Site-To-Site IPSec VPN & BGP over GRE with Ubuntu v18.08 & StrongSwan v5.6.2 IKEv2 & Frrouting v6.0.2.2

On STC OpenStack Cloud

Taher A. Bahashwan

Cloud Advisory Expert

STC Solution

@taher9990

Oct 2019

Contents

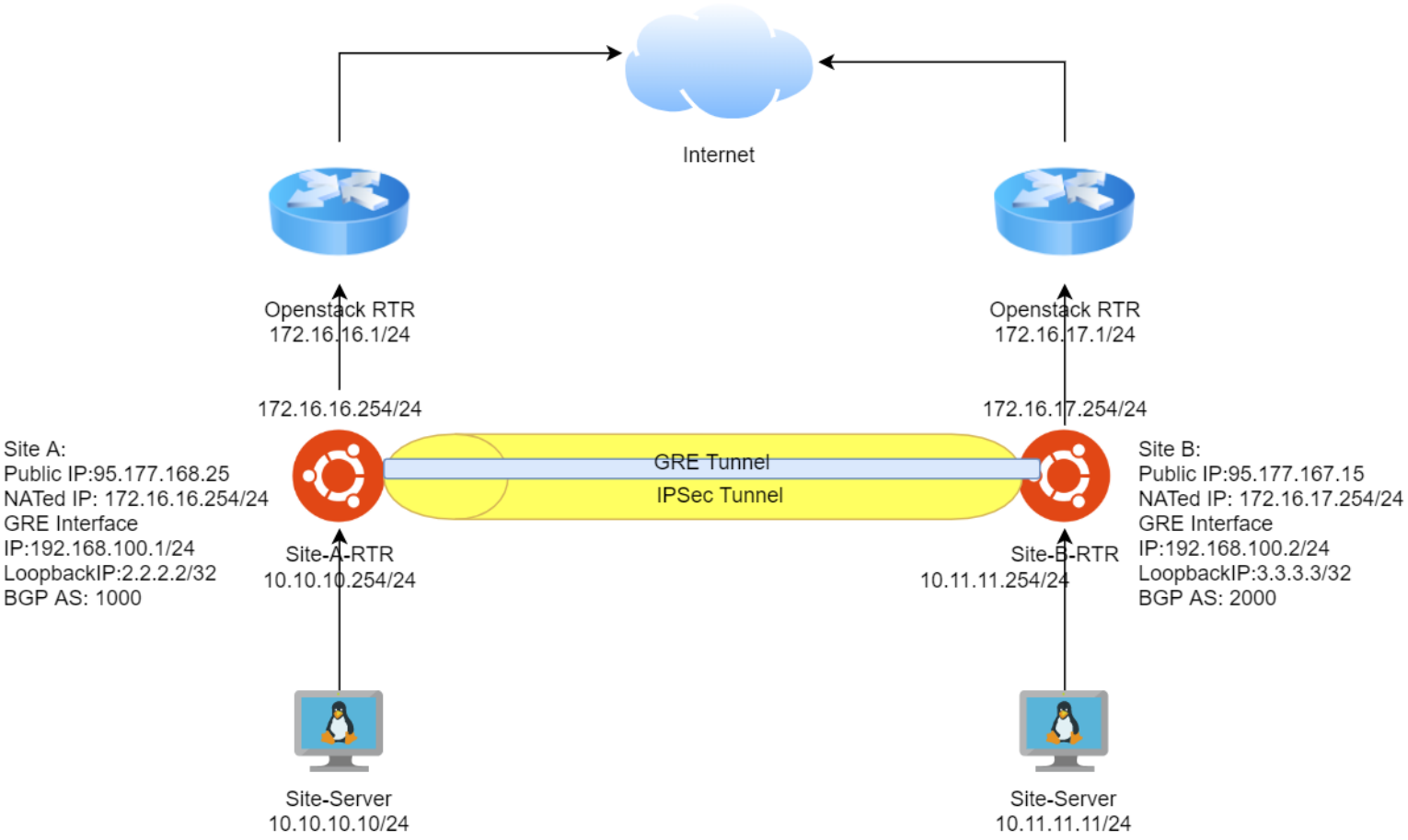
Disclaimer

This article is made for educational and testing purposes, and you might find few settings that are not made for production, please do your full testing and follow your organizations best practices and standards along with the steps and guides in this document to get a full complete working solution.

WARNING --- IPs Misuse

All Public IPs that we use in this article are randomly selected from STC Public Cloud, and they will be deleted from our Cloud tenant after we complete the test, so you are not allowed to use or conduct any activity in to these IPs, if activity identified it will be considered as criminal activity, STC Cloud personnel have the right to take legal actions against you or your organization.

Network Topology



Successful Tunnel Status

Test7-Site-A-RTR

```
root@test7-site-a-rtr:/home/ubuntu# ipsec status Site-A-To-Site-B
Security Associations (1 up, 0 connecting):
Site-A-To-Site-B[4]: ESTABLISHED 109 seconds ago, 172.16.16.254[95.177.168.25]...95.177.167.15[95.177.167.15]
Site-A-To-Site-B{3}:  INSTALLED, TUNNEL, reqid 3, ESP in UDP SPIs: c9f69f10_i c71cca69_o
Site-A-To-Site-B{3}:   172.16.16.0/24 === 172.16.17.0/24
root@test7-site-a-rtr:/home/ubuntu# ping 10.11.11.11
PING 10.11.11.11 (10.11.11.11) 56(84) bytes of data.
64 bytes from 10.11.11.11: icmp_seq=1 ttl=63 time=1.72 ms
64 bytes from 10.11.11.11: icmp_seq=2 ttl=63 time=1.00 ms
^C
--- 10.11.11.11 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 1.002/1.362/1.722/0.360 ms
root@test7-site-a-rtr:/home/ubuntu#
```

```
root@test7-site-b-rtr:/home/ubuntu# ipsec status Site-B-To-Site-A
Security Associations (1 up, 0 connecting):
Site-B-To-Site-A[1]: ESTABLISHED 113 seconds ago, 172.16.17.254[95.177.167.15]...95.177.168.25[95.177.168.25]
Site-B-To-Site-A{1}:  INSTALLED, TUNNEL, reqid 1, ESP in UDP SPIs: c71cca69_i c9f69f10_o
Site-B-To-Site-A{1}:   172.16.17.0/24 === 172.16.16.0/24
root@test7-site-b-rtr:/home/ubuntu# ping 10.10.10.10
PING 10.10.10.10 (10.10.10.10) 56(84) bytes of data.
64 bytes from 10.10.10.10: icmp_seq=1 ttl=63 time=1.87 ms
64 bytes from 10.10.10.10: icmp_seq=2 ttl=63 time=0.795 ms
^C
--- 10.10.10.10 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 0.795/1.336/1.877/0.541 ms
root@test7-site-b-rtr:/home/ubuntu#
```

Test7-Site-B-RTR

Routes status from Frr

Test7-Site-A-RTR

```
test7-site-a-rtr# show ip route
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, E - EIGRP, N - NHRP,
       T - Table, v - VNC, V - VNC-Direct, A - Babel, D - SHARP,
       F - PBR,
       > - selected route, * - FIB route

S>* 0.0.0.0/0 [1/0] is directly connected, ens3, 00:28:34
C>* 2.2.2.2/32 is directly connected, lo1, 00:35:37
B>* 3.3.3.3/32 [20/0] via 192.168.100.2, gre, 00:03:12
C>* 10.10.10.0/24 is directly connected, ens4, 00:35:37
B>* 10.11.11.0/24 [20/0] via 192.168.100.2, gre, 00:03:12
C>* 172.16.16.0/24 is directly connected, ens3, 00:35:37
C>* 192.168.100.0/24 is directly connected, gre, 00:35:37
test7-site-a-rtr#
```

```
test7-site-b-rtr# show ip route
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, E - EIGRP, N - NHRP,
       T - Table, v - VNC, V - VNC-Direct, A - Babel, D - SHARP,
       F - PBR,
       > - selected route, * - FIB route

S   0.0.0.0/0 [1/0] is directly connected, ens3, 00:03:24
K>* 0.0.0.0/0 [0/100] via 172.16.17.1, ens3, 00:03:25
K * 0.0.0.0/0 [0/101] via 10.11.11.254, ens4, 00:03:25
B>* 2.2.2.2/32 [20/0] via 192.168.100.1, gre, 00:03:17
C>* 3.3.3.3/32 is directly connected, lo1, 00:03:25
B>* 10.10.10.0/24 [20/0] via 192.168.100.1, gre, 00:03:17
C>* 10.11.11.0/24 is directly connected, ens4, 00:03:25
C>* 172.16.17.0/24 is directly connected, ens3, 00:03:25
C>* 192.168.100.0/24 is directly connected, gre, 00:03:25
test7-site-b-rtr#
```

Setup and Prepare Ubuntu Servers

Server Specs

```
CPU: 2 Memory: 4 GB, HDD: 30 GB
          Icon name: computer-vm
            Chassis: vm
     Virtualization: kvm
   Operating System: Ubuntu 18.04.3 LTS
             Kernel: Linux 5.0.0-31-generic
       Architecture: x86-64
```

Below is a screenshot for the servers hosted in STC Public Cloud

Instance Name	IP Address	Flavor	Key Pair	Status	Availability Zone	Task	Power State	Time since created	Actions
Cirros-Client-TEST7-Site-B	10.11.11.11	R1-Generic-1	taher	Active	zone-1	None	Running	1 hour, 7 minutes	Console
TEST7-Site-B-RTR	TEST7-Site-B-Internet-NW 172.16.17.254 Floating IPs: 95.177.167.15 TEST7-Site-B-NW 10.11.11.254	R1-Generic-2	taher	Active	zone-1	None	Running	1 hour, 7 minutes	Console
Cirros-Client-TEST7-Site-A	10.10.10.10	R1-Generic-1	taher	Active	zone-1	None	Running	1 hour, 8 minutes	Console
TEST7-Site-A-RTR	TEST7-Site-A-NW 10.10.10.254 TEST7-Site-A-Internet-NW 172.16.16.254 Floating IPs: 95.177.168.25	R1-Generic-2	taher	Active	zone-1	None	Running	1 hour, 9 minutes	Console

Configurations here applied to both Servers in both sites

Site-A-Network IPs:

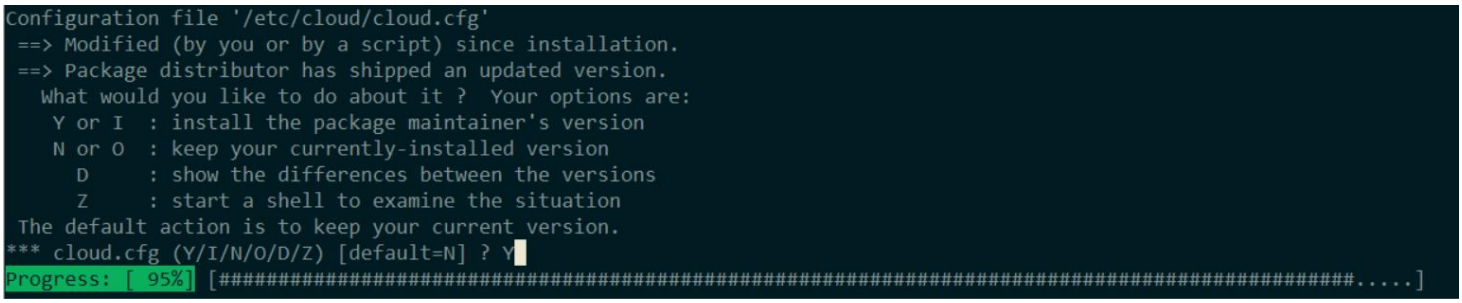
Public IP:95.177.168.25
NATed IP: 172.16.16.254/24
GRE Interface IP:192.168.100.1/24
LoopbackIP:2.2.2.2/32
BGP AS: 1000

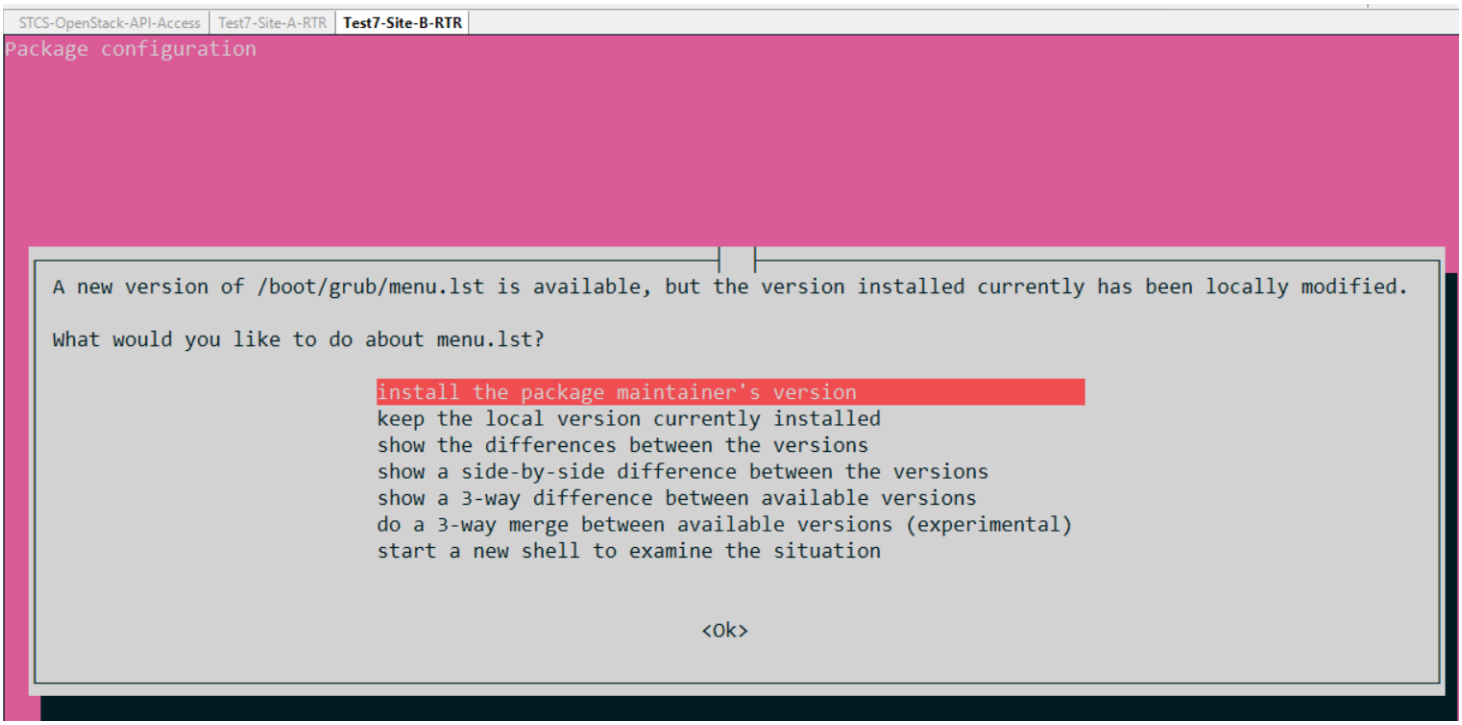
Site-B-Network IPs:

Public IP:95.177.167.15
NATed IP: 172.16.17.254/24
GRE Interface IP:192.168.100.2/24
LoopbackIP:3.3.3.3/32
BGP AS: 2000

```
timedatectl set-timezone Asia/Riyadh
passwd root
passwd ubuntu
apt update && sudo apt upgrade -y
```

When start the update you will get below screenshots you would need to choose yes as explained:






```
apt install -y traceroute && apt install -y network-manager &&
apt install -y firewalld
sudo apt install strongswan -y
sudo apt-get install -y --install-recommends linux-generic-hwe-
18.04

cat >> /etc/ssh/sshd_config << EOF
PubkeyAuthentication yes
AuthenticationMethods publickey password
AuthorizedKeysFile      .ssh/authorized_keys
PermitRootLogin yes
PasswordAuthentication yes
PermitEmptyPasswords no
ChallengeResponseAuthentication no
UsePAM yes
EOF


If you want to access your servers with root user directly you
can Remove anything before these words "ssh-rsa":
vi /root/.ssh/authorized_keys
```

Note: It is not recommended to access the server with root, we do it here only for test and demo purposes

```
cat >> /etc/sysctl.conf << EOF
net.ipv4.ip_forward = 1
net.ipv4.conf.all.accept_redirects = 0
net.ipv4.conf.all.send_redirects = 0
EOF

sysctl -p

service sshd restart
```

Let us now update GRUB and do the reboot so we can get the updated kernel

```
update-grub & reboot
```

Diabling & Masking IPTables on both sites routes:

We are going to use Firewalld so it is mandatory to stop and maks IPTables

```
sudo su
sudo systemctl stop iptables && sudo systemctl mask iptables &&
sudo systemctl status iptables && sudo apt-get remove ufw
```

Make sure that Friewalld is running:

```
sudo systemctl start firewalld
sudo systemctl enable firewalld
sudo systemctl status firewalld
```

Setup Network Configurations

Adding Loopback Interfaces Permanently

Then to make these interfaces persistence creates below files

Loopback-Site-A

```
cat >> /etc/systemd/network/10-lo1.netdev<<EOF
[NetDev]
Name=lo1
Kind=dummy
EOF

cat >> /etc/systemd/network/20-lo1.network<<EOF
[Match]
Name=lo1

[Network]
Address=2.2.2.2/32
EOF

sudo netplan --debug apply
```

Loopback-Site-B

```
cat >> /etc/systemd/network/10-lo1.netdev<<EOF
[NetDev]
Name=lo1
Kind=dummy
EOF

cat >> /etc/systemd/network/20-lo1.network<<EOF
[Match]
Name=lo1

[Network]
Address=3.3.3.3/32
EOF


sudo netplan --debug apply
```

Add GRE Interfaces & Configurations

Site-A-GRE-Tunnel-Configuration

```
nmcli connection add type ip-tunnel ifname gre mode gre remote
172.16.17.254 local 172.16.16.254 ip4 192.168.100.1/24  con-name
"GRE-TEST"
nmcli connection up GRE-TEST
```

Site-B-GRE-Tunnel-Configuration

```
nmcli connection add type ip-tunnel ifname gre mode gre remote
172.16.16.254 local 172.16.17.254 ip4 192.168.100.2/24  con-name
"GRE-TEST"
nmcli connection up GRE-TEST
```

NAT Internal Networks to Internet

Site-A

Configure the NAT for Networks 10.10.10.0/24 to be able to reach to Internet

```
firewall-cmd --permanent --direct --passthrough ipv4 -t nat -I
POSTROUTING -o ens3 -j MASQUERADE -s 10.10.10.0/24
```

Site-B

Configure the NAT for Networks 10.11.11.0/24 to be able to reach to Internet

```
firewall-cmd --permanent --direct --passthrough ipv4 -t nat -I
POSTROUTING -o ens3 -j MASQUERADE -s 10.11.11.0/24
```

```
sysctl -p /etc/sysctl.conf
```

Setup & Install Frrouting on both Sites

```
udo apt upgrade --fix-missing && sudo apt --fix-broken install
wget http://archive.ubuntu.com/ubuntu/pool/main/c/c-ares/libc-
ares2_1.14.0-1_amd64.deb
```

```
wget http://ftp.br.debian.org/debian/pool/main/f/frr/frr_6.0.2-2_amd64.deb
sudo dpkg -i libc-ares2_1.14.0-1_amd64.deb
sudo dpkg -i frr_6.0.2-2_amd64.deb
sudo apt-get update
```

Or you can install it with below commands from the downloaded packages:

```
sudo apt-get install -f /home/ubuntu/libc-ares2_1.14.0-1_amd64.deb -y
sudo apt-get install -f /home/ubuntu/frr_6.0.2-2_amd64.deb -y
apt --fix-broken install
```

Change permissions for Frrouting to have full access

```
chmod 777 /etc/frr/
```

Enable BGP

```
vi /etc/frr/daemons
bgpd=yes
```

Below is the example of that

```
# This file tells the frr package which daemons to start.
#
# Sample configurations for these daemons can be found in
# /usr/share/doc/frr/examples/.
#
# ATTENTION:
#
# When activation a daemon at the first time, a config file, even if it is
# empty, has to be present *and* be owned by the user and group "frr", else
# the daemon will not be started by /etc/init.d/frr. The permissions should
# be u=rw,g=r,o=.
# When using "vtysh" such a config file is also needed. It should be owned by
# group "frrvty" and set to ug=rw,o= though. Check /etc/pam.d/frr, too.
#
# The watchfrr and zebra daemons are always started.
#
bgpd=yes
ospfd=no
ospf6d=no
ripd=no
ripngd=no
isisd=no
pimd=no
ldpd=no
nhrpd=no
eigrpd=no
babeld=no
sharpd=no
pbrd=no
bfdd=no

#
# If this option is set the /etc/init.d/frr script automatically loads
-- INSERT --
```

Restart Frrouting

```
sudo systemctl stop frr
sudo systemctl start frr
sudo systemctl enable frr

sudo systemctl status frr
```

Below is the success example of Frrouting status

```
root@test7-site-a-rtr:/home/ubuntu# sudo systemctl status frr
● frr.service - FRRouting
   Loaded: loaded (/lib/systemd/system/frr.service; enabled; vendor preset: enabled)
   Active: active (running) since Thu 2019-10-10 02:48:15 +03; 6s ago
     Docs: https://frrouting.readthedocs.io/en/latest/setup.html
    Tasks: 9 (limit: 4648)
   CGroup: /system.slice/frr.service
           ├─2827 /usr/lib/frr/watchfrr -d zebra bgpd staticd
           ├─2846 /usr/lib/frr/zebra -d -A 127.0.0.1 -s 90000000
           ├─2850 /usr/lib/frr/bgpd -d -A 127.0.0.1
           └─2857 /usr/lib/frr/staticd -d -A 127.0.0.1

Oct 10 02:48:14 test7-site-a-rtr watchfrr.sh[2838]: Cannot stop staticd: pid file not found
Oct 10 02:48:15 test7-site-a-rtr zebra[2846]: client 14 says hello and bids fair to announce only bgp routes vrf=0
Oct 10 02:48:15 test7-site-a-rtr zebra[2846]: client 20 says hello and bids fair to announce only vnc routes vrf=0
Oct 10 02:48:15 test7-site-a-rtr zebra[2846]: client 27 says hello and bids fair to announce only static routes vrf=0
Oct 10 02:48:15 test7-site-a-rtr watchfrr[2827]: zebra state -> up : connect succeeded
Oct 10 02:48:15 test7-site-a-rtr watchfrr[2827]: bgpd state -> up : connect succeeded
Oct 10 02:48:15 test7-site-a-rtr frrinit.sh[2805]:  * Started watchfrr
Oct 10 02:48:15 test7-site-a-rtr watchfrr[2827]: staticd state -> up : connect succeeded
Oct 10 02:48:15 test7-site-a-rtr watchfrr[2827]: all daemons up, doing startup-complete notify
Oct 10 02:48:15 test7-site-a-rtr systemd[1]: Started FRRouting.
```

Install & Configure Network Manager on both Sites

```
sudo apt-get install -y network-manager
systemctl start network-manager
systemctl enable network-manager
```

Making Network Manager as the default rerender for the network interfaces:
By adding the highlighted line below underneath `version: 2`

```
vi /etc/netplan/50-cloud-init.yaml
    version: 2
    renderer: NetworkManager
```

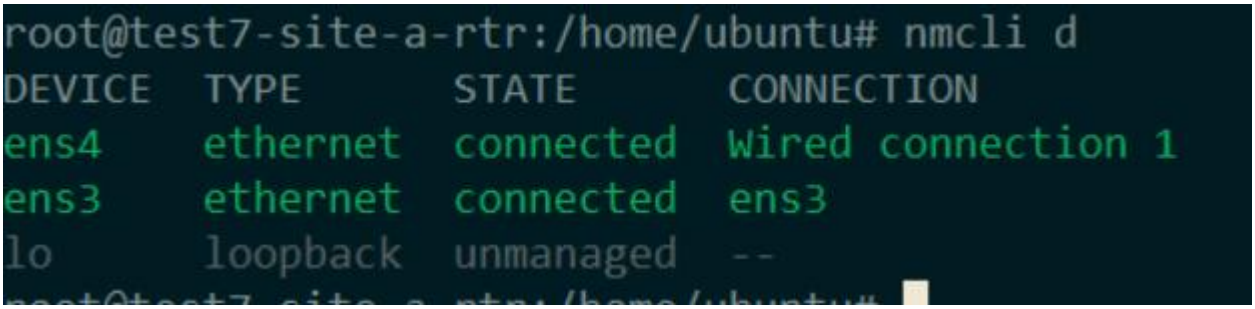
```
sudo  systemctl restart NetworkManager.service
sudo netplan --debug apply
```

Then append below line under `NetworkManager.conf` to avoid the network manager of setting the default routes and all the routes will be controlled by Frrouting

```
cat >> /etc/NetworkManager/NetworkManager.conf<<EOF
never-default=true
EOF
```

Then check if all interfaces are managed by Network Manager

```
nmcli d
```



Note: If any of the interfaces is not managed or not connected you can use below commands to fix that:

```
nmcli dev connect ens4
ip link set ens4 up
```

Configure Frrouting:

Site-A

```
touch /var/log/frr/frr.log
chmod 777 /var/log/frr/frr.log
cat >> /etc/frr/frr.conf<<EOF
log file /var/log/frr/frr.log  debug
debug bgp keepalives
debug bgp neighbor-events
debug bgp update-groups
debug bgp updates in
debug bgp updates out
debug bgp zebra
EOF

sudo vtysh
config term

ip route 0.0.0.0/0 ens3
no ip route 0.0.0.0/0 ens4

interface ens3
 ip address 172.16.16.254/24
!
interface ens4
 ip address 10.10.10.254/24
!
```

```
interface lo1
  ip address 2.2.2.2/32
!
router bgp 1000
bgp router-id 172.16.16.254
 neighbor 192.168.100.2 remote-as 2000
 !
 address-family ipv4 unicast
  network 2.2.2.2/32
  network 10.10.10.0/24
  redistribute nhrp
 exit-address-family
 !
 address-family ipv4 vpn
  neighbor 192.168.100.2 activate
 exit-address-family


do wr me
quit
quit
quit
```

Then you need now to flush the kernel routing table:

```
sudo ip route flush 0.0.0.0/0
```

Site-A- Before and after flushing kernel routes

```
root@test7-site-a-rtr:/home/ubuntu# ip r
default via 172.16.16.1 dev ens3 proto dhcp metric 100
default via 10.10.10.254 dev ens4 proto dhcp metric 101
10.10.10.0/24 dev ens4 proto kernel scope link src 10.10.10.254 metric 101
172.16.16.0/24 dev ens3 proto kernel scope link src 172.16.16.254 metric 100
192.168.100.0/24 dev gre proto kernel scope link src 192.168.100.1 metric 675
root@test7-site-a-rtr:/home/ubuntu# sudo ip route flush 0.0.0.0/0
root@test7-site-a-rtr:/home/ubuntu#
root@test7-site-a-rtr:/home/ubuntu# ip r
default dev ens3 proto static metric 20
10.10.10.0/24 dev ens4 proto kernel scope link src 10.10.10.254 metric 101
172.16.16.0/24 dev ens3 proto kernel scope link src 172.16.16.254 metric 100
192.168.100.0/24 dev gre proto kernel scope link src 192.168.100.1 metric 675
root@test7-site-a-rtr:/home/ubuntu#
```

Site-B

```
sudo vtysh
config term

ip route 0.0.0.0/0 ens3
no ip route 0.0.0.0/0 ens4
!
interface ens3
 ip address 172.16.17.254/24
!
interface ens4
 ip address 10.11.11.254/24
!
interface lo1
  ip address 3.3.3.3/32
!
router bgp 2000
bgp router-id 172.16.17.254
 neighbor 192.168.100.1 remote-as 1000
 !
 address-family ipv4 unicast
  network 3.3.3.3/32
  network 10.11.11.0/24
 exit-address-family
 !
 address-family ipv4 vpn
  neighbor 192.168.100.1 activate
 exit-address-family


do wr me
quit
quit
quit


sudo ip route flush 0.0.0.0/0
```

Note:

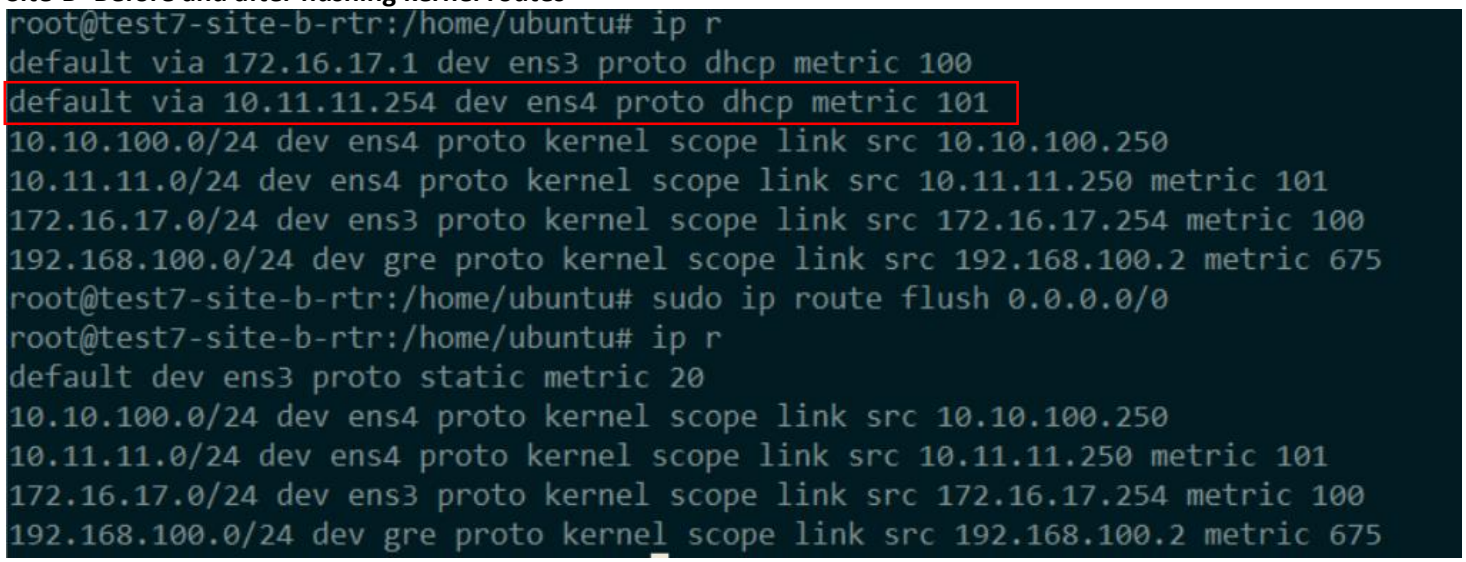
The default routes will be duplicated and therefore you would need to delete the second interface default route for the first time

```
ip route del 0.0.0.0/0 dev ens4

Then fluch the kernel routes:
sudo ip route flush 0.0.0.0/0


service frr restart
```

Site-B- Before and after flushing kernel routes



Show Ubuntu Network Configurations

Site-A BGP & Frrouting Configurations

```
root@test7-site-a-rtr:/home/ubuntu# vtysh
test7-site-a-rtr# show running-config
Building configuration...

Current configuration:
!
frr version 6.0.2
frr defaults traditional
hostname test7-site-a-rtr
```

```
log syslog informational
no ipv6 forwarding
service integrated-vtysh-config
!
ip route 0.0.0.0/0 ens3
!
interface ens3
 ip address 172.16.16.254/24
!
interface ens4
 ip address 10.10.10.254/24
!
interface lo1
 ip address 2.2.2.2/32
!
router bgp 1000
 bgp router-id 172.16.16.254
 neighbor 192.168.100.2 remote-as 2000
 !
 address-family ipv4 unicast
  network 2.2.2.2/32
  network 10.10.10.0/24
  redistribute nhrp
 exit-address-family
 !
 address-family ipv4 vpn
  neighbor 192.168.100.2 activate
 exit-address-family
!
line vty
!
end
test7-site-a-rtr# show ip route
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, E - EIGRP, N - NHRP,
       T - Table, v - VNC, V - VNC-Direct, A - Babel, D - SHARP,
       F - PBR,
       > - selected route, * - FIB route

S>* 0.0.0.0/0 [1/0] is directly connected, ens3, 01:09:35
C>* 2.2.2.2/32 is directly connected, lo1, 01:16:38
```

```
B>* 3.3.3.3/32 [20/0] via 192.168.100.2, gre, 00:44:13
C>* 10.10.10.0/24 is directly connected, ens4, 01:16:38
B>* 10.11.11.0/24 [20/0] via 192.168.100.2, gre, 00:44:13
C>* 172.16.16.0/24 is directly connected, ens3, 01:16:38
C>* 192.168.100.0/24 is directly connected, gre, 01:16:38
test7-site-a-rtr# show ip bgp summary

IPv4 Unicast Summary:
BGP router identifier 172.16.16.254, local AS number 1000 vrf-id
0
BGP table version 12
RIB entries 7, using 1120 bytes of memory
Peers 1, using 21 KiB of memory

Neighbor        V         AS MsgRcvd MsgSent   TblVer  InQ OutQ
Up/Down State/PfxRcd
192.168.100.2   4       2000      72      77        0    0    0
00:44:20            2

Total number of neighbors 1

IPv4 VPN Summary:
BGP router identifier 172.16.16.254, local AS number 1000 vrf-id
0
BGP table version 0
RIB entries 0, using 0 bytes of memory
Peers 1, using 21 KiB of memory

Neighbor        V         AS MsgRcvd MsgSent   TblVer  InQ OutQ
Up/Down State/PfxRcd
192.168.100.2   4       2000      72      77        0    0    0
00:44:20            0

Total number of neighbors 1
test7-site-a-rtr#
```

Site-A Network Configurations

```
root@test7-site-a-rtr:/home/ubuntu# cat /etc/netplan/50-cloud-
init.yaml
```

```
# This file is generated from information provided by
# the datasource.  Changes to it will not persist across an
instance.
# To disable cloud-init's network configuration capabilities,
write a file
# /etc/cloud/cloud.cfg.d/99-disable-network-config.cfg with the
following:
# network: {config: disabled}
network:
    version: 2
    renderer: NetworkManager
    ethernets:
        ens3:
            dhcp4: true
            match:
                macaddress: 02:0b:19:ec:73:de
            set-name: ens3
root@test7-site-a-rtr:/home/ubuntu#
```

Site-A ifconfig

```
root@test7-site-a-rtr:/home/ubuntu# ifconfig -a
ens3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.16.16.254  netmask 255.255.255.0  broadcast
172.16.16.255
        inet6 fe80::b:19ff:feec:73de  prefixlen 64  scopeid
0x20<link>
        ether 02:0b:19:ec:73:de  txqueuelen 1000  (Ethernet)
        RX packets 9027  bytes 2899550 (2.8 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 7485  bytes 1356356 (1.3 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions
0

ens4: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.10.10.254  netmask 255.255.255.0  broadcast
10.10.10.255
        inet6 fe80::22e:5df2:5923:572a  prefixlen 64  scopeid
0x20<link>
```

```
        ether 02:d3:48:eb:97:e4  txqueuelen 1000  (Ethernet)
        RX packets 449  bytes 19688 (19.6 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 465  bytes 21082 (21.0 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions
0

erspan0: flags=4098<BROADCAST,MULTICAST>  mtu 1450
        ether 00:00:00:00:00:00  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions
0

gre: flags=209<UP,POINTOPOINT,RUNNING,NOARP>  mtu 1476
        inet 192.168.100.1  netmask 255.255.255.0  destination
192.168.100.1
        inet6 fe80::f56b:703c:e185:39be  prefixlen 64  scopeid
0x20<link>
        unspec AC-10-10-FE-00-00-00-00-00-00-00-00-00-00-00-00-00
txqueuelen 1000  (UNSPEC)
        RX packets 122  bytes 8527 (8.5 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 211  bytes 14186 (14.1 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions
0

gre0: flags=128<NOARP>  mtu 1476
        unspec 00-00-00-00-30-30-30-3A-00-00-00-00-00-00-00-00
txqueuelen 1000  (UNSPEC)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions
0

gretap0: flags=4098<BROADCAST,MULTICAST>  mtu 1462
        ether 00:00:00:00:00:00  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
```

```
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions
0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 172  bytes 16080 (16.0 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 172  bytes 16080 (16.0 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions
0

lo1: flags=195<UP,BROADCAST,RUNNING,NOARP>  mtu 1500
        inet 2.2.2.2  netmask 255.255.255.255  broadcast 0.0.0.0
        inet6 fe80::7cb1:a4ff:feaa:ccb  prefixlen 64  scopeid
0x20<link>
        ether 7e:b1:a4:aa:0c:cb  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 10  bytes 700 (700.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions
0

root@test7-site-a-rtr:/home/ubuntu#
```

root@test7-site-a-rtr:/home/ubuntu# ls /etc/systemd/network/

```
10-lo1.netdev  20-lo1.network

root@test7-site-a-rtr:/home/ubuntu# cat /etc/systemd/network/10-
lo1.netdev

[NetDev]

Name=lo1

Kind=dummy
```

```
root@test7-site-a-rtr:/home/ubuntu# cat /etc/systemd/network/20-
lo1.network

[Match]

Name=lo1


[Network]

Address=2.2.2.2/32

root@test7-site-a-rtr:/home/ubuntu#
```

Site-B BGP & Frrouting Configurations

```
test7-site-b-rtr# show running-config
Building configuration...

Current configuration:
!
frr version 6.0.2
frr defaults traditional
hostname test7-site-b-rtr
log syslog informational
no ipv6 forwarding
service integrated-vtysh-config
!
ip route 0.0.0.0/0 ens3
!
interface ens3
 ip address 172.16.17.254/24
!
interface ens4
 ip address 10.11.11.254/24
!
interface lo1
 ip address 3.3.3.3/32
!
router bgp 2000
 bgp router-id 172.16.17.254
 neighbor 192.168.100.1 remote-as 1000
```

```
 !
 address-family ipv4 unicast
  network 3.3.3.3/32
  network 10.11.11.0/24
 exit-address-family
 !
 address-family ipv4 vpn
  neighbor 192.168.100.1 activate
 exit-address-family
!
line vty
!
end
test7-site-b-rtr# show ip route
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, E - EIGRP, N - NHRP,
       T - Table, v - VNC, V - VNC-Direct, A - Babel, D - SHARP,
       F - PBR,
       > - selected route, * - FIB route

S   0.0.0.0/0 [1/0] is directly connected, ens3, 00:46:43
K>* 0.0.0.0/0 [0/100] via 172.16.17.1, ens3, 00:46:44
K * 0.0.0.0/0 [0/101] via 10.11.11.254, ens4, 00:46:44
B>* 2.2.2.2/32 [20/0] via 192.168.100.1, gre, 00:46:36
C>* 3.3.3.3/32 is directly connected, lo1, 00:46:44
B>* 10.10.10.0/24 [20/0] via 192.168.100.1, gre, 00:46:36
C>* 10.11.11.0/24 is directly connected, ens4, 00:46:44
C>* 172.16.17.0/24 is directly connected, ens3, 00:46:44
C>* 192.168.100.0/24 is directly connected, gre, 00:46:44
test7-site-b-rtr#
test7-site-b-rtr#
test7-site-b-rtr# show ip bgp summary

IPv4 Unicast Summary:
BGP router identifier 172.16.17.254, local AS number 2000 vrf-id
0
BGP table version 4
RIB entries 7, using 1120 bytes of memory
Peers 1, using 21 KiB of memory
```

```
Neighbor        V         AS MsgRcvd MsgSent   TblVer  InQ OutQ
Up/Down State/PfxRcd
192.168.100.1   4       1000      58      54        0    0    0
00:46:42            2

Total number of neighbors 1

IPv4 VPN Summary:
BGP router identifier 172.16.17.254, local AS number 2000 vrf-id
0
BGP table version 0
RIB entries 0, using 0 bytes of memory
Peers 1, using 21 KiB of memory

Neighbor        V         AS MsgRcvd MsgSent   TblVer  InQ OutQ
Up/Down State/PfxRcd
192.168.100.1   4       1000      58      54        0    0    0
00:46:42            0

Total number of neighbors 1
test7-site-b-rtr#
```

Site-B Network Configurations

```
root@test7-site-b-rtr:/home/ubuntu# cat /etc/netplan/50-cloud-
init.yaml
# This file is generated from information provided by
# the datasource.  Changes to it will not persist across an
instance.
# To disable cloud-init's network configuration capabilities,
write a file
# /etc/cloud/cloud.cfg.d/99-disable-network-config.cfg with the
following:
# network: {config: disabled}
network:
    version: 2
    renderer: NetworkManager
    ethernets:
        ens3:
            dhcp4: true
```

```
            match:
                macaddress: 02:42:d1:27:f6:1f
            set-name: ens3
root@test7-site-b-rtr:/home/ubuntu#
```

Site-B ifconfig

```
root@test7-site-b-rtr:/home/ubuntu# ifconfig -a
ens3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.16.17.254  netmask 255.255.255.0  broadcast 172.16.17.255
        inet6 fe80::42:d1ff:fe27:f61f  prefixlen 64  scopeid 0x20<link>
        ether 02:42:d1:27:f6:1f  txqueuelen 1000  (Ethernet)
        RX packets 1449  bytes 131100 (131.1 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1216  bytes 126760 (126.7 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

ens4: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.11.11.254  netmask 255.255.255.0  broadcast 10.11.11.255
        inet6 fe80::6de7:a77:f2d5:20be  prefixlen 64  scopeid 0x20<link>
        ether 02:2c:b7:ca:3b:ca  txqueuelen 1000  (Ethernet)
        RX packets 301  bytes 13556 (13.5 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 297  bytes 13634 (13.6 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

erspan0: flags=4098<BROADCAST,MULTICAST>  mtu 1450
        ether 00:00:00:00:00:00  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

gre: flags=209<UP,POINTOPOINT,RUNNING,NOARP>  mtu 1476
        inet 192.168.100.2  netmask 255.255.255.0  destination 192.168.100.2
        inet6 fe80::3c08:7ead:b70a:da7c  prefixlen 64  scopeid 0x20<link>
        unspec AC-10-11-FE-00-00-00-00-00-00-00-00-00-00-00-00  txqueuelen 1000
(UNSPEC)
        RX packets 102  bytes 6724 (6.7 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 84  bytes 5703 (5.7 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

gre0: flags=128<NOARP>  mtu 1476
        unspec 00-00-00-00-30-30-30-3A-00-00-00-00-00-00-00-00  txqueuelen 1000
(UNSPEC)
```

```
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

gretap0: flags=4098<BROADCAST,MULTICAST>  mtu 1462
        ether 00:00:00:00:00:00  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 92  bytes 7144 (7.1 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 92  bytes 7144 (7.1 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo1: flags=195<UP,BROADCAST,RUNNING,NOARP>  mtu 1500
        inet 3.3.3.3  netmask 255.255.255.255  broadcast 0.0.0.0
        inet6 fe80::8aa:16ff:fe40:8695  prefixlen 64  scopeid 0x20<link>
        ether 0a:aa:16:40:86:95  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 10  bytes 700 (700.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

root@test7-site-b-rtr:/home/ubuntu# ls /etc/systemd/network/

```
10-lo1.netdev  20-lo1.network
root@test7-site-b-rtr:/home/ubuntu# cat /etc/systemd/network/10-lo1.netdev
[NetDev]
Name=lo1
Kind=dummy
root@test7-site-b-rtr:/home/ubuntu# cat /etc/systemd/network/20-lo1.network
[Match]
Name=lo1

[Network]
Address=3.3.3.3/32
root@test7-site-b-rtr:/home/ubuntu#
```

Note: that these interfaces (`erspan0, gre0, lo and gretap0`) are added automatically

IPSec Setup on Ubuntu 18.04

Site-A-Setup IPSec Configurations

```
cat > /etc/ipsec.secrets <<EOF
95.177.168.25 95.177.167.15 : PSK "P@ssw0rd"
EOF

cat >> /etc/ipsec.conf<<EOF
config setup
        charondebug="all"
        uniqueids=yes
        strictcrlpolicy=no

conn Site-A-To-Site-B
   #aggressive = no
   #fragmentation = yes
    keyexchange = ikev2
    authby=secret
    installpolicy = yes
    type = tunnel
    left=172.16.16.254
    right=95.177.167.15
    leftid=95.177.168.25
    rightid=95.177.167.15
    leftsubnet=172.16.16.0/24
    rightsubnet=172.16.17.0/24
    ike=aes256-sha2_256-modp1024!
    esp=aes256-sha2_256!
    forceencaps = yes
    keyingtries=0
    ikelifetime=28800s
    lifetime=3600s
    dpddelay=10s
    dpdtimeout=60s
    dpdaction=restart
    auto=start
EOF

sudo ipsec restart
```

```
sudo tail -f /var/log/syslog
```

Site-B-Setup IPSec Configurations

```
cat >> /etc/ipsec.secrets <<EOF
95.177.167.15 95.177.168.25 : PSK "P@ssw0rd"
EOF

cat > /etc/ipsec.conf<<EOF
config setup
        charondebug="all"
        uniqueids=yes
        strictcrlpolicy=no

conn Site-B-To-Site-A
    #aggressive = no
    #fragmentation = yes
    keyexchange = ikev2
    authby=secret
    installpolicy = yes
    type = tunnel
    left=172.16.17.254
    right=95.177.168.25
    leftid=95.177.167.15
    rightid=95.177.168.25
    leftsubnet=172.16.17.0/24
    rightsubnet=172.16.16.0/24
    ike=aes256-sha2_256-modp1024!
    esp=aes256-sha2_256!
    forceencaps = yes
    keyingtries=0
    ikelifetime=28800s
    lifetime=3600s
    dpddelay=10s
    dpdtimeout=60s
    dpdaction=restart
    auto=start
EOF

sudo ipsec restart
```

IPSec Show Configurations

Site-A IPsec Configurations:

```
root@test7-site-a-rtr:/home/ubuntu# cat /etc/ipsec.conf
# ipsec.conf - strongSwan IPsec configuration file

# basic configuration

config setup
        # strictcrlpolicy=yes
        # uniqueids = no

# Add connections here.

# Sample VPN connections

#conn sample-self-signed
#      leftsubnet=10.1.0.0/16
#      leftcert=selfCert.der
#      leftsendcert=never
#      right=192.168.0.2
#      rightsubnet=10.2.0.0/16
#      rightcert=peerCert.der
#      auto=start

#conn sample-with-ca-cert
#      leftsubnet=10.1.0.0/16
#      leftcert=myCert.pem
#      right=192.168.0.2
#      rightsubnet=10.2.0.0/16
#      rightid="C=CH, O=Linux strongSwan CN=peer name"
#      auto=start
config setup
        charondebug="all"
        uniqueids=yes
        strictcrlpolicy=no

conn Site-A-To-Site-B
   #aggressive = no
   #fragmentation = yes
```

```
    keyexchange = ikev2
    authby=secret
    installpolicy = yes
    type = tunnel
    left=172.16.16.254
    right=95.177.167.15
    leftid=95.177.168.25
    rightid=95.177.167.15
    leftsubnet=172.16.16.0/24
    rightsubnet=172.16.17.0/24
    ike=aes256-sha2_256-modp1024!
    esp=aes256-sha2_256!
    forceencaps = yes
    keyingtries=0
    ikelifetime=28800s
    lifetime=3600s
    dpddelay=10s
    dpdtimeout=60s
    dpdaction=restart
    auto=start
root@test7-site-a-rtr:/home/ubuntu#
```

Note: To add more subnets to the rightsubnet or left you can do it in this way

```
    leftsubnet={10.10.10.0/24,10.10.20.0/24,…}
```

```
root@test7-site-a-rtr:/home/ubuntu# cat /etc/ipsec.secrets
95.177.168.25 95.177.167.15 : PSK "P@ssw0rd"
```

Site-B IPsec Configurations:

```
root@test7-site-b-rtr:/home/ubuntu# cat /etc/ipsec.conf
config setup
        charondebug="all"
        uniqueids=yes
        strictcrlpolicy=no
```

```
conn Site-B-To-Site-A
    #aggressive = no
    #fragmentation = yes
    keyexchange = ikev2
    authby=secret
    installpolicy = yes
    type = tunnel
    left=172.16.17.254
    right=95.177.168.25
    leftid=95.177.167.15
    rightid=95.177.168.25
    leftsubnet=172.16.17.0/24
    rightsubnet=172.16.16.0/24
    ike=aes256-sha2_256-modp1024!
    esp=aes256-sha2_256!
    forceencaps = yes
    keyingtries=0
    ikelifetime=28800s
    lifetime=3600s
    dpddelay=10s
    dpdtimeout=60s
    dpdaction=restart
    auto=start
root@test7-site-b-rtr:/home/ubuntu#


root@test7-site-b-rtr:/home/ubuntu# cat /etc/ipsec.secrets
95.177.167.15 95.177.168.25 : PSK "P@ssw0rd"
```

Show and Troubleshooting Commads

ipsec status
ipsec statusall
ipsec restart
ipsec up <connection name>

tcpdump -ttttnnvvS -i any -nn icmp or esp or udp port 500 or udp port 4500

tail -f /var/log/secure

tail -f var/log/daemon.log
tail -f/var/log/auth.log
tail -f /var/log/messages

IPsec Detailed Status and Results

Site-A IPsec XFRM Policies and States

```
root@test7-site-a-rtr:/home/ubuntu# sudo ip xfrm policy
src 172.16.16.0/24 dst 172.16.17.0/24
        dir out priority 375423
        tmpl src 172.16.16.254 dst 95.177.167.15
                proto esp spi 0xc4c7afab reqid 3 mode tunnel
src 172.16.17.0/24 dst 172.16.16.0/24
        dir fwd priority 375423
        tmpl src 95.177.167.15 dst 172.16.16.254
                proto esp reqid 3 mode tunnel
src 172.16.17.0/24 dst 172.16.16.0/24
        dir in priority 375423
        tmpl src 95.177.167.15 dst 172.16.16.254
                proto esp reqid 3 mode tunnel
src 0.0.0.0/0 dst 0.0.0.0/0
        socket in priority 0
src 0.0.0.0/0 dst 0.0.0.0/0
        socket out priority 0
src 0.0.0.0/0 dst 0.0.0.0/0
        socket in priority 0
src 0.0.0.0/0 dst 0.0.0.0/0
```

```
        socket out priority 0
src ::/0 dst ::/0
        socket in priority 0
src ::/0 dst ::/0
        socket out priority 0
src ::/0 dst ::/0
        socket in priority 0
src ::/0 dst ::/0
        socket out priority 0
root@test7-site-a-rtr:/home/ubuntu#

root@test7-site-a-rtr:/home/ubuntu# sudo ip xfrm state
src 172.16.16.254 dst 95.177.167.15
        proto esp spi 0xc4c7afab reqid 3 mode tunnel
        replay-window 0 flag af-unspec
        auth-trunc hmac(sha256)
0x179fc761edf3403cf2ff53fb95b6a128d0847f992ca2704687887074df5070
fb 128
        enc cbc(aes)
0x229cff9b7d312d28ff55c3e8568bfbe4a94d31200621fb827fde45aa7f1fb9
27
        encap type espinudp sport 4500 dport 4500 addr 0.0.0.0
        anti-replay context: seq 0x0, oseq 0x12, bitmap
0x00000000
src 95.177.167.15 dst 172.16.16.254
        proto esp spi 0xcf266e43 reqid 3 mode tunnel
        replay-window 32 flag af-unspec
```

```
        auth-trunc hmac(sha256)
0x81a83929914cb4eee38e53d6a5fc8630f69057d45b7f45c2da4a1e2f083c30
77 128

        enc cbc(aes)
0x42c4e4173d4794ac4e9deaf81f870b37c7bf660e13ed0dcff7f3cc46a5d13b
91

        encap type espinudp sport 4500 dport 4500 addr 0.0.0.0

        anti-replay context: seq 0x12, oseq 0x0, bitmap
0x0003ffff

root@test7-site-a-rtr:/home/ubuntu#
```

Site-B IPsec XFRM Policies and States

```
root@test7-site-b-rtr:/home/ubuntu# sudo ip xfrm policy
src 172.16.17.0/24 dst 172.16.16.0/24
        dir out priority 375423
        tmpl src 172.16.17.254 dst 95.177.168.25
                proto esp spi 0xcf266e43 reqid 1 mode tunnel
src 172.16.16.0/24 dst 172.16.17.0/24
        dir fwd priority 375423
        tmpl src 95.177.168.25 dst 172.16.17.254
                proto esp reqid 1 mode tunnel
src 172.16.16.0/24 dst 172.16.17.0/24
        dir in priority 375423
        tmpl src 95.177.168.25 dst 172.16.17.254
                proto esp reqid 1 mode tunnel
src 0.0.0.0/0 dst 0.0.0.0/0
        socket in priority 0
src 0.0.0.0/0 dst 0.0.0.0/0
        socket out priority 0
src 0.0.0.0/0 dst 0.0.0.0/0
        socket in priority 0
src 0.0.0.0/0 dst 0.0.0.0/0
        socket out priority 0
src ::/0 dst ::/0
        socket in priority 0
src ::/0 dst ::/0
        socket out priority 0
```

```
src ::/0 dst ::/0
        socket in priority 0
src ::/0 dst ::/0
        socket out priority 0
root@test7-site-b-rtr:/home/ubuntu#



root@test7-site-b-rtr:/home/ubuntu# sudo ip xfrm state

src 172.16.17.254 dst 95.177.168.25

        proto esp spi 0xcf266e43 reqid 1 mode tunnel

        replay-window 0 flag af-unspec

        auth-trunc hmac(sha256)
0x81a83929914cb4eee38e53d6a5fc8630f69057d45b7f45c2da4a1e2f083c30
77 128

        enc cbc(aes)
0x42c4e4173d4794ac4e9deaf81f870b37c7bf660e13ed0dcff7f3cc46a5d13b
91

        encap type espinudp sport 4500 dport 4500 addr 0.0.0.0

        anti-replay context: seq 0x0, oseq 0x14, bitmap
0x00000000

src 95.177.168.25 dst 172.16.17.254

        proto esp spi 0xc4c7afab reqid 1 mode tunnel

        replay-window 32 flag af-unspec

        auth-trunc hmac(sha256)
0x179fc761edf3403cf2ff53fb95b6a128d0847f992ca2704687887074df5070
fb 128

        enc cbc(aes)
0x229cff9b7d312d28ff55c3e8568bfbe4a94d31200621fb827fde45aa7f1fb9
27

        encap type espinudp sport 4500 dport 4500 addr 0.0.0.0
```

```
        anti-replay context: seq 0x14, oseq 0x0, bitmap
0x000fffff

root@test7-site-b-rtr:/home/ubuntu#
```

Site-A IPsec status all

```
root@test7-site-a-rtr:/home/ubuntu# ipsec statusall

Status of IKE charon daemon (strongSwan 5.6.2, Linux 5.0.0-31-
generic, x86_64):

  uptime: 73 minutes, since Oct 10 03:00:56 2019

  malloc: sbrk 2560000, mmap 0, used 764144, free 1795856

  worker threads: 11 of 16 idle, 5/0/0/0 working, job queue:
0/0/0/0, scheduled: 8

  loaded plugins: charon aesni aes rc2 sha2 sha1 md4 md5 mgf1
random nonce x509 revocation constraints pubkey pkcs1 pkcs7
pkcs8 pkcs12 pgp dnskey sshkey pem openssl fips-prf gmp agent
xcbc hmac gcm attr kernel-netlink resolve socket-default
connmark stroke updown eap-mschapv2 xauth-generic counters

Listening IP addresses:

  172.16.16.254

  10.10.10.254

  2.2.2.2

  192.168.100.1

Connections:

Site-A-To-Site-B:  172.16.16.254...95.177.167.15  IKEv2,
dpddelay=10s

Site-A-To-Site-B:   local:  [95.177.168.25] uses pre-shared key
authentication

Site-A-To-Site-B:   remote: [95.177.167.15] uses pre-shared key
authentication
```

Site-A-To-Site-B: child: 172.16.16.0/24 === 172.16.17.0/24 TUNNEL, dpdaction=restart

Security Associations (1 up, 0 connecting):

Site-A-To-Site-B[4]: ESTABLISHED 53 minutes ago, 172.16.16.254[95.177.168.25]...95.177.167.15[95.177.167.15]

Site-A-To-Site-B[4]: IKEv2 SPIs: fdd16118d814d07a_i 6c2a628458b3a018_r, pre-shared key reauthentication in 6 hours*

Site-A-To-Site-B[4]: IKE proposal: AES_CBC_256/HMAC_SHA2_256_128/PRF_HMAC_SHA2_256/MODP_1024

Site-A-To-Site-B{4}: INSTALLED, TUNNEL, reqid 3, ESP in UDP SPIs: cf266e43_i c4c7afab_o

Site-A-To-Site-B{4}: AES_CBC_256/HMAC_SHA2_256_128, 1710 bytes_i (20 pkts, 50s ago), 1710 bytes_o (20 pkts, 590s ago), rekeying in 34 minutes

Site-A-To-Site-B{4}: 172.16.16.0/24 === 172.16.17.0/24

root@test7-site-a-rtr:/home/ubuntu#

Site-B IPsec status all

root@test7-site-b-rtr:/home/ubuntu# ipsec statusall

Status of IKE charon daemon (strongSwan 5.6.2, Linux 5.0.0-31-generic, x86_64):

uptime: 54 minutes, since Oct 10 03:20:31 2019

malloc: sbrk 2568192, mmap 0, used 759408, free 1808784

worker threads: 11 of 16 idle, 5/0/0/0 working, job queue: 0/0/0/0, scheduled: 5

loaded plugins: charon aesni aes rc2 sha2 sha1 md4 md5 mgf1 random nonce x509 revocation constraints pubkey pkcs1 pkcs7 pkcs8 pkcs12 pgp dnskey sshkey pem openssl fips-prf gmp agent xcbc hmac gcm attr kernel-netlink resolve socket-default connmark stroke updown eap-mschapv2 xauth-generic counters

Listening IP addresses:

172.16.17.254

10.11.11.254

3.3.3.3

192.168.100.2

Connections:

Site-B-To-Site-A: 172.16.17.254...95.177.168.25 IKEv2, dpddelay=10s

Site-B-To-Site-A: local: [95.177.167.15] uses pre-shared key authentication

Site-B-To-Site-A: remote: [95.177.168.25] uses pre-shared key authentication

Site-B-To-Site-A: child: 172.16.17.0/24 === 172.16.16.0/24 TUNNEL, dpdaction=restart

Security Associations (1 up, 0 connecting):

Site-B-To-Site-A[1]: ESTABLISHED 54 minutes ago, 172.16.17.254[95.177.167.15]...95.177.168.25[95.177.168.25]

Site-B-To-Site-A[1]: IKEv2 SPIs: fdd16118d814d07a_i 6c2a628458b3a018_r, pre-shared key reauthentication in 6 hours*

Site-B-To-Site-A[1]: IKE proposal: AES_CBC_256/HMAC_SHA2_256_128/PRF_HMAC_SHA2_256/MODP_1024

Site-B-To-Site-A{2}: INSTALLED, TUNNEL, reqid 1, ESP in UDP SPIs: c4c7afab_i cf266e43_o

Site-B-To-Site-A{2}: AES_CBC_256/HMAC_SHA2_256_128, 1881 bytes_i (22 pkts, 15s ago), 1881 bytes_o (22 pkts, 615s ago), rekeying in 35 minutes

Site-B-To-Site-A{2}: 172.16.17.0/24 === 172.16.16.0/24

root@test7-site-b-rtr:/home/ubuntu#