## [Dynamic DNS with ddclient and CentOS](http://www.southofdallas.com/?p=93)

I had wanted to set up a dynamic dns arrangement for a long time to permit me to ssh into a server behind my home NAT firewall that is connected via DSL. DynDNS was a logical choice because I had used an account there years ago and the service seemed easy, at least to begin to configure. The problem was, it turned out over the full course of the setup DynDNS was no easier to set up than some other services and DynDNS didn’t let me use any of my existing domains. So ultimately I decided to use the dynamic services of Zoneedit which is my DNS provider.  
   
ddclient was originally developed for use with the DynDNS Service but it also supports Zoneedit and every other dynamic dns provider I have ever heard of. But the main reason I chose to use it was that I could get it to work when nothing else would. In any event there is a ddclient rpm in the CentOS 4.4 repositories so even the effort to make it start on boot has already been handled.

The toughest thing about the setup is figuring out what to put in the ddclient.conf file, but I’ve got the scoop on that so here is the step by step. For the purposes of this walk through we will assume you have a domain name called urdomain.net and have configured a zone for it on Zoneedit. We will also assume that you have a CentOS 4.4 box (we’ll call this the target machine) running behind a NAT firewall/router that gets a dynamically assigned DNS address from your ISP.

1) Check your router’s documentation and see what you need to do to forward ports to the machine you want to appear on the internet. Most likely you want to run a web server or ssh server. In our example we’ll assume you want to be able to ssh in to your network to access files you have at home with sftp. You’ll need to find out how to make your router accept connections on port 22 and forward those connections to the private address on your LAN for the target machine.

2) Find out what IP address is currently assigned to your router by going to <http://checkip.dyndns.org> from a browser on any computer attached to your LAN that accesses the internet through your router. You’ll get back a simple text page with one line on it that gives the IP address you’re connecting from, which because your router is doing NAT is the address of your router. You’ll note we are not using the Zoneedit checkip address, that’s because it fails to reply about half the time and we can’t have that.

3) From a source outside your LAN (maybe a server you have shell access to or maybe a dial up account you maintain), try and ssh to the target machine using the IP address you’ve obtained. If you’ve set up port forwarding correctly and got the IP address correct you should be able to get in and you’ll be ready to continue. Don’t bother to proceed until you can get to your server this way because any problems you experience thereafter may not be related to your dynamic dns setup.

4) After confirming you can get to the server with the dynamically assigned IP, create an entry for the server in Zoneedit using a name you choose like foo.urdomain.net. Now try and ssh to the server using foo.urdomain.net. If that works you’re looking good.

5) Install ddclient on the target machine. Dead easy — yum install ddclient. It may bring along some dependencies, that’s ok.

6) Edit /etc/ddclient/ddclient.conf. I’d take everything out of the existing config file except what I was going to actually use. Here are the entries I’d suggest.

daemon=300 # check’s your IP address every 300 seconds  
 syslog=yes # logs update messages to syslog  
 mail-failure=root # mail failed update msgs to root  
 pid=/var/run/ddclient.pid # record PID in file.  
 ssl=yes # use ssl-support. Works with ssl-library

use=web, web=checkip.dyndns.org/, web-skip=’IP Address’ #the instructions ddclient uses to check your IP.

server=www.zoneedit.com, \  
 protocol=zoneedit1, \  
 login=urzoneeditlogin, \  
 password=urzoneeditpassword \  
 foo.urdomain.net

The last block it treated as a single line because of the slashes at the end of each line. This block tells ddclient what server to send IP updates to, what protocol to use, how to log in to Zoneedit and what address to update. Pretty simple. In addition to checking a website to see what your ip address is, ddclient can query many types of NAT routers to get the information. I was unsuccessful in configuring ddclient to query my router, but the configuration provide her works well for all types of routers. Getting the information from the router would be cleaner, but is not essential to getting up and going.

7) Start the ddclient daemon with /sbin/service ddclient start. Insure that ddclient will run at boot by /sbin/chkconfig ddclient on. You should be set. ddclient will check the checkip.dyndns.org website every 5 minutes and the DNS record on Zoneedit for the target machine when it finds changes. You can now access the target machine remotely with its fully qualified domain name.

What has been left unsaid here is any discussion of the wisdom of allowing access behind your firewall. You should understand the risks prior to undertaking any of this and implement appropriate safety measures on the target machine just as you would for any machine directly connected to the internet. Since it is behind your firewall it would be possible for an attacker to access the other machines on your network once the target machine is cracked. Network security is outside the scope of this article. Its your responsibility to provide for the security of your network and permitting outside access through your NAT firewall will make your network inherently unsafe. The author disclaims any liability for any damages you suffer if you follow this advice and get owned.

Have fun and good luck.