

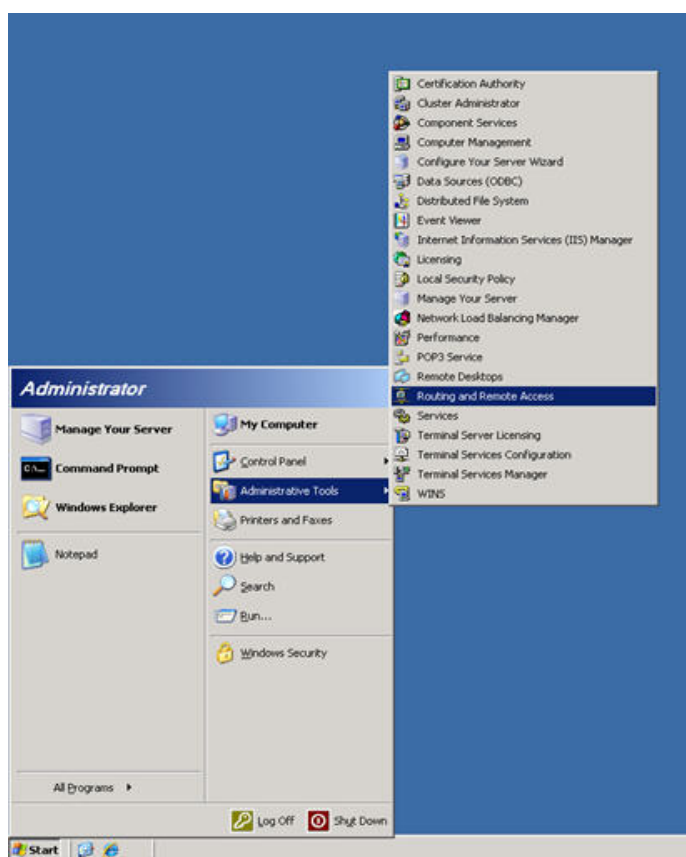
Enabling VPN on your VPS

Part 1 – Configuring VPN Access to your VPS Environment

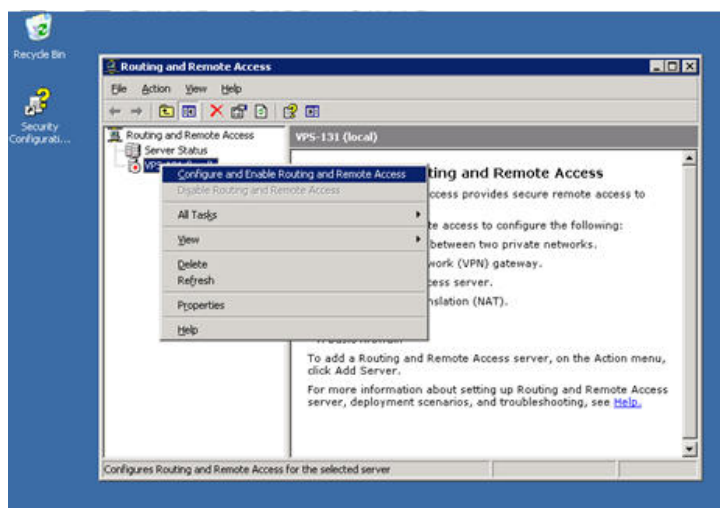
The first six (6) steps in this configuration guide outline the steps to enable a VPN connection to your VPS environment. In Addition, most VPS administrators will want the added security provided by a firewall. Steps 7 through 13 provide the instruction for setting up a basic firewall.

The firewall will block non-secure connections to your VPS environment. However without “punching holes” into the firewall you will not be able to access the VPS via Remote Desktop and you will be locking both yourself, and your customers, from the ability to connect to the VPS. Therefore it is critical that you follow steps 14 through 18 to enable the VPN ports in order for VPN and Remote Desktop to work.

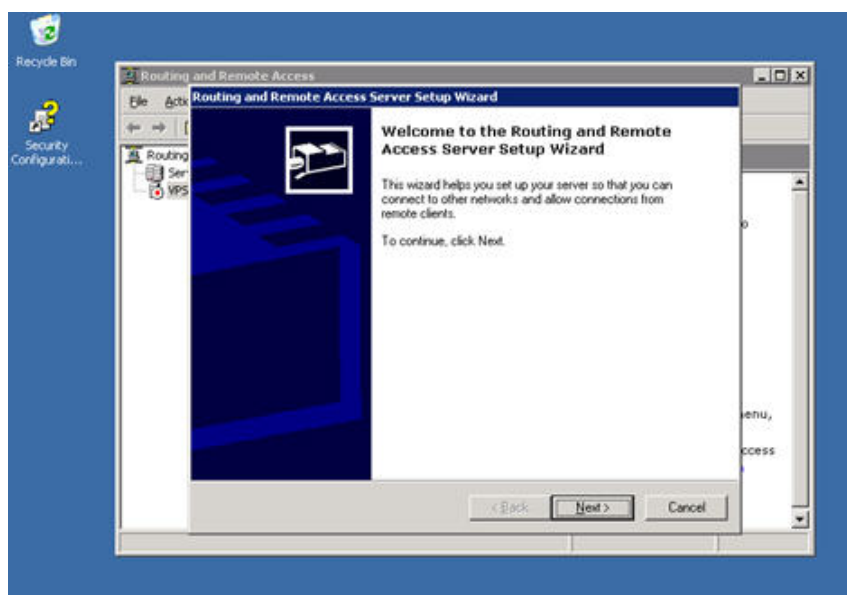
- 1) The first thing that you’ll need to do is open a ticket with support asking that **Routing and Remote Access** be “enabled” on your VPS. We’ll need your account number and VPS subscription number in order to do this.
- 2) Once this has been completed by MailStreet, Remote Desktop into you VPS node.
- 3) Once connected, select **Start |Administrative Tools | Routing and Remote Access**:



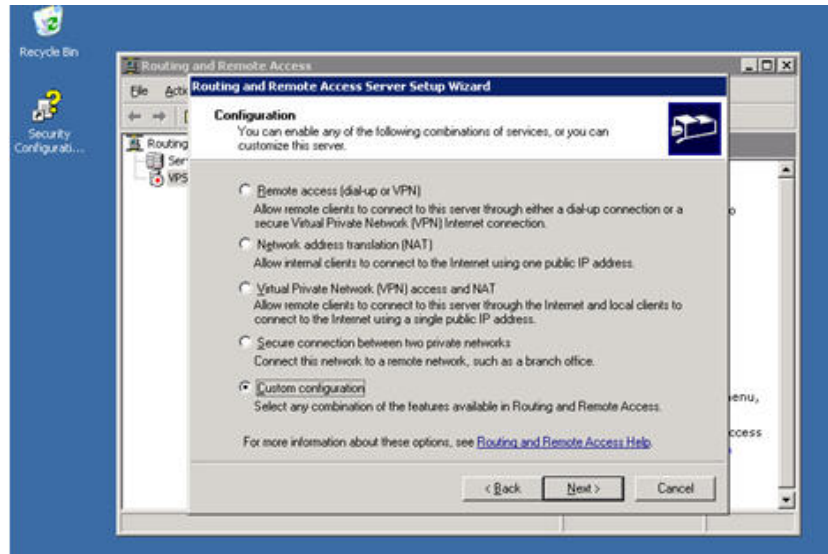
- 4) Right-Click on the displayed machine name and select **“Configure and Enable Routing and Remote Access”**:



- 5) When the configuration wizard starts, click the **[Next]** button:



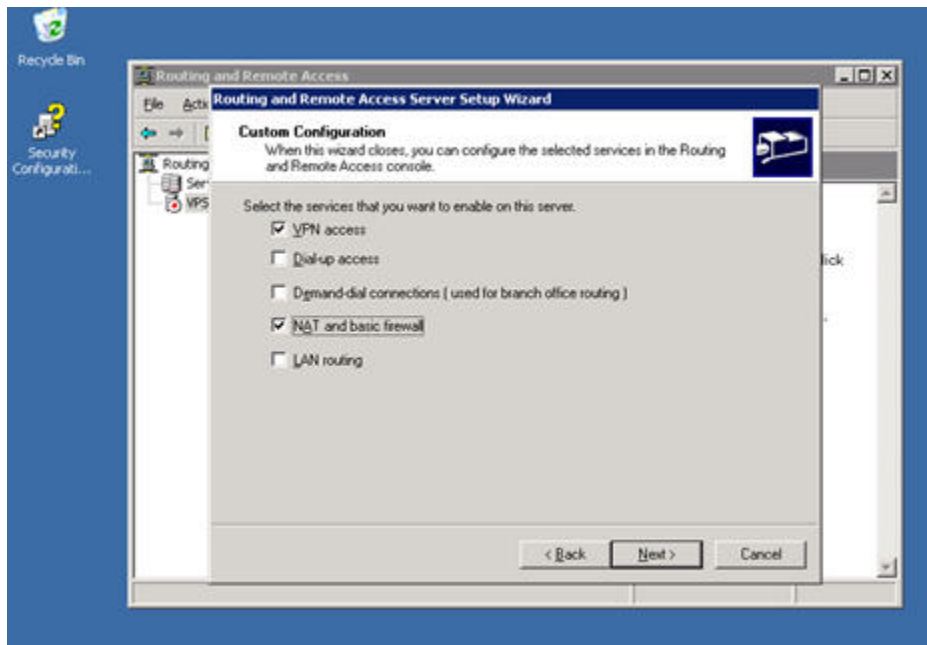
6) Select the **Custom Configuration** option, then click the **[Next]** button:



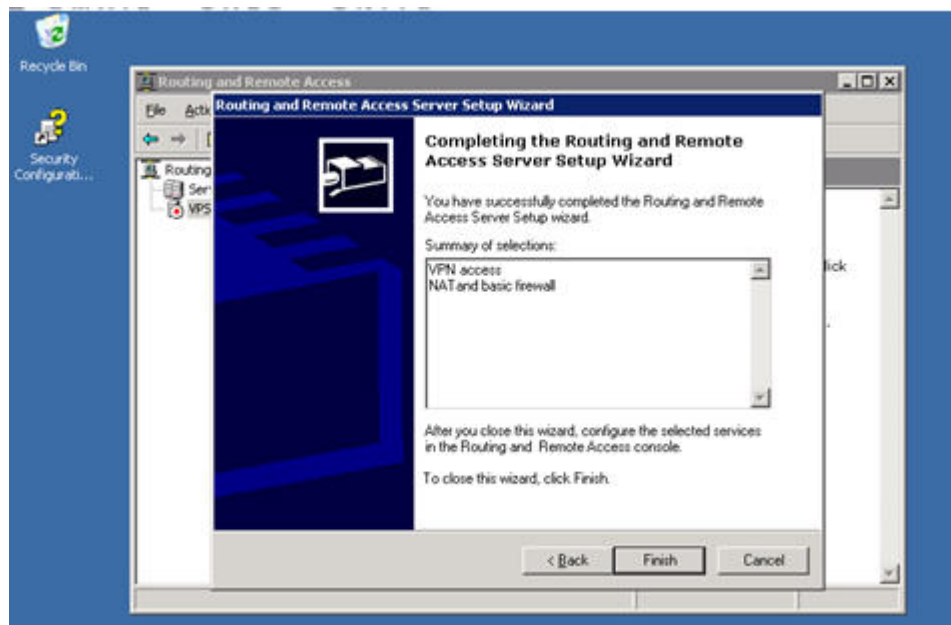
Part 2 -- Configuring IP Address Pool for VPN clients.

Steps 7 through 13 provide the instruction for setting up the IP Address Pool for connecting clients (users), but you must also complete all of the instruction provided in steps 14 through 18 to ensure that the Firewall allows VPN communication to your VPS environment.

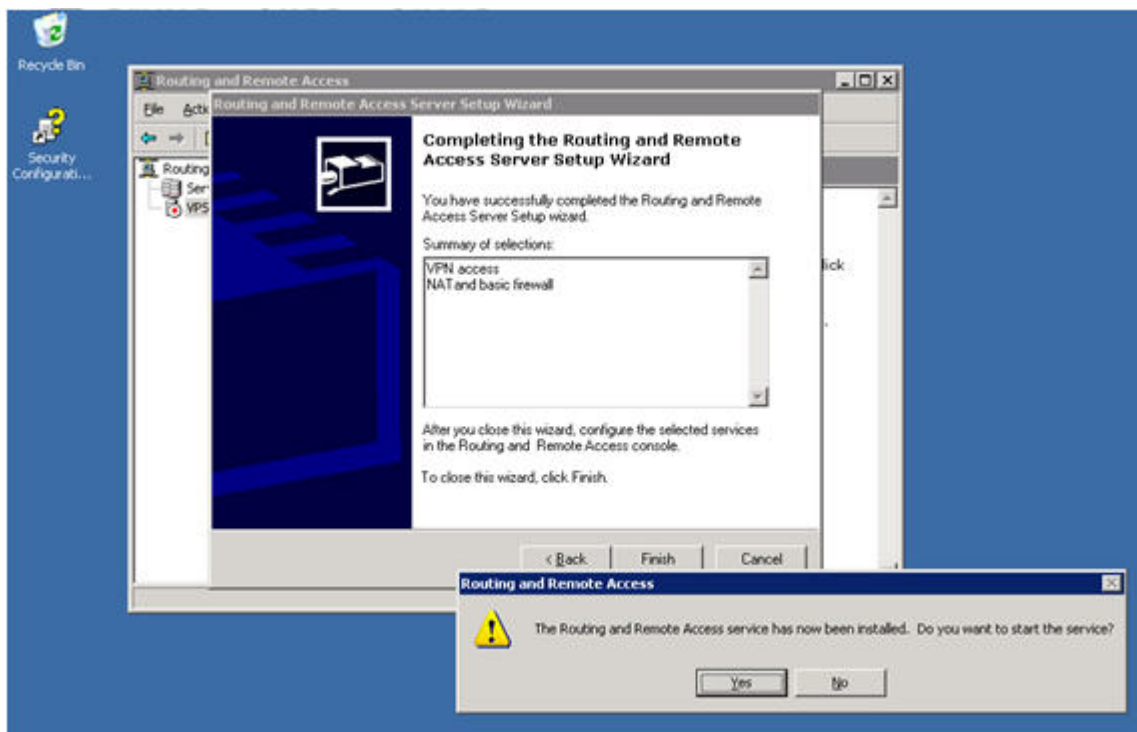
- 7) Click multiple selections: **VPN access** and **NAT and Basic firewall**, and then click the **[Next]** button:



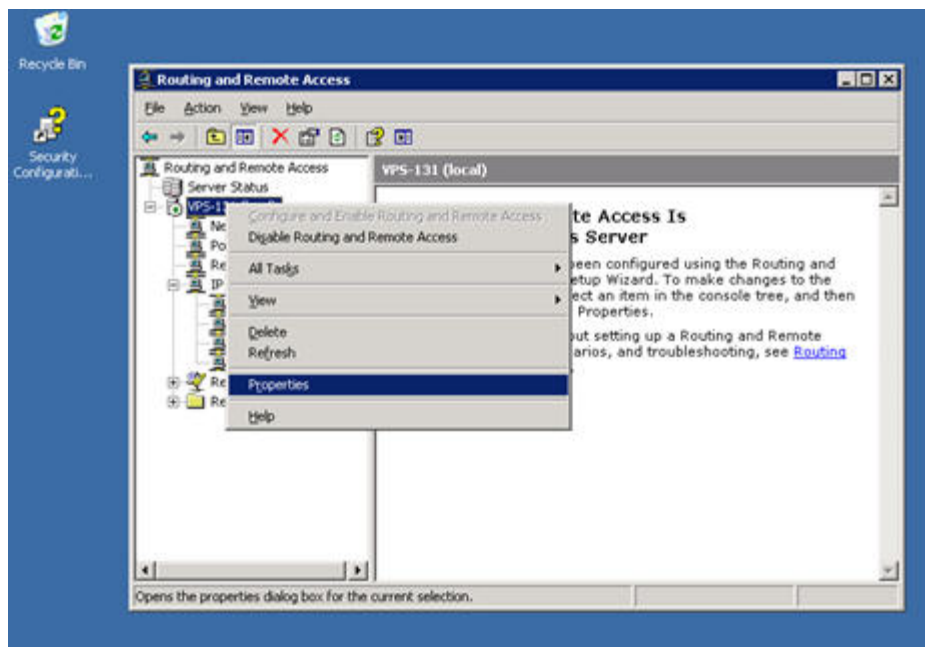
- 8) Verify that both options are selected and click the **[Finish]** button:



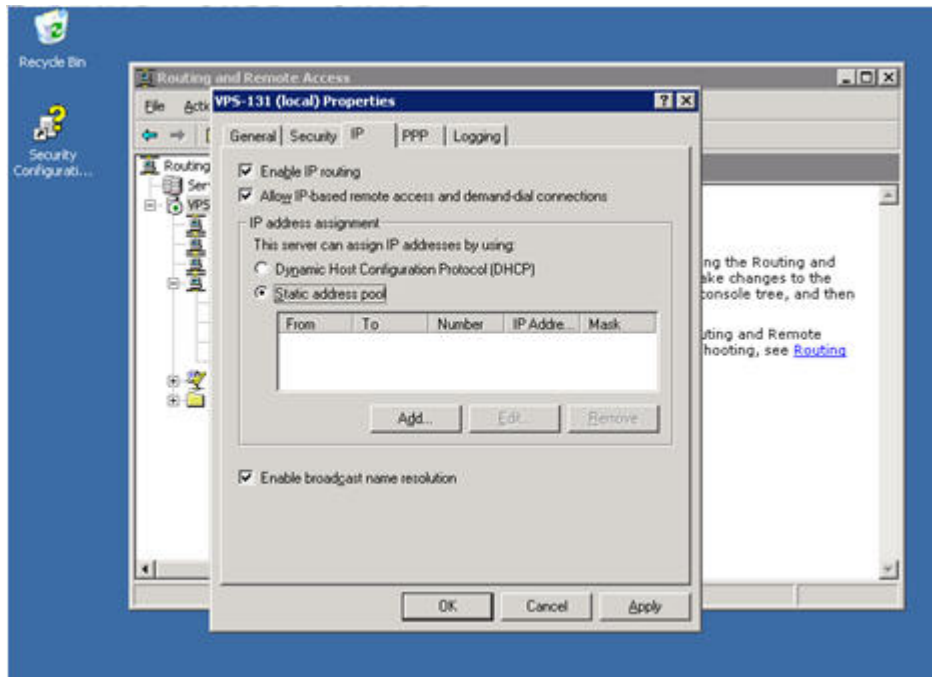
- 9) Click the **[Yes]** button to start the Routing and Remote Access Service (RRAS) and wait for the service to start:



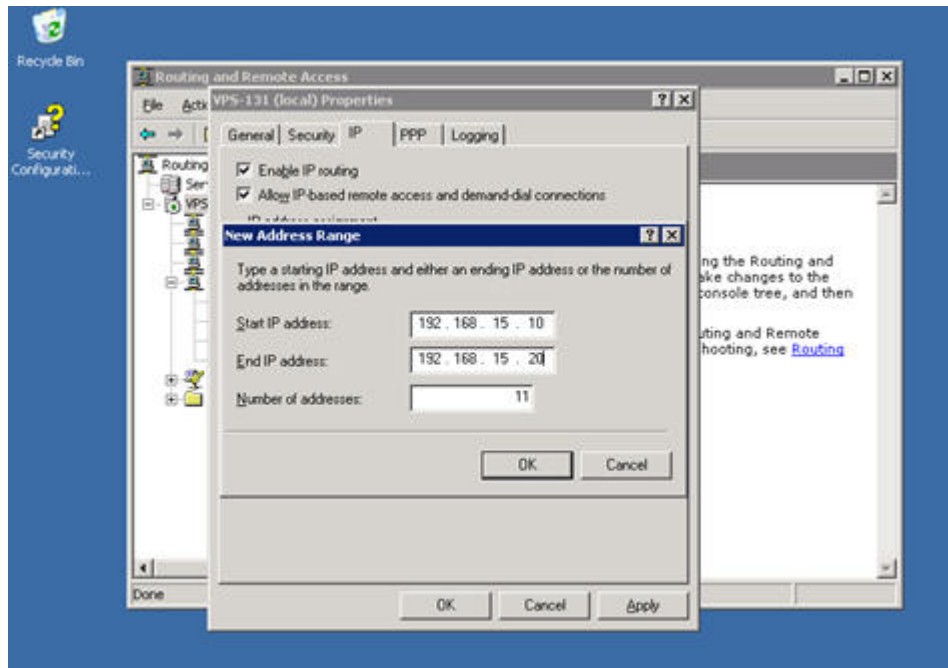
- 10) Once the RRAS service has started, you'll need to assign an IP pool for it to use. In the **Routing and Remote Access Window**, Right-click on the Machine Name and select **Properties** from the menu:



11) Choose the IP Tab and then select the Static address Pool option:



- 12) Hit the **[Add]** button, then enter a starting address (**192.168.15.10**), and an ending address (**192.168.15.20**) You can use this block or select your own – just make sure that the block you choose is
- not the same as the network(s) that you will be connecting from, and
 - The block you assign uses private address space (**192.168.x.x / 172.16.32.x / 10.0.0.0**)

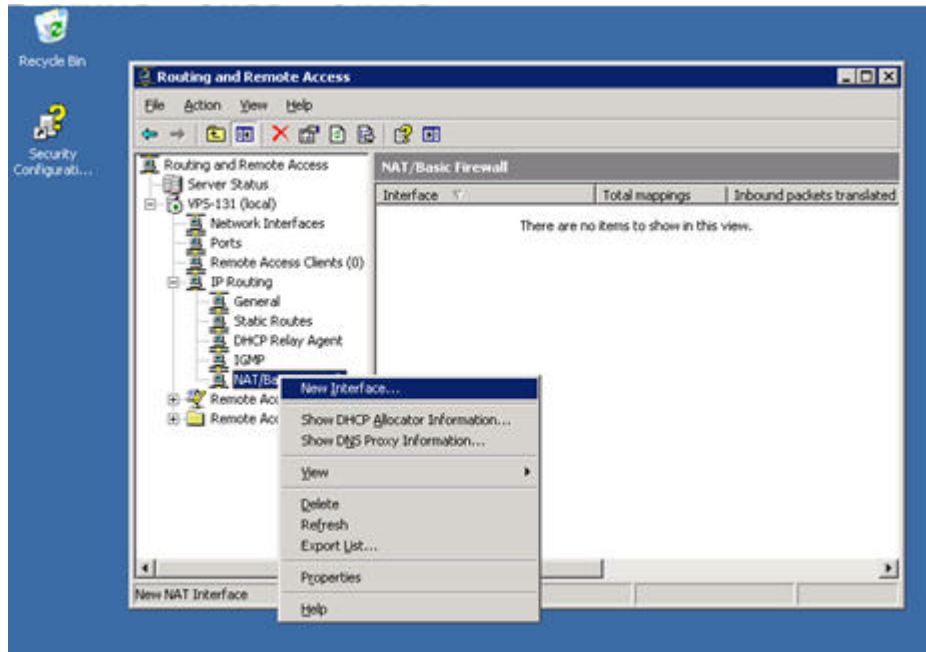


13) Select **[OK]**, then **[Apply]**. Routing and Remote Access / VPN is now enabled and running on your VPS.

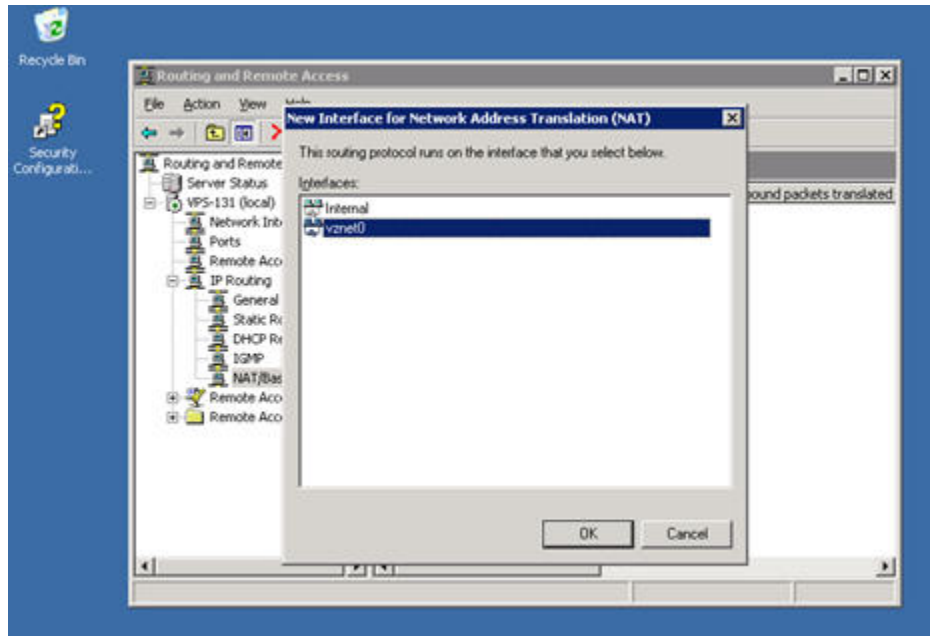
Part 3 - Enable Services to run through the Firewall

It is important that you complete the remaining steps in order to allow services (such as Remote Desktop and VPN) to run through your Firewall, AS A MINIMUM, you DO want to enable Remote service (port 3389) and VPN service (port 1723).

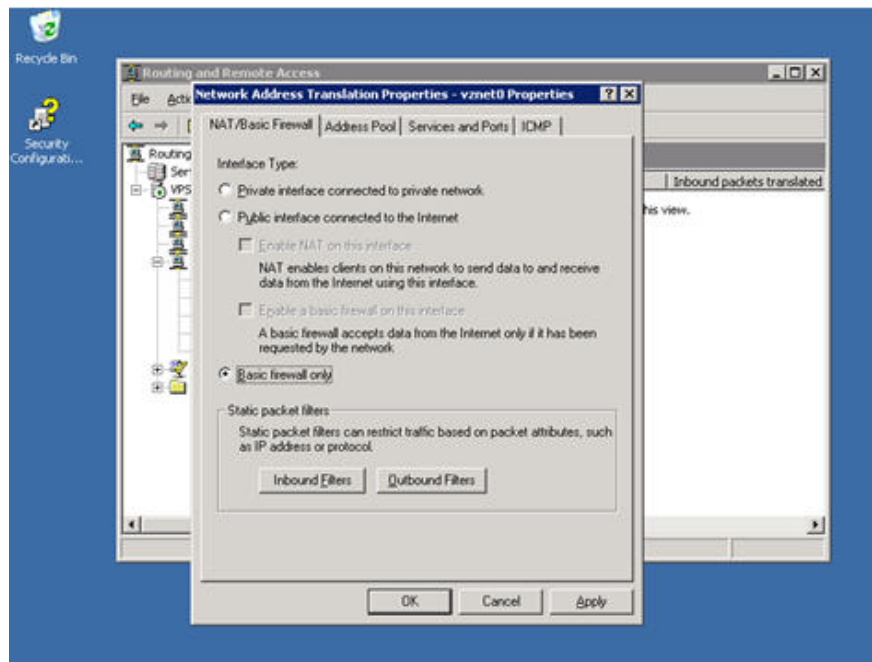
- 14) To secure or lockdown you VPS instance so that only those ports this VPS needs to support are accessible from the “outside” you’ll need to configure and Enable the Routing and Remote Access Basic Firewall. To do this, right-click on the **NAT/Firewall** icon under the **IP Routing** options and select **New Interface....** from the menu:



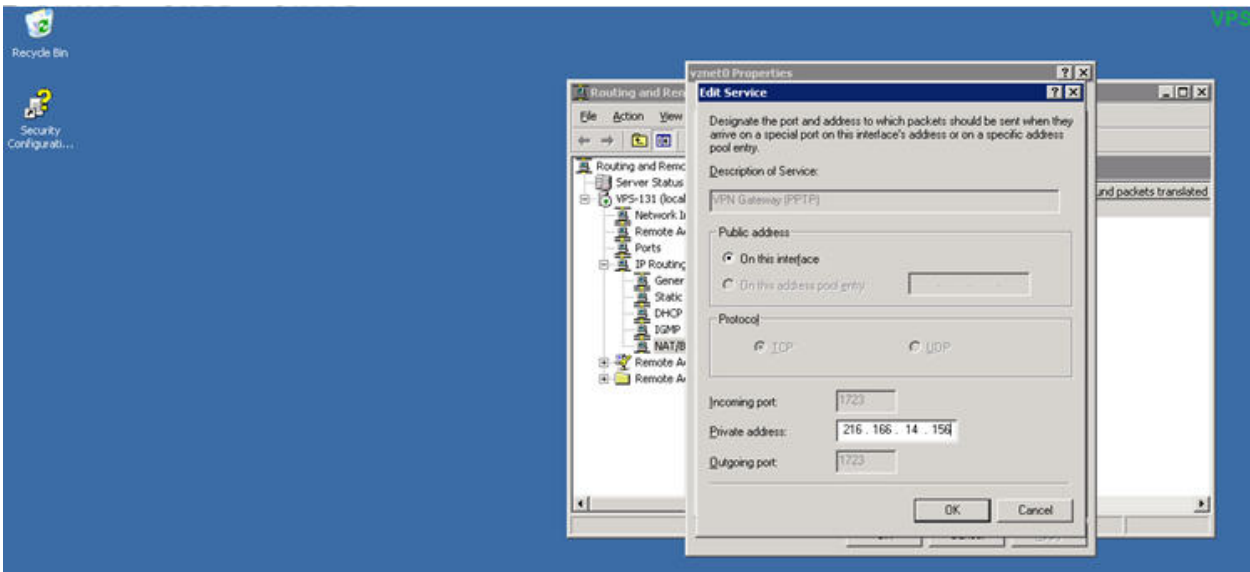
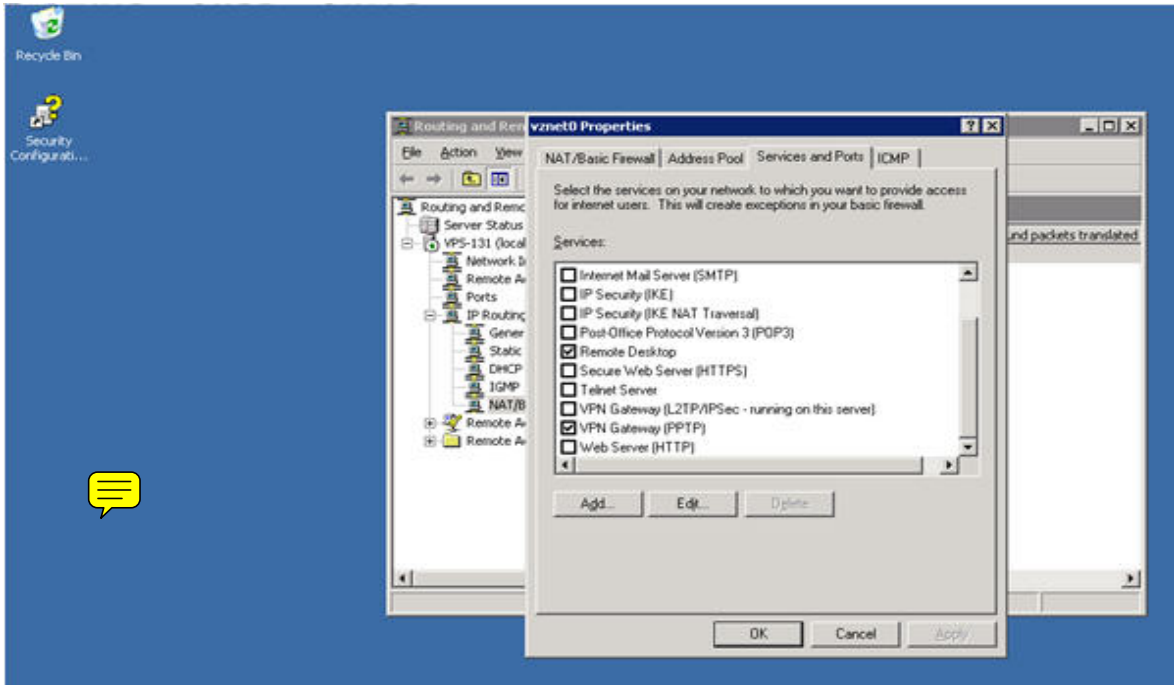
15) Choose the **vznet0** option, then click the [OK] button:



16) Choose the **Basic Firewall Only Option** and click the [OK] button:



- 17) From the **Services and Ports** Tab, check those boxes next to the application ports you want to be able to access from the network/Internet. For Example, Remote Desktop or VPN (PPTP). Each time you select a port, you'll be prompted to enter a private IP address, this will be the address of the VPS (for example 216.166.14.156):



- 18) Be careful! If you do not do this correctly, you will prevent yourself from connecting to your VPS.

If this happens, call support and have them “Stop” the Routing and Remote Access Service on your VPS, RDP back in and make the appropriate changes.