

## Re: Public Namespace and Private Network

**Source:**

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.dns/2005-02/0641.html>

---

**From:** dm4714 (spam\_at\_spam.net)

**Date:** 02/17/05

Date: Wed, 16 Feb 2005 22:15:47 -0600

Thanks for your response, Herb. See below

On other comment – currently today, all my customers access my servers using IP address. Trying to implement DNS seems like it is going to be more demanding that just handing them a static IP and hoping you never try to consolidate or move servers around.

My customers network is a closed environment – other than them having the ability to access servers on my network and possibly the Internet using their ISP.

My network is a closed environment and we have the ability to access the Internet.

I've learned a lot about DNS in the past week, but I'm almost regretting that I recommended that we use this for our internal name resolution between our customers. Me and my big mouth!

I should have said... D-N-S what?

"Herb Martin" <news@LearnQuick.com> wrote in message  
news:eks02w\$EFHA.2052@TK2MSFTNGP09.phx.gbl...

>

> "dm4714" <spam@spam.net> wrote in message

> news:uyVRoC#EFHA.560@TK2MSFTNGP15.phx.gbl...

>> I registered a domain called mycompany.com.

>>

>> I have a number of internal customers that need to access my internal

>> website. Each customer has a circuit into our business for direct

>> access.

>

> Didn't we just go through this a couple of days ago?

>

>> I have set up a DNS server for mycompany.com and created a primary zone.

> I

>> have placed a few A records to point to various servers that we have.

>>

microsoft.public.windows.server.dns: Re: Public Namespace and Private Network

>> *Since most of our customers have Internet access already, they can use*  
>> *the*  
>> *public namespace to resolve the DNS names to private IP addresses that*  
> *they*  
>> *can access through their internal network to us.*  
>  
> *Ok, so mycompany.com is publicly delegated from*  
> *Com to a DNS server that every customer can reach?*

Yes. Originally, my plan was to have a DNS server on the inside of the private network. The only problem with this was that some customers forwarded their Internet access to their ISP — which would never be able to perform an iterative lookup to our private server after querying root, gTLD server. It would fail trying to connect to mycompany.com DNS server.

>  
> *Ok, as long as their routing is correct this much works.*  
>  
>> *Testing would seem to indicate this works.*  
>  
> *Makes sense.*  
>  
>> *I will also have a secondary server on our internal network for customers*  
>> *without Internet access to point to.*  
>  
> *Ok, that it is a seconary is irrelevant to them (only*  
> *meaningful to you.)*  
>  
> *(You probably should disable recursion on this*  
> *DNS server -- if it doesn't have the answer you*  
> *don't want it going to the Internet since they don't*  
> *"do Internet". And this should be the FULL Disable*  
> *Recursion in the Advanced tab which really means*  
> *don't process recursive queries and therefore don't*  
> *Recure and DON'T EVEN forward. This DNS server*  
> *isn't going to work for your users that NEED*  
> *Internet resolution now.)*

Yes, on my internal DNS server, I have disabled recursion. This way, if they do not have Internet access and key in microsoft.com, my DNS server will not try and resolve the name for them. It will only look for names that are within my server's zone files.

>  
>> *My question is this.... does anyone see anything wrong with the scenario?*  
>  
> *So you will instruct them to use YOUR DNS server*  
> *for their OWN CLIENTS and they will be unable to*  
> *use their own DNS?*

They will not use my internal DNS server unless they do not have have dedicated internet access. If they do have a DNS without Internet access, then my plan is for them to add a forward lookup to my server.

If their clients have to put DNS entires to my server, then they will only have DNS lookup for my zone. Otherwise, if they already have DNS entries for their internal server (without Internet access), they will have to add a forward lookup to my internal server.

- >
- > *Or if they have only one zone they will and their clients*
- > *use their own DNS server, will you have them forward*
- > *to you?*

This is what I would like to do. Do multiple zones on their server matter?

- >
- > *Should work.*
- >
- > *What about clients who have multiple zone-trees, but no*
- > *Internet access?*
- >
- > *They will have to include you into whatever scheme they*
- > *currenty use to hook the trees together, either holding a*
- > *secondary for your zone (you must allow this) or some*
- > *substitute OR by delegating from their internal root*
- > *down to your DNS server that they may use.*

You've lost me here. I suppose some of them could have an AD DNS configuration --- and it may cause me problems. I'm hoping they since my name is publically registered, that they can simply add a forward looking to my server (without recursion enable) or some sort of "conditional forwarding" for my domain.

I really do not want to entertain the thought of my customers becoming secondaries to my zones. This would require more maintenance for all involved, in addition to publishing them a list of everything we have setup on our DNS.

- >
- >
- >> *I mean, my network and my customers networks are their responsibility. I*
- >> *cannot expect them to install DNS servers, secondary zones, or anything*
- >> *of*
- >> *the like on their side. I'm trying to make this a seamless transition*
- >> *for*
- >> *them with respect to accessing our servers.*
- >
- > *You are expecting that they will have IP and have no*
- > *DNS servers of their own?*

I did not mention this, but all our customers have IP and they currently talk to our networking with it.

- >
- > *That is an unlikely assumption on a network with routers,*
- > *but possible.*
- >
- > *And they are going to have to change every one of their*
- > *clients to use your DNS server (which shouldn't be a big*
- > *deal if they have no DNS server.)*

Agreed.

- >
- >> *Yes, they could use HOSTS files, but that defeats the purpose as there*
- >> *are*
- >> *hundreds of clients at each of our customers. Some customers may have*
- > *their*
- >> *own DNS that forwards to their ISP. Others may not have Internet access*
- > *at*
- >> *all which is why I wish to have an internal secondary that they can point*
- >> *use to resolve resources within my zone.*
- >>
- >> *Are there any security issues that I need to be concerned with?*
- >
- > *It's not really a security issue since presumably your*
- > *network is already open to them for something more*
- > *sensitive than your DNS names....*
- >
- >> *I realize someone could possibly see www.mycompany.com points to a server*
- > *on*
- >> *the 192.168.33.x network. But this should not be a problem as this is*
- >> *non-routable through Internet.*
- >
- > *Correct. If I see this (from outside) and cannot route to it*
- > *(I cannot from here) then I will at best waste my time*
- > *trying.*
- >
- >> *Opinions?*
- >
- > *It's pretty goofy (seriously it has a flaky feel, to someone*
- > *who has spent a long time consulting and designing solution)*
- > *but it CAN work.*

These sorts of things for me, in my experience, never seem easy because of the environment that I work in. Seems like some of the basic concepts in books are overly simplified and real-world solutions are never truly given. I mean, I wish I could just have to internet facing DNS servers and be done with it. But unfortunately, all my customers do not have the same network infrastructure and some are less sophisticated than others. Yes, some of our customers only use dial-up for Internet access.

>  
> *If it meets your needs -- your biggest problem will likely*  
> *be those people who say they have no Internet access and*  
> *then next week put one into their system.*  
>  
> *Then they won't be able to figure out why their clients*  
> *pointed at you no longer work -- OR they will point*  
> *them to themselves and break access to you...or...*  
>  
> *Worst of all, they will put BOTH sets of DNS servers*  
> *on the client and get RANDOM results that work one*  
> *day for one client and not for another, and change the*  
> *next day.*

I would agree. This is a risk and this will have to be communicated to all customers once DNS environment is implemented.

>  
>  
> --  
> *Herb Martin*  
>  
>  
> *"dm4714" <spam@spam.net> wrote in message*  
> *news:uyVRoC#EFHA.560@TK2MSFTNGP15.phx.gbl...*  
>> *I registered a domain called mycompany.com.*  
>>  
>> *I have a number of internal customers that need to access my internal*  
>> *website. Each customer has a circuit into our business for direct*  
>> *access.*  
>>  
>> *I have set up a DNS server for mycompany.com and created a primary zone.*  
> *I*  
>> *have placed a few A records to point to various servers that we have.*  
>>  
>> *Since most of our customers have Internet access already, they can use*  
>> *the*  
>> *public namespace to resolve the DNS names to private IP addresses that*  
> *they*  
>> *can access through their internal network to us.*  
>>  
>> *Testing would seem to indicate this works.*  
>>  
>> *I will also have a secondary server on our internal network for customers*  
>> *without Internet access to point to.*  
>>  
>> *My question is this.... does anyone see anything wrong with the scenario?*  
>> *I mean, my network and my customers networks are their responsibility. I*  
>> *cannot expect them to install DNS servers, secondary zones, or anything*  
>> *of*  
>> *the like on their side. I'm trying to make this a seamless transition*

>> *for*  
>> *them with respect to accessing our servers.*  
>>  
>> *Yes, they could use HOSTS files, but that defeats the purpose as there*  
>> *are*  
>> *hundreds of clients at each of our customers. Some customers may have*  
> *their*  
>> *own DNS that forwards to their ISP. Others may not have Internet access*  
> *at*  
>> *all which is why I wish to have an internal secondary that they can point*  
>> *use to resolve resouces within my zone.*  
>>  
>> *Are there any security issues that I need to be concerned with?*  
>>  
>> *I realize someone could possibly see www.mycompany.com points to a server*  
> *on*  
>> *the 192.168.33.x network. But this should not be a problem as this is*  
>> *non-routable through Internet.*  
>>  
>> *Opinions?*  
>>  
>>  
>  
>