

Linux, New Corporate Network, Cisco Routers, T1 Ethernet Handoff, DMZ...

Source: <http://linux.derkeiler.com/Newsgroups/comp.os.linux.networking/2006-03/msg00614.html>

- *From:* "J S" <jrs0628REMOVEME@xxxxxxxxxxxxxxxxxx>
 - *Date:* Mon, 20 Mar 2006 09:06:40 -0500
-

First off, I want to thank everyone for even reading this long, drawn out post. =) I am not new to the networking world (I am extremely close to having my bachelors in networking and security), but when it comes to putting it in action I am a newbie.

I am setting up a network for a company that I am part owner of. I don't think it's that complex on a corporate scale, but I still have a lot of questions and hesitations that I was hoping everyone could help me out on. Just a side note, I am on a tight budget!

btw, all the addresses here are definetly fake =)

Ok, for starters, here is what is happening. We recently rented a building in town and have signed the papers to have an optical fiber line installed. We have 2.0Mbs up and down, but it is upgradeable to 100Mbs on the fly if we ever need it. They are doing an Ethernet handover to my equipment. We are supposedly allowed to have as many IP addresses as we need, but we are starting out with 10 to start with (or that's what I want, I don't think we will even need all 10) We just have to let them know the reason and we get more. So far not a problem.. =)

Here is where things start to get a little more flexible as far as my plans go, so I'm open for advice. I plan on having the Ethernet cable from the internet go into my Cisco 2621 router that has 3 10/100Mbs FE interfaces.

I am undecided if I should:

- a) Use the second port for the DMZ by connecting it to its own switch and use the third port to connect to my internal network.. Or
- b) Don't use the second port, and have the third port connect to one side of a 24 port switch, then have another 2621 router connect to the other end of the same switch creating the "sandwich" DMZ setup with the public devices in the middle.

Obviously b would cause me to have to buy another router, or I could get a cheap Cisco 2611 router that only has 10Mbs Ethernet interfaces and use that as the router that connects to the internet considering that my connection

is only going to be 2.0Mbs up/down initially, then upgrade later if I need it.

My next question is about addressing the networks mentioned above. I have no problem with the concepts of routing, subnets, etc, but when it comes to doing a live setup I get a little confused. Since my ISP is going to be giving me 10 static IPs to use, will I make that network that uses these IP's the DMZ? I've never done anything with real static IP's before; will they be giving me an actual subnet with a broadcast address, etc? Here's what I'm thinking will happen:

Let's say my ISP gives me 194.50.50.20–30 to use as my static IPs and I do use option B that I described above with two routers. Will I be using 194.50.50.50.20 for the interface coming out of the exterior router going out to the DMZ switch, then 194.50.50.50.21 for the interior router's interface on the other side of the same switch, then use the other 8 addresses left over for any servers (see below for my server setup). I'll then use NAT for all my internal hosts to access the internet and DMZ. So I guess this is what I am referring to:

<http://personal.ecu.edu/jrs0628/layout1.JPG>

I guess what it comes down to with this part, is that I am extremely confused as to how the addressing scheme will be done when I'm handed static IPs.

Now, a little about what this network will actually be doing. On the interior side I will have about 10 workstations and 10 VoIP based phones in another 24 port 10/100Mbs switch. The phones will be interacting with our PBX server that uses a straight VoIP connection all the way to our service provider. I am not sure if I should place this PBX server on the same switch that Router 2 connects to above, or if I should add another network port to the router so that router 2 connects to two inside networks; 192.168.1.1 AND 192.168.2.1. That way I can separate my internal sever network from my workstations.

The 10 workstations will all be on a windows domain using Samba as the PDC and for file sharing for the network. This PDC will be placed in the intranet (maybe in the separate server segment I mentioned above, or does it have to reside in the same subnet?). I will then have a MySQL server that handles our administrative database on the internal network. To interact with the database, I will have an Apache web server that will serve just the inside workstations. Also on the inside network will be a server that handles NTP, DHCP, maybe VPN. I am extremely confused on whether or not to put the VPN server in the intranet or the DMZ. Any ideas here?

I also am not sure if I want to put my DNS server on the internal network or in the DMZ as well. I don't really forward any DNS requests to my ISP, my server looks everything up. I have thought about putting a DNS server in both the DMZ and internal network and have the internal DNS forward to the master DNS server in the DMZ. Any ideas here as well?

Now, in the DMZ I will have another Apache server, but this will be a proxy server I think that will forward everything to the internal Apache server on the intranet. All connections to this server from the internet will be using SSL. There will also be a mail relay server (haven't researched this as much) that will forward all mail to my internal mail server. Any connections to the external mail server will be using SSL as well over POP.

I also have two other dedicated servers that I rent in another state that runs Apache and a MySQL server for our primary public website. I want to mirror the MySQL database to my internal MySQL database server so that we have a backup that can be used to do local SELECTS (reads) from our internal servers. So here is what I think I am looking at:

<http://personal.ecu.edu/jrs0628/layout2.JPG>

So I guess the bottom line is am I going at this the right way? Besides all the random, broad questions above, what should I be concerned about? What security risks am I running using the layout above? What can I do to save money? What things am I missing regarding having a dedicated internet connection with static IP addresses?

Just a FYI, all of my servers are completely Linux based.

I'm sorry for raising so many questions, and for this post being so long. I'm trying to make sure I get everything out there. I'm not looking for someone to solve my problems, but just shed some light on my questions and hesitations. If anyone could help me on this project, even if it's just answering one of my many questions, I would be more than grateful for your time. Thank you!