Table of contents

1  Introduction .................................................................................................................................................... 3
1.1  Goal of this document ............................................................................................................................ 3
1.2  VPN Network topology .................................................................................................................................. 3
1.3  Netgear FVS114 Restrictions..................................................................................................................... 3
1.4  Netgear FVS114 VPN Gateway ............................................................................................................. 3
1.5  Netgear FVS114 VPN Gateway product info ......................................................................................... 3
2  Netgear FVS114 VPN configuration ............................................................................................................. 4
3  TheGreenBow IPSec VPN Client configuration ............................................................................................. 8
3.1  VPN Client Phase 1 (IKE) Configuration ................................................................................................ 8
3.2  VPN Client Phase 2 (IPSec) Configuration .......................................................................................... 10
3.3  Open IPSec VPN tunnels ..................................................................................................................... 10
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 software with a Netgear FVS114 VPN router to establish VPN connections for remote access to corporate network.

1.2 VPN Network topology

In our VPN network example (diagram hereafter), we will connect TheGreenBow IPSec VPN Client software to the LAN behind the Netgear FVS114 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 FVS114 Restrictions

No known restrictions.

1.4 Netgear FVS114 VPN Gateway

Our tests and VPN configuration have been conducted with Netgear FVS114 firmware release V1.1_10.

1.5 Netgear FVS114 VPN Gateway product info

All product info, User Guide and knowledge base for the Netgear FVS114 VPN Gateway can be found on the Netgear website: http://www.netgear.com/

<table>
<thead>
<tr>
<th>Netgear FVS114 Product page</th>
<th><a href="http://kb.netgear.com/app/products/model/a_id/2419">http://kb.netgear.com/app/products/model/a_id/2419</a></th>
</tr>
</thead>
<tbody>
<tr>
<td>Netgear FVS114 FAQ/Knowledge Base</td>
<td><a href="http://kb.netgear.com/app/products/model/a_id/2419">http://kb.netgear.com/app/products/model/a_id/2419</a></td>
</tr>
</tbody>
</table>
2 Netgear FVS114 VPN configuration

This section describes how to build an IPSec VPN configuration with your Netgear FVS114 VPN router. Once connected to your Netgear FVS114 VPN gateway, select “VPN” and “IKE Policies” tabs. Click on “Add” to create an IKE Policy.
In this configuration, we've selected the Aggressive Mode and chose for the local ID (fvx_local.com) and Remote ID (fvx_remote.com) an FQDN Identifier (it shall match respectively to Remote ID and Local ID for the VPN Client software).

Also, we set a Preshared Key (1234567890) and chose the different algorithms for IKE (i.e. 3DES, SHA which shall match the IKE part in Phase 1 of the VPN Client software).

Click on “Apply” once you finished configuring “IKE Policies”.

### IKE Policy Configuration

<table>
<thead>
<tr>
<th>General</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy Name</td>
<td>Gateway1</td>
</tr>
<tr>
<td>Direction/Type</td>
<td>Responder</td>
</tr>
<tr>
<td>Exchange Mode</td>
<td>Aggressive Mode</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Local</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Local Identity Type</td>
<td>Fully Qualified Domain Name</td>
</tr>
<tr>
<td>Local Identity Data</td>
<td>fvs_local</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Remote</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote Identity Type</td>
<td>Fully Qualified Domain Name</td>
</tr>
<tr>
<td>Remote Identity Data</td>
<td>fvs_remote</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>IKE SA Parameters</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Encryption Algorithm</td>
<td>3DES</td>
</tr>
<tr>
<td>Authentication Algorithm</td>
<td>SHA-1</td>
</tr>
<tr>
<td>Authentication Method</td>
<td>Pre-shared Key</td>
</tr>
<tr>
<td>Diffie-Hallman (DH) Group</td>
<td>Group 2 (1024 Bit)</td>
</tr>
<tr>
<td>SA Life Time</td>
<td>23000 (secs)</td>
</tr>
</tbody>
</table>

[Apply]
Go to the tab “VPN” and “VPN Policies”.
Click on “Add Auto Policy” to create a VPN Policy.
In VPN – Auto policy, we’ve configured an IP for Remote VPN Endpoint. Which should match Remote IP configuration and as well as “VPN client address” in VPN Client.

Local IP range is the LAN subnet of FVS114.

Click on “Apply” once you finished configuring “VPN Policies”.

---

**VPN - Auto Policy**

**General**
- Policy Name: Remot1
- IKE policy: Gateway1
- IKE Keep Alive
- Remote VPN Endpoint
- Address Type: IP Address
- Address Data: 192.168.10.1
- SA Life Time: 86400 (Seconds)
- 0 (Kbytes)
- IPSec PFS
- PFS Key Group: Group 2 (1024 Bit)
- NetBIOS Enable

**Traffic Selector**
- Local IP
  - Subnet address
  - Start IP address: 192.168.0.0
  - Finish IP address: 0.0.0.0
  - Subnet Mask: 255.255.255.0
- Remote IP
  - Single address
  - Start IP address: 192.168.10.0
  - Finish IP address: 0.0.0.0
  - Subnet Mask: 0.0.0.0

**AH Configuration**
- Enable Authentication
- Authentication Algorithm: MD5

**ESP Configuration**
- Enable Encryption
- Encryption Algorithm: 3DES
- Enable Authentication
- Authentication Algorithm: SHA-1

**Buttons:**
- Back
- Apply
- Cancel
3 TheGreenBow IPSec VPN Client configuration

This section describes the required configuration to connect to a Netgear FVS114 VPN router via VPN connections.

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

![Phase 1 Configuration](image)

You may use Preshared key or Certificates for User Authentication with the Netgear FVS114 router. This configuration is one example of what can be accomplished in term of User Authentication. You may want to refer to either the Netgear FVS114 router user guide or TheGreenBow IPSec VPN Client software User Guide for more details on User Authentication options.
Phase 1 Advanced configuration
3.2 VPN Client Phase 2 (IPSec) Configuration

![Phase 2 Configuration](image)

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

VPN Client Virtual IP address

3.3 Open IPSec VPN tunnels

Once both Netgear FVS114 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 a Netgear FVS114 VPN router.

```
2011-02-21 13:41:35 Default (Sa Gateway 1 P1) SEND phase 1 Aggressive Mode 
2011-02-21 13:41:35 Default (Sa Gateway 1 P1) RECV phase 1 Aggressive Mode 
2011-02-21 13:41:35 Default (Sa Gateway 1 P1) SEND phase 1 Aggressive Mode [HASH] [FA] [KEY_EXCH] [NONCE] [ID] [ID] 
2011-02-21 13:41:35 Default (Sa Gateway 1 P1) SEND phase 1 Aggressive Mode [HASH] [FA] [KEY_EXCH] [NONCE] [ID]
2011-02-21 13:41:35 Default (Sa Gateway 1 P1) SEND phase 2 Quick Mode [HASH] [FA] [KEY_EXCH] [NONCE] [ID] [ID] 
2011-02-21 13:41:35 Default (Sa Gateway 1 P1) SEND phase 2 Quick Mode [HASH]
```
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 (http://www.wireshark.org/docs/).
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

<table>
<thead>
<tr>
<th>Line 1</th>
<th>Default (SA CNXVPN1-P1) SEND phase 1 Main Mode [SA][VID]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Line 2</td>
<td>Default (SA CNXVPN1-P1) RECV phase 1 Main Mode [SA][VID]</td>
</tr>
<tr>
<td>Line 3</td>
<td>Default (SA CNXVPN1-P1) SEND phase 1 Main Mode [KEY][NONCE]</td>
</tr>
<tr>
<td>Line 4</td>
<td>Default (SA CNXVPN1-P1) RECV phase 1 Main Mode [KEY][NONCE]</td>
</tr>
<tr>
<td>Line 5</td>
<td>Default (SA CNXVPN1-P1) SEND phase 1 Main Mode [ID][HASH][NOTIFY]</td>
</tr>
<tr>
<td>Line 6</td>
<td>Default (SA CNXVPN1-P1) RECV phase 1 Main Mode [ID][HASH][NOTIFY]</td>
</tr>
<tr>
<td>Line 7</td>
<td>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</td>
</tr>
<tr>
<td>Line 8</td>
<td>Default (SA CNXVPN1-CNXVPN1-P2) SEND phase 2 Quick Mode [SA][KEY][ID][HASH][NONCE]</td>
</tr>
<tr>
<td>Line 9</td>
<td>Default RECV Informational [HASH][NOTIFY] with NO_PROPOSAL_CHOSEN error</td>
</tr>
<tr>
<td>Line 10</td>
<td>Default CNXVPN1-P1 deleted</td>
</tr>
</tbody>
</table>

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:

| Line 1 | Default (SA CNXVPN1-P1) SEND phase 1 Main Mode [SA][VID] |
| Line 2 | Default RECV Informational [NOTIFY] with NO_PROPOSAL_CHOSEN error |

### 5.6 « INVALID ID INFORMATION » error

| Line 1 | Default (SA CNXVPN1-P1) SEND phase 1 Main Mode [SA][VID] |
| Line 2 | Default (SA CNXVPN1-P1) RECV phase 1 Main Mode [SA][VID] |
| Line 3 | Default (SA CNXVPN1-P1) SEND phase 1 Main Mode [KEY][NONCE] |
| Line 4 | Default (SA CNXVPN1-P1) RECV phase 1 Main Mode [KEY][NONCE] |
| Line 5 | Default (SA CNXVPN1-P1) SEND phase 1 Main Mode [ID][HASH][NOTIFY] |
| Line 6 | Default (SA CNXVPN1-P1) RECV phase 1 Main Mode [ID][HASH][NOTIFY] |
| Line 7 | 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 |
| Line 8 | Default (SA CNXVPN1-CNXVPN1-P2) SEND phase 2 Quick Mode [SA][KEY][ID][HASH][NONCE] |
| Line 9 | Default RECV Informational [HASH][NOTIFY] with INVALID_ID_INFORMATION error |
| Line 10| Default RECV Informational [HASH][DEL] |
| Line 11| 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 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](http://www.thegreenbow.com)

Technical support by email at support@thegreenbow.com

Sales contacts by email at sales@thegreenbow.com
Secure, Strong, Simple.
TheGreenBow Security Software