Full mesh secure & scalable VPN network with WireGuard v1.0.202 & Ubuntu

On STC OpenStack Cloud

Taher A. Bahashwan

Cloud Advisory Expert

STC Solution

@taher9990

Oct 2020

https://github.com/taher9990

Contents

Disclaimer

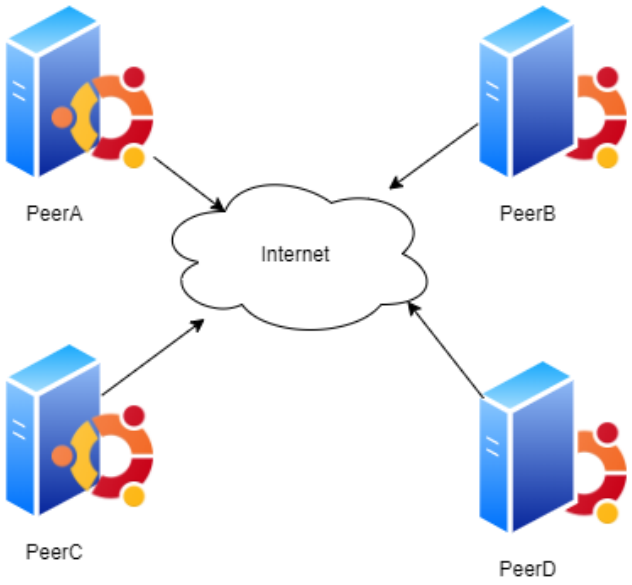
This article is made for educational and testing purposes, and you might find few settings that are not made for production, please do your full testing and follow your organizations best practices and standards along with the steps and guides in this document to get a full complete working solution.

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

Public IP: 95.177.218.228
Tunnel IP: 10.200.200.1/32
Wireguard Port: 44444



Public IP: 95.177.218.232
Tunnel IP: 10.200.200.2/32
Wireguard Port: 44444

Public IP: 95.177.218.233
Tunnel IP: 10.200.200.3/32
Wireguard Port: 44444

Public IP: 95.177.218.234
Tunnel IP: 10.200.200.4/32
Wireguard Port: 44444

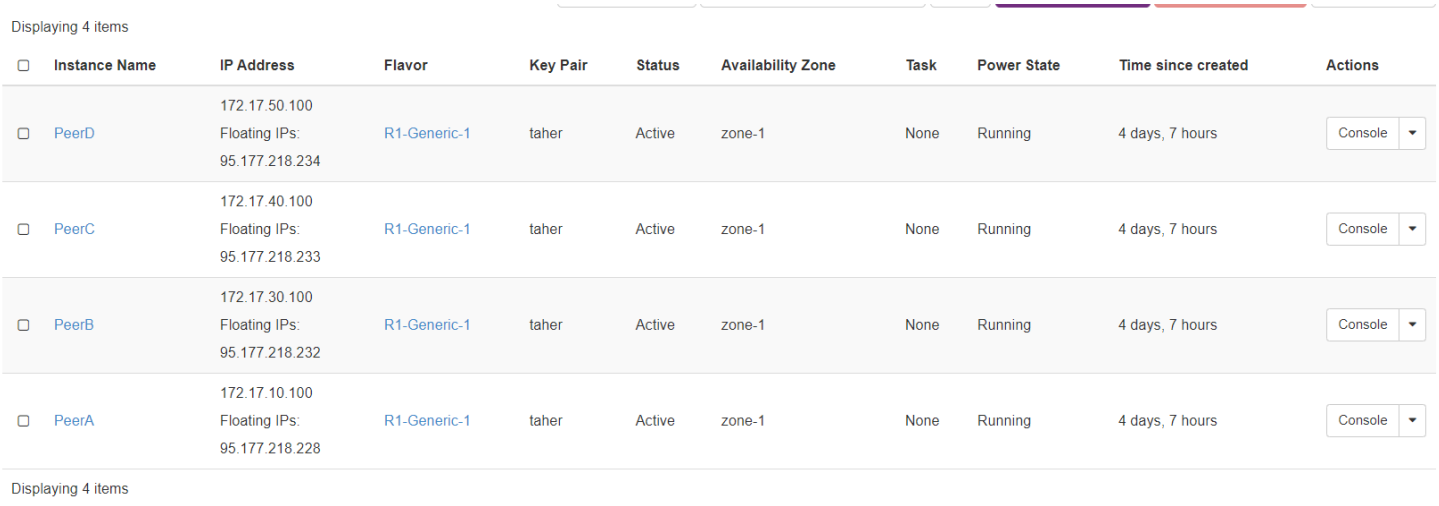
Successful Tunnel Status

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



Displaying 4 items

Instance Name	IP Address	Flavor	Key Pair	Status	Availability Zone	Task	Power State	Time since created	Actions
PeerD	172.17.50.100 Floating IPs: 95.177.218.234	R1-Generic-1	taher	Active	zone-1	None	Running	4 days, 7 hours	Console
PeerC	172.17.40.100 Floating IPs: 95.177.218.233	R1-Generic-1	taher	Active	zone-1	None	Running	4 days, 7 hours	Console
PeerB	172.17.30.100 Floating IPs: 95.177.218.232	R1-Generic-1	taher	Active	zone-1	None	Running	4 days, 7 hours	Console
PeerA	172.17.10.100 Floating IPs: 95.177.218.228	R1-Generic-1	taher	Active	zone-1	None	Running	4 days, 7 hours	Console

Displaying 4 items

Servers & Tunnel IPs

PeerANetwork IPs:

Public IP: 95.177.218.228

Tunnel IP: 10.200.200.1/32

Wireguard Port: 44444

PeerB-Network IPs:

Public IP: 95.177.218.232

Tunnel IP: 10.200.200.2/32

Wireguard Port: 44444

PeerC-Network IPs:

Public IP: 95.177.218.233

Tunnel IP: 10.200.200.3/32

Wireguard Port: 44444

PeerD-Network IPs:

Public IP: 95.177.218.234

Tunnel IP: 10.200.200.4/32

Wireguard Port: 44444

Common System configurations applied on all servers

```
sudo su –
timedatectl set-timezone Asia/Riyadh
sudo add-apt-repository ppa:wireguard/wireguard
sudo apt-get update
sudo apt-get install wireguard –y

sudo su -
hostnamectl set-hostname PeerA
systemctl restart systemd-hostnamed
 su ubuntu
sudo hostnamectl set-hostname PeerA
sudo systemctl restart systemd-hostnamed
sudo su -
```

Note: Change PeerA with the name of each server e.g PeerB

WireGuard setup

Generate Pre-shared key to use it on all servers:

```
wg genpsk > psk
```

Take this key and save it into each server

Common WireGuard configurations applied on all servers

1- Generate Private & public Key on all servers

```
umask 077; wg genkey | tee privatekey | wg pubkey > publickey
```

2- Add generated Pre shared key to all server

```
touch psk
cat >psk<<EOF
RrDNbpkGT6//9eU4eMa1cJmRaVNdnBcVc6I2oQBFvBY=
EOF
```

3- Add the generated public key only (publickey) in step 1 and save it into each server

```
touch PeerA-PublicKey
cat>PeerA-PublicKey<<EOF
oEGg3q2bx+vPgCoEFqkLzLKZC/oZdwG116/gIOZ4gxU=
EOF
touch PeerB-PublicKey
cat>PeerB-PublicKey<<EOF
zszrQrD5R1HtHkLY1ubF3dVlk7vMUP0Jud6GlaT84G4=
EOF
touch PeerC-PublicKey
cat>PeerC-PublicKey<<EOF
pmLUBZE0m0CMstOn0zea+kIv+E4EvrQcS6khYScbc0Q=
EOF
touch PeerD-PublicKey
cat>PeerD-PublicKey<<EOF
2SSJ0ADvzxhnY5Afrdij+6XJA3/SFCsBT2OgVgO0UzM=
EOF
```

4- Enable WireGuard on all servers so that it can automatically run when the server reboots

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

5- Enable routing on all servers

```
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
echo 1 > /proc/sys/net/ipv4/ip_forward
```

WireGuard Configurations for each server

Server: PeerA Configurations

```
cat >>/etc/wireguard/wg0.conf<<EOF
[Interface]
Address = 10.200.200.1/24
SaveConfig = true
ListenPort = 44444
PrivateKey = /root/privatekey

[Peer]
PublicKey = /root/PeerB-PublicKey
PresharedKey = /root/psk
AllowedIPs = 10.200.200.2/32
Endpoint = 95.177.218.232:44444

[Peer]
PublicKey = /root/PeerC-PublicKey
PresharedKey = /root/psk
AllowedIPs = 10.200.200.3/32
Endpoint = 95.177.218.233:44444

[Peer]
PublicKey = /root/PeerD-PublicKey
PresharedKey = /root/psk
AllowedIPs = 10.200.200.4/32
Endpoint = 95.177.218.234:44444
```

```
EOF

chown -v root:root /etc/wireguard/wg0.conf
chmod -v 600 /etc/wireguard/wg0.conf

wg-quick up wg0
systemctl enable wg-quick@wg0.service
wg-quick save wg0
cp /etc/wireguard/wg0.conf /tmp/$(uname -n)-wireguard-$(date
+%Y-%m-%d_%H:%M:%S).conf
```

Server: PeerB Configurations

```
touch /etc/wireguard/wg0.conf

cat >>/etc/wireguard/wg0.conf<<EOF

[Interface]
Address = 10.200.200.2/24
SaveConfig = true
ListenPort = 44444
PrivateKey = /root/privatekey

[Peer]
PublicKey = /root/PeerA-PublicKey
PresharedKey = /root/psk
AllowedIPs = 10.200.200.1/32
Endpoint = 95.177.218.228:44444

[Peer]
PublicKey = /root/PeerC-PublicKey
PresharedKey = /root/psk
AllowedIPs = 10.200.200.3/32
Endpoint = 95.177.218.233:44444

[Peer]
PublicKey = /root/PeerD-PublicKey
```

```
PresharedKey = /root/psk
AllowedIPs = 10.200.200.4/32
Endpoint = 95.177.218.234:44444


EOF

chown -v root:root /etc/wireguard/wg0.conf
chmod -v 600 /etc/wireguard/wg0.conf

wg-quick up wg0
systemctl enable wg-quick@wg0.service
wg-quick save wg0
cp /etc/wireguard/wg0.conf /tmp/$(uname -n)-wireguard-$(date
+%Y-%m-%d_%H:%M:%S).conf
```

Server: PeerC Configurations

```
touch etc/wireguard/wg0.conf
cat >>/etc/wireguard/wg0.conf<<EOF
[Interface]
Address = 10.200.200.3/24
SaveConfig = true
ListenPort = 44444
PrivateKey = /root/privatekey

[Peer]
PublicKey = /root/PeerA-PublicKey
PresharedKey = /root/psk
AllowedIPs = 10.200.200.1/32
Endpoint = 95.177.218.228:44444

[Peer]
PublicKey = /root/PeerB-PublicKey
PresharedKey = /root/psk
AllowedIPs = 10.200.200.2/32
Endpoint = 95.177.218.232:44444
```

```
[Peer]
PublicKey = /root/PeerD-PublicKey
PresharedKey = /root/psk
AllowedIPs = 10.200.200.4/32
Endpoint = 95.177.218.234:44444


EOF
chown -v root:root /etc/wireguard/wg0.conf
chmod -v 600 /etc/wireguard/wg0.conf
wg-quick up wg0
systemctl enable wg-quick@wg0.service
wg-quick save wg0
cp /etc/wireguard/wg0.conf /tmp/$(uname -n)-wireguard-$(date
+%Y-%m-%d_%H:%M:%S).conf
```

Server: PeerD Configurations

```
touch etc/wireguard/wg0.conf
cat >>/etc/wireguard/wg0.conf<<EOF
[Interface]
Address = 10.200.200.4/24
SaveConfig = true
ListenPort = 44444
PrivateKey = /root/privatekey

[Peer]
PublicKey = /root/PeerA-PublicKey
PresharedKey = /root/psk
AllowedIPs = 10.200.200.1/32
Endpoint = 95.177.218.228:44444

[Peer]
PublicKey = /root/PeerB-PublicKey
PresharedKey = /root/psk
AllowedIPs = 10.200.200.2/32
Endpoint = 95.177.218.232:44444
```

```
[Peer]
PublicKey = /root/PeerC-PublicKey
PresharedKey = /root/psk
AllowedIPs = 10.200.200.3/32
Endpoint = 95.177.218.233:44444

EOF
chown -v root:root /etc/wireguard/wg0.conf
chmod -v 600 /etc/wireguard/wg0.conf
wg-quick up wg0
systemctl enable wg-quick@wg0.service
wg-quick save wg0
cp /etc/wireguard/wg0.conf /tmp/$(uname -n)-wireguard-$(date
+%Y-%m-%d_%H:%M:%S).conf
```

Configurations Completed

Till here all the configurations completed, in the next section will explain how to add addition Peer or server to the existing network.

Adding additional Server in the future

To add additional server in the future you need only to apply below few steps:

1- Apply the common system configurations as explained in under common system config section in this doc.

2- Generate new private and public Key for this server

```
umask 077; wg genkey | tee privatekey | wg pubkey > publickey
```

3- Copy the Pre shared key and Public Key to the new server.

```
touch psk
cat >psk<<EOF
RrDNbpkGT6//9eU4eMa1cJmRaVNdnBcVc6I2oQBFvBY=
EOF
```

To copy the public keys of all other servers to this new server please refer to section “Common WireGuard configurations applied on all servers” step number 3.

4- Now add the new configurations for the new server which will include all servers.

```
touch etc/wireguard/wg0.conf
cat >>/etc/wireguard/wg0.conf<<EOF
[Interface]
Address = 10.200.200.5/24
SaveConfig = true
ListenPort = 44444
PrivateKey = /root/privatekey
```

```
[Peer]
PublicKey = /root/PeerA-PublicKey
PresharedKey = /root/psk
AllowedIPs = 10.200.200.1/32
Endpoint = 95.177.218.228:44444

[Peer]
PublicKey = /root/PeerB-PublicKey
PresharedKey = /root/psk
AllowedIPs = 10.200.200.2/32
Endpoint = 95.177.218.232:44444

[Peer]
PublicKey = /root/PeerC-PublicKey
PresharedKey = /root/psk
AllowedIPs = 10.200.200.3/32
Endpoint = 95.177.218.233:44444

[Peer]
PublicKey = /root/PeerD-PublicKey
PresharedKey = /root/psk
AllowedIPs = 10.200.200.4/32
Endpoint = 95.177.218.234:44444

EOF
chown -v root:root /etc/wireguard/wg0.conf
chmod -v 600 /etc/wireguard/wg0.conf
wg-quick up wg0
systemctl enable wg-quick@wg0.service
wg-quick save wg0
cp /etc/wireguard/wg0.conf /tmp/$(uname -n)-wireguard-
$(date +%Y-%m-%d_%H:%M:%S).conf
```

Note: All below steps to be done on the other existing server

5- Copy the new server public Key to all other servers.

```
cat publickey
```

Copy the content of this file and go to each server and add it, you can do that by below commands

```
touch PeerF-PublicKey
cat>PeerF-PublicKey<<EOF
```

```
<Here put the new key that generated in step 2 above
publickey>
EOF
```

6- Now go to each server and execute below command

```
wg set wg0 peer PeerF-PublicKey preshared-key psk
allowed-ips 10.200.200.5/32 endpoint 95.177.218.235:44444
wg-quick save wg0
```

Testing WireGuard

Below commands will show you the WireGuard Configurations

```
wg
wg show
wg showconf wg0
```

Configure firewall rules on the server

We will need to set up a few firewall rules to manage our VPN and DNS traffic.

Track VPN connection

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

Allowing incoming VPN traffic on the listening port

```
iptables -A INPUT -p udp -m udp --dport 44444 -m conntrack -
-ctstate NEW -j ACCEPT
```

Allow both TCP and UDP recursive DNS traffic

```
iptables -A INPUT -s 10.200.200.0/24 -p tcp -m tcp --dport
53 -m conntrack --ctstate NEW -j ACCEPT
iptables -A INPUT -s 10.200.200.0/24 -p udp -m udp --dport
53 -m conntrack --ctstate NEW -j ACCEPT
```

Allow forwarding of packets that stay in the VPN tunnel

```
iptables -A FORWARD -i wg0 -o wg0 -m conntrack --ctstate NEW
-j ACCEPT
```

Set up nat

```
iptables -t nat -A POSTROUTING -s 10.200.200.0/24 -o eth0 -j
MASQUERADE
```

We also want to ensure that the rules remain persistent across reboots.

```
apt-get install iptables-persistent
systemctl enable netfilter-persistent
netfilter-persistent save
```

Troubleshooting WireGuard

In case the tunnel is not up or you face any issue please follow below steps:

1- Make sure that you have latest configurations of /etc/wireguard/wg0.conf file
You can take a copy of it with below command

```
cp /etc/wireguard/wg0.conf /tmp/$(uname -n)-wireguard-$(date +%Y-%m-%d_%H:%M:%S).conf
```

2- Re-establish the connectivity again by first bring the tunnel down on the impacted server

```
wg-quick down wg0
```

3- Now clear the content of /etc/wireguard/wg0.conf file

```
> /etc/wireguard/wg0.conf
```

4- Make sure that the backed up configurations are correct, you need to double check below points before you copy it back again to the > /etc/wireguard/wg0.conf :
   a. Make sure the private keys of each server is correct.
   b. Make sure the public keys of each server is correct.
   c. Make sure the preshared key on each server is correct.
   d. Make sure the public IPs and endpoint IPs are correct.

5- Now copy back the backup copy to of your configurations to /etc/wireguard/wg0.conf

```
cp <type the path of backup file> /etc/wireguard/wg0.conf
```

6- Bring the tunnel up again and save the configurations:

```
wg-quick up wg0
wg-quick save wg0
```

Debugging & Logging

To enable debugging and logging execute below commands

```
modprobe wireguard
echo module wireguard +p > /sys/kernel/debug/dynamic_debug/control
```

Now view the log with below command:

```
journalctl -flu wg-quick@wg0
```

Or

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