Cobia® v0.5

VPN Module Users Guide

July 31, 2008

(rev-c)

StillSecure®
www.stillsecure.com
StillSecure
100 Superior Plaza Way
Suite 200
Superior, CO 80027
P (303) 381-3800
F (303) 381-3880

Table of Contents

Chapter 1. Introduction

This chapter provides an overview of the VPN Module.

VPN Overview

A Virtual Private Network (VPN) is a private, secure communication path (tunnel) between devices across a public network (the Internet). VPNs use strong encryption to secure the data that is sent back and forth between the devices, ensuring that the data is not altered or understood by other devices or users.

VPN Module Overview

The VPN module is software that facilitates the communication between remote users and resources inside of the network. The VPN module is based on OpenVPN™ which is a full-featured open source SSL VPN Solution. See the following link for more information about OpenVPN:

http://www.openvpn.net

Chapter 2. System Configuration

This chapter describes how to enable and disable the VPN service, configure the VPN module, create and revoke client keys, provides a list of configurable items, and describes how to modify the configuration file.

Enabling and Disabling VPN Service

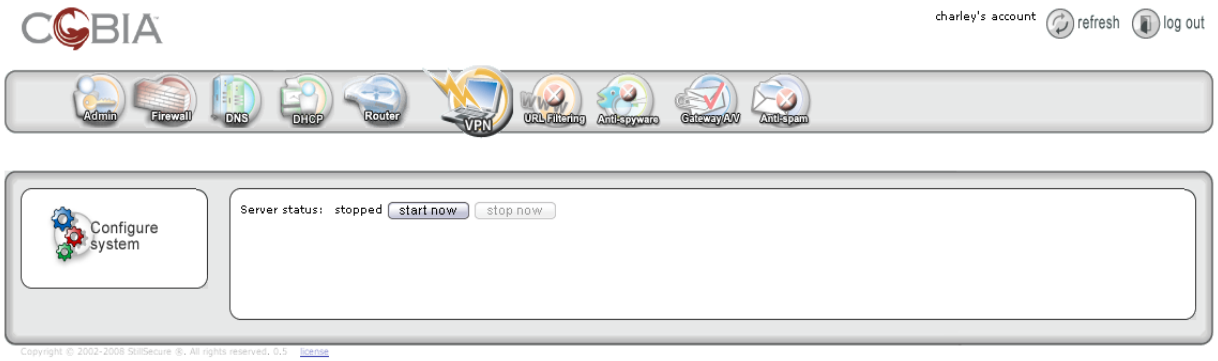
The VPN service is turned off by default.

To enable or disable the VPN service:

Cobia home window>>VPN module

Click **start now** to start the VPN service. Click **stop now** to stop the VPN service.

Figure 1: VPN Module



Configuring the VPN Module

The VPN module is based on OpenVPN. OpenVPN uses client and server keys for encryption, and needs access through a firewall. You need to create keys for the clients on the Cobia server and install the OpenVPN client on any endpoint that will be accessing your network through the VPN module. The VPN module adds the firewall rule to the Firewall module.

This section describes the following:

- "Creating Client Keys" on page 6
- "Revoking Client Keys" on page 6
- "Modifying the Configuration Files" on page 9

Client Keys

OpenVPN uses a certificate (public key) and a private key for the server and each client, and a master Certificate Authority (CA) certificate and key (to sign the server and client certificates).

This section describes how to add and revoke client keys.

Creating Client Keys

This section describes how to add client keys.

To add a client key:

Command line window

1. Log in to the Cobia server as `root` using SSH or directly with a keyboard.
2. Enter the following command to go to the OpenVPN directory:

   ```
   cd /etc/openvpn
   ```

3. Enter the following command to create a key:

   ```
   ./createclientkey <clientname>
   ```

   where <*clientname*> is the name of the resulting ZIP file.
   For example:
   `./createclientkey pike`
   creates this ZIP file:
   `/etc/openvpn/keys/pike.zip`

4. Provide this ZIP file to the client:
   a. Copy the ZIP file from the Cobia server (using WinSCP, SCP, or something similar) to a computer that has an email program.
   b. Email the ZIP file to the client.

Revoking Client Keys

This section describes how to revoke client keys. After you revoke the key, the client cannot access the network through the VPN module.

To revoke a client key:

Command line window

1. Log in to the Cobia server as `root` using SSH or directly with a keyboard.
2. Enter the following command to go to the OpenVPN directory:

   ```
   cd /etc/openvpn
   ```

3. Enter the following command to revoke a key:

   ```
   ./revokeclientkey <clientname>
   ```

   where <*clientname*> is the name of the key or user.
   For example:
   `./revokeclientkey pike`
   revokes the privileges for the user `pike`, moves the `pike.tar` file into the `/etc/openvpn/revoked-certificates` directory, and reloads the OpenVPN configuration.

Configuration File

This section lists the parameters that you can modify in the configuration file and in the vars file. These files, accessed through the user interface, contain descriptions, examples, and suggested uses. If you think you might want to modify one of the settings, be sure to consult the comments in the file to be sure you completely understand the settings and ramifications if you change them. You may *not* need to modify any of these settings;

however, if you do, refer to the instructions in “Modifying the Configuration Files” on page 9 for the specific steps.

The VPN configuration file is located in the following directory:

`/etc/openvpn/openvpn.conf`

The configuration file contains the following options:

- Local IP address that OpenVPN listens on:
  - local a.b.c.d
- TCP/UDP port that OpenVPN listens on:
  - proto udp
  - port 500
- Tunnel:
  - dev tun
  - dev-node MyTap
- Certificate and Key:
  - ca keys/ca.crt
  - cert keys/server.crt
  - key keys/server.key
- Diffie-Hellman parameters:
  - dh keys/dh1024.pem
- Server mode and VPN subnet:
  - server 10.8.0.0 255.255.255.0
- Record of client <-> virtual IP address:
  - ifconfig-pool-persist ipp.txt
- Server mode for ethernet bridging:
  - server-bridge 10.8.0.4 255.255.255.0 10.8.0.50 10.8.0.100
- Push routes:
  - push "route 172.100.1.0 255.255.255.0"
- Assign specific IP addresses:
  - client-config-dir ccd
  - route 10.9.0.0 255.255.255.252
  - ifconfig-push 10.9.0.1 10.9.0.2
- Enable different firewall access policies:
  - learn-address ./script
  - push "redirect-gateway"
- Push Windows-specific network settings:
  - push "dhcp-option DNS 10.8.0.1"
- Enable clients to see each other:
  - client-to-client
- Multiple clients:
  - duplicate-cn
- Ping
  - keepalive 10 120
- HMAC firewall
  - openvpn --genkey --secret ta.key
  - tls-auth ta.key 0

  - cipher BF-CBC
- Enable compression:
  - comp-lzo
- Maximum clients:
  - max-clients 100
- Reduce daemon's privileges:
  - user nobody
  - group nobody
- Persist options:
  - persist-key
  - persist-tun
- Logging:
  - status openvpn-status.log
  - log openvpn.log
  - log-append openvpn.log
  - verb 3
- Silence repeating messages:
  - mute 20

Vars File

The VPN vars file is located in the following directory:

`/etc/openvpn/easy-rsa/2.0/vars`

The vars file contains the following options:

- Certificate default values:
  - export KEY_COUNTRY="US"
  - export KEY_PROVINCE="MyState"
  - export KEY_CITY="MyCity"
  - export KEY_ORG="MyOrg"
  - export KEY_EMAIL="myuser@myhost.mydomain"
- The top level of the easy-rsa tree:
  - export EASY_RSA="`pwd`"
  - export EASY_RSA_BIN="/etc/openvpn/easy-rsa/2.0"
- The requested executables:
  - export OPENSSL="openssl"
  - export PKCS11TOOL="pkcs11-tool"
  - export GREP="grep"
- The openssl.cnf file:
  - export KEY_CONFIG=`$EASY_RSA_BIN/whichopensslcnf $EASY_RSA_BIN`
- Point to your key directory:
  - export KEY_DIR="$EASY_RSA/keys"
- Specify rm -rf warning:
  - echo NOTE: If you run ./clean-all, I will be doing a rm -rf on $KEY_DIR
- Key size:
  - export KEY_SIZE=1024

- Number of days to root CA key expiration:
  - export CA_EXPIRE=3650
- Number of days to certificates expiration:
  - export KEY_EXPIRE=3650

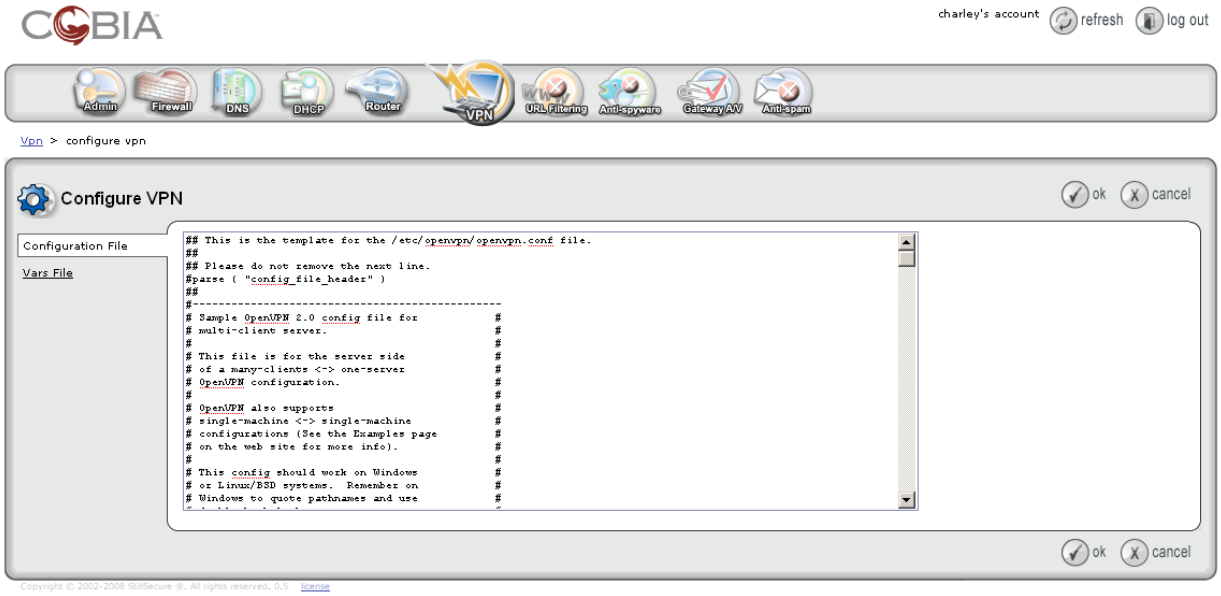
Modifying the Configuration Files

This section provides detailed instructions on modifying the configuration files using the user interface.

To modify the configuration files:

Cobia main window>>VPN module>>Configure system

Figure 2: Configure VPN system



1 Select the **Configuration file** menu option or the **Vars file** menu option.

2 Locate the section in the configuration file you want to modify. For example:

```
# TCP or UDP server?
```

3 Make the corrections. For example to change the server from UDP to TCP:

a Find the following lines:

```
;proto tcp
proto udp
```

b Remove the semicolon (;) from the beginning of the first line to change the line from a remark to a line that is processed:

```
proto tcp
```

c Add a semicolon (;) to the beginning of the second line to change the line from a line that is processed to a remark

```
proto udp
```

4 Click **ok** to save the file and return to the VPN home window.

TIP

You can copy the entire contents of the configuration file into a text editor, make your edits there, and paste it back into the user interface. This will enable you to use the search features of your text editor to find sections quickly.

NOTE

The previous version of the file is not retained, so use caution when making modifications, or create a backup copy before you make any edits.

Installing the VPN Client

Each endpoint connecting through the VPN module to the network must have the OpenVPN client installed. This section describes how to install the following clients:

- "Linux" on page 10
- "Windows" on page 11
- "Mac" on page 11

Linux

This section describes how to install OpenVPN on a Linux machine.

To install the OpenVPN client:

Browser window and command line window

1 Log in to the Linux machine and open a browser window.

2 Download the Linux client from the Cobia server:

a Navigate to:

```
https://<IP address>/vpn/downloads/index.html
```

Where:
<IP address> = The IP address of your Cobia server.
For example: `https://192.168.40.60/vpn/downloads/index.html`.

The **VPN Downloads** window opens.

b Click **Linux**.

c Click **OK** to save the RPM file to the Linux machine.

3 Install the OpenVPN client by following the instructions on the OpenVPN Web site for installing with an RPM package:

http://openvpn.net/index.php/documentation/howto.html#install

4 Install the keys (created in "Creating Client Keys" on page 6):

a Log in to the Linux client machine using SSH or directly with a keyboard.

b Navigate to the OpenVPN directory by entering the following at the command line:

```
cd /etc/openvpn
```

c Unzip the key files given to you by your system administrator by entering the following at the command line:

`unzip <filename>`

where <*filename*> is the name of the ZIP file. For example:
`unzip jasmine.zip`

5 Start OpenVPN by entering the following command at the command line:

```
service openvpn start
```

6 **Optional** – To start OpenVPN everytime you boot the Linux box, enter the following at the command line:

```
chkconfig --level 3 openvpn on
```

Windows

This section describes how to install OpenVPN on a Windows 2000 or later machine.

To install the OpenVPN client:

Browser window and Windows desktop

1 Log in to the Windows machine and open a browser window.

2 Download the Windows client from the Cobia server:

a Navigate to:

`https://<IP address>/vpn/downloads/index.html`

Where:
<*IP address*> = The IP address of your Cobia server.
For example: `https://192.168.40.60/vpn/downloads/index.html`.

The **VPN Downloads** window opens.

b Click **Windows**.

c Click **OK** to save the EXE file to the Windows machine.

3 Install the OpenVPN client by following the instructions in the *"Installation using the bundled OpenVPN package with OpenVPN GUI included"* section on the OpenVPN Web site for Windows:

http://openvpn.se/install.txt

4 Install the keys (created in "Creating Client Keys" on page 6):

a Select **Start>>OpenVPN>>OpenVPN configuration file** directory. A README.txt file opens in a file explorer window.

b Copy the contents of the ZIP file provided to you by your system administrator to the OpenvPN configuration file directory.

5 Start OpenVPN:

a Select **Start>>Control Panel>>Administrative Tools>>Services**.

b Right-click **OpenVPN** and select **Properties**.

c On the **General** tab, select a **Startup type** of **Automatic**. This service will start every time you start Windows.

d Click **Start** to start the service.

Mac

This section describes how to install OpenVPN on a Mac machine.

To install the OpenVPN client:

Browser window and Mac desktop

1. Log in to the Mac machine and open a browser window.
2. Download the Mac client from the Cobia server:
   a. Navigate to:

      `https://<IP address>/vpn/downloads/index.html`

      Where:
      <IP address> = The IP address of your Cobia server.
      For example: `https://192.168.40.60/vpn/downloads/index.html`.

      The **VPN Downloads** window opens.
   b. Click **Mac**.
   c. Click **OK** to save the DMG file to the Mac machine.
3. Install the OpenVPN client by following the instructions on the OpenVPN Web site for Mac OS X:

   http://www.tunnelblick.net/README.txt
4. Install the keys (created in "Creating Client Keys" on page 6):
   a. Navigate to the `$HOME/Library/openvpn` directory. Create it if it does not already exist.
   b. Copy the contents of the ZIP file provided by your system administrator into `$HOME/Library/openvpn`.
5. Start Tunnelblick (OpenVPN for Mac OS X):
   a. Locate the Tunnelblick tunnel icon on the status bar.
   b. Click on the icon, and choose to connect to your network.

See the following link for more information on Tunnelblick:

http://code.google.com/p/tunnelblick/

Appendix A. Conventions

Conventions Used in Cobia

Color

Color is used in Cobia as follows:

- **Yellow background** – Modified, but not yet saved
- **Green background** – New, but not yet saved
- **Red background** – Deleted, but not yet saved
- **Gray background** – There are default settings for the option that you can override here.

Conventions Used in this Document

The conventions used in this document are described in this section:

Navigation Paragraph

Navigation paragraphs provide a quick visual on how to get to the screen or area discussed.

Example:

Cobia main window>>Admin Module>>Configure system

Tip Paragraph

Tips provide helpful, but not required information.

Example:

TIP

Hover the cursor over the "x dhcp servers with errors" text to get additional information in a pop-up window.

Note Paragraph

Notes notify you of important information.

Example:

NOTE

If there is no activity for 30 minutes, the configuration window times out and you must log in again.

Caution Paragraph

Cautions notify you of conditions that can cause errors or unexpected results.

Example:

CAUTION

Do not rename the files or they will not be seen by Cobia.

Warning Paragraph

Warnings notify you of conditions that can lock your system or cause damage to your data.

Example:

WARNING

Do not log in using SSH—this kills your session and causes your session to hang.

Bold Font

Bold font indicates the text that appears on a window or screen.

Example:

6 Enter a name in the **Host name** field.

Task Paragraph

Task paragraphs summarize the instructions that follow.

Example:

To configure Ethernet interfaces:

Italic Text

Italic text is used in the following cases:

- **Showing emphasis** –

  Low – You are not protected from potentially unsafe macros. (*Not recommended*).

- **Introducing new terms** –

  The SMS server contains a database of logical groups with common attributes called *collections*. SMS operates only on *clients* (devices) that are members of a collection.

- **Indicating document titles** –

  Cobia Installation Guide

- **Indicating a variable entry in a command** –

  `https://``<`*`IP_address`*`>`**`/index.html`**

  In this case, you must replace <*IP_address*> with the actual IP address, such as **`10.0.16.99`**. Do not type the angled brackets.

Underlined Text

Underlined text indicates an active link.

Example:

http://cobia.stillsecure.org/?q=node/27

Courier Font

Courier font is used in the following cases:

- **Indicating path names** –

  Change the working directory to the following:

  C:\Program Files<*MyCompany*>**\Cobia**

- **Indicating text; enter exactly as shown** –

  Enter the following URL in the browser address field:

  https://<*IP_address*>**/index.html**

  In this case, you must replace <*IP_address*> with the actual IP address, such as **10.0.16.99**. Do not type the angled brackets.

- **Indicating file names** –

  nac.properties

Angled Brackets

Angled brackets enclose variable text that needs to be replaced with your specific values.

Example:

https://<*IP_address*>**/index.html**

In this case, you must replace <*IP_address*> with the actual IP address, such as **10.0.16.99**. Do not type the angled brackets.

Square Brackets

Square brackets are used in the following cases:

- **Indicating keys to press on the keyboard** –

  [Ctrl]+[Shift]+[r]

- **Indicating a variable section in a *.INI file** –

  ```
  [Global]
  NASList=192.168.200.135
  ```

- **Indicating a list in a properties file** –

  ```
  Compliance.ObjectManager.DHCPConnectorServers=[192.168.51.130,
  192.168.99.1]
  ```

Terms

Terms are defined in the "Glossary" on page 22.

Example:

M

MAC	Media Access Control – The unique number that identifies a physical network interface. Generally referred to as the MAC address.

Appendix B. Glossary

C

client	A computer that requests services from another (server).

D

daemon	TBD

E

encryption	TBD

I

IP	Internet Protocol – A protocol by which data is sent from one computer to another on the Internet.

L

log	A written record of events.

R

route	The path network traffic takes from the source to the destination.

S

server	A computer that provides services to another (client).
subnet	A section of a network that shares part of the IP address of that network.

T

TCP	Transfer Control Protocol - A protocol (set of rules) used (with IP) to send data over the Internet.
tunnel	TBD

U

UDP	User Datagram Protocol - A limited-service protocol used to exchange messages between computers over the Internet.

V

VPN	Virtual Private Network – A secure method of using the Internet to gain access to an organization's network.

Index