

▷ SONICWALL TECH NOTE :

## Virtual IP Issues

### Overview

This tech note provides more information about issues encountered when trying to get an IP address for the virtual adapter when using the Global VPN Client (GVC).

There are a number of reasons why the virtual adapter may fail to retrieve an IP address. This document will discuss some of the more common reasons and provide some procedures to resolve these issues.

### Invalid Configuration on the Firewall

The most common the virtual adapter cannot obtain an IP address is the firewall not being configured properly.

If you are using internal DHCP server on the firewall for your GVC clients, ensure the following settings on your firewall are properly configured:

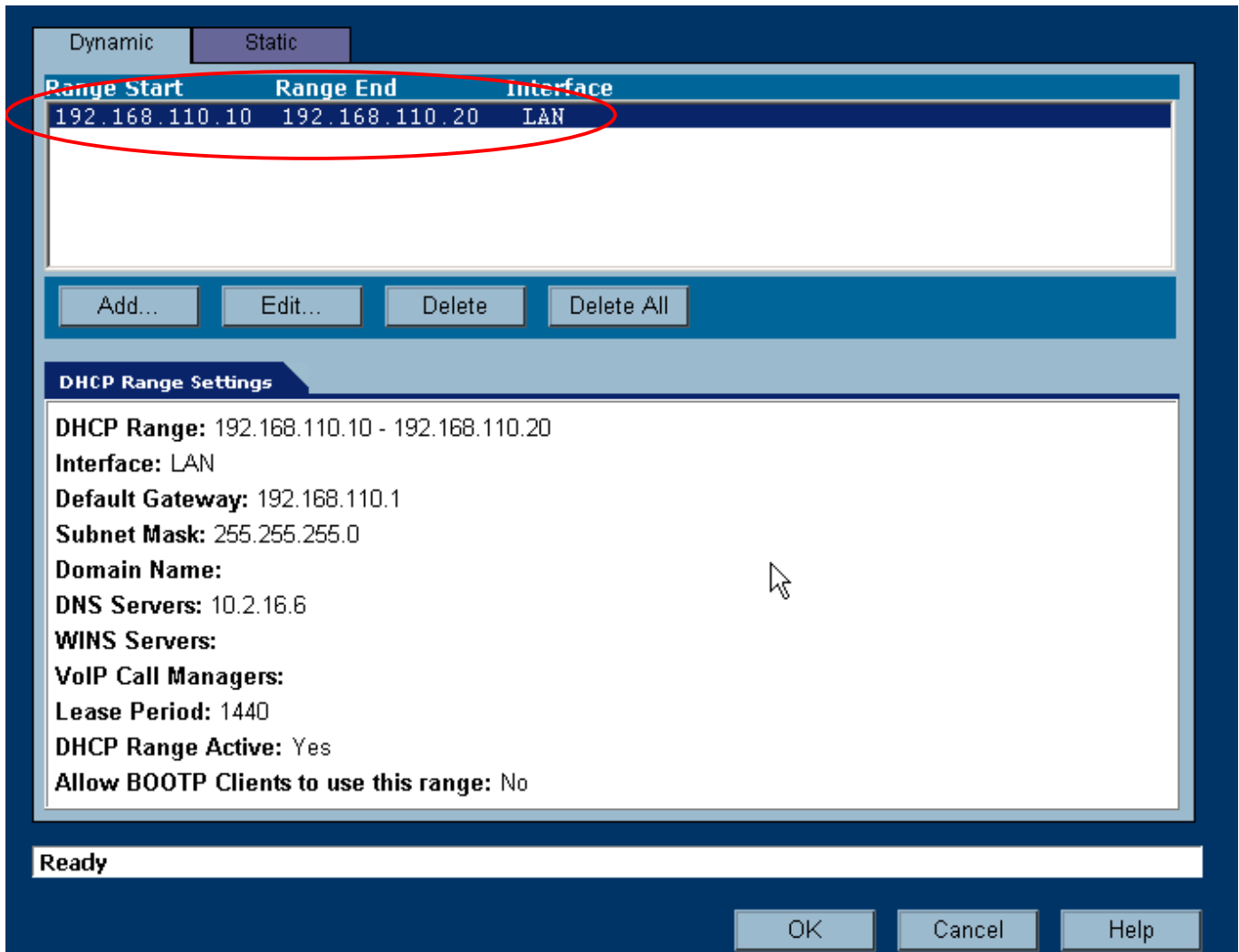
- Enable the internal DHCP server:
  1. In the Management UI, click on Network and open the DHCP Server Settings page.
  2. Make sure **Enable DHCP Server** is checked.




Screenshot 1: Enabling the internal DHCP server

- Configure a DHCP scope in the LAN network, and assign it to the LAN interface:
  1. In the Network > DHCP Server Settings page, click on **Configure**.
  2. In the DHCP Server Configuration window, there should be an IP range listed. If so, make sure it is assigned to an interface that is assigned to your LAN (LAN by default in SonicOS Standard, X0 by default in SonicOS Enhanced).
  3. If there is no range displayed, or if the range is assigned to an interface in a different zone, click **Add**.
  4. In the Dynamic Range Configuration window, add the new range and make sure you assign it to an interface in the LAN.

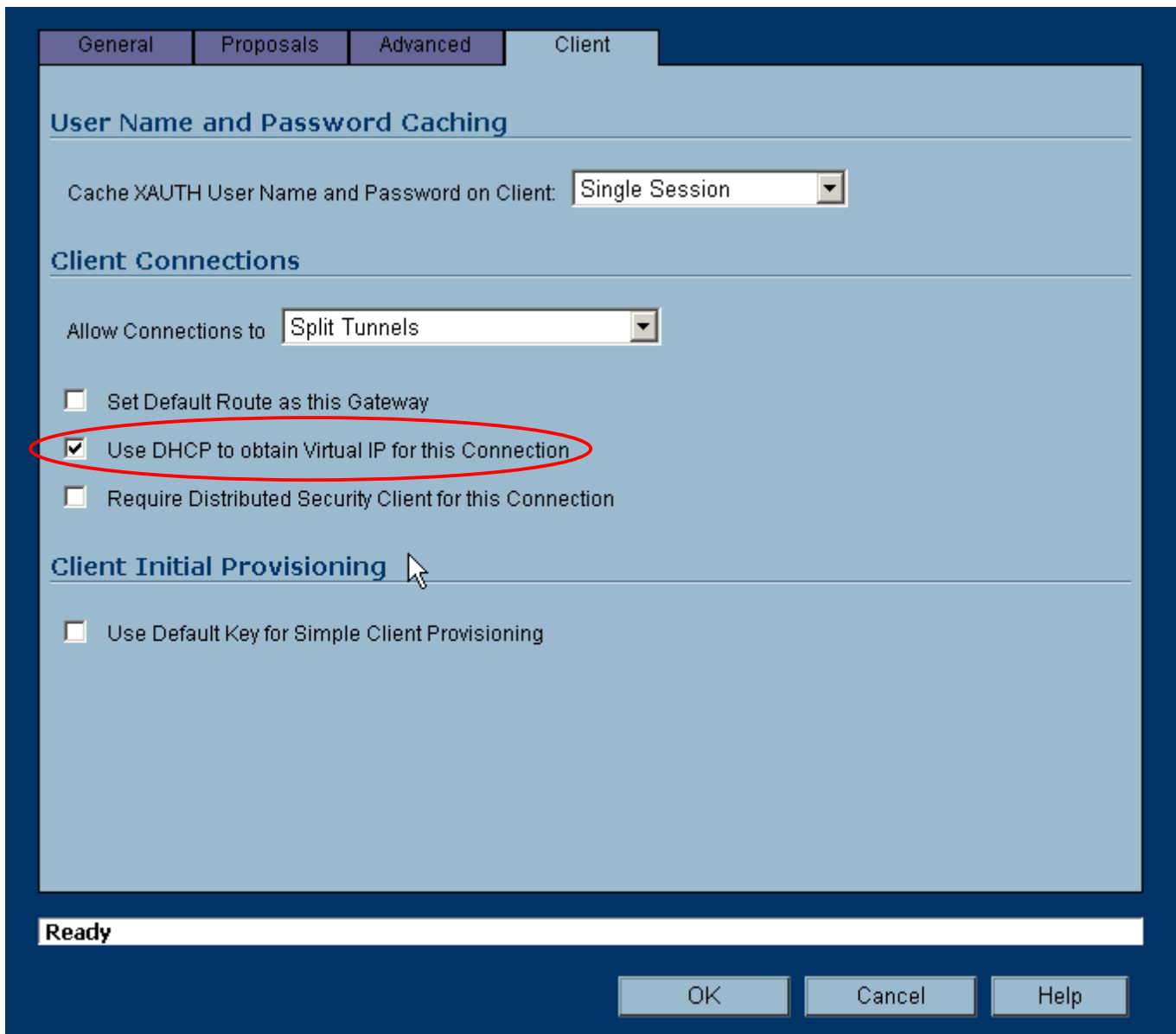
▷ SONICWALL TECH NOTE :



Screenshot 2: Configuring a DHCP scope in the LAN network

- On the 'Client' page of your Group VPN policy select 'Use DHCP to obtain Virtual IP for this Connection'
  - Click on **VPN** on the left of the management UI to open the VPN > Settings page.
  - Click on the notepad icon  to edit the Group VPN Policy.
  - In the VPN Policy screen, click on the **Client** tab.
  - Check **Use DHCP to obtain Virtual IP for this Connection**.

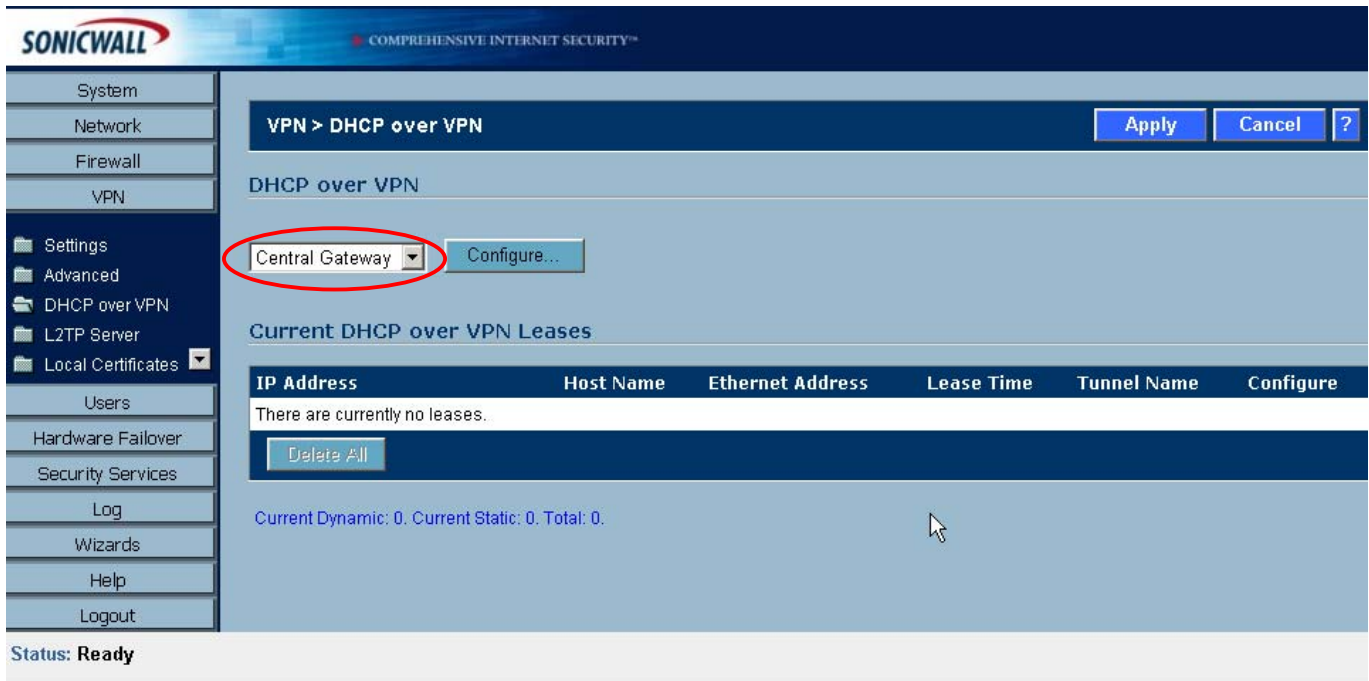
▷ SONICWALL TECH NOTE:



Screenshot 3: Selecting 'Use DHCP to obtain Virtual IP for this Connection'

- Make sure the DHCP is configured on the Central Gateway for the VPN.
  1. Click on **VPN** on the left of the management UI and then click **DHCP over VPN** to open the VPN > DHCP over VPN page.
  2. Select to use **Central Gateway** as shown in Screenshot 4.

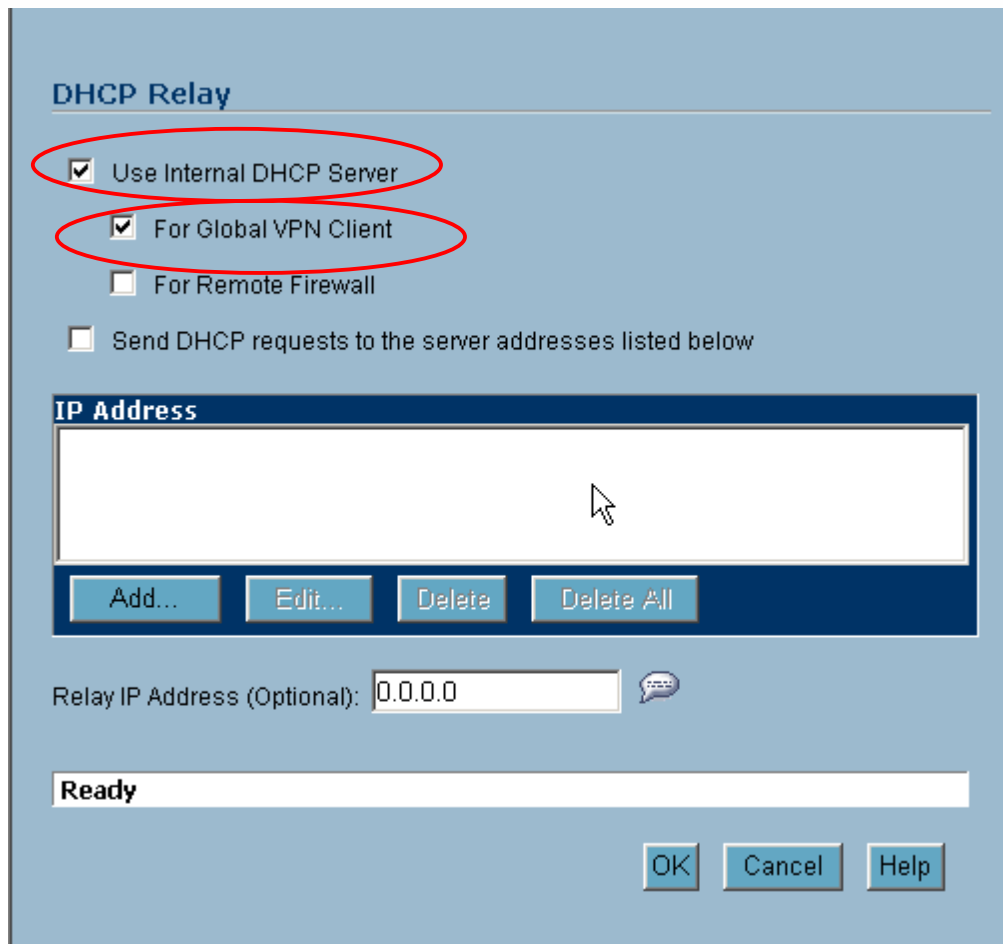
▷ SONICWALL TECH NOTE:



Screenshot 4: Configuring DHCP over VPN to use the Central Gateway

- Select the following options to use the internal DHCP server as shown in Screenshot 5.
  1. Use Internal DHCP Server
  2. For Global VPN Client

▷ SONICWALL TECH NOTE :



Screenshot 5: Configuring the Central Gateway

If you are using an external DHCP server, the DHCP server can be on the primary LAN network or on a routed network from the Primary LAN interface. Ensure the following settings on your firewall are properly configured:

- On the 'Client' page of your Group VPN policy select **Use DHCP to obtain Virtual IP for this Connection** as shown in Screenshot 3.
- Configure the external DHCP server with a scope to assign DHCP lease from to GVC clients.
- If the DHCP scope is the **SAME** as the Primary LAN network then no additional steps are required.
- If the DHCP scope is *not the same* as the Primary LAN network, then configure the Relay IP address as shown in Screenshot 5.
- In the current release, SonicOS 2.1.x.x, if the DHCP server is on a routed network from the Primary LAN interface, then in addition to the Relay IP address, need to setup IP helper on the router.

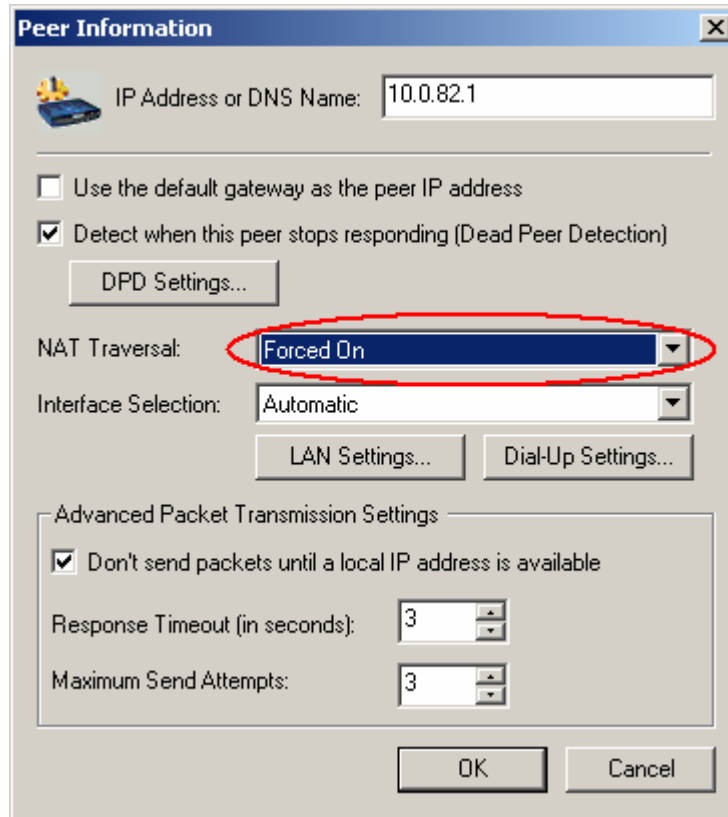
**ESP Traffic is Blocked**

GVC may be run from behind a firewall or other device that allows ISAKMP traffic to pass through, but does not allow ESP traffic to pass through. The DHCP requests that get sent for the virtual adapter are sent down the tunnel like any other traffic and are thus encapsulated in ESP. The ESP packets are simply dropped by the firewall with no indication back to GVC.

To work around this problem, GVC is enabled to detect a NAT device in the middle. When GVC detects a NAT device, it encapsulates all ESP traffic (including DHCP packets) using the UDP header. The UDP header uses the same port as ISAKMP control traffic. Therefore the Peer must separate the IKE control traffic from the data traffic. The default for NAT Traversal is shown in Screenshot 6.

▷ SONICWALL TECH NOTE :

To configure the NAT traversal setting from the client, select the Connection in GVC and then select **File -> Properties**. Select the **Peers** tab and then select the appropriate peer (head-end firewall) and choose **Edit**. Next choose **NAT Traversal** and select **Forced On**. See Screenshot 6.



Screenshot 6: Setting the client to force NAT traversal

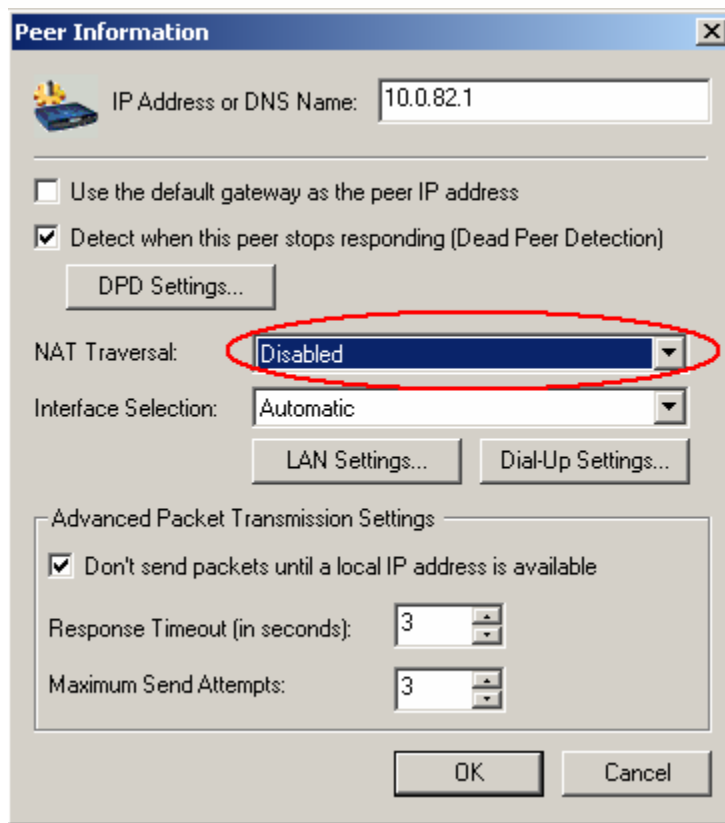
**NAT Traversal UDP Encapsulated ESP Traffic is Blocked**

Occasionally GVC may be run from behind a NAT device that improperly handles NAT traversal packets (ESP packets encapsulated in ISAKMP). These packets are discarded by the NAT device without any notification sent back to GVC.

To work around this problem, set GVC never to perform NAT traversal. This means that ESP traffic will not be encapsulated in UDP. In order for this to work, the NAT device must be in 'IPsec pass-through' mode. This mode will prevent multiple GVC clients running simultaneously behind a single NAT device.

To disable NAT traversal in the client, select the Connection in GVC and then select **File -> Properties**. Select the **Peers** tab and then select the appropriate peer (head-end firewall) and choose **Edit**. Next choose **NAT Traversal** and select **Disabled** (see Screenshot 7 below).

▷ SONICWALL TECH NOTE :



Screenshot 7: Setting the client to disable NAT traversal

Another workaround for this problem is to update both the client and the firmware. Starting with version 3.0.0.0 of GVC and SonicOS 2.1.x.x (enhanced) of the firewall firmware, a new NAT traversal specification is supported that can bypass many NAT devices that improperly handle UDP encapsulated ESP packets. This is done by switching the port used for ISAKMP from the default 500 to 4500. See your network administrator for information on how to update to the latest release of GVC and/or the firewall firmware.