

## NA HW1 隨筆

環境: virtualbox using Ubuntu 18.04.2 as Router and ClientPC

### 建立 ClientPC

設定為內部網路

Ubuntu 會自動 DHCP 幫你連到內網(連不到代表 DHCP 做錯了)

### 建立 Router

Two network adapter

一個用於 NAT

一個用於內部網路

在/etc/network/interfaces 中設一靜態 ip

```
auto enp0s8
iface enp0s8 inet static
address 10.113.33.254
netmask 255.255.255.0
network 10.113.33.0
broadcast 10.113.33.255
```

啟動此網卡

```
sudo apt install ifupdown
ifup enp0s8
```

### DHCP

安裝

```
sudo apt-get -y install isc-dhcp-server
```

把 enp0s8 設為預設 dhcp

```
sudo nano /etc/default/isc-dhcp-server
INTERFACES="" 改為 INTERFACES=" enp0s8 "
```

對 DHCP 設定檔進行服務需求設定

```
sudo nano /etc/dhcp/dhcpd.conf
subnet 10.113.33.0 netmask 255.255.255.0 {
    range 10.113.33.100 10.113.33.200;
    option domain-name-servers 8.8.8.8;
    option domain-name "internal.example.org";
    option subnet-mask 255.255.255.0;
    option routers 10.113.33.254;
    option broadcast-address 10.113.33.255;
    max-lease-time 7200;
}
```

```
/etc/init.d/isc-dhcp-server restart
```

## VPN

安裝 wireguard

```
sudo add-apt-repository ppa:wireguard/wireguard
```

```
sudo apt-get update
```

```
sudo apt-get install wireguard
```

/etc/wireguard/ 下新增 wg0.conf 檔

```
[Interface]
```

```
PrivateKey = <Private Key>
```

```
Address = <Peer IP>
```

```
[Peer]
```

```
PublicKey = <Public Key>
```

```
Endpoint = <Server Public IP>:<Port>
```

```
AllowedIPs = 10.113.0.0/16
```

```
PersistentKeepalive = 25
```

```
sudo wg-quick up wg0
```

```
sudo wg
```

測試 ping 140.113.0.254

讓 WireGuard 開機啟動

```
systemctl enable wg-quick@wg0
```

## Firewalls

```
iptables -F
```

```
iptables -X
```

```
iptables -F -t mangle
```

```
iptables -t mangle -X
```

```
iptables -F -t nat
```

```
iptables -t nat -X
```

```
iptables -P INPUT DROP
```

```
iptables -A INPUT -i lo -j ACCEPT
```

```
iptables -A INPUT -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT
```

```
iptables -A INPUT -i wg0 -s 10.113.0.0/16 -j ACCEPT
```

```
sudo iptables -A INPUT -i enp0s8 -j ACCEPT
```

## NAT 和 iptable 設定

啟動 ip\_forward

```
vim /etc/sysctl.conf  
net.ipv4.ip_forward=1
```

iptables

enp0s3 是連 NAT 的網卡

enp0s8 是連內網的網卡

```
sudo iptables -t nat -A POSTROUTING -o enp0s3 -j MASQUERADE  
sudo iptables -A FORWARD -i enp0s8 -o enp0s3 -j ACCEPT  
sudo iptables -A FORWARD -i enp0s8 -o wg0 -j ACCEPT  
sudo iptables-save
```

安裝 iptable persistent 並設定

```
sudo apt install iptables-persistent  
sudo dpkg-reconfigure iptables-persistent
```