CS 4400 System Administration

Project 4: Configure a DNS Server

Note: This project is worth a total of 2 points. You can do just one point, or both.

Internal Caching DNS Server (1 pt)

The machines ***inside*** your network also need to use DNS. The point of having an internal caching DNS server is to speed up and cache general purpose access to any Internet hostname (not just www.yourcompany.com). This way you won't have to hard code the UNI DNS server IP addresses into your configuration every time you create/modify an internal machine. Create a new internal caching DNS server.

For the purpose of this exercise, it will be acceptable to host the internal DNS caching on the firewall, or else, the same machine hosting dhcp. This DNS server should cache requests (save IP addresses to host names), and if it doesn't know the IP address, forward on the request to UNI's DNS servers.

If you have dhcp set up, the dhcp server should hand out this internal DNS address along with IP addresses.

You should submit to me in a Google doc:

- 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 internal caching DNS server.

External DNS Server (1 pt)

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 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. (If you put the dns service on your firewall, make a justification for it.)

It may be ok for 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.

You should submit to me in a Google doc:

- 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.

Resources for both Projects:

- General DNS – Chapter 16, p. 498-512
- PfSense (internal dns server) https://docs.netgate.com/pfsense/en/latest/services/dns/resolver.html
- 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