TheGreenBow IPSec VPN Client
Configuration Guide
Qno QVM660

WebSite:  http://www.thegreenbow.com
Contact:  support@thegreenbow.com
Table of contents

1 Introduction .................................................................................................................................................... 3
1.1 Goal of this document ............................................................................................................................ 3
1.2 VPN Network topology ........................................................................................................................... 3
1.3 Qno QVM660 Restrictions .................................................................................................................... 3
1.4 Qno QVM660 VPN Gateway .................................................................................................................. 3
1.5 Qno QVM660 VPN Gateway product info .............................................................................................. 3

2 Qno QVM660 VPN configuration ................................................................................................................... 4

3 TheGreenBow IPSec VPN Client configuration ............................................................................................. 7
3.1 VPN Client Phase 1 (IKE) Configuration ................................................................................................ 7
3.2 VPN Client Phase 2 (IPSec) Configuration ............................................................................................. 9
3.3 Open IPSec VPN tunnels ....................................................................................................................... 9

4 Tools in case of trouble ................................................................................................................................ 11
4.1 A good network analyser: wireshark .................................................................................................... 11

5 VPN IPSec Troubleshooting ......................................................................................................................... 12
5.1 « PAYLOAD MALFORMED » error (wrong Phase 1 [SA]) .................................................................. 12
5.2 « INVALID COOKIE » error .................................................................................................................. 12
5.3 « no keystate » error ............................................................................................................................ 12
5.4 « received remote ID other than expected » error ................................................................................ 12
5.5 « NO PROPOSAL CHOSEN » error ..................................................................................................... 13
5.6 « INVALID ID INFORMATION » error ................................................................................................. 13
5.7 I clicked on “Open tunnel”, but nothing happens .................................................................................. 13
5.8 The VPN tunnel is up but I can’t ping ! ................................................................................................. 13

6 Contacts ....................................................................................................................................................... 15
1 Introduction

1.1 Goal of this document

This configuration guide describes how to configure TheGreenBow IPSec VPN Client with a Qno VPN router.

1.2 VPN Network topology

In our VPN network example (diagram hereafter), we will connect TheGreenBow IPSec VPN Client to the LAN behind the Qno router. The VPN client is connected to the Internet with a DSL connection or through a LAN. All the addresses in this document are given for example purpose.

1.3 Qno QVM660 Restrictions

No known restriction.

1.4 Qno QVM660 VPN Gateway

Our tests and VPN configuration have been conducted with Qno QVM660 firmware release 2.0.14.6RC2-Qno.

1.5 Qno QVM660 VPN Gateway product info

It is critical that users find all necessary information about Qno QVM660 VPN Gateway. All product info, User Guide and knowledge base for the Qno QVM660 VPN Gateway can be found on the Qno website: www.qno.com.tw/english/

2 Qno QVM660 VPN configuration

This section describes how to build an IPSec VPN configuration with your Qno QVM660 VPN router. First step would be to login and go to ‘VPN’ menu and then “Summary” to configure your router.

Click on “Add New Tunnel” for a new tunnel or “Edit” for an existing tunnel.

Then, select the type of VPN tunnel i.e. “Client to Gateway” you need to create.
In ‘Local Group Setup’ section, please select ‘Domain Name (FQDN) Authentication’ and the ‘Domain Name’ you’ve configured to reach your gateway. On the LAN side, select ‘Subnet’ type.

In ‘Remote Client Group’ section, you need to select ‘E-mail (User FQDN) Authentication’.

Those parameters will be required in TheGreenBow IPSec VPN Client software.
In the ‘IPSec Setup’ section, we need to select parameters for Phase1 and Phase2 as well as the Preshared Key ("123456") and Aggressive Mode. Those parameters will be required into IKE Parameters (Phase 1) and ESP Parameters (Phase 2) in TheGreenBow IPSec VPN Client software.

Then click on “Apply”.

Now you’ve completed the configuration of the Qno QVM660 VPN router.
3 TheGreenBow IPSec VPN Client configuration

This section describes the required configuration to connect to a QNO QVM660 VPN router.

To download the latest release of TheGreenBow IPSec VPN Client software, please go to http://www.thegreenbow.com/vpn_down.html.

3.1 VPN Client Phase 1 (IKE) Configuration

The remote VPN Gateway IP address is either an explicit IP address, or a DNS Name.

So, here you find the same parameters as in "IPSec Setup" in the router (IKE, preshared key).

The ‘Remote Gateway’ shall match the ‘Local Security Gateway Type’ in the Qno QVM660 VPN router under the “Local Group Setup” section.

Then click on ‘P1 Advanced’.
Don’t forget to set ‘NAT-T’ to ‘Automatic’ and to select ‘Aggressive Mode’ as selected it in the Qno QVM660 VPN router.

The Local ID in the VPN Client shall match the ‘Remote Client Setup’ in the Qno QVM660 VPN router.

Click on “Ok”.

Now you’ve completed configuration of the Phase 1.
3.2 VPN Client Phase 2 (IPSec) Configuration

You may define a static virtual IP address here.
If you use 0.0.0.0, you will have error “Local-ID” is missing. It does not prevent you from establishing a tunnel.

Enter the IP address (and subnet mask) of the remote LAN.

Phase 2 Configuration

The part ESP shall match the Phase2 group in the Qno QVM660 VPN router.

3.3 Open IPSec VPN tunnels

Once both Qno QVM660 router and TheGreenBow IPSec VPN Client software have been configured accordingly, you are ready to open VPN tunnels. First make sure you enable your firewall with IPSec traffic.

1. Click on “Save & Apply” to take into account all modifications we’ve made on your VPN Client configuration
2. Click on “Open Tunnel”, or generate traffic that will automatically open a secure IPSec VPN Tunnel (e.g. ping, IE browser)
3. Select “Connections” to see opened VPN Tunnels
4. Select “Console” if you want to access to the IPSec VPN logs and adjust filters to display less IPSec messaging. The following example shows a successful connection between TheGreenBow IPSec VPN Client and the Qno QVM660 VPN router.
4 Tools in case of trouble

Configuring an IPSec VPN tunnel can be a hard task. One missing parameter can prevent a VPN connection from being established. Some tools are available to find source of troubles during a VPN establishment.

4.1 A good network analyser: wireshark

Wireshark is a free software that can be used for packet and traffic analysis. It shows IP or TCP packets received on a network card. This tool is available on website http://www.wireshark.org/. It can be used to follow protocol exchange between two devices. For installation and use details, read its specific documentation.
5 VPN IPSec Troubleshooting

5.1 « PAYLOAD MALFORMED » error (wrong Phase 1 [SA])

If you have an « PAYLOAD MALFORMED » error you might have a wrong Phase 1 [SA], check if the encryption algorithms are the same on each side of the VPN tunnel.

5.2 « INVALID COOKIE » error

If you have an « INVALID COOKIE » error, it means that one of the endpoint is using a SA that is no more in use. Reset the VPN connection on each side.

5.3 « no keystate » error

Check if the preshared key is correct or if the local ID is correct (see « Advanced » button). You should have more information in the remote endpoint logs.

5.4 « received remote ID other than expected » error

The « Remote ID » value (see « Advanced » Button) does not match what the remote endpoint is expected.
5.5 « NO PROPOSAL CHOSEN » error

If you have an « NO PROPOSAL CHOSEN » error, check that the « Phase 2 » encryption algorithms are the same on each side of the VPN Tunnel.

Check « Phase 1 » algorithms if you have this:

5.6 « INVALID ID INFORMATION » error

If you have an « INVALID ID INFORMATION » error, check if « Phase 2 » ID (local address and network address) is correct and match what is expected by the remote endpoint.

Check also ID type ("Subnet address" and "Single address"). If network mask is not check, you are using a IPV4_ADDR type (and not a IPV4_SUBNET type).

5.7 I clicked on “Open tunnel”, but nothing happens.

Read logs of each VPN tunnel endpoint. IKE requests can be dropped by firewalls. An IPSec Client uses UDP port 500 and protocol ESP (protocol 50).

5.8 The VPN tunnel is up but I can’t ping !

If the VPN tunnel is up, but you still cannot ping the remote LAN, here are a few guidelines:

- Check Phase 2 settings: VPN Client address and Remote LAN address. Usually, VPN Client IP address should not belong to the remote LAN subnet
- Once VPN tunnel is up, packets are sent with ESP protocol. This protocol can be blocked by firewall. Check that every device between the client and the VPN server does accept ESP
- Check your VPN server logs. Packets can be dropped by one of its firewall rules.
- Check your ISP support ESP
• If you still cannot ping, follow ICMP traffic on VPN server LAN interface and on LAN computer interface (with Wireshark for example). You will have an indication that encryption works.
• Check the “default gateway” value in VPN Server LAN. A target on your remote LAN can receive pings but does not answer because there is a no “Default gateway” setting.
• You cannot access to the computers in the LAN by their name. You must specify their IP address inside the LAN.
• We recommend you to install wireshark (http://www.wireshark.org) on one of your target computer. You can check that your pings arrive inside the LAN.
6 Contacts

News and updates on TheGreenBow web site: http://www.thegreenbow.com

Technical support by email at support@thegreenbow.com

Sales contacts by email at sales@thegreenbow.com