Google Cloud VPN Interop Guide

Using Cloud VPN With VyOS

Disclaimer: This interoperability guide is intended to be informational in nature and contains examples only. Customers should verify this information via testing.

Contents

- Contents
- Introduction
- Environment Overview
- Topology
- Preparation
  - Overview
  - Getting Started
  - IPsec Parameters
- Configuration
  - Configuration - GCP
    - Verifying the GCP Configuration
    - Updating the Firewall Rules in GCP
  - Configuration - VyOS
    - Prerequisites
    - Entering Configuration Mode
    - IPsec ESP Configuration
    - Saving the Configuration
- Testing the IPsec connection
- Troubleshooting the IPsec connection
  - Resetting the IPsec connection

Introduction

This guide walks you through the process of configuring VyOS, a Linux-based network operating system that provides software-based network routing, firewall, and VPN functionality, for integration with Google Cloud VPN. This information is provided as an example only. This guide is not meant to be a comprehensive overview of IPsec and assumes that you have basic familiarity with the IPsec protocol.

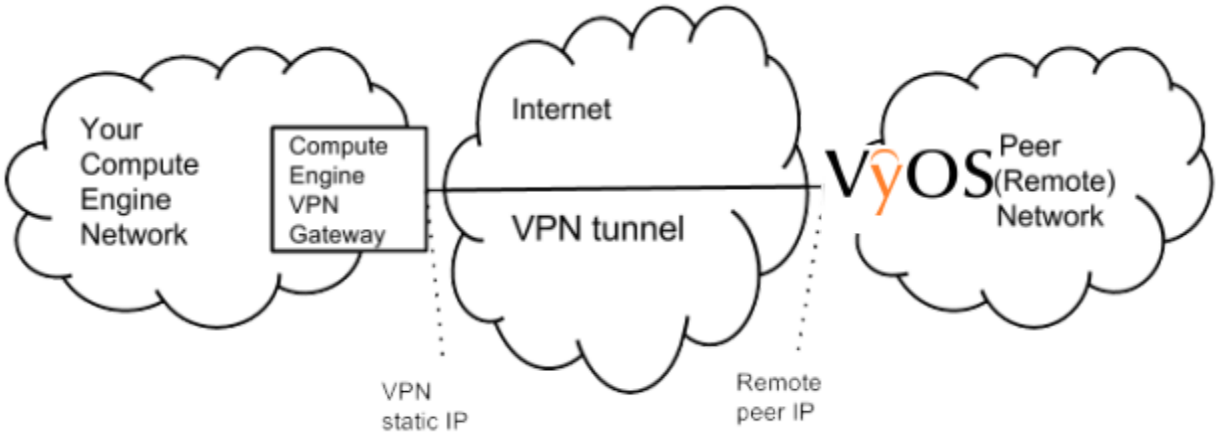
Environment overview

The following equipment was used in the creation of this guide:

Vendor:	VyOS
Model:	amd64.iso
Software Rev:	1.1.7

Topology

The topology outlined by this guide is a basic site-to-site IPsec VPN tunnel configuration using the referenced device:



Preparation

Overview

The configuration samples that follow include many value substitutions that are provided only as examples. Using values that are appropriate to your environment, replace any references to IP addresses, device IDs, shared secrets or keys, account information, or project names. Values unique to your environment are highlighted in **bold**.

This guide is not meant to be a comprehensive setup overview for the device referenced, but rather is intended to help you establish IPsec connectivity to Google Compute Engine. The following is a high-level overview of the configuration process that this guide covers:

- Select the appropriate IPsec configuration.
- Configure the internet facing interface of your device (outside interface).
- Configure IKEv2 and IPsec.
- Test the tunnel.

Getting started

The first step in configuring your VyOS virtual route for use with the Google Cloud VPN service is to ensure that you meet the following prerequisite conditions:

- VyOS is successfully deployed to either virtual or physical hardware. Installation is out of scope for this guide, but you can find detailed instructions at the VyOS project homepage.
- You have at least one configured and verified functional *internal* interface.
- You have one configured and verified functional *external* interface.

IPsec parameters

For the VyOS Router IPsec configuration, use the following details:

Parameter	Value
IPsec Mode	ESP+Auth Tunnel mode (Site-to-Site)
Auth Protocol	Pre-shared Key
Key Exchange	IKEv2
Start	auto
Perfect Forward Secrecy (PFS)	on
Dead Peer Detection (DPD)	aggressive
INITIAL_CONTACT (uniqueids)	on

The IPsec configuration used in this guide is specified below:

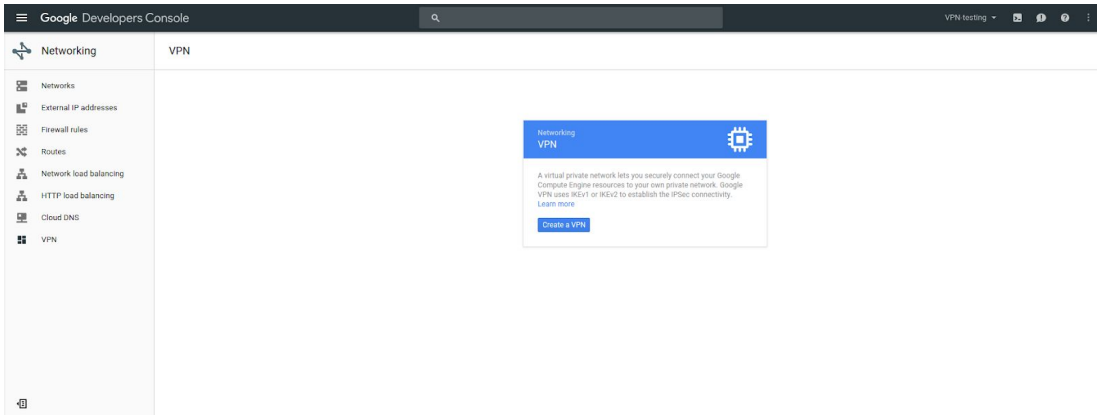
Phase	Cipher role	Cipher
Phase 1	Encryption	aes-256
	Integrity	sha-256
	prf	sha1-96
	Diffie-Hellman (DH)	Group 14 (modp_2048)
	Phase 1 lifetime	36,000 seconds (10 hours)
Phase 2	Encryption	aes-cbc-256
	Integrity	sha-256
	Phase 2 lifetime	10,800 seconds (3 hours)

Configuration

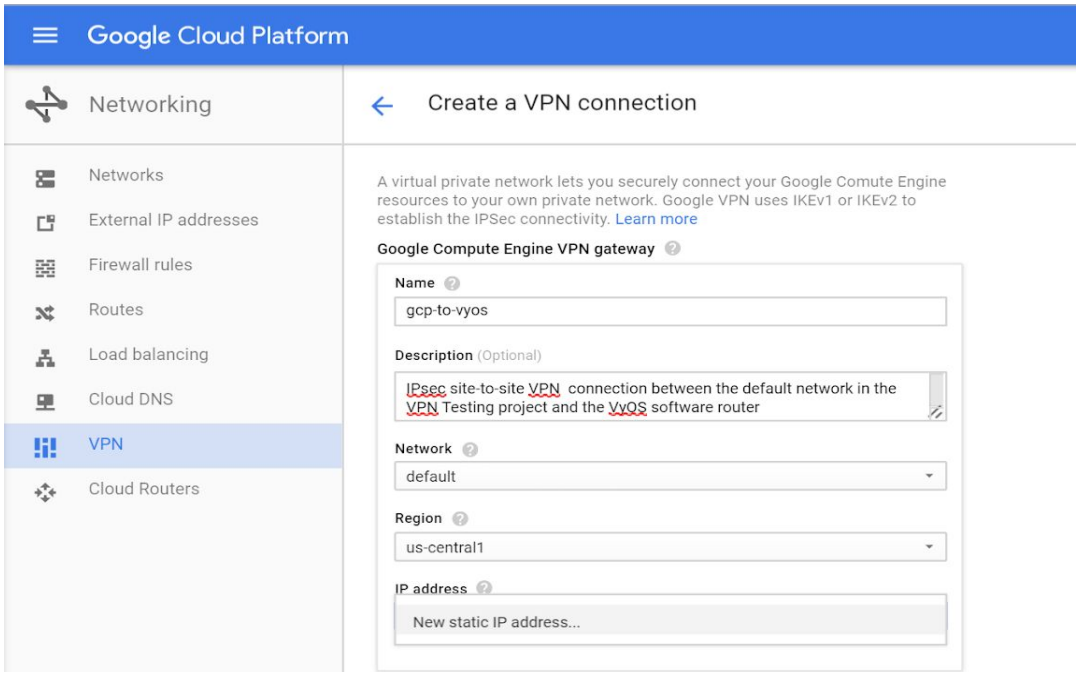
Configuring GCP

This section walks through the Google Cloud VPN configuration. Sign in to the Google Cloud Platform Console and select Hybrid Connectivity from the main menu.

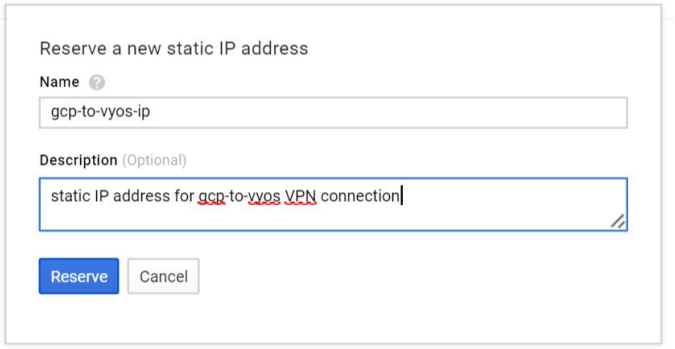
1. Create a new VPN instance. Select the VPN node and click **Create a VPN** from the main task pane:



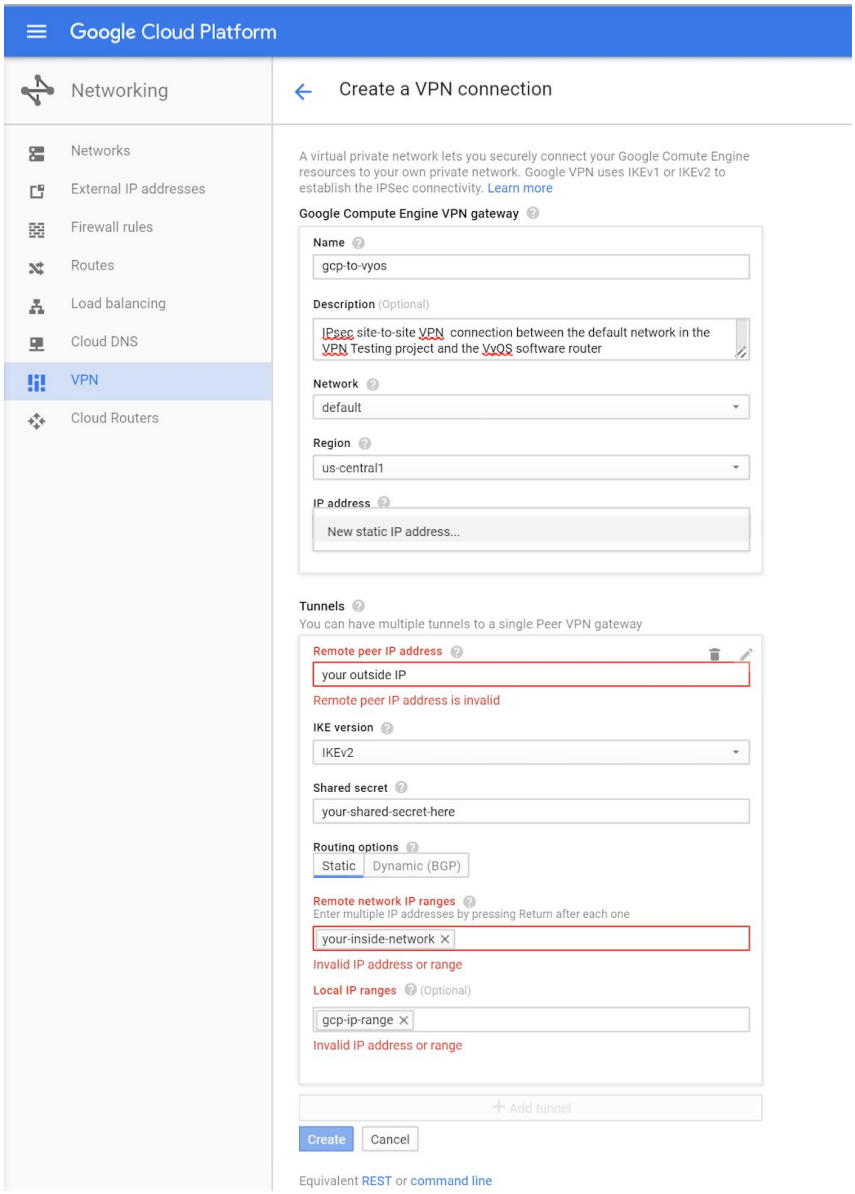
2. On this page, you enter all the parameters that you need to create a new VPN connection. Provide a name and description for the VPN instance, and provide a public IP address for the VPN instance. You can select an existing address if available, or assign a new static IP address:



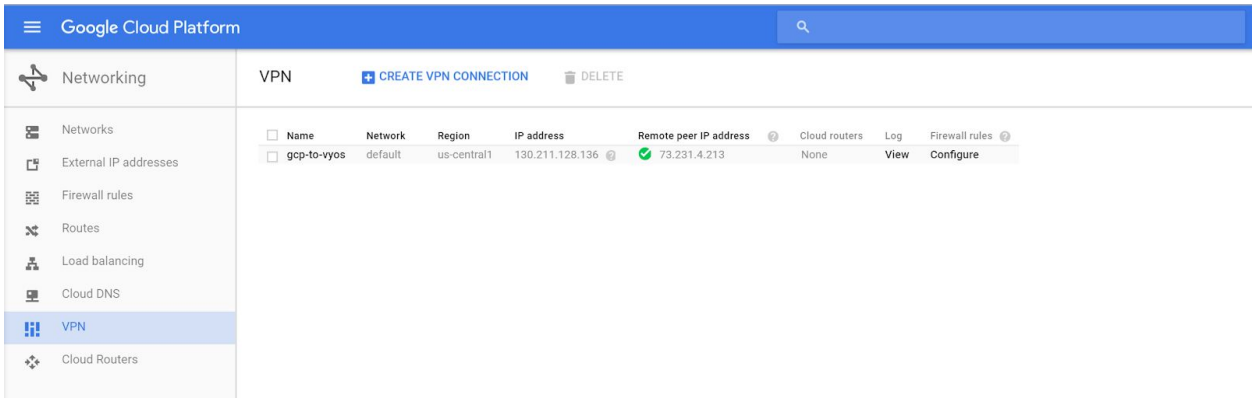
3. To reserve a new static IP, enter values for **Name** and **Description**, and then click **Reserve**:



4. Under **IP address**, select the newly created static IP. This IP is used as the **remote peer** in the VyOS configuration. Under **Remote peer IP address**, enter the outside interface address of the VyOS router. For **IKE version**, select a version (IKEv2 is recommended). For **Shared secret**, enter your shared secret, which is used for IPsec mutual authentication. Finally, under **Remote network IP ranges**, enter the IP range of the VyOS router inside network:

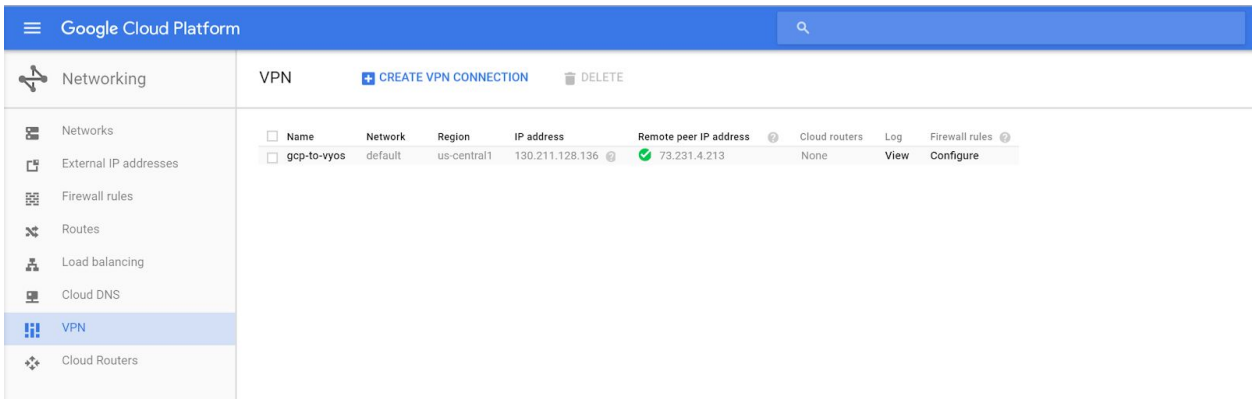


5. Click **Create**, and then click the back arrow to return to the status screen. Note that the connection will fail until the VyOS router has been configured. Here's a successful connection shown for reference:



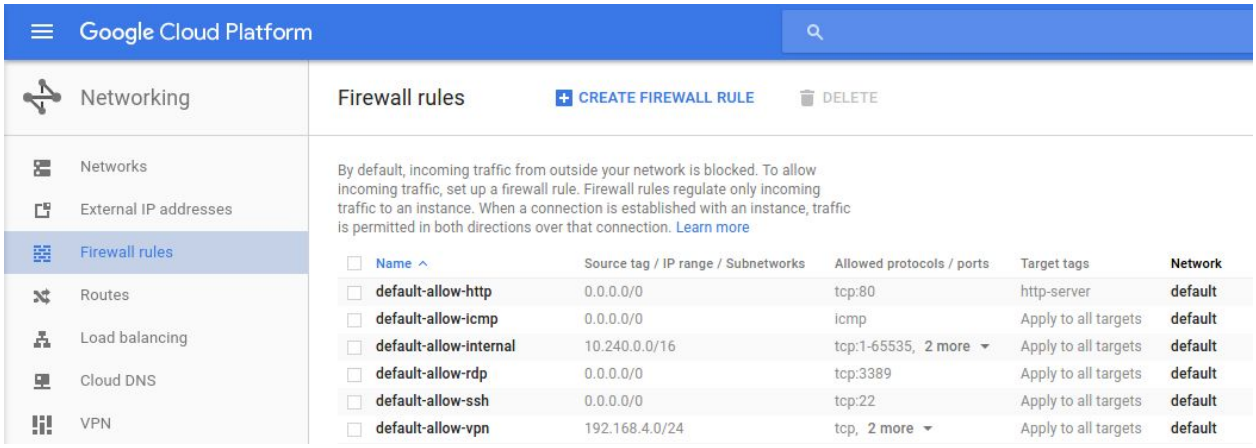
Verify the GCP configuration

With the VyOS virtual router configuration complete, and the IPsec connection initiated, the GCP Console should reflect a connected status under VPN connections:



Update the firewall rules in GCP

At this point, IPsec configuration is complete. We recommend that you verify the firewall rules in GCP to ensure that the required port rules are in place. These rules allow traffic to pass between the local and remote networks:



Configuring VyOS

Prerequisites

This section walks through the VyOS virtual router configuration. As a prerequisite, the router must be configured with at least one outside interface (public routable IP address) and at least one inside interface (internal IP space that's connected to GCP through VPN. Verify that the interfaces are set up correctly by checking the running configuration:

```
vyos@vyos:~$  show configuration
```

The following sample interface configuration is provided for reference:

```
ethernet eth0 {
     address 1.1.1.1/24
     description OUTSIDE
     duplex auto
     hw-id 00:0c:29:44:3b:0f
 }
ethernet eth1 {
     address 192.168.0.1/24
     description INSIDE
     duplex auto
     hw-id 00:0c:29:44:3b:19
     smp_affinity auto
     speed auto
   }
 loopback lo {
 }
```

Enter configure mode

- To get started with the VyOS virtual router configuration, connect to the router through SSH. When you are connected, enter `configure` mode to begin configuration:

```
vyos@vyos:~$ configure
[edit]
```

IPsec ESP configuration

```
set vpn ipsec esp-group gcp-esp compression 'disable'
set vpn ipsec esp-group gcp-esp lifetime '10800'
set vpn ipsec esp-group gcp-esp mode 'tunnel'
set vpn ipsec esp-group gcp-esp pfs 'enable'
set vpn ipsec esp-group gcp-esp proposal 1 encryption 'aes256'
set vpn ipsec esp-group gcp-esp proposal 1 hash 'sha1'
```

IPsec IKE configuration

```
set vpn ipsec ike-group gcp-ike ikev2-reauth 'no'
set vpn ipsec ike-group gcp-ike key-exchange 'ikev2'
set vpn ipsec ike-group gcp-ike lifetime '36000'
set vpn ipsec ike-group gcp-ike proposal 1 encryption 'aes256'
set vpn ipsec ike-group gcp-ike proposal 1 hash 'sha1'
set vpn ipsec ike-group gcp-ike proposal 1 dh-group 14
```

IPsec tunnel configuration

The last step is to configure the IPsec tunnel. In the following example, set the *peer* to the Google Cloud VPN static IP address configured above, and set the *pre-shared-secret* to the `PreSharedKey` set in the Google Cloud VPN configuration above.

```
set vpn ipsec ipsec-interfaces interface 'eth1'
set vpn ipsec site-to-site peer 2.2.2.2 authentication id '1.1.1.1'
set vpn ipsec site-to-site peer 2.2.2.2 authentication mode
'pre-shared-secret'
set vpn ipsec site-to-site peer 2.2.2.2 authentication pre-shared-secret
'SomePreSharedKey'
set vpn ipsec site-to-site peer 2.2.2.2 ike-group 'gcp-ike'
set vpn ipsec site-to-site peer 2.2.2.2 local-address '1.1.1.1'
set vpn ipsec site-to-site peer 2.2.2.2 tunnel 0 allow-nat-networks 'disable'
```

```
set vpn ipsec site-to-site peer 2.2.2.2 tunnel 0 allow-public-networks
'disable'
set vpn ipsec site-to-site peer 2.2.2.2 tunnel 0 esp-group 'gcp-esp'
set vpn ipsec site-to-site peer 2.2.2.2 tunnel 0 local prefix '192.168.0.0/24'
set vpn ipsec site-to-site peer 2.2.2.2 tunnel 0 remote prefix '10.0.0.0/21'
```

Save the configuration

1. To save the running configuration and set it as the startup default, use the following commands:

```
vyos@vyos# commit
[edit]


vyos@vyos# save
Saving configuration to '/config/config.boot'...
Done
[edit]
vyos@vyos#
```

2. When the save is complete, exit configuration mode:

```
vyos@vyos# exit
exit
vyos@vyos:~$
```

Testing the IPsec connection

You can test the IPsec tunnel from the router by using ICMP to ping a host on GCP. Be sure to use the *inside* interface on the VyOS, and make sure that the firewall rules have been set correctly to allow ICMP.

```
vyos@vyos:~$ ping 10.240.0.2
PING 10.240.0.2 (10.240.0.2) 56(84) bytes of data.
64 bytes from 10.240.0.2: icmp_req=1 ttl=64 time=47.1 ms
64 bytes from 10.240.0.2: icmp_req=2 ttl=64 time=46.4 ms
64 bytes from 10.240.0.2: icmp_req=3 ttl=64 time=46.2 ms
64 bytes from 10.240.0.2: icmp_req=4 ttl=64 time=46.8 ms
64 bytes from 10.240.0.2: icmp_req=5 ttl=64 time=46.6 ms
64 bytes from 10.240.0.2: icmp_req=6 ttl=64 time=46.0 ms
64 bytes from 10.240.0.2: icmp_req=7 ttl=64 time=50.0 ms
64 bytes from 10.240.0.2: icmp_req=8 ttl=64 time=48.1 ms
64 bytes from 10.240.0.2: icmp_req=9 ttl=64 time=46.0 ms
^C
--- 10.240.0.2 ping statistics ---
9 packets transmitted, 9 received, 0% packet loss, time 8082ms
rtt min/avg/max/mdev = 46.006/47.049/50.000/1.246 ms
vyos@vyos:~$
```

Troubleshooting the IPsec connection

If you have connection problems, the following commands can be useful for troubleshooting. To display the status of the IKEv2 security association, use the **`sh vpn ike sa`** command:

```
vyos@srv-gw0:~$ sh vpn ike sa
Peer ID / IP                            Local ID / IP
------------                            -------------
2.2.2.2                                 1.1.1.1
   State  Encrypt  Hash    D-H Grp  NAT-T  A-Time  L-Time
   -----  -------  ----    -------  -----  ------  ------
   up     aes256   sha1    5        no     734     3600
```

To display the status of the IKEv2 security association, use the **`sh vpn ipsec sa`** command:

```
vyos@srv-gw0:~$ show vpn ipsec sa
Peer ID / IP                            Local ID / IP
------------                            -------------
2.2.2.2                                 1.1.1.1
   Tunnel  State  Bytes Out/In   Encrypt  Hash    NAT-T  A-Time  L-Time  Proto
   ------  -----  -------------  -------  ----    -----  ------  ------  -----
   0       up     7.5M/230.6K    aes256   sha1    no     567     1800    all
```

Known issues

Tunnel configured with IKEv2 frequently goes down

If your tunnel with IKEv2 frequently goes down, the issue might be related to the gateway's strongSwan version. For more information, see this discussion. The suggested solution is to edit the `/etc/ipsec.conf` file to make the configuration for `esp` and `ike` identical, such as:

```
conn NAME
  ike=aes128-sha1-modp2048!
  esp=aes128-sha1-modp2048!
```

Alternatively, if the above solution doesn't work, you can use IKEv1 instead of IKEv2.

Resetting the IPsec connection

To reset the IPsec connection (initiate a reconnect), use the following command:

```
clear ipsec sa peer <remote-peer-IP>
```