Routing all Internet-bound Traffic Through a VPN Tunnel

Technote LCTN0009

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

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

Fax:
1-412-492-9386

E-Mail:
support@proxicast.com

Internet:
www.proxicast.com

This TechNote applies to LAN-Cell models:

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

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
May 14, 2008	First release

Introduction

There are some instances where you may wish to have all Internet-bound traffic from devices behind a remote LAN-Cell routed to a central office location before being sent to its final Internet destination. For example, some organizations already have centralized and standardized access control lists, content filtering, intrusion detection and prevention, firewalls and other Internet access controls in place. They want to prevent users in remote offices from having "direct" access to the Internet and need to force all Internet traffic through a central point.

You can easily create the necessary IPSec rules on the LAN-Cell to create a "site-to-site" VPN tunnel that forces all non-local LAN traffic to be sent to a central location. This Technote documents one example configuration of how to accomplish this using a LAN-Cell at both locations. If you are using a different brand of VPN appliance at your Main Office location, you will need to modify its configuration to be similar to the Main Office LAN-Cell in this example. This Technote is for illustration purposes only.

Example Network Topology

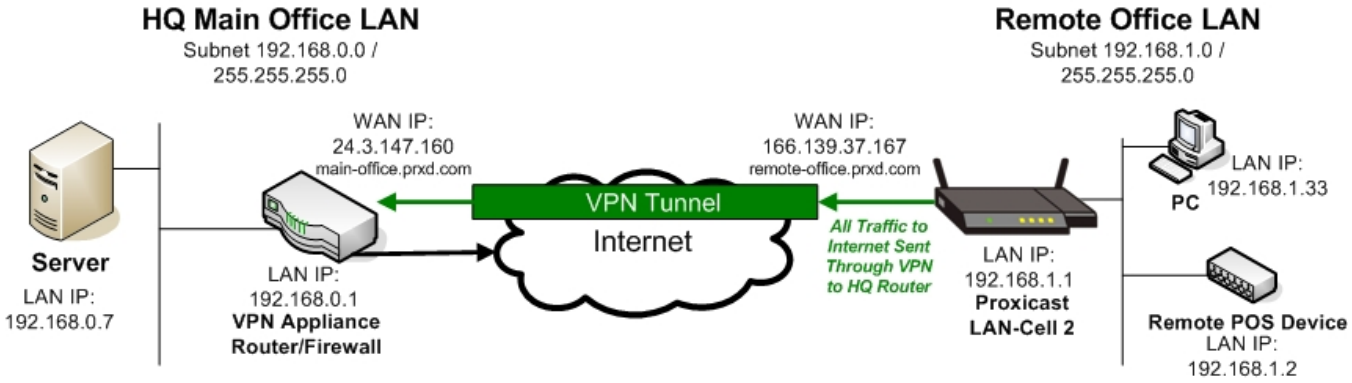

Figure 1: Example Network Topology

Usage Notes

- When configuring a VPN connection, it is helpful to have the LAN-Cell and your target VPN appliance physically near each other so that you can view the configuration and logs of each device while testing.
- In this example, the remote office LAN-Cell has a static WAN IP address (166.139.37.167). The same configuration is possible by replacing the static IP address with a fully qualified dynamic DNS name (e.g. *remote-office.prxd.com*) if your HQ VPN appliance supports DDNS tunnel end-points. You must set up a DynDNS account, hostname, and configure the remote LAN-Cell to update DynDNS with its current WAN IP address. See the *LAN-Cell User's Guide* for additional information on DDNS.
- For the sake of simplicity, the IPSec security settings were left at the factory defaults in this example. You may select any security settings as long as they match on both the LAN-Cell and your VPN appliance.
- There is additional information on LAN-Cell VPN configuration parameters in the *LAN-Cell User's Guide*.

Overview

The basic approach to achieving the desired VPN routing is to define a VPN Network Policy on the remote LAN-Cell which "catches" the entire range of possible IP addresses and sends the traffic to the related Gateway Policy for transmission to the remote VPN appliance at your Main Office location. In most cases, you will want to "exempt" the subnet of the devices attached to the LAN side of the LAN-Cell so that peer-to-peer traffic does not go through the VPN tunnel.

At the Main Office location, you must define a reciprocal Network Policy to allow the remote LAN-Cell to participate in the Main Office subnet(s).

> **Note**: You cannot use the LAN-Cell 2's **VPN Wizard** to define the necessary VPN settings for either the Remote or Main Office devices in this scenario. You must configure the Gateway and Network Policies individually using the **VPN CONFIG** screens.

Remote Office LAN-Cell Configuration

Start by exempting the LAN-Cell's LAN subnet from participating in the "Main Office LAN" Network Policy (to be defined later). Select the **SECURITY->VPN CONFIG** menu, then the **GLOBAL SETTING** tab (Figure 2).

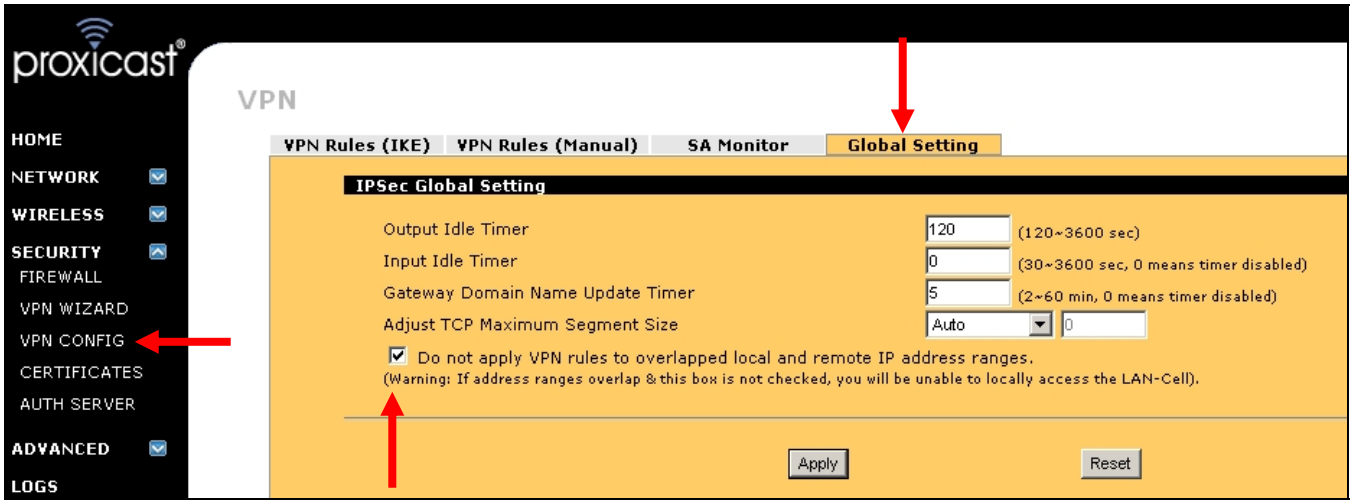

Figure 2: Exempting Overlapped Local & Remote IP Address Ranges

Check the box labeled "Do not apply VPN rules to overlapped local and remote IP address ranges." If you do not select this option, you will not be able to access the LAN-Cell for configuration from LAN-attached devices, as all traffic will be routed to through the VPN. Also, all local LAN traffic such as from a PC to a local printer will be forced through the tunnel. Click **APPLY** to save your settings.

> **Note**: On earlier LAN-Cell models, this checkbox is not available; however you can achieve the same results by adding the command `ipsec swSkipOverlapIp on` (case sensitive) to the LAN-Cell's autoexec.net file. See: TechNote *LCTN0004 Editing AUTOEXEC.NET.*

Next, create the Gateway Policy that defines the connection to your Main Office VPN device.

Select **SECURITY->VPN CONFIG** and click the **Add Gateway Policy** icon  (Figure 3).

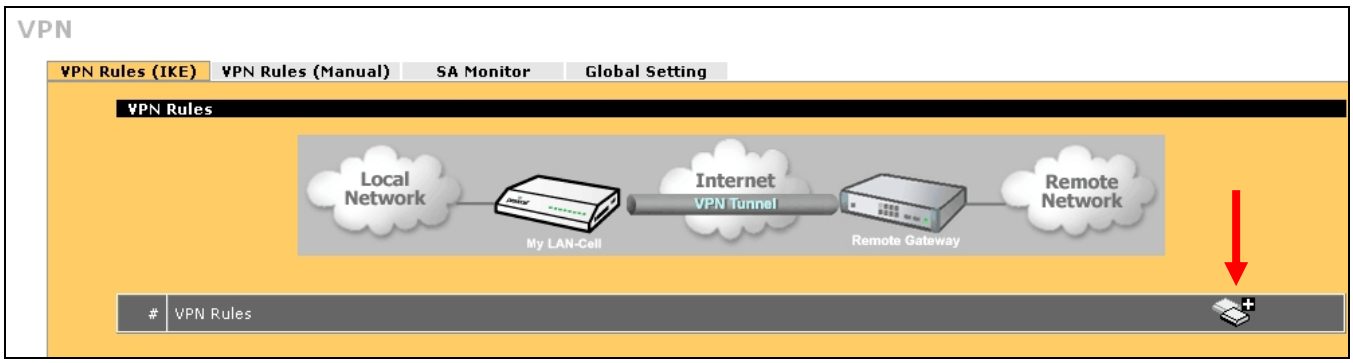

Figure 3: Add Gateway Policy

As shown in Figure 4, you must give the Gateway Policy a descriptive Name (up to 32 characters long). If your LAN-Cell has a static WAN IP address assigned by your ISP or cellular operator, enter that value as the My LAN-Cell address. Optionally you can enter a Dynamic DNS FQDN that is associated with your LAN-Cell's WAN (see the **Advanced->DNS->DDNS** screen) or you can enter 0.0.0.0 and the LAN-Cell will use its current WAN IP address.

For the Primary Remote Gateway, enter the public WAN IP address (or fully qualified domain name) of your Main Office's VPN appliance. In our example, this is 24.3.147.160 or *main-office.prxd.com*.

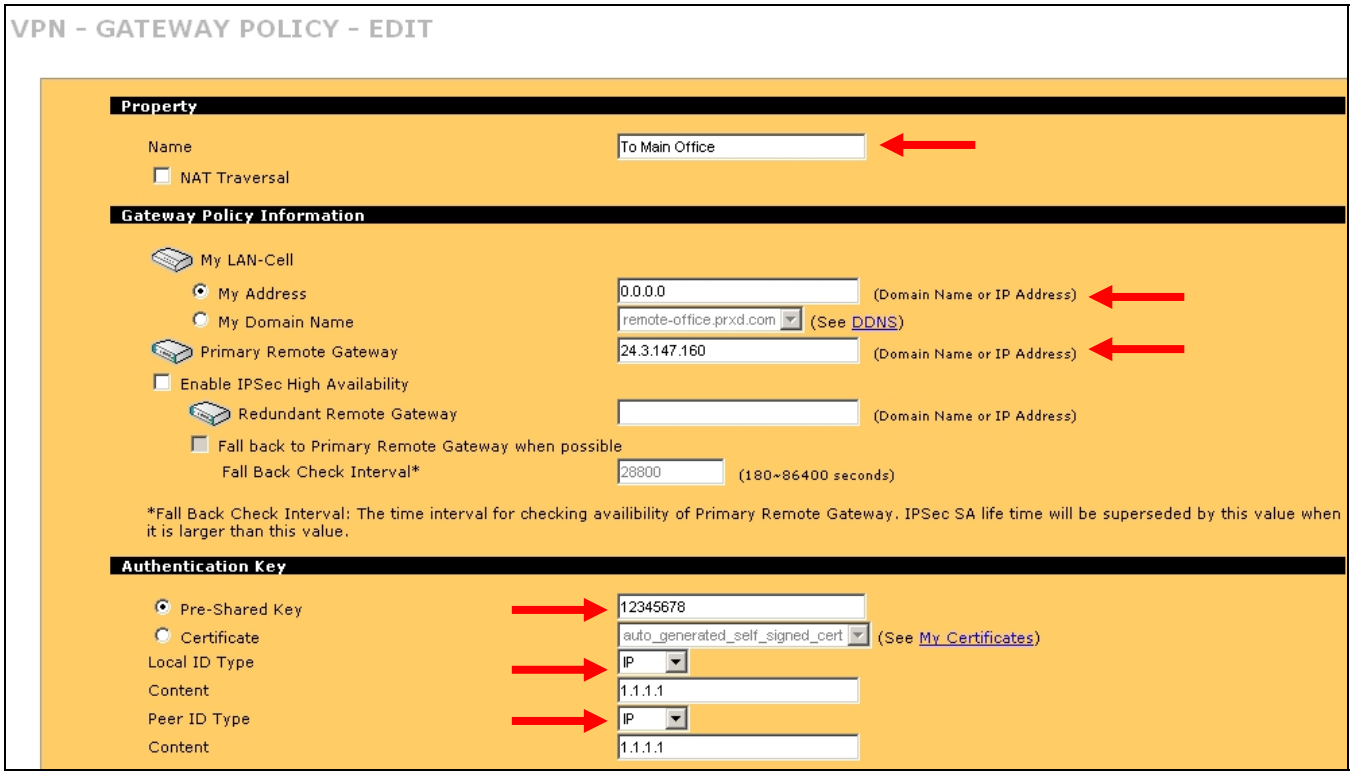

Figure 4: Gateway Policy Parameters

The LAN-Cell supports several different types of authentication, including X.509 digital certificates. It is easiest to configure the VPN tunnel with Pre-Shared Keys that are the same on both Main and Remote Office devices. 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.

Next, you must change the Local and Remote ID Type settings from their default values. The LAN-Cell uses the default value of blank (or IP = 0.0.0.0) to automatically fill these fields with the current IP address during Phase 1 IKE negotiation. For the "all traffic" tunnel we are creating, you must enter a non-zero value for the IP address (or select another ID type with non-blank values). The IP address entered does not matter as long as it matches on both the Main and Remote Office VPN devices. (Optionally, you can select Ethe -Mail or DNS/Hostname ID type if your Main Office VPN appliance supports these ID types).

In our example, we use 1.1.1.1 as the IP address value for both the Local and Remote IDs. Also in our example, we are leaving the remaining IKE Proposal fields on this screen at their default values: Main Mode Negotiation, DES Encryption, MD5 Authentication, SA Lifetime of 28800 seconds and Diffie-Hellman Key Group 1 (768 bits). When complete, click **APPLY** to save your settings and return to the **VPN Rules** screen.

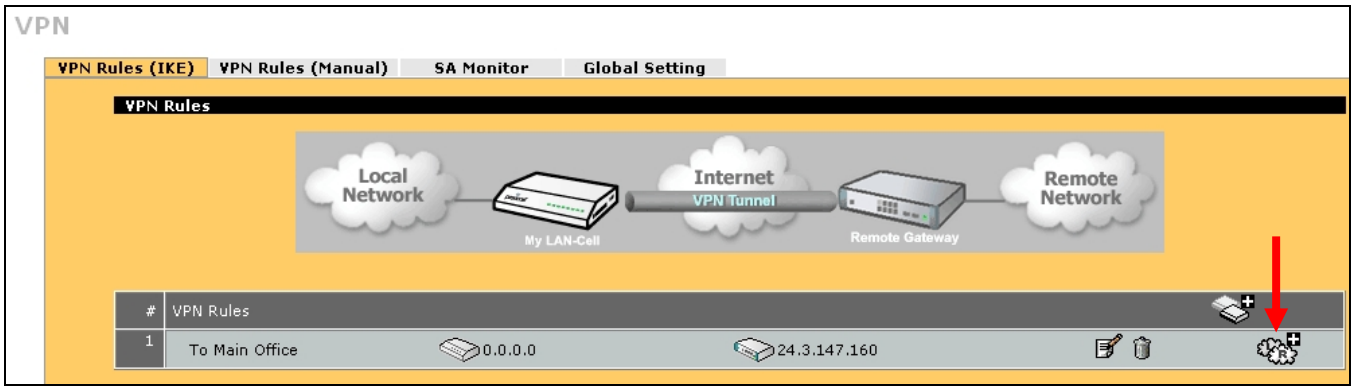

Figure 5: Gateway Policy Defined

Next, we must create a Network Policy that defines which IP address ranges that will be used on each end of the VPN tunnel. Click the **Add Network Policy** icon to enter this information (Figure 5).

Figure 6 illustrates the correct Network Policy settings for our example VPN tunnel.

Be certain to check the Active option. You must also give the Network Policy a descriptive Name. If you want the VPN tunnel to be established at all times, check the Nailed-Up option.

The "To Main Office" Gateway Policy associated with this Network Policy will be automatically selected since you are creating this Network Policy from the Gateway Policy screen.

Figure 6: Network Policy Parameters

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 Range Address as the Type and enter a Starting IP Address of 0.0.0.0 and an Ending IP Address of 255.255.255.255. This creates a rule that directs all IP traffic to be sent through the VPN tunnel (except the LAN-Cell's subnet that was excluded with the Global Setting option). Selecting the entire possible range of IP addresses for the Remote Network prevents the LAN-Cell from sending any IP packets directly to the Internet or any other non-local network addresses.

Again, for our example we will accept the default Phase 2 IPSec Proposal parameters of Tunnel Encapsulation, ESP Protocol, DES Encryption, SHA1 Authentication, SA Lifetime of 28800 seconds and no Perfect Forward Secrecy. Any other proposal settings are permissible as long as they match on both ends of the VPN tunnel.

Configuration of the Remote Office LAN-Cell is now complete.

To view the Network Policy associated with the Gateway Policy, 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 7).

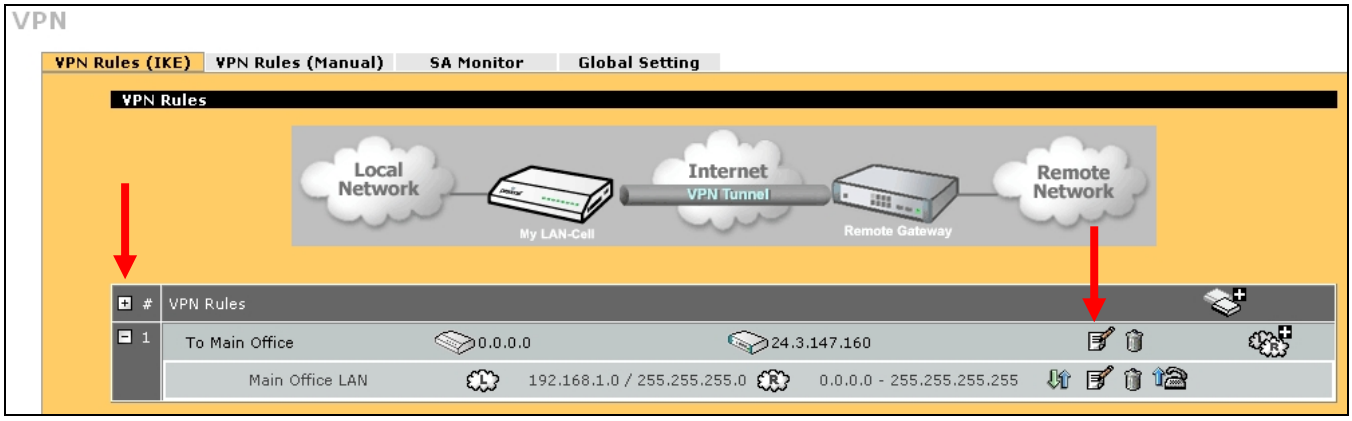

Figure 7: Displaying and Editing VPN Rules

Main Office Configuration

In our example we will configure a second LAN-Cell as our Main Office VPN appliance. The LAN-Cell is interoperable with most IPSec VPN devices. Configure your HQ VPN appliance similarly to the LAN-Cell shown in the example below.

Define a Gateway Policy for the Remote Office LAN-Cell's VPN end-point as shown in Figure 8.

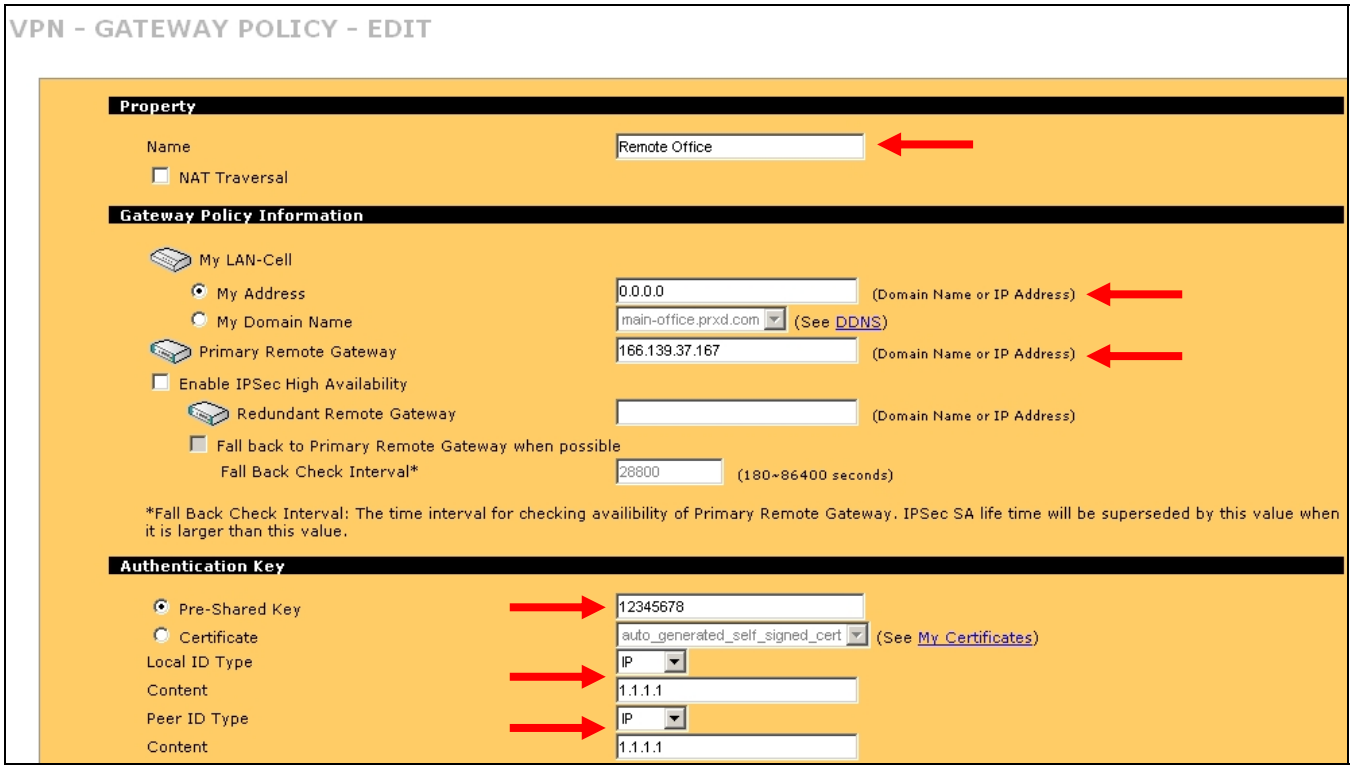

Figure 8: Main Office Gateway Policy

As on the remote site, give the Gateway Policy a descriptive Name. Leave the My LAN-Cell Address at 0.0.0.0 (or the assigned static IP address from your ISP). For the Primary Remote Gateway Address, enter the static public WAN IP address (166.139.37.167) assigned to your remote LAN-Cell (or use the DDNS name defined for the remote LAN-Cell).

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

Set the Local and Remote ID Types to IP and enter 1.1.1.1 as the address in each field to match the values entered on the remote LAN-Cell.

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

Next, define a Network Policy to permit the Remote Office LAN subnet to participate in the HQ VPN (Figure 9).

Figure 9: Remote Office Network Policy

The key for this Network Policy is to define the Local Address Range and Remote Network Subnet to match the corresponding values on the Remote Office LAN-Cell's Network Policy. The terms "Local" and "Remote" are relative to the device you're currently working on, so the addresses are opposite on each device. In our example, the Local Network is a Range from 0.0.0.0 to 255.255.255.255 and the Remote Network is the local subnet of the "remote" LAN-Cell or 192.168.1.1.

As before, we will use the default IKE Phase 2 parameters in our example: Tunnel Encapsulation, ESP Protocol, DES Encryption, SHA1 Authentication, SA Lifetime of 28800 seconds and no Perfect Forward Secrecy.

Testing the VPN Tunnel

If you selected the “Nailed Up” option on either Network Policy, the VPN tunnel should be established as soon as you complete defining both end-points.

You can also test the VPN tunnel by manually initiating a connection from the Remote Office LAN-Cell by clicking the **Dial** icon ( ) on the VPN Rules screen (Figure 10). Or you can simply attempt to access an Internet address using a web browser or “ping” command (Figure 11). Note – the first few ping packets may not be acknowledged while the VPN tunnel is being established.

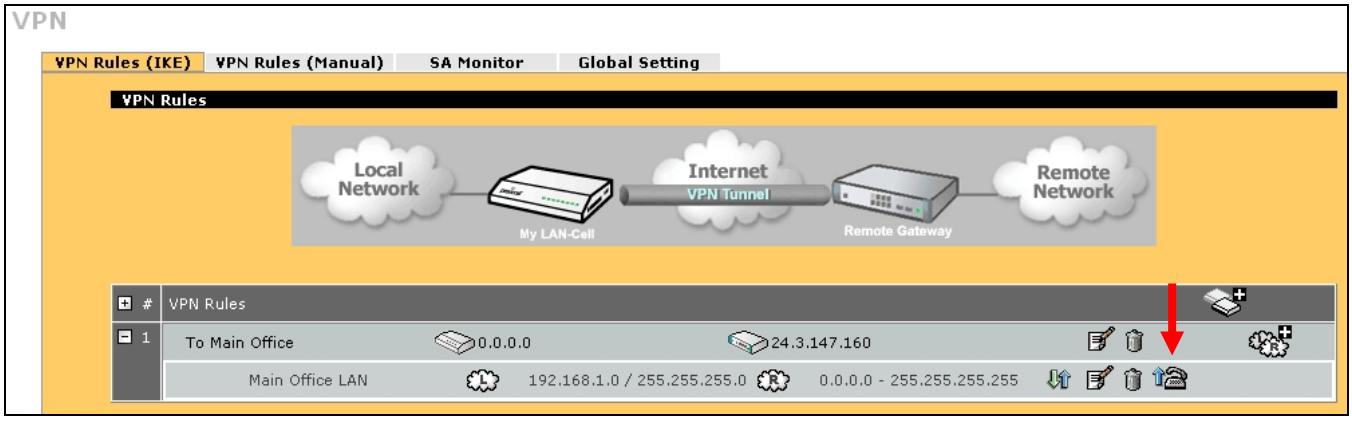

Figure 10: Manually Opening a VPN Tunnel

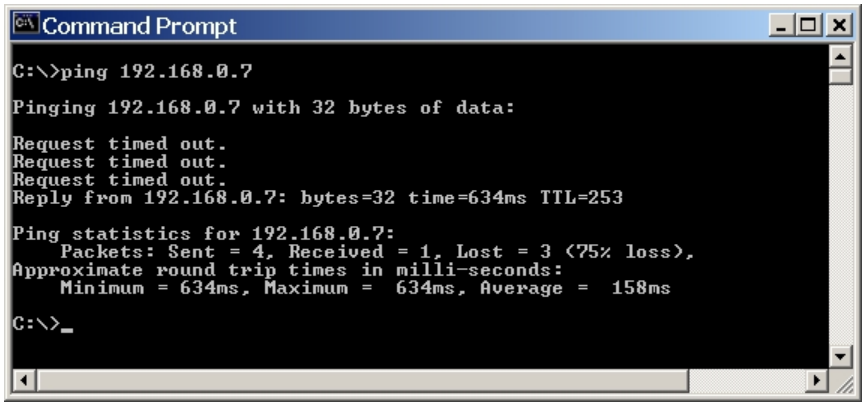

Figure 11: Pinging Through the VPN Tunnel

On either the LAN-Cell, you can observe the status of the tunnel using the **SA Monitor** tab under the **VPN CONFIG** menu (see Figure 12).

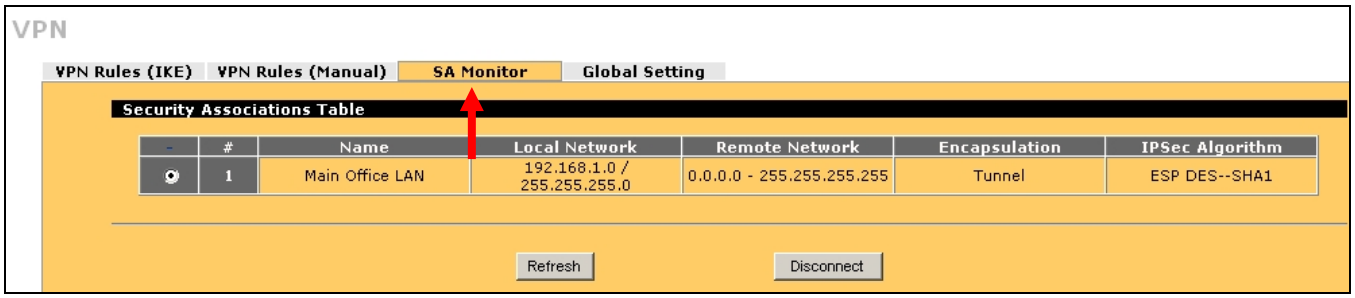

Figure 12: LAN-Cell SA Monitor Screen

You can also confirm that all non-local traffic is being sent through the VPN tunnel by temporarily disabling the Network Policy on the Remote Office LAN-Cell and observing that no Internet access is possible from client devices even though the LAN-Cell's WAN connection is active.

If the VPN tunnel is not being established, review the Troubleshooting tips in the next section.

Troubleshooting

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 : 0xAFE30B1DAB275562 / 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 : 0xAFE30B1DAB275562 / 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 : 0xAFE30B1DAB275562 / 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 : 0xAFE30B1DAB275562 / 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 : 0xAFE30B1DAB275562 / 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 : 0xAFE30B1DAB275562 / 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 : 0xAFE30B1DAB275562 / 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 : 0xAFE30B1DAB275562 / 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 : 0xAFE30B1DAB275562 / 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 : 0xAFE30B1DAB275562 / 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 : 0xAFE30B1DAB275562 / 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 : 0xAFE30B1DAB275562 / 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 : 0xAFE30B1DAB275562 / 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, but not with this example configuration. The LAN-Cell 2 supports 5 simultaneous non-overlapping VPN tunnels; the original LAN-Cell Mobile Gateway supports 2 VPN tunnels. This example configuration encompasses the entire range of possible IP addresses, so only 1 tunnel can be defined.

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 IPSec parameters.

Q: What if I have more than 1 subnet defined on the Remote LAN-Cell (e.g. DMZ, WLAN, VLAN)?

A: Replace the single "All IP Address" range Network Policy with 2 network policies – one covering addresses below your second subnet and one covering addresses above your second subnet. The main LAN subnet can be overlapped as long as the Global Setting option is checked.

Q: I forgot to check "*Do not apply VPN rules to overlapped local and remote IP address ranges*" and now I can't access the LAN-Cell locally. What should I do?

A: You can access the Remote Office LAN-Cell by entering the LAN-Cell's public WAN IP address (or DDNS name) in a web browser of a PC connected to the Internet.

From the Main Office LAN, you can enter the Remote Office LAN-Cell's LAN IP address in your browser to create a VPN tunnel to access the device.

You can use the blue serial console cable and a terminal emulation program such as HyperTerm to access the LAN-Cell's Systems Management Terminal interface. Go to menu 24.8 and enter the commands:

```
ipsec swSkipOverlapIp on
ipsec drop 1
```

then use the web interface to set the Global Setting check box.

You can press the hardware reset button for 10 seconds to return the LAN-Cell to its factory default settings.

# # #