

Re: Issue with port blocking on public DNS server

Source:

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.dns/2006-08/msg00211.html>

- *From:* "WimVM" <wimvm1@xxxxxxxxxx>
 - *Date:* Sun, 6 Aug 2006 00:28:34 +0200
-

Hello,

Have a look here:

<http://technet2.microsoft.com/WindowsServer/en/library/19a63021-cc53-4ded-a7a3-abaf82e7fb7c1033.mspx?mfr=t>

Select "Network Ports Used by DNS" and have a look for yourself...

I am talking about the "Destination Ports" in the "Responses to local DNS server" and "Responses to remote DNS server" "Traffic Type"-senario. As you can see "ANY PORT ABOVE 1023".

How do you secure this, that's my question. Or, is there a way to set these ports fixed in some way, ... There must be a workaround...

Thanks.

"Herb Martin" <news@xxxxxxxxxxxxxxxx> wrote in message news:e83BliNuGHA.5056@xxxxxxxxxxxxxxxxxxxxxxxxxxxx

"WimVM" <wimvm1@xxxxxxxxxx> wrote in message news:OMX37FMuGHA.4208@xxxxxxxxxxxxxxxxxxxxxxxxxxxx

Hello,

I have two public DNS servers running Windows 2003 Web Edition SP1. They are used as DNS server for hosting public domain names. On the same servers I have a mailserv running (MailEnable). I also do port filtering on the public network card (advanced options of the NIC).

I have these ports open:
-TCP: 25/53/110
-UDP: 53
-IP: 6/8/17

Everything works fine, except that I can not resolve external domain names (other then the domain names in my own DNS server) on the servers. This is ofcourse a requirement for the mail server...

Re: Issue with port blocking on public DNS server

Is this true when you are working FROM the Web/DNS server too?

If so, then the likely source of the problem includes:

1) Filtering outbound requests on port 53 FROM the DNS to the Internet

OR (perhaps more likely)

2) You have disabled "Recursion" in the ADVANCED TAB of the DNS

When I scan the ports used by DNS I note that it is not only using ports TCP53 and UDP53 but also DYNAMIC assign ports: 2 UDP and 1 TCP. They mostly are something like 1028 (TCP) and 1025/1026/1027(UDP). The problem is ofcourse that I can not block the ports in this way. As soon as the ports are changed (after reboot?), name resolution will fail.

DNS does not use dynamic ports (in the sense RPCs do) but it must send out a request for resolution (from the DNS server) on Port 53 DESTINATION with some high port as the response.

This is the way that pretty much all normal "client requests" work for any protocol, and if you wish to have your DNS server resolve "the Internet" then it must be such a "client" (do recursive requests or forward.)

Many people argue strongly against such an external (authoritative) server ever doing such things.

This is ONE of the reasons your DNS Zones should NOT be maintained by your servers but placed back at the REGISTRAR in almost all cases (except the largest companies.)

How can I solve this? How can I still use port filtering and resolve domain names without any problems.

Put your zones back at the registrar is the most comprehensive plan.

Make sure your DNS server can recurse (in ADVANCED) and have it either do that or forward. Open the required ports for outbound requests and responses if you do this.

--

Herb Martin, MCSE, MVP

Re: Issue with port blocking on public DNS server

Accelerated MCSE
<http://www.LearnQuick.Com>
[phone number on web site]

Thanks!