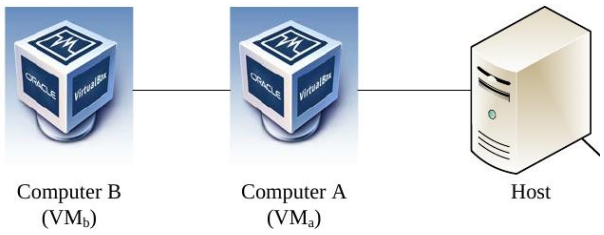
CNL Lab1 Report

2017.03.15

Contribution by each team member

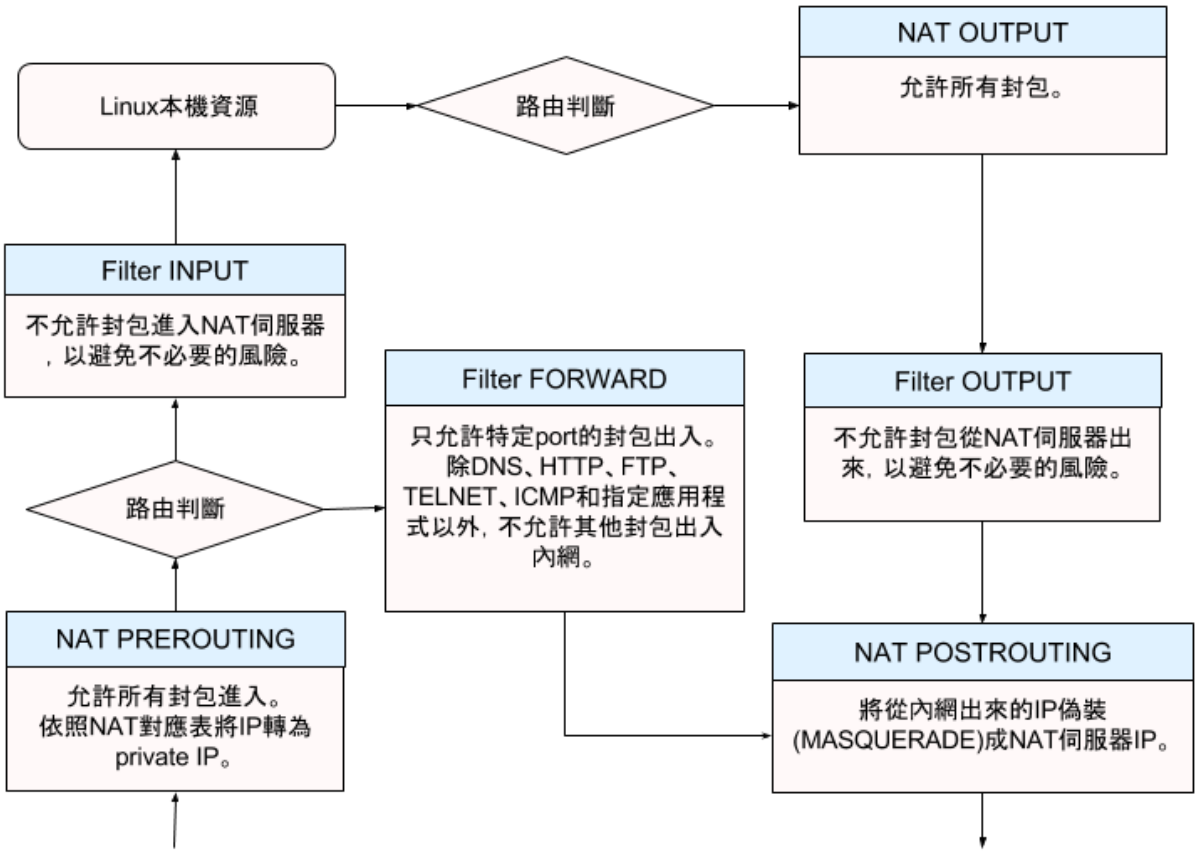
ID	Name	Contribution
b03902080	黃子賢	1/6
b03902022	于建民	1/6
b03902024	鄭筱樺	1/6
b03902026	徐新凱	1/6
b03902084	王藝霖	1/6
b03902126	高翊軒	1/6

Task



1. Enable ComputerB to get its private IP address by DHCP and ComputerA to translate ComputerB's private IP to public IP
2. Enable ComputerB to link to internet through ComputerA
3. Block packets except DNS, HTTP, FTP, Telnet, ICMP, and SSH

Flow Chart


Linux本機資源
路由判斷
NAT OUTPUT
允許所有封包。
Filter INPUT
不允許封包進入NAT伺服器，以避免不必要的風險。
Filter FORWARD
只允許特定port的封包出入。除DNS、HTTP、FTP、TELNET、ICMP和指定應用程式以外，不允許其他封包出入內網。
Filter OUTPUT
不允許封包從NAT伺服器出來，以避免不必要的風險。
路由判斷
NAT PREROUTING
允許所有封包進入。依照NAT對應表將IP轉為private IP。
NAT POSTROUTING
將從內網出來的IP偽裝(MASQUERADE)成NAT伺服器IP。

Verification through Wireshark

1. Execute `nslookup www.google.com` on ComputerB

Packets captured on ComputerA:

eth0

No.	Time	Source	Destination	Protoco	Length	Info
1	0.000000000	10.0.2.15	140.112.254.4	DNS	74	Standard query 0x88b2 A www.google.com
2	0.000085000	10.0.2.15	140.112.17.1	DNS	74	Standard query 0x88b2 A www.google.com
3	0.262078000	140.112.254.4	10.0.2.15	DNS	450	Standard query response 0x88b2 A 163.28.18.29
4	5.001558000	CadmusCo_04:16:c2	RealtekU_12:35:02	ARP	42	Who has 10.0.2.2? Tell 10.0.2.15
5	5.001787000	RealtekU_12:35:02	CadmusCo_04:16:c2	ARP	60	10.0.2.2 is at 52:54:00:12:35:02

eth1

No.	Time	Source	Destination	Protoco	Length	Info
1	0.000000000	192.168.100.20	140.112.254.4	DNS	74	Standard query 0x17ec A www.google.com
2	0.000100000	192.168.100.20	140.112.17.1	DNS	74	Standard query 0x17ec A www.google.com
3	0.001710000	140.112.254.4	192.168.100.20	DNS	450	Standard query response 0x17ec A 163.28.18.44 A
4	5.009803000	CadmusCo_ba:8a:d0	CadmusCo_91:8e:97	ARP	42	Who has 192.168.100.20? Tell 192.168.100.254
5	5.010068000	CadmusCo_91:8e:97	CadmusCo_ba:8a:d0	ARP	60	192.168.100.20 is at 08:00:27:91:8e:97

We can see the source IP of ComputerB has been changed from **192.168.100.20** to **10.0.2.15**, which means that ComputerA is able to do the correct translation.

2. ComputerB can connect to internet through ComputerA

Access `www.csie.ntu.edu.tw` on ComputerB

eth1

1	0.000000000	10.0.2.15	140.112.254.4	DNS	79	Standard query 0xcea1 A www.csie.ntu.edu.tw
2	0.000097000	10.0.2.15	140.112.17.1	DNS	79	Standard query 0xcea1 A www.csie.ntu.edu.tw
3	0.000461000	10.0.2.15	140.112.254.4	DNS	79	Standard query 0x93b8 AAAA www.csie.ntu.edu.tw
4	0.003191000	140.112.17.1	10.0.2.15	ICMP	107	Destination unreachable (Port unreachable)
5	0.003262000	140.112.254.4	10.0.2.15	DNS	204	Standard query response 0xcea1 A 140.112.30.26
6	0.003517000	140.112.254.4	10.0.2.15	DNS	126	Standard query response 0x93b8
7	0.003897000	10.0.2.15	140.112.30.26	TCP	74	49710 > http [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=29
8	0.006466000	140.112.30.26	10.0.2.15	TCP	60	http > 49710 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
9	0.006732000	10.0.2.15	140.112.30.26	TCP	54	49710 > http [ACK] Seq=1 Ack=1 Win=29200 Len=0
10	0.009177000	10.0.2.15	140.112.30.26	HTTP	351	GET / HTTP/1.1
11	0.009368000	140.112.30.26	10.0.2.15	TCP	60	http > 49710 [ACK] Seq=1 Ack=298 Win=65535 Len=0
12	1.042800000	140.112.30.26	10.0.2.15	HTTP	616	HTTP/1.1 301 Moved Permanently (text/html)
13	1.043291000	10.0.2.15	140.112.30.26	TCP	54	49710 > http [ACK] Seq=298 Ack=563 Win=29786 Len=0
14	5.004107000	CadmusCo_07:9e:fa	RealtekU_12:35:02	ARP	42	Who has 10.0.2.2? Tell 10.0.2.15
15	5.004261000	RealtekU_12:35:02	CadmusCo_07:9e:fa	ARP	60	10.0.2.2 is at 52:54:00:12:35:02
16	6.050166000	140.112.30.26	10.0.2.15	TCP	60	http > 49710 [FIN, ACK] Seq=563 Ack=298 Win=65535 Len=0
17	6.050683000	10.0.2.15	140.112.30.26	TCP	54	49710 > http [FIN, ACK] Seq=298 Ack=564 Win=29786 Len=0
18	6.050927000	140.112.30.26	10.0.2.15	TCP	60	http > 49710 [ACK] Seq=564 Ack=299 Win=65535 Len=0

3. Block packets except DNS, HTTP, FTP, Telnet, ICMP, and SSH

Access `www.google.com` on ComputerB (https packets blocked by ComputerA's firewall)

eth1

No.	Time	Source	Destination	Protoco	Length	Info
8	0.025260000	192.168.100.20	140.112.254.4	DNS	77	Standard query 0x0dd9 A www.google.com.tw
9	0.025370000	192.168.100.20	140.112.17.1	DNS	77	Standard query 0x0dd9 A www.google.com.tw
10	0.025724000	192.168.100.20	140.112.254.4	DNS	77	Standard query 0xa7f3 AAAA www.google.com.tw
11	0.028701000	140.112.254.4	192.168.100.20	DNS	251	Standard query response 0xa7f3 AAAA 2404:6800:4008:802::2003
12	0.028760000	140.112.254.4	192.168.100.20	DNS	415	Standard query response 0x0dd9 A 202.169.175.117 A 202.169.175.123 A 202.169.175.82 A 202.169.175.88 A 202.169.175.89
13	0.032109000	192.168.100.20	202.169.175.117	TCP	74	38995 > http [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=1121525 TSecr=0 WS=128
14	0.035481000	202.169.175.117	192.168.100.20	TCP	58	http > 38995 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
15	0.035740000	192.168.100.20	202.169.175.117	TCP	60	38995 > http [ACK] Seq=1 Ack=1 Win=29200 Len=0
16	0.064168000	192.168.100.20	202.169.175.117	HTTP	385	GET /?gfe_rd=cr&ei=Pc2_WK-0F-b88we6raKQAQ HTTP/1.1
17	0.064522000	202.169.175.117	192.168.100.20	TCP	54	http > 38995 [ACK] Seq=1 Ack=332 Win=65535 Len=0
18	0.096776000	202.169.175.117	192.168.100.20	HTTP	981	HTTP/1.1 302 Found (text/html)
19	0.096980000	192.168.100.20	202.169.175.117	TCP	60	38995 > http [ACK] Seq=332 Ack=928 Win=30591 Len=0
20	0.177322000	192.168.100.20	202.169.175.117	TCP	74	36485 > https [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=1121561 TSecr=0 WS=128
21	0.433421000	192.168.100.20	202.169.175.117	TCP	74	36486 > https [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=1121625 TSecr=0 WS=128
22	1.180943000	192.168.100.20	202.169.175.117	TCP	74	[TCP Retransmission] 36485 > https [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=1121812 TSecr=0 WS=128
23	1.433958000	192.168.100.20	202.169.175.117	TCP	74	[TCP Retransmission] 36486 > https [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=1121876 TSecr=0 WS=128
24	3.183285000	192.168.100.20	202.169.175.117	TCP	74	[TCP Retransmission] 36485 > https [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=1122313 TSecr=0 WS=128
25	3.439320000	192.168.100.20	202.169.175.117	TCP	74	[TCP Retransmission] 36486 > https [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=1122377 TSecr=0 WS=128

12 packets are dropped

```
vm@vm:~$ sudo iptables -L -n -v -x
Chain INPUT (policy DROP 0 packets, 0 bytes)
    pkts      bytes target     prot opt in     out     source               destination

Chain FORWARD (policy DROP 12 packets, 720 bytes)
    pkts      bytes target     prot opt in     out     source               destination
      27    27465 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           multiport sports 20,21,22,23,53,80
      22     4354 ACCEPT     udp  --  *      *       0.0.0.0/0            0.0.0.0/0           multiport sports 20,21,22,23,53,80
      33     3068 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           multiport dports 20,21,22,23,53,80
      25     1529 ACCEPT     udp  --  *      *       0.0.0.0/0            0.0.0.0/0           multiport dports 20,21,22,23,53,80
       0        0 ACCEPT     icmp --  *      *       0.0.0.0/0            0.0.0.0/0

Chain OUTPUT (policy DROP 0 packets, 0 bytes)
    pkts      bytes target     prot opt in     out     source               destination
```

Append the following three commands to shell script to log the dropped packets:

```
iptables -N LOGGING
iptables -A FORWARD -j LOGGING
iptables -A LOGGING -j LOG --log-prefix "IPTables- Dropped: " --log-level 4
```

Type `cat /var/log/kern.log | grep "IPTables-Dropped:"` and we can see the port 443 used by https is blocked.

```
Mar 15 12:49:22 cnl1-VirtualBox kernel: [  490.832458] IPTables-Dropped: IN=eth1 OUT=eth0 MAC=08:00:27:ec:e6:b8:08:00:27:07:9e:fa:08:0
0 SRC=192.168.100.20 DST=52.26.29.31 LEN=60 TOS=0x00 PREC=0x00 TTL=63 ID=32564 DF PROTO=TCP SPT=36130 DPT=443 WINDOW=29200 RES=0x00 SY
N URGP=0
```

Application

- Scenario: Use this design as an internal network of a company
- Assumption: All employees use computerB, and each packets have to go through computerA before reaching their destination

Security

- In order to make sure data security of the company, the company can disable some insecure ports. For example, the company can set the iptable in ComputerA to block ports like HTTP, and FTP, which forces employees to use more secure ports like HTTPs and SFTP.
- By blocking packets from malicious websites, the company can prevent workers to access those websites accidently.

Employee management

- The company can block some sites that will distract employees from their work, such as Facebook, and Line.

Solve the problem of insufficient IP addresses

- By using NAT and private IP, the company can reduce the number of IP addresses they use.