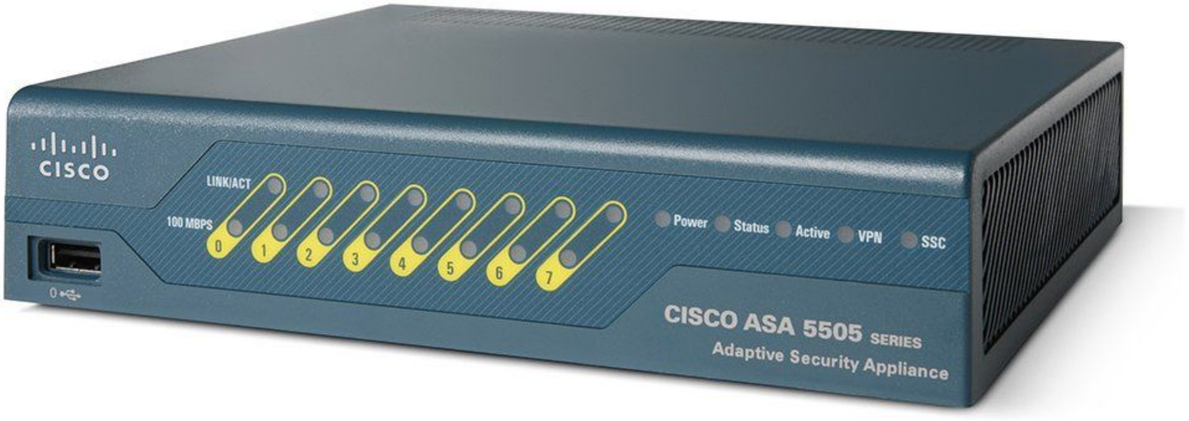
Google Cloud VPN Interop Guide

Using Cloud VPN With Cisco® ASA



Courtesy of Cisco Systems, Inc. Unauthorized use not permitted. Cisco® is a registered trademark or trademark of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

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

Contents

Introduction

This guide walks you through the process of configuring the Cisco ASA 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.

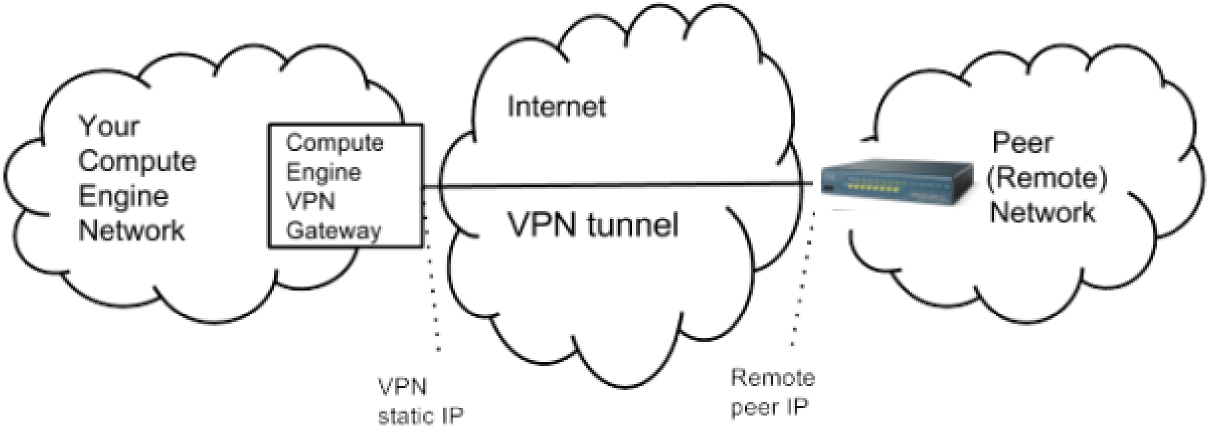
Environment Overview

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

Vendor:	Cisco
Model:	ASA5505
Firmware Rev:	M50FW080
Software Rev:	ASA 9.2(3), Device Manager 6.2(1)

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 Cisco ASA for use with the Google Cloud VPN service is to ensure that the following prerequisite conditions have been met:

- Cisco ASA online and functional with no faults detected
- Enable password for the Cisco ASA
- At least one configured and verified functional internal interface
- One configured and verified functional external interface

IPsec Parameters

For the Cisco ASA IPsec configuration, the following details will be used:

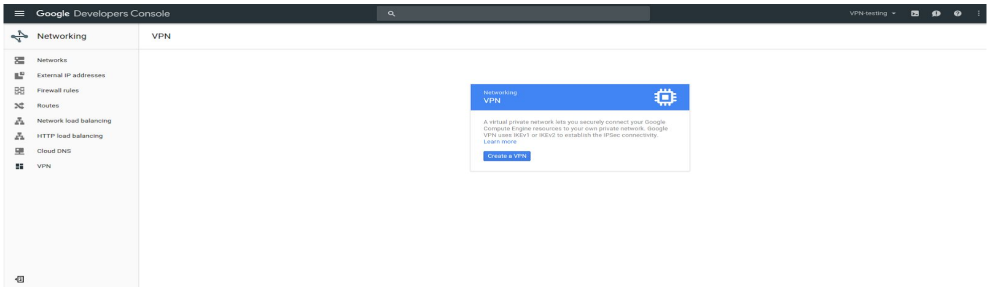
Parameter	Value
IPsec Mode	ESP+Auth Tunnel mode (Site-to-Site)
Auth Protocol	Pre-shared Key
Key Exchange	IKEv2
Start	auto
Perfect Forward Secrecy (PFS)	on
Dead Peer Detection (DPD)	aggressive
INITIAL_CONTACT (uniqueids)	on

The IPsec configuration used in this guide is specified below:

Phase	***Cipher Role***	***Cipher***
Phase 1	*Encryption*	*aes-256*
	Integrity	*sha-1*
	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-512*
	Phase 1 lifetime	*10,800 seconds*

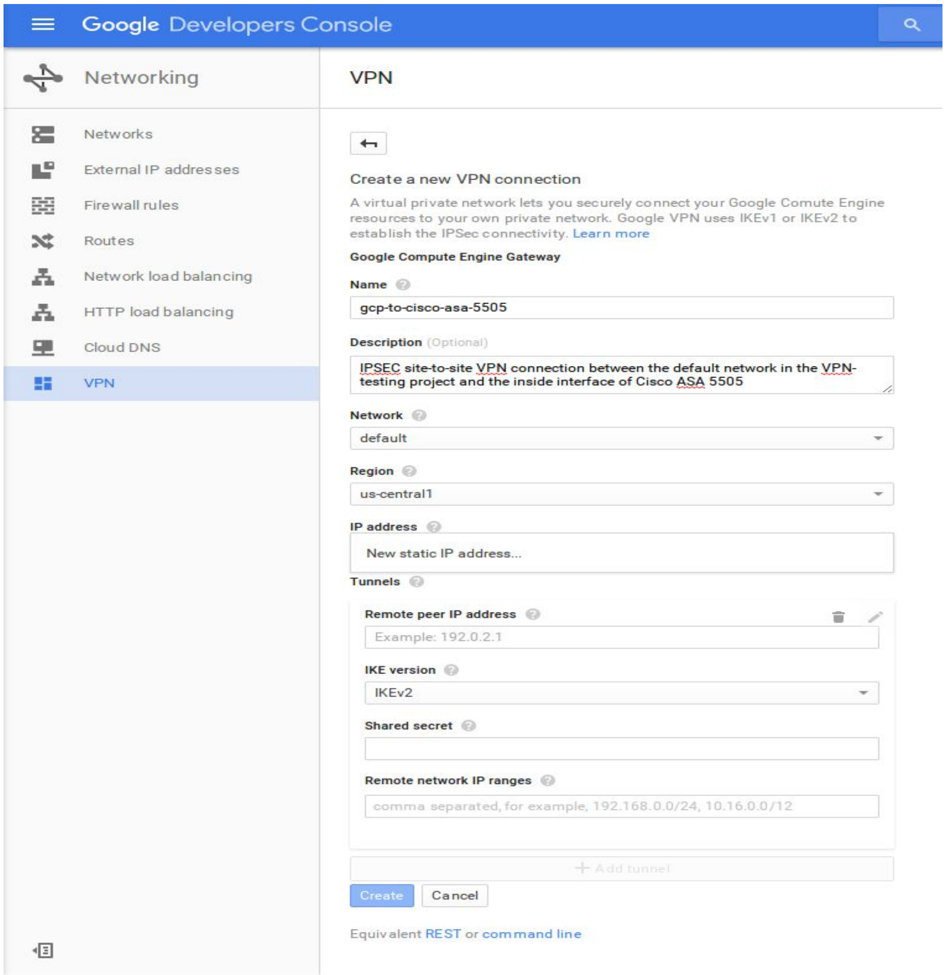
Configuration - GCP

This section provides a step-by-step walkthrough of the Google Cloud Platform 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:



A virtual private network lets you securely connect your Google Compute Engine resources to your own private network. Google VPN uses IKEv1 or IKEv2 to establish the IPSec connectivity.

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:



Create a new VPN connection

A virtual private network lets you securely connect your Google Comute Engine resources to your own private network. Google VPN uses IKEv1 or IKEv2 to establish the IPSec connectivity.

Google Compute Engine Gateway

Name: gcp-to-cisco-asa-5505

Description (Optional): IPSEC site-to-site VPN connection between the default network in the VPN-testing project and the inside interface of Cisco ASA 5505

Network: default

Region: us-central1

IP address: New static IP address...

Tunnels

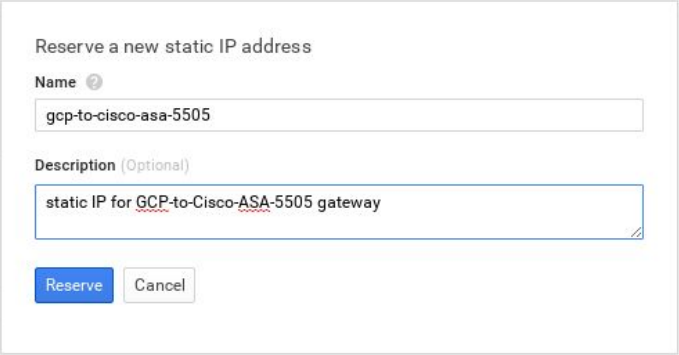
Remote peer IP address: Example: 192.0.2.1

IKE version: IKEv2

Shared secret:

Remote network IP ranges: comma separated, for example, 192.168.0.0/24, 10.16.0.0/12

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

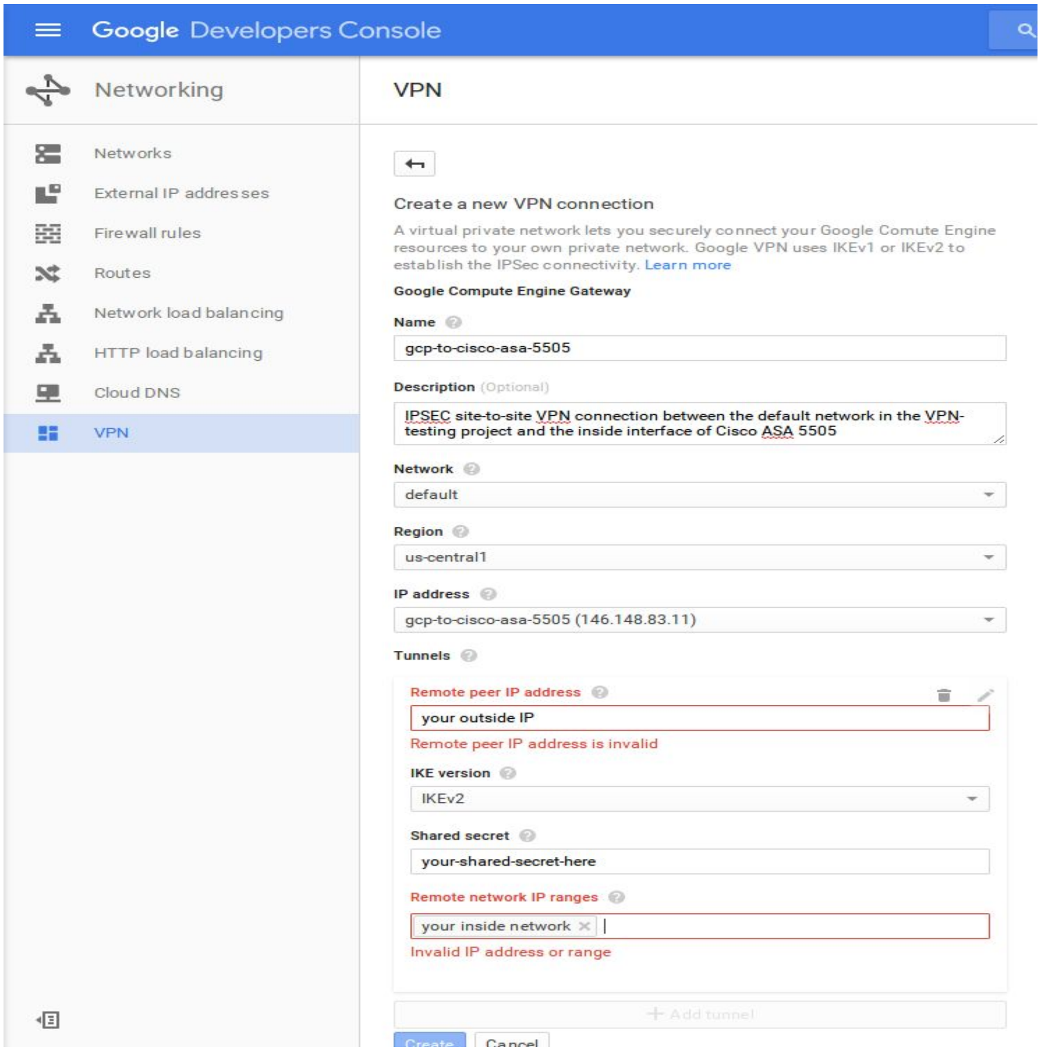


Reserve a new static IP address

Name: gcp-to-cisco-asa-5505

Description (Optional): static IP for GCP-to-Cisco-ASA-5505 gateway

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



VPN

Create a new VPN connection

A virtual private network lets you securely connect your Google Comute Engine resources to your own private network. Google VPN uses IKEv1 or IKEv2 to establish the IPSec connectivity. Learn more

Google Compute Engine Gateway

Name: gcp-to-cisco-asa-5505

Description (Optional): IPSEC site-to-site VPN connection between the default network in the VPN-testing project and the inside interface of Cisco ASA 5505

Network: default

Region: us-central1

IP address: gcp-to-cisco-asa-5505 (146.148.83.11)

Tunnels

Remote peer IP address: your outside IP

Remote peer IP address is invalid

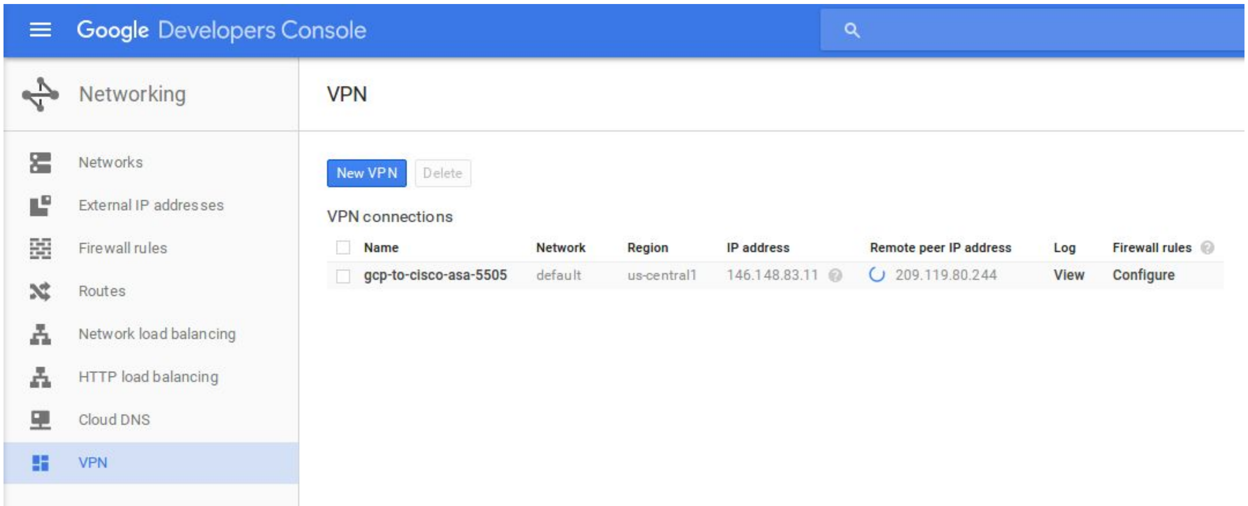
IKE version: IKEv2

Shared secret: your-shared-secret-here

Remote network IP ranges: your inside network ×

Invalid IP address or range

Click **Create**, then click the back arrow to return to the status screen. Note that the connection will fail until the ASA has been configured:



VPN connections

□	Name	Network	Region	IP address	Remote peer IP address	Log	Firewall rules
□	gcp-to-cisco-asa-5505	default	us-central1	146.148.83.11	209.119.80.244	View	Configure

Configuration - Cisco ASA 5505

Prerequisites

This section provides a step-by-step walkthrough of the Cisco ASA 5505 configuration. As a prerequisite, the Cisco ASA 5505 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. A sample interface configuration is provided below for reference:

```
interface Vlan1
 nameif inside
 security-level 100
 ip address 192.168.2.1 255.255.255.0
!
interface Vlan727
 nameif outside
 security-level 0
 ip address 209.119.80.244 255.255.255.248
```

Entering Configuration Mode

To get started with the Cisco ASA 5505 configuration, connect to the router via a management interface (telnet, SSH, tty, etc). Once connected, switch to **enable** mode to begin configuration and set the configuration source to **terminal**:

```
enable
Configure terminal
```

IPsec Proposal

Create an Internet Key Exchange (IKE) version 2 proposal object. IKEv2 proposal objects contain the parameters required for creating IKEv2 proposals when defining remote access and site-to-site VPN policies. IKE is a key management protocol that facilitates the management of IPsec-based communications. It is used to authenticate IPsec peers, negotiate and distribute IPsec encryption keys, and automatically establish IPsec security associations (SAs).

The following configuration snippet can be copied and pasted directly:

```
crypto ipsec ikev2 ipsec-proposal gcp
 protocol esp encryption aes-256
 protocol esp integrity sha-1
```

Access Lists

Create access-list objects for the IPsec connection. Access lists (ACLs) control traffic by the comparison of the source address of the IP packets to the addresses configured in the ACL. To create an access-list requires a reference-id (name or number), an action (permit or deny) a protocol, and a source and destination IP range. Create three access lists:

- **gcp-acl** - allow **any** egress traffic on the **inside** interface access to the **IP range** in GCP. This access list will be referenced by the main **crypto map**.
- **gcp-in** - allow ingress traffic from the GCP VPN endpoint to the **outside** IP of the ASA
- **gcp-filter** - allow ingress traffic from the GCP IP range to the **inside** IP range of the ASA

The following configuration snippet can be used if the specified IP ranges for both inside and outside networks, and local and remote IPsec endpoints, are modified:

```
access-list gcp-in extended permit ip host 146.148.83.11 host 209.119.80.244
access-list gcp-acl extended permit ip any4 10.240.0.0 255.255.0.0
access-list gcp-filter extended permit ip 10.240.0.0 255.255.0.0 192.168.2.0
255.255.255.0
```

Crypto Maps

Create crypto map objects for the IPsec connection. Crypto map entries represent the various elements of IPsec security associations, including the following which traffic IPsec should protect (defined in an access list), where to send IPsec-protected traffic (by peer identification), what IPsec security applies to this traffic (specified by a transform set) and the local address for IPsec traffic, which is identified by applying the crypto map to an interface. The format of the crypto map entry is:

```
crypto map name priority parameter options
```

A core component of IPsec configuration on Cisco is the **crypto map.** Crypto maps are used to define the following IPsec parameters:

- An **access list match** association defining which network ranges will be permitted through the tunnel
- Set **perfect forward secrecy** on the appropriate Diffie-Hellman group. Perfect forward secrecy causes **new keys** to be generated when establishing the IPsec SA
- Define the **IPsec peer** which will complete the tunnel. In this case it is the GCP VPN endpoint.
- Set the appropriate **IPsec proposal** and **key exchange protocol**. In the example below, the **gcp** proposal created earlier is being associated with this map using the IKEv2 protocol
- Enable this crypto map on the **outside** interface

The following configuration snippet can be used if the referenced access list and remote IPsec endpoint are modified:

```
crypto map gcp-vpn-map 1 match address gcp-acl
crypto map gcp-vpn-map 1 set pfs group14
crypto map gcp-vpn-map 1 set peer 146.148.83.11
crypto map gcp-vpn-map 1 set ikev2 ipsec-proposal gcp
crypto map gcp-vpn-map interface outside
```

IKE Policy

Create an IKEv2 policy configuration for the IPsec connection. The IKEv2 policy block sets the parameters for the IKE exchange. In this block, the following parameters are set:

- **Encryption algorithm** - set to AES-256 for this example
- **Integrity algorithm** - set to SHA512 for this example
- **Diffie-Hellman group** - IPsec uses the Diffie-Hellman algorithm to generate the initial encryption key between the peers. In this example it is set to group 14
- **Pseudo-Random Function (PRF)** - IKEv2 requires a separate method used as the algorithm to derive keying material and hashing operations required for the IKEv2 tunnel encryption. This is referred to as the **pseudo-random function** and is set to SHA
- **SA Lifetime** - set the lifetime of the security associations (after which a reconnection will occur). Set to 36,000 seconds.

In summary, this sample policy will use AES-256 to encrypt the secure channel, the SHA512 hash algorithm will be used to validate the identity of the remote peer and Diffie-Hellman group 14 will be utilized for key generation. Group 14 uses 2048 bit encryption blocks. Finally, a lifetime for the security association is set to 36,000 seconds.

The following configuration snippet can be copied and pasted directly:

```
crypto ikev2 policy 100
 encryption aes-256
 integrity sha512
 group 14
 prf sha
 lifetime seconds 36000
```

At this point, the IKEv2 protocol should be enabled on the **outside** interface:

```
crypto ikev2 enable outside
```

IPsec Security Associations

Create IPsec **security-association** rules. A security association is a relationship between two or more entities that describes how the entities will use security services to communicate securely. During tunnel establishment, the two peers negotiate security associations that govern authentication, encryption, encapsulation, and key management. These negotiations involve two phases: first, to establish the tunnel (the IKE SA) and second, to govern traffic within the tunnel (the IPsec SA). The following commands set the SA lifetime and timing parameters.

The following configuration snippet can be copied and pasted directly:

```
crypto ipsec security-association lifetime seconds 10800
crypto ipsec security-association replay window-size 128
crypto ipsec security-association pmtu-aging infinite
```

ISAKMP

Set the ISAKMP parameters. These commands set the configuration for the Internet Security Association Key Management Protocol (ISAKMP). This is the protocol used by IPsec to establish security associations. The following commands enable ISAKMP on the **outside** interface and set the ISAKMP **identity** method to address. This means that IPsec endpoints will be mutually identified by their IP address.

The next commands **disable NAT traversal**, and set IPsec protocol parameters. NAT traversal allows IPsec connections to initiate from behind a NAT and are **not supported** on GCP. The **do not fragment bit** (df-bit) in IP prevents IP packets from being broken up into smaller segments by routers.

The following configuration snippet can be copied and pasted directly:

```
crypto isakmp identity address
crypto isakmp disconnect-notify
no crypto isakmp nat-traversal
crypto ipsec df-bit clear-df outside
```

Group Policy

Create a **group-policy**. Group policies set the access policies and protocol specific connection parameters for the IPsec tunnel. In this example, an **internal** group policy named **gcp** is being created. Internal group policies require attributes be set on the ASA. The attribute being set in this example is the vpn-filter, set to **gcp-filter** and the **vpn-tunnel-protocol**, set to IKEV2.

The following configuration snippet can be copied and pasted directly:

```
group-policy gcp internal
group-policy gcp attributes
 vpn-filter value gcp-filter
 vpn-tunnel-protocol ikev2
```

Tunnel Group Configuration

Create the tunnel-group configuration. Tunnel group parameters set the access policies and protocol specific connection parameters for the IPsec tunnel. The first command sets the tunnel type to IPsec l2l (site-to-site or, in Cisco terms, *lan-to-lan*).

The next command block sets the general-attributes for the IPsec tunnel. In this case the default-group-policy for the tunnel is being set to the policy named **gcp** and the ipsec-attributes for the tunnel are being set. This section is critical as it is where **the shared secret created in the GCP configuration section is entered.** The same shared secret should be used for both local and remote authentication. In addition, the ISA key management protocol keep alive parameters are set.

The following configuration snippet can be used if the correct pre-shared key, remote peer IP address, and group policy are entered:

```
tunnel-group 146.148.83.11 type ipsec-l2l
tunnel-group 146.148.83.11 general-attributes
 default-group-policy gcp
tunnel-group 146.148.83.11 ipsec-attributes
 isakmp keepalive threshold 10 retry 3
 ikev2 remote-authentication pre-shared-key *****
 ikev2 local-authentication pre-shared-key *****
```

SLA Monitor (Optional)

Optionally, an SLA monitor configuration can be set. The SLA monitor setting configures a tracked object which will be used by the ASA to determine connection health. In this case, a host on the 10.240.0.0 network is being used for the health check:

```
sla monitor 1
type echo protocol ipIcmpEcho 10.240.0.2 interface inside
frequency 5
exit
sla monitor schedule 1 life forever start-time now
```

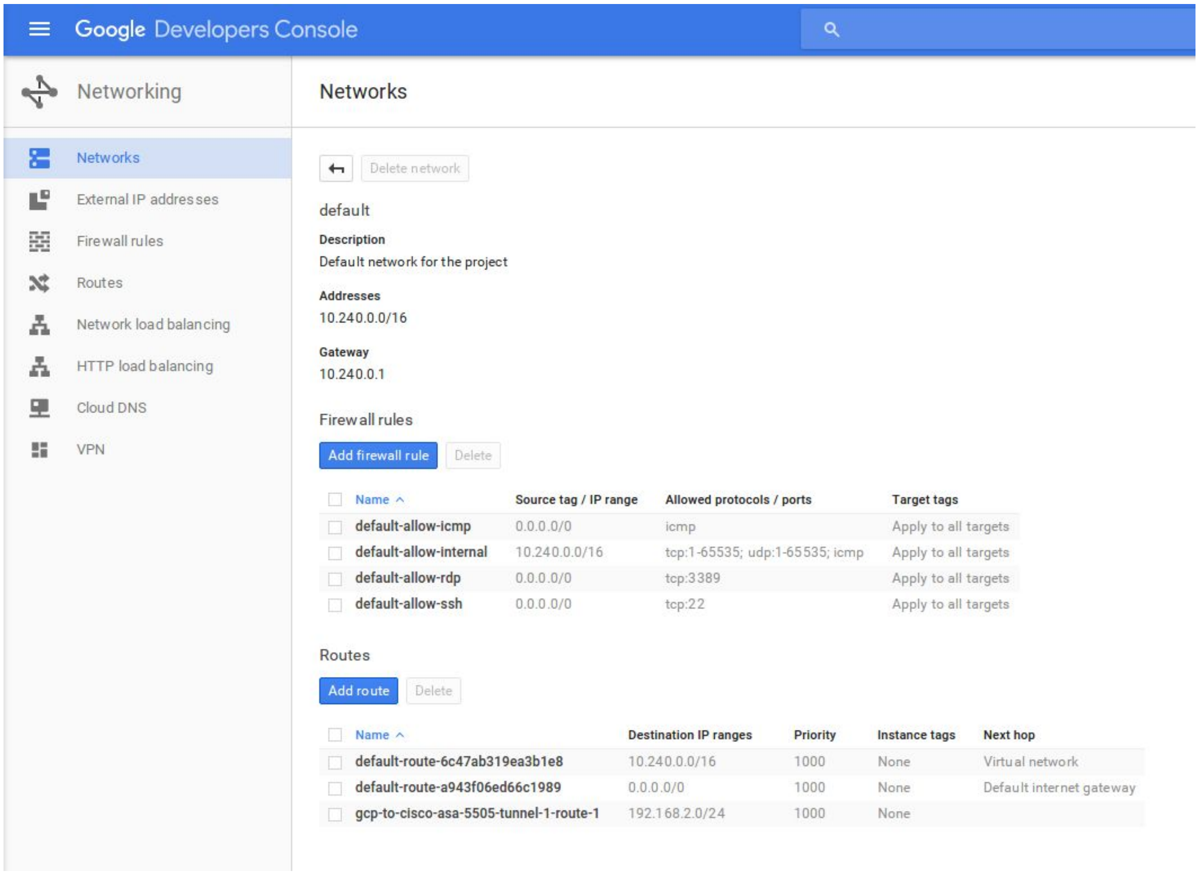
Saving the Configuration

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

```
write
copy run start
```

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:



Networks

default

Description
Default network for the project

Addresses
10.240.0.0/16

Gateway
10.240.0.1

Firewall rules

Name	Source tag / IP range	Allowed protocols / ports	Target tags
default-allow-icmp	0.0.0.0/0	icmp	Apply to all targets
default-allow-internal	10.240.0.0/16	tcp:1-65535; udp:1-65535; icmp	Apply to all targets
default-allow-rdp	0.0.0.0/0	tcp:3389	Apply to all targets
default-allow-ssh	0.0.0.0/0	tcp:22	Apply to all targets

Routes

Name	Destination IP ranges	Priority	Instance tags	Next hop
default-route-6c47ab319ea3b1e8	10.240.0.0/16	1000	None	Virtual network
default-route-a943f06ed66c1989	0.0.0.0/0	1000	None	Default internet gateway
gcp-to-cisco-asa-5505-tunnel-1-route-1	192.168.2.0/24	1000	None	

Testing the IPsec connection

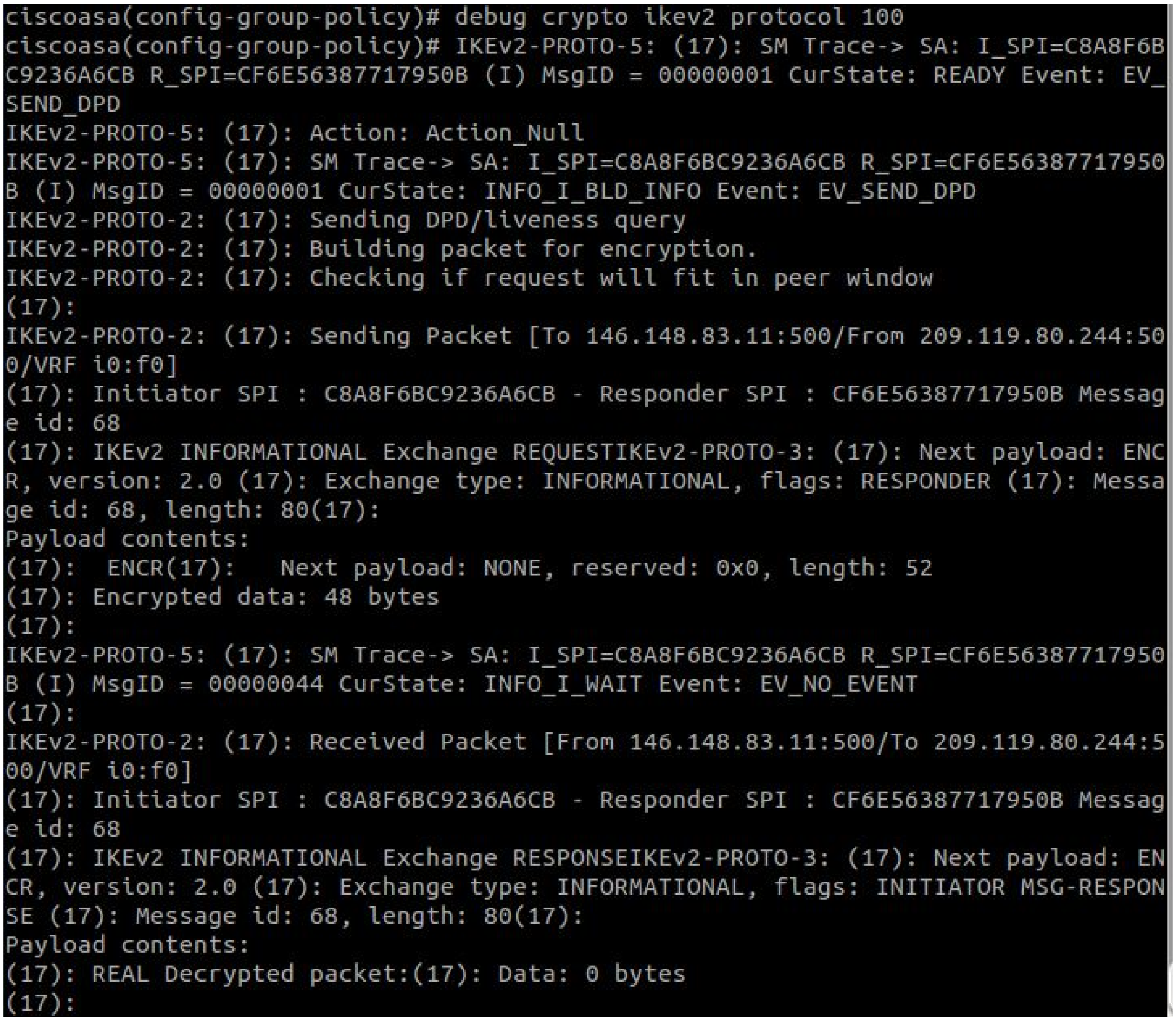
The IPsec tunnel can be tested from the router by using ICMP to ping a host on GCP. Be sure to use the **inside** interface on the ASA and make sure that the firewall rules have been set correctly to allow ICMP.

Troubleshooting the IPsec connection

In the event of connection problems, the following commands can be useful for troubleshooting. To display the event log of all IKEv2 protocol operations use the **debug crypto** command

```
debug crypto ikev2 protocol level
```

Below is sample output from debug level set to **100** on an **established** connection:



```
ciscoasa(config-group-policy)# debug crypto ikev2 protocol 100
ciscoasa(config-group-policy)# IKEv2-PROTO-5: (17): SM Trace-> SA: I_SPI=C8A8F6B
C9236A6CB R_SPI=CF6E56387717950B (I) MsgID = 00000001 CurState: READY Event: EV_
SEND_DPD
IKEv2-PROTO-5: (17): Action: Action_Null
IKEv2-PROTO-5: (17): SM Trace-> SA: I_SPI=C8A8F6BC9236A6CB R_SPI=CF6E56387717950
B (I) MsgID = 00000001 CurState: INFO_I_BLD_INFO Event: EV_SEND_DPD
IKEv2-PROTO-2: (17): Sending DPD/liveness query
IKEv2-PROTO-2: (17): Building packet for encryption.
IKEv2-PROTO-2: (17): Checking if request will fit in peer window
(17):
IKEv2-PROTO-2: (17): Sending Packet [To 146.148.83.11:500/From 209.119.80.244:50
0/VRF i0:f0]
(17): Initiator SPI : C8A8F6BC9236A6CB - Responder SPI : CF6E56387717950B Messag
e id: 68
(17): IKEv2 INFORMATIONAL Exchange REQUESTIKEv2-PROTO-3: (17): Next payload: ENC
R, version: 2.0 (17): Exchange type: INFORMATIONAL, flags: RESPONDER (17): Messa
ge id: 68, length: 80(17):
Payload contents:
(17):  ENCR(17):   Next payload: NONE, reserved: 0x0, length: 52
(17): Encrypted data: 48 bytes
(17):
IKEv2-PROTO-5: (17): SM Trace-> SA: I_SPI=C8A8F6BC9236A6CB R_SPI=CF6E56387717950
B (I) MsgID = 00000044 CurState: INFO_I_WAIT Event: EV_NO_EVENT
(17):
IKEv2-PROTO-2: (17): Received Packet [From 146.148.83.11:500/To 209.119.80.244:5
00/VRF i0:f0]
(17): Initiator SPI : C8A8F6BC9236A6CB - Responder SPI : CF6E56387717950B Messag
e id: 68
(17): IKEv2 INFORMATIONAL Exchange RESPONSEIKEv2-PROTO-3: (17): Next payload: EN
CR, version: 2.0 (17): Exchange type: INFORMATIONAL, flags: INITIATOR MSG-RESPON
SE (17): Message id: 68, length: 80(17):
Payload contents:
(17): REAL Decrypted packet:(17): Data: 0 bytes
(17):
```

Resetting the IPsec connection

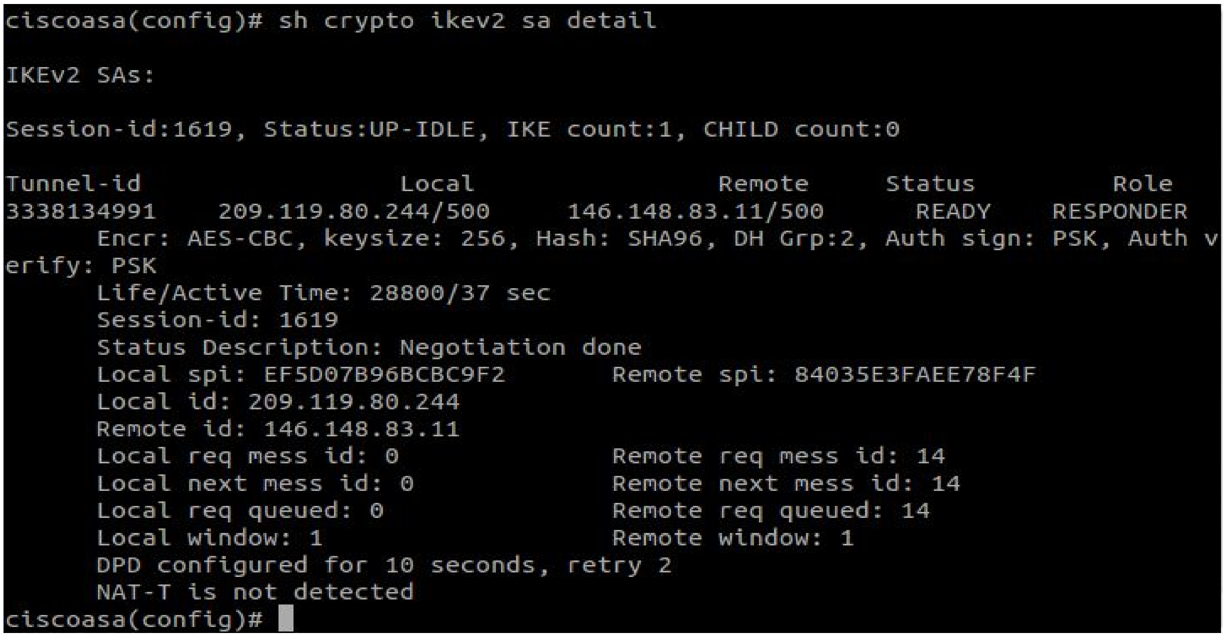
To reset the IPsec connection (initiate a reconnect), use the following command:

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

Verify IKEv2 SA

To check on the status of the IKEv2 security associations use the **sh crypto** command:

```
sh crypto ikev2 sa detail
```

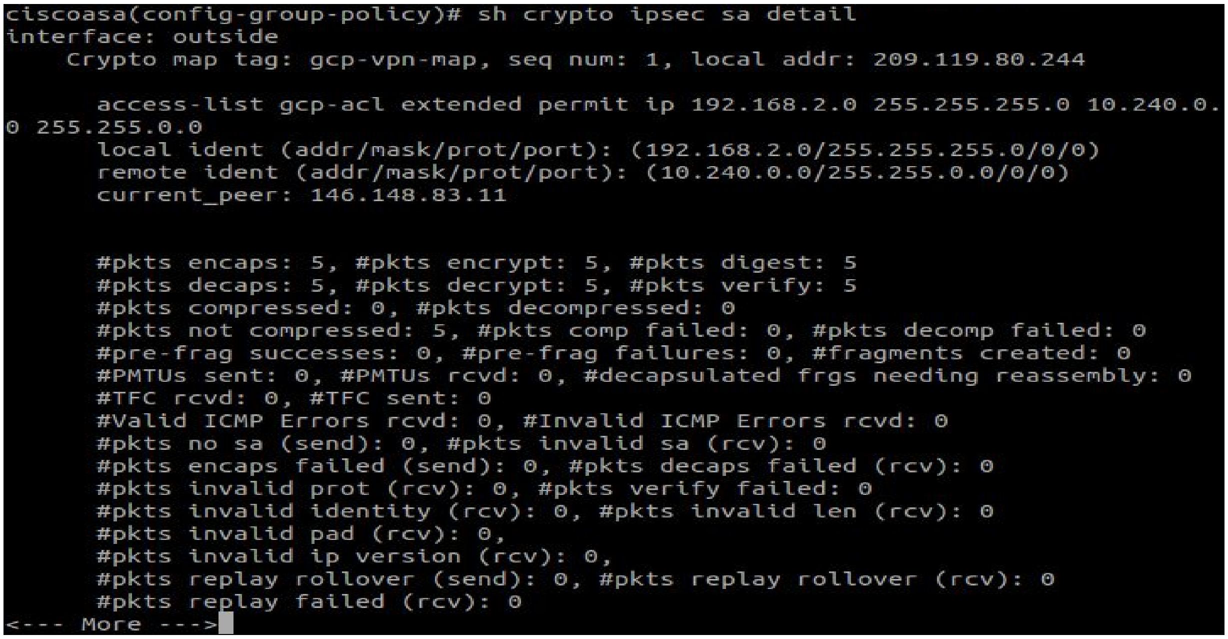


```
ciscoasa(config)# sh crypto ikev2 sa detail

IKEv2 SAs:

Session-id:1619, Status:UP-IDLE, IKE count:1, CHILD count:0

Tunnel-id                 Local                 Remote     Status         Role
3338134991    209.119.80.244/500     146.148.83.11/500      READY    RESPONDER
      Encr: AES-CBC, keysize: 256, Hash: SHA96, DH Grp:2, Auth sign: PSK, Auth v
erify: PSK
      Life/Active Time: 28800/37 sec
      Session-id: 1619
      Status Description: Negotiation done
      Local spi: EF5D07B96BCBC9F2       Remote spi: 84035E3FAEE78F4F
      Local id: 209.119.80.244
      Remote id: 146.148.83.11
      Local req mess id: 0              Remote req mess id: 14
      Local next mess id: 0             Remote next mess id: 14
      Local req queued: 0               Remote req queued: 14
      Local window: 1                   Remote window: 1
      DPD configured for 10 seconds, retry 2
      NAT-T is not detected
ciscoasa(config)#
```

Verify IPsec SA

To check on the status of the IPsec security associations use the **sh crypto** command:

```
sh crypto ipsec sa detail
```



```
ciscoasa(config-group-policy)# sh crypto ipsec sa detail
interface: outside
    Crypto map tag: gcp-vpn-map, seq num: 1, local addr: 209.119.80.244

      access-list gcp-acl extended permit ip 192.168.2.0 255.255.255.0 10.240.0.
0 255.255.0.0
      local ident (addr/mask/prot/port): (192.168.2.0/255.255.255.0/0/0)
      remote ident (addr/mask/prot/port): (10.240.0.0/255.255.0.0/0/0)
      current_peer: 146.148.83.11


      #pkts encaps: 5, #pkts encrypt: 5, #pkts digest: 5
      #pkts decaps: 5, #pkts decrypt: 5, #pkts verify: 5
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 5, #pkts comp failed: 0, #pkts decomp failed: 0
      #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
      #TFC rcvd: 0, #TFC sent: 0
      #Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
      #pkts no sa (send): 0, #pkts invalid sa (rcv): 0
      #pkts encaps failed (send): 0, #pkts decaps failed (rcv): 0
      #pkts invalid prot (rcv): 0, #pkts verify failed: 0
      #pkts invalid identity (rcv): 0, #pkts invalid len (rcv): 0
      #pkts invalid pad (rcv): 0,
      #pkts invalid ip version (rcv): 0,
      #pkts replay rollover (send): 0, #pkts replay rollover (rcv): 0
      #pkts replay failed (rcv): 0
<--- More --->
```

Packet Tracer

In addition, for more advanced troubleshooting, Cisco provides a packet-tracer utility:

```
packet-tracer input < internal interface name> icmp x.x.x.x 8 0 y.y.y.y detailed
```

Where:

- < internal interface> = the name on the interface where the internal machine is located.
- x.x.x.x = IP of the internal host
- y.y.y.y = IP or remote host

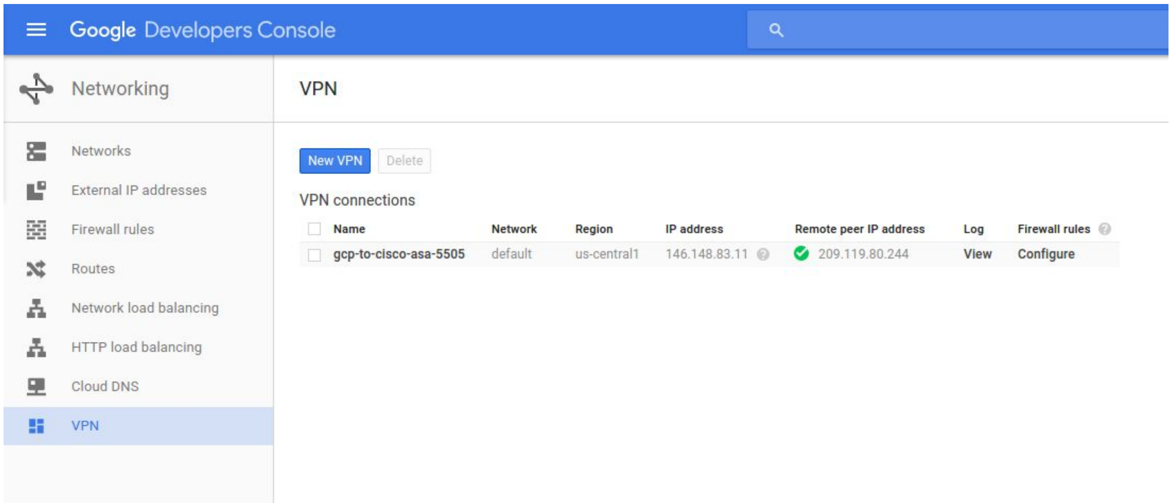
Sample output is provided below:

```
Phase: 1
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
 Forward Flow based lookup yields rule:
 in  id=0xd9a222d0, priority=1, domain=permit, deny=false
       hits=33344865, user_data=0x0, cs_id=0x0, l3_type=0x8
       src mac=0000.0000.0000, mask=0000.0000.0000
       dst mac=0000.0000.0000, mask=0100.0000.0000
       input_ifc=inside, output_ifc=any

Phase: 2
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
in   0.0.0.0         0.0.0.0         via 209.119.81.230, outside

Phase: 3
Type: UN-NAT
Subtype: static
Result: ALLOW
Config:
nat (inside,outside) source static inside_subnets inside_subnets destination static
broad-subnet broad-subnet no-proxy-arp route-lookup
Additional Information:
NAT divert to egress interface outside
Untranslate 10.197.0.2/0 to 10.197.0.2/0

Phase: 4
```

```
Type: ACCESS-LIST
Subtype:
Result: DROP
Config:
Implicit Rule
Additional Information:
 Forward Flow based lookup yields rule:
 in  id=0xd9a2ecc0, priority=500, domain=permit, deny=true
       hits=0, user_data=0x6, cs_id=0x0, reverse, flags=0x0, protocol=0
       src ip/id=192.168.2.1, mask=255.255.255.255, port=0, tag=0
       dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=0, dscp=0x0
       input_ifc=inside, output_ifc=any

Result:
input-interface: inside
input-status: up
input-line-status: up
output-interface: outside
output-status: up
output-line-status: up
Action: drop
Drop-reason: (acl-drop) Flow is denied by configured rule
```

Verifying the GCP Configuration

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



□	Name	Network	Region	IP address	Remote peer IP address	Log	Firewall rules
□	gcp-to-cisco-asa-5505	default	us-central1	146.148.83.11	✓ 209.119.80.244	View	Configure