

Re: Site-to-Site VPN client routing question – clients at branch office not able to access network at HQ

Re: Site-to-Site VPN client routing question – clients at branch office not able to access network at HQ

Source:

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.networking/2007-10/msg00306.html>

- *From:* "Bill Grant" <not.available@online>
 - *Date:* Sun, 14 Oct 2007 15:22:14 +1000
-

First of all, a warning about using a DC as a router. This is always a bad idea.

Your DC might only have one NIC, but as soon as your VPN connection is made it has two IP addresses, so you get all sorts of problems (the old multihomed DC problems from N T plus some new ones). I would recommend that you use some other machine as your router, not the DC.

The next thing to note is that you do not have two links. The routing works through the one VPN link. The routing is set up on the demand-dial interfaces, so it is important that the demand-dial interfaces are actually bound to the connection, no matter which server initiates the connection.

You do not need to manually enter any IP addresses on the clients to get the routing to work. All the routing is done by the RRAS servers.

On the RRAS server at HQ, configure a demand-dial interface. Using the new static route wizard in RRAS, configure a route to 192.168.1.0/24 but do not enter a gateway address. Instead, select the demand-dial interface from the dropdown list. This route will be stored in the registry until something connects to the dd interface.

On the RRAS server in Shanghai, configure a demand-dial interface and give it a static route to 194.1.1.0/24 as above. Configure this interface to initiate a VPN connection to the RRAS server in Singapore. Note that you must use the name of the demand-dial interface on the Singapore RRAS server as your username. This makes sure that the connection is made to the correct dd interface and sets up the correct route back to Shanghai through the VPN link.

When the Singapore RRAS router gets the connection request it checks that the username matches one of its demand-dial interfaces. (If it does not, it connects like a dialup VPN client and the static route is not added to the routing table. Site to site routing then fails). When the connection is made to the dd interface, the subnet route back to Shanghai is added to the routing table using the dd interface as the gateway.

Now the VPN link acts like a simple IP router. Any traffic for the Singapore subnet reaching the Shanghai RRAS router is sent through the VPN tunnel. Similarly any traffic reaching the RRAS server in Singapore which is on the Shanghai subnet will be routed through the VPN tunnel.

If you always connect from the Shanghai end, you are finished. If you want to be able to connect from Singapore you need to make sure that you can use the name of the dd interface on the Shanghai RRAS server

Re: Site-to-Site VPN client routing question – clients at branch office not able to access network at HQ

Re: Site-to-Site VPN client routing question – clients at branch office not able to access network at HQ

as the username and that the Shanghai server has this name set up as a valid account name.

This setup assumes that the RRAS routers are the default gateways for each LAN. If they are not you need extra routing on the LAN to get the VPN traffic to the RRAS routers.

"Hii Sing Chung" <singchung@xxxxxxxxxxx> wrote in message
news:0481E662-8754-4E23-AD46-415A48BCDED1@xxxxxxxxxxxxxxxxxxx

I have a small network (5 clients) at Shanghai (192.168.1.0/24) and my HQ is in Singapore (97 clients, 194.1.1.0/24). My task is to connect the 2 networks using Windows RRAS. In HQ I already has a RRAS server (SGRAS01) that I setup using Windows 2000 server. It has been running well for 5 years, serving VPN clients. SGRAS01 has 2 physical network interfaces, one connecting to the Internet, one sitting on 194.1.1.0 network. I set up a Windows 2003 server at Shanghai (SHDC01), it is a domain controller of the same domain at my HQ (no child domain). SHDC01 has only 1 network card, it is behind a TP-LINK TL-R402M router. I also configured a persistent demand dial interface on SHDC01 to connect to SGRAS01, and a corresponding demail dial interface on SGRAS01 (currently disabled). The Windows Firewall hasn't been enabled yet on SHDC01. Right now I wish to accomplish the Shanghai-Singapore 1-way connection first, before going into the 2-way VPN connection (I am prepared to change the router). I set a fixed IP (194.1.1.49) on the Dial-in tab of the user account (ddsusser) used for the demand dial interface on SHDC01. The clients on the Shanghai networks are configured (using DHCP) to route packets destined for 194.1.1.0 through SHDC01. A route print on any clients can verify the routing entry 194.1.1.0 255.255.255.0 192.168.1.2, where 192.168.1.2 is the IP address of SHDC01. The demand dial connection from SHDC01 to SGRAS01 is successful, and SHDC01 has no problem connecting to any clients on the 194.1.1.0 networks. However, all the clients on the Shanghai network cannot access any clients on Singapore network, tracert shows the packets are lost after going through SHDC01. The clients on the Shanghai network can access Singapore network if they use direct vpn connection to SGRAS01, which they have been doing all this while.

You can see the screen captures here:

<http://singchung.spaces.live.com/blog/cns!CEF9A5068D415432!404.entry>

Any help or suggestions is very much appreciated.

Sing Chung

Re: Site-to-Site VPN client routing question – clients at branch office not able to access network a2HQ