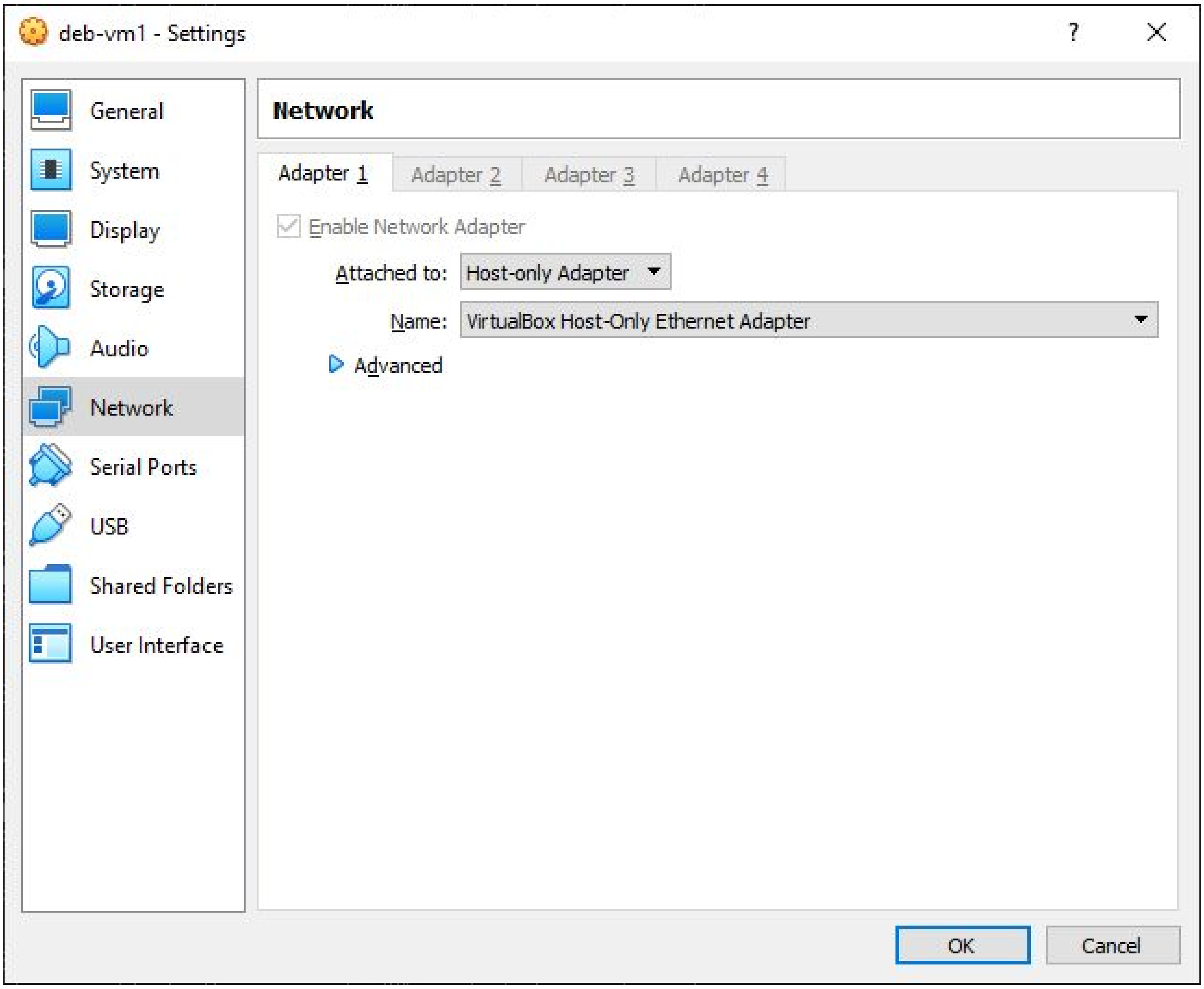
Homework 5

by Alexander Krupskiy

VM1 - Debian 10 (VirtualBox)



Network

☑ Enable Network Adapter

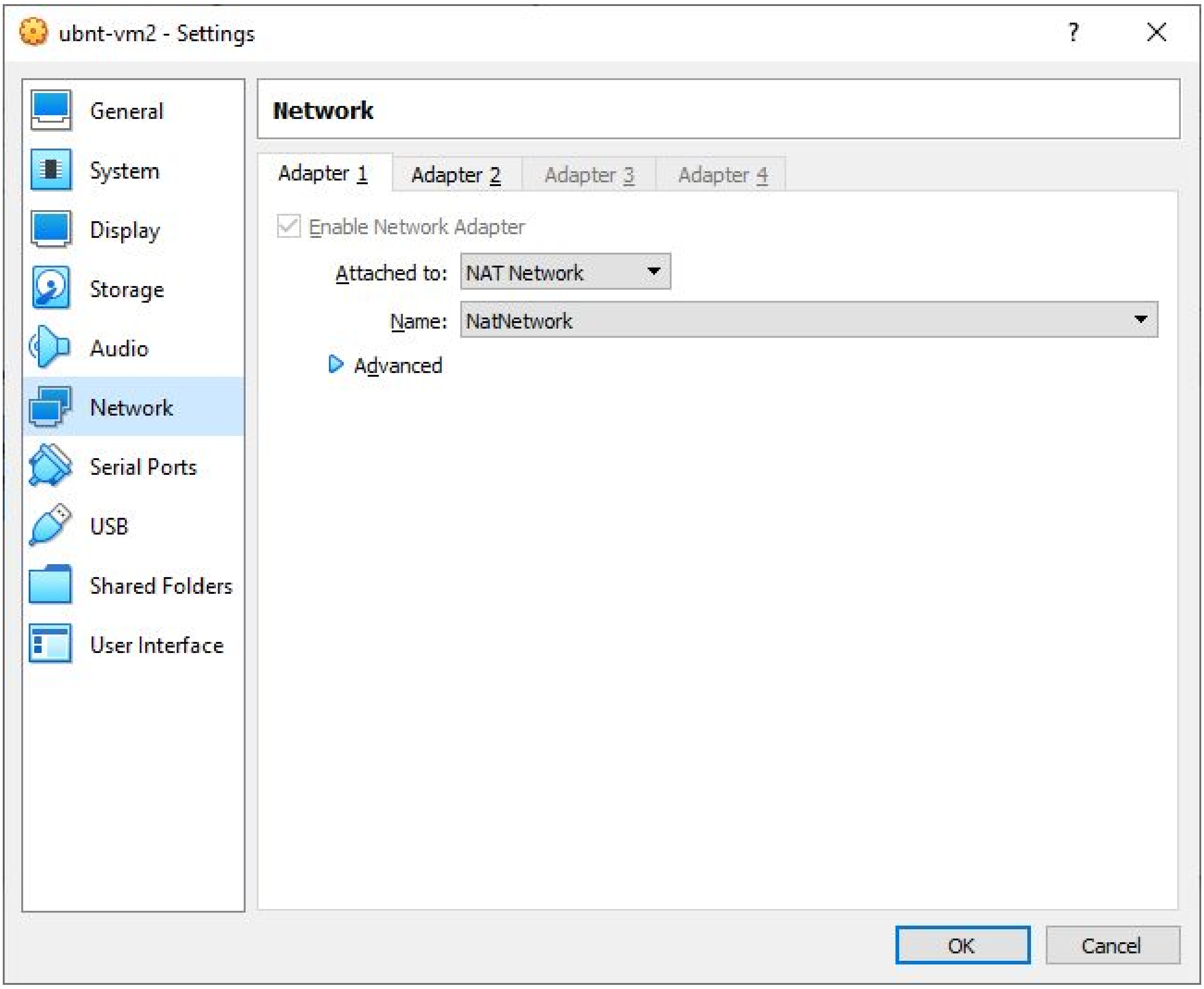
Attached to: Host-only Adapter

Name: VirtualBox Host-Only Ethernet Adapter

```
ak@deb-vm1:~$ ip addr
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
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default
qlen 1000
    link/ether 08:00:27:ab:5b:59 brd ff:ff:ff:ff:ff:ff
    inet 192.168.56.3/24 brd 192.168.56.255 scope global enp0s3
       valid_lft forever preferred_lft forever
ak@deb-vm1:~$ ip route
default via 192.168.56.2 dev enp0s3 onlink
169.254.0.0/16 dev enp0s3 scope link metric 1000
192.168.56.0/24 dev enp0s3 proto kernel scope link src 192.168.56.3
 pkts bytes target     prot opt in     out     source               destination
ak@deb-vm1:~$ traceroute google.com
traceroute to google.com (172.217.23.142), 30 hops max, 60 byte packets
 1  192.168.56.2 (192.168.56.2)  0.422 ms  0.250 ms  0.325 ms
 2  172.31.26.86 (172.31.26.86)  36.622 ms  36.816 ms  36.676 ms
 3  ec2-54-93-0-46.eu-central-1.compute.amazonaws.com (54.93.0.46)  47.956 ms
ec2-54-93-0-158.eu-central-1.compute.amazonaws.com (54.93.0.158)  47.928 ms
ec2-54-93-0-209.eu-central-1.compute.amazonaws.com (54.93.0.209)  44.673 ms
 4  100.66.8.74 (100.66.8.74)  55.296 ms 100.65.19.112 (100.65.19.112)  61.519 ms 100.65.19.48
(100.65.19.48)  61.475 ms
```

```
 5  100.66.11.132 (100.66.11.132)  54.920 ms 100.66.10.42 (100.66.10.42)  59.660 ms
100.66.10.194 (100.66.10.194)  59.414 ms
 6  100.66.10.134 (100.66.10.134)  50.905 ms 100.66.7.109 (100.66.7.109)  51.687 ms 100.66.7.5
(100.66.7.5)  44.632 ms
 7  100.66.5.71 (100.66.5.71)  51.301 ms  55.861 ms 100.66.6.11 (100.66.6.11)  49.671 ms
 8  100.65.15.9 (100.65.15.9)  38.383 ms 100.65.14.135 (100.65.14.135)  37.312 ms 100.66.5.95
(100.66.5.95)  40.516 ms
 9  100.65.14.5 (100.65.14.5)  38.214 ms 100.95.4.133 (100.95.4.133)  38.729 ms 100.95.20.135
(100.95.20.135)  38.104 ms
10  100.95.4.135 (100.95.4.135)  38.715 ms 100.100.24.54 (100.100.24.54)  38.133 ms
100.95.4.135 (100.95.4.135)  38.455 ms
11  100.95.6.17 (100.95.6.17)  53.016 ms 100.100.24.8 (100.100.24.8)  41.609 ms 100.100.24.24
(100.100.24.24)  54.939 ms
12  100.95.6.33 (100.95.6.33)  39.570 ms 150.222.194.150 (150.222.194.150)  39.409 ms
150.222.194.128 (150.222.194.128)  40.973 ms
13  52.93.23.233 (52.93.23.233)  39.054 ms 52.93.23.207 (52.93.23.207)  40.605 ms 52.93.111.11
(52.93.111.11)  43.441 ms
14  74.125.146.150 (74.125.146.150)  43.428 ms 74.125.32.106 (74.125.32.106)  43.250 ms
209.85.149.182 (209.85.149.182)  42.931 ms
15  74.125.146.150 (74.125.146.150)  44.309 ms 74.125.49.104 (74.125.49.104)  42.443 ms
74.125.146.150 (74.125.146.150)  44.184 ms
16  216.239.54.63 (216.239.54.63)  42.046 ms * 108.170.251.193 (108.170.251.193)  41.827 ms
17  209.85.241.74 (209.85.241.74)  42.610 ms 216.239.54.63 (216.239.54.63)  40.659 ms
fra16s18-in-f142.1e100.net (172.217.23.142)  41.176 ms
```

VM2 - Ubuntu 18.04 LTS (VirtualBox)



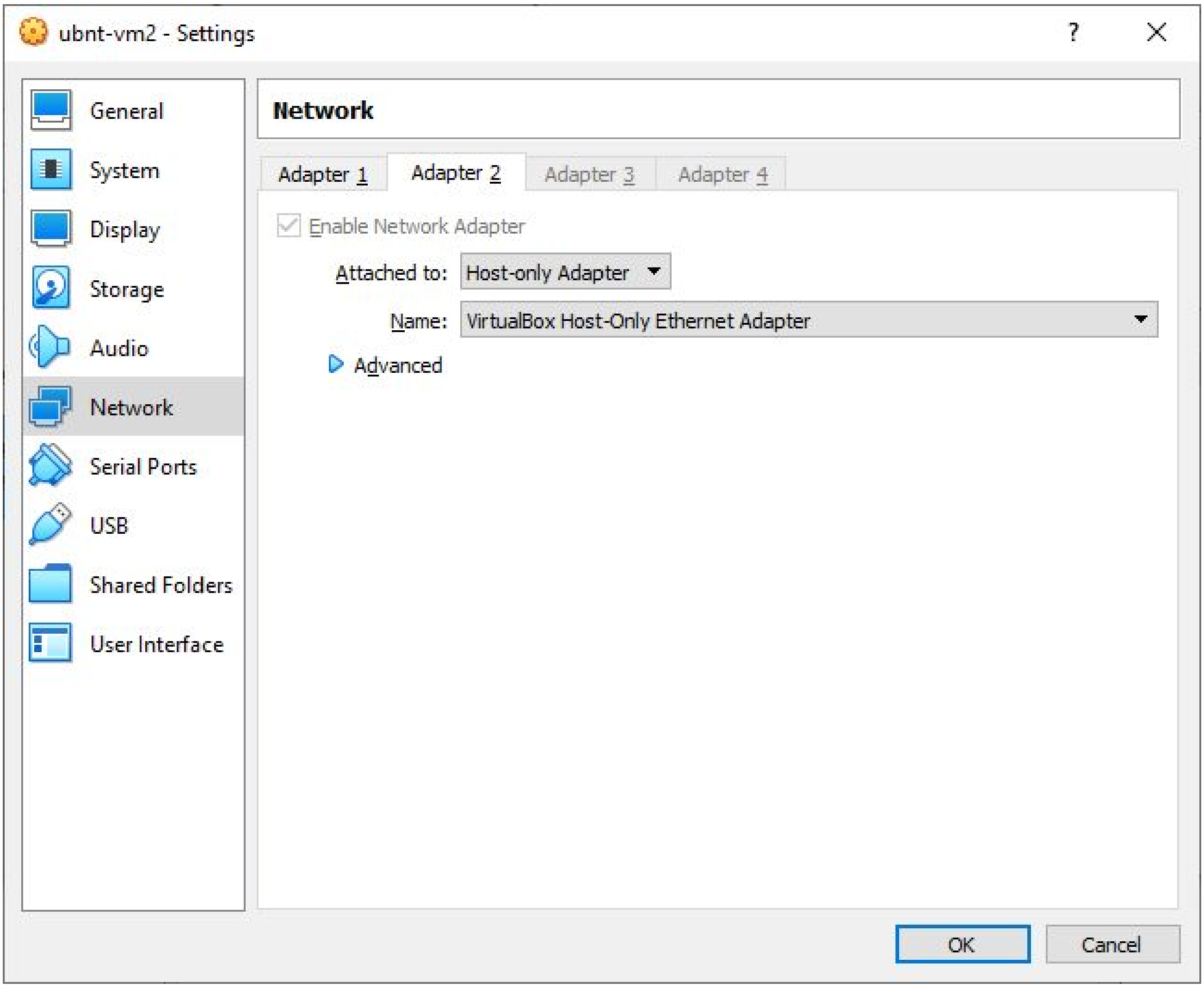
ubnt-vm2 - Settings

Network

☑ Enable Network Adapter

Attached to: NAT Network

Name: NatNetwork



☑ Enable Network Adapter

Attached to: Host-only Adapter

Name: VirtualBox Host-Only Ethernet Adapter

▷ Advanced

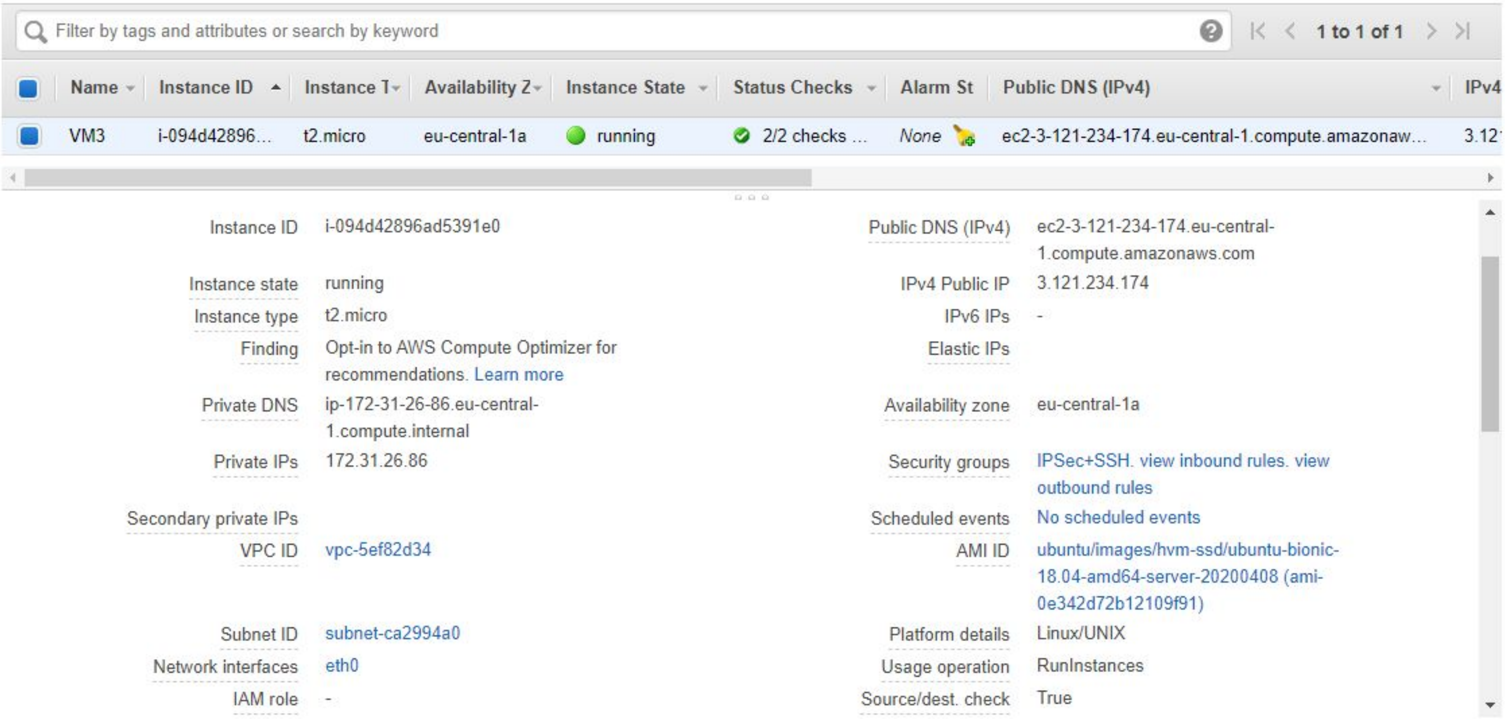
```
ak@ubnt-vm2:~$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default
qlen 1000
    link/ether 08:00:27:4a:6d:67 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.6/24 brd 10.0.2.255 scope global dynamic enp0s3
       valid_lft 486sec preferred_lft 486sec
    inet6 fe80::a00:27ff:fe4a:6d67/64 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 08:00:27:32:56:29 brd ff:ff:ff:ff:ff:ff
    inet 192.168.56.2/24 brd 192.168.56.255 scope global enp0s8
       valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fe32:5629/64 scope link
       valid_lft forever preferred_lft forever
ak@ubnt-vm2:~$ ip route
default via 10.0.2.1 dev enp0s3 proto dhcp src 10.0.2.6 metric 100
10.0.2.0/24 dev enp0s3 proto kernel scope link src 10.0.2.6
10.0.2.1 dev enp0s3 proto dhcp scope link src 10.0.2.6 metric 100
192.168.56.0/24 dev enp0s8 proto kernel scope link src 192.168.56.2
ak@ubnt-vm2:~$ sudo cat /etc/racoon/psk.txt
3.121.234.174 passwd
ak@ubnt-vm2:~$ sudo cat /etc/racoon/racoon.conf
log debug;
path pre_shared_key "/etc/racoon/psk.txt";
listen {
        isakmp 10.0.2.6 [500];
        isakmp_natt 10.0.2.6 [4500];
}
remote 3.121.234.174 {
        nat_traversal on;
        exchange_mode main;
        proposal {
                encryption_algorithm 3des;
                hash_algorithm sha1;
                authentication_method pre_shared_key;
                dh_group modp1024;
                lifetime time 86400 sec;
        }
}
sainfo anonymous {
        pfs_group modp1024;
        lifetime time 28800 sec;
        encryption_algorithm 3des;
        authentication_algorithm hmac_sha1;
        compression_algorithm deflate;
}
ak@ubnt-vm2:~$ sudo ip xfrm state
src 10.0.2.6 dst 3.121.234.174
        proto esp spi 0x07a6ce60 reqid 0 mode tunnel
        replay-window 4
        auth-trunc hmac(sha1) 0xeedb4260ddf0d046aa4a6150b0cf649a1cbf9c39 96
        enc cbc(des3_ede) 0x781df825cd6c34833e8682b926d39ff1bd8d08b5ca673ddc
        encap type espinudp sport 4500 dport 4500 addr 0.0.0.0
        anti-replay context: seq 0x0, oseq 0x2585, bitmap 0x00000000
        sel src 0.0.0.0/0 dst 0.0.0.0/0
src 3.121.234.174 dst 10.0.2.6
        proto esp spi 0x0df68cc1 reqid 0 mode tunnel
        replay-window 4
        auth-trunc hmac(sha1) 0xb977047fd162f316d270ef7e1d6b219d0f14266f 96
        enc cbc(des3_ede) 0xfecf427f181302b217ca5b3630f05e2a90c912af96b69a57
        encap type espinudp sport 4500 dport 4500 addr 0.0.0.0
        anti-replay context: seq 0x2582, oseq 0x0, bitmap 0xffffffff
        sel src 0.0.0.0/0 dst 0.0.0.0/0
ak@ubnt-vm2:~$ sudo ip xfrm policy
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 0.0.0.0/0 dst 0.0.0.0/0
        socket in priority 0
src 0.0.0.0/0 dst 192.168.56.0/24
        dir fwd priority 1
        tmpl src 3.121.234.174 dst 10.0.2.6
                proto esp reqid 0 mode tunnel
src 0.0.0.0/0 dst 192.168.56.0/24
        dir in priority 1
        mark 0x9/0xffffffff
        tmpl src 3.121.234.174 dst 10.0.2.6
                proto esp reqid 0 mode tunnel
src 192.168.56.0/24 dst 0.0.0.0/0
        dir out priority 1
        mark 0x9/0xffffffff
        tmpl src 10.0.2.6 dst 3.121.234.174
                proto esp reqid 0 mode tunnel
ak@ubnt-vm2:~$ cat ./xfrm_mark.sh
```

```
#!/bin/bash
ip xfrm policy flush
ip xfrm policy add src 192.168.56.0/24 dst 0.0.0.0/0 dir out priority 1 tmpl src 10.0.2.6 dst
3.121.234.174 proto esp reqid 0 mode tunnel mark 9
ip xfrm policy add src 0.0.0.0/0 dst 192.168.56.0/24 dir in priority 1 tmpl src 3.121.234.174
dst 10.0.2.6 proto esp reqid 0 mode tunnel mark 9
ip xfrm policy add src 0.0.0.0/0 dst 192.168.56.0/24 dir fwd priority 1 tmpl src 3.121.234.174
dst 10.0.2.6 proto esp reqid 0 mode tunnel
ak@ubnt-vm2:~$ sudo iptables -t mangle -L -n
Chain PREROUTING (policy ACCEPT)
target     prot opt source               destination
MARK       all  --  192.168.56.0/24     !192.168.56.0/24      MARK set 0x9
MARK       all  -- !192.168.56.0/24      192.168.56.0/24      MARK set 0x9

Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination

Chain POSTROUTING (policy ACCEPT)
target     prot opt source               destination
ak@ubnt-vm2:~$ sudo iptables -t nat -L -n
Chain PREROUTING (policy ACCEPT)
target     prot opt source               destination

Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination

Chain POSTROUTING (policy ACCEPT)
target     prot opt source               destination
```

In the task there was demand to block all traffic but traceroute and ssh at VM1-VM3 with firewall. If we will go strict with the task - we will broke our IPSec tunnel and DNS requests also, so I add only forward rules at VM2 to allow traceroute, ssh and DNS requests from VM1 to external networks.

```
ak@ubnt-vm2:~$ sudo iptables -t filter -L -n
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination
ACCEPT     icmp --  0.0.0.0/0            0.0.0.0/0            icmptype 3
ACCEPT     icmp --  0.0.0.0/0            0.0.0.0/0            icmptype 11
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0            tcp dpt:22
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0            tcp spt:22
ACCEPT     udp  --  0.0.0.0/0            0.0.0.0/0            udp dpt:53
ACCEPT     udp  --  0.0.0.0/0            0.0.0.0/0            udp spt:53
ACCEPT     udp  --  0.0.0.0/0            0.0.0.0/0            udp dpts:33434:33523
DROP       all  --  0.0.0.0/0            0.0.0.0/0

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
```

VM3 - Ubuntu 18.04 LTS (EC2)



Filter by tags and attributes or search by keyword

1 to 1 of 1

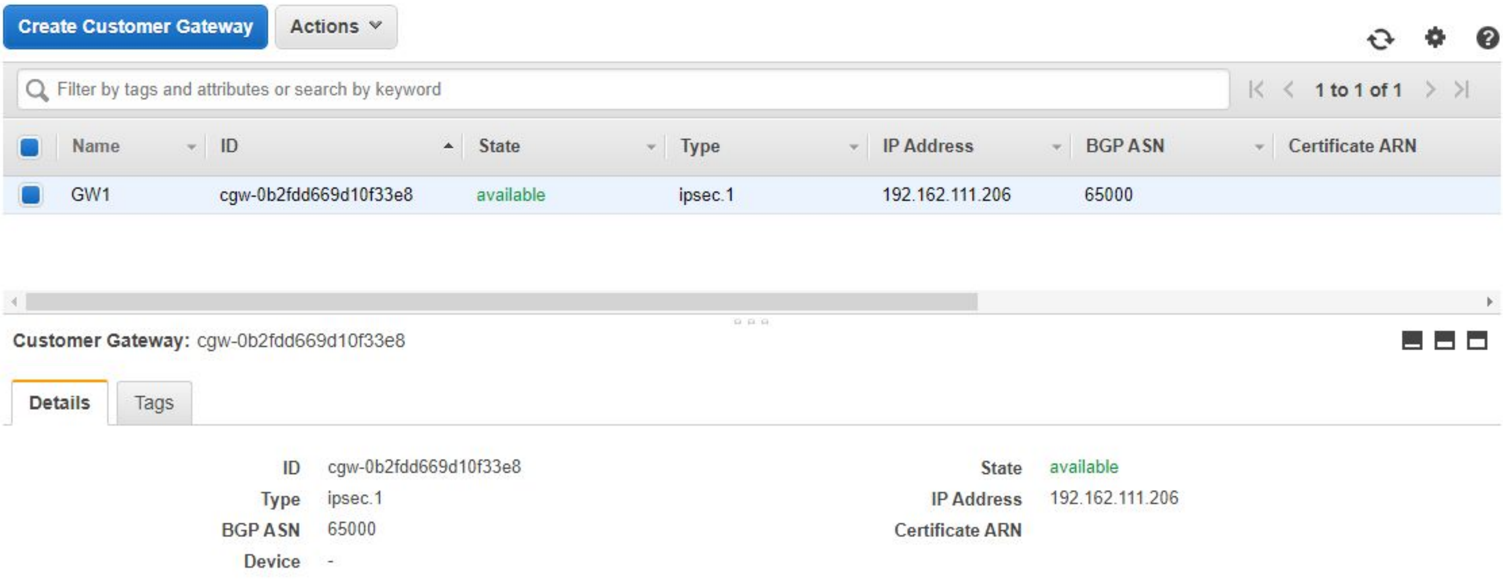
Name	Instance ID	Instance T	Availability Z	Instance State	Status Checks	Alarm St	Public DNS (IPv4)	IPv4
VM3	i-094d42896...	t2.micro	eu-central-1a	running	2/2 checks ...	None	ec2-3-121-234-174.eu-central-1.compute.amazonaw...	3.12

Instance ID	i-094d42896ad5391e0	Public DNS (IPv4)	ec2-3-121-234-174.eu-central-1.compute.amazonaws.com
Instance state	running	IPv4 Public IP	3.121.234.174
Instance type	t2.micro	IPv6 IPs	-
Finding	Opt-in to AWS Compute Optimizer for recommendations. Learn more	Elastic IPs	
Private DNS	ip-172-31-26-86.eu-central-1.compute.internal	Availability zone	eu-central-1a
Private IPs	172.31.26.86	Security groups	IPSec+SSH. view inbound rules. view outbound rules
Secondary private IPs		Scheduled events	No scheduled events
VPC ID	vpc-5ef82d34	AMI ID	ubuntu/images/hvm-ssd/ubuntu-bionic-18.04-amd64-server-20200408 (ami-0e342d72b12109f91)
Subnet ID	subnet-ca2994a0	Platform details	Linux/UNIX
Network interfaces	eth0	Usage operation	RunInstances
IAM role	-	Source/dest. check	True

```
ubuntu@ip-172-31-26-86:~$ ip addr
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: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 9001 qdisc fq_codel state UP group default qlen
1000
    link/ether 02:8d:dd:61:04:dc brd ff:ff:ff:ff:ff:ff
    inet 172.31.26.86/20 brd 172.31.31.255 scope global dynamic eth0
       valid_lft 3122sec preferred_lft 3122sec
    inet6 fe80::8d:ddff:fe61:4dc/64 scope link
       valid_lft forever preferred_lft forever
ubuntu@ip-172-31-26-86:~$ ip route
default via 172.31.16.1 dev eth0 proto dhcp src 172.31.26.86 metric 100
172.31.16.0/20 dev eth0 proto kernel scope link src 172.31.26.86
172.31.16.1 dev eth0 proto dhcp scope link src 172.31.26.86 metric 100
ubuntu@ip-172-31-26-86:~$ sudo cat /etc/racoon/psk.txt
192.162.111.0   passwd
ubuntu@ip-172-31-26-86:~$ sudo cat /etc/racoon/racoon.conf
log debug2;
path pre_shared_key "/etc/racoon/psk.txt";
listen {
        isakmp 172.31.26.86 [500];
        isakmp_natt 172.31.26.86 [4500];
}
remote 192.162.111.0 {
        nat_traversal on;
        exchange_mode main;
        proposal {
                encryption_algorithm 3des;
                hash_algorithm sha1;
                authentication_method pre_shared_key;
                dh_group modp1024;
                lifetime time 86400 sec;
        }
}
sainfo anonymous {
        pfs_group modp1024;
        lifetime time 28800 sec;
        encryption_algorithm 3des;
        authentication_algorithm hmac_sha1;
        compression_algorithm deflate;
}
ubuntu@ip-172-31-26-86:~$ sudo ip xfrm state
src 172.31.26.86 dst 192.162.111.0
        proto esp spi 0x000f7622 reqid 0 mode tunnel
        replay-window 4
        auth-trunc hmac(sha1) 0x0f63c4588115bc5dd01811d9f43a98e2228728aa 96
        enc cbc(des3_ede) 0x55a66319ec36df31cc6fc5e990968819def63f95ad60ec4a
        encap type espinudp sport 4500 dport 30300 addr 0.0.0.0
        anti-replay context: seq 0x0, oseq 0x8, bitmap 0x00000000
        sel src 0.0.0.0/0 dst 0.0.0.0/0
src 192.162.111.0 dst 172.31.26.86
        proto esp spi 0x0e280dbb reqid 0 mode tunnel
        replay-window 4
        auth-trunc hmac(sha1) 0xba6fb3af27dc76242df5b7e1599cf0dacfb97180 96
        enc cbc(des3_ede) 0x30a7dee5a51b6c3a8fb8635cedbf47938c631f7908db3f43
        encap type espinudp sport 30300 dport 4500 addr 0.0.0.0
        anti-replay context: seq 0x8, oseq 0x0, bitmap 0x000000ff
        sel src 0.0.0.0/0 dst 0.0.0.0/0
ubuntu@ip-172-31-26-86:~$ sudo ip xfrm policy
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 0.0.0.0/0 dst 0.0.0.0/0
        socket in priority 0
src 0.0.0.0/0 dst 192.168.56.0/24
        dir out priority 1
        tmpl src 172.31.26.86 dst 192.162.111.0
                proto esp reqid 0 mode tunnel
src 192.168.56.0/24 dst 0.0.0.0/0
        dir fwd priority 1
        tmpl src 192.162.111.0 dst 172.31.26.86
                proto esp reqid 0 mode tunnel
src 192.168.56.0/24 dst 0.0.0.0/0
        dir in priority 1
        tmpl src 192.162.111.0 dst 172.31.26.86
                proto esp reqid 0 mode tunnel
ubuntu@ip-172-31-26-86:~$ cat ./xfrm.sh
#!/bin/bash
ip xfrm policy flush
ip xfrm policy add src 192.168.56.0/24 dst 0.0.0.0/0 dir in priority 1 tmpl src 192.162.111.0
dst 172.31.26.86 proto esp reqid 0 mode tunnel
ip xfrm policy add src 192.168.56.0/24 dst 0.0.0.0/0 dir fwd priority 1 tmpl src 192.162.111.0
dst 172.31.26.86 proto esp reqid 0 mode tunnel
ip xfrm policy add src 0.0.0.0/0 dst 192.168.56.0/24 dir out priority 1 tmpl src 172.31.26.86
dst 192.162.111.0 proto esp reqid 0 mode tunnel
ubuntu@ip-172-31-26-86:~$ sudo iptables -t mangle -L -n
Chain PREROUTING (policy ACCEPT)
target     prot opt source               destination

Chain INPUT (policy ACCEPT)
target     prot opt source               destination
```

```
Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination

Chain POSTROUTING (policy ACCEPT)
target     prot opt source               destination
ubuntu@ip-172-31-26-86:~$ sudo iptables -t nat -L -n
Chain PREROUTING (policy ACCEPT)
target     prot opt source               destination

Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination

Chain POSTROUTING (policy ACCEPT)
target     prot opt source               destination
MASQUERADE  all  --  192.168.56.0/24      0.0.0.0/0
```

AWS site-2-site VPN (bonus task)

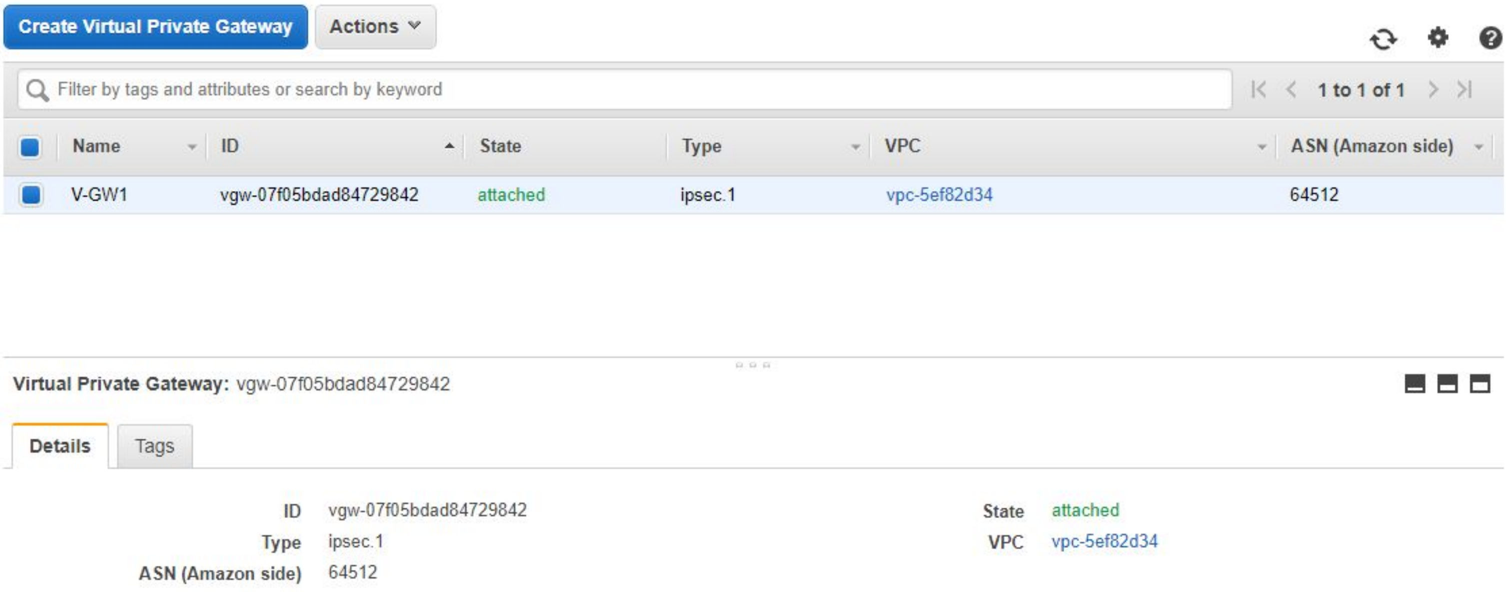


Name	ID	State	Type	IP Address	BGP ASN	Certificate ARN
GW1	cgw-0b2fdd669d10f33e8	available	ipsec.1	192.162.111.206	65000	

Customer Gateway: cgw-0b2fdd669d10f33e8

ID cgw-0b2fdd669d10f33e8
Type ipsec.1
BGP ASN 65000
Device -

State available
IP Address 192.162.111.206
Certificate ARN



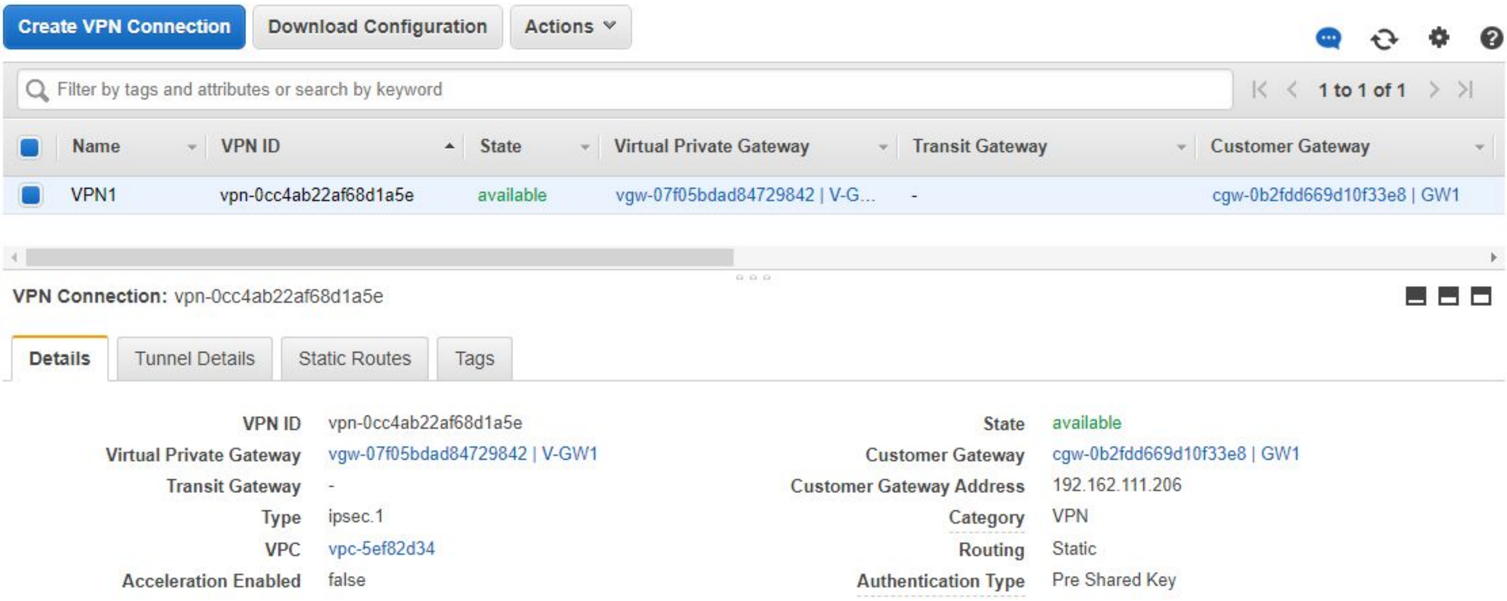
Create Virtual Private Gateway
Actions
Filter by tags and attributes or search by keyword
1 to 1 of 1

Name	ID	State	Type	VPC	ASN (Amazon side)
V-GW1	vgw-07f05bdad84729842	attached	ipsec.1	vpc-5ef82d34	64512

Virtual Private Gateway: vgw-07f05bdad84729842

ID vgw-07f05bdad84729842
Type ipsec.1
ASN (Amazon side) 64512

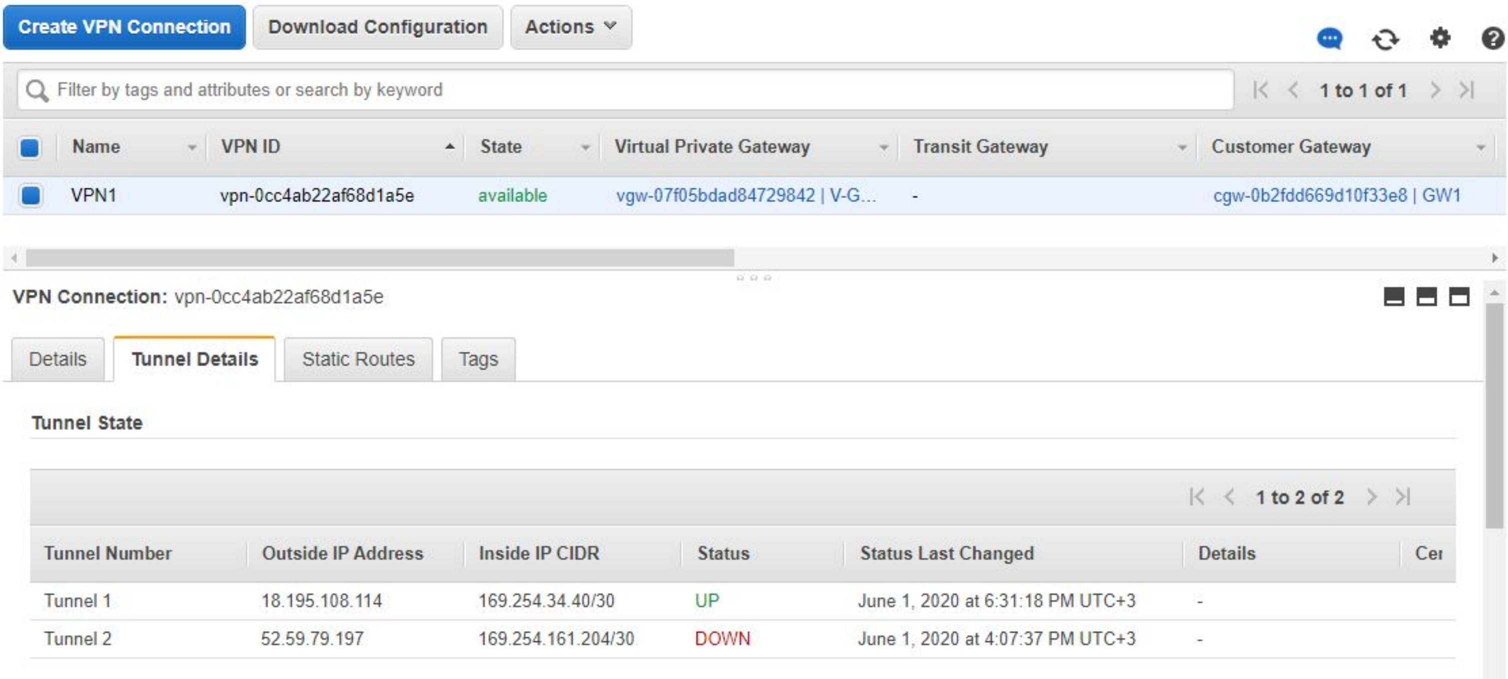
State attached
VPC vpc-5ef82d34



Name	VPN ID	State	Virtual Private Gateway	Transit Gateway	Customer Gateway
VPN1	vpn-0cc4ab22af68d1a5e	available	vgw-07f05bdad84729842 | V-G...	-	cgw-0b2fdd669d10f33e8 | GW1

VPN Connection: vpn-0cc4ab22af68d1a5e

VPN ID	vpn-0cc4ab22af68d1a5e	State	available
Virtual Private Gateway	vgw-07f05bdad84729842 | V-GW1	Customer Gateway	cgw-0b2fdd669d10f33e8 | GW1
Transit Gateway	-	Customer Gateway Address	192.162.111.206
Type	ipsec.1	Category	VPN
VPC	vpc-5ef82d34	Routing	Static
Acceleration Enabled	false	Authentication Type	Pre Shared Key

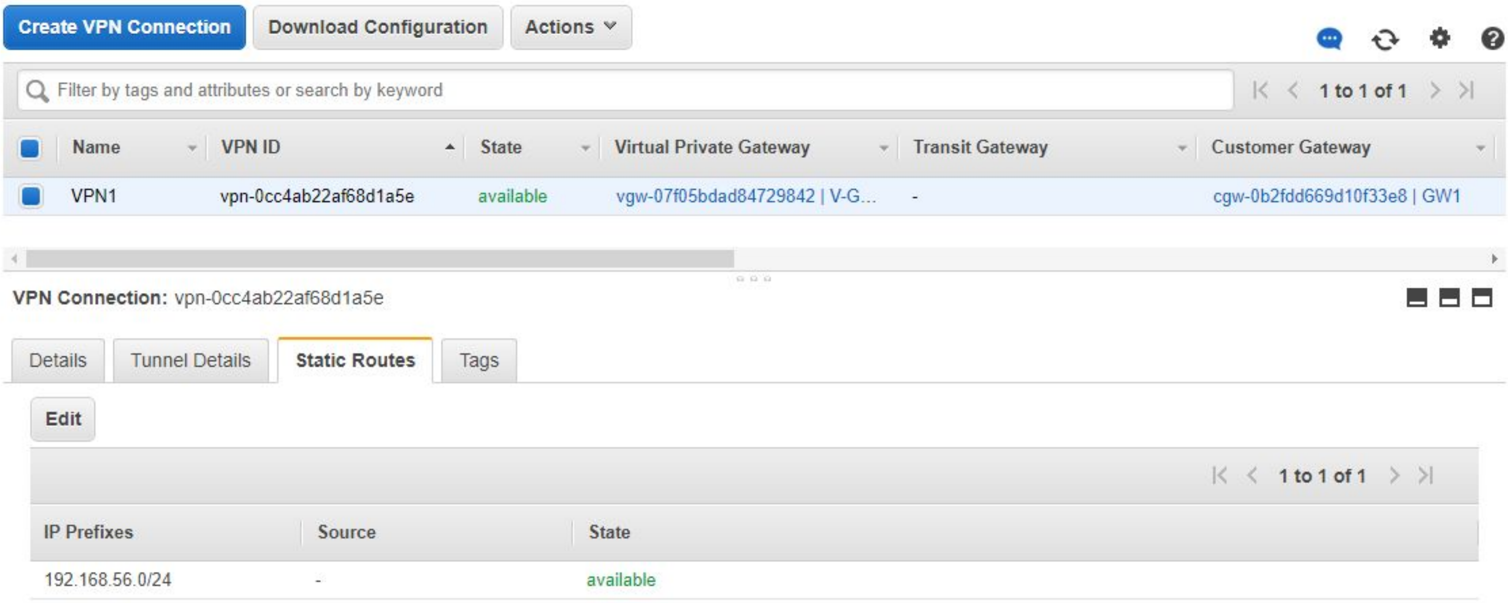


Name	VPN ID	State	Virtual Private Gateway	Transit Gateway	Customer Gateway
VPN1	vpn-0cc4ab22af68d1a5e	available	vgw-07f05bdad84729842 | V-G...	-	cgw-0b2fdd669d10f33e8 | GW1

VPN Connection: vpn-0cc4ab22af68d1a5e

Tunnel State

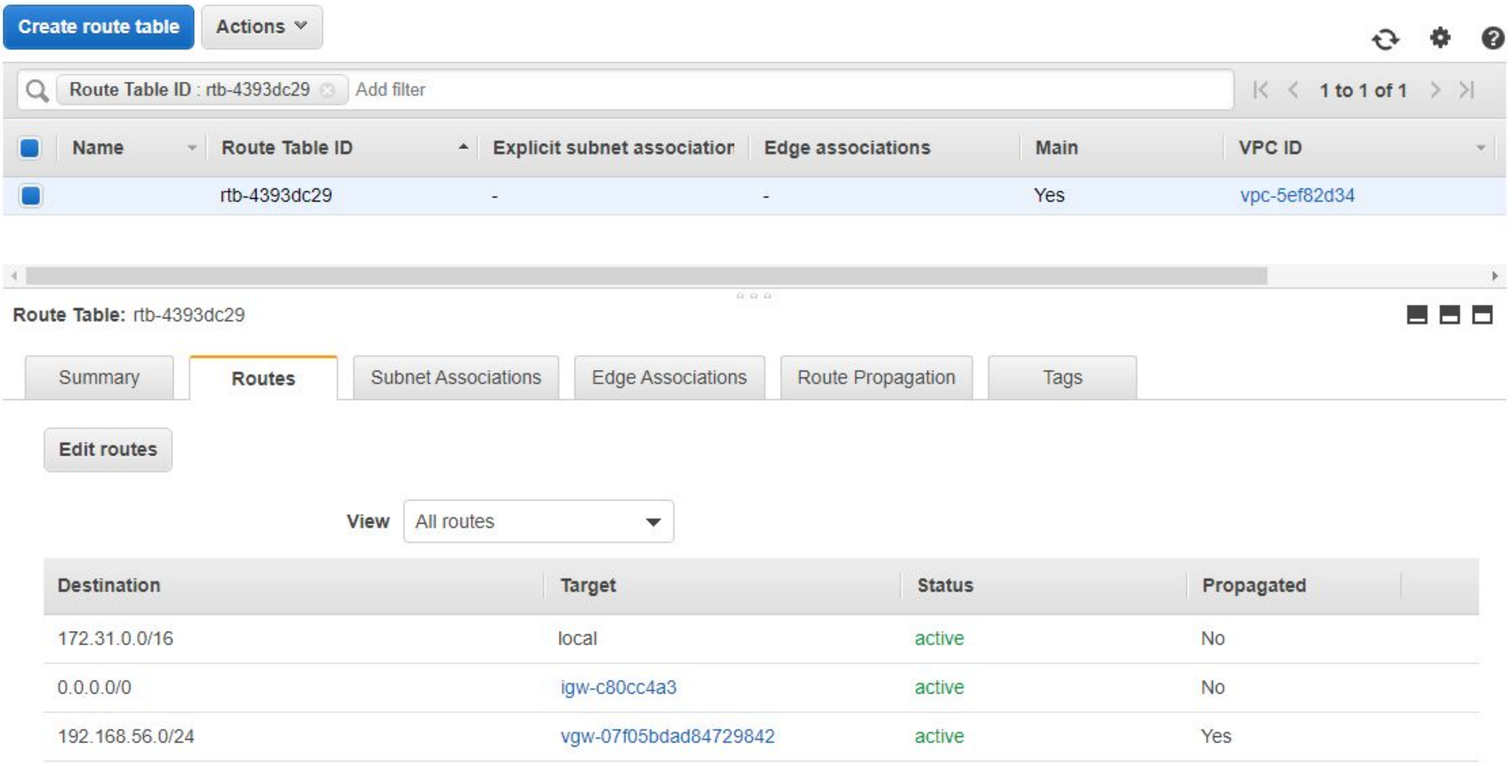
Tunnel Number	Outside IP Address	Inside IP CIDR	Status	Status Last Changed	Details	Cer
Tunnel 1	18.195.108.114	169.254.34.40/30	UP	June 1, 2020 at 6:31:18 PM UTC+3	-	
Tunnel 2	52.59.79.197	169.254.161.204/30	DOWN	June 1, 2020 at 4:07:37 PM UTC+3	-	



Name	VPN ID	State	Virtual Private Gateway	Transit Gateway	Customer Gateway
VPN1	vpn-0cc4ab22af68d1a5e	available	vgw-07f05bdad84729842 | V-G...	-	cgw-0b2fdd669d10f33e8 | GW1

VPN Connection: vpn-0cc4ab22af68d1a5e

IP Prefixes	Source	State
192.168.56.0/24	-	available



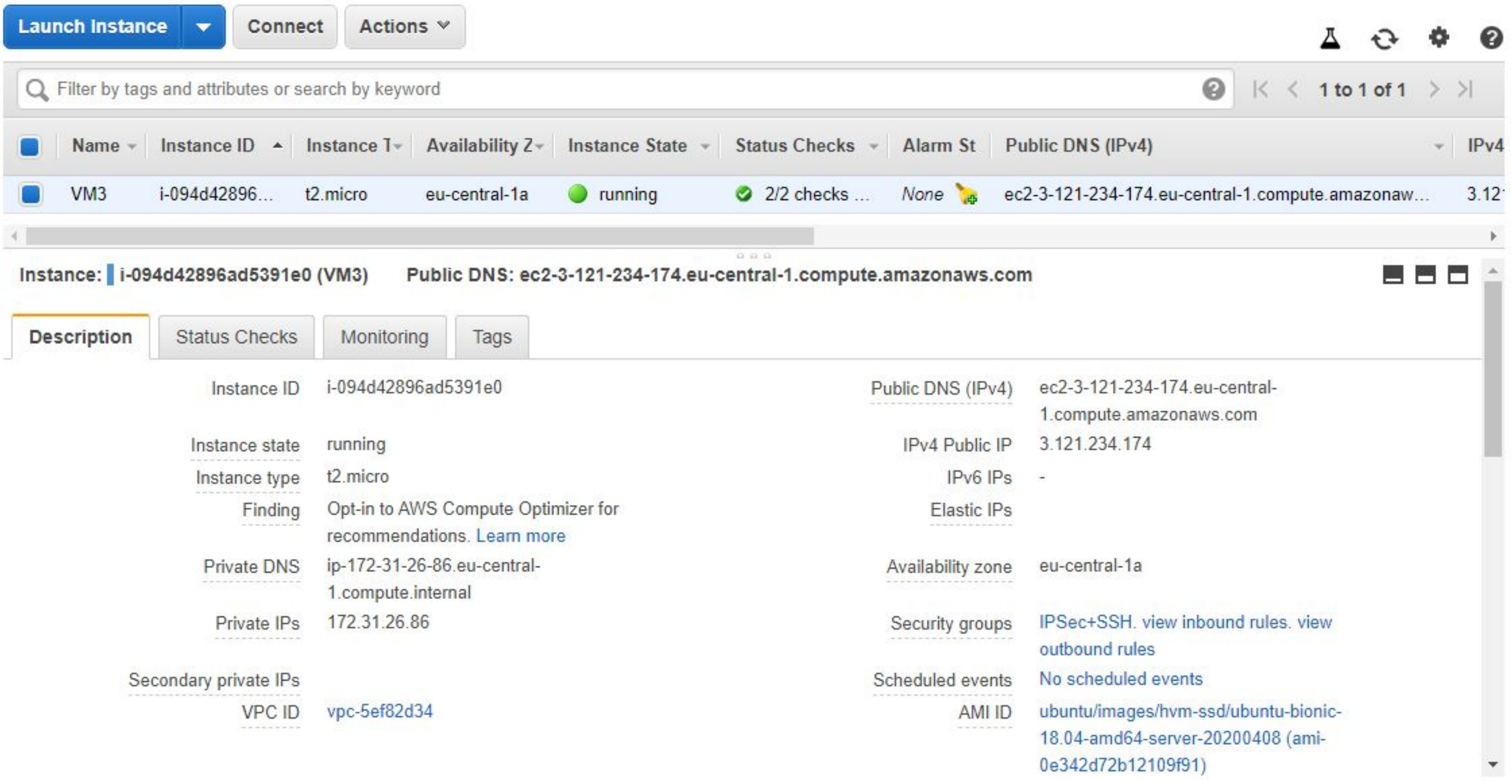
Route Table ID : rtb-4393dc29

Name	Route Table ID	Explicit subnet associatior	Edge associations	Main	VPC ID
	rtb-4393dc29	-	-	Yes	vpc-5ef82d34

Route Table: rtb-4393dc29

View: All routes

Destination	Target	Status	Propagated
172.31.0.0/16	local	active	No
0.0.0.0/0	igw-c80cc4a3	active	No
192.168.56.0/24	vgw-07f05bdad84729842	active	Yes



Name	Instance ID	Instance T	Availability Z	Instance State	Status Checks	Alarm St	Public DNS (IPv4)	IPv4
VM3	i-094d42896...	t2.micro	eu-central-1a	running	2/2 checks ...	None	ec2-3-121-234-174.eu-central-1.compute.amazonaw...	3.12

Instance: i-094d42896ad5391e0 (VM3) Public DNS: ec2-3-121-234-174.eu-central-1.compute.amazonaws.com

Instance ID	i-094d42896ad5391e0	Public DNS (IPv4)	ec2-3-121-234-174.eu-central-1.compute.amazonaws.com
Instance state	running	IPv4 Public IP	3.121.234.174
Instance type	t2.micro	IPv6 IPs	-
Finding	Opt-in to AWS Compute Optimizer for recommendations. Learn more	Elastic IPs	
Private DNS	ip-172-31-26-86.eu-central-1.compute.internal	Availability zone	eu-central-1a
Private IPs	172.31.26.86	Security groups	IPSec+SSH. view inbound rules. view outbound rules
Secondary private IPs		Scheduled events	No scheduled events
VPC ID	vpc-5ef82d34	AMI ID	ubuntu/images/hvm-ssd/ubuntu-bionic-18.04-amd64-server-20200408 (ami-0e342d72b12109f91)

VM1 - Debian 10 (VirtualBox)

```
ak@deb-vm1:~$ uname -a
Linux deb-vm1 4.19.0-9-amd64 #1 SMP Debian 4.19.118-2 (2020-04-29) x86_64 GNU/Linux
ak@deb-vm1:~$ ip addr
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
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default
qlen 1000
    link/ether 08:00:27:ab:5b:59 brd ff:ff:ff:ff:ff:ff
    inet 192.168.56.3/24 brd 192.168.56.255 scope global enp0s3
       valid_lft forever preferred_lft forever
ak@deb-vm1:~$ ip route
```

```
default via 192.168.56.2 dev enp0s3 onlink
169.254.0.0/16 dev enp0s3 scope link metric 1000
192.168.56.0/24 dev enp0s3 proto kernel scope link src 192.168.56.3
ak@deb-vm1:~$ ping -c 4 172.31.26.86
PING 172.31.26.86 (172.31.26.86) 56(84) bytes of data.
64 bytes from 172.31.26.86: icmp_seq=1 ttl=63 time=48.8 ms
64 bytes from 172.31.26.86: icmp_seq=2 ttl=63 time=45.2 ms
64 bytes from 172.31.26.86: icmp_seq=3 ttl=63 time=75.5 ms
64 bytes from 172.31.26.86: icmp_seq=4 ttl=63 time=39.4 ms

--- 172.31.26.86 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 8ms
rtt min/avg/max/mdev = 39.388/52.210/75.460/13.836 ms
```

VM2 - Ubuntu 18.04 LTS (VirtualBox)

```
ak@ubnt-vm2:~$ uname -a
Linux ubnt-vm2 4.15.0-101-generic #102-Ubuntu SMP Mon May 11 10:07:26 UTC 2020 x86_64 x86_64
x86_64 GNU/Linux
ak@ubnt-vm2:~$ ip addr
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
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default
qlen 1000
    link/ether 08:00:27:4a:6d:67 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.6/24 brd 10.0.2.255 scope global dynamic enp0s3
       valid_lft 399sec preferred_lft 399sec
    inet6 fe80::a00:27ff:fe4a:6d67/64 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 08:00:27:32:56:29 brd ff:ff:ff:ff:ff:ff
    inet 192.168.56.2/24 brd 192.168.56.255 scope global enp0s8
       valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fe32:5629/64 scope link
       valid_lft forever preferred_lft forever
4: ip_vti0@NONE: <NOARP> mtu 1480 qdisc noop state DOWN group default qlen 1000
    link/ipip 0.0.0.0 brd 0.0.0.0
5: Tunnel1@NONE: <POINTOPOINT,NOARP,UP,LOWER_UP> mtu 1419 qdisc noqueue state UNKNOWN group
default qlen 1000
    link/ipip 10.0.2.6 peer 18.195.108.114
    inet 169.254.34.42 peer 169.254.34.41/30 scope global Tunnel1
       valid_lft forever preferred_lft forever
ak@ubnt-vm2:~$ ip route
default via 10.0.2.1 dev enp0s3 proto dhcp src 10.0.2.6 metric 100
10.0.2.0/24 dev enp0s3 proto kernel scope link src 10.0.2.6
10.0.2.1 dev enp0s3 proto dhcp scope link src 10.0.2.6 metric 100
169.254.34.40/30 dev Tunnel1 proto kernel scope link src 169.254.34.42
172.31.0.0/16 dev Tunnel1 scope link metric 100
192.168.56.0/24 dev enp0s8 proto kernel scope link src 192.168.56.2
ak@ubnt-vm2:~$ sudo iptables -t mangle -L -n
Chain PREROUTING (policy ACCEPT)
target     prot opt source               destination

Chain INPUT (policy ACCEPT)
target     prot opt source               destination
MARK       esp  --  18.195.108.114       10.0.2.6             MARK set 0x64

Chain FORWARD (policy ACCEPT)
```

```
target     prot opt source               destination
TCPMSS     tcp  --  0.0.0.0/0            0.0.0.0/0            tcp flags:0x06/0x02 TCPMSS clamp
to PMTU

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination

Chain POSTROUTING (policy ACCEPT)
target     prot opt source               destination
ak@ubnt-vm2:~$ sudo ipsec statusall
Status of IKE charon daemon (strongSwan 5.6.2, Linux 4.15.0-101-generic, x86_64):
  uptime: 94 minutes, since Jun 01 18:30:40 2020
  malloc: sbrk 1630208, mmap 0, used 745360, free 884848
  worker threads: 11 of 16 idle, 5/0/0/0 working, job queue: 0/0/0/0, scheduled: 6
  loaded plugins: charon 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:
  10.0.2.6
  192.168.56.2
  169.254.34.42
Connections:
     Tunnel1:  %any...18.195.108.114  IKEv1, dpddelay=10s
     Tunnel1:   local:  [192.162.111.206] uses pre-shared key authentication
     Tunnel1:   remote: [18.195.108.114] uses pre-shared key authentication
     Tunnel1:   child:  0.0.0.0/0 === 0.0.0.0/0 TUNNEL, dpdaction=restart
Security Associations (1 up, 0 connecting):
     Tunnel1[1]: ESTABLISHED 94 minutes ago,
10.0.2.6[192.162.111.206]...18.195.108.114[18.195.108.114]
     Tunnel1[1]: IKEv1 SPIs: 1839cf37070ee47d_i* 55f9ec8be5d6bc01_r, pre-shared key
reauthentication in 6 hours
     Tunnel1[1]: IKE proposal: AES_CBC_128/HMAC_SHA1_96/PRF_HMAC_SHA1/MODP_1024
     Tunnel1{2}:  REKEYED, TUNNEL, reqid 1, expires in 9 minutes
     Tunnel1{2}:   0.0.0.0/0 === 0.0.0.0/0
     Tunnel1{3}:  INSTALLED, TUNNEL, reqid 1, ESP in UDP SPIs: c9987827_i 42d43019_o
     Tunnel1{3}:  AES_CBC_128/HMAC_SHA1_96/MODP_1024, 1105524 bytes_i, 1106112 bytes_o (13168
pkts, 0s ago), rekeying in 43 minutes
     Tunnel1{3}:   0.0.0.0/0 === 0.0.0.0/0
ak@ubnt-vm2:~$ sudo ip xfrm state
src 10.0.2.6 dst 18.195.108.114
        proto esp spi 0xebb96f91 reqid 1 mode tunnel
        replay-window 0 flag af-unspec
        mark 0x64/0xffffffff
        auth-trunc hmac(sha1) 0xb92889486c2a1a74ca8dc12c23b348185d7cbad4 96
        enc cbc(aes) 0xd26b8c3c5dc78c440ed8fad444854eea
        encap type espinudp sport 4500 dport 4500 addr 0.0.0.0
        anti-replay context: seq 0x0, oseq 0x3a, bitmap 0x00000000
src 18.195.108.114 dst 10.0.2.6
        proto esp spi 0xccb40d5a reqid 1 mode tunnel
        replay-window 32 flag af-unspec
        auth-trunc hmac(sha1) 0x33984c37e838dc7ff38964c9881edde3ff4dad4d 96
        enc cbc(aes) 0xe1ebde179d064e0dd8dcef35fc832751
        encap type espinudp sport 4500 dport 4500 addr 0.0.0.0
        anti-replay context: seq 0x37, oseq 0x0, bitmap 0xffffffff
ak@ubnt-vm2:~$ sudo ip xfrm policy
src 0.0.0.0/0 dst 0.0.0.0/0
        dir out priority 399999
        mark 0x64/0xffffffff
        tmpl src 10.0.2.6 dst 18.195.108.114
                proto esp spi 0x42d43019 reqid 1 mode tunnel
```

```
src 0.0.0.0/0 dst 0.0.0.0/0
        dir fwd priority 399999
        mark 0x64/0xffffffff
        tmpl src 18.195.108.114 dst 10.0.2.6
                proto esp reqid 1 mode tunnel
src 0.0.0.0/0 dst 0.0.0.0/0
        dir in priority 399999
        mark 0x64/0xffffffff
        tmpl src 18.195.108.114 dst 10.0.2.6
                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
ak@ubnt-vm2:~$ ping -c 4 -I 192.168.56.2 172.31.26.86
PING 172.31.26.86 (172.31.26.86) from 192.168.56.2 : 56(84) bytes of data.
64 bytes from 172.31.26.86: icmp_seq=1 ttl=64 time=39.7 ms
64 bytes from 172.31.26.86: icmp_seq=2 ttl=64 time=79.3 ms
64 bytes from 172.31.26.86: icmp_seq=3 ttl=64 time=40.9 ms
64 bytes from 172.31.26.86: icmp_seq=4 ttl=64 time=39.3 ms

--- 172.31.26.86 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 39.355/49.848/79.300/17.015 ms
```

VM3 - Ubuntu 18.04 LTS (EC2)

```
ubuntu@ip-172-31-26-86:~$ uname -a
Linux ip-172-31-26-86 5.3.0-1019-aws #21~18.04.1-Ubuntu SMP Mon May 11 12:33:03 UTC 2020
x86_64 x86_64 x86_64 GNU/Linux
ubuntu@ip-172-31-26-86:~$ ip addr
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: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 9001 qdisc fq_codel state UP group default qlen
1000
    link/ether 02:8d:dd:61:04:dc brd ff:ff:ff:ff:ff:ff
    inet 172.31.26.86/20 brd 172.31.31.255 scope global dynamic eth0
       valid_lft 2215sec preferred_lft 2215sec
    inet6 fe80::8d:ddff:fe61:4dc/64 scope link
       valid_lft forever preferred_lft forever
ubuntu@ip-172-31-26-86:~$ ip route
default via 172.31.16.1 dev eth0 proto dhcp src 172.31.26.86 metric 100
172.31.16.0/20 dev eth0 proto kernel scope link src 172.31.26.86
172.31.16.1 dev eth0 proto dhcp scope link src 172.31.26.86 metric 100
ubuntu@ip-172-31-26-86:~$ ping -c 4 192.168.56.3
```

```
PING 192.168.56.3 (192.168.56.3) 56(84) bytes of data.
64 bytes from 192.168.56.3: icmp_seq=1 ttl=63 time=39.1 ms
64 bytes from 192.168.56.3: icmp_seq=2 ttl=63 time=42.3 ms
64 bytes from 192.168.56.3: icmp_seq=3 ttl=63 time=47.7 ms
64 bytes from 192.168.56.3: icmp_seq=4 ttl=63 time=40.3 ms

--- 192.168.56.3 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 39.191/42.415/47.751/3.277 ms
ubuntu@ip-172-31-26-86:~$ ping -c 4 192.168.56.2
PING 192.168.56.2 (192.168.56.2) 56(84) bytes of data.
64 bytes from 192.168.56.2: icmp_seq=1 ttl=64 time=38.4 ms
64 bytes from 192.168.56.2: icmp_seq=2 ttl=64 time=38.4 ms
64 bytes from 192.168.56.2: icmp_seq=3 ttl=64 time=38.3 ms
64 bytes from 192.168.56.2: icmp_seq=4 ttl=64 time=39.1 ms

--- 192.168.56.2 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 38.332/38.602/39.158/0.353 ms
```