

Re: Setting up AD trust Across NAT

Source:

http://www.tech-archive.net/Archive/Win2000/microsoft.public.win2000.active_directory/2005-10/msg00147.html

- *From:* "Brian" <Brian@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Thu, 6 Oct 2005 06:24:03 -0700
-

Thank you that's exactly the type of explanation I was looking for. Not the answer I was looking for but at least I know exactly what is going on.

"Ace Fekay [MVP]" wrote:

> In news:BB919406-7181-440D-8D4E-72E6D98E2CFB@xxxxxxxxxxxxxx,
> Brian <Brian@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx> made this post, which I then
> commented about below:
>> I am trying to set up a Windows AD 2003 trust with a domain that is
>> sitting on the other side of a router that is doing NAT. Both
>> subnets are private to the internet. Our domain is 10.x.x.x and
>> their domain is 192.168.x.x. The Router sitting between us is using
>> NAT to Translate their 192.168.x.x address to 10.x.x.x. So for
>> example, their DC is 192.168.5.5 and when I ping it by name I get a
>> reply of 10.10.5.5. So I guess my question is how do I setup name
>> resolution between the two domains. If I do a zone transfer or a
>> conditional forward to their DNS then when I ask DNS what is the IP
>> address of their DC, it will say 192.168.5.5 which is no good to me.
>> I need it to say 10.10.5.5. I thought about setting up a secondary
>> zone in our DNS and just manually entering all the Host records for
>> all of their servers but I wasn't sure if I needed enteries for
>> things like name servers, LDAP servers and all the other AD related
>> stuff that is in our DNS. If this secondary zone thing will work can
>> you tell me all of the enteries I will need to add besides Host
>> records for server names.
>>
>> I've also heard something about a DNS Proxy is that something that I
>> could possibly use?
>>
>> Any other ideas would be greatly appreciated.
>
> Unfortunately, NAT won't work here. LDAP, RPC, Netlogon and Kerberos will
> not traverse a NAT. Since the domains are not of the same forest, and you
> are attempting an "external" domain to domain trust between two domains in
> different forests, Kerberos won't be a factor in external trusts, which are
> NT style trusts, and uses NTLM. NTLM doesn't use DNS, so setting up
> secondary zones, etc, will be nice for FQDN resolution, but will not help
> with external trust.

Re: Setting up AD trust Across NAT

◆ *Thread*