

ViPNet TUNNEL: Head Office to Branch Office

Step 2: To configure the first ViPNet Coordinator in the Head Office, please, select

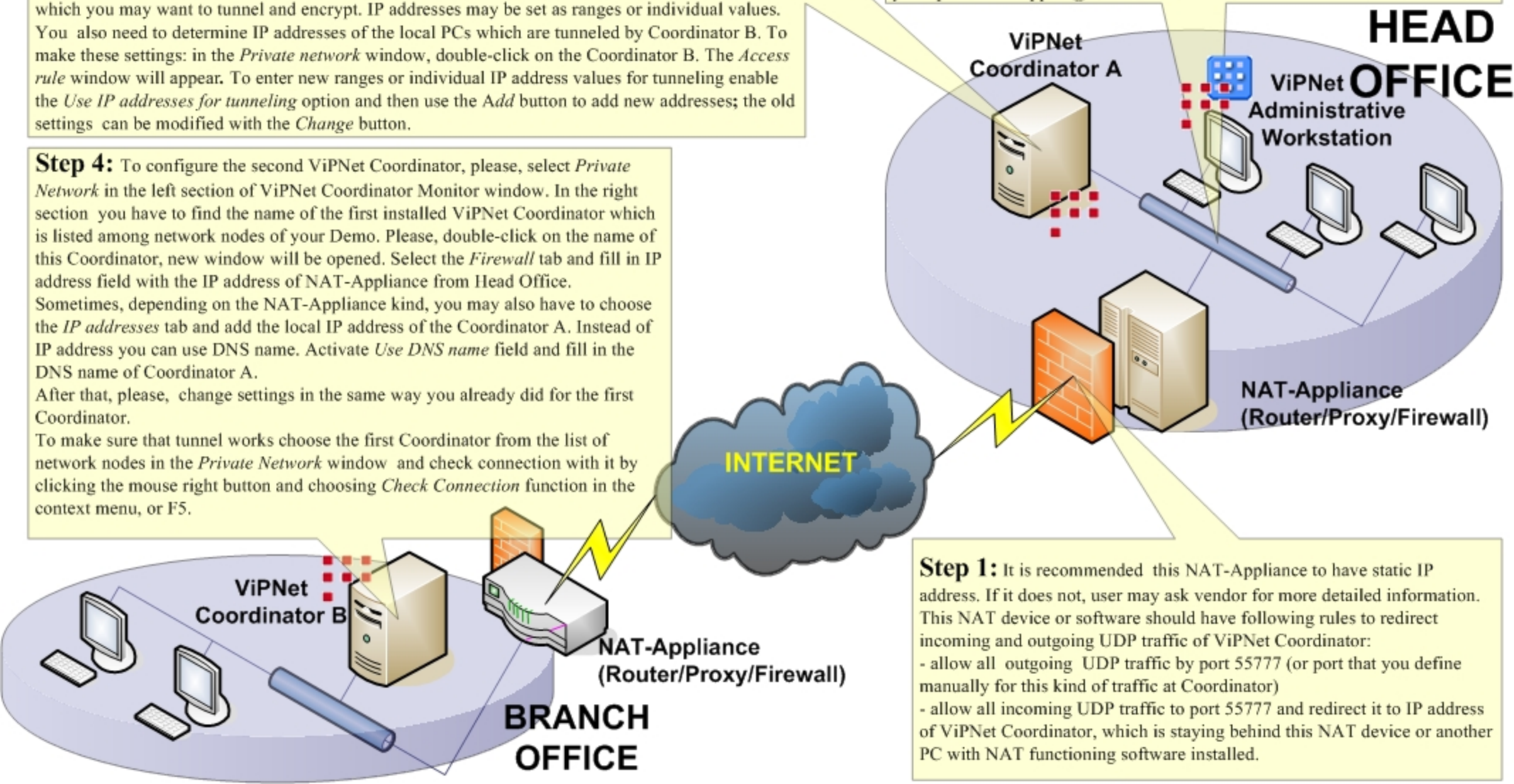
Settings in the left section of ViPNet Coordinator Monitor and activate *Use Firewall* option. New fields will be accessible below. From the list of network adapters, please, select the adapter which is used to connect ViPNet Coordinator to its nearest NAT-Appliance. In the *Firewall Type* field, please, 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. 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 4: 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.

Step 3: 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 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.