TheGreenBow IPSec VPN Client
Configuration Guide
NetGear FVS318 (v3)

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

1 Introduction ................................................................................................................... 0
  1.1 Goal of this document ............................................................................................... 0
  1.2 VPN Network topology ............................................................................................. 0
  1.3 NetGear FVS318v3 Restrictions ............................................................................... 0
  1.4 NetGear FVS318v3 VPN Gateway .......................................................................... 0
2 NetGear FVS318v3 VPN configuration ........................................................................... 0
3 TheGreenBow IPSec VPN Client configuration ............................................................... 0
  3.1 VPN Client Phase 1 (IKE) Configuration ................................................................. 0
  3.2 VPN Client Phase 2 (IPSec) Configuration ............................................................... 0
  3.3 Open IPSec VPN tunnels......................................................................................... 0
4 Tools in case of trouble ................................................................................................. 0
  4.1 A good network analyser: ethereal ........................................................................... 0
5 VPN IPSec Troubleshooting .......................................................................................... 0
  5.1 « PAYLOAD MALFORMED » error (wrong Phase 1 [SA])........................................ 0
  5.2 « INVALID COOKIE » error ..................................................................................... 0
  5.3 « no keystate » error ............................................................................................... 0
  5.4 « received remote ID other than expected » error ..................................................... 0
  5.5 « NO PROPOSAL CHOSEN » error ......................................................................... 0
  5.6 « INVALID ID INFORMATION » error ..................................................................... 0
  5.7 I clicked on “Open tunnel”, but nothing happens ..................................................... 0
  5.8 The VPN tunnel is up but I can’t ping ! ................................................................... 0
6 Contacts ..................................................................................................................... 0
1 Introduction

1.1 Goal of this document
This configuration guide describes how to configure TheGreenBow IPSec VPN Client with a NetGear ProSafe VPN Firewall FVS318 v3 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 NetGear 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 NetGear FVS318 v3 Restrictions
No Known restrictions.

1.4 NetGear FVS318 v3 VPN Gateway
Our tests and VPN configuration have been conducted with NetGear FVS318 v3 firmware release version v3.0_19.
2 NetGear FVS318 VPN configuration

This section describes how to build an IPSec VPN configuration with your NetGear FVS318 VPN router. Once connected to your VPN gateway, you must select “VPN WIZARD” under “VPN” tab then click “Next”. You need to setup the connection name and the pre shared key. You must select “A remote VPN client”.

Step 1 of 3: Connection Name, Connection type and Pre-Shared Key

What is the new Connection Name? TheGreenBow
What is the pre-shared key? abcdefgh
This VPN tunnel will connect to:
- A remote VPN Gateway
- A remote VPN client

To modify the default phase 1 local and remote IDs, select “IKE Policies” under “VPN” tab, click “Edit” then update “Local Identity Data” and “Remote Identity Data” fields.
You must specify the IP address of the client. Select "VPN Policies" under "VPN" tab then click "Edit". Select "Single address" for "Remote IP" and put the client virtual address in the "Start IP address" field.

<table>
<thead>
<tr>
<th>General</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy Name</td>
</tr>
<tr>
<td>IKE policy</td>
</tr>
<tr>
<td>Remote VPN Endpoint</td>
</tr>
<tr>
<td>Address Data</td>
</tr>
<tr>
<td>SA Life Time</td>
</tr>
<tr>
<td>0</td>
</tr>
<tr>
<td>IPSec PFS</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Traffic Selector</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local IP</td>
</tr>
<tr>
<td>Start IP address</td>
</tr>
<tr>
<td>Finish IP address</td>
</tr>
<tr>
<td>Subnet Mask</td>
</tr>
<tr>
<td>Remote IP</td>
</tr>
<tr>
<td>Start IP address</td>
</tr>
<tr>
<td>Finish IP address</td>
</tr>
<tr>
<td>Subnet Mask</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>AH Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Authentication</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ESP Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Encryption</td>
</tr>
<tr>
<td>Enable Authentication</td>
</tr>
</tbody>
</table>

| NETBIOS Enable |
3 TheGreenBow IPSec VPN Client configuration

3.1 VPN Client Phase 1 (IKE) Configuration

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

In “Advanced” window, select “Aggressive Mode” and fill “Local ID” and “Remote ID” with the mirror values set on the router.
### 3.2 VPN Client Phase 2 (IPSec) Configuration

![Phase 2 Configuration](image)

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

### 3.3 Open IPSec VPN tunnels

Once both NetGear FVS318 v3 router and TheGreenBow IPSec VPN Client have been configured accordingly, you are ready to open VPN tunnels.

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.
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: ethereal

Ethereal 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 tools is available on website http://www.ethereal.com/. 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

115911 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode [SA][VID]
115913 Default (SA CNXVPN1-P1) RECV phase 1 Main Mode [SA][VID]
115915 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode [KEY][NONCE]
115915 Default (SA CNXVPN1-P1) RECV phase 1 Main Mode [KEY][NONCE]
115915 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode [ID][HASH][NOTIFY]
115915 Default (SA CNXVPN1-P1) RECV phase 1 Main Mode [ID][HASH][NOTIFY]
115915 Default phase 1 done: initiator id c364cd70: 195.100.205.112, responder id c364cd72: 195.100.205.114, src: 195.100.205.112 dst: 195.100.205.114
115915 Default (SA CNXVPN1-CNXVPN1-P2) SEND phase 2 Quick Mode [SA][KEY][ID][HASH][NONCE]
115915 Default RECV Informational [HASH][NOTIFY] with NO_PROPOSAL_CHOSEN error
115915 Default CNXVPN1-P1 deleted

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:

115911 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode [SA][VID]
115911 Default RECV Informational [NOTIFY] with NO_PROPOSAL_CHOSEN error

5.6 « INVALID ID INFORMATION » error

122623 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode [SA][VID]
122625 Default (SA CNXVPN1-P1) RECV phase 1 Main Mode [SA][VID]
122625 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode [KEY][NONCE]
122626 Default (SA CNXVPN1-P1) RECV phase 1 Main Mode [KEY][NONCE]
122626 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode [ID][HASH][NOTIFY]
122626 Default (SA CNXVPN1-P1) RECV phase 1 Main Mode [ID][HASH][NOTIFY]
122626 Default phase 1 done: initiator id c364cd70: 195.100.205.112, responder id c364cd72: 195.100.205.114, src: 195.100.205.112 dst: 195.100.205.114
122626 Default (SA CNXVPN1-CNXVPN1-P2) SEND phase 2 Quick Mode [SA][KEY][ID][HASH][NONCE]
122626 Default RECV Informational [HASH][NOTIFY] with INVALID_ID_INFORMATION error
122626 Default CNXVPN1-P1 deleted

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 Ethereal 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 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 ethereal (http://www.ethereal.com) 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 at +33 1 43 12 39 37 or by email at info@thegreenbow.com