

Re: AD Trusts and Firewall

Source:

http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active_directory/2007-11/msg01099

- *From:* "Joseph T Corey" <jcorey@xxxxxxxxxxxxxxxx>
 - *Date:* Tue, 20 Nov 2007 10:19:34 -0500
-

I'll attempt to break this down the best I can (without confusing myself).

First, you can pretty much ignore the client ports in MS's example IF the domain in which a client is a member of does not have a traverse over a firewall (which appears to be the case here). Also, trusted domains/forests only require communication between the domain/forest in which it explicitly trusts (any transitivity with child domains all happens through the root of the trust – unless a shortcut trust is created).

In your case, you will need to setup communication through the firewall for all ports listed under "Server Ports" in MS's documentation for all of the domain controllers on each side of any trust you create (assuming there is a firewall between the trusts).

If I have your scenario incorrect, please let me know as it was difficult to understand what you were trying to accomplish.

--
Joseph T. Corey MCSE, Security+
Systems Administrator
jcorey@xxxxxxxx

"ldr_78" <ldr78@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message
news:D11652B0-99FE-4517-8209-42AEF5A03476@xxxxxxxxxxxxxxxxxxxxxxxx

I've seen this document but I do not know between which machines these protocols should be opened.

In my case shall the 2 domain controllers behind a firewall be able to communicate with the Root domain or only with one DC of the Child ?

Regards and thanks for you help

Laurent

"Joseph T Corey" wrote:

Microsoft has this pretty well documented:

<http://support.microsoft.com/kb/179442>

Re: AD Trusts and Firewall

<http://technet2.microsoft.com/windowsserver/en/library/108124dd-31b1-4c2c-9421-6adbc1ebceca1>

Hope that helps!

--

Joseph T. Corey MCSE, Security+
Systems Administrator
jcorey@xxxxxxx

"ldr_78" <ldr_78@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message
news:D699B7F6-020A-40CB-A04B-8A8A97A28B6F@xxxxxxxxxxxxxxxxxxxx

- > Hi,
- > I've got some questions concerning Trusts and Firewalls. (I hope my
- > explanation will be clear).
- > I have an Active Directory Forest (ad.local) with an empty root domain
- > (ADROOT)
- > 2 domain controllers are installed for this root domain.
- > I have a child domain (d1.ad.local) with 2 domain controllers.
- > This child domain is trusted with other Windows domains for migration
- > purposes.
- >
- > I need now to install some Domain controllers on other sites protected
- > with
- > firewall where I will need to add some trusts with their local domain > for
- > migration purpose.
- >
- > What are the firewall rules to be added between each of these elements
- > (For
- > the Moment nothing is opened) ?
- >
- > Best Regards
- >
- > This can be summarized like
- > ADROOT
- > |--DC1
- > |--DC2
- > |
- > Legacy Domains--/Trust/- D1.ad.local -/FW/--- -/Trust/- > Legacy
- > Domains
- > |--DC3 |--DC5
- > |--DC4 |--DC6
- > ||