

## Re: .local and .com

**Source:**

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.dns/2004-11/0130.html>

---

**From:** Steve Duff [MVP] (*ergodic\_at\_ergodic-systems.com*)

**Date:** 11/07/04

Date: Sat, 6 Nov 2004 18:03:55 -0800

You want to host the mycompany.com DNS outside of your own server. DNS hosting is very inexpensive; most registrars offer it free for domains you've registered with them. You add your public A, CNAME and MX records for mycompany.com there. A number of DNS hosting services are also starting to offer SPF and TXT records also. If that is important to you, you should evaluate several to see which works best.

Your firewall should block outside queries to your DNS server for security reasons. You do not want your private DNS visible outside your LAN at all. You add your LAN IPs for mycompany.local AD domain on this server. Everything on the LAN must query DNS through this server – that is an AD requirement.

The only time you will run into a bit of a problem with this is if your gateway router or firewall will not "loop" its public IP address.

To understand: consider somebody on your LAN tries to go to www.mycompany.com. Your DNS queries then queries your public DNS for this name, and gets back the public IP address for it. So far, so good. But if your gateway router doesn't (and surprisingly many don't) know how to loop its own public IP address back to your LAN, the user can't reach it.

The solution in most cases is to simply "shadow" your own copy of "mycompany.com" on your private DNS listing the private LAN IPs for the various internal services.

Unless the number of DNS names is very large this is quite easy to configure manually. Now when someone on the LAN queries www.mycompany.com they will get the local LAN IP for that service direct from your own server. The rest of the public Internet gets the public IP from the public DNS server.

I will mention that there are always security considerations to running services especially web and ftp on a private LAN server. You should have a good, stateful, hardware firewall in place and configure it carefully to restrict outside access to just that which is needed.

Keep on top of updates and signatures, and always keep your eyes open and your nose to the server.

Nothing kills a morning quite like finding out a bunch of hey-duders have parked 100GB of illegal MP3s on your server.

Steve Duff, MCSE, MVP  
Ergodic Systems, Inc.

"Douglas Merrill" <DouglasMerrill@discussions.microsoft.com> wrote in message news:79269967-D398-46D7-99E3-0733E8C267CF@microsoft.com...

- > *My question(s) are regarding .local vs. .com*
- >
- > *We will be implementing a Windows Small Business 2003 Server using Exchange and IIS.*
- >
- > *We have already registered "mycompany.com" and services such as e-mail and web hosting are currently be hosted by a third-party hosting company. We would like to bring these services in-house. I know we will have to contact the company that manages the "mycompany.com" DNS record and have them make changes to the MX and A Records to point to our public IP address.*
- >
- > *After reading other posts and researching on the Microsoft web site it is recommended to use a private/internal domain name such as mycompany.local vs. mycompany.com for security and name resolution issues since we are not hosting our own public name servers.*
- >
- > *If we configure our server to use "mycompany.local" how will we go about configuring DNS on our server to:*
- >
- > *1. Use our "mycompany.com" domain for hosting e-mail and web services in-house (on our "mycompany.local" domain controller) and allow outside users to send us e-mail and view our web site?*
- >
- > *2. Allow our internal users to access "mycompany.com" and other external domains when they are configured to use the "mycompany.local" DNS server.*
- >
- > *Any advise would be appreciated.*