Homework 1
Network Environment Setting

prlin, bogay

國立陽明交通大學資工系資訊中心

Purpose

- The goal is to build an intranet that provides several services including DHCP, NAT, VPN, DNS, Mail, LDAP, WWW, etc.
- Know what you should know about the configuration and management of these services.

Overview

- Create an intranet which contains several VMs:
  - "Router"
    - The only VM is directly connected to the outside world (Internet).
    - Provides NAT and DHCP.
    - Can connect to all VMs inside your subnet.
    - Can connect to the VPN server and the whole 10.113.0.0/16 intranet.
  - "Agent"
    - Simulates a simple VM inside your subnet to help TAs and OJ verify results.
  - "Client" (Optional)
    - Simulates a simple VM inside your subnet to help you verify results.

Topology (1)
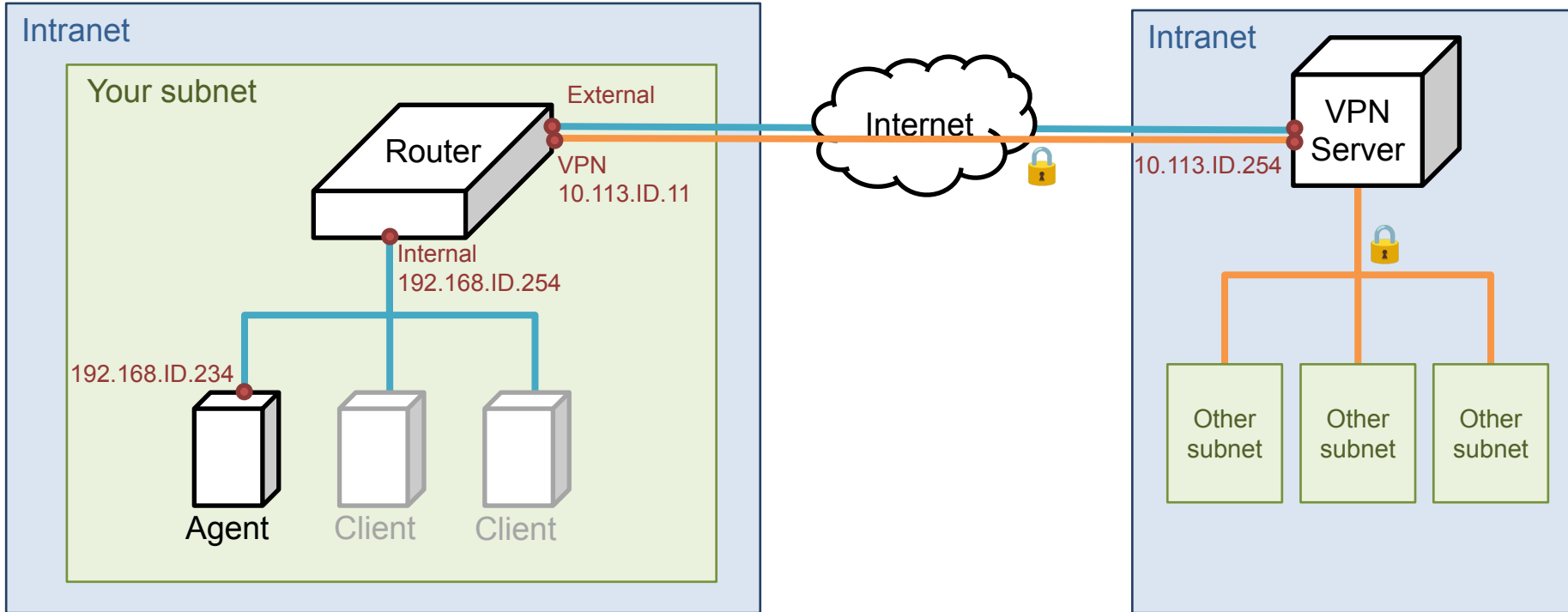
Definitions

- Internet
  - The IP addresses that are not in our intranet.
- Intranet
  - 10.113.0.0/16, a private network for you to do your homework.
- OJ
  - Online Judge system, https://nasaoj.cs.nycu.edu.tw/ .
- ID
  - See the profile page on OJ.
- Your subnet
  - 192.168.{ID}.0/24, a subnet of intranet controlled by yourself.
- VPN server
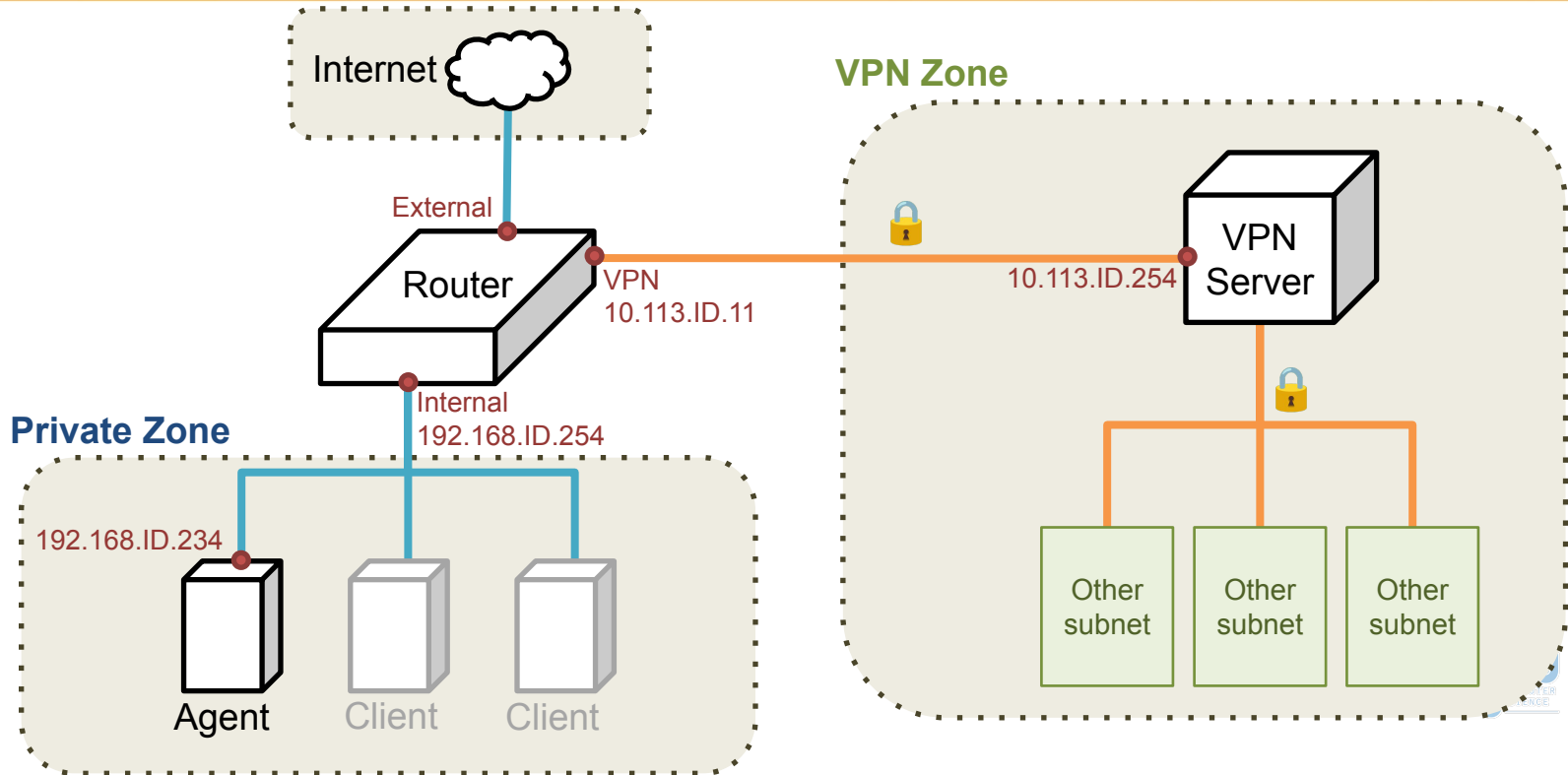 - A WireGuard server which connects subnets together.

Requirements (1/4)

- "Router"
  - Any OS is acceptable.
  - This VM MUST have these network interfaces:
    - External: Internet facing
      - Provides NAT on this interface. Packets from your subnet can go to the Internet through this interface.
      - IP: No limitation.
    - Internal: To your subnet (192.168.{ID}.0/24)
      - Provides DHCP on this interface. IP offered by DHCP should from 192.168.{ID}.111 to 192.168.{ID}.222 .
      - IP: 192.168.{ID}.254
    - VPN: To WireGuard server and intranet (10.113.0.0/16)
      - Connected to the WireGuard server.
      - Everyone in the intranet can access your public services through this interface.
      - IP: 10.113.{ID}.11
  - Enable **sshd** service on port 22.

Requirements (2/4)

- "Agent"
  - **Get this VM OVA file below, don't install this VM by yourself.**
    - Download from https://bit.ly/na2024agent
    - This VM will get IP 192.168.{ID}.234 by DHCP (Hint: MAC binding).
  - OJ will log in to "Agent" to judge your VMs' settings.

Topology (2)

Internet

VPN Zone

External

Router

VPN
10.113.ID.11

VPN
Server

10.113.ID.254

Private Zone

Internal
192.168.ID.254

192.168.ID.234

Agent

Client

Client

Other
subnet

Other
subnet

Other
subnet

Requirements (3/4)

- Routing
  - All inbound and outbound traffic in and out your subnet should go through "Router".
  - Traffic from **Private zone** to Internet should be NAT masqueraded.
  - Traffic from **Private zone** to **VPN zone** should not be NAT masqueraded.
  - Traffic from **VPN zone** to **Private zone** should go to its destination.

Requirements (4/4)

- Firewall
    - Consider you are providing services to the Internet, so several firewall configurations must be taken for security.
    - Configure firewall rules on "Router".
    - Rules:
        - By default, all connections from Internet and **VPN zone** to **Private zone** should be rejected.
        - By default, all connections from **Private zone** to **VPN zone** should be rejected.
        - SSH connections from anywhere to "Agent" are allowed.
        - SSH connections from **VPN zone** to "Router" are not allowed.
        - ICMP connections from anywhere to anywhere are allowed.
        - Allow HTTP (80)/HTTPS (443) from **Private zone** to **VPN zone**.

Grading

Automated grading (Online Judge), 100pts

- Enable Router's sshd service. (5%)
- Trace Route from Agent to Internet. (15%)
- Trace Route from Agent to **VPN zone.** (15%)
- IP offered by DHCP should be 192.168.{ID}.111-222 (20%)
- Agent get IP 192.168.{ID}.234 by DHCP (15%)
- Check Firewall rules for Router (15%)
- Check Firewall rules for Agent (15%)

Hints

- How to check if Internet connection is fine?
  - Ping 8.8.8.8 from different VMs.
  - Ping www.google.com from different VMs.
- How to check WireGuard is connected?
  (Please make sure your private key is correct.)
  - Ping 10.113.$ID.254 (intranet gateway).
- In the final project, you need to deploy these service on cloud.

Appendix: VM Network

- We assume that you use Virtualbox. You can choose other VM hypervisor. However, the network structure should satisfy the requirements.
- About the network interfaces type (take Virtualbox as an example):
  - You can use "NAT" for the External interface of "Router"; "Internal Network" for the Internal interface of "Router".
  - For other VMs, you should only assign an interface with the type of "Internal Network". That is, all the network traffics from these VMs should go through the Internal interface of "Router".

Appendix: VM Network

- VirtualBox
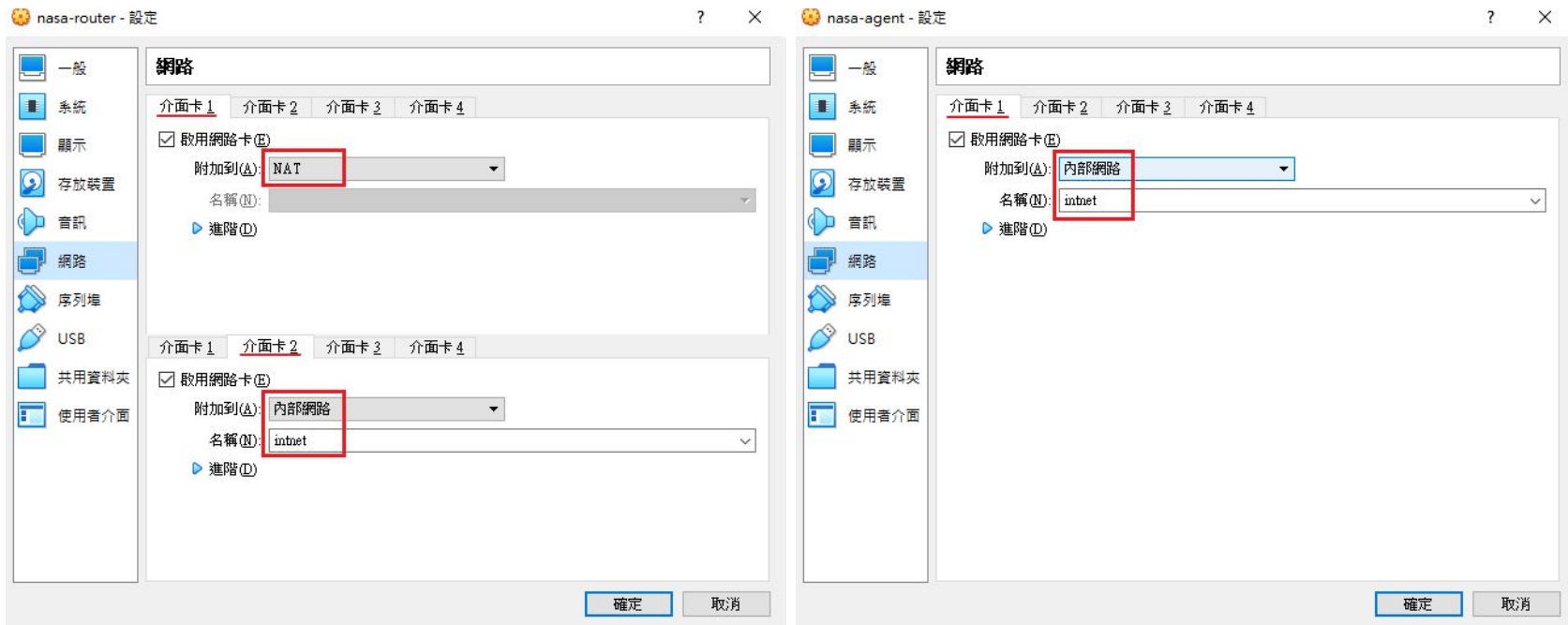
Appendix: Online Judge System

- Login into https://nasaoj.cs.nycu.edu.tw/
  - You can login with NYCU or CSIT account.

Wireguard – Get key

- Install WireGuard
- Configurate VPN connection
  - Download the configuration file
  - Apply it to connect VPN server

SysJudge   Problems ▾   Debug Tools ▾   Admin ▾

WireGuard Key Reloader

WireGuard Key Reloader (Beta)   ✕

This tool can help yout to generate a new WireGuard Keys Config without TA's help.

When you click the "Generate" Button, server will generate a new config for you and restart wireguard server for you automated(CD: 1 hr)

If you have ever clicked "Generate" button, the keys in "Profile" Page would not be update and you need to get your wg0.conf form "Download" button everytime.

Generate   Download

16

Wireguard – Configuration

- 4 IPs are provided
- You can use them to set up additional test VMs in **VPN zone**

```
[Interface]
PrivateKey = 6DjdaOxdYgR8yBPXTXV7Dn7pFc6iWeBiPEpvTrXI1Ek=
Address = 10.113.51.11/32

# [Interface]
# PrivateKey = GEvJ2Idm6qIF4EJTsx8ij7qymk4FOTFbSp8DgOIehm8=
# Address = 10.113.51.12/32

# [Interface]
# PrivateKey = qCZ3Eyw287d+Vp7vJTRUBiEd/hZtTajODzMSw7e4dko=
# Address = 10.113.51.21/32

# [Interface]
# PrivateKey = OLGWjXai3TPYQRMnSm0OZIuPWcinX2cFwcRXbQDRymE=
# Address = 10.113.51.22/32

[Peer]
PublicKey = j8LQIh3EB/4OsPcqzqoljMpxue4Pkib2EUPah7z25B8=
AllowedIPs = 10.113.0.0/16, 192.168.0.0/16
Endpoint = 140.113.168.131:51051
PersistentKeepalive = 15
```
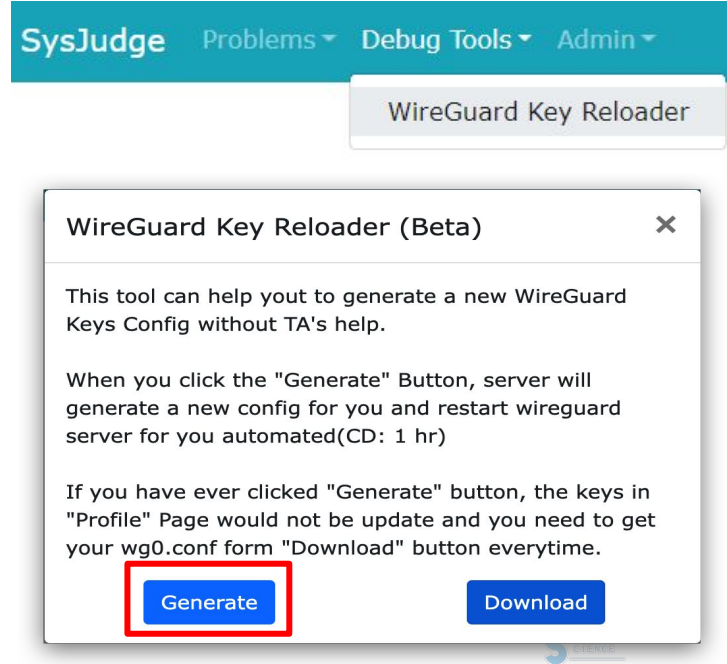
Wireguard – Regenerate key

- If you cannot connect to Wireguard
  - Regenerate key and configuration file
  - Download and apply it

Attention

- Your work will be tested by Online Judge system.
  - You can submit multiple judge requests. However, OJ will **cool down for 10 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 judging every time.**
  - We may do something bad when judging.
- Due date: 2024/03/27 Wed. 23:59:59

Help Me!

- Questions about this homework.
  1. Make sure you have studied through lecture slides and the HW spec.
  2. Clarify your problems and google them 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.

Help Me!

- UNIX 常見指令教學
  - https://it.cs.nycu.edu.tw/unix-basic-commands
- How To Ask Questions The Smart Way
  - https://github.com/ryanhanwu/How-To-Ask-Questions-The-Smart-Way

Good Luck!