

Re: External DNS & smtp relay security & recommendations

Source:

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.dns/2007-10/msg00087.html>

- *From:* rileymartin <rileymartin@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Sat, 6 Oct 2007 11:07:03 -0700
-

Thanks. Shouldn't I setup my internal DNS to forward to my external DNS server? What is usually done? Thanks.

"Anthony" wrote:

Hi Riley,

Its your choice if you feel you need to do that, although its hard to see what the benefit could be. So basically you are setting up a DMZ server to host DNS, IIS and SMTP services. Just make sure your internal DNS is kept separate. There is no connection between the two. Your internal DNS should be set up just the same as if you were not hosting a DNS service.

Anthony, <http://www.airdesk.com>

"rileymartin" <rileymartin@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message <news:249EA64B-a>> I'm not familiar with Linux so I went with what I knew which was Windows.

We would like to maintain control over as much as we can so we would like to run our own external DNS server rather than log into our registrar and update records through their web interface. We also want to move away from ISP hosted email and have our own Exchange server. I thought on the DNS server we could also run IIS and use it as an SMTP relay server so our Exchange server was better protected.

We're already using private IPs on our internal network and I thought I would use a 2nd router and configure NAT overload as well as access lists to protect the internal network. The external DNS server would connect directly to a fastethernet port on the Cablevision provided 851 router.

Re: External DNS & smtp relay security & recommendations

I hope that clears up more of what we're looking to do. If you have any more suggestions please let me know. Thanks again for your help.

"Anthony" wrote:

Hi Riley,

Its a bit of an open question, so here are a few general answers:

– Are you sure you need to run an external DNS server?

Maybe you do, but

often this arises through misunderstanding.

– Windows Server is an expensive choice of platform for this. Most people

doing this would do it on Linux

– If you really do need an external DNS server then you'd like to have a

DMZ

and a firewall device, so the external server does not have access to the

internal LAN

– If you need to use the Windows firewall, then its just a matter of

allowing inbound connections only on known specified ports for the

internet

services you are running, and nothing else

– If you are really looking for a DNS server to service clients inside

your

network, then its all much simpler. Just add a forwarder to the ISPs DNS,

or

use the Root Hints, and don't allow any access from outside at all.

If you'd like to explain a little more what you are doing with the DNS

you

may get a more specific answer,

Hope that helps,

Anthony, <http://www.airdesk.com>

"rileymartin" <rileymartin@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>

wrote in message

news:47706E40-7BE9-41B1-8797-491E6F906F8A@xxxxxxxxxxxxxxxxxxxx

Hi,

Re: External DNS & smtp relay security & recommendations

I purchased static IP address and cablemodem service and need to install an external DNS server and an SMTP relay service for an internal email server. I would like to use Windows 2003 server and turn on the firewall/ICS that comes with sp2. I looked up information on Technet for securing 2003 and DNS and didn't find any really good documents. What I did find was general information on Windows firewall/ICS and the general best practices for DNS I have listed below. Does anyone have any recommendations they can provide?
Thanks.

- 1) Protect the DNS infrastructure of your organization by utilizing an internal root and name space.
- 2) Only the external DNS server is configured with Internet root hints.
- 3) All internal DNS servers are configured only with the root hints pointing to the internal DNS servers hosting the root zone for your internal name space.
- 4) All DNS servers run on domain controllers with all DNS zones stored in Active Directory. Active Directory ACLs are utilized to secure administration of DNS. All DNS servers are configured with NTFS as the file system.
- 5) External DNS resolution is only performed by your external DNS server. The internal DNS servers point to the external DNS server.
- 6) Internal DNS servers are configured to

Re: External DNS & smtp relay security & recommendations

only permit zone transfers to specific internal DNS servers.

7) The default setting of cache pollution prevention is enabled.

8) UDP/TCP port 53 is only open between one of your internal DNS

servers

and

only your external DNS server through a firewall in your DMZ.

9) Only secure dynamic DNS updates are allowed for all zones except for

the

top-level and root zones, which do not allow dynamic updates at all.

10) All Internet name resolution is performed using proxy servers and

gateways.

11) Utilize Windows Firewall and create exceptions only for DNS ports

TCP

and UDP port 53.