TheGreenBow
Linux VPN Client

User Guide
# Table of Contents

1  Presentation ........................................................................................................................................... 3  
1.1  TheGreenBow VPN Client .............................................................................................................. 3  
1.2  TheGreenBow VPN Client features ................................................................................................. 3  

2  Software ................................................................................................................................................. 4  
2.1  Installation ..................................................................................................................................... 4  
2.2  Activation ....................................................................................................................................... 4  
2.3  Installation ..................................................................................................................................... 4  
2.4  Uninstallation ................................................................................................................................. 4  

3  User Interface ......................................................................................................................................... 5  
3.1  Overview ........................................................................................................................................ 5  
3.2  Login ............................................................................................................................................... 5  
3.3  Connections ................................................................................................................................... 6  
3.4  IPsec ............................................................................................................................................... 7  
3.5  Certificates ................................................................................................................................... 11  
3.6  Logs .............................................................................................................................................. 13  
3.7  System .......................................................................................................................................... 14  

4  Contact ................................................................................................................................................. 15  

5  Annex .................................................................................................................................................... 16  
5.1  TheGreenBow VPN Client specifications ..................................................................................... 16  
5.2  FAQ / Troubleshooting ................................................................................................................ 17
1 Presentation

1.1 TheGreenBow VPN Client

TheGreenBow Linux VPN Client is a VPN Client software designed for Linux workstations.

It enables to establish secure connections between the user device and the Information System of the company.

TheGreenBow VPN Client for Linux enables to open VPN connections with any VPN Gateways (see the list of qualified VPN gateways). TheGreenBow VPN Client implements IPsec, IKE V1, IKEV2 standards to be compatible with all VPN Gateways.

![Diagram of a network connection]

For most VPN gateways on the market, TheGreenBow provides a configuration guide. To configure your VPN gateway, see the list of configuration guides of VPN gateways.

1.2 TheGreenBow VPN Client features

TheGreenBow VPN Client provides the following features:

- Ability to support network in IPv4 and IPv6 simultaneously
- Ability to create IPsec VPN tunnel using either IKEv1 or IKEv2
- Multiple VPN tunnels
- VPN Tunnel on all media types: Ethernet, WiFi, 3G, satellite
- Certificate management
- "DPD" (Dead Peer Detection) features
- Mode config (IKEv1) and Mode CP (IKEv2) management
- Intuitive and powerful graphical interface

See chapter "TheGreenBow VPN Client specifications".
2 Software

2.1 Installation

2.1.1 Installation files
TheGreenBow Linux VPN software is released through a “tgbvpn-client_x.x.x.tar.gz” file. This compressed package contains the following files:
- tgbvpn-client_x.x.x.i386.deb => main installation file for TheGreenBow VPN
- INSTALL => instructions to install the software
- install.sh => script for an automated installation

Please use the following command to uncompress these files:
```
tar -zxvf tgbvpn-client_x.x.x.tar.gz
```

2.1.2 Installation requirements
TheGreenbow Linux VPN client requires an i386 Debian 8 distribution. Any other version or distribution is not supported.

Note: TheGreenBow Linux VPN Client requires the following packages:
- Strongswan software (version 5.x)
- Node.js software (API version 0.12)
The installation script ("install.sh") automatically installs these two packages.
Therefore, the workstation on which are installed these packages must be connected to the Internet.

2.2 Activation
No activation is required for version 0.9.1.
This release expires by 12/31/2016.

2.3 Installation
Installation requires to be logged as "root".

Once logged as "root", execute: "./install.sh"

2.4 Uninstallation
Uninstallation requires to be logged as "root".

Once logged as "root", execute: "apt-get remove tgbvpn-client"

2.5 Test configuration
A test tunnel is available here: "/usr/share/doc/tgbvpn-client/tgbvpn_demo.tgb"
You can import it (see chapter 3.4.1.2) to check that TheGreenBow VPN client is operational. After the tunnel is open you should be able to ping 192.168.175.50 machine.
3 User Interface

3.1 Overview

The GreenBow Linux VPN Client comes together with an intuitive and powerful graphical interface.

The Linux VPN Client interface enables to:
- Open/Close VPN tunnels
- Manage and configure IPsec tunnels
- Manage and configure certificates
- View connection and application logs

3.2 Login

After the first installation, the GUI is protected with default login / password: "admin" / "admin".

It is recommended to change these login and password in the "System" tab (see chapter 3.7 "System")
3.3 Connections

The connection page enables to open and close tunnels. It also enables to view the connection status of tunnels.

Clicking on the tunnel name opens the configuration of the tunnel.

Click on the "OPEN" button to open the tunnel: The GUI shows the status of the opened tunnel.
3.4 IPsec

3.4.1 Tunnel list

![IPsec Tunnels](image)

### 3.4.1.1 IKE Daemon management
The IKE daemon status (green or red led) shows the daemon is running or idle. Some VPN issues may need to restart the IKE daemon. Use the "Stop" and "Restart" button to restart the IKE daemon.

### 3.4.1.2 Tunnel import
The IPsec configuration page enables to import TheGreenBow VPN Configuration file (".tgb" files).


**Notes:**
The algorithms "auto" of a VPN configuration are not imported. It is recommended to check before importing a configuration that it does not include such algorithms.
For PSK configurations, if local and remote ID are not specified, the remote ID is automatically filled with the gateway DNS name.

### 3.4.1.3 Tunnel list management
The tunnel list enables to edit, copy or delete any IPsec tunnels.
3.4.2 Tunnel Configuration

Phase 1 / IKE SA Parameters:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connection name</td>
<td>This is the name of the tunnel you are creating.</td>
</tr>
<tr>
<td>Local Endpoint</td>
<td>Select the physical interface to use to communicate with the gateway.</td>
</tr>
<tr>
<td>Authentication Method</td>
<td>2 methods are available: certificate or Preshared Key</td>
</tr>
<tr>
<td>Pre Shared Key</td>
<td>Password or key shared with the remote gateway. Note: The pre shared key is a simple way to configure a VPN tunnel. However, it provides less flexibility in the management of security than using certificates.</td>
</tr>
<tr>
<td>Certificates</td>
<td>Select the user certificate to use. User certificates should be imported first from the certificate tab. After you have selected a certificate, its subject reads just below.</td>
</tr>
</tbody>
</table>
| Local ID Type           | "Local ID" is the identifier of the Authentication phase (Phase 1 / IKE Auth) that the VPN Client sends to the remote VPN gateway. The Local Id Type can be:  
<p>|                         | - IPV4 address: e.g. 195.100.205.101                  |
|                         | - IPV6 address: e.g. 2000:2000:2000::101               |
|                         | - A domain name (type = DNS), e.g. gw.mydomain.net      |
|                         | - Email address (type = email), e.g. <a href="mailto:support@thegreenbow.com">support@thegreenbow.com</a> |
|                         | - Certificate Subject (type = DER ASN1 DN), this case is automatic as soon as the Authentication method is &quot;certificate&quot; |
|                         | - A string (type = KEY ID), e.g. 123456                 |
| Local Id                | Enter the Local Id value according to the type you selected. You can use %any to let the client decides itself the Id. But for Preshared key case at least one of the twoIds (either Local or Remote) has to be defined (both can’t be %any). |</p>
<table>
<thead>
<tr>
<th><strong>Remote Id type</strong></th>
<th>&quot;Remote ID&quot; is the identifier the VPN Client expects from the remote VPN gateway. Same types as &quot;Local Id&quot; are available.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Remote Id</strong></td>
<td>Enter the Remote Id value according to the type you selected. You can use %any if the client should accept any Gateway Id. But for Preshared key case at least one of the two Ids (Local or Remote) has to be defined (both can’t be %any).</td>
</tr>
<tr>
<td><strong>Encryption algorithm</strong></td>
<td>Encryption algorithm used during Authentication phase: 3DES, AES-128, AES-192, AES-256.</td>
</tr>
<tr>
<td><strong>Hash algorithm</strong></td>
<td>Authentication algorithm used during Authentication phase: MD5, MD5_160, SHA1, SHA1_160, SHA2-256, SHA2-384, SHA2-512.</td>
</tr>
<tr>
<td><strong>Diffie-Hellman algorithm</strong></td>
<td>Diffie-Hellman key length DH1 (768), DH2 (1024), DH5 (1536), DH14 (2048), DH15 (3072), DH16 (4096), DH17 (6144), DH18 (8192)</td>
</tr>
<tr>
<td><strong>Phase 1 /IKE SA Lifetime (sec.)</strong></td>
<td>Phase 1 / IKE Authentication lifetime before re-negotiation. Expressed in seconds.</td>
</tr>
</tbody>
</table>

**Phase 2 / Child SA parameters:**

<table>
<thead>
<tr>
<th><strong>Connection type</strong></th>
<th>Only client-to-server is available in this version.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Local address / prefix</strong></td>
<td>This field is the virtual IP address. Since only Mode Config and CP mode is supported, it is not enabled. The gateway will choose and send the Virtual IP to use.</td>
</tr>
<tr>
<td><strong>Remote address / prefix</strong></td>
<td>This is the remote network the tunnel will give connectivity to. Since only Mode Config and CP mode is supported, it is not enabled. The gateway will choose and send the Remote Network the client will have access to.</td>
</tr>
<tr>
<td><strong>Encryption Algorithm</strong></td>
<td>Encryption algorithm negotiated during IPsec phase: SA: 3DES, AES-128, AES-192, AES-256</td>
</tr>
<tr>
<td><strong>Hash algorithm</strong></td>
<td>Authentication algorithm negotiated during IPsec phase MD5, MD5_160, SHA1, SHA1_160 and SHA2-256, SHA2 384, SHA2 512</td>
</tr>
<tr>
<td><strong>Diffie-Hellman algorithm</strong></td>
<td>Diffie-Hellman key length DH1 (768), DH2 (1024), DH5 (1536), DH14 (2048), DH15 (3072), DH16 (4096), DH17 (6144), DH18 (8192)</td>
</tr>
<tr>
<td><strong>Phase 2 / Child SA lifetime (sec.)</strong></td>
<td>Phase 2 / Child SA lifetime before re-negotiation. Expressed in seconds</td>
</tr>
</tbody>
</table>

After any tunnel modification, the configuration has to be updated. First click on "Save" in the IPsec Tunnel edition page, then click on "Update with changes" in the IPsec Tunnels page (Cf. screenshot below).
3.5 Certificates

3.5.1 Certificates list

The Linux VPN Client GUI enables to manage certificates which are used to open the VPN tunnels.

For each certificate, the following information is displayed:
- Name: Certificate short name filled in the import certificate page. This identifier will be referenced in the IPsec tunnel configuration page.
- Type of certificate: User / CA: identifies the type of certificate
- Serial: Certificate serial number
- Subject: Certificate's subject. Click on Certificate's subject open the detailed view of the certificate.
- Expiration date
- Delete: Remove the certificate from the internal VPN certificate directory.

3.5.2 Certificate import

The VPN Linux enables to import PKCS#12 certificates.
Certificate short name: This name must be chosen by the user. It will be used to reference the certificate in the Certificates list.

The password is the certificate's password which enables to read the PKCS12 certificate.

Please, be careful to choose a file to import before clicking on the "Import" button.
3.6 Logs

The application logs tab shows the application events: tunnel imported, certificate imported, opening and closing requests.

The IPsec logs tab shows detailed logs from IKE daemon: connection status, etc.

By default:
- application logs are saved in: /var/log/thegreenbowvpn/tgbserver.log
- IPsec logs are saved in: /var/log/charon.log

The Settings tab enables to configure logs levels, default logfiles paths, etc.
3.7 System

The System page enables to change the login / password for the access control to the application.

The System page also shows application version information and IKE daemon status information.
4 Contact

Information and update are available at: www.thegreenbow.com

Technical support via email at: support@thegreenbow.com

Sales via email at: sales@thegreenbow.com
## 5 Annex

### 5.1 TheGreenBow VPN Client specifications

<table>
<thead>
<tr>
<th>General</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Linux Distribution</td>
<td>Debian 8 32 Bits</td>
</tr>
<tr>
<td>Languages</td>
<td>English</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Connection / Tunnel</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Connection mode</td>
<td>Peer-to-Gateway (see the list of qualified VPN gateways and their configuration guides)</td>
</tr>
<tr>
<td>Tunneling Protocol</td>
<td>IKE based on Strongswan</td>
</tr>
<tr>
<td></td>
<td>Diffie-Hellmann DH Group 1 to 18</td>
</tr>
<tr>
<td></td>
<td>Full IPsec support using IKEv1 and IKEv2</td>
</tr>
<tr>
<td>Tunnel mode</td>
<td>Main mode</td>
</tr>
<tr>
<td>Config mode</td>
<td>Network settings automatically retrieved from the VPN gateway</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Cryptography</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Encryption</td>
<td>Symmetric: DES, 3DES, AES 128/192/256bit</td>
</tr>
<tr>
<td></td>
<td>Asymmetric: RSA</td>
</tr>
<tr>
<td></td>
<td>Diffie-Hellmann: DH1 (768), DH2 (1024), DH5 (1536), DH14 (2048), DH15 (3072), DH16 (4096), DH17 (6144), DH18 (8192)</td>
</tr>
<tr>
<td></td>
<td>Hash: MD5, SHA-1, SHA2-256, SHA2-384, SHA2-512</td>
</tr>
<tr>
<td>Authentication</td>
<td>Pre-shared key</td>
</tr>
<tr>
<td>PKI</td>
<td>Certificates: support format PKCS12</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Miscellaneous</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>NAT / NAT-Traversal</td>
<td>NAT-Traversal RFC 3947, IP address emulation, includes support for: NAT_OA, NAT keepalive</td>
</tr>
<tr>
<td>DPD</td>
<td>RFC3706. Detection of non-active IKE end points.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Administration</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Log and trace</td>
<td>Application and IPsec logs</td>
</tr>
<tr>
<td>License and activation</td>
<td>Contact TheGreenBow sales department</td>
</tr>
</tbody>
</table>
5.2 FAQ / Troubleshooting

Web browser no longer displays VPN pages when connection to https://localhost:3000
Maybe the application has crashed. You can start or restart it with the following commands:
systemctl start tgbvpn-client
systemctl restart tgbvpn-client

Is TheGreenBow VPN compatible with amd64 distribution?
No, only i386 distribution is supported so far

Usage of "sudo" for the installation
Using "sudo" is not recommended. Some of the scripts will report some errors if used.
Secure, Strong, Simple
TheGreenBow Security Software