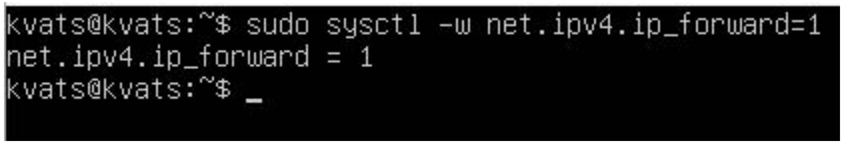
NSS Lab 6

Kaustav Vats
Sushant Kumar Singh

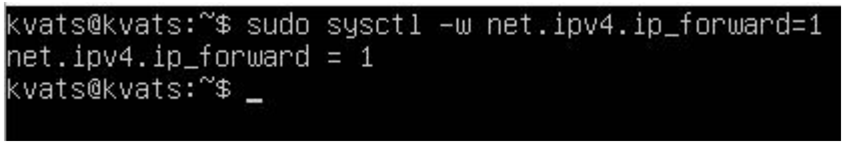
VM Details

- VM1 - 10.0.0.8
- VM2 - 10.0.0.9, 20.0.0.9
- VM3 - 20.0.0.4, 30.0.0.4
- VM4 - 30.0.0.5

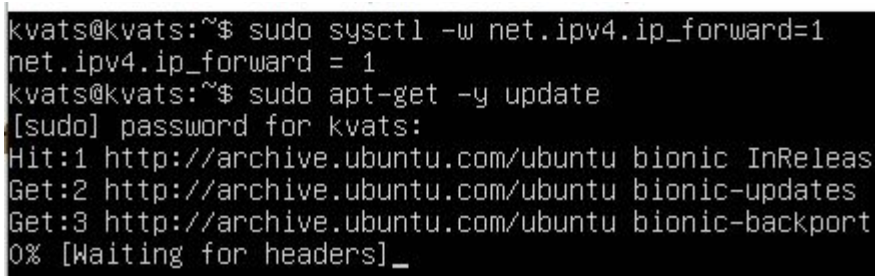


```
kvats@kvats:~$ sudo sysctl -w net.ipv4.ip_forward=1
net.ipv4.ip_forward = 1
kvats@kvats:~$ _
```

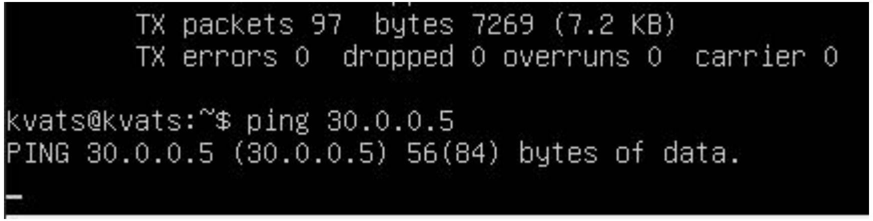
Here we enabled IP forwarding on VM2 and VM3



```
kvats@kvats:~$ sudo sysctl -w net.ipv4.ip_forward=1
net.ipv4.ip_forward = 1
kvats@kvats:~$ _
```



```
kvats@kvats:~$ sudo sysctl -w net.ipv4.ip_forward=1
net.ipv4.ip_forward = 1
kvats@kvats:~$ sudo apt-get -y update
[sudo] password for kvats:
Hit:1 http://archive.ubuntu.com/ubuntu bionic InReleas
Get:2 http://archive.ubuntu.com/ubuntu bionic-updates
Get:3 http://archive.ubuntu.com/ubuntu bionic-backport
0% [Waiting for headers]_
```



```
        TX packets 97  bytes 7269 (7.2 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0

kvats@kvats:~$ ping 30.0.0.5
PING 30.0.0.5 (30.0.0.5) 56(84) bytes of data.
_
```

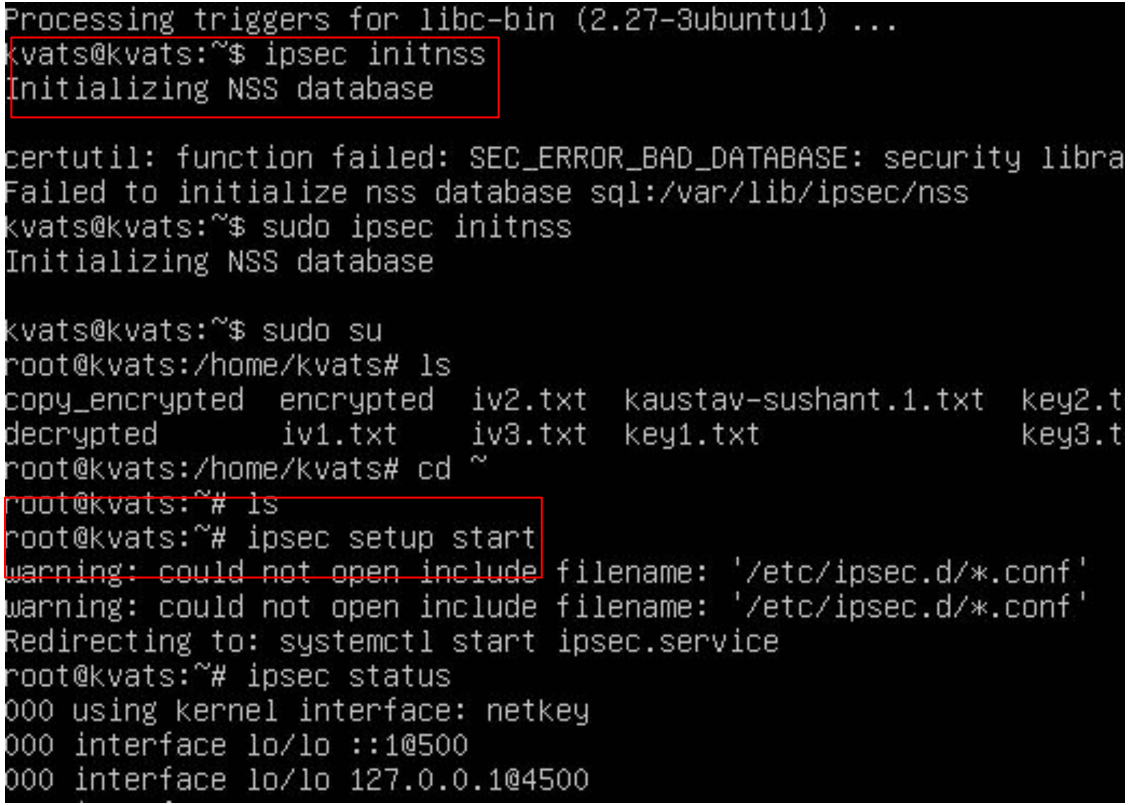
In above image you can see that VM1 is not able to ping VM4. Both Vm's are unaware of each other and are not able to ping each other.

After enabling IP forwarding on VM2 and VM3, we installed LibreSwarn on both the VM's. Using installation commands given in both the ref links, we installed LibreSwarn in our VM's.

wget https://download.libreswan.org/libreswan-3.20.tar.gz
tar -xzf libreswan-3.20.tar.gz
Make all
Or
Sudo apt install libreswarn

[1]
https://www.howtoforge.com/tutorial/libreswan-based-ipsec-vpn-using-preshared-and-rsa-keys/

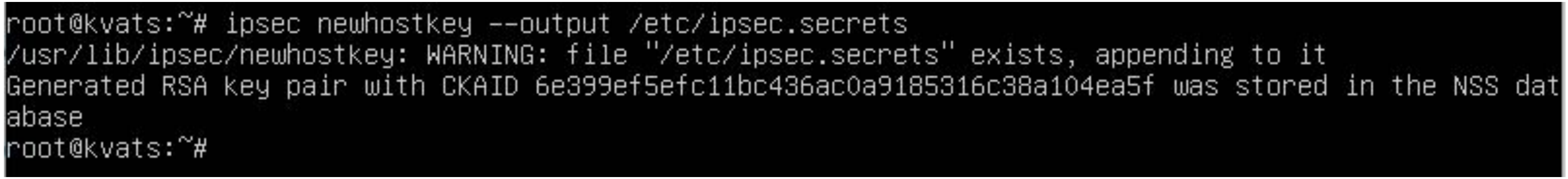
[2]
https://linoxide.com/ubuntu-how-to/configure-ipsec-vpn-libreswan/



```
Processing triggers for libc-bin (2.27-3ubuntu1) ...
kvats@kvats:~$ ipsec initnss
Initializing NSS database

certutil: function failed: SEC_ERROR_BAD_DATABASE: security libra
Failed to initialize nss database sql:/var/lib/ipsec/nss
kvats@kvats:~$ sudo ipsec initnss
Initializing NSS database

kvats@kvats:~$ sudo su
root@kvats:/home/kvats# ls
copy_encrypted  encrypted  iv2.txt  kaustav-sushant.1.txt  key2.t
decrypted       iv1.txt    iv3.txt  key1.txt               key3.t
root@kvats:/home/kvats# cd ~
root@kvats:~# ls
root@kvats:~# ipsec setup start
warning: could not open include filename: '/etc/ipsec.d/*.conf'
warning: could not open include filename: '/etc/ipsec.d/*.conf'
Redirecting to: systemctl start ipsec.service
root@kvats:~# ipsec status
000 using kernel interface: netkey
000 interface lo/lo ::1@500
000 interface lo/lo 127.0.0.1@4500
```



```
root@kvats:~# ipsec newhostkey --output /etc/ipsec.secrets
/usr/lib/ipsec/newhostkey: WARNING: file "/etc/ipsec.secrets" exists, appending to it
Generated RSA key pair with CKAID 6e399ef5efc11bc436ac0a9185316c38a104ea5f was stored in the NSS dat
abase
root@kvats:~#
```

Configuration of LibreSwarn [1]

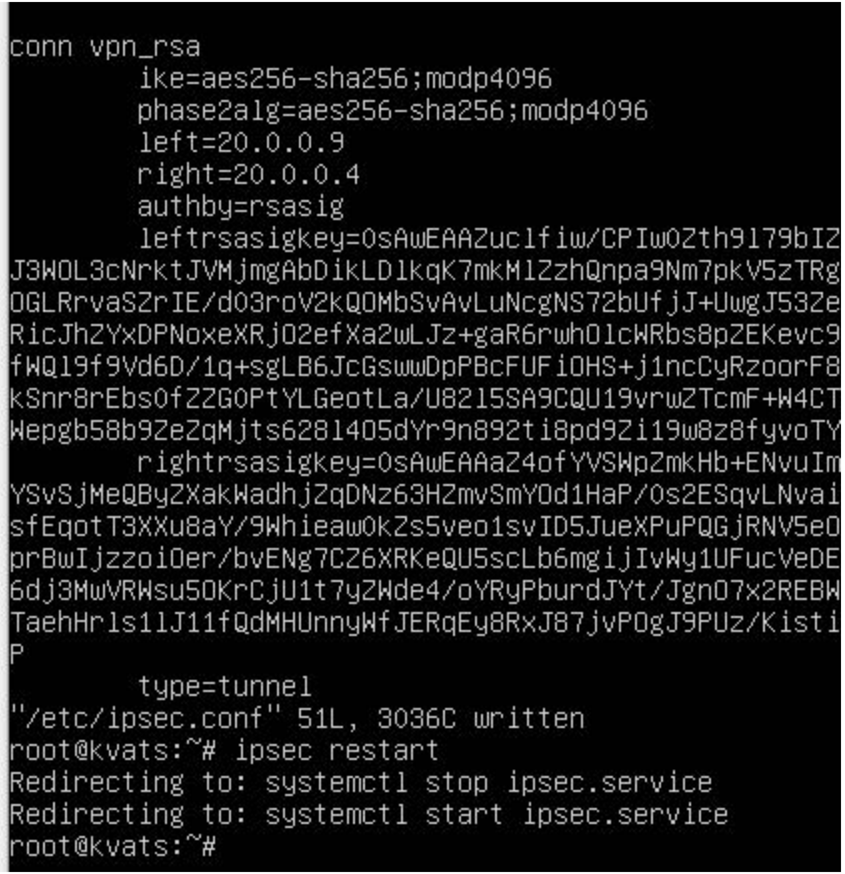
After installing LibreSwarn we initialized ipsec database.

Initnss initialize the database to store private RSA keys and Certificate keypairs.

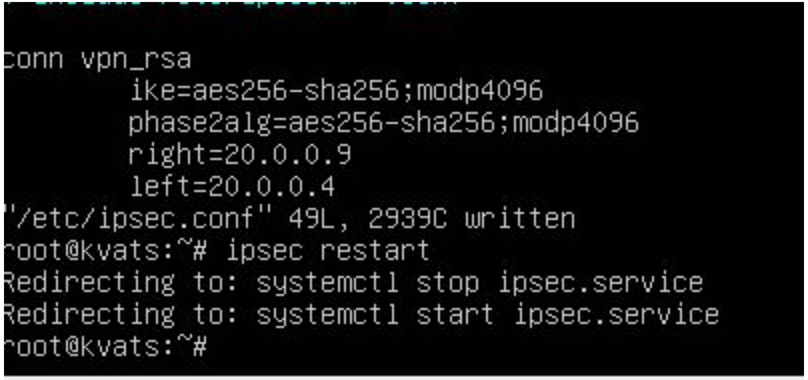
Here we started IPsec Service.

In last image, we created our public private key pairs and stored public key in /etc/ipsec.secrets

Above steps were done for both VM2 and VM3



```
conn vpn_rsa
        ike=aes256-sha256;modp4096
        phase2alg=aes256-sha256;modp4096
        left=20.0.0.9
        right=20.0.0.4
        authby=rsasig
        leftrsasigkey=0sAwEAAZuclfiw/CPIw0Zth9l79bIZ
J3WOL3cNrktJVMjmgAbDikLDlkqK7mkMlZzhQnpa9Nm7pkV5zTRg
OGLRrvaSZrIE/d03roV2kQOMbSvAvLuNcgNS72bUfjJ+UwgJ53Ze
RicJhZYxDPNoxeXRjO2efXa2wLJz+gaR6rwhOlcWRbs8pZEKevc9
fWQl9f9Vd6D/1q+sgLB6JcGswwDpPBcFUFiOHS+j1ncCyRzoorF8
kSnr8rEbs0fZZGOPtYLGeotLa/U82l5SA9CQU19vrwZTcmF+W4CT
Wepgb58b9ZeZqMjts628l405dYr9n892ti8pd9Zi19w8z8fyvoTY
        rightrsasigkey=0sAwEAAaZ4ofYVSWpZmkHb+ENvuIm
YSvSjMeQByZXakWadhjZqDNz63HZmvSmYOd1HaP/0s2ESqvLNvai
sfEqotT3XXu8aY/9Whieaw0kZs5veo1svID5JueXPuPQGjRNV5eO
prBwIjzzoiOer/bvENg7CZ6XRKeQU5scLb6mgijIvWy1UFucVeDE
6dj3MwVRWsu5OKrCjU1t7yZWde4/oYRyPburdJYt/JgnO7x2REBW
TaehHrls1lJ11fQdMHUnnyWfJERqEy8RxJ87jvPOgJ9PUz/Kisti
P
        type=tunnel
"/etc/ipsec.conf" 51L, 3036C written
root@kvats:~# ipsec restart
Redirecting to: systemctl stop ipsec.service
Redirecting to: systemctl start ipsec.service
root@kvats:~#
```



```
conn vpn_rsa
        ike=aes256-sha256;modp4096
        phase2alg=aes256-sha256;modp4096
        right=20.0.0.9
        left=20.0.0.4
"/etc/ipsec.conf" 49L, 2939C written
oot@kvats:~# ipsec restart
Redirecting to: systemctl stop ipsec.service
Redirecting to: systemctl start ipsec.service
oot@kvats:~#
```

Configuration of LibreSwarn [2] and Packet Transfer

Here we configured VM2 and VM3 to enable IKE tunneling and providing encryption

Configuration file - /etc/ipsec.conf

We set IKE to AES256-SHA256
We set the tunneling configuration of the VM
Left is the VM2 and Right is the VM3 (vica versa for configuration in VM3)

Here we added public keys of both parties. These public keys were generated at their respective VM’s. These public keys were transferred to between VM2 and VM3 using netcat. Then we observed that packets were encrypted in the tunnel.