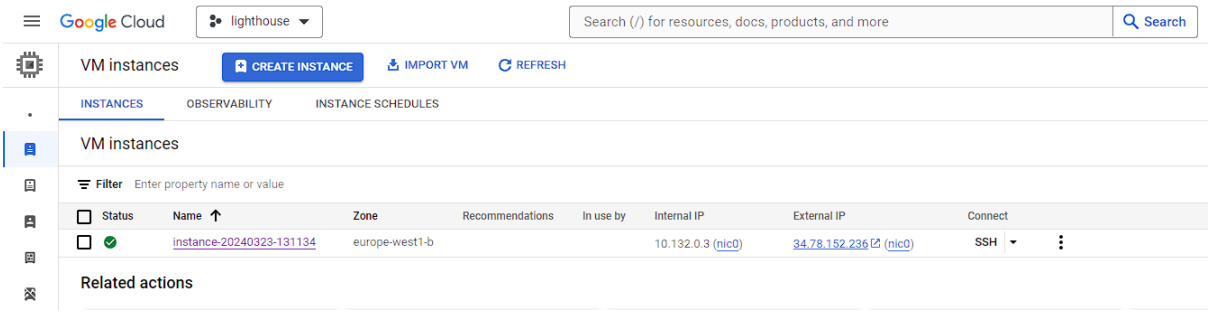
Cloud Networking Lab: Setting Up a Nebula Network with a Lighthouse on Google Cloud

Objective: This lab covers the process of creating a secure, peer-to-peer network using Nebula, with a focus on enabling connectivity for computers behind NATs. I'm use Google Cloud VM with a public IP to serve as the Lighthouse, facilitating network connectivity among nodes.

Google Cloud VM Setup:



Commands Used to set up Nebula Cert:

```
nebula-cert ca -name "My Nebula Network"
nebula-cert sign -name "Lighthouse" -ip "192.168.100.1/24"
nebula-cert sign -name "Lei" -ip "192.168.100.4/24"
```

Changes made to config.yaml:

```
pki:
  # The CAs that are accepted by this node. Mus
  ca: home/conorbrooke19/ca.crt
  cert: home/conorbrooke19/lighthouse1.crt
  key: home/conorbrooke19/lighthouse1.key
  # blocklist is a list of certificate fingerpr
  #blocklist:
  #   - c99d4e650533b92061b09918e838a5a0a6aaee21
  # disconnect_invalid is a toggle to force a c
  #disconnect_invalid: false

# The static host map defines a set of hosts wi
# A host can have multiple fixed IP addresses d
# The syntax is:
#   "{nebula ip}": ["{routable ip/dns name}:{ro
# Example, if your lighthouse has the nebula IP
lighthouse:
  # am_lighthouse is used to enable lighthouse
  # you have configured to be lighthouses in yo
  am_lighthouse: true
  # serve_dns optionally starts a dns listener
```

Starting Nebula in the SSH-in-browser console on Google Cloud:

```
conorbrooke19@instance-20240323-131134:/$ sudo ./usr/local/bin/nebula -config /home/conorbrooke19/config.yaml
INFO[0000] Firewall rule added                           firewallRule="map[caName: caSha: direction:outgoing endPort:0 groups:[] host:any ip: proto:0 startPort:0]"
INFO[0000] Firewall rule added                           firewallRule="map[caName: caSha: direction:incoming endPort:0 groups:[] host:any ip: proto:0 startPort:0]"
INFO[0000] Firewall started                              firewallHash=21716b47a7a140e448077fe66c31b4b42f232e996818d7dd1c6c4991e066dbdb
INFO[0000] Main HostMap created                          network=192.168.100.1/24 preferredRanges="[]"
INFO[0000] UDP hole punching enabled
INFO[0000] Nebula interface is active                    build=1.4.0 interface=nebula1 network=192.168.100.1/24 udpAddr="0.0.0.0:4242"
^CINFO[0344] Caught signal, shutting down                  signal=interrupt
INFO[0344] Goodbye
conorbrooke19@instance-20240323-131134:/$
```

Generate A Certificate for Local Machine Node

```
conorbrooke@DESKTOP-P208N5D:~$ nebula-cert ca -name "Conors-Cert"
conorbrooke@DESKTOP-P208N5D:~$ nebula-cert sign -name "local-machine-node" -ip "192.168.100.1/24"
```

Changing cert paths:

```
pki:
  # The CAs that are accepted by this node. Must
  ca: home/conorbrooke/ca.crt
  cert: home/conorbrooke/local-machine-node.crt
  key: home/conorbrooke/local-machine-node.key
```

Adding the Lighthouses external IP:

```
static_host_map:
  "192.168.100.1": ["34.78.152.236:4242"]
lighthouse:
  # am_lighthouse is used to enable lightho
  # you have configured to be lighthouses i
  am_lighthouse: false
```

Establishing a connection:

```
" vpnIp=192.168.100.1
INFO[0420] Handshake message sent                        handshake="map[stage:1 style:ix_psk0]" initiatorIndex=1707226491 udpAddrs="[34.78.152.236:4242]" vpnIp=192.168.100.1
INFO[0420] Handshake message sent                        handshake="map[stage:1 style:ix_psk0]" initiatorIndex=1707226491 udpAddrs="[34.78.152.236:4242]" vpnIp=192.168.100.1
INFO[0420] Handshake message sent                        handshake="map[stage:1 style:ix_psk0]" initiatorIndex=1707226491 udpAddrs="[34.78.152.236:4242]" vpnIp=192.168.100.1
INFO[0421] Handshake message sent                        handshake="map[stage:1 style:ix_psk0]" initiatorIndex=1707226491 udpAddrs="[34.78.152.236:4242]" vpnIp=192.168.100.1
INFO[0421] Handshake message sent                        handshake="map[stage:1 style:ix_psk0]" initiatorIndex=1707226491 udpAddrs="[34.78.152.236:4242]" vpnIp=192.168.100.1
INFO[0422] Handshake message sent                        handshake="map[stage:1 style:ix_psk0]" initiatorIndex=1707226491 udpAddrs="[34.78.152.236:4242]" vpnIp=192.168.100.1
INFO[0423] Handshake message sent                        handshake="map[stage:1 style:ix_psk0]" initiatorIndex=1707226491 udpAddrs="[34.78.152.236:4242]" vpnIp=192.168.100.1
INFO[0424] Handshake message sent                        handshake="map[stage:1 style:ix_psk0]" initiatorIndex=1707226491 udpAddrs="[34.78.152.236:4242]" vpnIp=192.168.100.1
INFO[0426] Handshake message sent                        handshake="map[stage:1 style:ix_psk0]" initiatorIndex=1707226491 udpAddrs="[34.78.152.236:4242]" vpnIp=192.168.100.1
INFO[0427] Handshake message sent                        handshake="map[stage:1 style:ix_psk0]" initiatorIndex=1707226491 udpAddrs="[34.78.152.236:4242]" vpnIp=192.168.100.1
INFO[0429] Handshake timed out                           durationNs=9086339136 handshake="map[stage:1 style:ix_psk0]" initiatorIndex=1707226491 remoteIndex=0 udpAddrs="[34.78.152.236:4242]
" vpnIp=192.168.100.1
INFO[0480] Handshake message sent                        handshake="map[stage:1 style:ix_psk0]" initiatorIndex=3706424230 udpAddrs="[34.78.152.236:4242]" vpnIp=192.168.100.1
```

Pinging to lighthouse from node:

```
conorbrooke@DESKTOP-P208N5D:~$ ping 192.168.100.1
PING 192.168.100.1 (192.168.100.1) 56(84) bytes of data.
64 bytes from 192.168.100.1: icmp_seq=1 ttl=64 time=0.018 ms
64 bytes from 192.168.100.1: icmp_seq=2 ttl=64 time=0.033 ms
64 bytes from 192.168.100.1: icmp_seq=3 ttl=64 time=0.026 ms
64 bytes from 192.168.100.1: icmp_seq=4 ttl=64 time=0.022 ms
64 bytes from 192.168.100.1: icmp_seq=5 ttl=64 time=0.022 ms
64 bytes from 192.168.100.1: icmp_seq=6 ttl=64 time=0.025 ms
```

Connecting another node to the lighthouse on a separate device:

```
conor@Dev-System:/$ sudo ./usr/local/bin/nebula -config /home/conor/config.yaml
INFO[0000] Firewall rule added                           firewallRule="map[caName: caSha: direction:outgoing endPort:0 groups:[] host:any ip: proto:0 startPort:0]"
INFO[0000] Firewall rule added                           firewallRule="map[caName: caSha: direction:incoming endPort:0 groups:[] host:any ip: proto:0 startPort:0]"
INFO[0000] Firewall started                              firewallHash=21716b47a7a140e448077fe66c31b4b42f232e996818d7dd1c6c4991e066dbdb
INFO[0000] Main HostMap created                          network=192.168.100.2/24 preferredRanges="[]"
INFO[0000] UDP hole punching enabled
INFO[0000] Nebula interface is active                    build=1.4.0 interface=nebula1 network=192.168.100.2/24 udpAddr="0.0.0.0:4242"
INFO[0000] Handshake message sent                        handshake="map[stage:1 style:ix_psk0]" initiatorIndex=1666975910 udpAddrs="[34.78.152.236:4242]" vpnIp=192.168.100.3
INFO[0000] Handshake message sent                        handshake="map[stage:1 style:ix_psk0]" initiatorIndex=1666975910 udpAddrs="[34.78.152.236:4242]" vpnIp=192.168.100.3
INFO[0000] Handshake message sent                        handshake="map[stage:1 style:ix_psk0]" initiatorIndex=1666975910 udpAddrs="[34.78.152.236:4242]" vpnIp=192.168.100.3
```

Testing connection between Nodes:

Pinging from node 2 (laptop) to node 1 (local machine):

```
conor@Dev-System:~$ ping 192.168.100.2
PING 192.168.100.2 (192.168.100.2) 56(84) bytes of data.
64 bytes from 192.168.100.2: icmp_seq=1 ttl=64 time=0.066 ms
64 bytes from 192.168.100.2: icmp_seq=2 ttl=64 time=0.034 ms
64 bytes from 192.168.100.2: icmp_seq=3 ttl=64 time=0.037 ms
64 bytes from 192.168.100.2: icmp_seq=4 ttl=64 time=0.051 ms
64 bytes from 192.168.100.2: icmp_seq=5 ttl=64 time=0.050 ms
64 bytes from 192.168.100.2: icmp_seq=6 ttl=64 time=0.050 ms
64 bytes from 192.168.100.2: icmp_seq=7 ttl=64 time=0.035 ms
64 bytes from 192.168.100.2: icmp_seq=8 ttl=64 time=0.044 ms
64 bytes from 192.168.100.2: icmp_seq=9 ttl=64 time=0.050 ms
64 bytes from 192.168.100.2: icmp_seq=10 ttl=64 time=0.030 ms
64 bytes from 192.168.100.2: icmp_seq=11 ttl=64 time=0.035 ms
```