Report

IPsec VPN: connecting IoT devices to cloud

Anastasia Safargalieva, Soumya Lekkala
Group 7

1. The first configuration that we did is securing Cloud S. Cloud S was public in the beginning, we will make it private by assigning IPs of Client-A1 and Client-A2 to the Server-1 and Server-2 of the Cloud S network.

In order to change the IP address of the network from `172.48.48.49` to `10.1.0.1`, we changed it in the vagrant file for Gateway S configuration.

We also created 2 gateways from A to S and from B to S. Commands for this are added to the `cloud_s_gateway.sh`. We also generated public shared keys (PSK) for both routes.

Packets coming from gateway A to S:

```
echo 172.30.30.30 172.16.16.16 : PSK
\"uYGc2rYbryqSLHpVqYNJCoG2LaxWDDpADEwydN9XYSfWuvChdEtRIFoGAhDUJ0yJwy1TX
gv6UevTglwRrvMzuL766gGedgzv7YylOsth0dFBlsTZv2fHaC4pLeMRZrzRq23f4YzvH3Ra
a0aT1SYhOGDVv08VEav5BLCjAPBirO36pmIs76mdC8nsYCGHP8efMXW2J0g39jR3iRVahW7
yKimhgCjpkm1mTikb5mG323oWSglFjyTgPNoCm2mumCT3\">> /etc/ipsec.secrets
```

Packets coming from gateway B to S:

```
echo 172.30.30.30 172.18.18.18 : PSK
\"HMXJumvFLTN1noNm8ET4WOeKD5Ec4KFMqwZ5Pyx9jYreob2e0InG4ferASftV0EPMh7TD
1oXu7IEslyhBpRd2lwIBqONA36rEHSsW9mFxD5rskLSo1Zi5JKxqjB8R1mfvfLx4RdasEwe
cgL2OvCiXZaJk6ez2xZBhd2WIEO5DNqpjiJEBSalsb4eo4IYSs661WAMQ2W25efEY0oDnvo
L5gGXoGuLFZbJ1CWrigq2dqVFNgdDxdk6ruSVPWNXBdxY\">> /etc/ipsec.secrets
```

We also enabled NAT for Cloud S:

```
 iptables -t nat -A POSTROUTING -o enp0s8 -j MASQUERADE
```

Then we implemented DNAT for the Cloud S by adding the following script to the `cloud_s_gateway.sh.`

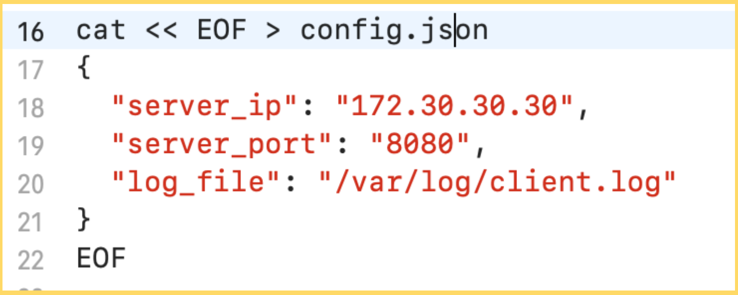
```
## DNAT
iptables -t nat -A PREROUTING -i enp0s8 -p tcp --source 172.18.18.18
--dport 8080 -j DNAT --to-destination 10.1.0.2
iptables -A INPUT -p esp --source 172.18.18.18 -j ACCEPT
iptables -A INPUT --source 172.18.18.18 -j DROP
iptables -t nat -A PREROUTING -i enp0s8 -p tcp --source 172.16.16.16
--dport 8080 -j DNAT --to-destination 10.1.0.3
iptables -A INPUT -p esp --source 172.16.16.16 -j ACCEPT
iptables -A INPUT --source 172.16.16.16 -j DROP
```

The next step was configuring the VPN itself. For this in the file `cloud_s_gateway.sh` we wrote all properties that we want the cloud VPN to have, and a script to connect the cloud VPN to gateway a and gateway b.

```
cat > /etc/ipsec.conf <<EOL
config setup
        charondebug=all
        uniqueids=yes
        strictcrlpolicy=no
conn cloud-vpn
        type=tunnel
        keyexchange=ikev2
        authby=secret
        leftfirewall=yes
        left=172.30.30.30
        leftsubnet=172.30.30.30/32
        ike=aes256-sha2_256-modp2048!
        esp=aes256-sha2_256!
        dpdaction=restart
        auto=start
conn gateway-a-vpn
        also=cloud-vpn
        right=172.16.16.16
        rightsubnet=172.16.16.16/32
conn gateway-b-vpn
        also=cloud-vpn
        right=172.18.18.18
        rightsubnet=172.18.18.18/32
EOL
```

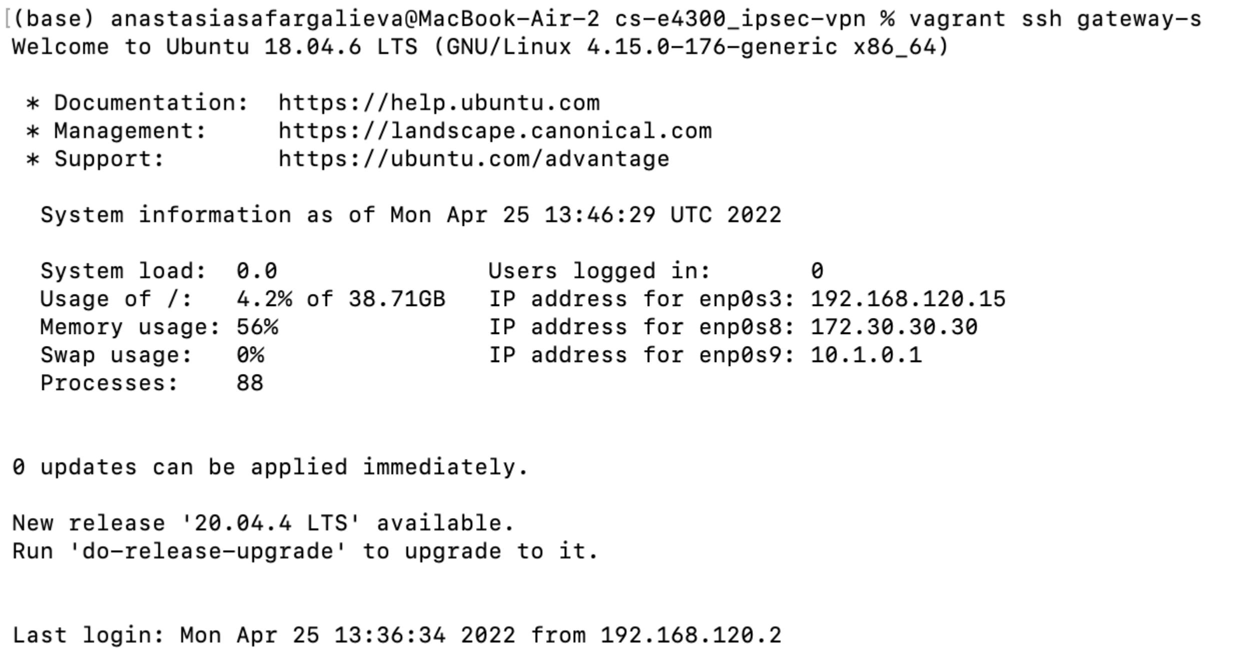
After we transferred servers A and B to the Gateway S we need to disable the configuration for the servers A and B and rebuild the entire topology for the VM setup.

2. Then we automate config json file by editing `client.sh`.



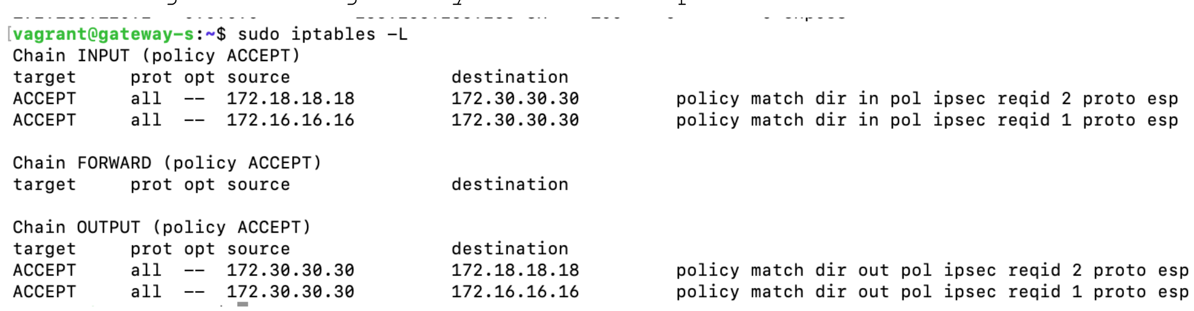
```
cat << EOF > config.json
{
  "server_ip": "172.30.30.30",
  "server_port": "8080",
  "log_file": "/var/log/client.log"
}
EOF
```

3. In order to run the configuration we run `vagrant up` and `vagrant ssh gateway-s` inside our folder.



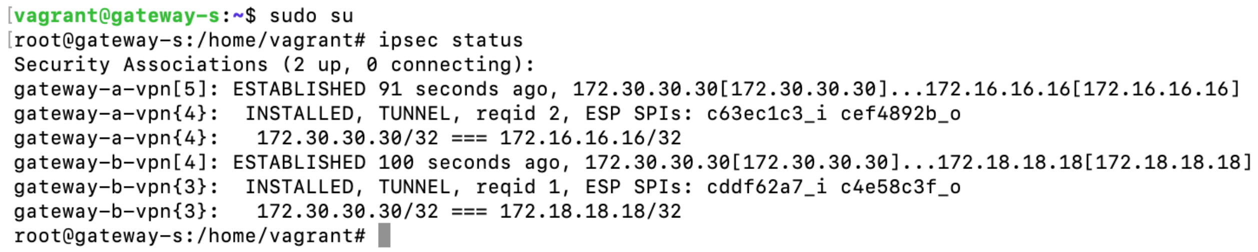
```
[(base) anastasiasafargalieva@MacBook-Air-2 cs-e4300_ipsec-vpn % vagrant ssh gateway-s
Welcome to Ubuntu 18.04.6 LTS (GNU/Linux 4.15.0-176-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Mon Apr 25 13:46:29 UTC 2022

  System load:  0.0               Users logged in:       0
  Usage of /:   4.2% of 38.71GB   IP address for enp0s3: 192.168.120.15
  Memory usage: 56%               IP address for enp0s8: 172.30.30.30
  Swap usage:   0%                IP address for enp0s9: 10.1.0.1
  Processes:    88


0 updates can be applied immediately.

New release '20.04.4 LTS' available.
Run 'do-release-upgrade' to upgrade to it.


Last login: Mon Apr 25 13:36:34 2022 from 192.168.120.2
```

Then run `vagrant ssh gateway-s` and `sudo iptables -L`



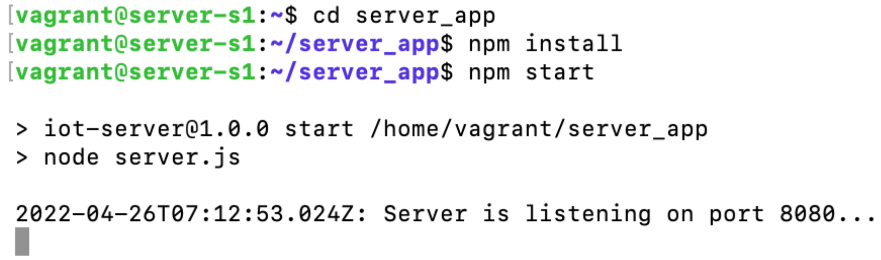
```
[vagrant@gateway-s:~$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     all  --  172.18.18.18         172.30.30.30         policy match dir in pol ipsec reqid 2 proto esp
ACCEPT     all  --  172.16.16.16         172.30.30.30         policy match dir in pol ipsec reqid 1 proto esp

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     all  --  172.30.30.30         172.18.18.18         policy match dir out pol ipsec reqid 2 proto esp
ACCEPT     all  --  172.30.30.30         172.16.16.16         policy match dir out pol ipsec reqid 1 proto esp
```

These are the tunnels we established



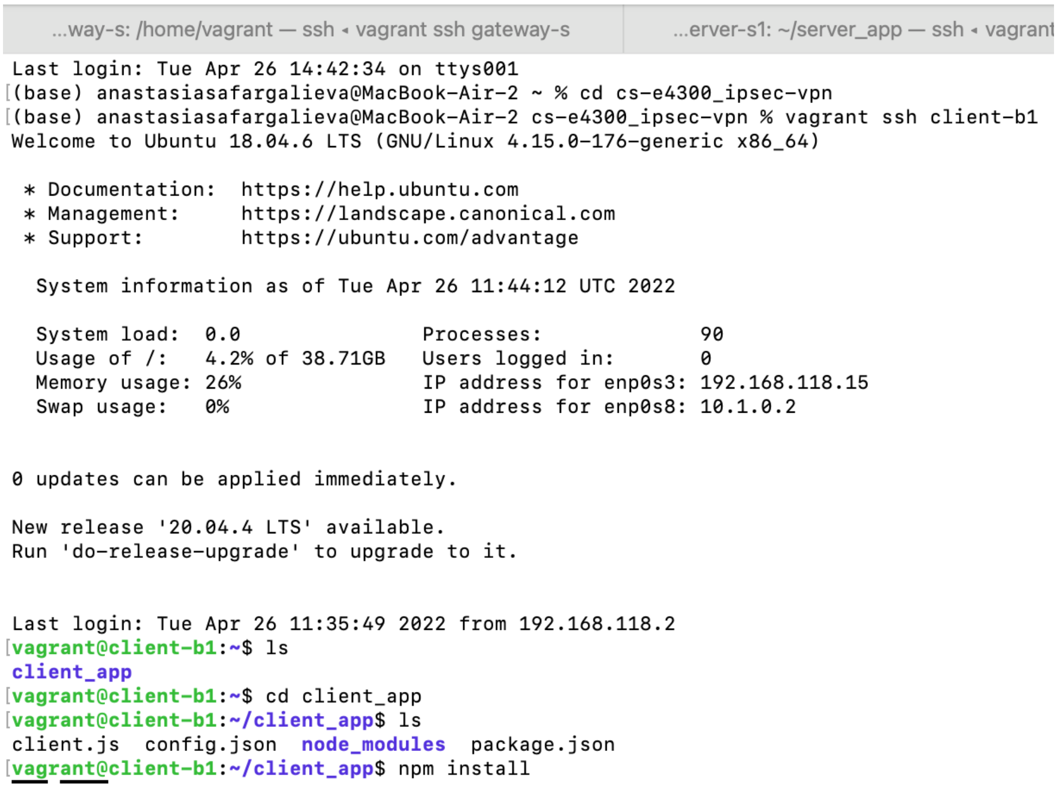
```
[vagrant@gateway-s:~$ sudo su
[root@gateway-s:/home/vagrant# ipsec status
Security Associations (2 up, 0 connecting):
gateway-a-vpn[5]: ESTABLISHED 91 seconds ago, 172.30.30.30[172.30.30.30]...172.16.16.16[172.16.16.16]
gateway-a-vpn{4}:  INSTALLED, TUNNEL, reqid 2, ESP SPIs: c63ec1c3_i cef4892b_o
gateway-a-vpn{4}:   172.30.30.30/32 === 172.16.16.16/32
gateway-b-vpn[4]: ESTABLISHED 100 seconds ago, 172.30.30.30[172.30.30.30]...172.18.18.18[172.18.18.18]
gateway-b-vpn{3}:  INSTALLED, TUNNEL, reqid 1, ESP SPIs: cddf62a7_i c4e58c3f_o
gateway-b-vpn{3}:   172.30.30.30/32 === 172.18.18.18/32
root@gateway-s:/home/vagrant# 
```

Then we ran `vagrant ssh server-s1` and open `server_app`. Inside the server s1 we install npm and then run it.



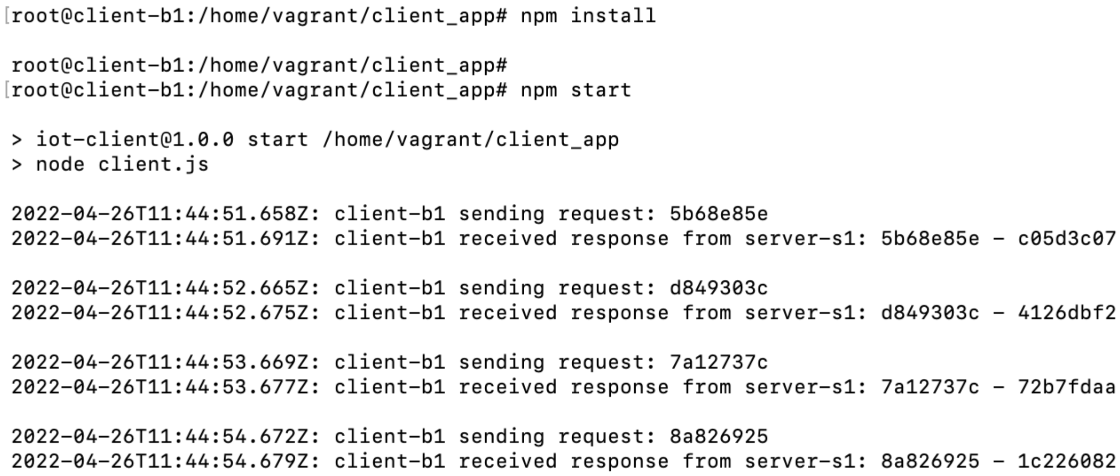
```
[vagrant@server-s1:~$ cd server_app
[vagrant@server-s1:~/server_app$ npm install
[vagrant@server-s1:~/server_app$ npm start

> iot-server@1.0.0 start /home/vagrant/server_app
> node server.js

2022-04-26T07:12:53.024Z: Server is listening on port 8080...
```

In the third terminal we open `client-b1` for the `server-s1`.


...way-s: /home/vagrant — ssh ◂ vagrant ssh gateway-s
...erver-s1: ~/server_app — ssh ◂ vagrant

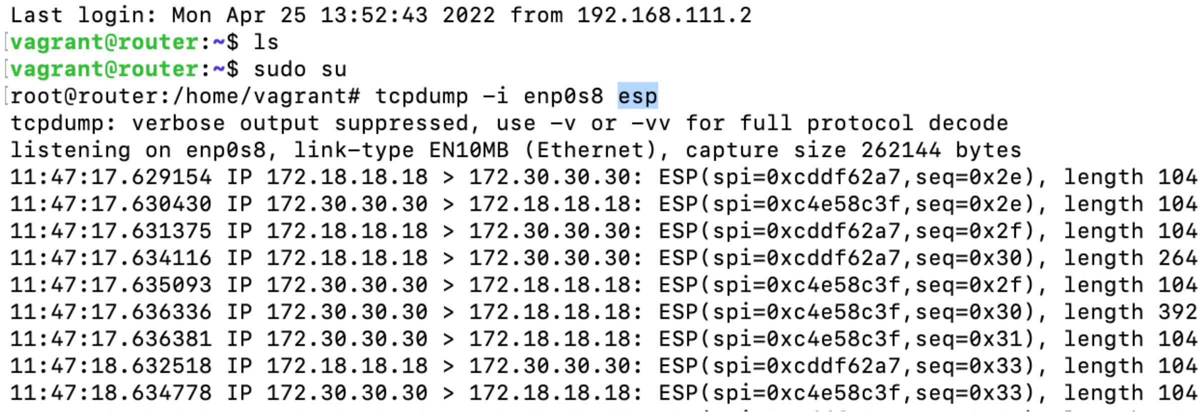
```
Last login: Tue Apr 26 14:42:34 on ttys001
[(base) anastasiasafargalieva@MacBook-Air-2 ~ % cd cs-e4300_ipsec-vpn
[(base) anastasiasafargalieva@MacBook-Air-2 cs-e4300_ipsec-vpn % vagrant ssh client-b1
Welcome to Ubuntu 18.04.6 LTS (GNU/Linux 4.15.0-176-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Tue Apr 26 11:44:12 UTC 2022

  System load:  0.0               Processes:             90
  Usage of /:   4.2% of 38.71GB   Users logged in:       0
  Memory usage: 26%               IP address for enp0s3: 192.168.118.15
  Swap usage:   0%                IP address for enp0s8: 10.1.0.2


0 updates can be applied immediately.

New release '20.04.4 LTS' available.
Run 'do-release-upgrade' to upgrade to it.


Last login: Tue Apr 26 11:35:49 2022 from 192.168.118.2
[vagrant@client-b1:~$ ls
client_app
[vagrant@client-b1:~$ cd client_app
[vagrant@client-b1:~/client_app$ ls
client.js  config.json  node_modules  package.json
[vagrant@client-b1:~/client_app$ npm install
```

Then we start npm with `sudo su` rights.



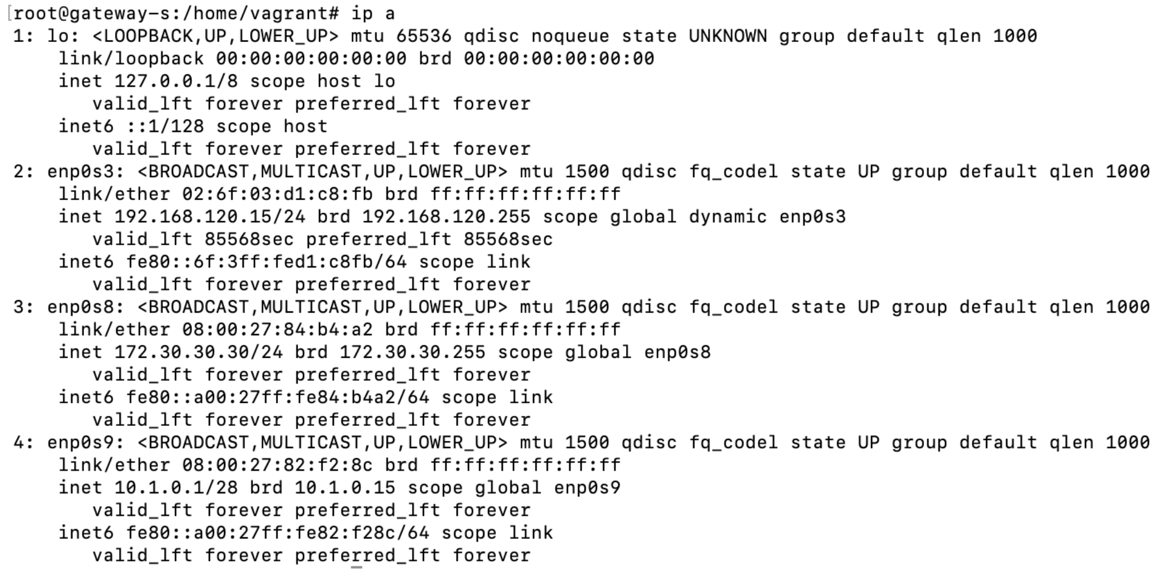
```
[root@client-b1:/home/vagrant/client_app# npm install

root@client-b1:/home/vagrant/client_app#
[root@client-b1:/home/vagrant/client_app# npm start

> iot-client@1.0.0 start /home/vagrant/client_app
> node client.js

2022-04-26T11:44:51.658Z: client-b1 sending request: 5b68e85e
2022-04-26T11:44:51.691Z: client-b1 received response from server-s1: 5b68e85e - c05d3c07

2022-04-26T11:44:52.665Z: client-b1 sending request: d849303c
2022-04-26T11:44:52.675Z: client-b1 received response from server-s1: d849303c - 4126dbf2

2022-04-26T11:44:53.669Z: client-b1 sending request: 7a12737c
2022-04-26T11:44:53.677Z: client-b1 received response from server-s1: 7a12737c - 72b7fdaa

2022-04-26T11:44:54.672Z: client-b1 sending request: 8a826925
2022-04-26T11:44:54.679Z: client-b1 received response from server-s1: 8a826925 - 1c226082
```

We also checked that the connwction is secure with esp protocol.



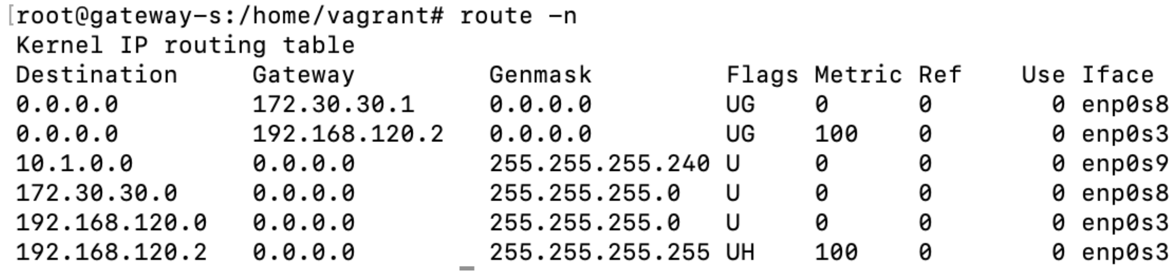
```
Last login: Mon Apr 25 13:52:43 2022 from 192.168.111.2
[vagrant@router:~$ ls
[vagrant@router:~$ sudo su
[root@router:/home/vagrant# tcpdump -i enp0s8 esp
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp0s8, link-type EN10MB (Ethernet), capture size 262144 bytes
11:47:17.629154 IP 172.18.18.18 > 172.30.30.30: ESP(spi=0xcddf62a7,seq=0x2e), length 104
11:47:17.630430 IP 172.30.30.30 > 172.18.18.18: ESP(spi=0xc4e58c3f,seq=0x2e), length 104
11:47:17.631375 IP 172.18.18.18 > 172.30.30.30: ESP(spi=0xcddf62a7,seq=0x2f), length 104
11:47:17.634116 IP 172.18.18.18 > 172.30.30.30: ESP(spi=0xcddf62a7,seq=0x30), length 264
11:47:17.635093 IP 172.30.30.30 > 172.18.18.18: ESP(spi=0xc4e58c3f,seq=0x2f), length 104
11:47:17.636336 IP 172.30.30.30 > 172.18.18.18: ESP(spi=0xc4e58c3f,seq=0x30), length 392
11:47:17.636381 IP 172.30.30.30 > 172.18.18.18: ESP(spi=0xc4e58c3f,seq=0x31), length 104
11:47:18.632518 IP 172.18.18.18 > 172.30.30.30: ESP(spi=0xcddf62a7,seq=0x33), length 104
11:47:18.634778 IP 172.30.30.30 > 172.18.18.18: ESP(spi=0xc4e58c3f,seq=0x33), length 104
```

4. ip a command



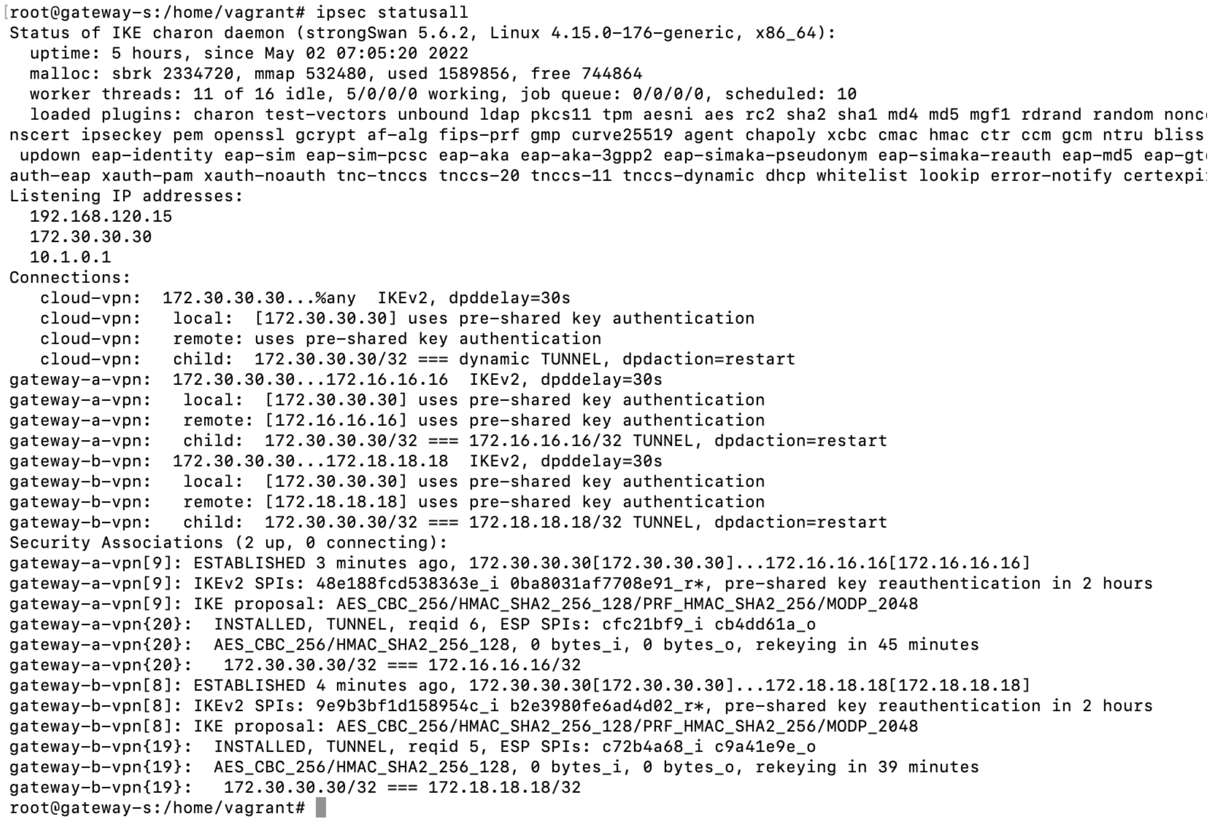
```
[root@gateway-s:/home/vagrant# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 02:6f:03:d1:c8:fb brd ff:ff:ff:ff:ff:ff
    inet 192.168.120.15/24 brd 192.168.120.255 scope global dynamic enp0s3
       valid_lft 85568sec preferred_lft 85568sec
    inet6 fe80::6f:3ff:fed1:c8fb/64 scope link
       valid_lft forever preferred_lft forever
3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:84:b4:a2 brd ff:ff:ff:ff:ff:ff
    inet 172.30.30.30/24 brd 172.30.30.255 scope global enp0s8
       valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fe84:b4a2/64 scope link
       valid_lft forever preferred_lft forever
4: enp0s9: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:82:f2:8c brd ff:ff:ff:ff:ff:ff
    inet 10.1.0.1/28 brd 10.1.0.15 scope global enp0s9
       valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fe82:f28c/64 scope link
       valid_lft forever preferred_lft forever
```

5. route -n



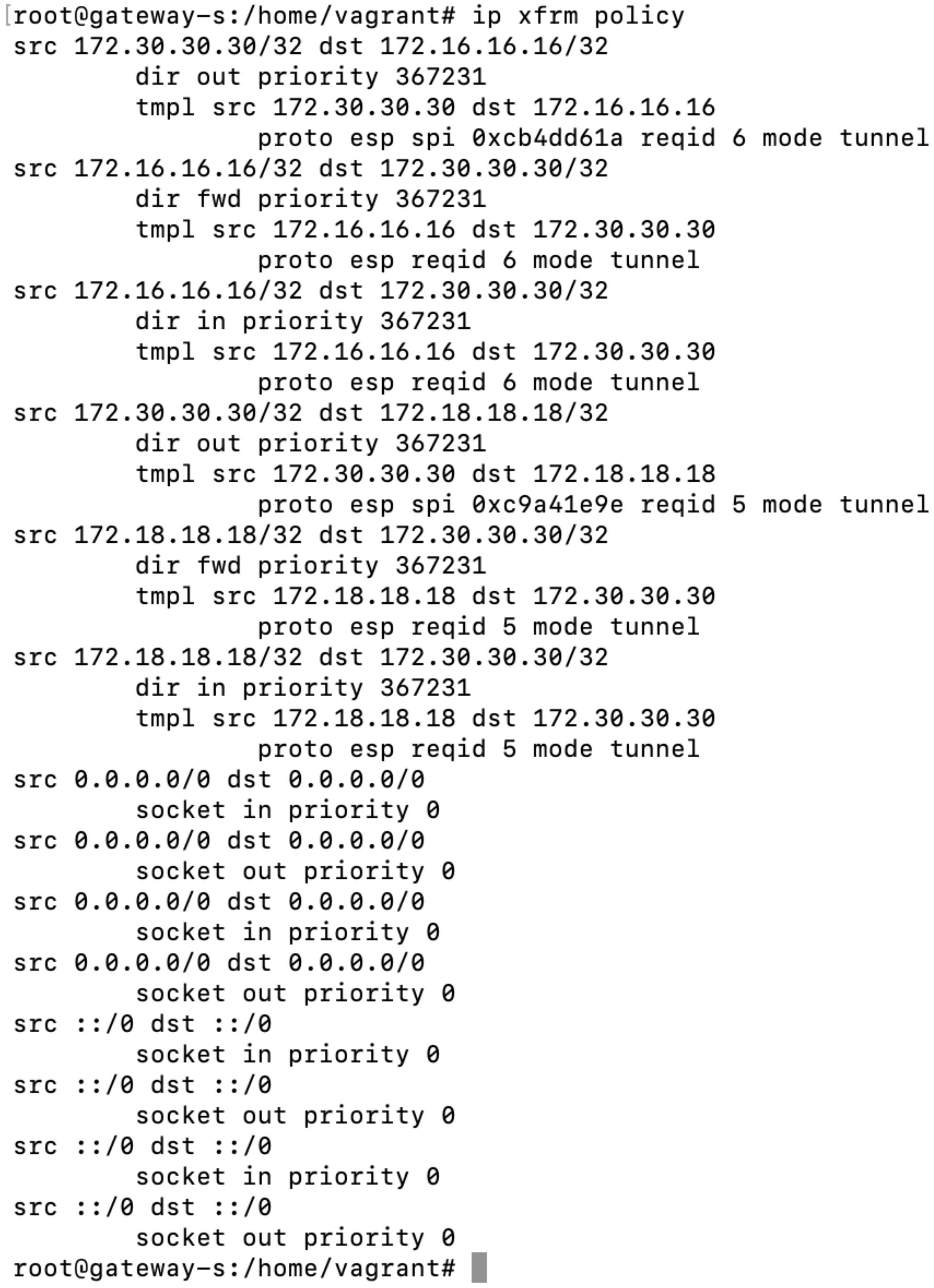
```
[root@gateway-s:/home/vagrant# route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         172.30.30.1     0.0.0.0         UG    0      0        0 enp0s8
0.0.0.0         192.168.120.2   0.0.0.0         UG    100    0        0 enp0s3
10.1.0.0        0.0.0.0         255.255.255.240 U     0      0        0 enp0s9
172.30.30.0     0.0.0.0         255.255.255.0   U     0      0        0 enp0s8
192.168.120.0   0.0.0.0         255.255.255.0   U     0      0        0 enp0s3
192.168.120.2   0.0.0.0         255.255.255.255 UH    100    0        0 enp0s3
```

6. ipsec statusall



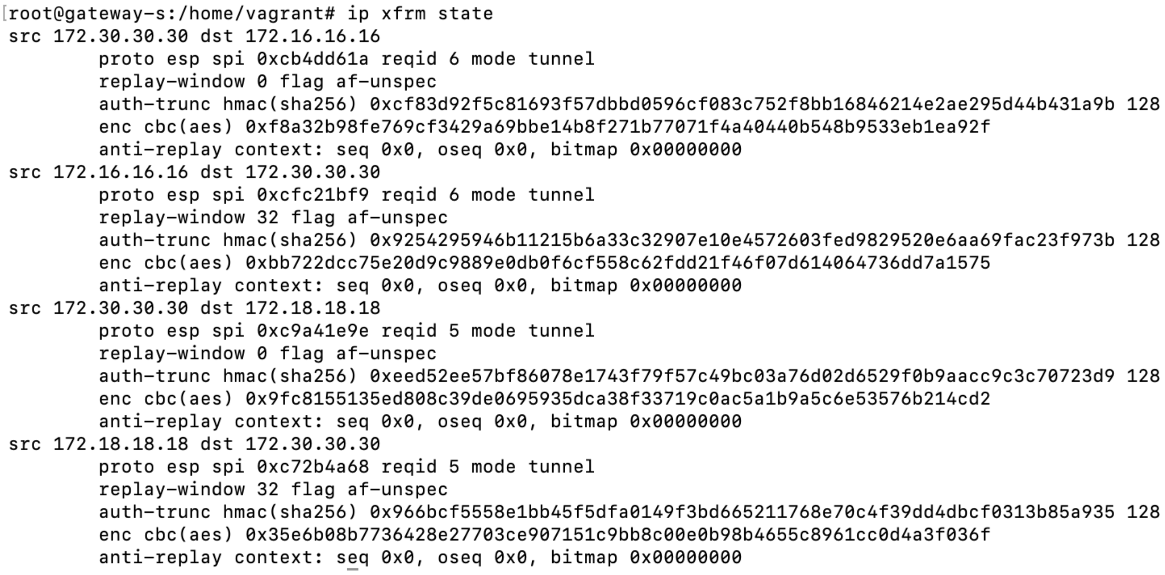
```
root@gateway-s:/home/vagrant# ipsec statusall
Status of IKE charon daemon (strongSwan 5.6.2, Linux 4.15.0-176-generic, x86_64):
  uptime: 5 hours, since May 02 07:05:20 2022
  malloc: sbrk 2334720, mmap 532480, used 1589856, free 744864
  worker threads: 11 of 16 idle, 5/0/0/0 working, job queue: 0/0/0/0, scheduled: 10
  loaded plugins: charon test-vectors unbound ldap pkcs11 tpm aesni aes rc2 sha2 sha1 md4 md5 mgf1 rdrand random nonc
nscert ipseckey pem openssl gcrypt af-alg fips-prf gmp curve25519 agent chapoly xcbc cmac hmac ctr ccm gcm ntru bliss
 updown eap-identity eap-sim eap-sim-pcsc eap-aka eap-aka-3gpp2 eap-simaka-pseudonym eap-simaka-reauth eap-md5 eap-gt
auth-eap xauth-pam xauth-noauth tnc-tnccs tnccs-20 tnccs-11 tnccs-dynamic dhcp whitelist lookip error-notify certexpi
Listening IP addresses:
  192.168.120.15
  172.30.30.30
  10.1.0.1
Connections:
   cloud-vpn:  172.30.30.30...%any  IKEv2, dpddelay=30s
   cloud-vpn:   local:  [172.30.30.30] uses pre-shared key authentication
   cloud-vpn:   remote: uses pre-shared key authentication
   cloud-vpn:   child:  172.30.30.30/32 === dynamic TUNNEL, dpdaction=restart
gateway-a-vpn:  172.30.30.30...172.16.16.16  IKEv2, dpddelay=30s
gateway-a-vpn:   local:  [172.30.30.30] uses pre-shared key authentication
gateway-a-vpn:   remote: [172.16.16.16] uses pre-shared key authentication
gateway-a-vpn:   child:  172.30.30.30/32 === 172.16.16.16/32 TUNNEL, dpdaction=restart
gateway-b-vpn:  172.30.30.30...172.18.18.18  IKEv2, dpddelay=30s
gateway-b-vpn:   local:  [172.30.30.30] uses pre-shared key authentication
gateway-b-vpn:   remote: [172.18.18.18] uses pre-shared key authentication
gateway-b-vpn:   child:  172.30.30.30/32 === 172.18.18.18/32 TUNNEL, dpdaction=restart
Security Associations (2 up, 0 connecting):
gateway-a-vpn[9]: ESTABLISHED 3 minutes ago, 172.30.30.30[172.30.30.30]...172.16.16.16[172.16.16.16]
gateway-a-vpn[9]: IKEv2 SPIs: 48e188fcd538363e_i 0ba8031af7708e91_r*, pre-shared key reauthentication in 2 hours
gateway-a-vpn[9]: IKE proposal: AES_CBC_256/HMAC_SHA2_256_128/PRF_HMAC_SHA2_256/MODP_2048
gateway-a-vpn{20}:  INSTALLED, TUNNEL, reqid 6, ESP SPIs: cfc21bf9_i cb4dd61a_o
gateway-a-vpn{20}:  AES_CBC_256/HMAC_SHA2_256_128, 0 bytes_i, 0 bytes_o, rekeying in 45 minutes
gateway-a-vpn{20}:   172.30.30.30/32 === 172.16.16.16/32
gateway-b-vpn[8]: ESTABLISHED 4 minutes ago, 172.30.30.30[172.30.30.30]...172.18.18.18[172.18.18.18]
gateway-b-vpn[8]: IKEv2 SPIs: 9e9b3bf1d158954c_i b2e3980fe6ad4d02_r*, pre-shared key reauthentication in 2 hours
gateway-b-vpn[8]: IKE proposal: AES_CBC_256/HMAC_SHA2_256_128/PRF_HMAC_SHA2_256/MODP_2048
gateway-b-vpn{19}:  INSTALLED, TUNNEL, reqid 5, ESP SPIs: c72b4a68_i c9a41e9e_o
gateway-b-vpn{19}:  AES_CBC_256/HMAC_SHA2_256_128, 0 bytes_i, 0 bytes_o, rekeying in 39 minutes
gateway-b-vpn{19}:   172.30.30.30/32 === 172.18.18.18/32
root@gateway-s:/home/vagrant#
```

7. ip xfrm policy



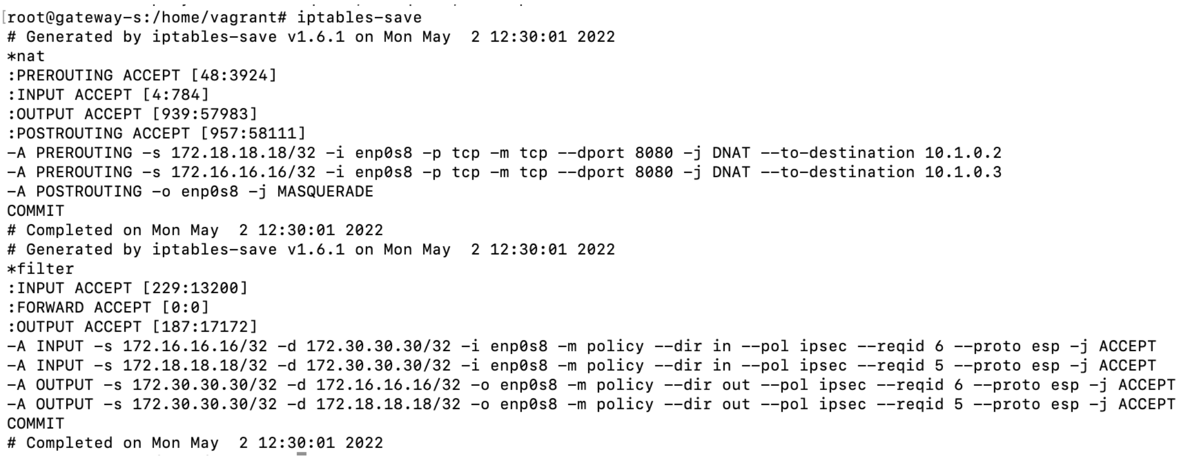
```
[root@gateway-s:/home/vagrant# ip xfrm policy
 src 172.30.30.30/32 dst 172.16.16.16/32
         dir out priority 367231
         tmpl src 172.30.30.30 dst 172.16.16.16
                 proto esp spi 0xcb4dd61a reqid 6 mode tunnel
 src 172.16.16.16/32 dst 172.30.30.30/32
         dir fwd priority 367231
         tmpl src 172.16.16.16 dst 172.30.30.30
                 proto esp reqid 6 mode tunnel
 src 172.16.16.16/32 dst 172.30.30.30/32
         dir in priority 367231
         tmpl src 172.16.16.16 dst 172.30.30.30
                 proto esp reqid 6 mode tunnel
 src 172.30.30.30/32 dst 172.18.18.18/32
         dir out priority 367231
         tmpl src 172.30.30.30 dst 172.18.18.18
                 proto esp spi 0xc9a41e9e reqid 5 mode tunnel
 src 172.18.18.18/32 dst 172.30.30.30/32
         dir fwd priority 367231
         tmpl src 172.18.18.18 dst 172.30.30.30
                 proto esp reqid 5 mode tunnel
 src 172.18.18.18/32 dst 172.30.30.30/32
         dir in priority 367231
         tmpl src 172.18.18.18 dst 172.30.30.30
                 proto esp reqid 5 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@gateway-s:/home/vagrant#
```

8. ip xfrm state



```
root@gateway-s:/home/vagrant# ip xfrm state
src 172.30.30.30 dst 172.16.16.16
        proto esp spi 0xcb4dd61a reqid 6 mode tunnel
        replay-window 0 flag af-unspec
        auth-trunc hmac(sha256) 0xcf83d92f5c81693f57dbbd0596cf083c752f8bb16846214e2ae295d44b431a9b 128
        enc cbc(aes) 0xf8a32b98fe769cf3429a69bbe14b8f271b77071f4a40440b548b9533eb1ea92f
        anti-replay context: seq 0x0, oseq 0x0, bitmap 0x00000000
src 172.16.16.16 dst 172.30.30.30
        proto esp spi 0xcfc21bf9 reqid 6 mode tunnel
        replay-window 32 flag af-unspec
        auth-trunc hmac(sha256) 0x9254295946b11215b6a33c32907e10e4572603fed9829520e6aa69fac23f973b 128
        enc cbc(aes) 0xbb722dcc75e20d9c9889e0db0f6cf558c62fdd21f46f07d614064736dd7a1575
        anti-replay context: seq 0x0, oseq 0x0, bitmap 0x00000000
src 172.30.30.30 dst 172.18.18.18
        proto esp spi 0xc9a41e9e reqid 5 mode tunnel
        replay-window 0 flag af-unspec
        auth-trunc hmac(sha256) 0xeed52ee57bf86078e1743f79f57c49bc03a76d02d6529f0b9aacc9c3c70723d9 128
        enc cbc(aes) 0x9fc8155135ed808c39de0695935dca38f33719c0ac5a1b9a5c6e53576b214cd2
        anti-replay context: seq 0x0, oseq 0x0, bitmap 0x00000000
src 172.18.18.18 dst 172.30.30.30
        proto esp spi 0xc72b4a68 reqid 5 mode tunnel
        replay-window 32 flag af-unspec
        auth-trunc hmac(sha256) 0x966bcf5558e1bb45f5dfa0149f3bd665211768e70c4f39dd4dbcf0313b85a935 128
        enc cbc(aes) 0x35e6b08b7736428e27703ce907151c9bb8c00e0b98b4655c8961cc0d4a3f036f
        anti-replay context: seq 0x0, oseq 0x0, bitmap 0x00000000
```

9. iptables-save



```
root@gateway-s:/home/vagrant# iptables-save
# Generated by iptables-save v1.6.1 on Mon May  2 12:30:01 2022
*nat
:PREROUTING ACCEPT [48:3924]
:INPUT ACCEPT [4:784]
:OUTPUT ACCEPT [939:57983]
:POSTROUTING ACCEPT [957:58111]
-A PREROUTING -s 172.18.18.18/32 -i enp0s8 -p tcp -m tcp --dport 8080 -j DNAT --to-destination 10.1.0.2
-A PREROUTING -s 172.16.16.16/32 -i enp0s8 -p tcp -m tcp --dport 8080 -j DNAT --to-destination 10.1.0.3
-A POSTROUTING -o enp0s8 -j MASQUERADE
COMMIT
# Completed on Mon May  2 12:30:01 2022
# Generated by iptables-save v1.6.1 on Mon May  2 12:30:01 2022
*filter
:INPUT ACCEPT [229:13200]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [187:17172]
-A INPUT -s 172.16.16.16/32 -d 172.30.30.30/32 -i enp0s8 -m policy --dir in --pol ipsec --reqid 6 --proto esp -j ACCEPT
-A INPUT -s 172.18.18.18/32 -d 172.30.30.30/32 -i enp0s8 -m policy --dir in --pol ipsec --reqid 5 --proto esp -j ACCEPT
-A OUTPUT -s 172.30.30.30/32 -d 172.16.16.16/32 -o enp0s8 -m policy --dir out --pol ipsec --reqid 6 --proto esp -j ACCEPT
-A OUTPUT -s 172.30.30.30/32 -d 172.18.18.18/32 -o enp0s8 -m policy --dir out --pol ipsec --reqid 5 --proto esp -j ACCEPT
COMMIT
# Completed on Mon May  2 12:30:01 2022
```