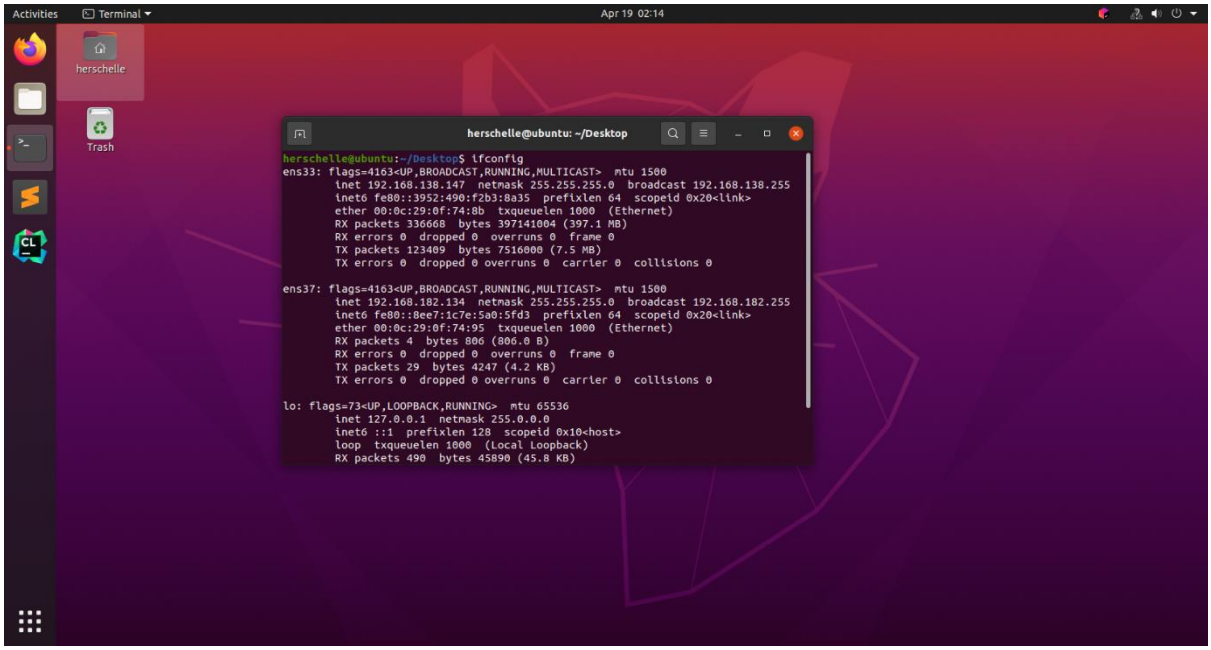
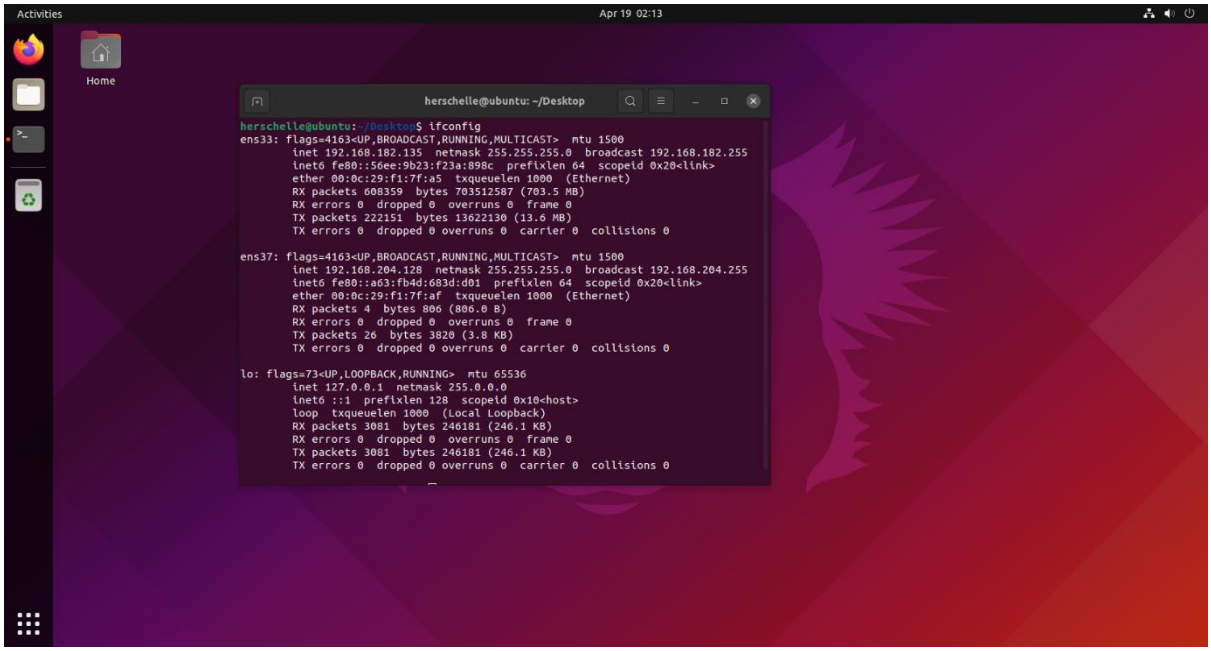
IP of VM2: 192.168.182.134

IP of VM3: 192.168.182.135

VM2:-



VM3:-



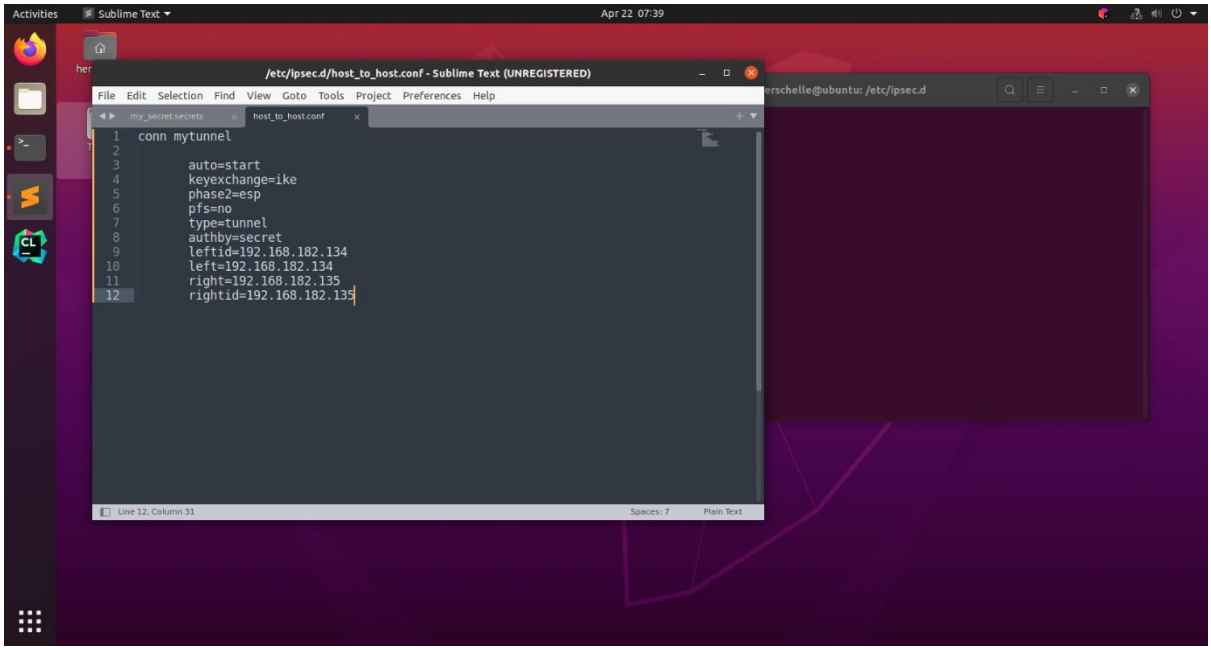
On VM2 and VM3 do the following:

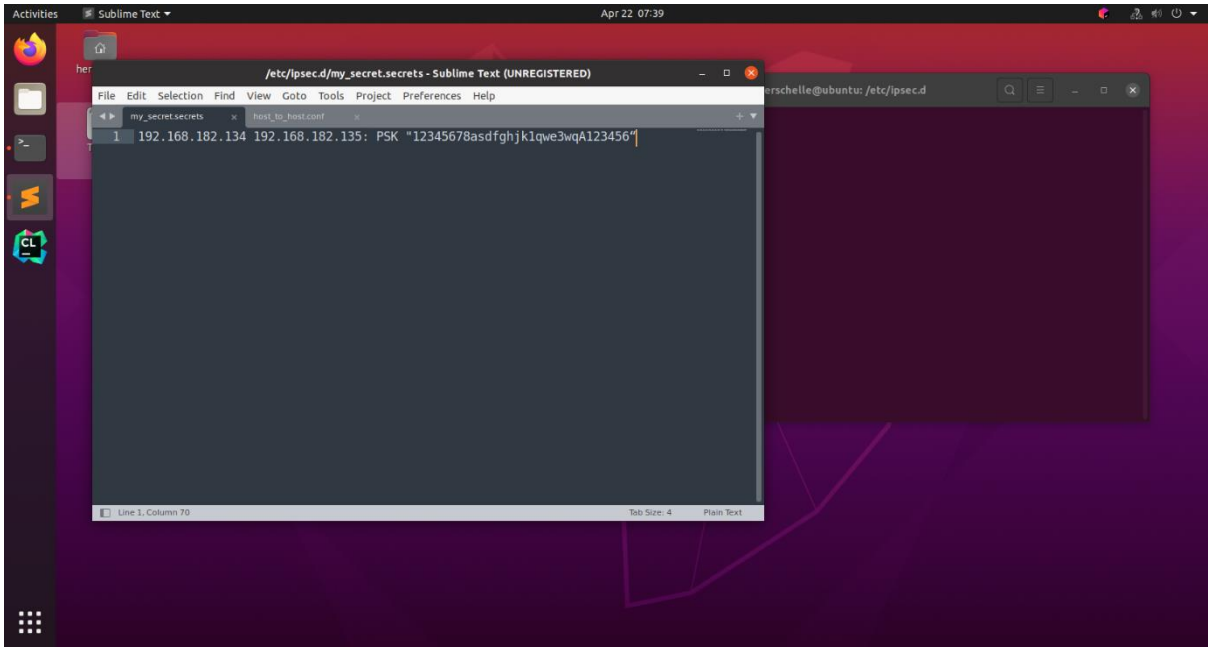
apt-get install libreswan

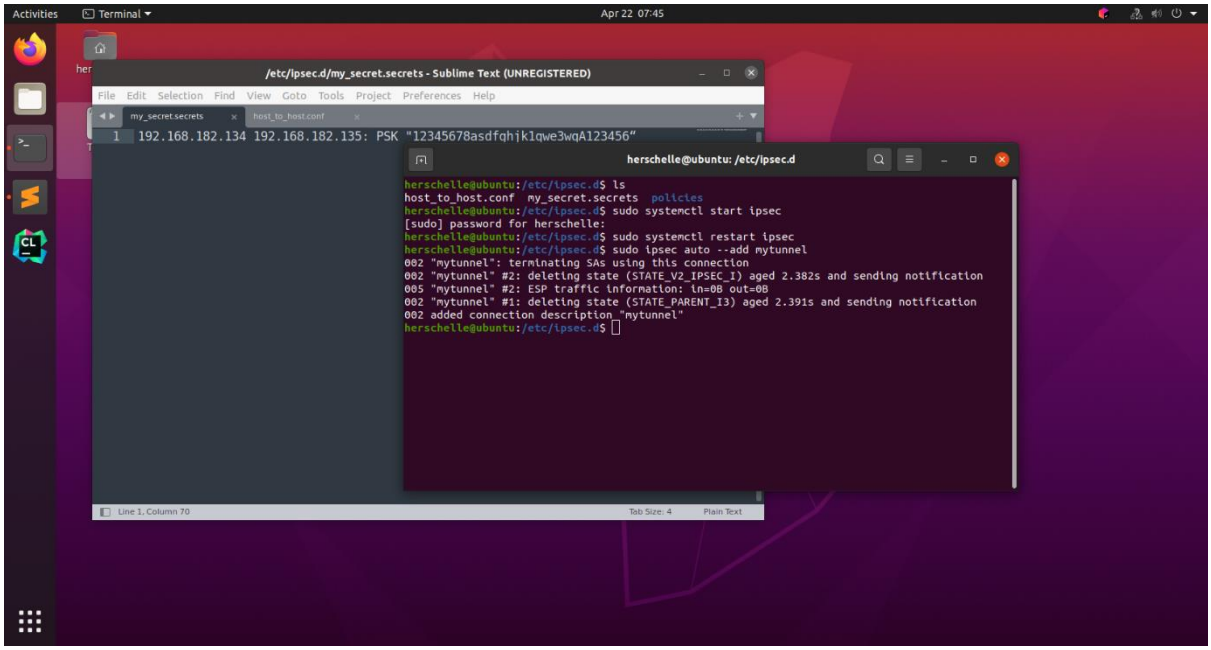
systemctl enable ipsec

ipsec initnss

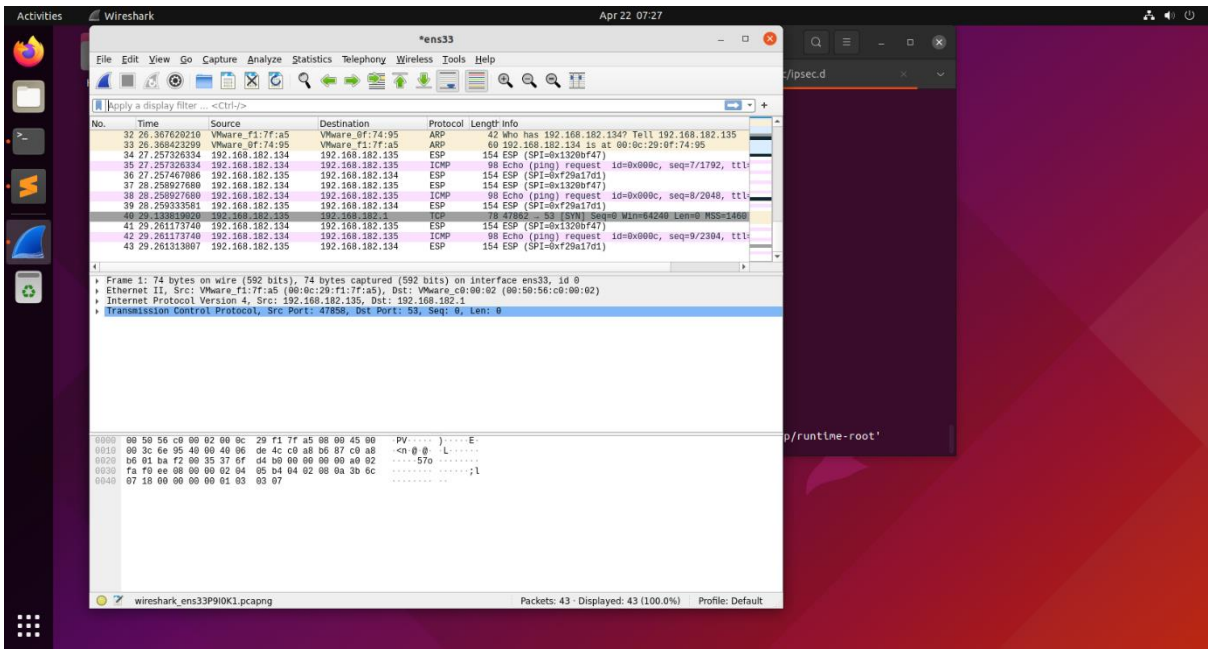
In /etc/ipsec.d/ directory add the following files with following data


Activities
Sublime Text
Apr 22 07:39
/etc/ipsec.d/host_to_host.conf - Sublime Text (UNREGISTERED)
File Edit Selection Find View Goto Tools Project Preferences Help
my_secret.secrets
host_to_host.conf
conn mytunnel
auto=start
keyexchange=ike
phase2=esp
pfs=no
type=tunnel
authby=secret
leftid=192.168.182.134
left=192.168.182.134
right=192.168.182.135
rightid=192.168.182.135
Line 12, Column 31
Spaces: 7
Plain Text
erschelle@ubuntu: /etc/ipsec.d


Activities
Sublime Text
Apr 22 07:39
/etc/ipsec.d/my_secret.secrets - Sublime Text (UNREGISTERED)
File Edit Selection Find View Goto Tools Project Preferences Help
my_secret.secrets
host_to_host.conf
192.168.182.134 192.168.182.135: PSK "12345678asdfghjk1qwe3wqA123456"
Line 1, Column 70
Tab Size: 4
Plain Text
erschelle@ubuntu: /etc/ipsec.d



Ping from VM2 and fire up wireshark on VM3 and we can see esp packets.



Wireshark/Tcpdump acts weirdly with IPsec, it decrypts the incoming packet which can see in the screenshot above. The same is written at the end of the below link.

https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/6/html/security_guide/sec-host-to-host_vpn_using_libreswan

To verify that packets are being sent via the VPN tunnel, issue a command as `root` in the following format:

```
~]# tcpdump -n -i interface esp or udp port 500 or udp port 4500
00:32:32.632165 IP 192.1.2.45 > 192.1.2.23: ESP(spi=0x63ad7e17,seq=0x1a), length 132
00:32:32.632592 IP 192.1.2.23 > 192.1.2.45: ESP(spi=0x4841b647,seq=0x1a), length 132
00:32:32.632592 IP 192.0.2.254 > 192.0.1.254: ICMP echo reply, id 2489, seq 7, length 64
00:32:33.632221 IP 192.1.2.45 > 192.1.2.23: ESP(spi=0x63ad7e17,seq=0x1b), length 132
00:32:33.632731 IP 192.1.2.23 > 192.1.2.45: ESP(spi=0x4841b647,seq=0x1b), length 132
00:32:33.632731 IP 192.0.2.254 > 192.0.1.254: ICMP echo reply, id 2489, seq 8, length 64
00:32:34.632183 IP 192.1.2.45 > 192.1.2.23: ESP(spi=0x63ad7e17,seq=0x1c), length 132
00:32:34.632607 IP 192.1.2.23 > 192.1.2.45: ESP(spi=0x4841b647,seq=0x1c), length 132
00:32:34.632607 IP 192.0.2.254 > 192.0.1.254: ICMP echo reply, id 2489, seq 9, length 64
00:32:35.632233 IP 192.1.2.45 > 192.1.2.23: ESP(spi=0x63ad7e17,seq=0x1d), length 132
00:32:35.632685 IP 192.1.2.23 > 192.1.2.45: ESP(spi=0x4841b647,seq=0x1d), length 132
00:32:35.632685 IP 192.0.2.254 > 192.0.1.254: ICMP echo reply, id 2489, seq 10, length 64
```

Where *interface* is the interface known to carry the traffic. To end the capture with **tcpdump**, press `Ctrl` + `C` .

Note

The **tcpdump** commands interacts a little unexpectedly with `IPsec` . It only sees the outgoing encrypted packet, not the outgoing plaintext packet. It does see the encrypted incoming packet, as well as the decrypted incoming packet. If possible, run **tcpdump** on a router between the two machines and not on one of the endpoints itself.