SONICWALL TECH NOTE:

# The Peer is Not Responding to Phase 1 ISAKMP Requests

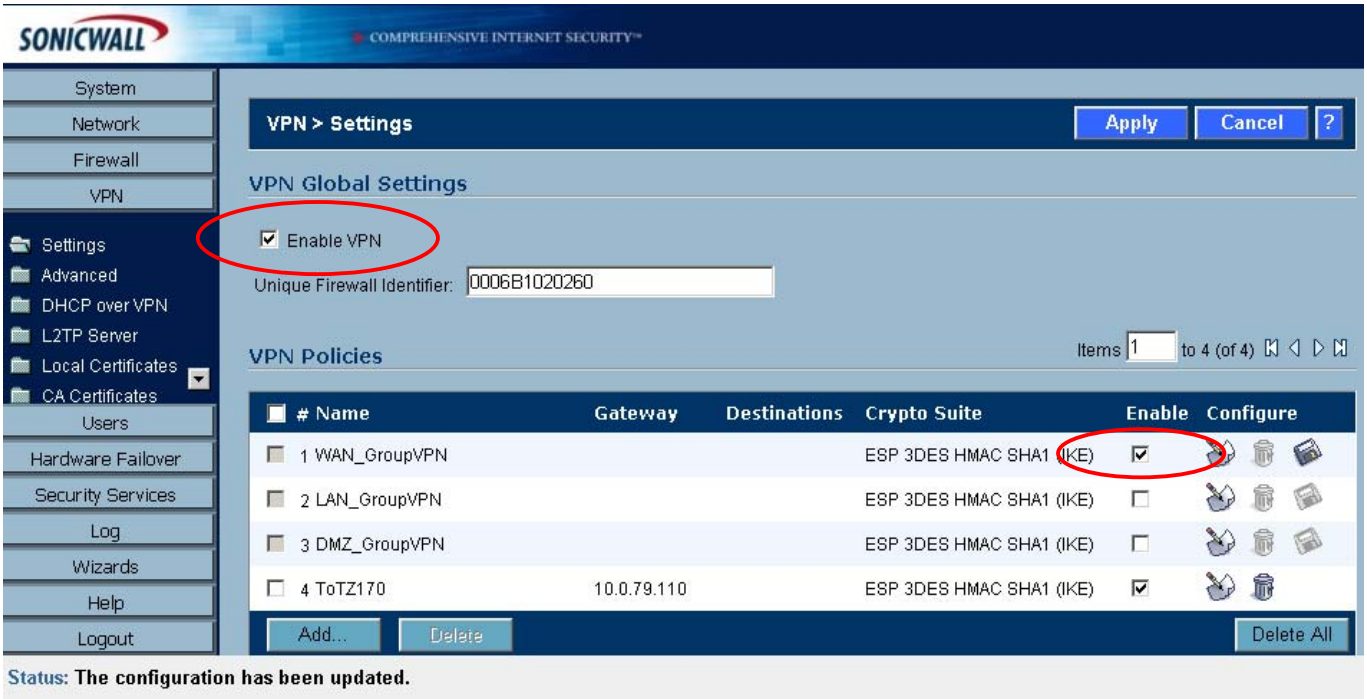
## Overview

This tech note provides information about the log entry "`The peer is not responding to phase 1 ISAKMP requests`" when using the Global VPN Client (GVC).

This message is a general failure message, meaning that a phase 1 ISAKMP request was sent to the peer firewall, but there was no response. There are many possible reasons why this could happen. Some of the more common reasons are discussed here, and some solutions are offered that may help solve the problem.

## Firewall is not Configured

One of the most common reasons why GVC cannot connect to a peer firewall is that the firewall has not been configured to accept GVC connections. SonicWALL firewalls use the GroupVPN policy to allow GVC to connect. Check the firewall VPN settings and verify VPN is enabled and GroupVPN policy is enabled as shown in Screenshot 1.




Screenshot 1: Enabling GroupVPN

## Wrong IP Address or Domain Name

Another reason the peer may not respond is that the peer does not exist. If the wrong IP address or domain name was entered for the peer, then there will be no response. Check with your network administrator to ensure the correct IP address or domain name was given and entered.

## Internet Connection is Down

Another reason the peer would not respond is that there is currently no way to reach the peer. The Internet connection may not be up. Follow these steps to ensure you have a good Internet connection:

1. From the DOS command line type "**ipconfig**" to make sure you have an IP address. If you don't have an IP address, you can't get to the Internet. If you have an IP address, go to Step 3. If not and you are using wireless go to Step 2 or contact your system administrator.

2. If you are using wireless, make sure your wireless connection is associated to your wireless access point with the correct SSID and that you have good signal strength. If your wireless device is WEP enabled, or has some other form of security in place, ensure those settings are correct.

3. Verify Internet access by browsing the web (for example, www.yahoo.com or www.google.com). If you can browse the web your Internet connection is alive and the DNS server is correctly resolving domain names. Go to Step 7.

4. If you cannot connect to a web address (Step 3), ping your default gateway. If you can't ping your default gateway, it is probably down. If your default gateway is down, contact your system administrator. An exception to this is if you are using a SonicWALL wireless device that has WiFiSec Enforcement enabled (see Step 6). In this case your pings will fail but your device may still be alive.

5. From the DOS command line type "**nslookup**" to make sure you can resolve domain names to IP addresses (for example: 'nslookup www.sonicwall.com'). If you see a "Name:" / "Address:" pair returned, the name was properly resolved. If you get 'Non-existent domain' returned, the name was not properly resolved and may be incorrect. If you get 'DNS request timed out', you DNS server(s) didn't respond and your Internet connection may be down.

6. If you're using a SonicWALL wireless device that has WiFiSec Enforcement enabled, make sure you set up a GVC connection to your default gateway before you try to connect to an external firewall.

7. If the Internet access is working and you still cannot connect, check the logs on the GVC and firewall. The GVC log will indicate "`Starting ISAKMP Phase 1 negotiation`" and the firewall log will indicate "`IKE Responder: Received Aggressive Mode request (Phase 1)`". If you only see the GVC log and not the firewall log, then the ISAKMP packet is not getting to the firewall. Contact you network administrator.

## Behind Unfriendly Device

Sometimes when you have an Internet connection and you still cannot reach the peer, it's because there is a Network Address Translation (NAT) device or a firewall in the middle that is blocking your ISAKMP packets.

It is sometimes difficult to know if you are behind a NAT device. Some general rules of thumb are:

- If you are in a hotel, Internet café or other public place, chances are you are behind a NAT device
- If your IP address (found by running the 'ipconfig' command) is 10.x.x.x or 192.x.x.x or 172.x.x.x, you've been given a private IP address and must be behind a NAT device to reach the Internet
- If you have several computers at home and they all connect through the same cable modem or DSL Internet connection, you're probably behind a NAT device

To know for sure if you are behind a NAT device, run the 'ipconfig' command and make note of the IP address specified. Thenopen the following link in your web browser: http://www.myipaddress.org If the IP address listed there is different than the one output from the 'ipconfig' command, you are behind a NAT device.

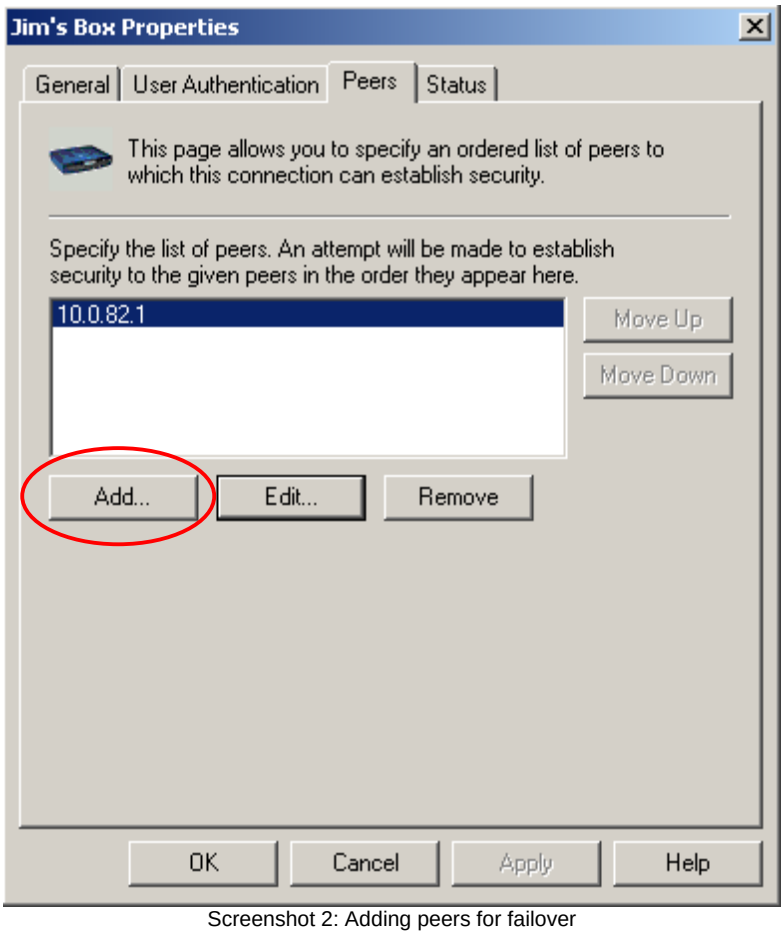
Determining if you are behind a firewall is more difficult. Generally speaking, however, most devices today that perform NAT also act as firewalls. Likewise, most firewalls are capable of performing NAT.

If you are behind a device that blocks all ISAKMP packets, there is little that can be done. Contact the administrator of the device to ensure that the device is properly configured to allow ISAKMP packets through.

## Peer is Unavailable

Sometimes the peer you are trying to connect to is just not available. Contact your network administrator to check on the status of the device. Also, you can add failover peers to your connection settings. If one peer does not respond, the next one in the list will be attempted. You can specify up to five peers.

To add failover peers to your connection, select the Connection in GVC and then select **File -> Properties**. Select the **Peers** tab. From there choose **Add** to add another peer to the list as shown in Screenshot 2.




Screenshot 2: Adding peers for failover

## Conclusion

There are many reasons why the Global VPN Client would not be able to connect to a specified peer firewall. The most common causes have been listed here. If you've never connected to the peer before, it's likely the IP or DNS name is incorrect, or even that your firewall has not been properly configured. If you connect on a regular basis but are in a new location when the failure occurs, it's likely you don't have a good Internet connection or some device is blocking ISAKMP traffic.

Some solutions to these common problems have been presented here. If you are still experiencing difficulty, contact your network administrator.