HW1-0 - Environment Setup

bjhuang

Notice of Homework 1

- Homework 1-0 does not count toward your final grade.

  However, all subsequent parts depend on it.
- HW 1-1 (DNS), HW 1-2 (Mail), and HW 1-3 (LDAP) will be released following the course schedule on the NASA Course Website.
  - They will not be released earlier than scheduled.
- The deadline for all homework assignments is 6/22 at 23:59 (UTC+8).

Purpose

- The goal is to build two network zones
  - DMZ
    - VPN, Mail, WWW reverse proxy, etc.
  - Private zone
    - DHCP, DNS, LDAP, WWW backend etc.
- Know what you should know about the configuration and management of these services

Overview

- Router
  - The VM has direct Internet access
  - Provides NAT and Firewall
  - Able to connect all VMs in intranet
- Agent
  - Simulate simple VMs inside two zones separately help TA and OJ to verify results
- Client (Optional)
  - Any VMs you want for testing or running service

Definitions (1/2)

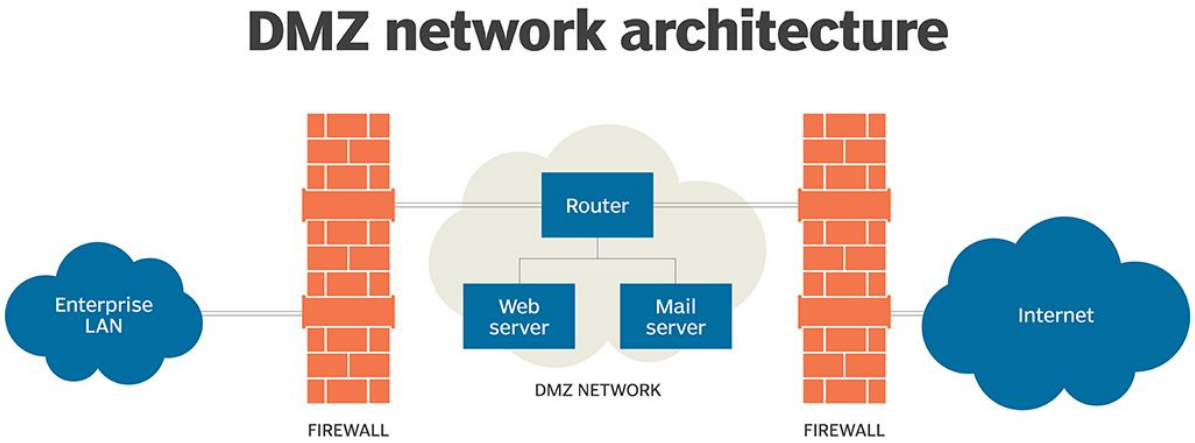
- OJ
  - Online Judge system, https://nasaoj-v3.it.cs.nycu.edu.tw/
- VPN server
  - A WireGuard server which connects your intranet so that OJ worker can access
- Internet
  - The IP addresses that are not in our intranet
- Intranet
  - A network zone including VPN zone, DMZ and your private zone which are managed by yourself

Definitions (2/2)

- VPN zone
  - A private network provided via WireGuard configuration for you and it can be accessed by online judge
- DMZ
  - 172.16.0.0/24, demilitarized zone
- Private zone
  - 172.16.1.0/24, a subnet of intranet managed by yourself
  - Shouldn't have direct access to Internet

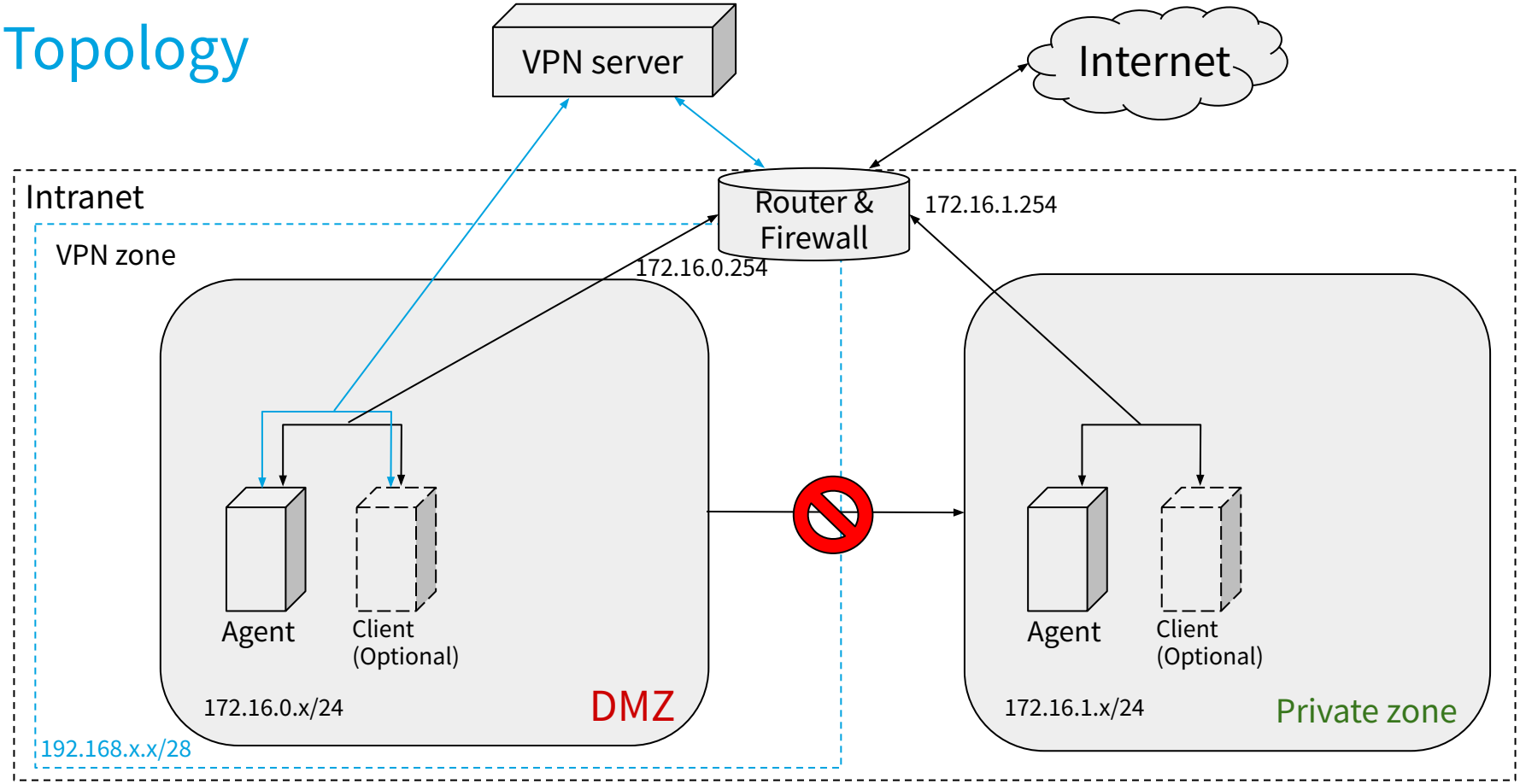
What is DMZ?

- The network zone between private zone and Internet
- Traffic from here to LAN should be monitored or checked by firewall



Source: What is a DMZ in Networking? | Definition from TechTarget

Topology


VPN server
Internet
Intranet
Router &
Firewall
172.16.1.254
VPN zone
172.16.0.254
Agent
Client
(Optional)
172.16.0.x/24
DMZ
192.168.x.x/28
Agent
Client
(Optional)
172.16.1.x/24
Private zone

Requirements

Routing (1/2)

- Router
  - Any OS is available
  - This VM must have these interfaces
    - External (For Internet access)
    - VPN zone (For OJ access)
    - DMZ (172.16.0.254/24)
    - Private zone (172.16.1.254/24)

Routing (2/2)

- All inbound and outbound traffic for your Private zone should go through Router
- Traffic from Private zone to Internet should be NAT masqueraded
- Set DNAT to both agents in DMZ and Private zone
  - Router's 10001 port should be mapped to DMZ agent's 2222 port
  - Router's 10002 port should be mapped to Private zone agent's 2222 port

Setup agent (1/2)

- Agent VM
  - OJ will login to **Agent containers** to judge your system
  - Setup **two VMs**
    - One is inside DMZ with IP 172.16.0.123
    - One is inside Private zone with IP 172.16.1.123
  - Install Docker for your Agent VMs
    - Install | Docker Docs

Setup agent (2/2)

- Agent is a Docker container inside your VM
  - Container image download link:
    https://nextcloud.it.cs.nycu.edu.tw/s/JGbHmEe5Pz5PxDm
  - Start the Docker container with specified image
    - This will enable Agents' 2222 and 55688 ports for connection
  - Please **don’t** revise any settings inside the container!

```
$ wget https://nextcloud.it.cs.nycu.edu.tw/public.php/dav/files/JGbHmEe5Pz5PxDm -O agent.tar
$ docker load < agent.tar
$ docker run -d --restart unless-stopped --name nap-agent --network host nap-agent
```

Firewall

- Configure firewall rules on Router
- Rules
  - By default, all connections from other zones to Private zone should be rejected
  - By default, all connections from Private zone to VPN zone should be rejected
  - DMZ to Private zone should be allowed for 55688 port
  - ICMP connections from anywhere to anywhere are allowed
  - Internet connection of DMZ and Private zone should be allowed
  - SSH connections from VPN zone to Router should be rejected
  - SSH connections from Router to both Agents should be allowed

OJ checkpoints

1. Router's VPN connection
2. Router’s DNAT to Agents in two zones
3. Two Agents' Internet connection
4. Trace route from Agent in Private zone
5. Check firewall rules for Router
6. Check firewall rules for Private zone

Help me!

- Previous SA slides
  - SA - 2025 課程內容 | NASA Course Website
- Appendix in previous NA slides
  - https://site.nasa.cs.nycu.edu.tw/na/2024/HW1.pdf
- How To Ask Questions The Smart Way
  - https://github.com/ryanhanwu/How-To-Ask-Questions-The-Smart-Way

Good Luck!