QuickVPN Troubleshooting Guide

First thing we need to make sure is that both the QuickVPN software client and the Small Business router's firmware are up to latest versions. This is a must before we attempt to connect or any type of troubleshooting can be done, to find these latest versions please visit our website www.cisco.com

If your clients have different router brands on the remote side trying to connect please make sure they are up to their latest firmware respectively. If it is a Consumer Cisco Linksys router please visit http://home.cisco.com to find their latest firmwares.

The Client that is trying to connect must have administrative rights otherwise the connection may not establish. QuickVPN also has issues with pirated copies of Windows, we strongly suggest if QuickVPN access is imperative for your business that you are running a legitimate copy of Windows OS, otherwise problems may occur that we cannot support.

When it comes to MAC users, unfortunately QuickVPN software client is not compatible there are other clients that may work but we do not offer support for them, please refer to this link for more information https://supportforums.cisco.com/docs/DOC-10266

When it comes to Wireless Broadband from cell phone carriers ***Verizon, ATT, Sprint, ETC*** the results have been hit or miss they either work or they don't mainly because of the connection the carriers are offering and their core router's firewalls that don't support VPN handshake negotiation as well as ports being un-blocked. Due to the inconsistency of this issue and if this is your case then we suggest visiting our Cisco Support Community https://supportforums.cisco.com/index.jspa where you might be able to find a solution on the forums, however at this time Cisco Small Business Support Center does not support air card issues.

If you have installed two NIC cards on the client's computer QuickVPN might try to utilize the connection that does not have an IP address assigned, simply disable the adapter that is not being used. This might also happen when being connected wirelessly and via Ethernet at the same time, if you are not using an adapter we simply recommend you disable it.

On the routers firewall please enable multicast pass-through, disable block WAN requests and enable https remote management and leave it in its default port.

Please make sure that VPN Pass-Through is enabled for IPSEC. Make sure that the router on the client's side also supports VPN connections. A good way to test this is to connect directly to the client's ISP modem and see if the tunnel establishes first and then try it behind the router.

On the RV120W or SA5XX Series it is mandatory to enable remote management for QuickVPN to work. Also for the RV120W make sure you disable the block fragmented packets feature or QuickVPN may not work.

If you are using port forwarding for the following ports **50, 51, 443, 60443, 500, 4500** then QuickVPN may not work, you can optionally use secondary ports for the same service protocols if you need to port forward them to your servers so QuickVPN can still use the primary ports and not create a conflict.

QuickVPN software has a built in log system with basic information so that anytime you want to perform troubleshooting, please refer to the log.txt that can be found in the QuickVPN folder; **C:/Program Files/Cisco Small Business/QuickVPN/log.txt**

On some occasions we have noticed that not creating a client security certificate can affect whether the connection gets established or not. If QuickVPN does not work without creating the certificate then try generating a security certificate, this is usually an additional security method to authenticate with QuickVPN but in some instances it has been the reason for the tunnel not to establish all together. After all your clients have been created generate and export for client the file to the QuickVPN folder and copy paste the certificate which has an extension of **.PEM** export this file to your desktop first and then transfer the file to the QuickVPN folder is this order. **C:/Program Files/Cisco Small Business/QuickVPN/**

If you are using any other type of VPN client software including Cisco VPN Any Connect then Quick VPN may not work, please make sure you don't have any other active VPN software running or installed on your PC, before you attempt to make QuickVPN work.

In order for QuickVPN to work it is recommended you change the LAN IP address to a different subnet than 192.168.1.X as many devices come by default in that subnet. This will cause an IP conflict and the tunnel will not establish.

Your Cisco router must have a direct public IP address for QuickVPN to work, please check under the status tab and your internet connection type and make sure it has a public IP address and it is not behind another router. This issue is more common with DSL connections; if you are behind another router/modem you should request your ISP to turn it into bridge mode so our router can be the border router between your LAN and your ISP.

We also recommend you lower your WAN MTU settings down from the 1500 default to avoid packet fragmentation which can be an issue with QuickVPN, especially in other countries outside the USA. The best way to find this value is to you is your ISP and asks or you can optionally do an MTU test yourself: http://help.expedient.com/broadband/mtu_ping_test.shtml

If you are using Windows XP, you must disable the Windows Firewall or create an exception for QuickVPN and any associated QuickVPN files for it to go through and connect. Make sure you have any additional security software like antivirus or extra firewalls disabled to test QuickVPN. If you are using **Windows Vista or Windows 7 the Windows firewall needs to be enabled** for QuickVPN to work properly.

In order for QuickVPN to work correctly please make sure that **IPsec Services & IKE Services** are started and running. To check these setting you can go **to start----run---services.msc** or from your **control panel---administrative tools----services**. If they are not started please start them manually and make sure they stay on.

The most common error message while trying to connect is the **Verifying Network….. Gateway Not Responding**, if you are getting this far but you are still getting this message we need to focus on several ports that could be being blocked by your ISP these ports are **50, 51, 443, 60443, 500, 4500** these ports have to be open in both sides client and router for the tunnel to establish successfully. In order to find out if these ports are being blocked we need to perform a port scan, we want to do this directly connected to your ISP modem if possible, if that can't be arranged then we would have to disable the routers firewall completely off before performing these scans.

Once we have that set up we can go to **www.grc.com-----services----Shields UP---proceed----all service ports.** This will begin a complete scan of all service port and tell us whether they are closed or opened and we need these specific ports to be opened. In some occasions you will receive a green stealth mode status which basically means your ISP is filtering traffic through these ports for security reasons. If this is the case you can perform another test this one will be done from the outside of your network.

You will need to download a program called Nmap http://www.nmap.org which is free and install it on a location outside your network, you can then perform a scan of your network and it will tell you with more precision if the ports are being closed, once installed you can us the following command **Nmap -sS -sU -p 500 –Pn 71.7.134.80 (Public IP Address)** this will tell you if the ports are being blocked. Unfortunately most ISP tier 1 support is adamant in proclaiming that all of the service ports are already open and they will not hesitate to tell you that all service ports are opened and that they do not block any ports and that the problem is our router. This may be true in ***some very few*** instances but if the port scan test results show otherwise you will need to insist on showing them a proof of the port scans and demand to speak to **tier 2 support/advanced support**.

After making sure that you have done all of the above mentioned steps and confirmed that none apply to your situation we can perform advanced troubleshooting with tier 2 support and analyze an advanced packet analysis to determine where the connection is being blocked and why it fails to connect, simply contact our **Small Business Support Center** at **1-866-606-1866**