HW1-1 Domain Name System

2026 NAP
Chung-Yu Hsu <hsuchy@it.cs.nycu.edu.tw>

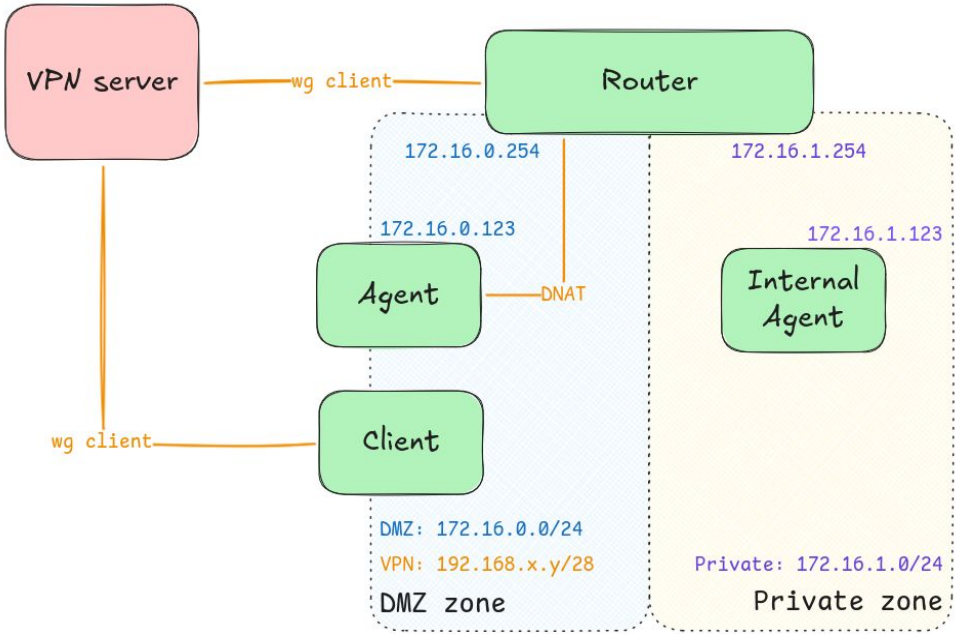
Spec is also available on hackmd (login required)

Requirement

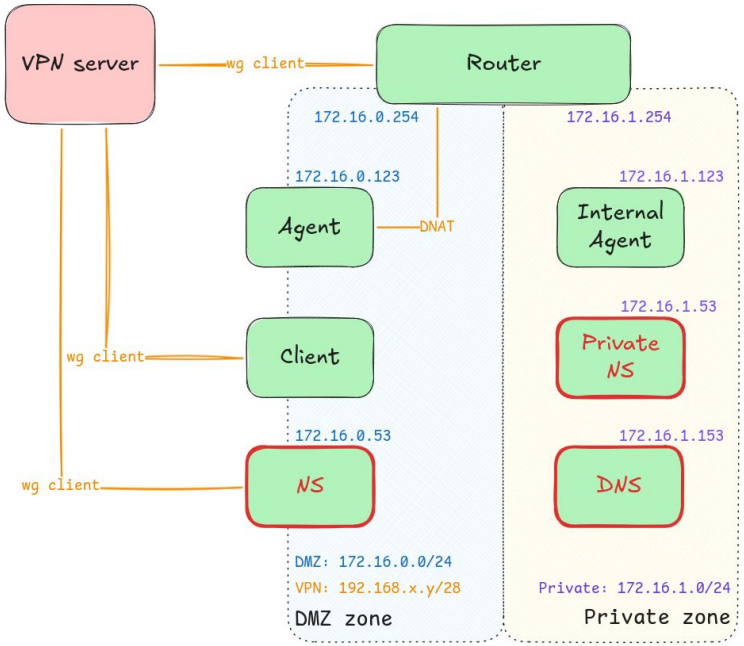
- In this homework, you are requested to build a series of DNS servers.
- Which includes:
  - Two authoritative name server
    - One primary
    - One secondary
  - A internal resolver
- You can use any DNS servers you want
  - However, only BIND9 are tested and guaranteed to pass.

Networking

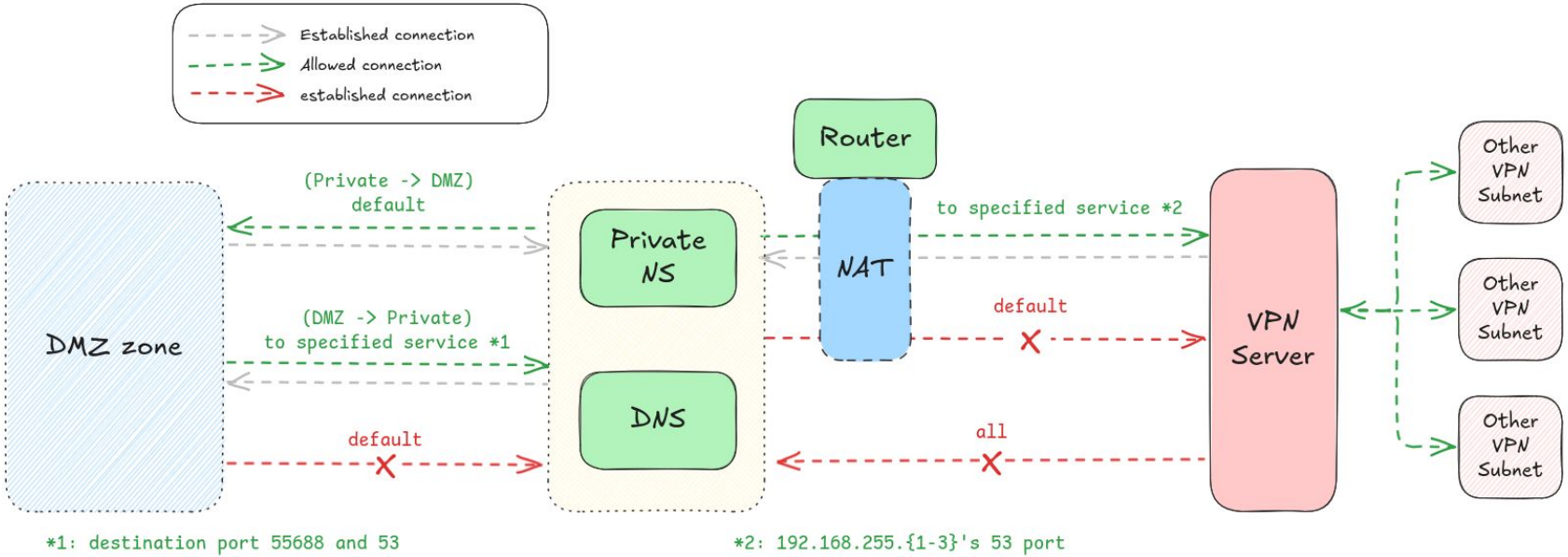
Original Network topology



Updated Network topology



Firewall


Established connection
Allowed connection
established connection
Router
(Private -> DMZ)
default
Private NS
NAT
to specified service *2
Other VPN Subnet
(DMZ -> Private)
to specified service *1
default
VPN Server
Other VPN Subnet
DMZ zone
DNS
default
all
Other VPN Subnet
*1: destination port 55688 and 53
*2: 192.168.255.{1-3}'s 53 port

Primary name server

Basic setting

- IP: `172.16.1.53`
- FQDN: `private-ns.${ID}.nasa.`

Requirement overview

- Serve as primary NS
- Zone resolution of `${ID}.nasa` **and corresponding reverse zone**
- Should **NOT** **resolve any other records** outside your designated zone
- Listen for update request
- Transfer zone to secondary server

Note: name server for zone nasa is at 192.168.255.1

Note2: You should run the wireguard tools to get the ID in the tool output.
Or you can also calculate the ID manually by the method provided in APPENDIX.

Private primary NS structure

- As you can see, the primary NS resides in private zone.
  - It is **not meant to be queried from outside**
    - which is the responsibility for secondary NS you will see later.
- The `private-ns.${ID}.nasa.` should be **untouchable from outside**
- But it should **appear as MNAME** of your SOA record.

Zone and view

- You should have 2 views in your managed zones: public and private.
  - private view: form **DMZ zone** and **Private zone**.
  - public view: from anyelse where.
- You should **at least** add the records on following pages to those zones

Forward zone

- View public
  - Zone ${ID}.nasa
    - router A <your router VPN IP>
    - client A <your client VPN IP>
    - ns A <your secondary NS VPN IP>
    - agent A <your router VPN IP>
    - internal-agent A <your router VPN IP>
- For NS and SOA records, figure it out by yourself.

Forward zone

- View private
  - `Zone ${ID}.nasa`
    - `router A 172.16.0.254`
    - `ns A 172.16.0.53`
    - `agent A 172.16.0.123`
    - `router A 172.16.1.254`
    - `private-ns A 172.16.1.53`
    - `dns A 172.16.1.153`
    - `internal-agent A 172.16.1.123`
- For NS and SOA records, figure it out by yourself.

Reverse zone

- **Figure out the PTR, NS and SOA records by yourself**
- For `192.168` reverse zone, we adopted **Classless in-addr.arpa subnet delegation.**
  - Assume you have VPN subnet `192.168.x.y`
  - Then your reverse zone will be `{ID}-sub28.{x}.168.192.in-addr.arpa`
- For the `172.16.{0|1}` reverse zone, it is trivial.

DNSSEC

- **Sign all the zone you managed.**
  - **EXCEPT** the reverse zone of private ip (i.e. `172.16.{0|1}`)
    - If you want, you can still sign these zones. We won't check, though.
- Using **Algo. 13** and **digest 2**
  - ECDSAP256SHA256 and SHA-256
- Upload your DS records via OJ tool.
  - You should upload DS for `{ID}.nasa` and `{ID}-sub28.{x}.168.192.in-addr.arpa`
  - Use following command to generate the DS record with correct format.
    - `dig @172.16.1.53 <zone> DNSKEY | dnssec-dsfromkey -f - <zone>`

Dynamic zone

- Support dynamic update with a TSIG key
  - **Generate yourself**, and upload to OJ via tool.
- Zone/records update policy
  - In `{ID}.nasa`, **ONLY** allow update **A record of** `dynamic{1-4}.{ID}.nasa`
  - In `{0|1}.16.172.in-addr.arpa`, **ONLY** allow update **PTR records**

Zone transfer

- Allow zone transfer request from secondary NS.
  - IXFR is optional
    - as long as whole transfer process can be completed within **10 seconds**.
- Notify secondary NS on zone update.

Secondary name server

Basic setting

- IP: `172.16.0.53`
- FQDN: `ns.${ID}.nasa.`

Requirement

- The secondary NS should be a **read-only replica** of primary NS
- Most of the requirement for secondary NS are same with primary
  - Except: Secondary NS should **not** be **updatable** nor **transferable**

Internal resolver

Basic setting

- IP: `172.16.1.153`
- FQDN: `dns.${ID}.nasa.`

Requirement overview

- Internal resolver is for internal service to query.
- The resolver should handle both:
  - Our **custom domain** (e.g. `nasa.`)
  - And all the **others domain**

Recursively Resolve and Forwarding

- Resolves `nasa.` and `168.192.in-addr.arpa`
  - Recursively, from root server (`192.168.255.1`)
  - For `{ID}.nasa.` and `16.172.in-addr.arpa`:
    - You should get **answer in private view instead**
- Resolves others from Cloudflare DNS Server (`1.1.1.1`)
- Only allow request from **DMZ and Private zone.**

Note: If you have difficult in resolve `nasa.` recursively, `static-stub` and `trust-anchors` may be handy for you.

Validate DNSSEC

- Validate all answers under `nasa.` and `168.192.in-addr.arpa`
  - Include `{ID}.nasa`
  - You should see **ad bit set in reponse flag** from your resolver.

Grading

Grading

- HW1-1 is weighted for 25% in the whole HW1 grade.

Grading

- Authoritative DNS (45%)
  - Forward (10%)
    - public view (5%), private view (5%)
  - Reverse (10%)
    - public view (5%), private view (5%)
  - Secondary NS (12%)
  - Dynamic update (13%)
    - The updated result appear on both primary server and secondary server (10%)

Grading

- Resolver (20%)
  - Can resolve the query properly (20%)
    - Resolve queries to nasa. and corresponding reverse zone (15%)
    - other zone (5%)
- DNSSEC (35%)
  - Your authoritative NS can be trusted by OJ resolver (10%)
    - Forward + Reverse (10%)
  - Your resolver can validate chain of trust and response authentic data (25%)
    - Forward (12%) (under `nasa.`)
    - Reverse (13%) (under `168.192.in-addr.arpa`)

Appendix

Getting your subnet

- After you run wireguard tools,

  You should be assigned with **one VPN subnet**, and **get three IPs**:

  - Router: `<first ip in your subnet>`
  - Clients: `<second ip in your subnet>`
  - NS: `<third ip in your subnet>`
- After that, you can get your subnet from your IP.
  - Let's say if your router IP is `192.168.8.17`

    then your subnet should be `192.168.8.16`

Getting your ID

- If your subnet is `192.168.x.y`, then your ID will be `x*16 + y/16`

  (in the context of this homework)

Reference

- Understanding views in BIND 9, with examples
- Using DNSTAP with BIND
- BIND9 document
- How To Ask Questions The Smart Way / 提問的智慧
- NA/NAP/SA Google forum

Reminder

- HW 1-2 (Mail), and HW 1-3 (LDAP) will be released in the following weeks.
  - Following the course schedule on the NASA Course Website.
- The deadline for all homework assignments is 6/22 at 23:59 (UTC+8).
- You need to pass ALL test cases for HW1-0 to HW1-3 **simultaneously.**
  - Otherwise you won't receive full credit of HW1
- We recommend using an **IaC approach** to manage your homework environment.
  - e.g. Ansible

Good Luck!

(He will be ded if you don't finish your homework)