

Re: DNS not doing recursive lookups

Source:

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.dns/2005-08/msg00717.html>

- *From:* "Ace Fekay [MVP]" <PleaseSubstituteMyActualFirstName&LastNameHere@xxxxxxxxxxxx>
 - *Date:* Thu, 18 Aug 2005 21:00:22 -0400
-

In news:4280AB78-B667-4C27-9DF2-5C6A298C1DB1@xxxxxxxxxxxx,
Rob Boylan <RobBoylan@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> made this post, which I
then commented about below:

- > I conceded that using a single-level domain is a bad idea. I have even
- > asked the migration group how I can undo it. (The answer was
- > basically start over from scratch) So I will tackle that little
- > project soon. In the meantime, I still have this little DNS problem.
- >
- > To eliminate all issues with the domain, I configured a brand new
- > server with Windows 2003 Enterprise Edition. I installed DNS and WINS
- > on it, but did not make it a domain controller (it's sitting in a
- > workgroup by itself). I gave it an IP address that passes through our
- > router's access-lists unfiltered and set the computer's network
- > interface to point to itself for DNS.
- >
- > This worked. I was able to perform recursive lookups. I tried it
- > first with EnableEDnsProbes set to 0, and then with the parameter set
- > to 1. Both ways worked, so the router apparently supports EDNS.
- >
- > I then applied the following in the access-list on our main router to
- > the IP on the test machine, which is similar to the filters on the
- > regular DNS servers (where xxx.xxx.xxx.xxx is the IP address of the
- > machine):
- >
- > permit udp any host xxx.xxx.xxx.xxx eq domain
- > permit tcp any host xxx.xxx.xxx.xxx eq domain
- > deny ip any host xxx.xxx.xxx.xxx
- >
- > Immediately, recursive lookups failed.
- >
- > Some research on the router and on Cisco's site revealed that I
- > needed the following:
- >
- > permit udp any host xxx.xxx.xxx.xxx eq domain
- > permit udp any eq domain host xxx.xxx.xxx.xxx
- > permit tcp any host xxx.xxx.xxx.xxx eq domain
- > permit tcp any eq domain host xxx.xxx.xxx.xxx
- > deny ip any host xxx.xxx.xxx.xxx

Re: DNS not doing recursive lookups

- >
- > Apparently, the NT DNS servers must source their lookups from port 53.
- > Otherwise they would not be working. But Window 2003 seems to use a
- > random source port. This was causing the responses back from the
- > root-servers to reach the deny statement and be dropped.

That's right. That's called the empherical response port, which is UDP >1024. All Windows machines do that. Makes it somewhat difficult for security. I would suggest to change the list to:

```
permit udp any host xxx.xxx.xxx.xxx eq domain
permit tcp any host xxx.xxx.xxx.xxx eq domain
permit udp any x.x.x.0 0.0.0.255 gt 1023
deny ip any host xxx.xxx.xxx.xxx
```

The "x.x.x.0 0 0.0.0.255" is a blanket subnet wide allowance. You can also choose just the specific IP by stating:
permit udp any x.x.x.x gt 1023

There are also reg entries to control the traffic on the DNS server to use specifically TCP and UDP 53, and not use the empherical ports, although I've never tested it. If you are going to implement this, I would suggest to test it during off-production hours. Look for the "SendPort" info:

813965 – Description of DNS registry entries in Windows 2000 Server, part 3 of 3:

<http://support.microsoft.com/default.aspx?kbid=813965>

Ace

• *References:*

- ◆ ***DNS not doing recursive lookups***
 ◇ *From: Rob Boylan*
- ◆ ***Re: DNS not doing recursive lookups***
 ◇ *From: Ace Fekay [MVP]*
- ◆ ***Re: DNS not doing recursive lookups***
 ◇ *From: Rob Boylan*
- ◆ ***Re: DNS not doing recursive lookups***
 ◇ *From: Ace Fekay [MVP]*
- ◆ ***Re: DNS not doing recursive lookups***
 ◇ *From: Ace Fekay [MVP]*
- ◆ ***Re: DNS not doing recursive lookups***
 ◇ *From: Rob Boylan*

• Prev by Date: ***Re: DNS Scavenging***

• Next by Date: ***Re: Unable to resolve MX using nslookup***

Re: DNS not doing recursive lookups

- Previous by thread: ***Re: DNS not doing recursive lookups***
- Next by thread: ***How to set up DNS for internal AD and outsourcing Web site***
- Index(es):
 - ◆ ***Date***
 - ◆ ***Thread***