



ViPNetTM

OFFICE/TUNNEL

ViPNet Private Network

Appendix to Administrator Guide

Version 1.4(Windows)



© 1991 – 2006 Infotecs GmbH, Potsdam.

This document is part of the software distribution and is subject to the same terms and conditions as the software itself.

You may not copy, reproduce, translate or in any other form replicate this document by any means without the prior **written** consent of Infotecs GmbH.

VIPNet is a registered trade mark of Infotecs JSC, Moscow, Russia.

All Trademarks are the property of their respective owners.

Infotecs GmbH
Hebbelstraße 41
D-14469 Potsdam
Germany

Tel: +49 (331) 817 03 76

Fax: +49 (331) 817 03 77

Email: support@infotecs.biz

WWW: <http://www.infotecs.biz>

Contents

ABOUT THIS DOCUMENT	4
SCHEMES OF USING VIPNET OFFICE (TUNNEL)	4
1 VIPNET OFFICE: HEAD OFFICE TO BRANCH OFFICE	4
STEP 1. SETTINGS FOR FIREWALL OR OTHER DEVICE WITH NETWORK ADDRESS TRANSLATION FUNCTION (NAT FUNCTION)	5
STEP 2. HEAD OFFICE VIPNET COORDINATOR SETTINGS	5
STEP 3. BRANCH OFFICE VIPNET COORDINATOR SETTINGS	5
STEP 4. VIPNET CLIENT SETTINGS (IN THE HEAD AND BRANCH OFFICES)	5
2 VIPNET OFFICE: MOBILE USER TO HEAD OFFICE	6
STEP 1. SETTINGS FOR FIREWALL OR OTHER DEVICE WITH NETWORK ADDRESS TRANSLATION FUNCTION (NAT FUNCTION)	6
STEP 2. HEAD OFFICE VIPNET COORDINATOR SETTINGS	6
STEP 3. HEAD OFFICE VIPNET CLIENT SETTINGS	7
STEP 4. MOBILE USER VIPNET CLIENT SETTINGS	7
3 VIPNET OFFICE: CLIENT-TO-CLIENT CONNECTION.....	7
STEP 1. SETTINGS FOR FIREWALL OR OTHER DEVICE WITH NETWORK ADDRESS TRANSLATION FUNCTION (NAT FUNCTION)	8
STEP 2. HEAD OFFICE VIPNET COORDINATOR SETTINGS	8
STEP 3. REMOTE VIPNET CLIENT SETTINGS (HOME OR MOBILE USER).....	8
4 VIPNET TUNNEL: HEAD OFFICE TO BRANCH OFFICE.....	9
STEP 1. SETTINGS FOR FIREWALL OR OTHER DEVICE WITH NETWORK ADDRESS TRANSLATION FUNCTION (NAT FUNCTION)	9
STEP 2. HEAD OFFICE VIPNET COORDINATOR SETTINGS.....	9
STEP 3. VERIFICATION OF IP ROUTING SETTINGS	10
STEP 4. BRANCH OFFICE VIPNET COORDINATOR SETTINGS.....	10
5 VIPNET OFFICE: MOBILE USER TO HEAD OFFICE (WITH USING DYNAMIC DNS SERVICE)10	
STEP 1. SETTINGS FOR FIREWALL OR OTHER DEVICE WITH NETWORK ADDRESS TRANSLATION FUNCTION (NAT FUNCTION)	11
STEP 2. HEAD OFFICE VIPNET COORDINATOR SETTINGS	11
STEP 3. HEAD OFFICE VIPNET CLIENT SETTINGS	11
STEP 4. MOBILE USER VIPNET CLIENT SETTINGS.....	12

About This Document

This document is an appendix to user guide for Administrator, which installs ViPNet OFFICE and ViPNet TUNNEL software.

This document contains basic schemes of using the ViPNet OFFICE and ViPNet TUNNEL software and step-by-step instructions of necessary settings after installing the software.

Schemes of Using ViPNet OFFICE (TUNNEL)

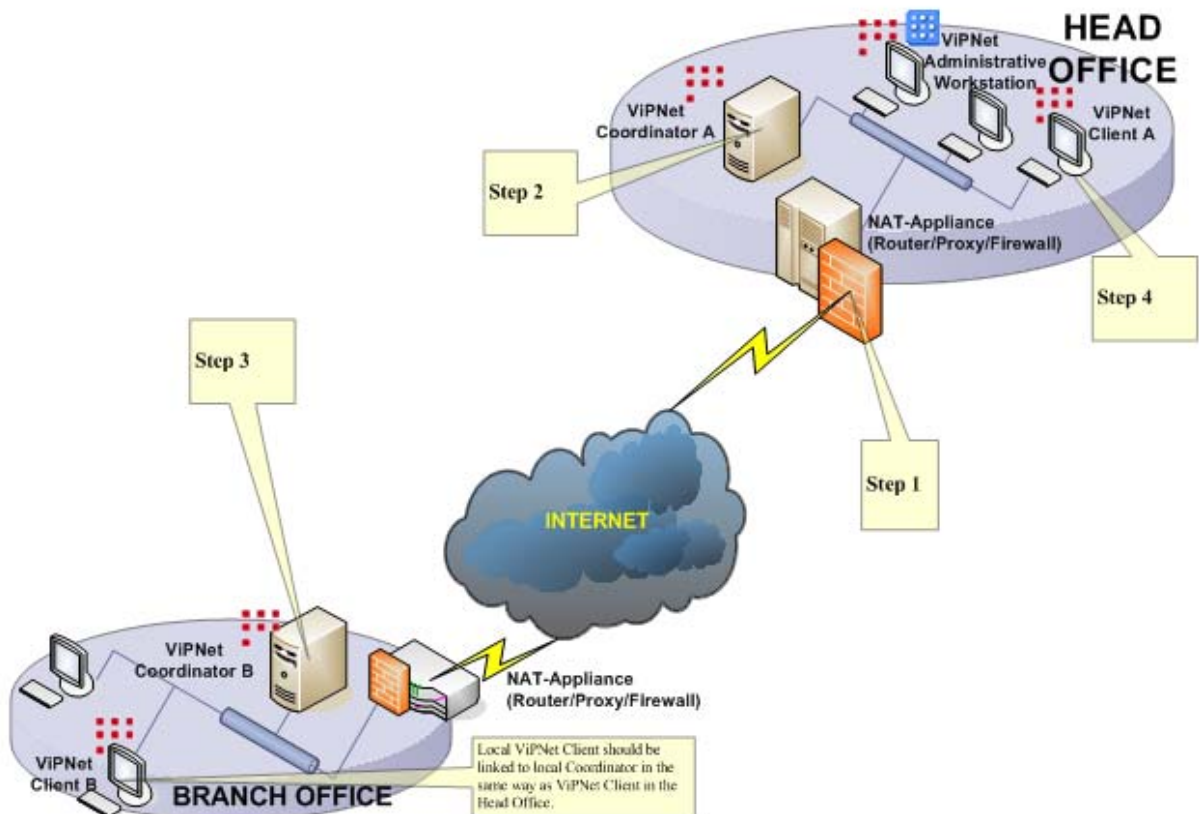
There are five basic schemes of using the ViPNet OFFICE and ViPNet TUNNEL:

1. ViPNet OFFICE: Head Office to Branch Office.
2. ViPNet OFFICE: Mobile user to Head Office.
3. ViPNet OFFICE: Client-to-Client Connection
4. ViPNet TUNNEL: Head Office to Branch Office.
5. ViPNet OFFICE: Mobile User to Head Office with using DNS names

Let's describe these schemes in detail.

1 ViPNet OFFICE: Head Office to Branch Office

This chapter describes a scheme of using ViPNet OFFICE software as applied to a connection between head office and branch office.



Now let's describe settings for ViPNet Coordinators and ViPNet Clients step-by-step:

Step 1. Settings for Firewall or Other Device with Network Address Translation Function (NAT Function)

It is recommended this NAT-Appliance to have static IP address. If it does not, user may ask vendor for more detailed information.

This NAT device or software should have following rules to redirect incoming and outgoing UDP traffic of ViPNet Coordinator:

- - allow all outgoing UDP traffic by port 55777 (or port that you define manually for this kind of traffic at Coordinator)
- - allow all incoming UDP traffic to port 55777 and redirect it to IP address of ViPNet Coordinator, which is staying behind this NAT device or another PC with NAT functioning software installed.

Step 2. Head Office ViPNet Coordinator Settings

To configure Head Office ViPNet Coordinator, please, choose **Settings** in the left section of ViPNet Coordinator Monitor window and activate the option **Use Firewall** in the right section. New fields will be accessible below. From the list of network adapters, please, select the adapter that is used to connect ViPNet Coordinator to NAT-Appliance. In the **Firewall Type** field, please, choose option **With static NAT**.

On the top of the **Settings** window you can find field **Port**. Please, fill in this field with port number that you use for configuring NAT-Appliance to redirect incoming/outgoing UDP traffic (by default 55777). The **Tunneling** button may be used to determine IP addresses of the local PCs with no ViPNet software installed, traffic from which you may want to tunnel and encrypt.

Step 3. Branch Office ViPNet Coordinator Settings

To configure the second ViPNet Coordinator B, please, select **Private Network** in left section of ViPNet Coordinator Monitor window. In the right section you have to find the name of the first ViPNet Coordinator A which is listed among network nodes of your VPN. Please, double-click on it and in the window that appears select the **Firewall** tab. Fill in **IP address** field with the IP address of NAT-Appliance from Head Office.

After that, please, change settings in the same way you already did for the first Coordinator A. Please, choose **Settings** in the left section of ViPNet Coordinator Monitor window and activate the option **Use Firewall** in the right section. New fields will be accessible below. From the list of network adapters, please, select the adapter that is used to connect ViPNet Coordinator to NAT-Appliance. In the **Firewall Type** field, please, choose option **With static NAT**.

On the top of the **Settings** window you can find field **Port**. Please, fill in this field with port number that you use for configuring NAT-Appliance to redirect incoming/outgoing UDP traffic (by default 55777). The **Tunneling** button may be used to determine IP addresses of the local PCs with no ViPNet software installed, traffic from which you may want to tunnel and encrypt.

Again, choose the first Coordinator A from the list of network nodes in the **Private Network** window and check connection with it by clicking the mouse right button and choosing **Check Connection** function in the context menu, or F5.

Step 4. ViPNet Client Settings (in the Head and Branch Offices)

To configure ViPNet Client you have to open Monitor program's window by clicking the ViPNet icon in the system tray. After that, please, select **Private Network** in the left section of the window that appears. Double-click on the name of a local Coordinator which is listed among network nodes. New window will be opened. Please, select **Firewall** tab and add the internal IP address of your local ViPNet Coordinator (this is a coordinator where this client is registered). Instead of IP address you can use DNS name. Activate **Use DNS name** field in **IP addresses** tab and fill in the DNS name of your local ViPNet Coordinator. Press **OK**.

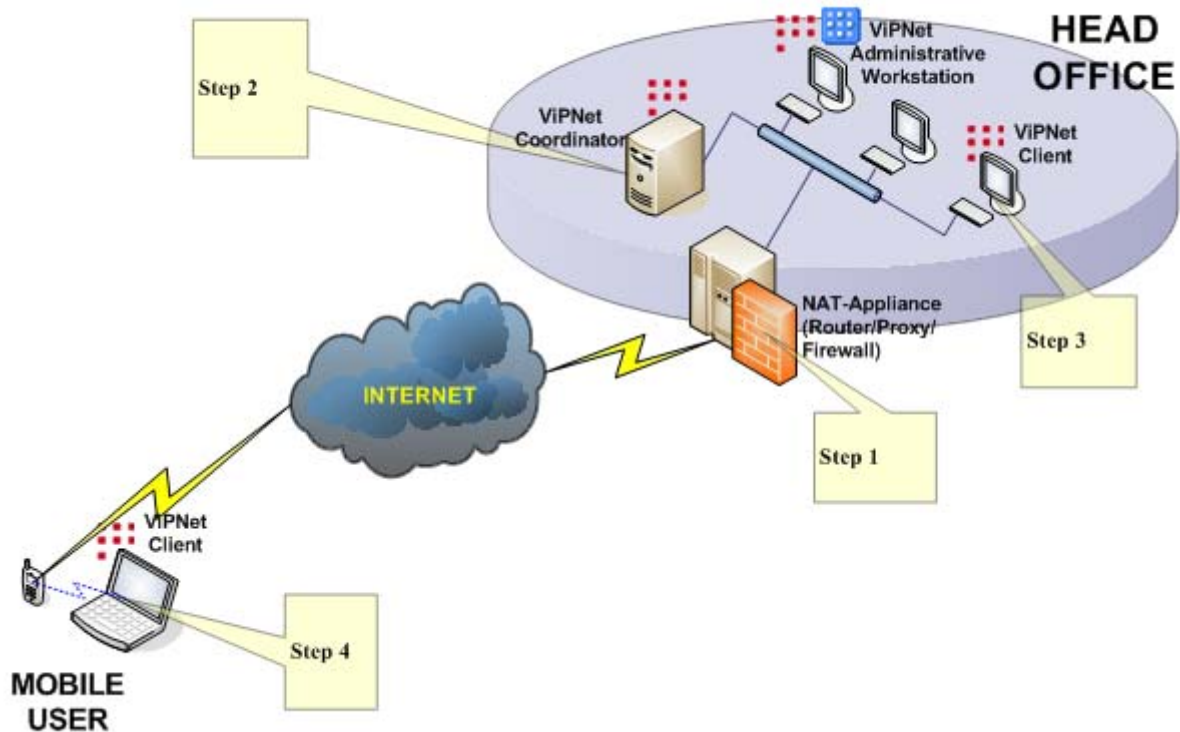
After that, please, select **Settings** in the left section of your ViPNet Monitor window and you will see your local ViPNet Coordinator in the right section. You have to activate **Use Firewall** option and define **Firewall type** as **ViPNet coordinator**. Press **Apply** button.

Again, choose Coordinator from the list in **Private Network** window and check connection with it by clicking the mouse right button and choosing **Check Connection** function in the context menu, or F5.

If all these settings are made correctly, the scheme will work.

2 ViPNet OFFICE: Mobile User to Head Office

This chapter describes a scheme of using ViPNet OFFICE software as applied to a connection between mobile user and head office.



Now let's describe settings for ViPNet Coordinators and ViPNet Clients step-by-step:

Step 1. Settings for Firewall or Other Device with Network Address Translation Function (NAT Function)

It is recommended this NAT-Appliance to have static IP address. If it does not, user may ask vendor for more detailed information.

This NAT device or software should have following rules to redirect incoming and outgoing UDP traffic of ViPNet Coordinator:

- - allow all outgoing UDP traffic by port 55777 (or port that you define manually for this kind of traffic at Coordinator)
- - allow all incoming UDP traffic to port 55777 and redirect it to IP address of ViPNet Coordinator, which is staying behind this NAT device or another PC with NAT functioning software installed.

Step 2. Head Office ViPNet Coordinator Settings

To configure Head Office ViPNet Coordinator, please, choose **Settings** in the left section of ViPNet Coordinator Monitor window and activate the option **Use Firewall** in the right section. New fields will be accessible below. From the list of network adapters, please, select the adapter that is used to connect ViPNet Coordinator to NAT-Appliance. In the **Firewall Type** field, please, choose option **With static NAT**.

On the top of the **Settings** window you can find field **Port**. Please, fill in this field with port number that you use for configuring NAT-Appliance to redirect incoming/outgoing UDP traffic (by default 55777). The **Tunneling** button may be used to determine IP addresses of the local PCs with no ViPNet software installed, traffic from which you may want to tunnel and encrypt.

Step 3. Head Office ViPNet Client Settings

To configure ViPNet Client you have to open Monitor program's window by clicking the ViPNet icon in the system tray. After that, please, select **Private Network** in the left section of the window that appears. Double-click on the name of a local Coordinator which is listed among network nodes. New window will be opened. Please, select **Firewall** tab and add the internal IP address of your local ViPNet Coordinator (this is a coordinator where this client is registered). Instead of IP address you can use DNS name. Activate **Use DNS name** field in **IP addresses** tab and fill in the DNS name of your local ViPNet Coordinator. Press **OK**.

After that, please, select **Settings** in the left section of your ViPNet Monitor window and you will see your local ViPNet Coordinator in the right section. You have to activate **Use Firewall** option and define **Firewall type** as **ViPNet coordinator**. Press **Apply** button.

Again, choose Coordinator from the list in **Private Network** window and check connection with it by clicking the mouse right button and choosing **Check Connection** function in the context menu, or F5.

Step 4. Mobile User ViPNet Client settings

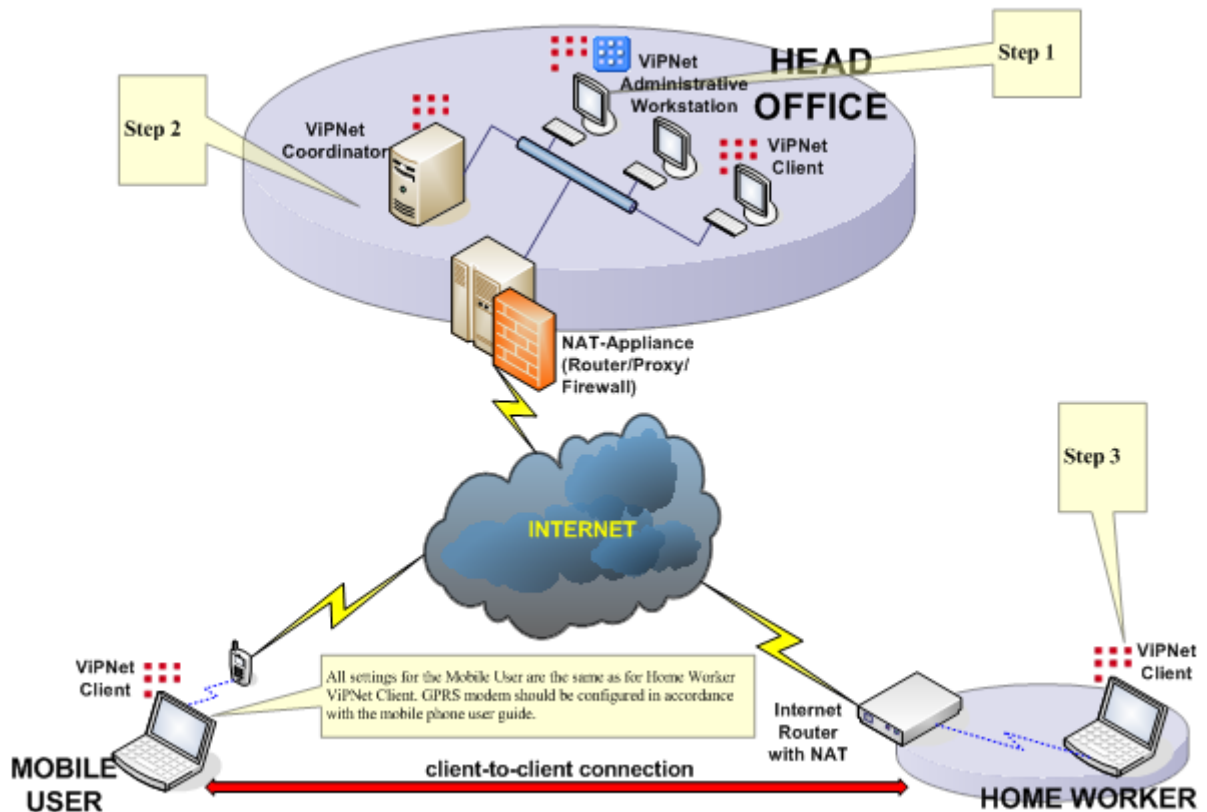
To configure ViPNet Client you have to open ViPNet Client Monitor by clicking the ViPNet icon in the system tray. After that, please, select **Private Network** in the left section of the window that appears. Double-click on the name of Coordinator which is listed among network nodes of your VPN in the right section of the Monitor. New window will be opened. Please, select the **Firewall** tab and add the public IP address of your Office NAT-Appliance.

After that, select **Settings** in the left section of your ViPNet Monitor window. You will see which ViPNet Coordinator is accessible as IP address server for your remote Client. You have to activate **Use Firewall** option and define Firewall type as **With dynamic NAT**. Click **Apply**.

Again, choose Coordinator from the list of network nodes in the **Private Network** window and check connection with it by clicking the mouse right button and choosing **Check Connection** function in the context menu, or F5.

3 ViPNet OFFICE: Client-to-Client Connection

This chapter describes a scheme of using ViPNet OFFICE software as applied to a connection between ViPNet Clients.



Now let's describe settings for ViPNet Coordinators and ViPNet Clients step-by-step:

Step 1. Settings for Firewall or Other Device with Network Address Translation Function (NAT Function)

It is recommended this NAT-Appliance to have static IP address. If it does not, user may ask vendor for more detailed information.

This NAT device or software should have following rules to redirect incoming and outgoing UDP traffic of ViPNet Coordinator:

- - allow all outgoing UDP traffic by port 55777 (or port that you define manually for this kind of traffic at Coordinator)
- - allow all incoming UDP traffic to port 55777 and redirect it to IP address of ViPNet Coordinator, which is staying behind this NAT device or another PC with NAT functioning software installed.

Step 2. Head Office ViPNet Coordinator Settings

To configure Head Office ViPNet Coordinator, please, choose **Settings** in the left section of ViPNet Coordinator Monitor window and activate the option **Use Firewall** in the right section. New fields will be accessible below. From the list of network adapters, please, select the adapter that is used to connect ViPNet Coordinator to NAT-Appliance. In the **Firewall Type** field, please, choose option **With static NAT**.

On the top of the **Settings** window you can find field **Port**. Please, fill in this field with port number that you use for configuring NAT-Appliance to redirect incoming/outgoing UDP traffic (by default 55777). The **Tunneling** button may be used to determine IP addresses of the local PCs with no ViPNet software installed, traffic from which you may want to tunnel and encrypt.

Step 3. Remote ViPNet Client Settings (Home or Mobile User)

To configure ViPNet Client you have to open ViPNet Client Monitor by clicking the ViPNet icon in the system tray. After that, please, select **Private Network** in the left section of the window that appears. Double-click on the name of Coordinator which is listed among network nodes of your VPN in the right

section of the Monitor. New window will be opened. Please, select the **Firewall** tab and add the public IP address of your Office NAT-Appliance. Click **OK**.

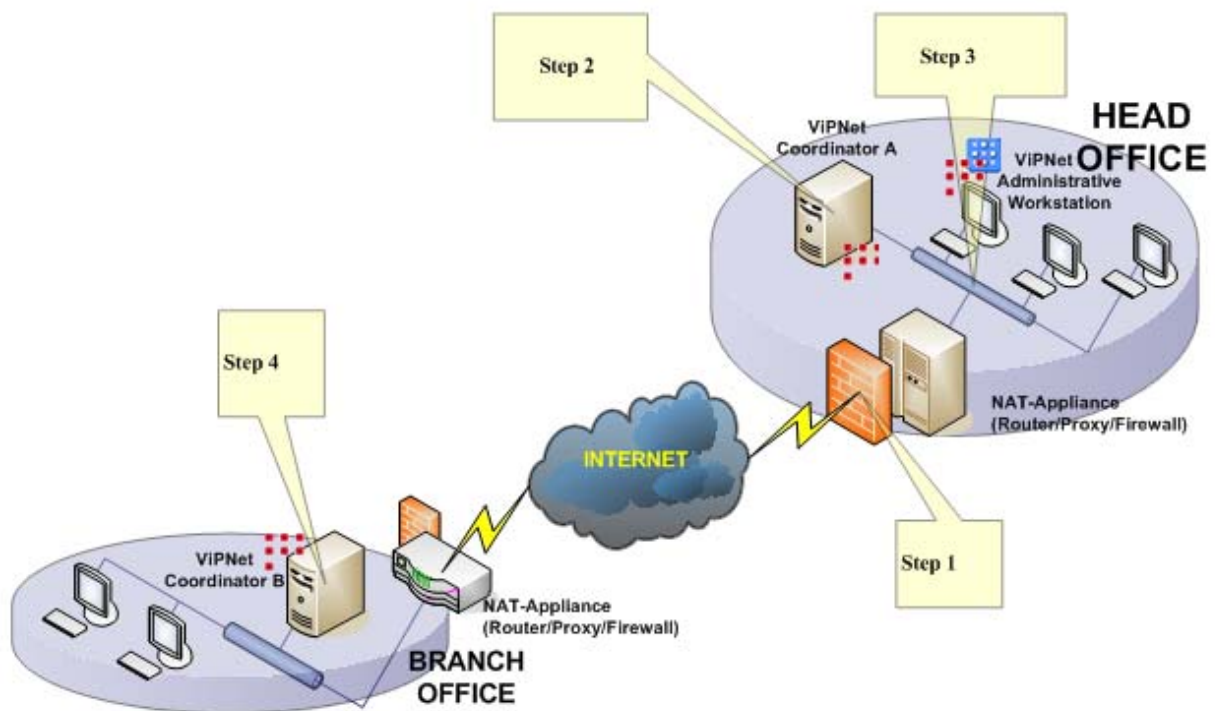
After that, select **Settings** in the left section of your ViPNet Monitor window. You will see which ViPNet Coordinator is accessible as IP address server for your remote Client. You have to activate **Use Firewall** option and define Firewall type as **With dynamic NAT**. Click **Apply**.

Again, choose Coordinator from the list of network nodes in the **Private Network** window and check connection with it by clicking the mouse right button and choosing **Check Connection** function in the context menu, or F5.

If all these settings are made correctly, the scheme will work.

4 ViPNet TUNNEL: Head Office to Branch Office

This chapter describes a scheme of using ViPNet TUNNEL software as applied to a connection between head office and branch office.



Now let's describe settings for ViPNet Coordinators and ViPNet Clients step-by-step:

Step 1. Settings for Firewall or Other Device with Network Address Translation Function (NAT Function)

It is recommended this NAT-Appliance to have static IP address. If it does not, user may ask vendor for more detailed information.

This NAT device or software should have following rules to redirect incoming and outgoing UDP traffic of ViPNet Coordinator:

- - allow all outgoing UDP traffic by port 55777 (or port that you define manually for this kind of traffic at Coordinator)
- - allow all incoming UDP traffic to port 55777 and redirect it to IP address of ViPNet Coordinator, which is staying behind this NAT device or another PC with NAT functioning software installed.

Step 2. Head Office ViPNet coordinator Settings

To configure the first ViPNet Coordinator in the Head Office, please, select **Settings** in the left section of ViPNet Coordinator Monitor and activate **Use Firewall** option. New fields will be accessible below. From the list of network adapters, please, select the adapter which is used to connect ViPNet

Coordinator to its nearest NAT-Appliance. In the **Firewall Type** field, please, select **With static NAT** option.

On the top of the right section of **Settings** window you can find **Port** field. Please, fill in this field with port number that you used for configuring NAT-Appliance to redirect incoming/outgoing UDP traffic (by default 55777). The **Tunneling** button may be used to determine IP addresses of the local PCs with no ViPNet software installed, traffic from which you may want to tunnel and encrypt. IP addresses may be set as ranges or individual values. You also need to determine IP addresses of the local PCs which are tunneled by Coordinator B. To make these settings: in the *Private network* window, double-click on the Coordinator B. The **Access rule** window will appear. Select **Tunnel** tab. To enter new ranges or individual IP address values for tunneling enable the **Use IP addresses for tunneling** option and then use the **Add** button to add new addresses; the old settings can be modified with the **Change** button.

Step 3. Verification of IP routing Settings

You have to make sure that IP routing is right for the tunneling through Coordinator A (or B). If Coordinator is the default gateway for internal PCs then you do not need to setup any additional routing rules. If your internal PCs have a firewall (dsl, internet gateway) as a default gateway (in most cases) you must make additional routing rules so that your information for the tunneling will go through Coordinator. How to setup these rules please check at the forum at <http://www.infotecs.biz/board/en/> or send your questions: support@infotecs.biz.

Step 4. Branch Office ViPNet Coordinator Settings

To configure the second ViPNet Coordinator, please, select **Private Network** in the left section of ViPNet Coordinator Monitor window. In the right section you have to find the name of the first installed ViPNet Coordinator which is listed among network nodes of your Demo. Please, double-click on the name of this Coordinator, new window will be opened. Select the **Firewall** tab and fill in **IP address** field with the IP address of NAT-Appliance from Head Office.

Sometimes, depending on the NAT-Appliance kind, you may also have to choose the **IP addresses** tab and add the local IP address of the Coordinator A. Instead of IP address you can use DNS name. Activate **Use DNS name** field and fill in the DNS name of Coordinator A.

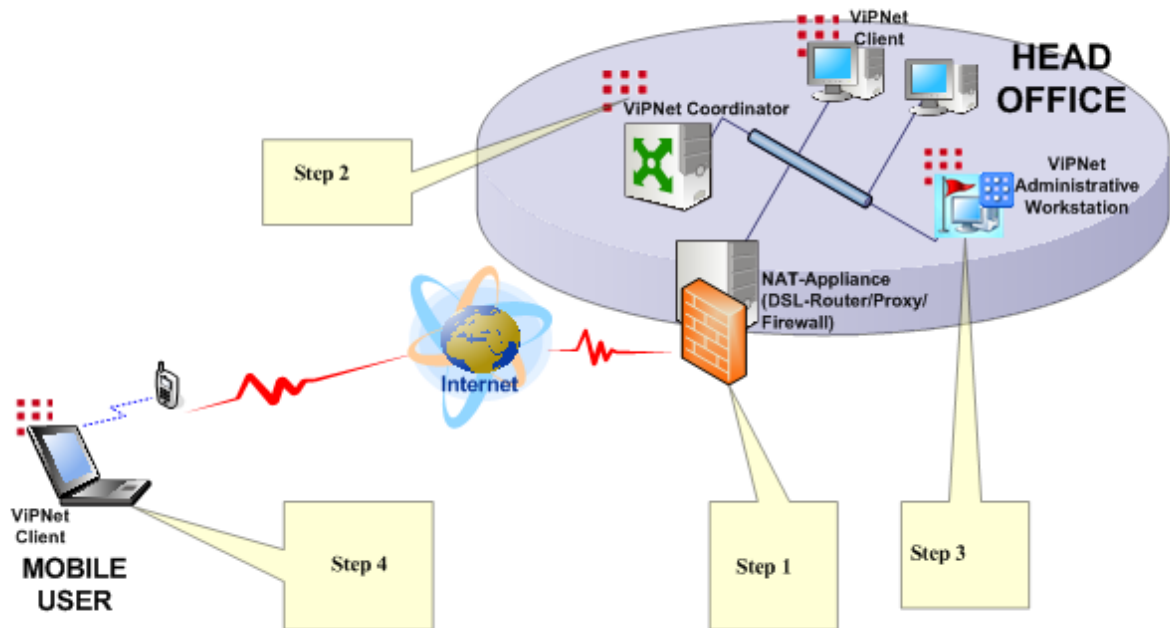
After that, please, change settings in the same way you already did for the first Coordinator.

To make sure that tunnel works choose the first Coordinator from the list of network nodes in the **Private Network** window and check connection with it by clicking the mouse right button and choosing **Check Connection** function in the context menu, or F5.

If all these settings are made correctly, the scheme will work.

5 ViPNet OFFICE: Mobile User to Head Office (with Using Dynamic DNS Service)

This chapter describes a scheme of using ViPNet OFFICE software as applied to a connection between mobile user and head office with using Dynamic DNS Service.



Now let's describe settings for ViPNet Coordinators and ViPNet Clients step-by-step:

Step 1. Settings for Firewall or Other Device with Network Address Translation Function (NAT Function)

It is recommended this NAT-Appliance to have static IP address. If it does not, user may ask vendor for more detailed information. Instead of static IP address Dynamic DNS service may be used.

This NAT device or software should have following rules to redirect incoming and outgoing UDP traffic of ViPNet Coordinator:

- - allow all outgoing UDP traffic by port 55777 (or port that you define manually for this kind of traffic at Coordinator)
- - allow all incoming UDP traffic to port 55777 and redirect it to IP address of ViPNet Coordinator, which is staying behind this NAT device or another PC with NAT functioning software installed.

Step 2. Head Office ViPNet Coordinator Settings

To configure Head Office ViPNet Coordinator, please, choose **Settings** in the left section of ViPNet Coordinator Monitor window and activate the option **Use Firewall** in the right section. New fields will be accessible below. From the list of network adapters, please, select the adapter that is used to connect ViPNet Coordinator to NAT-Appliance. In the **Firewall Type** field, please, choose option **With static NAT**.

On the top of the **Settings** window you can find field **Port**. Please, fill in this field with port number that you use for configuring NAT-Appliance to redirect incoming/outgoing UDP traffic (by default 55777). Activate the option **Fix external IP address...** only if static IP address is used to accomplish Internet connection. In this case fill this IP address in the **External IP address** field.

The **Tunneling** button may be used to determine IP addresses of the local PCs with no ViPNet software installed, traffic from which you may want to tunnel and encrypt.

Step 3. Head Office ViPNet Client Settings

To configure ViPNet Client you have to open Monitor program's window by clicking the ViPNet icon in the system tray. After that, please, select **Private Network** in the left section of the window that appears. Double-click on the name of a local Coordinator which is listed among network nodes. New window will be opened. Please, select **Firewall** tab and add the internal IP address of your local ViPNet Coordinator (this is a coordinator where this client is registered). Instead of IP address you can use DNS name. Activate **Use DNS name** field in **IP addresses** tab and fill in the DNS name of your local ViPNet Coordinator. Press **OK**.

After that, please, select **Settings** in the left section of your ViPNet Monitor window and you will see your local ViPNet Coordinator in the right section. You have to activate **Use Firewall** option and define **Firewall type** as **ViPNet coordinator**. Press **Apply** button.

Again, choose Coordinator from the list in **Private Network** window and check connection with it by clicking the mouse right button and choosing **Check Connection** function in the context menu, or F5.

Step 4. Mobile User ViPNet Client settings

To configure ViPNet Client you have to open ViPNet Client Monitor by clicking the ViPNet icon in the system tray. After that, please, select **Private Network** in the left section of the window that appears. Double-click on the name of Coordinator which is listed among network nodes of your VPN in the right section of the Monitor. New window will be opened. Please, select the **Firewall** tab and add the public IP (static) address of your Office NAT-Appliance or its dynamic DNS name. If you are not using standard port 55777 than change the meaning of the port number in the **Port** field. Sometimes depending on the NAT-Appliance type you have to additionally define the local IP address of your ViPNet Coordinator in the **IP addresses** tab.

After that, select **Settings** in the left section of your ViPNet Monitor window. You will see which ViPNet Coordinator is accessible as IP address server for your remote Client. You have to activate **Use Firewall** option and define Firewall type as **With dynamic NAT**. Click **Apply**.

Again, choose Coordinator from the list of network nodes in the **Private Network** window and check connection with it by clicking the mouse right button and choosing **Check Connection** function in the context menu, or F5.

If all these settings are made correctly, the scheme will work.