

Re: Vista, SBS 2003 and RAS not working

Source:

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.sbs/2008-06/msg01477.html>

- *From:* Joe <joe@xxxxxxxxxxxxxxxx>
 - *Date:* Tue, 17 Jun 2008 20:30:33 +0100
-

Alistair Thacker wrote:

Hi,

We have a windows SBS 2003 server straight out of the box, default install.

We have Vista SP1 client machines.

Everything is working tickety-boo except:

When we try to connect remotely using the Windows RAS connection manager (this is installed and configured with the default settings automatically when we joined the PCs to the domain), it connects to the server (extranet.evolution.ie) but then it takes about 30 seconds trying to authenticate, finally failing and giving the following message:

The VPN connection between your computer and the VPN server could not be completed. The most common cause for this failure is that at least one Internet device (for example, a firewall or a router) between your computer and the VPN server is not configured to allow Generic Routing Encapsulation (GRE) protocol packets. If the problem persists, contact your network administrator or Internet Service Provider. (Error 806) For customized troubleshooting information for this connection, click Help.

Things I have tried:

- 1) Running the SBS RAS set-up again. Always choosing the default options.
- 2) Turning off the Client's Firewall
- 3) Turning off the Server's Firewall
- 4) Searching Google for hours for a solution
- 5) Shouting at it.

None of these things has worked. Is there anything else you can think of that I should try?

Re: Vista, SBS 2003 and RAS not working

There are two common problems. You don't mention whether you are using a router or whether the SBS is hanging straight onto a DSL or cable modem (not recommended, by the way).

If there's a router involved, it needs to forward both TCP port 1723 and IP protocol 47 (the GRE that the error message mentions) to the server. You're getting a reply from the server, so TCP/1723 must be forwarded OK. Most routers don't mention IP protocols explicitly, at least on the web configuration pages, so there is usually no way to forward GRE by itself. Such routers usually have something called 'PPTP passthrough' or 'PPTP service' or something similar, which will forward both.

You mention that the clients are Vista machines, which means that their built-in firewall works on outgoing messages as well as incoming ones, and the firewall needs to be told that outgoing PPTP VPN connections should be allowed. You mention that you turned off the client firewall, but since the VPN still didn't work, you don't know for sure that the firewall wasn't an additional problem. If you get to the point where an XP machine will connect but a Vista one won't from the same location, this may well be the issue. Computers don't need to be joined to the domain to connect by VPN, by the way, so you can use other remote computers for testing, it's just that only domain machines get access to all network resources easily.

The other common problem is that VPN is a form of routing, and all the networks involved must have different network addresses. There are a few network addresses which are commonly used by default by routers and other equipment, and if the remote network address is the same as the SBS LAN one, then the initial TCP/1723 connection will be made but will not function correctly. The first data sent over the GRE tunnel is that for authentication, so if either GRE forwarding or TCP/IP routing isn't right, the client will claim to be connected, but authentication won't happen.

With the 192.168. group of private network addresses, the netmask is normally 255.255.255.0, which means that for IP address 192.168.x.y, the network address is 192.168.x.0, and the 'y' is the host address on that network. So if your SBS LAN address is 192.168.1.0, a common default, the remote router's network address must be something else, such as 192.168.20.0.

It's worth changing the SBS LAN address if it is the .1. variant (there's a wizard for doing that), as this is a very common default, and every remote location must be different from it. If this is the problem, and you change the remote router now to fix it, then the same thing may happen from another remote location in the future, when nobody will remember what happened this time. Pick something obscure, like 192.168.103.0.

I'll add to the other replies you've had, that VPN is not usually the right solution to a problem. Also, machines that will always connect remotely don't usually need to be domain members, and you may see problems that wouldn't happen to non-domain clients. VPN, with domain membership, is usually the best solution for laptops which are used on the LAN and remotely, as the network environment will remain the same (just a lot slower over VPN), and it's also necessary for a few specialised applications. In general, RDP over RWW has many advantages, the main disadvantage being the extra computers necessary. But the cost of a non-cutting-edge Vista Business machine without a monitor is fairly reasonable these days, even from reputable manufacturers like Dell and HP.