Homework 03

NAT、DHCP、Firewall、Proxy、LDAP

zjlin / yahsieh / hcchuang

Basic Knowledge

❑ DHCP

- Dynamically assigning IPs to clients

❑ NAT

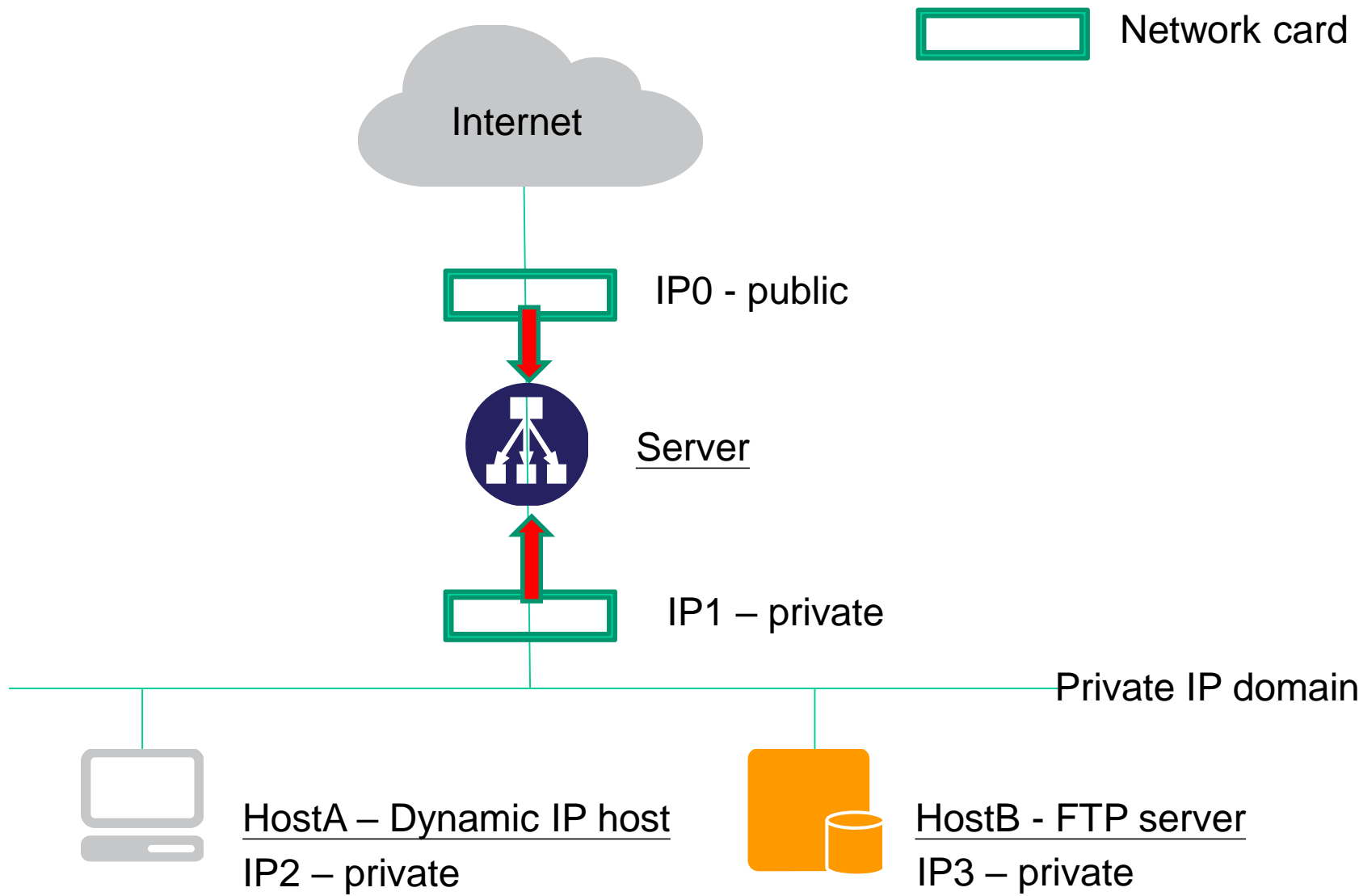- Translating addresses for clients

❑ Firewall

- Traffic filtering

❑ Proxy

- Intermediary of client and server to translate requests

Basic Knowledge – Isolated Execution Environment

❑ Provide a sandbox with limited access to resource

- Protect other programs from compromised one

❑ OS-level virtualization (Used in this HW)

- Resource isolation
  - ➢ File system, device…
- Lightweight
- Easy to manage

❑ Implementation

- FreeBSD: jail
- Linux: lxc

Architecture Overview

Network card

Internet

IP0 - public

Server

IP1 – private

Private IP domain

HostA – Dynamic IP host
IP2 – private
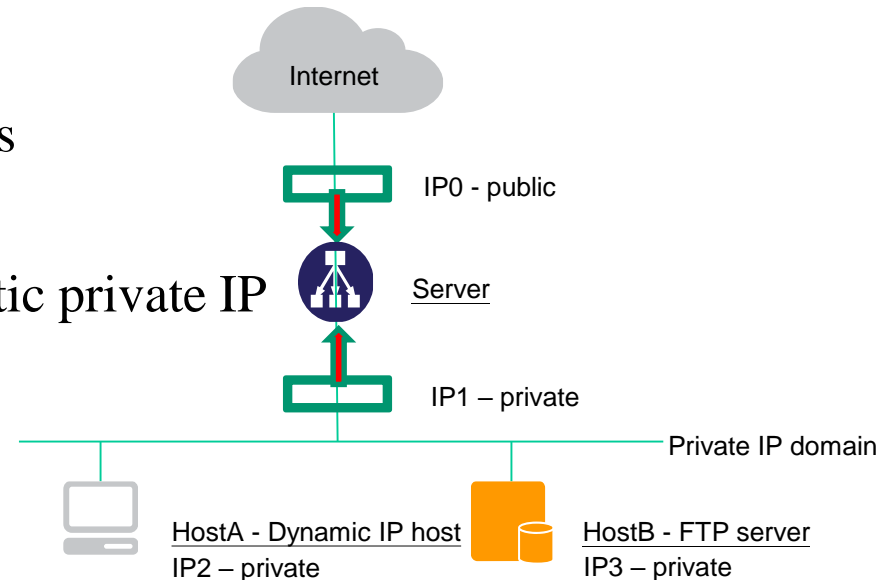
HostB - FTP server
IP3 – private

Architecture

❑ Server

- UNIX-based OS
- Act as a gateway for all services
- DHCP & NAT server
- ✓ A dedicated Public IP and a static private IP

❑ HostA

- ✓ A private IP via DHCP

❑ HostB

- An isolated execution environment on Server
- Runs FTP service
- ✓ A static private IP

Internet

IP0 - public

Server

IP1 – private

Private IP domain

HostA - Dynamic IP host
IP2 – private

HostB - FTP server
IP3 – private

Requirement – NAT & DHCP

❑ NAT

- HostA & HostB can access Internet via Server

❑ DHCP

- Provided by Server
- Static range should be excluded

Requirement – Firewall

❑ Firewall

- Deny all connections come from <BadHost>

- Allow the connection from **140.113.235.151 ~ 140.113.235.154** to access HostB's **FTP** server

- Allow the connection from **140.113.235.151 ~ 140.113.235.154** to access HostB's **SSH** server (Server will redirect the request for port 222 to HostB's SSH server)

- Drop packets from **140.113.235.131 ~ 140.113.235.134** to access HostB's **FTP** and **SSH** server, and response TCP RST/ICMP unreachable

- The connection from other public IP to access HostB's **FTP** and **SSH** server should be denied and not response TCP RST/ICMP unreachable

- All public IP can't send ICMP echo request packets to Server (will not response ICMP ECHO-REPLY packets)

Requirement – Proxy

❑ FTP proxy

- Setup an FTP proxy on Server
- All FTP requests should be proxied to Host

❑ HTTP proxy

- Setup a **transparent** proxy on Server
- All http traffic should pass through this TP

● Hint

- ftp-proxy(8) (ftp)
- www/squid (http)
- www/privoxy (http)

Requirement – FTP with LDAP

❑ Authentication

- Use LDAP-Backend

❑ MemberOf

- Create group "sysgroup"
- Only member in "sysgroup" can login
- Use memberOf overlay

❑ LDAP config should use olc(on-line configuration)

Additional – DHCP Client in Jail/LXC

❑ Use IOCell

- Make sure to upgrade FreeBSD version >= 11.1-RELEASE
- Compile kernel to support VIMAGE, RACCT, RCTL
- ZFS

❑ LXC

- privileged or unprivileged

❑ Reference

- https://github.com/bartekrutkowski/iocell
- http://iocell.readthedocs.io/en/latest/basic-use.html
- https://wiki.archlinux.org/index.php/Linux_Containers

Hand-in

❑ Demo

- 5/23 (Wed.) 16:00~18:00 19:00~21:00

❑ Help

- Email ta@nasa.cs.nctu.edu.tw
- Goto CSCC to ask professional 3F at office hour!