SSH Jump Server

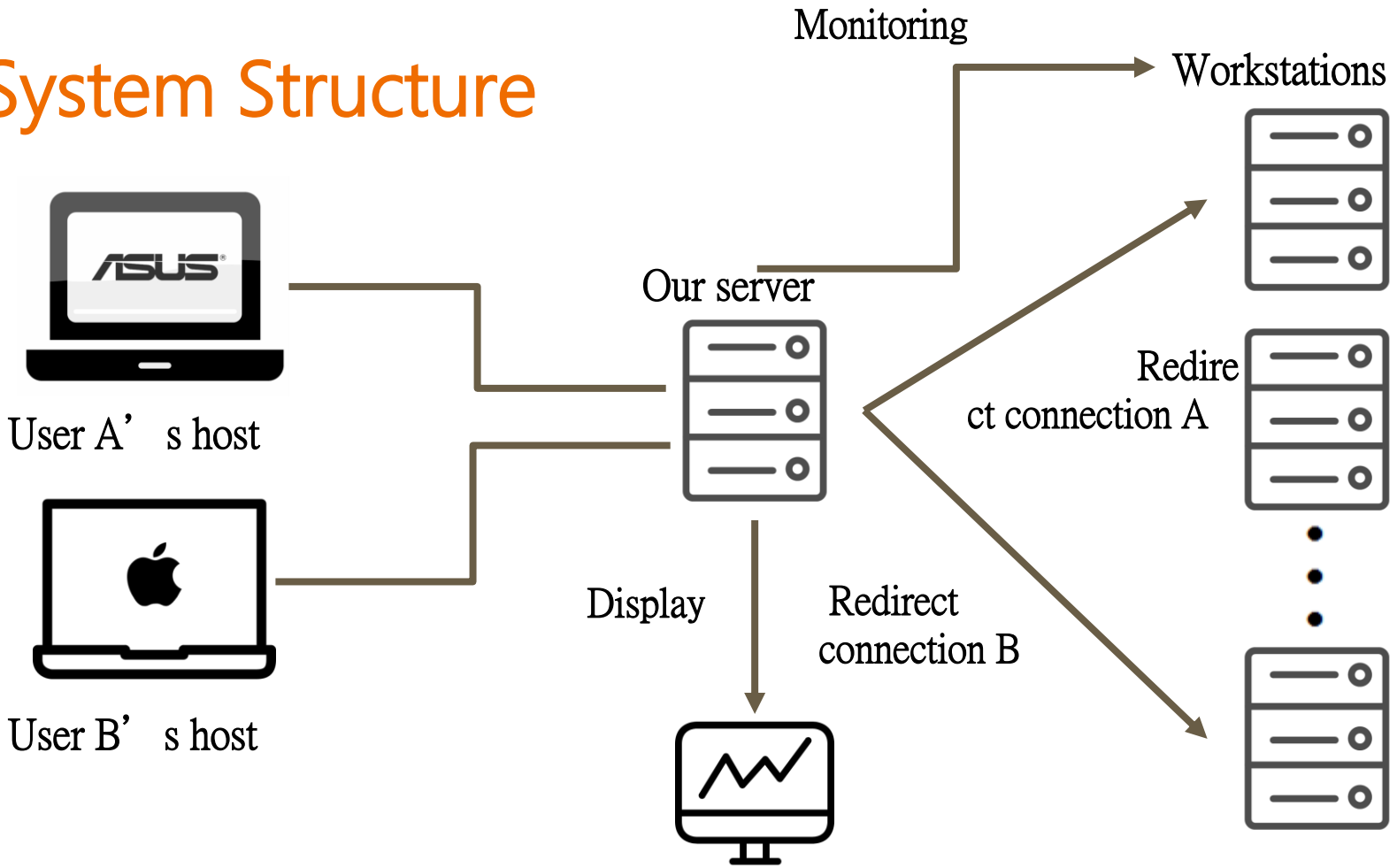
Group 13
B07902066 黃禹喆 B07902062 張彧瑋
B07902068 陳柏豪 B07902080 黃義峰

Environment

Jump server OS: CentOS7

Language: Python(ssh-forward-proxy server), shell script(client), javascript+css+html(monitor)

System Structure



SSH Proxy Server Implementation

1. Jump server opens a socket listening on port 4000.
2. Client connects to port 4000 on jump server. Then the jump server will accept the client’ s connection, and open another thread to interact with the client.
3. The thread decides the optimal workstation serverto redirect the connection to according to the filter rule that is passed down, build another ssh flow between the proxy server and the workstation server.
4. The server continues to support the connection as a proxy until the client stops the connection.

Reference: https://github.com/lincheney/ssh-forward-proxy

Monitor Implementation

1.Backend: Open servers on each workstation. Servers listen on port 7474, and send out the devices’ status back to the jump server when the jump server requests.

2.Frontend: Send request to the workstation devices, and update the current status.

Functions

1. Create a jump server as an gateway of workstations.

2. The jump server should monitor loading of workstations(ex. CPU usage) and redirect connection requests according to workstation load.

3. Display the result of monitoring and redirecting on an administration page.

Final Result

```
cnlab2021@cnlab2021:~/Desktop$ ./connect.sh
Username:b07902062
Password:
Filter(cpu/mem):cpu
uname -a
Linux linux6 5.10.13-arch1-1 #1 SMP PREEMPT Wed, 03
64 GNU/Linux
ls
CA_HW3
CA_HW4
HW2
HW5.scala
IR_hw2
IRhw1
Loopy Tippy
ML_hw6
MyRepo
NASA_LAB10
NASA_LAB11
```

DEVICE	CPU(%)	MEM(MiB)
linux1.csie.ntu.edu.tw	43.4	20158.1
linux2.csie.ntu.edu.tw	51.6	11677.2
linux3.csie.ntu.edu.tw	83.4	55925.7
linux4.csie.ntu.edu.tw	75.7	2372.2
linux5.csie.ntu.edu.tw	71.0	18998.3
linux6.csie.ntu.edu.tw	64.7	17515.1

USER	DEVICE
b07902062	linux6.csie.ntu.edu.tw

Final Result

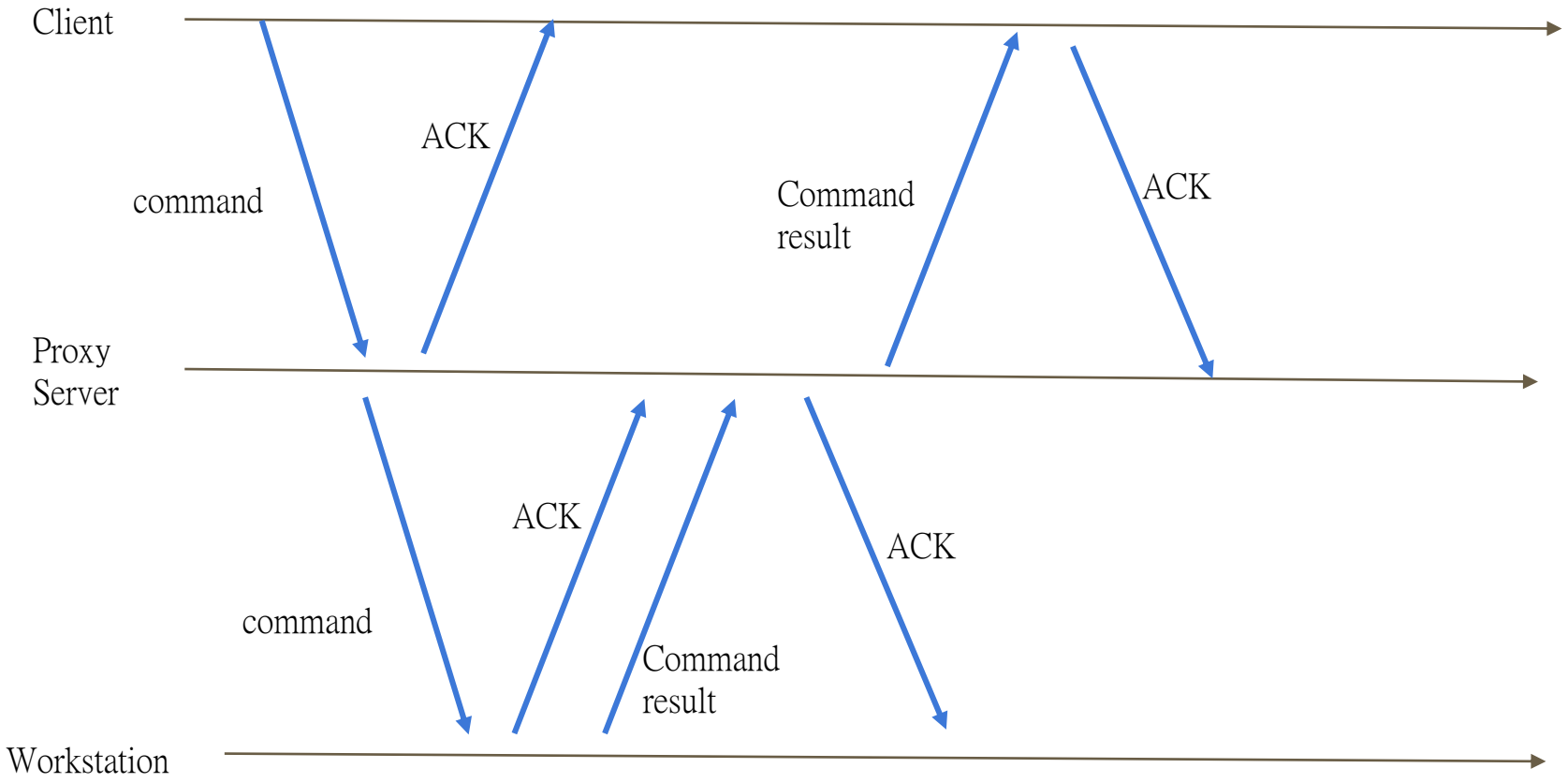
- tshark Result on SSH Proxy Server

```
1 0.000000000   172.17.0.1 ? 172.17.0.2   TCP 134 43218 ? 4000 [PSH, ACK] Seq=1 Ack=1 Win=501 Len=68 TSval=2258018101 TSecr=3869683488
2 0.001228242   172.17.0.2 ? 140.112.30.37 SSH 118 Client: Encrypted packet (len=64)
3 0.001782017 140.112.30.37 ? 172.17.0.2   TCP 54 22 ? 48240 [ACK] Seq=1 Ack=65 Win=65535 Len=0
4 0.004637654 140.112.30.37 ? 172.17.0.2   SSH 310 Server: Encrypted packet (len=256)
5 0.004649187   172.17.0.2 ? 140.112.30.37 TCP 54 48240 ? 22 [ACK] Seq=65 Ack=257 Win=501 Len=0
6 0.005396030   172.17.0.2 ? 172.17.0.1   TCP 326 4000 ? 43218 [PSH, ACK] Seq=1 Ack=69 Win=501 Len=260 TSval=3869788415 TSecr=2258018101
7 0.005434685   172.17.0.1 ? 172.17.0.2   TCP 66 43218 ? 4000 [ACK] Seq=69 Ack=261 Win=501 Len=0 TSval=2258018107 TSecr=3869788415
```

172.17.0.1: Client

172.17.0.2: SSH Proxy Server

140.112.30.37: Workstation


Client
command
ACK
Command
result
ACK
Proxy
Server
command
ACK
Command
result
ACK
Workstation

Demonstration

Q&A

Thank you for listening!