CS 4400 System Administration

Project 5: Configure an External DNS Server

Project Information:

Activity Points	2
Due Date	Monday of Week 10

Description:

Obviously we aren't going to want to use IP addresses to refer to the various machines in our network forever. Instead, we want to use fully qualified domain names (FQDNs), like 'www.yourcompany.com'. Your task is to set up a DNS server to perform this name resolution.

This DNS should respond to queries on the ***public and private side*** of your firewall and will resolve to the two server machines (Linux and Windows) .

You can choose to use either the Linux server or Windows server to be used for a DNS server. Just make sure machines on each side of the firewall can gain access.

For example, if you have a webserver set up on one of the two servers, I should be able to access it by typing 'www.yourcompany.com', no matter which side of the firewall I'm on (LAN, WAN, or DMZ).

The documentation should have:

- The domain name you chose, and the subdomains you picked for the Linux and Windows servers. (something like win.diesburgrocks.com and linux.diesburgrocks.com) NOTE: You do not have to actually "register" and "pay for" this domain. We will just point our machines at your DNS server first when they make queries. (You will have to look up what a "self-signed certificate" means, and why it is ok here.)
- A short description of what service you used for DNS and why you chose it
- A summary of the steps you took to get the DNS service working
- Any configuration files that you had to modify
- The IP address of your DNS server.

Please do the following:

1. Choose a made-up domain name, like diesburgrocks.com. (This assignment will be much easier if the domain name does not already exist. Also, pick something other than diesburgrocks.com, even if it is so true.)
2. Set up an external DNS server for your new domain to respond to requests. The domain name should point to your DNS server. (For example, if I set up a DNS server on Windows to handle DNS requests for diesburgrocks.com, then diesburgrocks.com should resolve to the Windows server.)

3. Create hostname records so that win.<yourdomainanme>.com and linux.<yourdomainname>.com resolve to the Windows server and Linux server, respectively. (For example, linux.diesburgrocks.com should resolve to my Linux server, even if it is not running the DNS server.)
4. Make sure the computers in your LAN can resolve off your DNS server. Hint: You'll need to modify pfsense to check your DNS server ***first*** before it asks other DNS servers in the wild.
5. Make sure the servers in your DMZ can resolve off your DNS server.
6. Make another Windows 11 machine and put it in the WAN. This machine will simulate a machine outside your private networks (out in the Internet) trying to access your domain.
7. For your WAN machine to access your DNS server, you'll have to set up port-forwarding on pfsense. (See the wiki for hints.)
8. Create a demo video of it working (more information on the wiki)
9. Update your network diagram to make sure it shows both the IP address for the new WAN Windows 11 computer and which server is now the DNS server. You should also put FQDNs under the servers.
10. Turn in the documentation and demo video links by the due date.

Resources:

- Bind (external dns server) for Linux – Chapter 16, (starting on page 525)
- Bind example zone file https://bind9.readthedocs.io/en/v9_18_4/chapter3.html
- Windows 2019 (external dns server) - https://msftwebcast.com/2019/10/install-and-setup-dns-service-on-windows-server-2019.html (Yes, this is for 2019. It's not too different.)