SWsoft, Inc.

Plesk™ VPN

Administrator's Guide

Plesk 7.5 Reloaded

SWsoft

ISBN: N/A
SWsoft Inc
13800 Coppermine Drive
Suite 112
Herndon
VA 20171 USA
Tel: +1 (703) 815 5670
Fax: +1 (703) 815 5675

Contents

Table of Figures

CHAPTER 1

Preface

In This Chapter

About This Guide

This Guide explains how to use Plesk™ Virtual Private Networking (hereinafter referred to as the VPN Module), a Plesk™ module that allows the administrator to set up a VPN connection between a Plesk-enabled server and a remote host through the control panel interface.

Documentation Conventions

Before you start using this guide, it is important to understand the documentation conventions used in it.

Typographical Conventions

The following kinds of formatting in the text identify special information.

Formatting convention	Type of Information	Example
Special Bold	Items you must select, such as menu options, command buttons, or items in a list.	Go to the **QoS** tab.
	Titles of chapters, sections, and subsections.	Read the **Basic Administration** chapter.
Italics	Used to emphasize the importance of a point, to introduce a term or to designate a command line placeholder, which is to be replaced with a real name or value.	These are the so-called *shared VPSs*. To destroy a VPS, type `vzctl destroy` *vpsid*.
`Monospace`	The names of commands, files, and directories.	Use `vzctl start` to start a VPS.

`Preformatted`	On-screen computer output in your command-line sessions; source code in XML, C++, or other programming languages.	`Saved parameters for VPS 101`
`Monospace Bold`	What you type, contrasted with on-screen computer output.	**`# rpm –V virtuozzo-release`**
CAPITALS	Names of keys on the keyboard.	SHIFT, CTRL, ALT
KEY+KEY	Key combinations for which the user must press and hold down one key and then press another.	CTRL+P, ALT+F4

General Conventions

Be aware of the following conventions used in this book.

- Chapters in this guide are divided into sections, which, in turn, are subdivided into subsections. For example, Documentation Conventions is a section, and General Conventions is a subsection.
- When following steps or using examples, be sure to type double-quotes ("), left single-quotes (`), and right single-quotes (') exactly as shown.
- The key referred to as RETURN is labeled ENTER on some keyboards.

The root path usually includes the `/bin`, `/sbin`, `/usr/bin` and `/usr/sbin` directories, so the steps in this book show the commands in these directories without absolute path names. Steps that use commands in other, less common, directories show the absolute paths in the examples.

Feedback

If you spot a typo in this guide, or if you have thought of a way to make this guide better, we would love to hear from you!

If you have a suggestion for improving the documentation (or any other relevant comments), try to be as specific as possible when formulating it. If you have found an error, please include the chapter/section/subsection name and some of the surrounding text so we can find it easily.

Please submit a report by e-mail to userdocs@sw-soft.com.

CHAPTER 2

Using Plesk™ VPN

Virtual Private Networking technologies allow communications between geographically distributed LAN segments over a public network. VPN message traffic passes through public networking infrastructures, such as the Internet via secure tunnel protocols.

One of the most useful implementations of VPN is allowing access to a local network for a single remote host. For example, if a user needs to get access to a remote network from his home computer, he/she must establish a VPN connection.

The Plesk™ VPN module allows the administrator to set up a point-to-point connection between two Plesk hosts or between your Plesk host and any other computer. At present, the Plesk™ VPN module supports connection to the server only from a single remote host and does not support connections from multiple hosts. The module is based on the OpenVPN solution which uses OpenSSL for encryption and the virtual TUN/TAP driver for tunneling.

In This Chapter

How to Access the VPN Module

To access the Plesk™ VPN module, select the Modules shortcut in the navigation pane and click the Virtual Private Networking icon in the Modules group.

Software Requirements: You should have one of the following operating systems to use the OpenVPN solution: Linux, Windows 2000/XP and higher, OpenBSD, FreeBSD, NetBSD, Mac OS X, and Solaris.

If you access the module for the first time, the first page that opens is the VPN Preferences page (on page 8). You cannot get access to other VPN module options unless you specify the preferences for your VPN connection.

Setting up VPN Preferences

To set up a VPN connection:

1 Access the VPN module in your control panel.

2 On the **Preferences** page that opens, specify the following parameters:

Remote Address - enter the host name or IP address of the host you want to communicate to. Leave this field blank if you wish the other party to be able to connect to your server from different addresses or if the remote IP address is not known in advance. Note, however, that one server cannot be involved in simultaneous communication with two or more remote hosts.

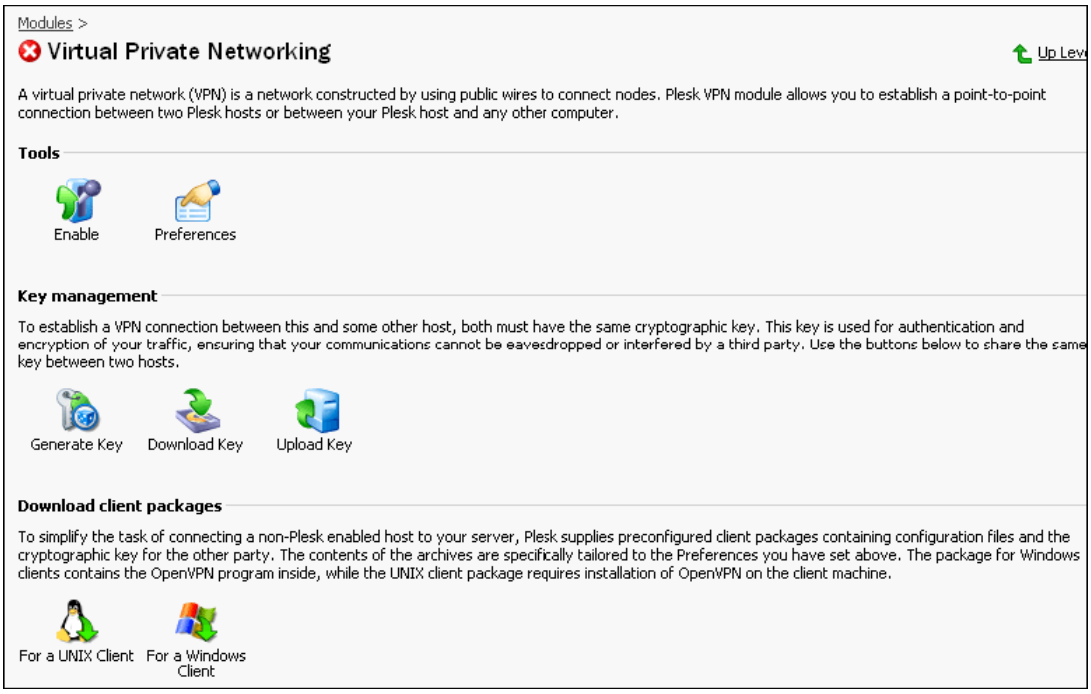
Remote UDP port - specify the port on the remote host to which UDP packets from this server will be sent. The default port is 1194. Note that though VPN uses only UDP for the encrypted traffic flow, all IP protocols, including TCP, are supported over the virtual private network. You can leave this field blank if you have not specified the remote address above.

Local UDP port - Your server will listen for incoming VPN traffic on this local UDP port. The default port is 1194. You can leave this field blank if you do not want to allocate a specific port, but in that case you must specify the remote address and port fields above to allow the local host to be the initiating party.

Local peer address and **Remote peer address** - two hosts connected by a VPN channel need to have a pair of virtual network interfaces to route the traffic through. You need to assign two IP addresses to them, one for each side of the VPN circuit. These IP addresses should be chosen from some private address spaces and it is important that they should not overlap with any of the IP addresses present within the local networks on either side of the tunnel. These two addresses must differ only in the two least significant bits. You can pick .1 and .2 for the last octets, for example. Note that the default values are only an illustration! Always check the real configuration of your network so that you do not run into IP collision problems.

3 Click **OK** to apply the connection parameters or **Cancel** to cancel the operation.

After you finish configuring the VPN connection parameters, you will be taken to the VPN Module main page.



Modules >

Virtual Private Networking

Up Lev

A virtual private network (VPN) is a network constructed by using public wires to connect nodes. Plesk VPN module allows you to establish a point-to-point connection between two Plesk hosts or between your Plesk host and any other computer.

Tools

Key management

To establish a VPN connection between this and some other host, both must have the same cryptographic key. This key is used for authentication and encryption of your traffic, ensuring that your communications cannot be eavesdropped or interfered by a third party. Use the buttons below to share the same key between two hosts.

Download client packages

To simplify the task of connecting a non-Plesk enabled host to your server, Plesk supplies preconfigured client packages containing configuration files and the cryptographic key for the other party. The contents of the archives are specifically tailored to the Preferences you have set above. The package for Windows clients contains the OpenVPN program inside, while the UNIX client package requires installation of OpenVPN on the client machine.

Figure 1: VPN Module main page

Note that the VPN module is initially disabled. To use the VPN functionality, enable the module by clicking the Enable button.

Managing Keys

To establish a VPN connection between your Plesk-enabled server and a remote host, both sides must have the same cryptographic key. This key is required for authentication and encryption of your traffic, ensuring that your communications cannot be eavesdropped or interfered by a third party. Do not forget to share the same key between both communicating parties each time you generate or upload a new key!

A cryptographic key is generated automatically and saved to a special directory during module installation. However, you might want to replace the initial key with the new one.

To generate a new VPN key:

Click the Generate Key button in the Key management group. The new key will automatically replace the existing key.

Note: After the new key is generated, your old key will become invalid! In order to continue communication, you must share the new key with the other communicating party.

To save the generated key to your local machine:

1. Click the Download Key button in the Key management group.
2. Save the key to a specified location on your disk.

   You can then transmit this key file to another host on removable media or through another secure way.

If you received a cryptographic key from another machine and want to upload it:

1. Click the Upload Key button in the Key management group.
2. On the next page, specify the location of the key file and click OK.

This way of key management is especially useful if you are establishing a VPN connection between two Plesk-enabled servers. If the remote host does not have the Plesk control panel, it is more convenient to use client packages (on page 10).

Using Client Packages

To simplify the task of connecting a non-Plesk enabled host to your server, Plesk supplies preconfigured client packages containing configuration files and the cryptographic key for the other party. The contents of the archives are specifically tailored to the Preferences you have specified earlier.

If your client is running the Windows OS, click the For a Windows Client button to download and save the client package on your local machine.

The client package is a ZIP archive that contains the following files:

`Install TAP device.bat` - installs the TAP driver on your computer

`Uninstall TAP device.bat` - uninstalls the TAP driver from your computer

`Connect to VPN.bat` - establishes a VPN connection

`System` folder - contains the cryptographic key and your VPN preferences.

To install and uninstall the TAP drivers, you must have Windows administrator rights on your computer.

To install the TAP driver, run the `install TAP device.bat` file. After the driver is installed, you can establish a VPN connection to the Plesk-enabled server by running the `connect to VPN.bat` file. The OpenVPN software itself is contained within the client package and does not require any installation or removal procedures.

If your client is running a Unix OS, click the For a Unix client button to download and save the client package on your local machine. The package contains the `openvpn.conf` file with your current VPN preferences and the `vpn-key` file that is a cryptographic key for your VPN connection. If you are using this package, OpenVPN (version 2.0) must be already installed on the client machine. For smooth operation, we advise that you use OpenVPN 2.0 beta 11 as the module was tested on this beta version.

If the preferences on the Plesk server change or a new key is generated or uploaded to the Plesk server, the client packages must be downloaded again because they include your current key and existing VPN preferences.

Starting/Stopping a VPN Connection

To enable/disable a VPN connection from the Plesk control panel:

Click the Enable/Disable button in the Tools group on the VPN Module page.

If you want to disable a VPN connection on a Windows client, close the Connect to VPN dialog box that appeared when you established your connection. When the Windows user logs out, the VPN connection shuts down as well.

Index