# The Network

## Site-to-Site VPN using Windows 2003

Filed under: Networking, Security, Tech Stuff, Windows — Written by Chrissy on Friday, April 28th, 2006 @ 12:44 am

[super old post, reposted] A few weeks ago, I asked in an IT forum if it was possible to have a "perma-VPN" connection with Windows XP. After searching for awhile, I found that Microsoft calls perma-VPNs "Demand-Dial Interfaces" and these can only be found

in the Windows Server family, not Windows XP. The best way to get as close to a perma-vpn as possible in XP is to Use Dial Up Networking to login. It initiates the

connection for you and you can go about your day. The blinkie icon and actual having to dial in reminded me that this was not a transparent solution..and I really wanted one. So I decided to look into a better solution. You can use a Windows 2003 server on your network to do WAN dialing using RRAS and Demand Dial Connections. Its

incredible easy to setup.

For kicks, I even installed Win2k3 on my laptop (lots of unused licenses at work) and just do a Demand Dial connection to each of the two outside servers. Outlook works like a charm where ever I go. Here is a quickie view of the topology of my network: (the name of my domain is windomain.com)

Function of Server Physical Location Internal IP (behind firewall) External Hostname

|  |  |  |  |
| --- | --- | --- | --- |
| Main | Downtown LA | 10.0.0.100 | dtown.windomain.net |
| Backup | Santa Monica LA 10.0.1.100 | | sm.windomain.net |
| Laptop | West Hollywood | 10.0.2.100 | weho.windomain.net |

As stated previously, each of the three machines are Windows 2003 servers. I will explain more about the "External Hostnames" in a bit.

The "firewall" is a regular broadband router with VPN Pass-through enabled and port 1723 forwarding to the internal RRAS server.

Because I pay for bandwidth on the Main server, I decided to try to route as little traffic through it as possible. Thus, Laptop maintains two Demand-Dial Interfaces even though I could have actually reached Backup via the WAN link through Main.

Why did I list "External Hostname?" Well, only one server has a truly static hostname and in order for this WAN to work smoothly, hostnames for dial-ins are important. Backup and Laptop are on SoHo DSL lines sotheir IPs change every now and again so I use my internal DNS server to give the external IPs a DNS entry. When their IP changes due to a power outage or firewall reboot, I simply go update the DNS for windomain.net to point to the new IP. Each ofthe servers use my internal DNS server so they don't look for "real" entries of windomain.net, which of course, would not have the sm, weho and dtown entries.

I won't go into extreme detail on how to setup the RRAS but here's a quick idea of what I did to connect Main and Backup

4/1/2009 8:28 AM

## Details

1. On all three servers, I setup RRAS to support Demand-Dial Interfaces

2. On Main, I opened the RRAS interface and right clicked on Interfaces then selected "Create new Demand-Dial Interface"

3. I named the Interface Main2Backup

4. On the next few prompts, I selected VPN and PPTP

5. When prompted to enter a hostname for the router to which I am connecting, I typed in sm.windomain.net

6. I selected Route packets on this interface and create new user account for remote router to dial [back]in

7. Destination -> Add -> Destination (recall the IP address for Backup/sm above) is 10.0.1.0. Subnet is 255.255.255.0. Metric is left at 1.

8. Next I was prompted to create a new user. The username is created from the name of the Interface. In this instance, my username is Main2Backup

9. Now, I am prompted for the dial-out credentials. Immediately after I am finished with this setup, I will go setup a Demand-Dial Interface on Backup. I know that I will follow the same pattern so the username I will create on Backup/sm will be Backup2Main. I enter this information now.

10. Finish. Repeat the above steps with slightly different hostname, interface name and dial-in account name on Backup. Eventually, the same will be done on Laptop.

## Conclusion,

Windows 2003 RRAS provides an awesome and easy solution for setting up WANs without physical router hardware. The process can take as little as a few minutes once appropriate DNS entries have been made.