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

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 the Google Cloud VPN service. This information is provided as an example only. Please note that this guide is not meant to be a comprehensive overview of IPsec and assumes basic familiarity with the IPsec protocol.

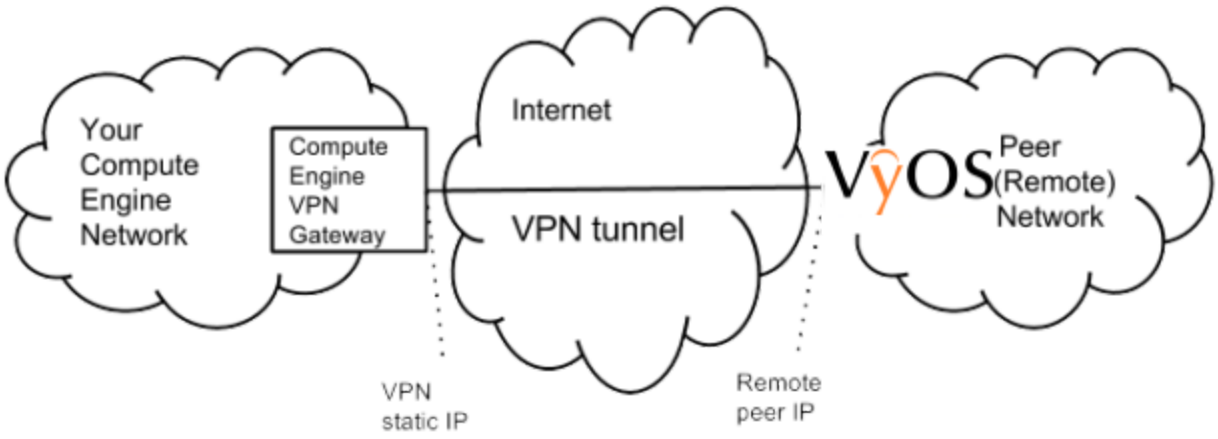
Environment Overview

The equipment used in the creation of this guide is as follows:

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 which follow will include numerous value substitutions provided for the purposes of example only. Any references to IP addresses, device IDs, shared secrets or keys, account information or project names should be replaced with the appropriate values for your environment when following this guide. Values unique to your environment will be highlighted in **bold**.

This guide is not meant to be a comprehensive setup overview for the device referenced, but rather is only intended to assist in the creation of IPsec connectivity to Google Compute Engine. The following is a high level overview of the configuration process which will be covered:

- Selecting the appropriate IPsec configuration
- Configuring the internet facing interface of your device (outside interface)
- Configuring IKEv2 and IPsec
- Testing 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 the following prerequisite conditions have been met:

- VyOS successfully deployed to either virtual or physical hardware. Installation is out of scope for this guide, but detailed installation instructions can be found at the VyOS project homepage.
- At least one configured and verified functional internal interface
- One configured and verified functional external interface

IPsec Parameters

For the VyOS Router IPsec configuration, the following details will be used:

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

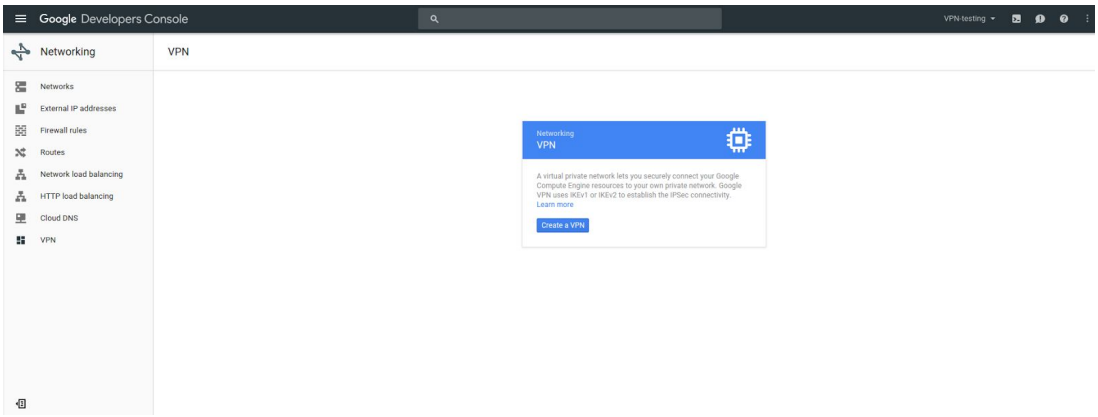
The IPsec configuration used in this guide is specified below:

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)*

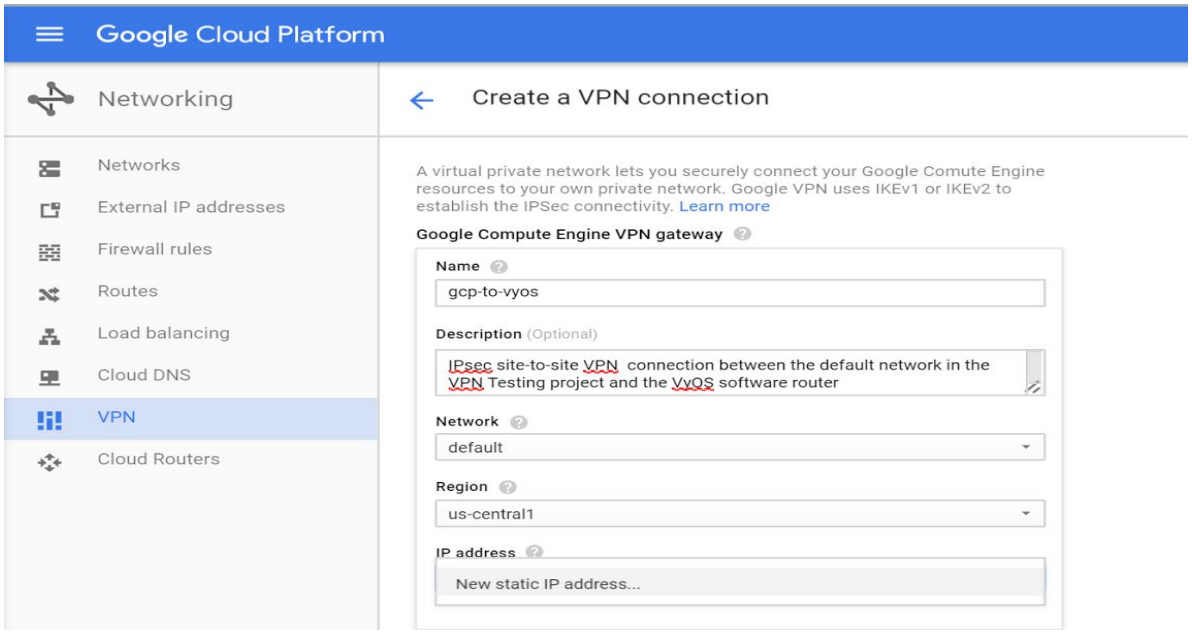
Configuration

Configuration - GCP

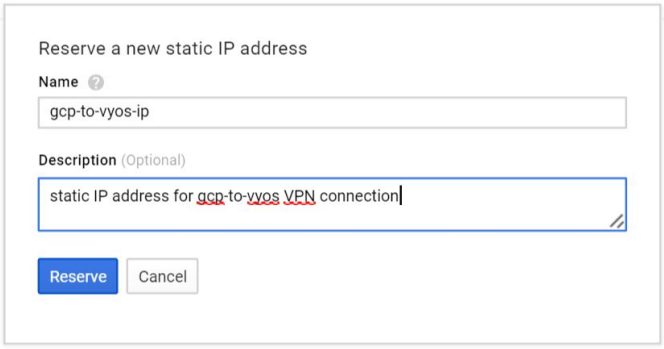
This section provides a step-by-step walkthrough of the Google Cloud VPN configuration. Log on to the Google Cloud Platform Developers Console and select Networking from the main menu. To create a new VPN instance, select the VPN node and click **Create a VPN** from the main task pane:



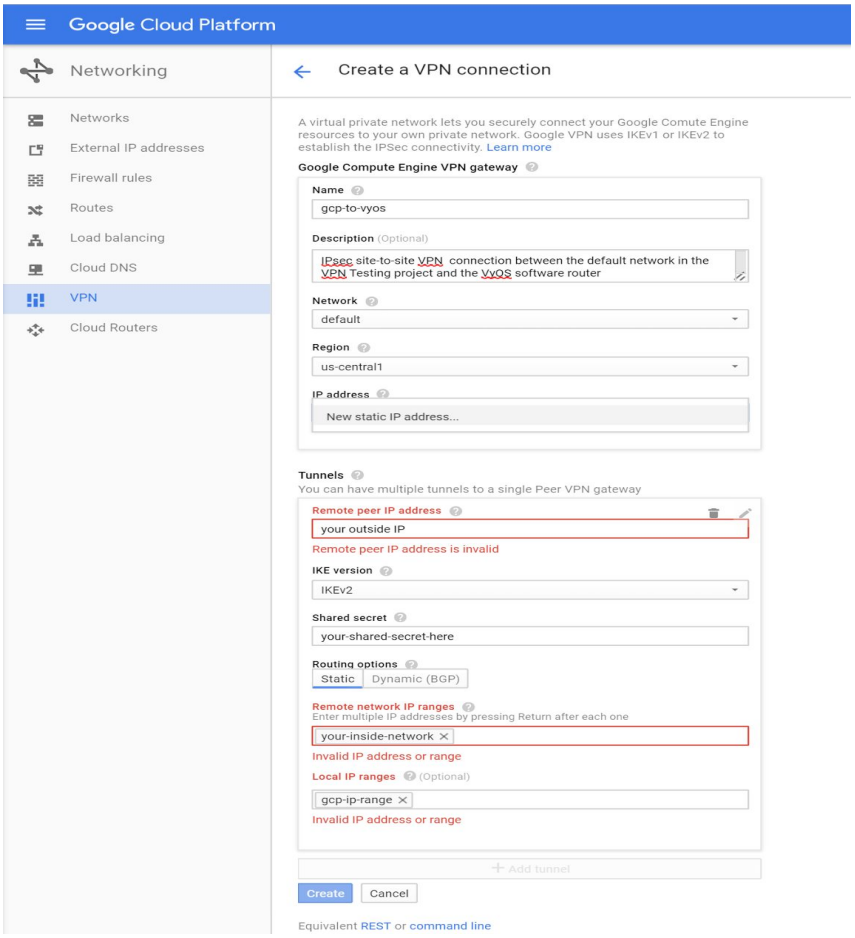
All parameters needed to create a new VPN connection are entered on this page. Provide a **Name** and **Description** for the VPN instance. The VPN instance requires a **public IP address.** An existing address can be selected if available, or a **New static IP address** can be assigned:



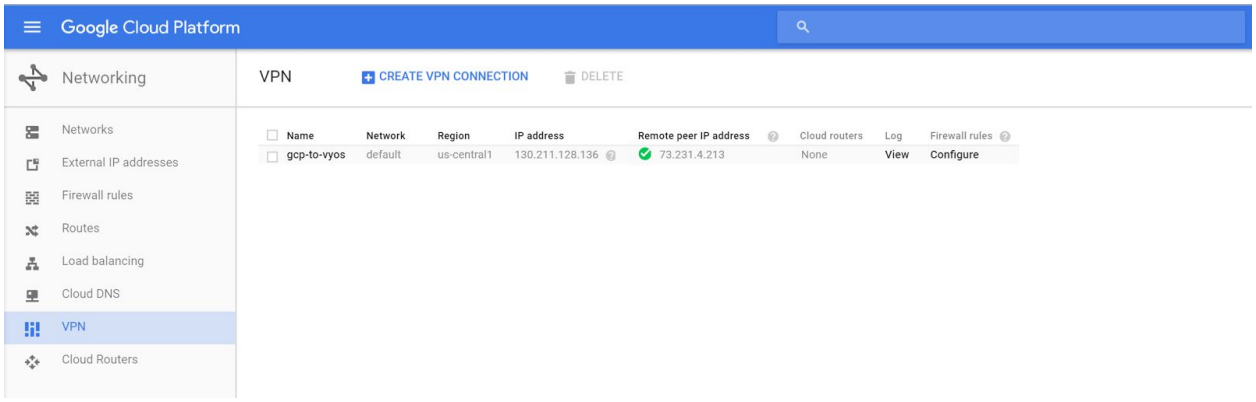
To reserve a new static IP, enter a **Name** and **Description** and click Reserve:



Select the newly created static IP under **IP-address**. This IP will be used as the **remote peer** in the VyOS configuration. Enter the **outside interface address** of the VyOS router as the **Remote peer IP address**. Select an IKE version (IKEv2 is recommended) and enter a **Shared secret** to be used for IPsec mutual authentication. Finally, enter the IP range of the VyOS router **inside network** under **Remote network IP ranges**:

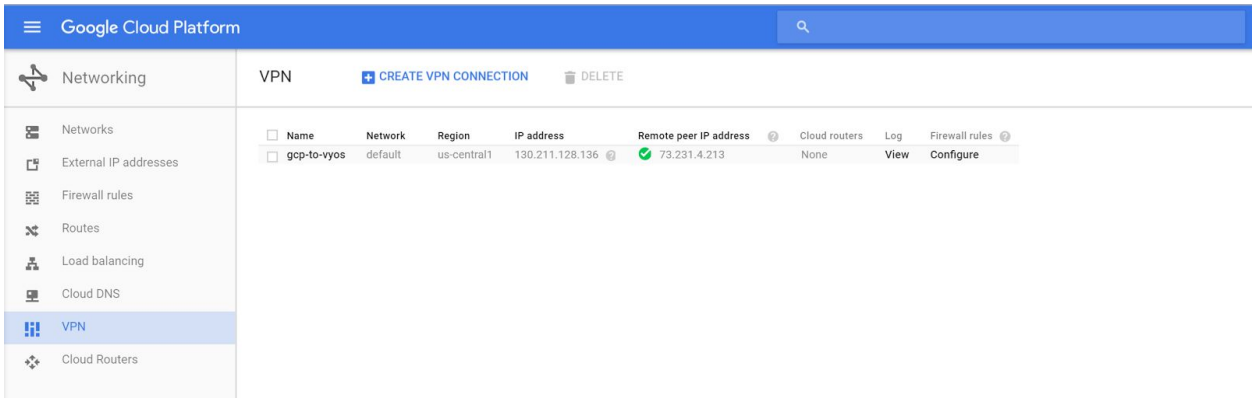


Click **Create**, then click the back arrow to return to the status screen. Note that the connection will fail until the VyOS router has been configured. Successful connection shown for reference:



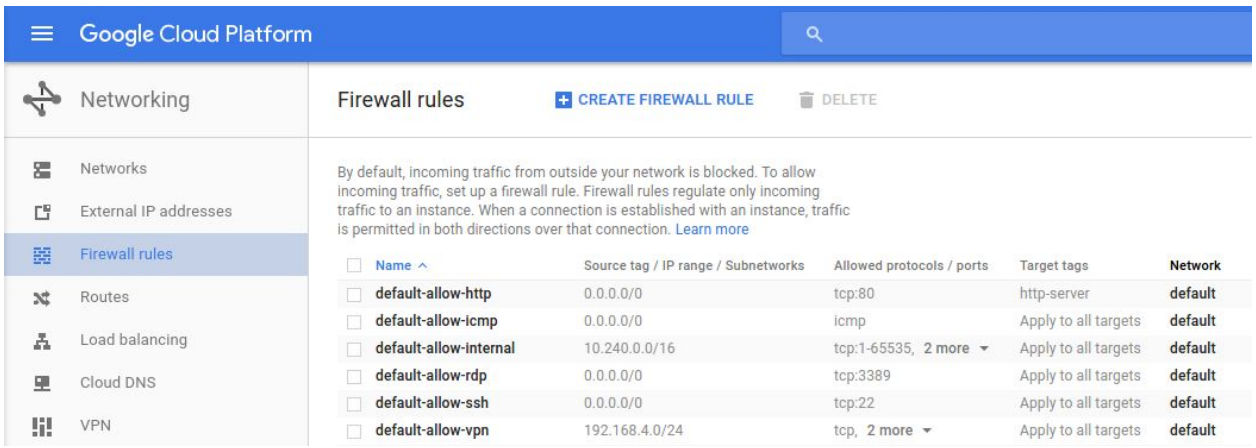
Verifying the GCP Configuration

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



Updating the Firewall Rules in GCP

At this point IPsec configuration is complete and the firewall rules in GCP should be verified to ensure that the required port rules are in place allowing traffic to pass between the local and remote networks:



Configuration - VyOS

Prerequisites

This section provides a step-by-step walkthrough of the VyOS virtual router configuration. As a prerequisite, the router should be configured with at least one *outside* interface (public routable IP address) and at least one *inside* interface (internal IP space which will be connected to GCP via VPN. Verify the interfaces are setup correctly by checking the running configuration:

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

A sample interface configuration is provided below 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 {
}
```

Entering Configuration Mode

To get started with the VyOS virtual router configuration, connect to the router via SSH. Once 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 example below, the *peer* should be set to the **Google Cloud VPN static IP address** configured above. The *pre-shared-secret* should be set 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'
```

Saving the Configuration

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#
```

Once saved, exist configuration mode:

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

Testing the IPsec connection

The IPsec tunnel can be tested 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

In the event of 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 the discussion here. The suggested solution is to edit the /etc/ipsec.conf file to include the same pfs config to esp as ike, such as 'esp=aes128-sha1-modp2048!'.

Alternatively, you can use IKEv1 instead of IKEv2 if the above solution does not work.

Resetting the IPsec connection

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

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