Supplement to ViPNet VPN Documentation

Quick Start

Global contacts page http://www.vipnet.com/

Contents

About This Document

This document is designed for the network administrators intending to deploy and configure ViPNet VPN virtual private networks in their organizations. You can use this document as a quick reference to create and configure a protected network, without reading the full version of the user's guide.

Preparing for the Setup

Before ViPNet VPN setup, think over your protected network structure and check network connection settings on the computer that will function as a coordinator. To do this:

- Decide on which computer you are going to deploy the ViPNet network administrator's workstation. You choose either a client, or a coordinator. Install the ViPNet Network Manager program on the ViPNet network administrator's workstation.

- On a computer with installed ViPNet Network Manager, deploy a client (by installing ViPNet Client) or a coordinator (by installing ViPNet Coordinator). ViPNet Client or ViPNet Coordinator allows you to send keys and software updates from ViPNet Network Manager to ViPNet hosts, while the ViPNet

Network Manager program is intended for network administering and cannot interact with other hosts.

- Decide which program will be used to deploy a coordinator: ViPNet Coordinator for Windows, ViPNet Coordinator HW or ViPNet Coordinator VA. Make sure that your ViPNet VPN license allows you to add the chosen coordinator type. You can deploy ViPNet Coordinator HW only on the special hardware platform. ViPNet Coordinator VA is an image of the ViPNet software that is intended for functioning in a virtual environment.

- Decide on which computer the coordinator will be deployed. For example, you may install the coordinator on a computer where private data are stored, and you need to provide protected access to these data; or it may be any other computer or server. A coordinator must be always accessible from all clients, in other words, the computer with installed ViPNet Coordinator must be always switched on and connected to the network. You may establish protected connection to a coordinator (as well as to a client) over the RDP protocol, or access public resources on a coordinator or a client.

- After you have decided on which computer you will deploy the coordinator, make sure that this computer has a static private IP address.

- On the DSL router, behind which the future coordinator is located, configure a port forwarding rule for the coordinator's IP address. Set forwarding of UDP traffic from port 55777 to port 55777.

- If the computer, on which you are going to install ViPNet Coordinator, does not have a static public IP address, configure the Dynamic DNS service on the corresponding router. To do this, you should create an account on some dynamic DNS service web site, for example, www.dyndns.com.

Deploying the ViPNet Network Administrator's Workstation

When you are deploying a ViPNet network based on the ViPNet VPN software, you should deploy the ViPNet network administrator's workstation first, by installing ViPNet Network Manager, then ViPNet Client or ViPNet Coordinator on the network administrator's computer. You will use the ViPNet Network Manager program for network administering, while the ViPNet Client or ViPNet Coordinator program is required to link the administrator's workstation with other ViPNet hosts.

To install the software on the ViPNet network administrator's workstation:

1 Run the ViPNet VPN setup program and install the ViPNet Network Manager software on the ViPNet network administrator's workstation.

> **Note:** To get your link for setup file download, you should fill in a form accessible by the following link: http://infotecs.ru/downloads/cdownload_demo.php?i_id_file=6742

2 Run the ViPNet VPN setup program again and install the ViPNet Client or ViPNet Coordinator program on the ViPNet network administrator's workstation. On the first page of the ViPNet VPN setup program, select the **I do have a key set (.dst file) for this ViPNet Client (Coordinator)** check box. You can create a `*.dst` file later in ViPNet Network Manager.

After the ViPNet Client or ViPNet Coordinator software installation is completed, the "ViPNet software is installed on your computer. But the program cannot be loaded because the keys are not installed. Do you want to install the keys now?" message will be displayed.

3 Start ViPNet Network Manager and register it.

4 Upon completing the registration, create the administrator password. This password is required only for the ViPNet Network Manager software and cannot be saved.

5 The **Create ViPNet Network Wizard** will be started. When you start the wizard, you have the following options:

- o Follow the wizard instructions and create the basic network structure.

- o Close the wizard and create a network later. The minimum network structure will be created (one coordinator and one client, on which ViPNet Network Manager is installed) and the main ViPNet Network Manager window will be displayed.

6 If you continue working with the ViPNet Network Creation wizard, on the **Location for the ViPNet Administrator's Workstation** page, choose the network host type, on which you want to deploy the ViPNet administrator's workstation.

7 If necessary, on the **Automatic network structure creation** page, rename coordinators and clients. Follow the instructions in Preparing for the Setup (on page 3): specify the coordinator's local IP address, DNS names (dyndns), or static public IP address.

8 On the last page of the wizard, clear the **Create key sets upon completing ViPNet Network Creation Wizard** check box. We recommend you to create key sets after you have made the required settings in ViPNet Network Manager.
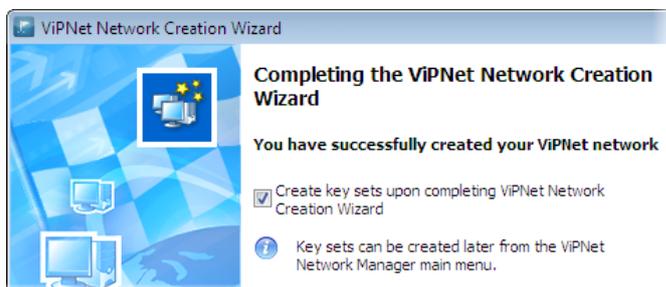

Figure 1. The last page of the ViPNet Network Creation Wizard

Upon you have completed the wizard, ViPNet Network Manager will be launched. The ViPNet network administrator's workstation is marked with the icon 📁 or 📁 in ViPNet Network Manager.

9 Decide if user passwords should be saved to the registry (for example, to make the logo procedure quicker and easier). To do this, in the main ViPNet Network Manager window, in the navigation pane, click the required ViPNet client, click the **Keys** tab, and select or clear the **Allow to save password** check box.

10 Upon the configuration, save key sets for the ViPNet hosts. To do this:

- On the **Tools** menu, select **Keys**, and then click **Save Key Sets**.
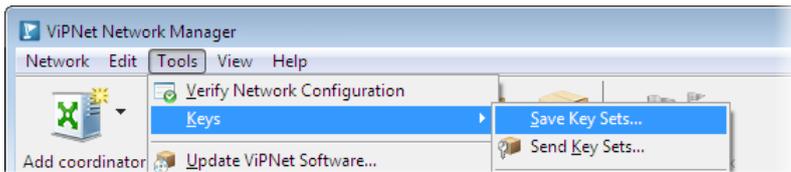

Figure 2. Saving key sets

- In the **Browse For Folder** window, navigate to the folder to save the key sets to.

Upon the key sets have been created, in Windows Explorer, the folder will be opened, where key sets, user passwords of ViPNet hosts have been saved to.

Key sets files have a `.dst` extension and are stored in folders named after the corresponding ViPNet hosts. ViPNet user passwords are saved as a list in the `ViPNet.txt` file. You can view the ViPNet host administrator's password, which is valid for all the hosts on your ViPNet network, in the **My Network** section, on the **Passwords** tab.

11 Open the folder created for the ViPNet network administrator's workstation and double-click the *.dst file to install the keys.

12 Open the `ViPNet.txt` file containing ViPNet user passwords. Copy the user password for the ViPNet network administrator's workstation's host.

13 Start ViPNet Monitor:

- If you use Windows 7 or an earlier version of the Microsoft Windows operating system, on the **Start** menu, choose **All Programs** > **ViPNet** > **ViPNet Client (Coordinator)** > **Monitor**

- If you use the Windows 8 operating system, on the **Start** screen, open the **Apps** list and choose **ViPNet** > **Monitor**.

ViPNet Monitor is the ViPNet Client or ViPNet Coordinator user interface.

14 Paste the copied user password into the **Password** box. If you have allowed password saving in ViPNet Network Manager, you may save the password to the registry.

As a result, the ViPNet Network Manager and ViPNet Client or ViPNet Coordinator software installation on the ViPNet network administrator's workstation is completed.

15 Copy the saved key sets on a removable drive. You will need them for ViPNet Coordinator setup (on page 8), as well as for ViPNet Client setup when you install the program on users' work computers (see Installing ViPNet Client on a User's Computer on page 8).

ViPNet Network Manager Interface

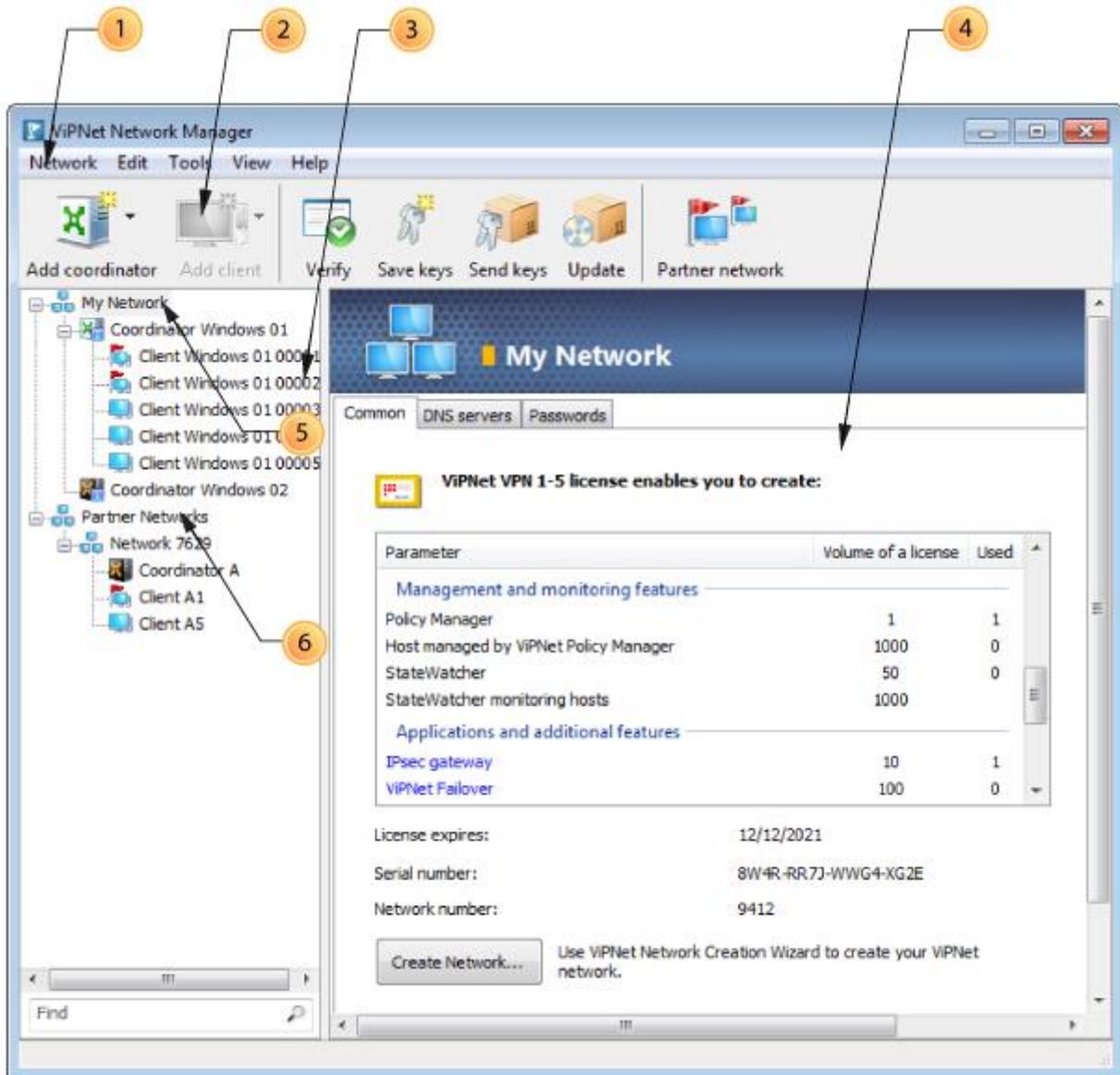The ViPNet Network Manager window is shown in the figure below:

Figure 3. ViPNet Network Manager interface

The following elements are marked with numbers in the figure:

1 The menu bar.

2 The toolbar. To add or remove buttons displayed on the toolbar, on the **View** menu, click **Customize Toolbar**.

3 The navigation pane. Displays the tree-like structure of your ViPNet network.

4 The view pane. Displays properties tabs for the element currently selected in the navigation pane.

5 **My Network** section. Contains all coordinators and clients of your ViPNet network.

6 **Partner Networks** section. This section is displayed only if you have established partner network connections to other ViPNet networks. It contains a list of your partner networks.

ViPNet Coordinator Setup

You should install ViPNet Coordinator on computers that will function as servers in your ViPNet network. A coordinator ensures delivery of ViPNet keys and software updates to clients and exchange of ViPNet hosts' status information and their current addresses. Both a client and a coordinator can exchange encrypted messages and files with other ViPNet hosts.

To install ViPNet Coordinator:

1   Run the ViPNet VPN setup program and, in the displayed window, click **Second step. Deploy network servers (ViPNet Coordinator installation)**.

2   Follow the instructions. You may leave the default settings.

3   Install the keys by double-clicking the *.dst file you have received from your ViPNet network administrator.

> **Note:** To save a `*.dst` file for a ViPNet host, in the main ViPNet Network Manager window, in the navigation pane, select this host. In the view pane, click the **Keys** tab and click **Save keys**.

4   Run ViPNet Coordinator Monitor:

   o   If you use Windows 7 or an earlier version of the Microsoft Windows operating system, on the **Start** menu, choose **All Programs** > **ViPNet** > **ViPNet Coordinator** > **Monitor**.

   o   If you use the Windows 8 operating system, on the **Start** screen, open the **Apps** list and choose **ViPNet** > **Monitor**.

5   To log on to the program, enter the ViPNet host's user password.

> **Note:** The user password is stored in the `vipnet.txt` file that is created automatically when you save keys to the folder.

Installing ViPNet Client on a User's Computer

You should install ViPNet Client on users' computers where traffic protection is required.

To install the ViPNet Client software on a user's computer:

1   Disable the firewall integrated in applications such as Kaspersky Internet Security, Norton Internet Security and so on, if such applications are running on your computer.

> **Warning:** If such a program is running together with the ViPNet software, it may cause conflicts because ViPNet Monitor has its own implemented firewall. Programs that do not have an implemented firewall, for example, Kaspersky Anti-Virus and Norton Anti-Virus, are compatible with the ViPNet software.

2   Run the ViPNet VPN setup program and, in the displayed window, click **Third step. Configure ViPNet network clients (ViPNet Client installation)**.

3   Follow the instructions. You may leave the default settings.

4   After restart, install the keys by double-clicking the `*.dst` file you have received from your ViPNet network administrator.

> **Note:** To save a `*.dst` file for a ViPNet host, in the main ViPNet Network Manager window, in the navigation pane, select this host. In the view pane, click the **Keys** tab and click **Save keys**.

5   Run ViPNet Client Monitor:

   o   If you use Windows 7 or an earlier version of the Microsoft Windows operating system, on the **Start** menu, choose **All Programs** > **ViPNet** > **ViPNet Client** > **Monitor**

   o   If you use the Windows 8 operating system, on the **Start** screen, open the **Apps** list and choose **ViPNet** > **Monitor**.

> **Note:** The user password is stored in the `vipnet.txt` file that is created automatically when you save keys to the folder.

Recommendations on ViPNet Coordinator and ViPNet Client Configuration and Use

For the ViPNet network to function correctly, follow the recommendations below:

•   The ViPNet Coordinator must operate uninterruptedly. At ViPNet Coordinator startup, host user logon should be required. For the ViPNet Coordinator Monitor to start automatically even at emergency reboot, you should configure saving user password to the registry, as well as autologon to the operating system. For more information on system autologon configuration, see the

document "Common Scenarios of ViPNet VPN Administering. Supplement to ViPNet Documentation."

- Never exit the ViPNet Coordinator Monitor and ViPNet Client Monitor programs. If ViPNet Monitor is not running, we do not guarantee security of your ViPNet network. To hide the main program window, click **Close** in the upper right corner of the window.

- In ViPNet Client and ViPNet Coordinator, an integrated personal firewall is integrated. By default, on all ViPNet clients and coordinators, the network filters are configured that allow all public network IP traffic. It means that the integrated firewall is disabled. This allows to avoid network access problems if, on a ViPNet host, another firewall (for example, Windows Firewall) is installed.

  If you want to block unwanted IP traffic, in ViPNet Client or ViPNet Coordinator, configure the corresponding network filters. To control firewalls on the ViPNet hosts of your network centrally, we recommend you to use the ViPNet Policy Manager program.

  If you are an experienced ViPNet administrator, you can block all unprotected connections and allow only necessary IP traffic. In this case, disable all other firewalls including Windows Firewall.

Warning: We recommend that you should not configure allowing network filters unless it is necessary.

  For more information about network filter configuring, see the document "Common Scenarios of ViPNet VPN Administering," section "Peculiarities of the Integrated Firewall."

- By default, virtual IP addresses are used within a WAN, and real IP addresses are used within a LAN. For the IP addresses used by ViPNet hosts in your network to be displayed in the **Private Network** section of the main window:

  o On the **Service** menu, click **Options**.

  o In the **Options** dialog box, in the navigation pane, select **General**.

  o In the view pane, select the **Show IP addresses in the Private Network section** check box.

Note: To configure clients, in ViPNet Monitor software, log onto the administrator mode.