

Re: Cannot join to domain over VPN

Source:

http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active_directory/2007-06/msg00790

- *From:* "Ace Fekay [MVP]" <PleaseAskMe@xxxxxxxxxxxxxxxx>
 - *Date:* Sun, 17 Jun 2007 22:32:13 -0400
-

In [news:FEF10069-EE57-4876-AAEF-60E38D806AB4@xxxxxxxxxxxxxxxx](mailto:FEF10069-EE57-4876-AAEF-60E38D806AB4@xxxxxxxxxxxxxxxx), maverick <maverick@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx> typed:

Hi All,

I have 2 Sites which are connected by VPN. I tried to install a DC at site2, and this machine which needs to point its DNS to the DC in Site1 is correct and pings and resolves fine. When I try to join this machine to the domain, it doesn't do it and comes up with 'Semaphore timeout'.

I had a word with the network guy who confirmed that all ports are wide open, so shouldn't be a port/firewall problem (clean portquery).. Changing MTU size and stuff also proved futile. What do I do to get this to work? Can somebody shed some light please?

Thanks
Maverick

As far as the 'semaphore' error, that tells me it's a port being blocked.

What type of VPN is connecting the offices? Is it a site to site using Cisco PIX and L2TP? Whatever the brand name, are the routes set for both routers on each end (built-in if the PIX are the devices) that have the other office's subnet in its routing table? Herb suggested pinging, nslookup, etc. Can you post their results, as well as the ipconfig /all as he requested?

A word about MTU size: it MUST be 1500. If this is over an ADSL line, it may cause issues. LDAP, RPC and Kerberos fail with MTUs less than 1500. I can't find the article explaining it, but have found altered MTUs causing problems.

--
Regards,
Ace

Re: Cannot join to domain over VPN

This posting is provided "AS-IS" with no warranties or guarantees and confers no rights.

Ace Fekay, MCSE 2003 & 2000, MCSA 2003 & 2000, MCSE+I, MCT, MVP
Microsoft MVP – Directory Services
Microsoft Certified Trainer

Infinite Diversities in Infinite Combinations

Having difficulty reading or finding responses to your post?
Instead of the website you're using, try using OEx (Outlook Express or any other newsreader), and configure a news account, pointing to news.microsoft.com. Anonymous access. It's free – no username or password required nor do you need a Newsgroup Usenet account with your ISP. It connects directly to the Microsoft Public Newsgroups. OEx allows you to easily find, track threads, cross-post, sort by date, poster's name, watched threads or subject. It's easy:

How to Configure OEx for Internet News
<http://support.microsoft.com/?id=171164>

"Quitting smoking is easy. I've done it a thousand times." – Mark Twain