

RE: Trusting external domain

Source:

http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active_directory/2005-05/msg00362

- *From:* "Ryan" <Ryan@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Thu, 5 May 2005 19:07:34 -0700
-

Joe,

I had a similar issue. There is likely be a better, and more correct way, but this worked for me. If anyone has a better way, I would be interested in hearing it too :)

Assumptions:

You are using 2000 or 2003 domains.

Firewall is ANY <-> ANY (all ports open, both ways), or correct ports open from DMZ to internal (see end of message).

Go into the primary zone (active directory-integrated) in each domain and allow zone transfers to the IP's on the other domain's DNS servers.

Create secondary DNS zones in each domain for the other domain (eg: domain 123.abc.com has a zone record for 456.abc.com, and vice verse). Point them to the DNS server in the other domain.

Once you have verified that your secondary zones have pulled all of the DNS info, try testing your trust connectivity again.

Here is an article on the ports that need to be open (you may want to close down your firewall access from the DMZ to your internal domain). They do not mention it, but I discovered, that if you get long login times when terminal servicing into servers in the trusting domain, you will also want to open TCP port 1026.

<http://support.microsoft.com/kb/q179442/>

Good luck!

-Ryan

"Joe" wrote:

- > I have a domain that I put in a dmz. This domain is 123.abc.com. The
- > internal domain is 456.abc.com. I did not make this a child domain as it is
- > in the dmz and I am worried about security issues. I am looking to make a
- > one way trust so that the DMZ domain trusts the internal domain.
- >

RE: Trusting external domain

- > I have DNS running in the DMZ controller but I can't get the domains to talk
- > to each other. Neither of them know how to talk. I think that it is a
- > DNS issue but I am not sure. My access lists for the firewall are allowing
- > all traffic so I don't see that as an issue. Any insight would be
- > appreciated

- **Follow-Ups:**

- ◆ **Re: Trusting external domain**
◇ From: SPollack

- **References:**

- ◆ **Trusting external domain**
◇ From: Joe

- Prev by Date: **Re: gpo folder missing from sysvol folder**
- Next by Date: **Re: Trusting external domain**
- Previous by thread: **Trusting external domain**
- Next by thread: **Re: Trusting external domain**
- Index(es):
 - ◆ **Date**
 - ◆ **Thread**