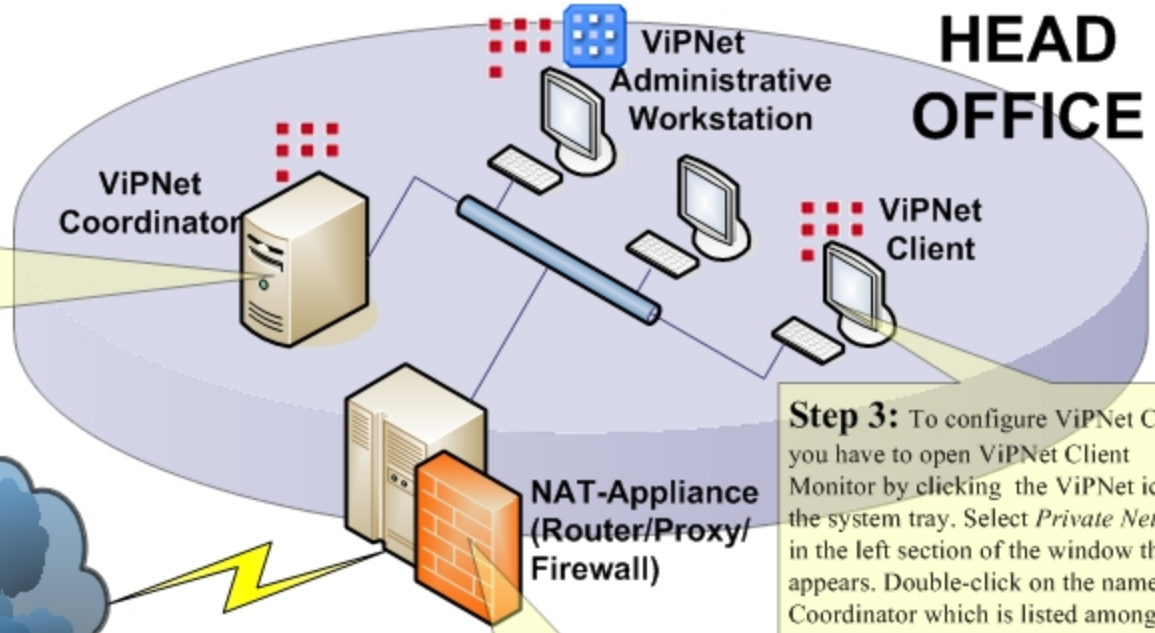
ViPNet OFFICE: mobile user to head office

Step 2: 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: To configure ViPNet Client you have to open ViPNet Client Monitor by clicking the ViPNet icon in the system tray. 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 IP address of your local ViPNet Coordinator. OK. 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. After that, please, select *Settings* in the left section of your ViPNet Monitor. You will see your local ViPNet Coordinator in the right section. You have to activate *Use Firewall* option and select Firewall type as ViPNet Coordinator. 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.

Step 1: 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.

MOBILE USER

Step 4: 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.