

Network Administration HW2

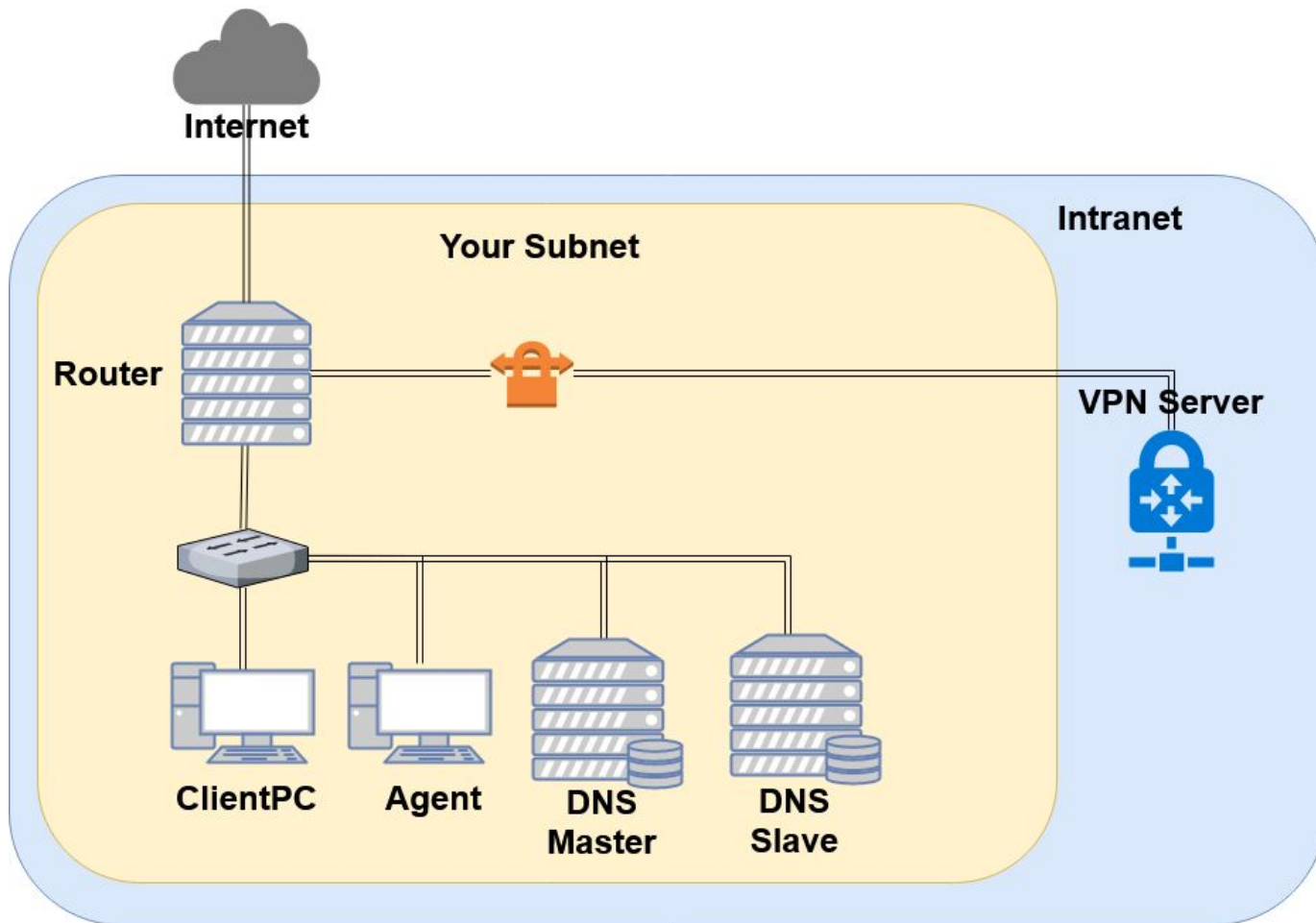
yca

Part 1: DNS

Purpose

- Knowing the basic usage of DNS.
- Knowing the basic configuration of BIND.

Overview - DNS



Overview (Cont.)

- ❑ Use “**{student_ID}.nasa.**” as your domain name.
- ❑ ns1.{student_ID}.nasa.
 - IP: **10.113.ID.1**
 - Master zone
 - ❑ {student_ID}.nasa.
- ❑ ns2.{student_ID}.nasa.
 - IP: **10.113.ID.2**
 - Slave zone
 - ❑ {student_ID}.nasa.

Requirements

- ❑ Setup a DNS servers with BIND.
 - `ns1.{student_ID}.nasa.`
 - Serve your own domain.
 - ❑ `{student_ID}.nasa.`
 - Be able to query from the intranet. (`10.113.x.x/16`)
- ❑ Setup another DNS server with BIND
 - `ns2.{student_ID}.nasa.`
 - Slave zone for “`{student_ID}.nasa.`” synchronized from ns1.
 - Updates should be synchronized
 - ❑ SOA must have same Serial number

Requirements (Cont.)

- ❑ DHCP
 - You have to configure the DHCP server to suggest the clients to use your internal DNS as the primary DNS.
 - Set nameserver to your internal DNS.
 - Set search domain to your domain.
- ❑ Properly query for “**{other_student_ID}.nasa.**”.
- ❑ Security
 - Only allow zone transfer from **Slave** and **Agent**.
 - Only allow recursion from **Agent**.

Requirements (Cont.)

- ❑ Add A record for the machines.
 - **router**
 - **ns1** (DNS Master)
 - **ns2** (DNS Slave)
 - **agent** (Agent)
- ❑ Add CNAME record
 - **nasa** => **nasa.cs.nctu.edu.tw**.
 - **web** => **agent**
- ❑ Confuse your BIND version number.
 - `$ dig version.bind txt chaos @server`
 - For **ns1**, use “**Name Server 1**”.
 - For **ns2**, use “**Name Server 2**”.
 - Only allow queries from your internal network.

Requirements (Cont.)

❑ VIEW

- Add A record for **view.{your_domain}**.
 - ❑ For queries from **10.113.1.x/24**
 - Answer **140.113.235.131**
 - ❑ For queries from **10.113.ID.x/24**
 - Answer **140.113.235.151**
 - ❑ For other queries
 - Answer **10.113.ID.87**
- You have to set up VIEW for both the master and the slave server.
 - ❑ Is there any elegant way to do it?

Requirements (Cont.)

- ❑ Allow **reverse lookup** from the intranet.
 - The answers should be **forward-confirmed**.
 - Return NXDOMAIN if there is no corresponding A record.
- ❑ Add **SSHFP** record of your machines' ssh key fingerprint.
 - For the following machines
 - ❑ **router**
 - ❑ **ns1** (DNS Master)
 - ❑ **ns2** (DNS Slave)
 - ❑ **agent** (agent)
 - The algorithm **ECDSA** and **ED25519** should be implement.
 - The hash type **SHA-256** should be implement.

Requirements (Cont.)

❑ DNSSEC

- Normally, after you registered a domain name and set up a DNS to serve the subdomain. If you want DNSSEC to secure your records, it's necessary to publish the DS record to the nameserver of the top-level domain.

Manage DNSSEC DS Records

Upgrade to Premium DNS and get automated DNSSEC. [Take me there now >](#)

NGINX-REPO.COM

Choose how to set up your DS records.

Key tag	Algorithm	Digest Type	Digest	Max Sig Life	Flags	Protocol	Key Data Alg	Public Key
17385	7	1	c1b9f7f1425bc44976...	N/A	N/A	N/A	N/A	
17385	7	2	98216f4d66d24dbb7...	N/A	N/A	N/A	N/A	

[Add DS Record](#)

[Save](#) [Cancel](#)

Requirements (Cont.)

❑ DNSSEC

- **nasa.** → **{student_ID}.nasa.**
 - ❑ In this scenario we are serving a private TLD which is not delegated from root DNS server, thus the trust chain from root will be broken.
- You need to manage the DS record on <https://nasa.nctu.me/> for the DNSSEC.
 - ❑ It has a **1-day cooldown** on the OJ.
- You must use **NSEC3** to implement it.
- Tool for you to check the trust chain.
 - ❑ **delv(1)**
 - ❑ <https://github.com/dnsviz/dnsviz>

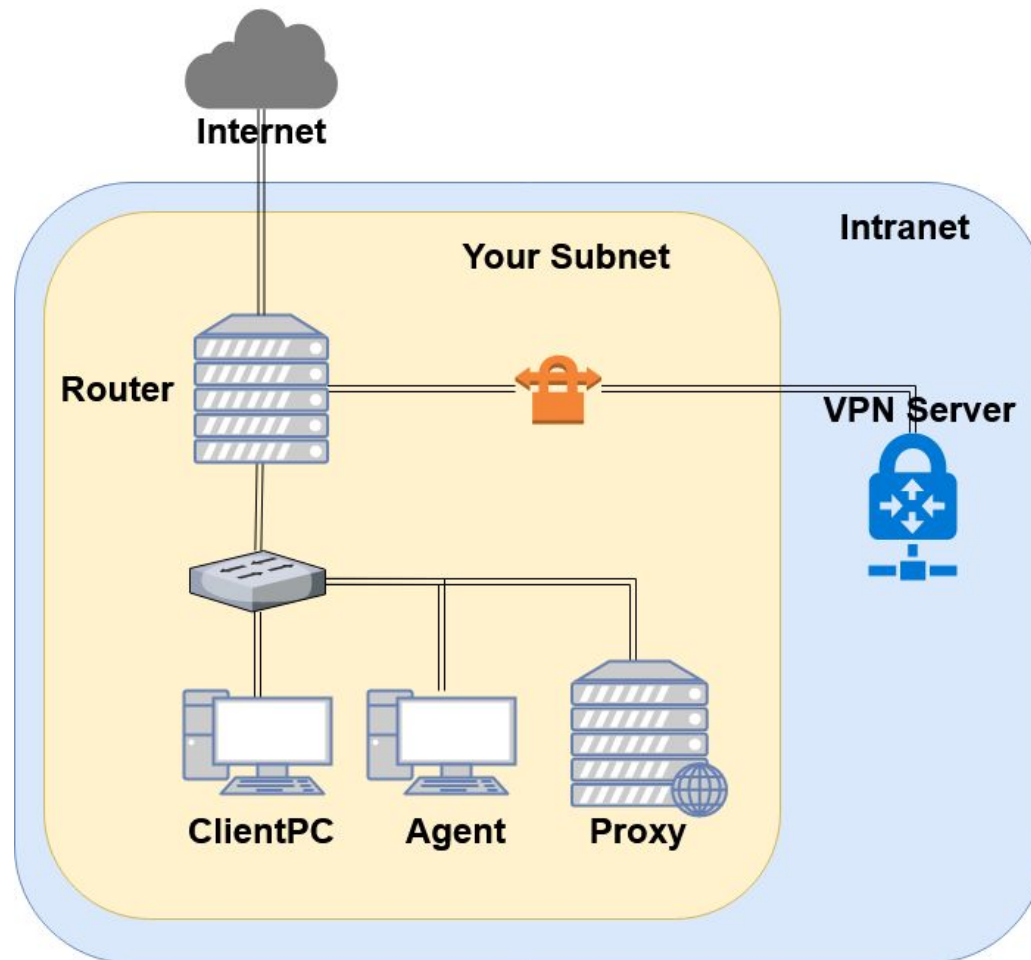
Part 2. Server Load Balancer

Purpose

- Knowing the basic usage of a load balancer.
- Knowing the basic concept of the reverse proxy.

Overview - Server Load Balancer

- ❑ You may have several service on one machine.



Requirements

- ❑ You have to re-deploy your “Agent” by downloading the new file from OJ.
- ❑ Reverse proxy
 - Make a reverse proxy under `http://$yourdomain/reverse/`
 - ❑ Round-robin
 - `10.113.ID.129:8001`
 - `10.113.ID.129:8002`
 - Make a reverse proxy under `http://$yourdomain/ip/`
 - ❑ `10.113.ID.129:8003`
 - ❑ Pass non-standard HTTP headers to the backend.
 - “X-Forwarded-For”
 - “X-Real-IP”: The real client IP.

Requirements (Cont.)

- ❑ Prevent DDoS
 - Set timeout of HTTP request to be 5 seconds.
 - Each user can only have 10 connections opened.
 - Each user can only have 30 connections opened within 10 seconds.
 - If a user send over 20 HTTP requests within 5 seconds, then blacklist the user's IP.
 - ❑ Return 403 for any new request from this user.
 - ❑ Refuse any new connection from this user.
 - ❑ Until 10 seconds after they stop sending requests and establishing connections.

Part 3: Firewall

- ❑ You have to properly adjust your firewall rules to let the new services in this homework run correctly.
- ❑ Recall the rules.
 - By default, all connections from outside (include Intranet) to your subnet should be rejected.
 - By default, all services only trust the connections from your subnet.
 - SSH connections from anywhere to “Agent” are allowed.
 - ICMP connections from anywhere to anywhere are allowed.
- ❑ **You won't get any points for this part, but you will get some points down for the incorrect firewall setting.**

DEMO

- ❑ Your work will be tested by our online judge system
 - Submit a judge request when you are ready.
 - You can submit request multiple times. However, **the score of the last submission instead of the submission with the highest score,** will be taken.
 - **Late submissions are not accepted.**
 - Please check your score at OJ after judge completed.
 - Rate-limit: 60 minutes cool-down
- ❑ Scoring start at : **2020/4/29 00:00**
 - You can test your works once the judge is prepared. However, **make sure to submit at least once after this time,** otherwise no score will be taken.
- ❑ Deadline: **2020/5/7 23:59**

Help!

- ❑ <https://groups.google.com/forum/#!forum/nctunasa>
 - You may send email to ta@nasa.cs.nctu.edu.tw for these reasons:
 - ❑ You get a weird result from OJ.
 - ❑ You have some personal issues that don't want to post to the public.
 - ❑ You are in a special situation that needs to contact us.
 - ❑ Your question is not "May I ask TAs a question?"
 - Try to use the google groups first. We regret that we may not be able to reply every email. Thank you for understanding.
 - How To Ask Questions The Smart Way
 - ❑ <http://www.catb.org/~esr/faqs/smart-questions.html>
 - ❑ <https://github.com/ryanhanwu/How-To-Ask-Questions-The-Smart-Way>
- ❑ Office Hours:
 - 3GH, EC 3F CSCC