Homework 2
Domain Name System

rzhung

國立陽明交通大學資工系資訊中心

Computer Center of Department of Computer Science, NYCU

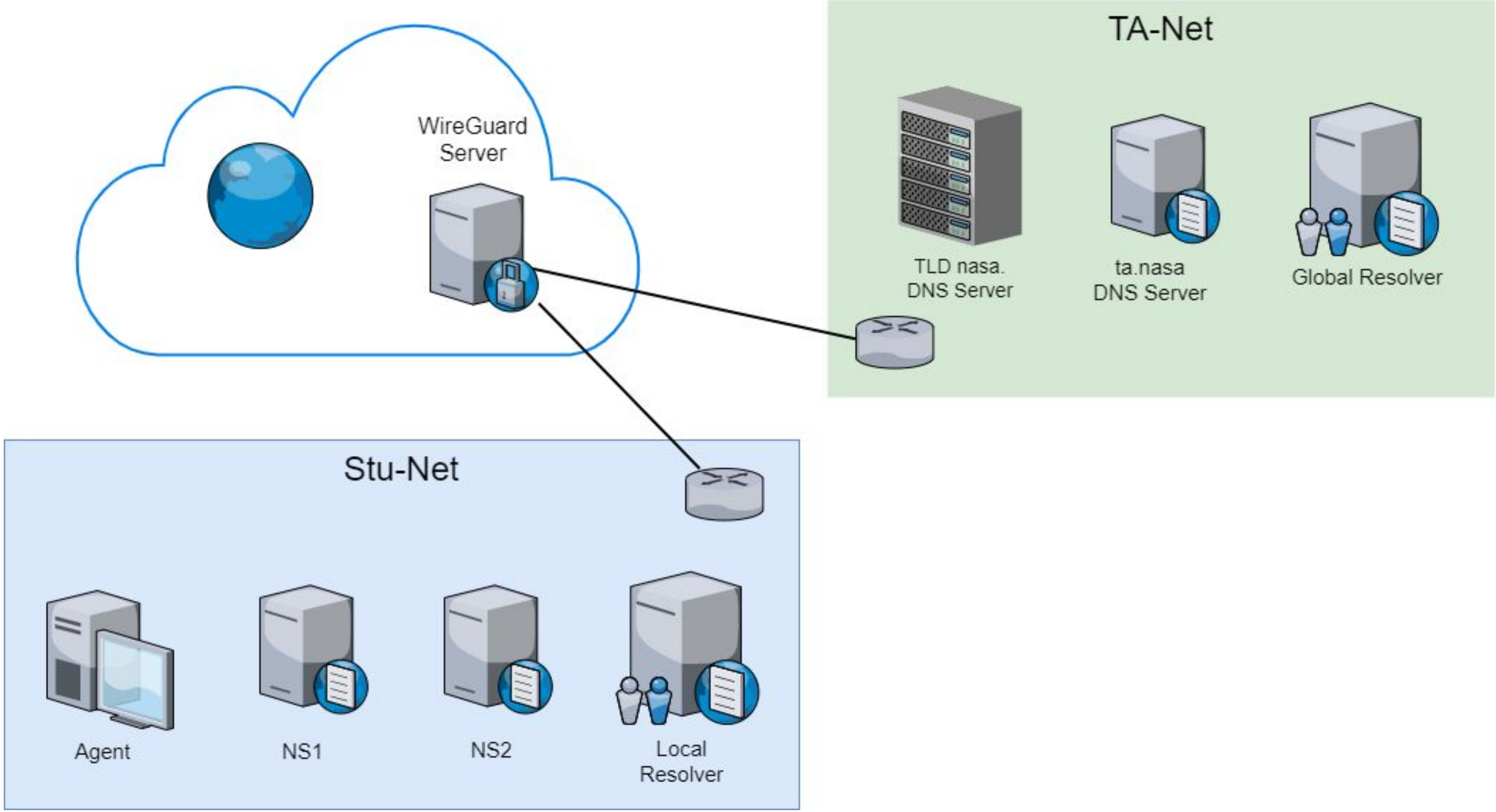
Purpose

- The goal is to build a complete DNS in intranet, which may include DNS Delegation, Authoritative-Only DNS, DNSSEC, Resolver, etc.
- Know what you should know about configuring and managing of these services.

Overview

- Whole intranet has following roles.
    - “TA-Net”
        - As the administrarive system of this intranet
        - Global Resolver: resolver.ta.nasa. 172.16.254.10
            - Only the router is allowed to send queries.
        - .nasa TLD Server: ns1.nasa. 172.16.254.1
            - Also, delegate related reverse maps to the associated server.
    - “Stu-Net”
        - {ID}.nasa / reverse map associated with your Local Net
        - Authoritative-Only DNS
            - NS1/NS2
        - Resolver

Topology (1)


WireGuard Server
TA-Net
TLD nasa. DNS Server
ta.nasa DNS Server
Global Resolver
Stu-Net
Agent
NS1
NS2
Local Resolver

2-1 Authoritative-Only DNS

國立陽明交通大學資工系資訊中心

Computer Center of Department of Computer Science, NYCU

Requirements (1/4) - Basic

- Use “{ID}.nasa” as your domain name.
- Server: 172.16.{ID}.1
  - Zone: {ID}.nasa
    - nameservers: ns1, ns2
    - ns1.{ID}.nasa. A 172.16.{ID}.1
    - ns2.{ID}.nasa. A 172.16.{ID}.2
  - Zone: {ID}.16.172.in-addr.arpa.
    - nameservers: ns1, ns2
    - ns1.{ID}.nasa. A 172.16.{ID}.1
    - ns2.{ID}.nasa. A 172.16.{ID}.2

Requirements (2/4) - Basic

- Server: 172.16.{ID}.2
    - Synchronized from ns1
        - Zone: {ID}.nasa.
        - Zone: {ID}.16.172.in-addr.arpa.
    - Offering domain name service for Local-Net (172.16.{ID}.0/24)
        - Zone: {ID}.nasa.
            - nameservers: ns
            - ns.{ID}.nasa. A 172.16.{ID}.2
        - Serve Resource Record for hosts(172.16.{ID}.0/24) with Local IP

Requirements (3/4) Records

- Serve following Resource Record in both area. (5%)
  - agent.{ID}.nasa.   A   172.16.{ID}.123
  - nasa.{ID}.nasa   CNAME   nasa.cs.nctu.edu.tw
- Serve following Resource Record in specify area.
  - Local (172.16.{ID}.0/24) (5%)
    - {ID}.nasa.   A   172.16.{ID}.2
    - router.{ID}.nasa.   A   172.16.{ID}.254
    - resolver.{ID}.nasa.   A   172.16.{ID}.10
  - Intranet (Other VPN LAN) (5%)
    - {ID}.nasa.   A   172.16.{ID}.1
    - router.{ID}.nasa.   A   10.113.{ID}.1
    - resolver.{ID}.nasa.   A   172.16.254.10

Requirements (4/4) - Misc

- As an Authoritative-Only DNS server, set the right setting for the recursion queries.(5%)
- To prevent unexcepted RR replcation, only allow slave and agent to send axfr.(5%)
- Obfuscate your BIND version number. (5%+Bonus)
  - $ dig version.bind txt chaos @server
  - For ns1, use “Name Server 1”.
  - For ns2, use “Name Server 2”.
  - Only allow queries from your local network. (Bonus: +10%)
- Allow reverse lookup from the intranet.
  - The answers should be forward-confirmed. (5%)
  - Return NXDOMAIN if there is no corresponding A record. (5%)

2-2 DNSSEC

國立陽明交通大學資工系資訊中心

Computer Center of Department of Computer Science, NYCU

Requirements (1/2)

- Make DNSSEC Working (15%)
- DNSSEC Trust Chain: nasa. → {ID}.nasa.
  - After setting correctly, you can verify the trust chain with resolver.ta.nasa
- Manage your DS Record on "https://nasa.nycucs.org"
  - Generate DS record with Algorigm: RSA/SHA-256 and Digest type SHA-256
  - Only update your {Key Tag} and {Key Digest}
  - Use [Debug Tool] > [DNSSEC Record Updater] to manage your DS RR.
- You must use NSEC3 to implement it (5%)
  - Salt with specify value: 140113

Requirements (2/2)

- Add SSHFP records of your machines’ ssh key fingerprints. (10%)
  - For the following machines
    - agent
    - router (optional)
    - ns1 (optional)
    - ns2 (optional)
  - The algorithm RSA and ECDSA and ED25519 should be implemented.
  - The hash type SHA-256 should be implemented.

2-3 Local Resolver

Requirements (1/2)

- This section doesn't limit the software that you use for DNS.
- Make sure the resolver can respond correct answer from the proper server.
  - You shouldn't forward your query to the global resolver in this section.
  - Forward resolution (5%)
    - nasa.
    - Internet domains, e.g. nasa.cs.nctu.edu.tw
  - Reverse resolution (10%)
    - 16.172.in-addr.arpa.
    - Internet reverse maps, e.g. 140.113.17.32
  - Local Forwarding (5%)
    - {ID}.nasa

Requirements (2/2)

- DNSSEC must not affect resolver working (5%)
  - DNSSEC checking is required.
  - If DNSSEC trust anchor does not set properly, you can use +cd to bypass in dig.
  - Trust anchor must set properly with correct environment (Bonus +10%)
    - Using dig will get ad flag in response
- Security
  - Only Allow 172.16.{ID}.0/24 and 10.113.0.0/24 to use this resolver. (5%)

Attention

- Your work will be tested by Online Judge system.
  - You can submit multiple judge requests. However, OJ will **cool down for several minutes** after each judge.
  - We will take the last submitted score instead of the highest score.
  - Late submissions will not be accepted.
- Make sure everything is fine after reboot.
- **Backup your VM before judge every time.**
  - We may do something bad when judging.
- Due date: 2022/04/08 Fri. 23:59:59

Help Me!

- TA office hours: 15:30~17:20 Wed. at EC 324 (PC Lab).
    - We do not allow walk-ins except TA office hours or e-mail appointments.
- Questions about this homework.
    1. Make sure you have studied through lecture slides and the HW spec.
    2. Clarify your problems and google it to find out solutions.
    3. Ask them on https://groups.google.com/g/nctunasa .
        - Be sure to include all information you think others would need.
- We <u>MIGHT</u> give out hints on google group.
    - Be sure to join the group!
- Do not mail us unless it's personal or you're making an appointment.

Good Luck!