from the Remote LAN-Cell at the same time?

A: Yes. The LAN-Cell 2 supports 5 simultaneous non-overlapping VPN tunnels; the original LAN-Cell Mobile Gateway supports 2 VPN tunnels. Simply define the Gateway and Network Policies you need for each tunnel.

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

A: Yes if your HQ VPN device supports Dynamic DNS endpoints. Check with the VPN device manufacturer for support of DDNS addresses versus static IP addresses. The LAN-Cell can establish VPN tunnels with DDNS addressed devices.

Q: Can the Main Office initiate the VPN tunnel connection?

A: Yes. The Remote Office LAN-Cell will respond to requests for an IPSec tunnel from any WAN device that has the correct IKE & IPSec parameters.

Q: Can I have the same subnet on each end of the VPN tunnel?

A: Each end of the VPN tunnel must be unique subnet, however it is possible to have the private subnet of the remote LAN-Cell be a subset of the private HQ network. For example, if the HQ LAN is 10.0.0.0 / 255.0.0.0 the LAN-Cell's LAN subnet could be 10.1.1.0 / 255.255.255.0. In order to allow local devices behind the LAN-Cell to communicate with each other and manage the LAN-Cell, you must check the *Do not apply VPN rules to overlapped local and remote IP address ranges* checkbox on the VPN Config Global Options screen. You may need to define additional static routes on the LAN-Cell and/or your HQ VPN device to permit traffic to reach the necessary addresses.

Q: Can I force all Internet bound traffic from the LAN-Cell to go through the VPN tunnel before going onto the Internet?

A: Yes. See TechNote *LCTN0009: Routing all Internet-bound Traffic Through a VPN Tunnel* for an example of how to configure this type of VPN tunnel.

###