

## Re: Member Server Login Slow DMZ–Internal Subnet

*Source:* <http://www.derkeiler.com/Newsgroups/microsoft.public.win2000.security/2003-05/0131.html>

---

*From:* Dmitry Korolyov ([d\\_\\_k\\_at\\_mail.ru](mailto:d__k_at_mail.ru))

*Date:* 05/01/03

Date: Fri, 2 May 2003 01:33:46 +0400

--

Dmitry Korolyov

"Steve K." <[skonde@hotmail.com](mailto:skonde@hotmail.com)> wrote in message  
news:ONN6bhCEDHA.2500@TK2MSFTNGP11.phx.gbl...

> But did I mention that the firewall log showed a successful port 53  
> connection to each DC from the DMZ machine? Though I do see what you are  
> saying about AD subnet-sites and services. The only DNS server specified  
in

> the DMZ machine is the closest AD DC DNS. Should I put a reference to  
the

> other two DNS servers in?

This is not required, but you can do it to provide fault tolerance.

> BTW, Member Server which was originally installed in the internal subnet  
> (10.) now has a 192. address.

>

> Do you think I need to put a DC on my DMZ subnet in order to speed up  
login

> time?

No, since your DNS configuration seems to be ok, you better check the subnet  
to site mapping issue. Though usually it is not recommended placing domain  
members in DMZ. In this case if "bad guys" get access to that server, they  
will automatically get some access across your domain. If you do not need to  
host any services which require AD connectivity, you better use stand-alone  
servers in DMZ.

>

> Steve

>

>

>

> "Dmitry Korolyov" <[d\\_\\_k@mail.ru](mailto:d__k@mail.ru)> wrote in message

> news:eH3tNaCEDHA.2704@TK2MSFTNGP11.phx.gbl...

> > Long logins usually indicate DNS or site misconfiguration. In your case,  
> the

> > server most likely was unable to determine the site it belongs to, since  
> the

> > DMZ's subnet was not added to any site in AD. Therefore, it was  
impossible

> > to determine the closest domain controller which should perform

> > authentication, and random DC was selected. Since you have 2 remote DCs

> and

> > 1 local its 66% probability that remote DC is used.

> > Talking about DNS, the server might first try to perform resolution (for  
> AD)

> > in external DNS and was unable to find anything, and only then tried

## microsoft.public.win2000.security: Re: Member Server Login Slow DMZ-Internal Subnet

```
> > internal. This usually gets fixed by changing adapter bindings or DNS
> server
> > orders.
> >
> > --
> > Dmitry Korolyov
> >
> >
> > "Steve K." <skonde@hotmail.,com> wrote in message
> > news:#CwhaVCEdHA.1840@TK2MSFTNGP10.phx.gbl...
> > > I had a requirement to place a member server on my DMZ and have it
login
> > > to
> > > AD across the firewall. I set up a rule containing this machine and
the
> > > three DC's on my internal subnet.
> > >
> > > During login it it took a LONG time (over 5 minutes) after entering a
> > > user
> > > name and password (and hitting enter immediately :) ) seemingly
hanging
> > > on
> > > "Please Wait...Loading your personal settings...".
> > >
> > > Eventually the account was able to login and I was even able to browse
> > > AD.
> > >
> > > My question is two part.
> > >
> > > 1: In my firewall log I noticed that this member server was
attempting
> > > to
> > > establish a connection to all three of my DC's even though two of them
> > > are
> > > remote. Why isn't it just getting what it needs from the local DC
> > > (local
> > > being attached to the third nic in the firewall as opposed to a T1)?
> > >
> > > 2: Why the long login time?
> > >
> > > Here are the ports opened in the rule between the member server and
the
> > > three DC's. Our DMZ is set up behind our firewall not in front. We
are
> > > not
> > > using a NAT firewall, we are using an application proxy and routing.
> > >
> > > - 123 tcp
> > >
> > > - 135 tcp
> > >
> > > - 137 udp
> > >
> > > - 138 udp
> > >
> > > - 139 tcp
> > >
> > > - 53 udp
> > >
> > > - 53 tcp
> > >
> > > - 88 udp
```

microsoft.public.win2000.security: Re: Member Server Login Slow DMZ–Internal Subnet

```
> > >  
> > > - 88 tcp  
> > >  
> > > - 389 tcp  
> > >  
> > > - 389 udp  
> > >  
> > > - 445 tcp  
> > >  
> > > - 3269 tcp  
> > >  
> > > - 8 icmp (ping)  
> > >  
> > >  
> > >  
> > > Thanks in Advance  
> > >  
> > > Steve K.  
> > >  
> > >  
> > >  
> >  
> >  
>  
>
```