Computer Network Laboratory

Firewall and NAT Report Team 10

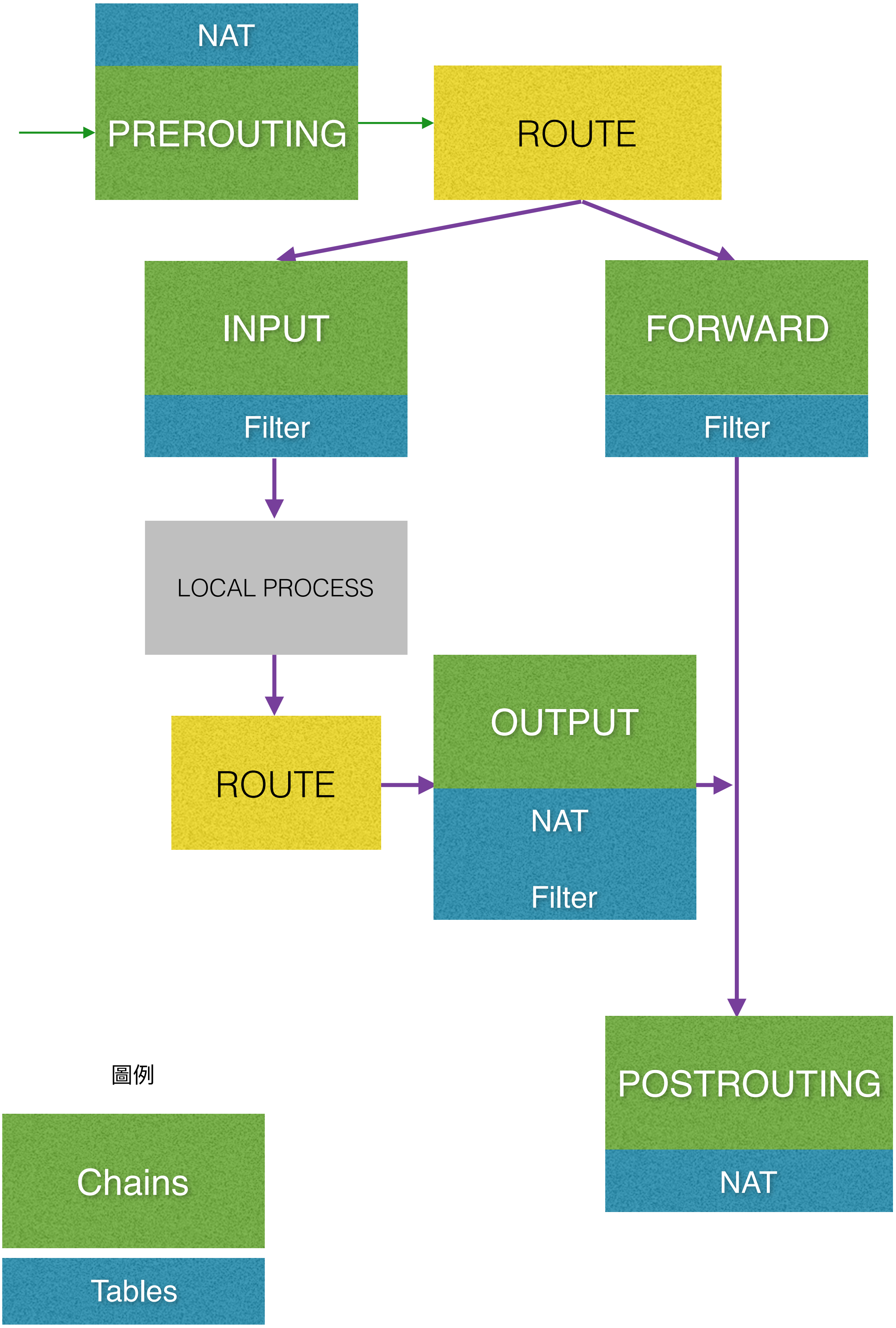
Members

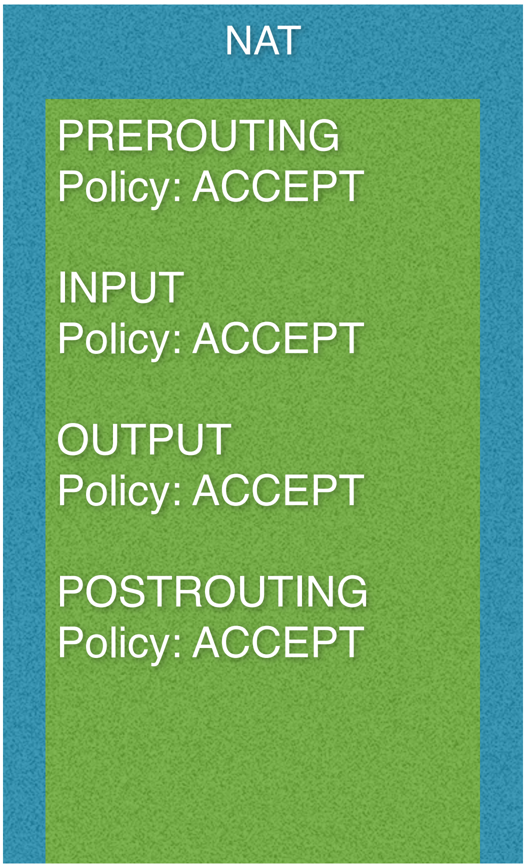
B01501085	莊東諺	B03902087	周景軒
B00401062	羅文斌	B01902051	張君瑋
B02501091	周宇霖	B03902023	尤沐惠

0. 簡介

在這次的實驗中我們使用Linux系統中的 iptables 指令來實作Firewall以及NAT server，並且設定DHCP server。我們使用兩台虛擬機器(Linux Ubuntu 14.04)，第一台機器 A 作為主要的NAT與DHCP server，並且寫入一些規則；第二台機器 B 則是一台測試機，主要從 A 取得分發的ip並且上網。在VirtualBox的設定中，A 有兩張網卡，第一張作為向外上網使用；第二張則是作為DHCP發放IP的網卡。在Firewall的規則中，我們必須阻擋除了HTTP、DNS、FTP、ICMP、Telnet、POP3/SMTP以外的服務。主要的實作方法是在 iptables 中把 FORWARD 的 default 設定成REJECT，之後再加上可以開放的 PORT 即可。

1. 流程圖


NAT
PREROUTING
ROUTE
INPUT
Filter
FORWARD
Filter
LOCAL PROCESS
ROUTE
OUTPUT
NAT
Filter
POSTROUTING
NAT
圖例
Chains
Tables



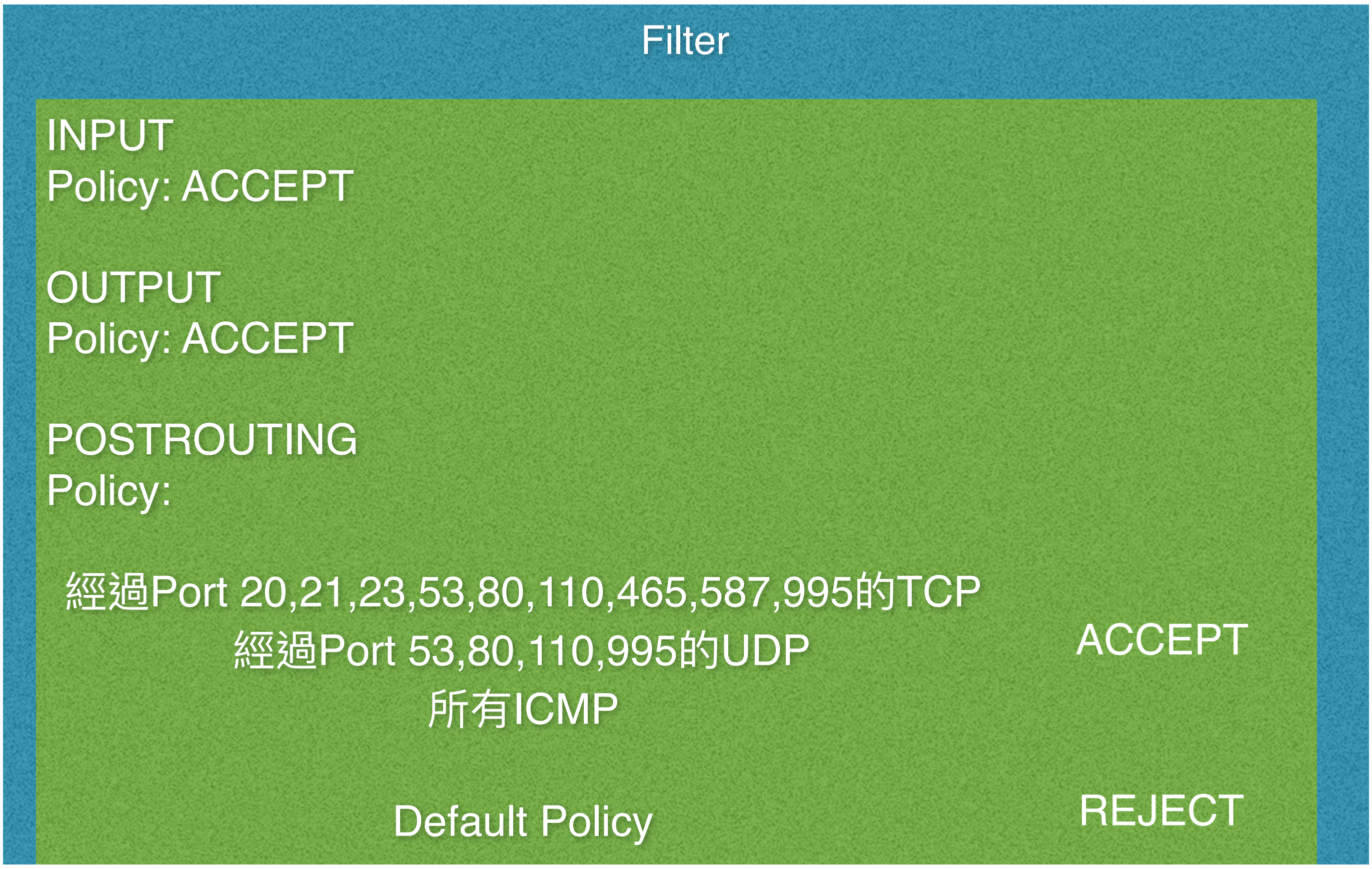
NAT

PREROUTING
Policy: ACCEPT

INPUT
Policy: ACCEPT

OUTPUT
Policy: ACCEPT

POSTROUTING
Policy: ACCEPT



Filter

INPUT
Policy: ACCEPT

OUTPUT
Policy: ACCEPT

POSTROUTING
Policy:

經過Port 20,21,23,53,80,110,465,587,995的TCP
經過Port 53,80,110,995的UDP
所有ICMP

ACCEPT

Default Policy

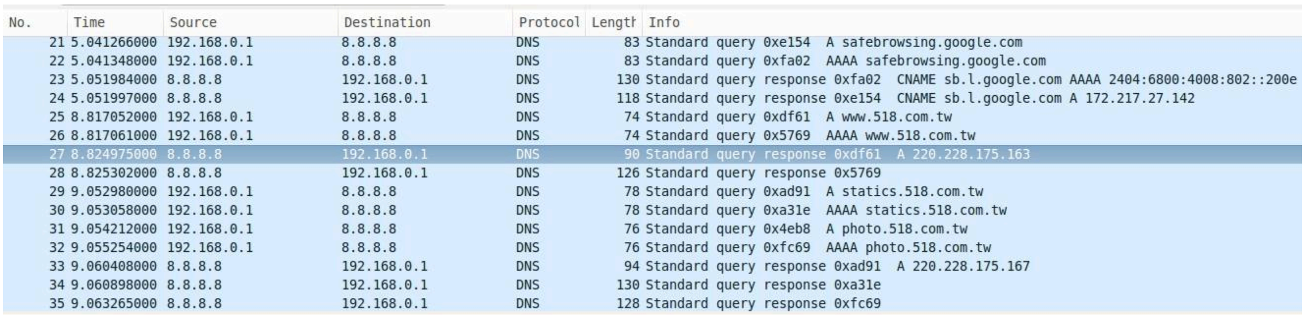
REJECT

2. Shell Script

```
#clear nat rules
iptables -t nat -F
iptables -t nat -X
iptables -t nat -Z

#clear filter rules
iptables -t filter -F
iptables -t filter -X
iptables -t filter -Z

#forwarding
iptables -t nat -A POSTROUTING -s 192.168.0.0/16 -o eth0 -j MASQUERADE

#accept some port
iptables -A FORWARD -p TCP -m multiport -i eth1 --dport
20,21,23,25,53,80,110,465,587,995 -j ACCEPT
iptables -A FORWARD -p TCP -m multiport -i eth1 --sport
20,21,23,25,53,80,110,465,587,995 -j ACCEPT
iptables -A FORWARD -p UDP -m multiport -i eth1 --dport 53,80,110,995 -j ACCEPT
iptables -A FORWARD -p UDP -m multiport -i eth1 --sport 53,80,110,995 -j ACCEPT
iptables -A FORWARD -p icmp -j ACCEPT

#reject others
iptables -A FORWARD -i eth1 -j REJECT

echo "1" > /proc/sys/net/ipv4/ip_forward
```

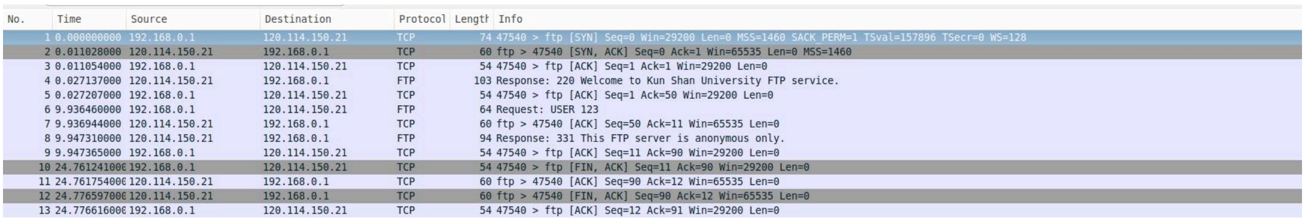
3. Wireshark Verification

DNS



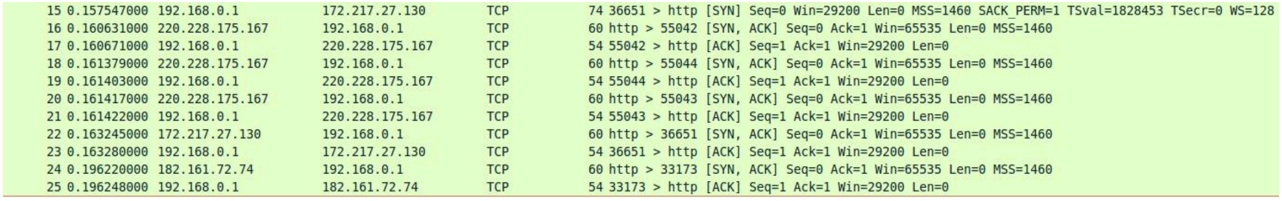
No.	Time	Source	Destination	Protocol	Length	Info
21	5.041266000	192.168.0.1	8.8.8.8	DNS	83	Standard query 0xe154 A safebrowsing.google.com
22	5.041348000	192.168.0.1	8.8.8.8	DNS	83	Standard query 0xfa02 AAAA safebrowsing.google.com
23	5.051984000	8.8.8.8	192.168.0.1	DNS	130	Standard query response 0xfa02 CNAME sb.l.google.com AAAA 2404:6800:4008:802::200e
24	5.051997000	8.8.8.8	192.168.0.1	DNS	118	Standard query response 0xe154 CNAME sb.l.google.com A 172.217.27.142
25	8.817052000	192.168.0.1	8.8.8.8	DNS	74	Standard query 0xdf61 A www.518.com.tw
26	8.817061000	192.168.0.1	8.8.8.8	DNS	74	Standard query 0x5769 AAAA www.518.com.tw
27	8.824975000	8.8.8.8	192.168.0.1	DNS	90	Standard query response 0xdf61 A 220.228.175.163
28	8.825302000	8.8.8.8	192.168.0.1	DNS	126	Standard query response 0x5769
29	9.052980000	192.168.0.1	8.8.8.8	DNS	78	Standard query 0xad91 A statics.518.com.tw
30	9.053058000	192.168.0.1	8.8.8.8	DNS	78	Standard query 0xa31e AAAA statics.518.com.tw
31	9.054212000	192.168.0.1	8.8.8.8	DNS	76	Standard query 0x4eb8 A photo.518.com.tw
32	9.055254000	192.168.0.1	8.8.8.8	DNS	76	Standard query 0xfc69 AAAA photo.518.com.tw
33	9.060408000	8.8.8.8	192.168.0.1	DNS	94	Standard query response 0xad91 A 220.228.175.167
34	9.060898000	8.8.8.8	192.168.0.1	DNS	130	Standard query response 0xa31e
35	9.063265000	8.8.8.8	192.168.0.1	DNS	128	Standard query response 0xfc69

FTP



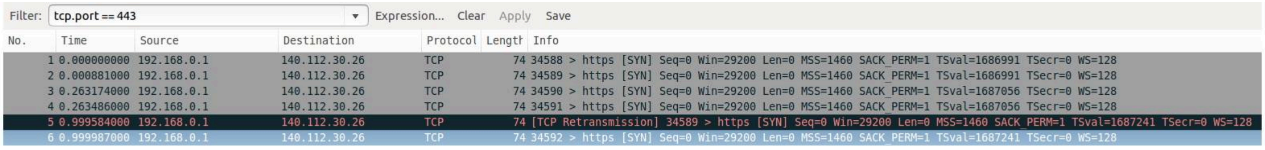
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.0.1	120.114.150.21	TCP	74	47540 > ftp [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=157896 TSecr=0 WS=128
2	0.011028000	120.114.150.21	192.168.0.1	TCP	60	ftp > 47540 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
3	0.011054000	192.168.0.1	120.114.150.21	TCP	54	47540 > ftp [ACK] Seq=1 Ack=1 Win=29200 Len=0
4	0.027137000	120.114.150.21	192.168.0.1	FTP	103	Response: 220 Welcome to Kun Shan University FTP service.
5	0.027207000	192.168.0.1	120.114.150.21	TCP	54	47540 > ftp [ACK] Seq=1 Ack=50 Win=29200 Len=0
6	9.936460000	192.168.0.1	120.114.150.21	FTP	64	Request: USER 123
7	9.936944000	120.114.150.21	192.168.0.1	TCP	60	ftp > 47540 [ACK] Seq=50 Ack=11 Win=65535 Len=0
8	9.947310000	120.114.150.21	192.168.0.1	FTP	94	Response: 331 This FTP server is anonymous only.
9	9.947365000	192.168.0.1	120.114.150.21	TCP	54	47540 > ftp [ACK] Seq=11 Ack=90 Win=29200 Len=0
10	24.76124100	192.168.0.1	120.114.150.21	TCP	54	47540 > ftp [FIN, ACK] Seq=11 Ack=90 Win=29200 Len=0
11	24.76175400	120.114.150.21	192.168.0.1	TCP	60	ftp > 47540 [ACK] Seq=90 Ack=12 Win=65535 Len=0
12	24.77659700	120.114.150.21	192.168.0.1	TCP	60	ftp > 47540 [FIN, ACK] Seq=90 Ack=12 Win=65535 Len=0
13	24.77661600	192.168.0.1	120.114.150.21	TCP	54	47540 > ftp [ACK] Seq=12 Ack=91 Win=29200 Len=0

HTTP



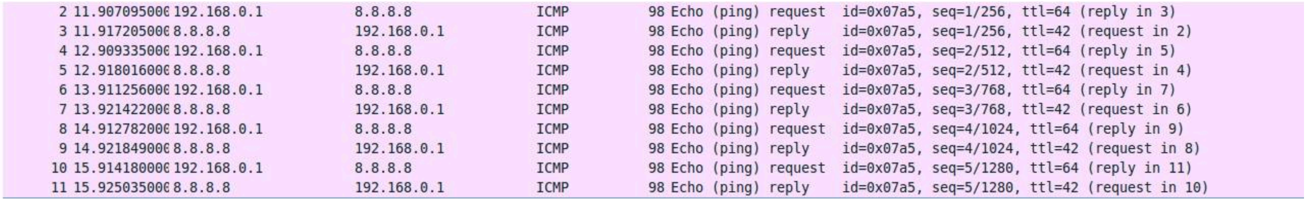
```
15 0.157547000 192.168.0.1       172.217.27.130    TCP    74 36651 > http [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=1828453 TSecr=0 WS=128
16 0.160631000 220.228.175.167   192.168.0.1       TCP    60 http > 55042 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
17 0.160671000 192.168.0.1       220.228.175.167   TCP    54 55042 > http [ACK] Seq=1 Ack=1 Win=29200 Len=0
18 0.161379000 220.228.175.167   192.168.0.1       TCP    60 http > 55044 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
19 0.161403000 192.168.0.1       220.228.175.167   TCP    54 55044 > http [ACK] Seq=1 Ack=1 Win=29200 Len=0
20 0.161417000 220.228.175.167   192.168.0.1       TCP    60 http > 55043 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
21 0.161422000 192.168.0.1       220.228.175.167   TCP    54 55043 > http [ACK] Seq=1 Ack=1 Win=29200 Len=0
22 0.163245000 172.217.27.130    192.168.0.1       TCP    60 http > 36651 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
23 0.163280000 192.168.0.1       172.217.27.130    TCP    54 36651 > http [ACK] Seq=1 Ack=1 Win=29200 Len=0
24 0.196220000 182.161.72.74     192.168.0.1       TCP    60 http > 33173 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
25 0.196248000 192.168.0.1       182.161.72.74     TCP    54 33173 > http [ACK] Seq=1 Ack=1 Win=29200 Len=0
```

HTTPS



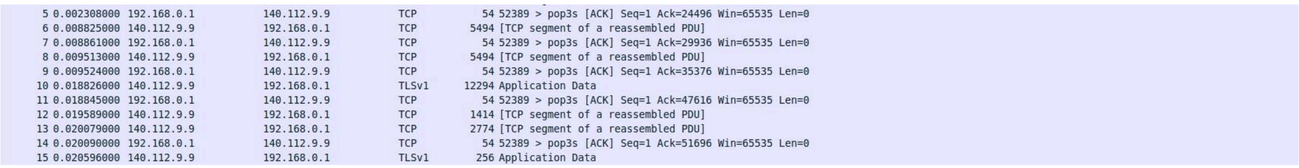
```
Filter: tcp.port == 443
No.  Time        Source        Destination      Protocol Length Info
   1 0.000000000 192.168.0.1   140.112.30.26    TCP      74 34588 > https [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=1686991 TSecr=0 WS=128
   2 0.000881000 192.168.0.1   140.112.30.26    TCP      74 34589 > https [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=1686991 TSecr=0 WS=128
   3 0.263174000 192.168.0.1   140.112.30.26    TCP      74 34590 > https [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=1687056 TSecr=0 WS=128
   4 0.263486000 192.168.0.1   140.112.30.26    TCP      74 34591 > https [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=1687056 TSecr=0 WS=128
   5 0.999584000 192.168.0.1   140.112.30.26    TCP      74 [TCP Retransmission] 34589 > https [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=1687241 TSecr=0 WS=128
   6 0.999987000 192.168.0.1   140.112.30.26    TCP      74 34592 > https [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=1687241 TSecr=0 WS=128
```

ICMP



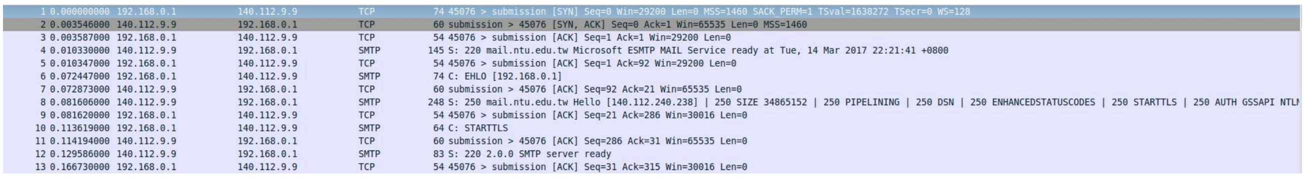
```
 2 11.907095000 192.168.0.1   8.8.8.8        ICMP   98 Echo (ping) request  id=0x07a5, seq=1/256, ttl=64 (reply in 3)
 3 11.917205000 8.8.8.8       192.168.0.1    ICMP   98 Echo (ping) reply    id=0x07a5, seq=1/256, ttl=42 (request in 2)
 4 12.909335000 192.168.0.1   8.8.8.8        ICMP   98 Echo (ping) request  id=0x07a5, seq=2/512, ttl=64 (reply in 5)
 5 12.918016000 8.8.8.8       192.168.0.1    ICMP   98 Echo (ping) reply    id=0x07a5, seq=2/512, ttl=42 (request in 4)
 6 13.911256000 192.168.0.1   8.8.8.8        ICMP   98 Echo (ping) request  id=0x07a5, seq=3/768, ttl=64 (reply in 7)
 7 13.921422000 8.8.8.8       192.168.0.1    ICMP   98 Echo (ping) reply    id=0x07a5, seq=3/768, ttl=42 (request in 6)
 8 14.912782000 192.168.0.1   8.8.8.8        ICMP   98 Echo (ping) request  id=0x07a5, seq=4/1024, ttl=64 (reply in 9)
 9 14.921849000 8.8.8.8       192.168.0.1    ICMP   98 Echo (ping) reply    id=0x07a5, seq=4/1024, ttl=42 (request in 8)
10 15.914180000 192.168.0.1   8.8.8.8        ICMP   98 Echo (ping) request  id=0x07a5, seq=5/1280, ttl=64 (reply in 11)
11 15.925035000 8.8.8.8       192.168.0.1    ICMP   98 Echo (ping) reply    id=0x07a5, seq=5/1280, ttl=42 (request in 10)
```

POP3



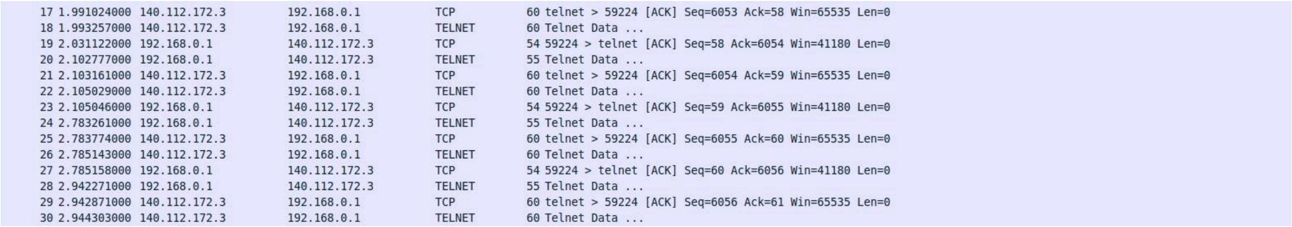
```
 5 0.002308000 192.168.0.1    140.112.9.9    TCP       54 52389 > pop3s [ACK] Seq=1 Ack=24496 Win=65535 Len=0
 6 0.008825000 140.112.9.9    192.168.0.1    TCP     5494 [TCP segment of a reassembled PDU]
 7 0.008861000 192.168.0.1    140.112.9.9    TCP       54 52389 > pop3s [ACK] Seq=1 Ack=29936 Win=65535 Len=0
 8 0.009513000 140.112.9.9    192.168.0.1    TCP     5494 [TCP segment of a reassembled PDU]
 9 0.009524000 192.168.0.1    140.112.9.9    TCP       54 52389 > pop3s [ACK] Seq=1 Ack=35376 Win=65535 Len=0
10 0.018826000 140.112.9.9    192.168.0.1    TLSv1  12294 Application Data
11 0.018845000 192.168.0.1    140.112.9.9    TCP       54 52389 > pop3s [ACK] Seq=1 Ack=47616 Win=65535 Len=0
12 0.019589000 140.112.9.9    192.168.0.1    TCP     1414 [TCP segment of a reassembled PDU]
13 0.020079000 140.112.9.9    192.168.0.1    TCP     2774 [TCP segment of a reassembled PDU]
14 0.020090000 192.168.0.1    140.112.9.9    TCP       54 52389 > pop3s [ACK] Seq=1 Ack=51696 Win=65535 Len=0
15 0.020596000 140.112.9.9    192.168.0.1    TLSv1    256 Application Data
```

SMTP



```
 1 0.000000000 192.168.0.1   140.112.9.9   TCP    74 45076 > submission [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=1638272 TSecr=0 WS=128
 2 0.003546000 140.112.9.9   192.168.0.1   TCP    60 submission > 45076 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
 3 0.003587000 192.168.0.1   140.112.9.9   TCP    54 45076 > submission [ACK] Seq=1 Ack=1 Win=29200 Len=0
 4 0.010330000 140.112.9.9   192.168.0.1   SMTP  145 S: 220 mail.ntu.edu.tw Microsoft ESMTP MAIL Service ready at Tue, 14 Mar 2017 22:21:41 +0800
 5 0.010347000 192.168.0.1   140.112.9.9   TCP    54 45076 > submission [ACK] Seq=1 Ack=92 Win=29200 Len=0
 6 0.072447000 192.168.0.1   140.112.9.9   SMTP   74 C: EHLO [192.168.0.1]
 7 0.072873000 140.112.9.9   192.168.0.1   TCP    60 submission > 45076 [ACK] Seq=92 Ack=21 Win=65535 Len=0
 8 0.081606000 140.112.9.9   192.168.0.1   SMTP  248 S: 250 mail.ntu.edu.tw Hello [140.112.240.238] | 250 SIZE 34865152 | 250 PIPELINING | 250 DSN | 250 ENHANCEDSTATUSCODES | 250 STARTTLS | 250 AUTH GSSAPI NTLM
 9 0.081620000 192.168.0.1   140.112.9.9   TCP    54 45076 > submission [ACK] Seq=21 Ack=286 Win=30016 Len=0
10 0.113619000 192.168.0.1   140.112.9.9   SMTP   64 C: STARTTLS
11 0.114194000 140.112.9.9   192.168.0.1   TCP    60 submission > 45076 [ACK] Seq=286 Ack=31 Win=65535 Len=0
12 0.129586000 140.112.9.9   192.168.0.1   SMTP   83 S: 220 2.0.0 SMTP server ready
13 0.166730000 192.168.0.1   140.112.9.9   TCP    54 45076 > submission [ACK] Seq=31 Ack=315 Win=30016 Len=0
```

Telnet



```
17 1.991024000 140.112.172.3   192.168.0.1     TCP     60 telnet > 59224 [ACK] Seq=6053 Ack=58 Win=65535 Len=0
18 1.993257000 140.112.172.3   192.168.0.1     TELNET  60 Telnet Data ...
19 2.031122000 192.168.0.1     140.112.172.3   TCP     54 59224 > telnet [ACK] Seq=58 Ack=6054 Win=41180 Len=0
20 2.102777000 192.168.0.1     140.112.172.3   TELNET  55 Telnet Data ...
21 2.103161000 140.112.172.3   192.168.0.1     TCP     60 telnet > 59224 [ACK] Seq=6054 Ack=59 Win=65535 Len=0
22 2.105029000 140.112.172.3   192.168.0.1     TELNET  60 Telnet Data ...
23 2.105046000 192.168.0.1     140.112.172.3   TCP     54 59224 > telnet [ACK] Seq=59 Ack=6055 Win=41180 Len=0
24 2.783261000 192.168.0.1     140.112.172.3   TELNET  55 Telnet Data ...
25 2.783774000 140.112.172.3   192.168.0.1     TCP     60 telnet > 59224 [ACK] Seq=6055 Ack=60 Win=65535 Len=0
26 2.785143000 140.112.172.3   192.168.0.1     TELNET  60 Telnet Data ...
27 2.785158000 192.168.0.1     140.112.172.3   TCP     54 59224 > telnet [ACK] Seq=60 Ack=6056 Win=41180 Len=0
28 2.942271000 192.168.0.1     140.112.172.3   TELNET  55 Telnet Data ...
29 2.942871000 140.112.172.3   192.168.0.1     TCP     60 telnet > 59224 [ACK] Seq=6056 Ack=61 Win=65535 Len=0
30 2.944303000 140.112.172.3   192.168.0.1     TELNET  60 Telnet Data ...
```

4. Application

firewall：當你以後成為台大資工系某程式設計課的老師，你希望可以在考試的三個小時裡關閉所有的連線，只能連上自己的Online Judge/Judgegirl System時，你可以使用firewall 擋下除了OJ以外的所有東西。設定Router讓此時FORWARD的IP只有Online Judge可以通過，其他的封包一律DROP。並且可以設定timer，在考試結束後就清空規則。

ex:

```
iptables -A FORWARD -p TCP -s 140.112.xxx.xxx -j ACCEPT
iptables -A FORWARD -i eth1 -j REJECT
sleep 10800
iptables -t filter -F
iptables -t filter -X
iptables -t filter -Z
```